ориентирован на киберзащиту. Киберзащита также является областью, где НАТО поддерживает Иорданию, в рамках технической помощи в области обороны и укрепления оборонного потенциала.

1.5. Киберпреступления и киберпреступники – классификация, методы «работы» и способы защиты

1.5.1. Классификация киберпреступников

В качестве введения следует отметить, что на момент выхода книги не существует всеобъемлющей классификации как самих киберпреступлений, так и осуществляющих их исполнителей (киберпреступников).

Поэтому здесь мы приведем только наиболее часто используемые экспертами термины и определения.

Начнем с того, что существует три основных термина – ***хакер***, ***фрикер*** и ***кракер***.

Хакер (Hacker) – индивидуум, который получает удовольствие от изучения деталей функционирования компьютерных систем и от «расширения их возможностей».

Кракер (Craker) – имеет основной задачей непосредственное осуществление процессов «взлома» компьютерной системы с целью получения несанкционированного доступа к чужой информации (кражи, подмены, шантажа).

Фрикер (Frecker) – это телефонный грабитель, занимающийся «выкачиванием» денег из клиентов телефонных компаний.

В свою очередь хакеры делятся на следующие типы (виды): «Белые шляпы», «Черные шляпы», «Серые шляпы», «Суицидники», «Скрипт-кидди», «Наемники», «Госнаемники».

В отличие от киберпреступников – *«Черных шляп»* (Black hat), *«Белые шляпы»* – это не киберпреступники, а обычные специалисты по ИТ-безопасности, в том числе работающие в крупных ИТ-компаниях, а также исследователи систем, ***не нарушающие закон***.

«Серые шляпы» (Gray hat) – это обычно исполнители мелких нарушений законодательства или нарушители каких-либо внутренних правил любого интернет-сервиса.

Фишеры (phishing, от *fishing* – рыбная ловля, выуживание, и *password* – пароль) – занимаются таким видом интернет-мошенничества, цель которого – получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и прочее.

Атаки фишеров становятся все более продуманными, применяются методы социальной инженерии. Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию.

Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении («если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован»). Забавно, но часто в качестве причины, по которой пользователь якобы должен выдать конфиденциальную информацию, фишеры называют необходимость улучшить антифишинговые системы («если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль»).

Дропперы (Dropper – бомбосбрасыватели) – это программы, которые скрытно устанавливают вредоносное ПО, встроенное в их код, на компьютер. Обычно программы загружаются на компьютер жертвы, сохраняются и запускаются без уведомления (или с ложным уведомлением). Дропперы используются для скрытной установки других вредоносных программ или для того, чтобы помочь таким программам избежать обнаружения (не каждая защитная программа способна проверить все компоненты внутри дроппера).

Дудосеры – человек, который организует и реализует DoS-атаки на серверы и сайты.

Ордеры – это люди, специализирующиеся на снятии денег с чужих карт.

Заливщик (ливщик) может детально «зарабатывать» до 1 млн евро в месяц. Этот вид киберпреступности ниже мы рассмотрим более подробно как один из наиболее распространенных.

Ботоводы – это люди, которые целенаправленно программными методами «накручивают» на свой (или чужой) канал подписчиков и просмотры. Ботовод – необязательно хозяин канала, бота или владелец сервиса по «накрутке». Но в мире Telegram-каналов *ботоводами называют людей, которые пользуются услугами сервисов накрутки*. Бот – это обычный аккаунт, у которого по ту сторону экрана находится не человек, а обычный скрипт. Бот ничего не покупает, не читает, не взаимодействует и не проявляет активность, пока скрипт не «попросит» что-либо сделать – подписаться, посмотреть пост, лайкнуть, написать. На момент выхода книги это наиболее распространенный метод борьбы с конкуренцией.

1.5.2. Классификация компьютерных преступлений по Интерполу

В 1991 году кодификатор «по Интерполу» был интегрирован в автоматизированную систему поиска и в настоящее время доступен подразделениям Национальных центральных бюро Международной уголовной полиции «Интерпол» более чем 120 стран мира.

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного[5].

QA – Несанкционированный доступ или перехват
QAH – компьютерный абордаж
QAI – перехват
QA1 – кража времени
QAZ – прочие виды несанкционированного доступа и перехвата

QD – Изменение компьютерных данных
QDL – логическая бомба
QDT – троянский конь
QDV – компьютерный вирус
QDW – компьютерный червь
QDZ – прочие виды изменения данных

QF – Компьютерное мошенничество (computer fraud)
QFC – мошенничество с банкоматами
QFF – компьютерная подделка
QFG – мошенничество с игровыми автоматами
QFM – манипуляции с программами ввода/вывода
QFP – мошенничества с платежными средствами
QFT – телефонное мошенничество
QFZ – прочие компьютерные мошенничества

QR – Незаконное копирование («пиратство»)
QRG – компьютерные игры
QRS – прочее программное обеспечение
QRT – топография полупроводниковых изделий
QRZ – прочее незаконное копирование

QS – Компьютерный саботаж
QSH – с аппаратным обеспечением
QSS – с программным обеспечением
QSZ – прочие виды саботажа

QZ – Прочие компьютерные преступления
QZB – с использованием компьютерных досок объявлений
QZE – хищение информации, составляющей коммерческую тайну
QZS – передача информации конфиденциального характера
QZZ – прочие компьютерные преступления

Несанкционированный доступ – неправомерный доступ к компьютерной системе или сети путем нарушения охранных мер.

Несанкционированный перехват – неправомерный и осуществленный с помощью технических средств перехват сообщений, приходящих в компьютерную систему или сеть, исходящих из компьютерной системы или сети и передаваемых в рамках компьютерной системы или сети.

Изменение компьютерных данных – неправомерное изменение компьютерных данных.

Компьютерное мошенничество – введение, изменение, стирание или подавление компьютерных данных или компьютерных программ или иное вмешательство в процесс обработки данных, которое влияет на результат обработки данных, что причиняет экономический ущерб или приводит к утрате собственности другого лица, с намерением получить незаконным путем экономическую выгоду для себя или для другого лица.

Компьютерный саботаж – введение, изменение, стирание или подавление компьютерных данных или компьютерных программ или создание помех ком-

пьютерным системам с намерением воспрепятствовать работе компьютера или телекоммуникационной системы.

1.5.3. Детализированный алгоритм типовой кибератаки

Рассмотрим перечень и содержание основных этапов стандартной кибератаки, имеющей целью ***кражу информации*** [https://cyberpedia.su/8x101d4.html].

Этап 1. Инвентаризация

Первый шаг в процессе создания перечня (инвентаризации) сети состоит в идентификации доменных имен и связанных с ними сетей, относящихся к данной организации. Доменные имена характеризуют присутствие в Интернете и являются сетевыми эквивалентами названия компании. Существует множество баз данных, которые можно опросить для получения необходимой информации.

Разные запросы предоставляют различную информацию. Основная часть сведений, используемых злоумышленниками в начале атаки, определяется запросами следующих типов:

- организационный. Выводит всю информацию, относящуюся к конкретной организации;
- доменный. Выводит всю информацию, относящуюся к конкретному домену;
- сетевой. Выводит всю информацию, относящуюся к конкретной сети или к одному IP-адресу;
- контактный. Выводит всю информацию, относящуюся к конкретному лицу, обычно – к ответственному сотруднику организации.

Этап 2. Опрос DNS

После определения всех связанных доменов можно начать опрос DNS (Domain Name Service – служба доменных имен). DNS представляет собой распределенную базу данных, используемую для отображения IP-адресов на имена сетевых компьютеров и наоборот. Если DNS сконфигурирована без учета требований зашиты, важная информация об организации становится доступной.

Пересылка «файла зоны» – наиболее уязвимое звено для киберпреступника.

Одной из наиболее серьезных ошибок конфигурации, которую может сделать системный администратор, является разрешение ненадежным пользователям Интернета выполнять пересылку зон DNS.

Пересылка файла зоны (zone transfer) позволяет вторичному управляющему серверу обновлять свою базу данных о зонах, по запросам к первичному управляющему серверу. Это делается для повышения надежности (резервирования) DNS на случай отказа первичного сервера имен. Обычно пересылку зоны DNS достаточно выполнять только на вторичных управляющих серверах DNS. Однако многие серверы DNS сконфигурированы неверно, поэтому выдают копию зоны любому, кто ее запросит. Это не так плохо, если выводятся только информация о подключенных к Интернету системах и реальные имена сетевых компьютеров, хотя поиск потенциальных целей для атаки упрощается. Настоящая проблема возникает тогда, когда организация не пользуется механизмом общих, личных DNS для отделения внешней информации DNS (которая является общедоступной) от своей внутренней (личной, частной)

информации. В этом случае атакующим раскрываются имена и IP-адреса внутренних сетевых компьютеров. Предоставление в Интернете информации о внутренних IP-адресах ненадежному пользователю аналогично предоставлению полной схемы или дорожной карты внутренней сети организации.

Этап 3. Разведка сети

После идентификации сетей злоумышленник пытается определить их топологию, а также потенциальные пути доступа.

Сканирование

Если рекогносцировка – это поиск источников информации, то сканирование – это обнаружение уязвимостей систем. Во время рекогносцировки атакующий получает: имена и телефоны сотрудников, диапазоны IP-адресов, серверы DNS и почтовые серверы. Теперь он определяет, какие системы достижимы из Интернета, с помощью утилит диапазонной проверки по ping, сканирования портов и автоматизированных средств исследования.

Сканирование портов

Применив диапазонное зондирование ICMP или TCP, злоумышленник находит функционирующие (живые) системы и при этом собирает некоторую полезную информацию. Затем приступает к *сканированию портов* каждой системы. Сканирование портов представляет собой процесс подключения к портам TCP и UDP исследуемой системы с целью выявления работающих служб или состояния порта LISTENING (прослушивание).

Идентификация «слушающих портов» важна в определении типа операционной системы и используемых приложений. Активные «слушающие» службы могут позволить неавторизованному пользователю получить доступ к системам с неправильной конфигурацией или к версиям программных продуктов с известными слабыми местами в защите.

Итак, существует множество средств и методов сканирования портов. Основная цель при сканировании портов состоит в выявлении слушающих портов TCP и UDP исследуемой системы. Вторая цель – определение типа сканируемой операционной системы. Конкретная информация об операционной системе используется на этапе построения «карты слабых мест». Требуется максимальная точность в выявлении уязвимых мест исследуемой системы или систем. Поэтому нужна определенная степень уверенности в том, что удастся идентифицировать операционную систему целевого объекта. Применяют методы захвата заголовков, которые извлекают информацию из служб FTP, telnet, SMTP, HTTP, POP и др. Это простейший способ определения операционной системы и соответствующего номера версии работающей службы.

Способы, которые могут быть использованы *для идентификации* операционной системы:

- проба пакетом FIN. На открытый порт посылается пакет FIN. Правильным поведением будет отсутствие ответа, однако многие реализации стека (например, в Windows NT) отправляют в ответ сообщение FIN/ACK;
- проба фальшивым флагом. В заголовке TCP пакета SYN устанавливается неопределенный флаг TCP. Некоторые операционные системы (например, Linux) передают установленный флаг в ответном пакете;

– выборка начального последовательного номера (ISN, Initial Sequence Number). Основная предпосылка состоит в поиске шаблона для начальной нумерации, применяемого в реализации TCP при отклике на запрос соединения;
– мониторинг бита запрета фрагментации (DF, Do not Fragment). Некоторые операционные системы для повышения производительности устанавливают бит (флаг) запрета фрагментации. Проверка этого бита позволяет определить тип операционной системы;
– начальный размер окна TCP. Отслеживается начальный размер окна в возвращаемых пакетах. Для некоторых реализаций стека это значение уникально и может существенно повысить точность идентификации;
– значение ACK. Стеки IP отличаются значением последовательного номера (Sequence Number), используемым для поля ACK (некоторые реализации посылают в ответ тот же номер, а другие– номер плюс один);
– подавление сообщений об ошибках ICMP;
– выборки информации сообщений об ошибках ICMP. Операционные системы отличаются объемом информации, которую они посылают в ответ на ошибки ICMP. Проверяя возвращенное сообщение, можно сделать некоторые предположения о типе операционной системы;
– целостность ответных сообщений об ошибках ICMP. Некоторые реализации стека изменяют заголовки IP в возвращаемых сообщениях об ошибках ICMP. Проверяя изменение заголовка, можно сделать некоторые предположения об операционной системе;
– тип службы (ToS, Type of Service). Большинство реализаций стека помещает в это поле значение 0, однако оно может варьироваться;
– обработка фрагментов. При повторной сборке пакета некоторые стеки переписывают новые данные поверх старых, а некоторые наоборот. Выяснив, как были собраны тестовые пакеты, можно сделать определенные предположения об операционной системе хоста;
– параметры TCP. Посылая пакеты несколькими параметрами (такими, как «нет операции», максимальный размер сегмента, коэффициент масштаба окна или метка времени), можно сделать некоторые предположения об операционной системе.

Этап 4. Составление карты

Далее злоумышленник составляет карту (план) своих последующих действий, где определяет конкретные цели, задачи и мотивы своего деяния.

После этого злоумышленник переходит на стадию совершения КП, где его действия уже нарушают законодательство РФ и других стран.

Этап 5. Получение доступа

Имея определенные цели, мотивы и задачи, киберпреступник получает доступ к объекту. На стадии получения доступа злоумышленник решает проблемы обхода систем защиты объекта, а также получения доступа к интересующему информационному ресурсу с минимальными правами.

Варианты получения доступа к объекту, то есть взлом системы, подробно представлены в зарубежной литературе: Макклур С., Скембрей Д., Куртц Дж., в российской литературе – Левина М.

Получив доступ к объекту с ограниченными правами, злоумышленник при помощи специализированных утилит производит эскалацию своих привилегий, т.е. расширяет свои полномочия.

Этап 6. Расширение полномочий

Чтобы получить информацию со взломанной машины и остальной части сети, необходимо расширить привилегии до статуса более мощной учетной записи.

Этот процесс называется *расширением привилегий*. Этот термин в общих чертах описывает процесс расширения возможностей владельца текущей учетной записи пользователя до возможностей более привилегированной учетной записи, такой как учетная запись администратора или запись SYSTEM. С точки зрения преступника, взлом учетной записи пользователя и последующая атака по расширению привилегий может быть проще, чем поиск на удаленной системе уязвимого места, которое сразу же могло предоставить права уровня суперпользователя. В любом случае, прошедший аутентификацию злоумышленник, скорее всего, будет иметь в своем распоряжении больше ресурсов, чем тот, кто не прошел аутентификацию, независимо от уровня привилегий.

В Windows каждый субъект доступа обладает некоторым (возможно, пустым) набором привилегий. Привилегии представляют собой права на выполнение субъектом действий, касающихся системы в целом, а не отдельных ее объектов.

Существуют следующие *привилегии* (наиболее основные):

- архивирование файлов и каталогов;
- завершение работы операционной системы и перезагрузка компьютера;
- изменение системного времени;
- доступ к компьютеру из сети;
- разрешение локального входа;
- отладка программ;
- принудительное удаленное завершение работы;
- загрузка и выгрузка драйверов устройств;
- управление аудитом и журналом безопасности;
- создание файла подкачки;
- увеличение приоритета диспетчирования;
- изменение параметров среды;
- смена владельца файлов или иных объектов;
- создание журналов безопасности.

При входе в систему пользователь (преступник) получает привилегии, а затем расширяет их до уровня, необходимого для решения поставленных целей.

Некоторые из перечисленных привилегий позволяют злоумышленнику, обладающему ими, преодолевать те или иные элементы защиты операционной системы. Рассмотрим эти привилегии.

- Привилегия создавать резервные копии информации позволяет пользователю игнорировать разграничение доступа при чтении файлов, директорий, ключей и значений реестра. Аналогично – восстанавливать.

– Привилегия назначать процессам высокий приоритет позволяет пользователю «завесить» операционную систему, создав процесс с высоким приоритетом и введя его в вечный цикл.
– Пользователь, обладающий привилегией изменять системные переменные среды, может, изменив значения переменных path и windir, добиться того, чтобы поиск операционной системой исполняемых модулей для загрузки начинался с личной директории пользователя. Если затем пользователь поместит в эту директорию под именем одной из системных библиотек программную закладку, при первом же обращении операционной системы к данной библиотеке данная программная закладка будет запущена с полномочиями системного процесса.
– Привилегия отлаживать программы позволяет пользователю обращаться к любому процессу по любому методу доступа. В частности, программа, запущенная таким пользователем, может изменить произвольным образом содержимое адресного пространства любого процесса операционной системы, что предоставляет такому пользователю практически неограниченные полномочия.
– Привилегия загружать и выгружать драйверы и сервисы позволяет пользователю выполнять произвольный код от имени и с правами операционной системы (псевдопользователя SYSTEM). Пользователь может внедрять в операционную систему программные закладки под видом драйверов и сервисов. Учитывая, что драйверы устройств Windows NT могут игнорировать большинство защитных функций операционной системы, эта привилегия дает обладающему ею субъекту практически неограниченные полномочия.
– Привилегия аудитора позволяет пользователю маскировать свои несанкционированные действия, изменяя политику аудита таким образом, чтобы эти действия не регистрировались.
– Привилегия добавлять записи в журнал аудита (создание журналов безопасности) позволяет пользователю записывать в журнал аудита произвольную информацию, в том числе и информацию, компрометирующую других пользователей.

Расширение привилегий – это очень мощный вид атак, которые используются для повышения уровня прав учетной записи пользователя до уровня администратора.

Этап 7. Кража информации

После расширения полномочий до необходимого злоумышленнику уровня он производит кражу информации, которая и является конечной целью его многоэтапной атаки.

1.5.4. «Залив денег на карту быстро и без предоплаты» – тонкости профессий заливщика, рефорда и ботовода

В современных социальных сетях (Одноклассники, Фейсбук, ВКонтакте) сегодня существует множество групп и сообществ по ***заливу денег на карту***.

«Залив» – это жаргонное выражение. Оно означает *перевод денежных средств с одного счета на другой*. Заливщик предлагает перевести на банковскую карту любую запрашиваемую человеком сумму. Или, проще говоря, сделать залив денег на карту

быстро. При этом обещает 100%-ный результат в течение 15–20 минут. Например, человеку требуется хоть какая-то сумма, чтобы дожить до зарплаты, и он вынужден обратиться к заливщику.

В популярном блоге «Бизнес в Интернете» Жук Александра [https://help-zarabotok.ru/zaliv-deneg-na-kartu-bystro-i-bez-predoplaty.html] подробно описан механизм «работы» таких заливщиков. Приведем ниже максимально близко к тексту ту часть материалов блога, которая на понятном простому пользователю Интернета языке описывает механизмы работы «заливщиков».

Итак, в социальных сетях заливщик обязуется «залить деньги» любому обратившемуся клиенту от 100 000 рублей и выше. Откуда у него такие деньги? Все просто. Один заливщик не скрывает, что взломал банковские счета и делится деньгами с людьми. Другой заливщик сообщает, что работает со списанными банковскими картами. Якобы на списанных картах остаются деньги, он их извлекает и безвозмездно раздает людям. Так в чем суть «развода»?

Как правило, обратившийся к заливщику «клиент» говорит, что ему не надо так много денег, примерно тысяч 10–20 хватит. Заливщик отвечает, что с такими «мелкими» суммами не работает и начинает психологически «давить» на человека, чтобы вызвать доверие.

Обычно заливщик на этом этапе использует следующие приемы.

1. Если вам нужны деньги, то работаем. Если отказываетесь, то прощаемся.
2. У меня мало времени на разговоры, люди в очереди ждут залива.
3. Всяческими способами показывает свою занятость. Например, долго не отвечает на сообщение человека.
4. Выкладывает фотки с пятитысячными купюрами, которые веером разложены на его столе.
5. Показывает скрины положительных отзывов от других людей.

После этих убедительных манипуляций человек соглашается на крупную сумму. Более жадный человек без промедления соглашается на залив денег. На лету ловит каждое слово заливщика, даже не дочитывает до конца его предложения.

И здесь наступает кульминационный момент. Заливщик сообщает, что нужно произвести ПРЕДОПЛАТУ (процент от заливаемой суммы). Процент устанавливает сам заливщик якобы для гарантии. Это может быть 10%, а может быть 30%. В среднем сумма предоплаты за залив денег на карту составляет от полутора до пяти тысяч российских рублей.

«Клиент» должен перечислить предоплату на указанный заливщиком реквизит. Условия залива денег на карту таковы, что это нужно сделать до момента залива денег на карту. После чего ждать несколько минут залив денег на оговоренную двумя сторонами сумму. Одни заливщики заранее говорят, что надо обязательно снять поступившую сумму. Другие этого не требуют. Просто просят перевести их процент на определенный реквизит.

Сегодня залив денег на карту весьма популярная услуга. Заливщиков в Интернете много, у каждого из них свои условия. Одни требуют предоставить паспорт. Другим не нужен документ. Третьи просят паспорт и фото на фоне личной страницы в соцсети. Аргументируют тем, что хотят иметь дело только с реальными людьми, а не фейками.

Далее происходит процесс залива денег на карту, и наступают «последствия».

Человек произвел предоплату заливщику и сидит, ждет чуда. В течение 10–15 минут заливщик отвечает ему, что программа обрабатывает вывод денежных средств. Просит подождать еще немного.

После 30 минут ожидания «клиент» опять пишет заливщику, Мошенник уже «исчез с горизонта» – просто прикарманил себе деньги и занес человека в черный список. Никакого залива денег на карту обманутый человек не получил. В этом процессе зарабатывают только сами мошенники.

Однако существуют и ***реальные заливщики***, схему работы которых популярно объясняет вышеупомянутый блогер Жук.

Они на самом деле существуют, но значительно отличаются от вышеописанных *мошенников*. Схема залива денег на карту у них другая. Как хорошо знают сотрудники соответствующих управлений МВД и ФСБ, в настоящее время орудуют большие организованные группы высокопрофессиональных киберпреступников. Они «по-настоящему» грабят банки, используя различные доступы к базам данных. Но поскольку сегодня любая банковская операция фиксируется в системе, эти преступники придумали самый лучший способ для «отмывки» денег – залив денег на карту.

Действия «настоящих» заливщиков отличаются от «мошенников»-заливщиков. Они:

– Никогда не просят паспортные данные.
– Переводят обговоренную сумму очень быстро, 5–10 минут.
– Ни за что на свете не признаются, откуда у них такие огромные суммы.
– Просят только номер банковской карты и ничего более.
– Предлагают перевести залив денег на несколько карт, имеющихся у человека.
– Никогда не просят предоплату.
– Не демонстрируют пачки денег в руках.
– Не допускают комментирования их залива.

После того как залив денег на карту прошел успешно и деньги на карту «клиенту» переведены, он требует вернуть назад 70% от суммы. *Оставшиеся деньги 30% остаются у человека*. Таким образом, украденные деньги поступили на счет «клиенту», а заливщик остался чистым перед лицом закона. Однако абсолютное большинство клиентов не понимают, что с того момента, как он пошел к банкомату снять залитые (сворованные) деньги, *он стал соучастником преступления*. След на отмытые деньги ведет к тому, кто получил залив, и современные «киберсыщики» рано или поздно придут по этому следу.

Итак, в первом случае «залив денег на карту» вы попрощаетесь со своими деньгами, а залива не получите. Во втором случае деньги получите, но вполне можете оказаться в тюрьме с большим сроком за преступление. И вы никогда не докажете, кто перевел вам эти деньги. Служба безопасности банка моментально устанавливает связь именно с владельцем карты.

И в заключение этого краткого обзора рассмотрим относительно недавно возникшую и стремительно набирающую активность в соцсетях категорию кибермошенников – ***рефоводы*** и их разновидности.

В основе деятельности рефоводов лежит такое понятие, как хайп.

В хайпах основным инструментом продвижения (реклама, «раскручивание» проектов) является *реферальная система*, основанная на деятельности многочис-

ленных рефоводов, лоховодов и ботоводов. В основном, это профессионалы, размещающие свои реферальные ссылки на различные проекты в наиболее популярных информационных ресурсах, соцсетях, форумах, блогах.

В этом «высокотехнологичном бизнесе» часто используют два основных сетевых термина, которые произошли от английского слова ***reference – ссылка***.

1. ***Рефералы*** – это привлеченные в хайп через реферальные ссылки новые инвесторы, сделавшие финансовые вложения в проект с целью получения прибыли.
2. ***Рефоводы*** – это зарегистрированные пользователи интернет-проекта, получившие ссылки и материалы рекламного характера, размещающие их в сети и получающие доход от инвестиций приведенных рефералов.

Эти два термина связаны с конкретным методом привлечения инвесторов, который осуществляется путем перехода потенциального клиента по предложенной рефордом ссылке.

Термин ***хайп*** (HYIP) ***«Yield Investment Program»*** означает высокодоходную инвестиционную программу.

В интернете существует целая ***хайп-индустрия***, когда инвесторы попадают в проекты через распространенные ссылки. В принципе – это своеобразная ***финансовая пирамида***, в которой администраторы проектов «делятся» доходом с рефоводами и рефералами.

Хотя в Интернете работают тысячи реальных хайпов, на которых реально можно заработать, но в этой сфере действуют и много мошеннических групировок, где вкладчики реально теряют средства, а псевдопроекты и лоховоды – зарабатывают.

Лоховоды (*псевдолидеры*) – это те не менее многочисленные пользователи Сети, которые обманным путем приглашают инвесторов в так называемые скам-проекты (давно не делающие выплат по каким-либо обстоятельствам).

С ростом количества проектов прогрессируют как сами лоховоды, так и их пирамидальные схемы. *Цель лоховодов – заработок на инвесторах, привлеченных в скам-проекты.*

Необходимо отметить, что для получения прибыли от хайпа лоховоды используют идентичные инструменты продвижения, а именно: рекламу и реферальные ссылки.

По сути рефералы, зарегистрировавшись по ссылкам рефоводов и вложив реальные *финансовые* средства в проект, должны получать реальный доход, его отсутствие свидетельствует о попадании инвесторов на «уловки» лоховодов.

Если рефоводы очень серьезно подходят к выбору проектов, то лоховоды обычно рекламируют «все подряд».

В свою очередь лоховодов (псевдолидеров) условно можно разделить на три группы.

1. Лоховоды, вымышляющие *условный токен и токенсейл*, привлекающие с их помощью потенциальных инвесторов уверениями в выгодности вложений и «сворачивающие» проект сразу же после сбора приличной суммы.
2. Неосознанные лоховоды – приглашающие своих знакомых и «знакомых знакомых» в проекты, не убедившись, платят они или нет.
3. Лоховоды, стремящиеся привлечь максимум инвесторов, чтобы самим больше заработать, но искренне не знающие, что проект не будет оплачен.

Опытные лоховоды действуют через *чаты и блоги* в социальных сетях, причем даже некоторые из них проводят *семинары и вэбинары*. Иногда бывают так убедительны, что на их уловки попадаются даже юридически грамотные инвесторы. Однако в большинстве случаев основная их цель – ***новички***. *Лоховоды*, в отличие от *рефоводов*, лгут, что вложения 100%-ю прибыльные, убеждая в этом потенциальных инвесторов.

Как и в любой финансовой пирамиде, в этом случае также данежные перечисления ранее привлеченным инвесторам делаются из вкладов, внесенных новыми. Поэтому такой хайп реально не будет работать без постоянного присоединения всех вкладчиков и сохранения старых, участвующих в реинвестах. Понятно, что здесь необходим регулярный приток средств, которому способствует работа рефоводов. Такая стратегия – основа долгого существования прибыльных хайпов.

На сайте блога (https://my-busines.ru/useful/refovody-kto-jeto-takie-refovody-byvajut-lohovody-i-botovody-otkrytye-i-anonimnye) можно прочитать определения еще одной разновидности интернет-бизнесменов – ***рефоводы-ботоводы***.

Понятия «роботы» (боты), «интернет-боты» естественным путем образовались от двух слов от чешского – ***robot*** и английского – ***bot***. Это программы, работающие через интерфейс *автоматически* или по определенному ботоводами времени.

Ботоводы – это разновидность рефоводов, непосредственно не занимающаяся помощью *рефералам* и общением с ними. Осуществляют размещение рекламы с реферальными ссылками в блогах, заполняемых с помощью ботов и программ массового постинга. В случае недостатка материалов на все заданные ресурсы боты размещают «запощенные» до полного их заполнения (берут не качеством информации, а количеством).

Ботоводы вкладывают средства в массовые закупки рекламы в соцсетях, форумах, посещаемых ресурсах. На них размещают свои реферальные ссылки в виде баннеров, видеороликов, «цепляющих» статей, «тизеров». Через клик по ним автоматически происходит перенаправление на хайпы, где заинтересованные пользователи делают свои депозиты. Рефералы, как правило, даже никогда не связываются с аплайном, распространившим ссылку, часто даже не подозревая, что сами ими являются.

К ботоводам также можно отнести и вышеупомянутых спамеров, рассылающих надоедливую рекламу не заинтересованным в этом людям.

Еще одна разновидность рефоводов, ***рефбек*** – это своеобразная гарантия рефералам в виде дополнительного дохода к прибыли от хайпа, его сумму определяют рефоводы. Администраторы хайпов всегда заинтересованы в грамотных рефоводах, поэтому оплачивают им повышенную реферальную комиссию, которой они и делятся с привлеченными ими инвесторами.

Юридическое право на рефбек имеют пользователи, официально зарегистрировавшиеся по реферальным ссылкам блогеров и внесшие свой депозит.

Рефбек – это достаточно эффективный легальный инструмент привлечения аудитории в проекты. Но не желая делиться своими средствами за выполненную работу, часть рефоводов предпочитают их не платить, хотя многие отдают рефералам до 50–70% своего личного заработка.

Открытость привлекает пользователей, поэтому среди рефоводов, показывающих свое лицо, основная часть – лоховоды, афиширующие фото и видео, имитирующие богатую жизнь.

Открытые рефоводы иногда показывают себя в видео о проектах и семинарах.

В основном все субъекты хайп-индустрии стараются соблюдать анонимность – не показывать лица, не сообщать адреса. Администраторы хайпов часто используют не свои фотографии, банковские карты и компании-однодневки.

Не афишируют себя и обычные инвесторы, используя для регистрации в проектах неверные данные.

Любой хайп станет скамом, поэтому для защиты репутации практикуется анонимность.

Как можно теперь понять из всего вышеизложенного, грань между *рефоводами, лоховодами и ботоводами* весьма условная. Рефоводы, размещая свои ссылки и баннеры, превращаются в ботоводов, а умолчав о проблемах проекта – в лоховодов. Последние могут продвигать не только скамы, но и прибыльные проекты.

1.5.5. Пример эффективного расследования киберпреступлений: взлет и падение русскоязычного хакера Fxmsp

1.5.5.1. Компания Group-IB – расследование и предотвращение киберпреступлений как важный компонент кибербезопасности

На момент выхода этой книги в мире существует уже несколько сотен средних и крупных компаний, специализирующихся исключительно на расследованиях и предотвращениях киберпреступлений и мошенничеств с использованием высоких технологий. Этот вид деятельности становится весьмо прибыльным бизнесом. Но и конкуренция на этом высокоинтеллектуальном рынке весьма высока.

В качестве типового примера представителя этого перспективного бизнеса здесь следует привести российскую компанию Group-IB, ставшую одной из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств.

Компания была основана Ильей Сачковым в 2003 году, штаб-квартира расположена в Москве. За 15 лет работы сотрудники Group-IB совместно с российскими и международными правоохранительными органами провели более 1000 расследований в 30 странах мира, 150 дел закончились для киберпреступников тюремными сроками. При участии криминалистов Group-IB были разоблачены несколько преступных групп, а их участники оказались за решеткой (Cron, Carberp, Hodprod, Germes).

Group-IB начинала работу с расследований киберпреступлений и компьютерной криминалистики. Полученный опыт и уникальные знания легли в основу высокотехнологичных продуктов, позволяющих не только эффективно расследовать, но и предотвращать киберпреступления. С помощью рассмотренной нами в одной из глав этой книги системы кибербразведки Threat Intelligence (мониторинг, анализ и прогнозирование угроз для компании) клиенты компаний оперативно получают информацию о киберугрозах – жизненно важный компонент эффективной защиты и бизнеса.

В 2015 году Group-IB стала единственной российской компанией в отчете аналитического агентства Gartner о рынке Threat Intelligence. В том же году компания названа в числе 7 самых влиятельных игроков в сфере информационной безопас-

ности по версии британской редакции издания Business Insider. В 2017-м международная компания IDC назвала Group-IB лидером российского сегмента этого рынка, а Forrester Research в отчете о мировом рынке Threat Intelligence оценило продукт Group-IB в 9 баллов из 10.

Лаборатория компьютерной криминалистики и исследования вредоносного кода Group-IB названа крупнейшей в Восточной Европе. В октябре 2011 года Group-IB первой в России открыла частный CERT-GIB – (Computer Emergency Response Team – Group-IB) – центр круглосуточного реагирования на инциденты информационной безопасности. За шесть лет работы специалистами CERT было заблокировано более 10 000 доменных имен в зонах «.РФ» и .RU» – в первую очередь тех, откуда шло управление ботнетами, распространение вредоносных программ и фишинга. Опыт и решения Group-IB позволяют эффективно предотвращать и бороться с кражами денег, угрозами экстремизма и терроризма, кибершпионажем, атаками на объекты критичной информационной инфраструктуры, перехватом управления ключевыми информационными ресурсами.

1.5.5.2. Аналитический отчет Group-IB «Fxmsp: невидимый бог сети»

В июне 2020 г. Group-IB представила сообществу аналитический отчет «Fxmsp: невидимый бог сети» (https://habr.com/ru/company/group-ib/blog/507846/), раскрывающий личность одного из самых активных продавцов доступов в корпоративные сети компаний, предоставлявшего свои услуги в «даркнете» около трех лет. За это время он скомпрометировал порядка 135 компаний в 44 странах мира. По минимальным оценкам прибыль Fxmsp за период его активности могла составлять 1,5 млн долл. (около 100 млн руб.). Несмотря на то что Fxmsp и ранее упоминался в публичных источниках, Group-IB впервые подробно описали ход собственного расследования и факты, не обнародованные ранее. Материалы по личности Fxmsp переданы в международные правоохранительные органы.

В октябре 2017 года на самом известном русскоязычном андеграундном форуме exploit[.]in появилось объявление о продаже доступа к корпоративным сетям ряда компаний – редкой для того времени услуги в андеграунде. Его автор впервые предложил доступ ко всем критически важным сегментам сетей скомпрометированных им организаций и заявил, что среди его жертв есть банк – уникальный по меркам того времени лот.

1 октября 2017 года – «день рождения» Fxmsp, как одного из самых известных продавцов доступа к корпоративным сетям на андеграундных форумах. Но известным на весь мир это имя стало в мае 2019 года, благодаря новости о получении доступа в защищенные сети трех ведущих антивирусных компаний. Fxmsp скопировал из внутренних сетей вендоров различные фрагменты кода антивирусных продуктов, модули аналитики, документацию по разработке и др. и выставил лот за 300 000 долл. Fxmsp писал о том, что это была целенаправленная акция. Ему понадобилось чуть больше трех лет, чтобы из рядового пользователя хакерского форума, не знающего, как монетизировать свои навыки взлома, стать одним из главных игроков русскоязычного андеграунда – со своим пулом постоянных клиентов и даже своим менеджером по продажам.

Рис. 1.1. Этапы деятельности хакера Fxmsp

Исследуя активность на хакерских форумах более 17 лет, эксперты Group-IB Threat Intelligence начали фиксировать рост предложений, связанных с продажей доступов к корпоративным сетям, начиная с 2017 года – с появления на хакерской сцене Fxmsp. На тот момент форумы в основном наводняли предложения по доступам к взломанным сайтам, единичным серверам, учетным записям. Во второй половине 2017 года в «элитной» нише продаж доступов в корпоративные сети самым заметным игроком и абсолютным лидером по числу лотов был продавец с никнеймом Fxmsp. Со временем он создал новый тренд в андеграундном коммьюнити, ***сделав продажу доступов не товаром, а сервисом*** – с обеспечением привилегированного доступа в сети компаний-жертв для своих клиентов.

Основная активность Fxmsp пришлась на 2018 год. После чего ниша некоторое время пустовала, а с начала 2019 года у киберпреступника появились «последователи», которые и сегодня ведут активную деятельность в андеграунде, взяв на вооружение техники Fxmsp. По данным цитируемого исследования Group-IB, с начала 2020 года более 40 киберпреступников промышляют «ремеслом» Fxmsp на андеграундных форумах. Всего за это время было выставлено более чем 150 лотов по продаже доступов в корпоративные сети компаний различных отраслей.

К моменту появления скандальной новости о взломе трех антивирусных вендоров Fxmsp фактически закончил свою «публичную» деятельность. Однако до сих пор (на момент выхода книги) этот наиболее известный «продавец доступов» пока остается на свободе, представляя угрозу для компаний широкого диапазона отраслей независимо от того, в какой стране они находятся. В связи с этим командой Threat Intelligence Group-IB было принято решение о подготовке данного отчета, *передачи его расширенной версии международным правоохранительным органам* и обнародовании имеющихся материалов об инструментах и тактике Fxmsp.

Рис. 1.2. Распределение жертв Fxmsp по индустриям

Отчет Group-IB прослеживает деятельность Fxmsp с первой регистрации на андеграундном форуме, зафиксированной системой Group-IB Threat Intelligence, до его исчезновения с хакерских площадок. Fxmsp не специализировался на компрометации конкретных компаний. Топ-3 его жертв составляют госорганизации, провайдеры IT-сервисов и ритейл. Среди атакованных Fxmsp компаний была и «крупная рыба»: так, 4 из них входят в рейтинг «Global 500 | Fortune» за 2019 год. В послужном списке Fxmsp присутствуют банки, ТЭК, телекоммуникационные операторы, а также организации энергетического сектора (рис. 1.2). Одна из них летом 2020 года пострадала от атаки шифровальщика. К этому времени сервисы от Fxmsp не предлагались в андеграунде уже 8 месяцев.

Данные, полученные в ходе исследования с использованием системы Group-IB Threat Intelligence, позволили выявить инструменты, которые использовал Fxmsp для компрометации компаний, определить – с большой степенью точности – число его жертв, а также установить предполагаемую личность киберпреступника. Отчет Group-IB поэтапно раскрывает, как из рядового пользователя даркнета, начинавшего с майнинга криптовалюты, менее чем за 3 года русскоязычный хакер Fxmsp, по самым скромным подсчетам, заработал около 1,5 млн долларов – и это без учета продаж в «привате», лотов без указания цены, а также повторных продаж доступов в сети компаний-жертв.

Вместе со своим сообщником под ником Lampeduza, взявшим на себя рекламу и сопровождение всех сделок, в период с октября 2017 по сентябрь 2019 года они выставили на продажу доступы в 135 компаний из 44 стран мира, включая США, Россию, Англию, Францию, Италию, Нидерланды, Сингапур, Японию, Австралию и многие другие (рис. 1.3). Несмотря на негласный закон в андеграундной среде не работать «по РУ», Fxmsp продавал два лота по российским жертвам, за что был «забанен» модераторами форума, но это не остановило преступника.

Рис. 1.3. Графическое распределение жертв Fxmsp

Своим названием «Невидимый бог сети» отчета Group-IB обязан одному из рекламных постов Lampeduza. Завоевав авторитет в андеграундной среде, группа обзавелась постоянными клиентами. Lampeduza привлекался лишь на стадии монетизации, в то время как Fxmsp занимался всеми этапами атаки, включая сканирование IP-диапазона в поисках открытого порта RDP 3389, брутфорс, закрепление в сети и установку бэкдоров.

Независимые эксперты полагают, что содержащаяся в цитируемом отчете информация в итоге все-таки позволит правоохранительным органам посадить за решетку «невидимого бога сети» – это только вопрос времени.

1.5.6. Легализация бизнеса по разработке шпионских программ как новая угроза кибербезопасности

1.5.6.1. Hacking Team – разработка и продажа шпионских программ для государственных организаций

Здесь необходимо обратить особое внимание читателя на следующий факт. С появлением разработчиков шпионского программного обеспечения и огромного нелегального рынка продавцов криминальных киберпродуктов эти продукты стали легко доступны тем людям с криминальными наклонностями, которые совсем не обладают какими-либо действительно серьезными познаниями в «компьютерных науках».

И лежащая здесь «на поверхности» проблема заключается в том печальном факте, что даже если органы правопорядка «вычислят» и «посадят» кибермошенника (киберпреступника): во-первых, его место в даркнете тут же займут другие продавцы доступов в корпоративные сети; а во-вторых – купившие уже раньше «продукт» злоумышленники будут и дальше «совершенствовать» свое ремесло, получив первый опыт «охоты за легкими деньгами».

К сожалению, об этом очень мало проходит информации в СМИ, в Интернете и об этом пока ничего не пишут в таких «толстых» научно-технических изданиях, как эта энциклопедия, но специалисты по кибербезопасности уже видят возникающую «на горизонте» новую опасную угрозу, истоки которой относятся к 2003 г.

В разд. 1.5.5.1 мы рассмотрели в качестве примера компанию Group-IB, зарабатывающую деньги на расследованиях киберпреступлений. Но сегодня хорошо зарабатывают и вполне себе «легальные» компании, специализирующиеся на разработке и продажах шпионских программ и других «экзотических штучек».

Одна из наиболее известных таких компаний, основанная в Италии в 2003 году Hacking Team с офисом в полсотни человек, базируется в Милане и специализируется на создании программ для взлома компьютеров и смартфонов (Android, BlackBerry, Windows Phone) с последующим наблюдением за «жертвой». При этом итальянская команда использует стандартныет «хакерские методы» – уязвимости «нулевого дня», вирусы, известные бреши и приемы по проникновению на машины.

Самый известный продукт Hacking Team – «Система удаленного контроля» (Remote Control System, также известна под кодовыми названиями Galileo и DaVinci). В июне 2014 года «Лаборатория Касперского» и компания Citizen Lab независимо друг от друга опубликовали отчеты по деятельности Hacking Team, рассказав подробности ее основного инструмента RCS. Это своего рода троян, который внедряется в компьютер «жертвы» и транслирует всю информацию «хозяину». RCS перехватывает данные любого типа еще до их зашифровки: текст, изображения, электронные таблицы, разговоры по Skype, электронные письма, чат-сообщения. При этом отследить, куда и кому пересылаются похищенные данные невозможно.

Сама компания описывает RCS как специфическое решение проблемы шифрования, из-за которого любые правоохранительные органы не имеют возможности наблюдать за преступниками, угрожающими обществу.

Hacking Team многократно заявляла, что продает свои продукты только государственным структурам, заверяя при этом, что не сотрудничает с правительствами стран, на которых наложены санкции со стороны США, ЕС, ООН, НАТО и АСЕАН.

Правда, опубликованная в результате хакерской атаки в 2015 г. описанная ниже в этом разделе электронная переписка, счета-фактуры и списки клиентов итальянской ИТ-компани утверждали об обратном. Так, среди клиентов итальянцев оказались спецслужбы Судана, находящегося под жесткими санкциями ООН с 2005 года.

Среди ее основных клиентов, суммы контрактов с которыми достигают миллионов долларов, – правительственные организации Мексики, Италии, Марокко, Саудовской Аравии, Чили, Венгрии, США, Казахстана, Судана, Узбекистана и других стран. Среди заказчиков шпионского оборудования были как страны с сомнительной репутацией на международной арене, так и госорганы вполне себе демократических государств (США, Люксембург, Южная Корея, Польша, Швейцария).

В ряде развитых стран технические решения Hacking Team были вне закона, потому у компании были проблемы с поставкой оборудования в Великобританию, а спецслужбы США использовали его почти исключительно за границей.

Международная правозащитная организация «Репортеры без границ» давно занесла Hacking Team в список «врагов Интернета» за общую беспринципность и использование хакерской программы Da Vinci.

Приведем здесь только основные характеристики шпионской программы. «Galileo предназначена для скрытых атак, заражения и наблюдения за целевыми ПК и смартфонами. Система позволяет тайно собирать данные из самых распространенных десктопных операционных систем: Windows, OS X и Linux. Кроме того, система дистанционного управления может мониторить все современные смартфоны: на Android, iOS, Blackberry и Windows Phone. После инфицирования цели вы можете получить доступ ко всей информации, включая звонки Skype, Facebook, Twitter, WhatsApp, Line, Viber, местоположению устройства, файлам, скриншотам, микрофону и др».

Чтобы понять «рентабельность» подобного бизнеса, приведем следующие данные (https://gazetaby.com/post/vzlom-hacking-team-belorusskie-svyazi-italyanskix-xakerov/97724/): «Лицензия на 10 одновременных целей с поддержкой всех платформ – примерно 370 тысяч евро. Она включает в себя: 5 пользователей, 2 анонимайзера, инъекционный прокси(беспроводной / LAN), RMI (для мобильных), 1 год обслуживания (обновление и поддержка), установка и обучение (5 дней). Если вы хотите добавить 50 целей, цена вырастет на 120 тысяч евро. Цена не включает в себя поставки оборудования.

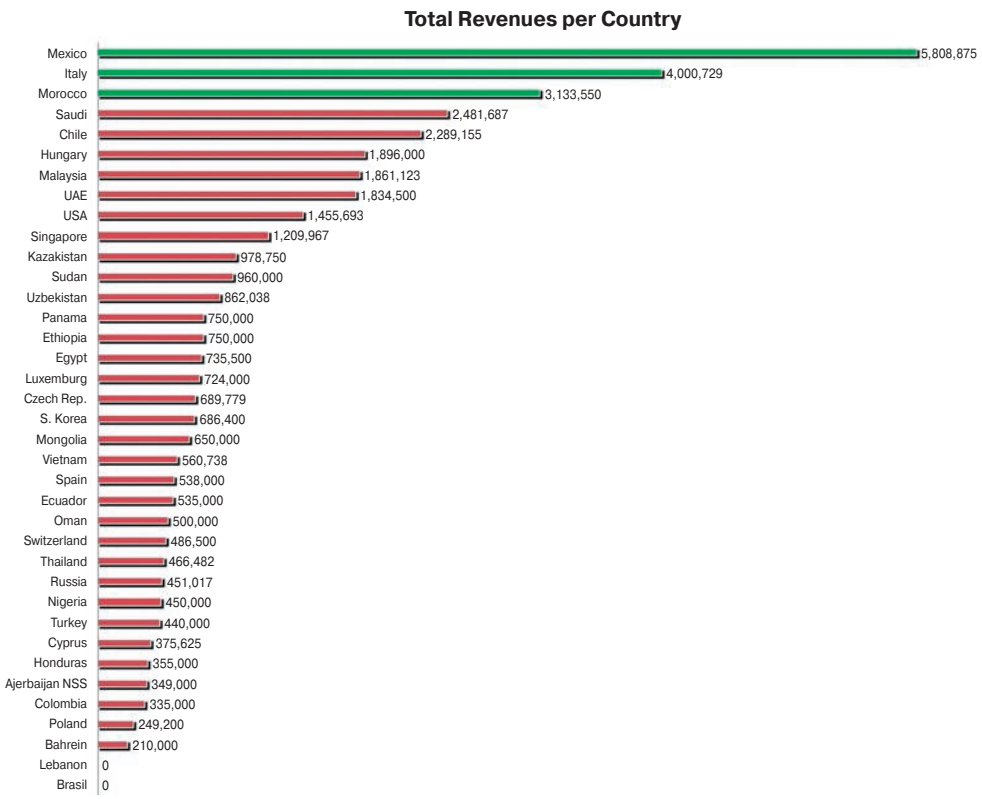

Рис. 1.4. Суммарная выручка компании Hacking Team с детализацией по странам

На рис. 1.4 представлена появившаяся в 2015 г. на сайте (https://zlonov.ru/hacking-team-facts-and-links/) информация о суммарной выручке этой компании с детализацией по странам и регионам.

Здесь мы видим и покупателей из России, Украины, Казахстана, Узбекистана и других стран бывшего СССР.

Таким образом, *подводя итоги* этого раздела, следует отметить, что за последние годы в мире произошли значительные изменения, о которых рядовые пользователи узнали не так давно: были обнаружены новые программы, которые использовались и как кибероружие, и как средства кибершпионажа.

Появились также частные компании, которые, согласно информации на их официальных сайтах, разрабатывают и предлагают правоохранительным органам *программы для нелегального сбора информации с компьютеров пользователей*. Кроме вышерассмотренной итальянской компании, на момент выхода книги мы наблюдаем активизацию коммерческой деятельности целого ряда других компаний (французкая Vupen и др.), *продающих готовые эксплойты* правительствам разных стран. Страны, у которых нет соответствующих собственных технических возможностей, могут «легально» покупать программы с подобным функционалом у таких частных компаний. Несмотря на наличие в большинстве стран законов, запрещающих создание и распространение вредоносных программ, подобные программы-шпионы предлагаются практически без какой-либо маскировки их функций.

Но пока таких компаний мало (по крайней мере, другие сегодня неизвестны рядовым потребителям) и конкуренции на этом рынке почти нет, что создает благоприятные условия для появления новых игроков и начала технологической гонки между ними. При этом эти компании не несут ответственности за дальнейшую судьбу созданных ими программ, которые могут использоваться для слежки, в межгосударственном шпионаже, либо с традиционной для обычного киберкриминала целью обогащения.

Очевидно, что ситуация осложняется возможностью появления подобных программ и на открытом рынке, где их могут перепродавать, например, подставные компании – кому и когда угодно.

Экспертам по кибербезопасности крупных и мелких компаний необходимо иметь в виду и эту угрозу и принимать соответствующие меры противодействия при разработке концепций и стратегий обеспечения корпоративной кибербезопасности.

1.5.6.2. Уникальный эпизод – открытый отчет хакера, взломавшего защиту компании Hacking Team

Спустя почти год после скандального взлома летом 2015 г. Hacking Team и утечки внутренних данных компании, в 2016 г. появился человек, взявший ответственность за случившееся на себя. На сайте PasteBin был опубликован объемный текст, автором которого выступил хакер, известный как Финиас Фишер (Phineas Fisher). Фишер в деталях рассказал о том, как он самостоятельно взломал Hacking Team, какие техники и инструменты для этого использовал, а также объяснил, зачем это сделал.

Итальянская компания Hacking Team прославилась на весь мир летом 2015 года, когда неизвестные взломали ее и опубликовали в интернете более 400 Гб внутренних файлов (от исходного кода до документов и почтовой переписки сотрудников). До этого момента о деятельности Hacking Team было известно немного, но после утечки данных любой специалист по кибербезопасности смог в деталях ознакомиться с тем, как работают компании, создающие инструменты для массовой слежки, разрабатывающие различные эксплоиты и софт на грани легального.

Хотя после взлома на всеобщее обозрение выплыли различные факты, часть из которых откровенно порочила репутацию Hacking Team (к примеру, сотрудничество с Ливией, Суданом, Эфиопией и другими странами, властям которых определенно не стоило продавать глобальный шпионский софт), руководство компании попыталось оправдаться и принести извинения. В итоге Hacking Team не слишком пострадала в результате этого скандала.

Публикация Финиаса Фишера была представлена в стиле *мануала* (руководства) для начинающих хакеров. Он не только в подробностях рассказывает о взломе Hacking Team, но читает настоящую лекцию об информационной безопасности в целом, рассказывая обо всем, начиная практически с самых азов. Фишер, в частности, пишет о том, почему использование Tor – это не панацея, учит правильно пользоваться поиском Google (как это делают пентестеры), а также объясняет, как правильно собирать личные данные о жертве и применять социальную инженерию. Мы рекомендуем читателю ознакомиться с полной версией текста на PasteBin.

Фишер утверждает, что входной точкой его атаки стало некое «встроенное устройство», подключенное к внутренней сети Hacking Team. Хакер не раскрывает подробностей о том, что это было за устройство, зато он отмечает, что обычно найти точку проникновения гораздо легче. Дело в том, что специально для атаки Фишер нашел 0-day в этом «встроенном устройстве», создал собственную прошивку для него и оснастил ее бэкдором. Хакер пишет, что на создание удаленного root-эксплоита у него ушло две недели, а также отказывается раскрывать данные о природе самой 0-day уязвимости. Фишер объясняет свое нежелание тем, что баг до сих пор не исправлен.

Здесь и далее мы даем максимально близко к оригиналу текст, взятый нами с сайта https://xakep.ru/2016/04/18/hacking-team-hack/, как наиболее понятным языком передающий суть отчета хакера.

Проникнув в сеть Hacking Team, Фишер какое-то время наблюдал и собирал данные. Он написал ряд собственных инструментов для атаки и использовал свой эксплоит всего раз – для внедрения в сеть, а затем возвращался в систему уже через оставленный там бэкдор. Также при проведении опытов было важно не дестабилизировать систему и не выдать своего присутствия, поэтому несколько недель Фишер тренировался и проверял все подготовленные инструменты, эксплоит и бэкдор в сетях других уязвимых компаний. Для последующего изучения сети Hacking Team Фишер использовал busybox, nmap, Responder.py, tcpdump, dsniff, screen и другие тулзы.

```
NoSQL, or rather NoAuthentication, has been a huge gift to the hacker
community [1]. Just when I was worried that they'd finally patched all of the
authentication bypass bugs in MySQL [2][3][4][5], new databases came into
style that lack authentication by design. Nmap found a few in Hacking Team's
internal network:

27017/tcp open  mongodb       MongoDB 2.6.5
| mongodb-databases:
|   ok = 1
|   totalSizeMb = 47547
|   totalSize = 49856643072
...
|_    version = 2.6.5

27017/tcp open  mongodb       MongoDB 2.6.5
| mongodb-databases:
|   ok = 1
|   totalSizeMb = 31987
|   totalSize = 33540800512
|   databases
...
|_    version = 2.6.5

They were the databases for test instances of RCS. The audio that RCS records
is stored in MongoDB with GridFS. The audio folder in the torrent [6] came
from this. They were spying on themselves without meaning to.
```

Потом Фишеру повезло. Он обнаружил пару уязвимых баз MongoDB, сконфигурированных совершенно неправильно. Именно здесь хакер нашел информацию о бэкапах компании, а затем добрался и до самих бэкапов. Самой полезной его находкой стал бэкап почтового сервера Exchange. Фишер принялся прицельно искать в нем информацию о паролях или хешах, которые могли бы предоставить ему доступ к «живому» серверу. Для этого он использовал pwdump, cachedump и lsadump, и удача снова ему улыбнулась. Фишер обнаружил учетные данные аккаунта администратора BES (BlackBerry Enterprise Server). Данные оказались действительны, что позволило Фишеру повысить свои привилегии в системе, в итоге получив пароли других пользователей компании, включая пароль администратора домена.

```
HACKINGTEAM  BESAdmin       bes32678!!!
HACKINGTEAM  Administrator  uu8dd8ndd12!
HACKINGTEAM  c.pozzi        P4ssword      <---- lol great sysadmin
HACKINGTEAM  m.romeo        ioLK/(90
HACKINGTEAM  l.guerra       4luc@=.=
HACKINGTEAM  d.martinez     W4tudul3sp
HACKINGTEAM  g.russo        GCBr0s0705!
HACKINGTEAM  a.scarafile    Cd4432996111
HACKINGTEAM  r.viscardi     Ht2015!
HACKINGTEAM  a.mino         A!e$$andra
HACKINGTEAM  m.bettini      Ettore&Bella0314
HACKINGTEAM  m.luppi        Blackou7
HACKINGTEAM  s.gallucci     1S9i8m4o!
HACKINGTEAM  d.milan        set!dob66
HACKINGTEAM  w.furlan       Blu3.B3rry!
HACKINGTEAM  d.romualdi     Rd13136f@#
HACKINGTEAM  l.invernizzi   L0r3nz0123!
HACKINGTEAM  e.ciceri       2O2571&2E
HACKINGTEAM  e.rabe         erab@4HT!
```

На этом этапе Фишер уже опасался, что его присутствие вот-вот заметят, поэтому принялся срочно скачивать информацию с почтового сервера компании. Однако хакера никто так и не обнаружил.

Изучив похищенные письма и документы, Фишер заметил, что пропустил кое-что важное – «Rete Sviluppo», изолированную сеть внутри основной сети Hacking Team, где команда хранила исходные коды своего RCS (Remote Control System), то есть шпионского ПО для слежки за пользователями. Рассудив, что у сисадминов должен быть доступ к этой сети, Фишер (уже обладающий привилегиями администратора домена) проник на компьютеры Мауро Ромео (Mauro Romeo) и Кристиана Поцци (Christian Pozzi). На их машины он подсадил кейлоггеры, софт, делающий снимки экрана, поработал с рядом модулей metasploit, а также просто изучил содержимое компьютеров. В системе Поцци обнаружился Truecrypt-том, и Фишер терпеливо дождался, пока разработчик его смонтирует, а затем скопировал оттуда все данные. Среди файлов с зашифрованного тома обнаружился обычный файл.txt с кучей разных паролей. Нашелся там и пароль от сервера Fully Automated Nagios, который имел доступ к закрытой сети Sviluppo для мониторинга. Фишер нашел то, что искал.

Кроме того, просматривая похищенную почту, хакер обнаружил, что одному из сотрудников дали доступ к репозиториям компании. Так как Windows-пароль сотрудника был уже известен Фишеру, он попробовал применить его же для доступа к git-серверу. И пароль сработал. Тогда Фишер попробовал sudo, и все вновь сработало. Для доступа к серверу GitLab и Twitter-аккаунту Hacking Team взломщик вообще использовал функцию «я забыл пароль», в сочетании с тем фактом, что он имел свободный доступ к почтовому серверу компании.

В конце Фишер отмечает, что он хотел бы посвятить данный взлом и этот подробный гайд многочисленным жертвам итальянских фашистов. Он заявляет, что компания Hacking Team, ее глава Давид Винченцетти (David Vincenzetti), давняя дружба компании с правоохранительными органами – все это части давно укоренившейся в Италии традиции фашизма.

После таких заявлений мотивы Фишера, который пишет о себе как о «этичном хакере», становятся яснее.

В конце этого раздела мы попробуем более детально рассмотреть ситуацию с подобными «этическими хакерами» на предмет соответствия их «хакерской этики» этике «общечеловеческой» и сделать свои авторские выводы о корректности использования приставки «этичный» со словом «хакер».

1.5.7. К вопросу о практике «технического симбиоза» кибермошенников и государственных спецслужб

Как известно, «дипломированных хакеров» не бывает – их ведь не готовят в высших учебных заведениях, на специальных «учебных курсах», семинарах, вэбинарах и т.п. Из мемуаров бывших сотрудников известного израильского секретного киберотряда 8200, о котором более подробно мы расскажем в разд. 6.7, мы знаем, что некоторые сотрудники этого считай лучшего в мире киберподразделения вообще не имели университетских дипломов.