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

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.

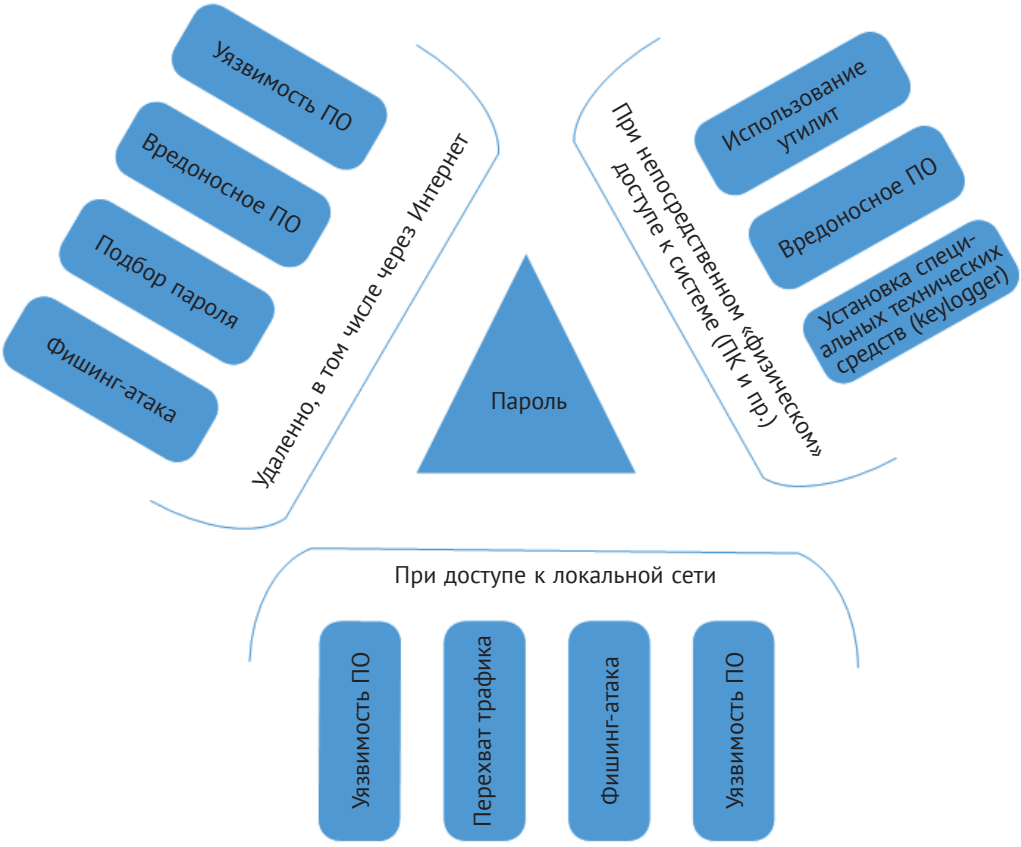

Рис. 1.1. Способы несанкционированного получения учетных данных

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.