УДК 004.056.5

Информационная безопасность в сети, способы ведения кибер-разведки и защиты от неё

Годунов Дмитрий Александрович – курсант Новосибирского высшего военного командного училища.

Гунаев Абумуслим Исмаилович – сержант Новосибирского высшего военного командного училища.

Аннотация: В статье рассматриваются основные способы проведения кибер-атак и способы защиты от них. Статья написана в первую очередь для лиц, которые не знакомы со сферой информационной безопасности с целью их краткого ознакомления с данной областью информатики. В статье также не рассматривается применение социальной инженерии и защиты от мошенников, поскольку данная информация относится к области психологии и социологии.

Ключевые слова: информационная безопасность, фишинг, MITM-атака, сбор данных, хакинг, пентестинг.

В современном мире информация становится всё более востребованной, поскольку благодаря ей можно влиять на различные сферы общественной жизни. Различные её виды можно применять абсолютно по-разному. Это может быть, например, информация об изменении роста цен на продукты, зная которую можно заранее купить дорожающий товар пока ещё по дешёвке, или знания о договорах между нефтяными конгломератами, влекущее падение цен на нефть, тем самым, создавая искусственное падение валюты стран, где продажа нефти является основным способом пополнения бюджета.

Однако, есть и иные виды информации. Под ними имеются ввиду знания, которые из открытых источников не получить. Речь идёт о незаконном получении информации о частной жизни человека, или же внутрекорпоративном состоянии компании. Как

правило, подобного рода знания применяются соответствующе, а именно: для проведения шантажа, спекуляций, диверсии, похищения, слежки и т.д.

И в данном докладе мы рассмотрим, каким образом различные преступные группировки, а так же крупнейшие разведки мира и конгломераты получают информацию о физических и юридических лицах, а так же способы защиты от них.

Перед началом рассмотрения вышеперечисленных вопросов, считаю необходимым ввести и объяснить ряд терминов и понятий, которые будут в дальнейшем непонятны неподготовленному читателю. Так же, при появлении англоязычных аббревиатур, они будут расшифровываться и переводиться.

- **Специалист по информационной безопасности (**в простонародии **«хакер»)** – человек, обладающий набором знаний и навыков в области кибербезопасности, социальной инженерии и программирывании. Как правило, различают этичных и неэтичных хакеров.

- **Этичный хакер (**он же **пентестер (White Hat Hacker)**) – специалист, помогающий компаниям находить и устранять бреши в их защите. Такие хакеры действуют по запросам от компаний, которые можно найти на различных сайтах и форумах.

- **Неэтичный хакер (Black Hat Hacker)** – специалист, применяющий свои навыки в целях перепродажи полученной незаконным путём информации.

- **Корпорация зла** – крупный конгломерат (Microsoft, Facebook, Google, Amazon и т.д.), которые продают свою продукцию по всему миру, но при этом не останавливаются ни перед чем, чтобы получить прибыль. Как правило, не гнушатся слежкой за деятельностью своих пользователей и передачей информации государственным органам (ФБР, МИ-6, ФСБ и т.д.).
- **Машина –** понятие в среде программистов и пентестеров, обозначающее виртуальную машину, ПК или ноутбук.

В среде специалистов в области кибербезопасности различают следующие виды деятельности:

- **Web-Hacking** – взлом сайтов и все что с этим связано.
- **Network Hacking** – взлом сетей и всего сетевого.
- **OSINT** – отдельное направление связанной с разведкой.

- **Forensic** – цифровая криминалистика, отлов хакеров преступников и прочих личностей.
- **Anonimity** – все что связано с анонимностью. Настройка безопасности машины (компьютера/ноутбука), VPS, подмена ip и проч.
- **Reverse Engineering** – это разбор программ на 0 и 1 с целью попытаться как она работает, разобрать её, изменить и запустить заново на языке Assembler или на другом языке программирования.
- **Социальная инженерия** – обман людей, проход на территорию противника обманным путем, психология, НЛП, разведка и все что с этим связано. Тесно интегрируется с OSINT.
- **Source code testing** – динамический и статический анализ исходного кода. Иными словами, пентестер проверяет насколько все грамотно спрограммировано и выявляет потенциальные уязвимости.
- **App pentest** – тестирование Android и IOS приложений на проникновение.
- **Wi-FI Hacking** – взлом беспроводных сетей.
- **Coding** - написание скриптов, программ для взлома. Это ветка развития программистов.

Глава 1.
Деятельность хакеров и способы защиты от них

«По данным Microsoft, хакеры с помощью сервера Exchange Server пытались заполучить информацию от целого ряда компаний в США. В корпорации считают, что за атакой стоит группировка Hafnium, якобы спонсируемая властями КНР.» [1]

«На сайт «Диктанта победы», посвященного Великой Отечественной войне, совершили DDoS-атаки. Об этом, как передает сайт партии «Единая Россия», являющейся организатором диктанта, сообщил руководитель ИТ-проектов партии Вячеслав Сатеев.» [3]

«Хакеры похитили данные 9 млн пассажиров EasyJet. В большинстве случаев злоумышленники сумели получить доступ только к адресам электронной почты пассажиров и данным об их полетах. Однако в небольшом числе случаев хакеры сумели похитить и данные банковских карт.» [4]

Эти и подобные заголовки довольно часто встречаются в газетных очерках и статьях. И, казалось бы… хакеры совершили атаку на какой-то объект или какое-то лицо… но вот как именно им удалось это? Об этом и будет рассказано в этой главе.

Следует различать следующие виды хакерских атак:

- **Fishing (рыбалка)** – суть атаки в том, чтобы получить от пользователей информацию (пароли, номера кредитных карт и т.д.) или деньги. Этот приём направлен не на одного пользователя, а на многих. Например, письма якобы от службы технической поддержки рассылаются всем известным клиентам какого-либо банка. Однако далеко не всегда. Является древнейшим и, зачастую, довольно эффективным способом взлома.

Зачастую современные хакеры применяют следующие варианты атак: в социальных сетях создают заранее подготовленные, или же покупают готовые аккаунты, как правило, лиц противоположного пола с целью более быстрого «втирания» в доверие к жертве. При общении, которое может длиться недели или даже месяцы, злоумышленник аккуратно приобщается к человеку, применяя навыки социальной инженерии, а так же знания, полученные в ходе OSINTa, если разведка проводилась. В ходе беседы в соц.сетях он может предлагать жертве посмотреть картинки, документы и файлы, что он отправлял ей, а так же перейти по ссылке , что бы посмотреть смешное видео или картинку в этой же соц.сети. Если потерпевший перейдёт по ссылке, то, как правило, открывается окно входа в соц.сеть (к примеру ВКонтакте) или видеохостинг (к примеру YouTube). Жертва вводит в окно логин и пароль, и её пересылает на ту страничку, о которой и говорил злоумышленник. Либо же, при нажатии на ссылку компьютер переходит на сайт, заражённый вирусом и компьютер заражается этим вирусом. Как правило, сайты с вирусами не применяют, поскольку, соц.сети как правило проверяют ссылки на благонадёжность, однако не всегда.

Предлагаю разобраться в том, что, всё-таки произошло, и как избежать характерных ошибок.

1. Злоумышленник, общаясь с потерпевшим, детально изучал его страницу. Фотографии, записи, комментарии, друзей, музыку, видео и т.д. с целью создания «портрета» жертвы. Он мог это сделать заранее или в ходе диалога.

Рекомендуется: Воздержаться от пользования соц.сетями вообще, либо же, если отказаться в их пользования невозможно, ограничить известную, действительно правильную информацию. Например: создать аккаунт с иными именем/фамилией/данными, написанными в анкете регистрации или же, содержать ни о

чём однозначно не говорящие файлы (фото, видео, музыку, документы и т.д.).

1. Длительное общение злоумышленника позволило ему войти в круг доверия жертвы, что в дальнейшем помогло при переходе человека по ссылке и заполнению полей регистрации.

Рекомендации: Лучше всего на данном этапе помогает паранойя, и чем она сильнее, тем лучше. Обратите внимание на страничку собеседника, пригласите его в видео чат, попросите прислать вам голосовые сообщения, сославшись на то, что заняты и не можете читать, однако слушать в состоянии. Вышеописанные действия не помогут против хорошо подготовленных мошенников (тех из них, которые месяцами создавали образ), однако новичков в данном способе взлома, вполне способны отогнать.

- **(D)DoS ((Distributed) Denial of Service) ((распределённый) отказ от обслуживания)** – вид атаки, похожий на «спам». Он заключается в подавлении веб-ресурса или сервера трафиком с пустыми запросами, чтобы спровоцировать перебои в работе сетевых ресурсов в крупных фирмах или гос.организациях.

Различия между DoS и DDoS в том, что DoS, как правило использует 1 источник пакетов, в то время, как DDoS использует всё, что имеет связь с Интернетом (ноутбуки, телефоны, умные часы, компьютеры, видеокамеры, ip-телефоны, принтеры, системы «умных» домов и т.д.).

Как правило, (D)DoS используется, чтобы недопустить попадание пользователей на сайт. Так же, (D)DoS гораздо чаще применяется для отвлечения внимания от другой, более значимой цели.

Рекомендации: Для защиты сетевых клиентов (серверов, выходящих в Интернет, и веб-сайтов) необходимо заранее поставить защиту от подобных атак. Современные компании, как правило, предлагают уже встроенную, либо устанавливаемую дополнительно, защиту в виде брандмауэров и firewall'ов. Так же, следует понимать, что нельзя ни в коем случае допустить злоумышленников до средств администрирования, которые и управляют защитой веб-клиентов. Как правило, к системам администрирования допускают лишь при физическом подключении (через кабель), что во много раз увеличивает безопасность. Иногда, правда, к средствам

администрирования дают право доступа через сеть Интернет, однако в данном случае вход в панель управления осуществляется через децентрализованные сети наподобие Tor или I2P.

- **Sniffing of network (Прослушивание сети)** – данная атака осуществляется с помощью аппаратных модулей, по типу SDR-приёмников (например HackRF one) либо wi-fi адаптеров (например, TP-Link или Alfa. Вторые у пентестеров ценятся больше). Она возможна ТОЛЬКО если злоумышленник попал в сеть.

Представим следующий пример.

Банк «ЗАО Кубань-холдинг» для осуществления документооборота использует внутрикорпоративную сеть wi-fi к которой подключены все сотрудники данного банка. Маршрутизатор имеет защиту от DDoS атак в виде firewall'a. Казалось бы, сеть защищена, безопасность гарантирована. Рабочий день начинается в 9:00. В 6:30 на парковке для клиентов возле банка стоит всего лишь один автомобиль. Постепенно, к началу рабочего дня, в это учреждение прибывают банкиры. К началу рабочего дня данные всех их клиентов уже у злоумышленников.

Предлагаю более детально разобраться в том, что произошло со стороны злоумышленников.

Для данного вида атак возможны несколько вариантов развития событий:

В 6:30 неэтичный хакер в машине на парковке запускает загрузочный флеш-накопитель с операционной системой Kali Linux (это бесплатная система, доступная любому желающему для проверки своих систем безопасности. Имеет множество программ, специализирующихся на проверке безопасности), подключает к ноутбуку wi-fi адаптер. Запускает загруженную операционную систему, после чего, переводит адаптер в режим мониторинга (это такой режим, когда wi-fi адаптер переводится в режим сканирования исходящего от ближайших сетей трафик). Затем, выбрав соответствующую сеть, переводят адаптер на мониторинг именно данной сети. Завершив все вышеуказанные действия, злоумышленники ждут.

К началу рабочего дня начинают подходить работники банка. Люди, как правило, любят всё бесплатное, поэтому велика вероятность того, что их телефоны уже были подключены к wi-fi банка ранее, однако, если такого не было сделано, то подключены их компьютры. Во всяком случае, как в телефонах, так и в компьютерах сотрудников при включении/ приближении к wi-fi зоне их банка, телефон/ ПК отправляет запрос на подключение к wi-fi с зашифрованным паролем. В этот момент маршрутизатор анализирует пароль и допускает устройство к подключению. В момент принятия маршрутизатором пароля, wi-fi адаптер злоумышленника, просканировав сеть, получает копию зашифрованного пароля. Теперь хакеру остаётся лишь расшифровать пароль, войти в сеть и, сканируя сеть, собирать данные по всей сети. И банку крупно повезёт, если под конец деятельности, чтоб зачистить следы, хакер не оставит в их сети вирусы с time-кодом (вирус работает как бомба с таймером).

Именно поэтому крайне не рекомендуется использовать сети в общественных местах, особенно без пароля.

Следующий способ проникновения в сеть, к примеру, того же банка, является broot force (грубая сила) это подбор паролей методом перебора заранее готовых вариантов паролей в словаре. С появлением протокола WPA2 (Wi-fi Protect Access (Защищённый доступ к wi-fi)) практически не применяется. Иногда работает со стандартными паролями типа: admin, 1234567890 и т.п.

Третьим вариантом проникновения в сеть является фишинг, аналогичный описанному выше. Однако, в данном сценарии, wi-fi адаптер в режиме мониторинга создаёт ложную wi-fi сеть, названную так же, как и сеть банка. После создания подставной сети, злоумышленник блокирует (глушит) wi-fi банка (wi-fi адаптеры могут глушить 1-2 wi-fi маршрутизатора), тем самым, прибывшие на работу сотрудники обнаруживают, что сеть банка на месте, однако, телефон сам не подключился к ней, равно как и компьютеры. Подключив устройство заново к якобы банковской сети, они сами отдают пароль в руки неэтичного хакера. Ему лишь остаётся свернуть подставную сеть и снять заглушку с их родной сети.

Рекомендации: Для защиты от данных видов атак следует создать пароль наиболее анархичный и сложный. В нём должны быть различные знаки, буквы как заглавные, так и строчные, а так же цифры, однако они должны быть расположены в хаотичном порядке. Как правило, 15-20 и более символов вполне могут усложнить жизнь

взломщикам. Так же, не стоит забывать про протокол WPA2. Данный протокол шифрует трафик сети таким образом, что, порой, время на расшифровку занимает много… лет. Ак же, хорошим способом защитить сеть является перевести сеть на кабеля, что так же не даёт возможности получить пароль без физического контакта проводов/коммутаторов/маршрутизаторов.

- **IPHijack (IP хайджек)** – вид атак, аналогичный сниффингу с той лишь разницей, что атака производится при физическом подключении пентестера к системе безопасности через кабели и провода. Как правило, применяется тогда, когда не остаётся иных способов проникнуть в систему. Зачастую себя не оправдывает. Защита от них аналогична защите от спуффинга.
- **Вирусы** – наиболее известный благодаря информации в СМИ и Интернете вариант атак. Вирусы бывают различного вида, однако, наиболее часто встречающиеся это вирусы-вымогатели и вирусы удалённого доступа. Первые делают блокировку компьютера или шифровку/удаление системы и требуют выкуп взамен за пароль от вируса, вторые осуществляют скрытое проникновение в систему для скачивания и отправки файлов. Однако видов вирусов гораздо больше.

Рекомендации: от вирусов могут помочь антивирусы, а так же практика пользователей в профилактике, предотвращении заражения и знаний по борьбе с вирусами, что, на мой взгляд, является главным способом борьбы с ними, поскольку именно человек является создателем вирусов и антивирусов, а значит, именно человек борется с ними. Антивирусы же выступают в роли помощников человека, облегчая его труд вплоть до принятия большинства обязанностей по борьбе с ними.

Глава 2.
Как корпорации зла воруют данные и как с этим бороться

Мобильные приложения «ВКонтакте», «Госуслуги» и «Одноклассники» вошли в тройку тех, которые собирают и обрабатывают больше всего персональных данных пользователей в России. К такому выводу пришли аналитики информационно-аналитического агентства TelecomDaily в своем исследовании. [5]

Возможно мало кто догадывается, но основными поставщиками данных для спец.служб различных стран являются далеко не частные лица, хотя умалять их деятельность так же не стоит. Как правило, спец.службы по типу FBI или ФСБ собирают данные пользователей через провайдеров (компании, предоставляющие доступ в Интернет), хранящих ваши данные на своих серверах (например, по причине закона «пакет Яровой»), что позволяет смотреть историю поисковых запросов пользователей даже

при их удалении. Другим не мало важным аспектом получения данных являются корпорации зла. Они регулярно передают данные спец.службам, иногда, правда, не специально «сливая» их в открытый доступ. [6] Сбор данных они осуществляют через наиболее популярные в массах приложения и программы, такие, как, например, «Телеграм», «ВКонтакте», «Instagram», «Tiktok» и прочие.

Чтобы защититься от их алгоритмов по сбору данных и дальнейшей передачи информации гос.органам иных стран, следует пользоваться программами с открытым исходным кодом, прошедшими сертификацию OpenSourse или GNU. Эти лицензии гарантируют отсутствие у создателей порывов сбора данных пользователей а так же открытый исходный код, просмотрев который, можно убедиться, что данные создатели не сделали никаких тайных скриптов сбора информации.

Однако, если нет возможности отказаться от проприетарных приложений, следует хотя бы не давать им права доступа на различные системы устройств, которые не важны для работы приложения, как, например, не давать приложениям доступ к фотографиям, если это приложение звонков или музыки.

В заключении хочется отметить, что данный доклад отражает лишь «верхушку» айсберга. В нём были освещены лишь основные, наиболее общие знания и примеры. Беречь или не беречь свою конфиденциальность- дело каждого отдельного человека. Цель данного доклада была лишь в том, что бы дать знания лицам, которые не были знакомы с данной тематикой, тем самым, подняв уровень грамотности читателей в области информационной безопасности.

Список литературы

1. Полякова Виктория Microsoft обвинила китайских хакеров в атаке на компании в США / РБК [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/technology_and_media/03/03/2021/603efba99a7947894b79a
2. Тип безопасности для WI-FI: что такое WPA, WPA2 PSK, шифрование [Электронный ресурс]. – Режим доступа: https://wifigid.ru/besprovodnye-tehnologii/wpa-i-wpa2-psk.
3. На сайт «Диктанта победы» совершили DDoS-атаки / РБК [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/rbcfreenews/5f511a419a79471c61f4a5dc.
4. Калюков Евгений Хакеры похитили данные 9 млн пассажиров EasyJet / РБК [Электронный ресурс]. – Режим доступа:

https://www.rbc.ru/technology_and_media/19/05/2020/5ec3e25d9a7947202c43736d.

5. Скрынникова Анастасия Аналитики назвали обладающие максимумом знаний о пользователях приложения / РБК [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/technology_and_media/30/11/2020/5fc0dfb59a7947399392a24d.

6. Юшков Михаил Данные 267 млн пользователей Facebook оказались в открытом доступе / РБК [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/technology_and_media/20/12/2019/5dfc4e449a79477ad8a1dd5b.

7. Виды хакерских атак [Электронный ресурс]. – Режим доступа: https://it-black.ru/vidy-khakerskikh-atak.

8. Взлом Wi-Fi с помощью Kali Linux [Электронный ресурс]. – Режим доступа: https://wifigid.ru/vzlom/vzlom-wi-fi-kali-linux.

9. DDoS-атака: что такое, как работает и можно ли защититься [Электронный ресурс]. – Режим доступа: https://eternalhost.net/blog/hosting/chto-takoe-ddos-ataka.

10. Что такое Black Hat, Grey Hat или White Hat Hacker? [Электронный ресурс]. – Режим доступа: https://techarks.ru/general/chto-takoe-black-hat-grey-hat-ili-white-hat-hacker.

11. Виды хакерских атак [Электронный ресурс]. – Режим доступа: https://zen.yandex.ru/media/id/5e6e890153be0d0a19b24803/vidy-hakerskih-atak-5e70f48d4337492a23d9ad5b.

12. Как стать этичным хакером в 2021 году [Электронный ресурс]. – Режим доступа: https://m.habr.com/ru/post/535918.

13. Зачем тебе анонимность? Как выжить в цифровом будущем? / YouTube [Электронный ресурс]. – Режим доступа: https://youtu.be/gzMZpCz0sv

{social}