**Урок 4.**

**День 4.**

**Тема: Типы атак социальной инженерии. Защита от социальной инженерии.**

Как мы уже не раз отмечали, человек является самым слабым звеном любой системы. На данном этапе после сбора информации об объекте вам следует подобрать наиболее успешный вариант для атаки на свою жертву.

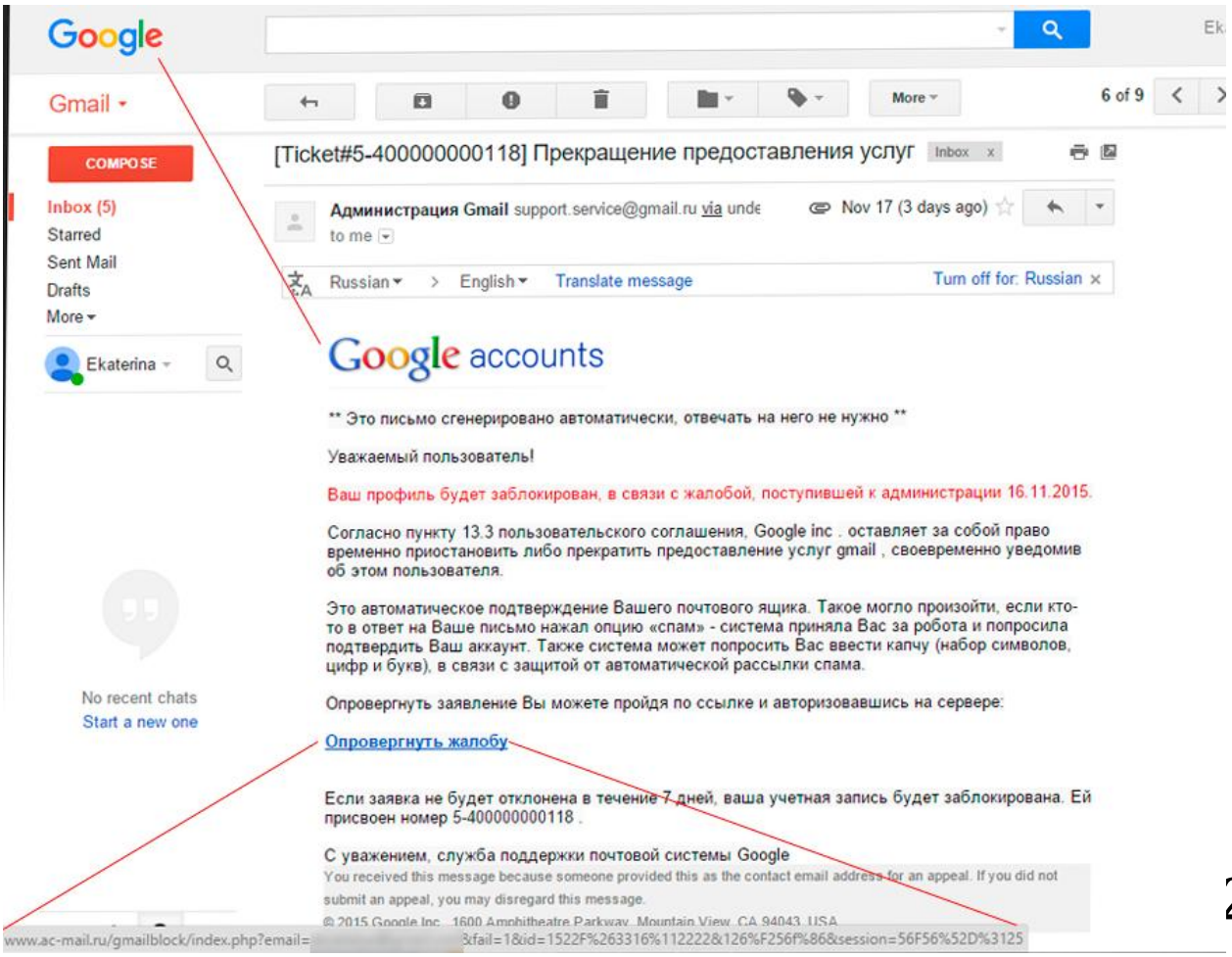
Существует несколько видов атак социальной инженерии:

**Претекстинг**. Это вид атаки на жертву где хакер выдает себя за другого человека с целью получения необходимой информации. Например, найдя в мусорном баке квитанцию из банка, хакер позвонил жертве, представившись сотрудником кредитного отдела, и сказал, что срок действия карты жертвы истекает и можно заказать новую. В ответ жертва сообщила, что это не так, и уточнила срок действия своей карты. Злоумышленник, сославшись на ошибку в системе, попросил уточнить еще и номер карты, после чего жертва сообщила и его. Хэднеги определяет претекстинг как «выдача себя за кого-то другого с целью получения личной информации». Это больше, чем просто нагромождение лжи, в некоторых случаях это может быть создание совершенно новой личности». В сериале «Мистер Робот», например, примером претекстинга является то, что Эллиот позвонил Майклу и сказал, что он из банка. Для сопротивления претекстингу важен здоровый уровень скептицизма. Не сообщайте конфиденциальную информацию по телефону. Критически относитесь с информации, которой с вами делиться этот случайный человек. Претекстинг эффективен только тогда, когда социальный инженер завоевывает ваше доверие с помощью правдоподобной информации и авторитета.



**Подделка принадлежности.** Очень хорошо работает в крупных организациях. В наше время несложно достать униформу сотрудника компании, например, форму сотрудника службы доставки, грузчика или простого рядового рабочего. Ни у кого не вызовет подозрений сотрудник службы доставки который ходит по кабинетам и ищет нужного человека. Хотя главной задачей для него будет найти незаблокированную рабочую станцию, оставленный без присмотра ноутбук или документы. Таким образом, также зачастую происходят установки различных шпионских гаджетов к сети организации. Сюда же относятся истории из прошлых уроков о группе «СОБР» и безработном Вильгельм Фойгте.

**Фишинг.** Главная идея данного метода состоит в создании поддельных сайтов и писем от организаций для получения доступа к приватной информации. Приведу наглядный пример фишинга. Вам приходит письмо о том, что вы сделали что-то неправильно и ваш ящик находится под угрозой блокировки, или же приходит к примеру письмо от якобы какой-либо официальной организации о каком- либо извещении, также для сотрудников организации могут приходить письма с вложениями с подписью для ознакомления с графиком отпусков и так далее. Как правило, в таких письмах всегда говорится о том что пользователю стоит перейти по ссылке или открыть какое-либо вложение.




2

*На картинке выше пример фишингового сайта , оповещающего пользователя о том, что якобы профиль будет заблокирован в связи с жалобой поступившей администрации ресурса.*

Есть техники, которые позволяют скрыть от пользователя реального получателя письма, например, указав в поле “Replay-To” accounts@google.com, в то время как в поле “Sender” будет указан отправитель someuser@google.com . Однако пользователи не склонны анализировать такие письма и увидят только то, что хочет составитель письма.

Еще один классический пример, - “Письма Счастья “ . В этом случае пользователь получает письмо, в котором говорится, что отправитель стал наследником огромного состояния и для его получения необходим поручитель, которому причитается в качестве вознаграждения 40% от суммы наследства, что составит около 5 миллионов долларов. Для того чтобы стать поручителем, необходимо выслать определенные данные. Зачастую такие письма не нацелены на какого-то конкретного человека. Отклик на них составляет около 0.01% однако и этого будет достаточно. И конечно же, - поддельные сайты. Даже если пользователь очень опытен, его все равно можно обмануть. В наше время можно зарегистрировать домен на подставного человека и получить SSL-сертификат на 60 дней, практически не проходя валидацию.

Для примера возьмем банк с более-менее привычным названием, например, Raiffeisen . По правилам всемирной паутины, зарегистрировать домен Raiffeisen.com нам никто не запретит. А большинство конечных пользователей не заметят подмены. Дальше – дело техники. Как вариант

можно разослать пользователям письмо с просьбой ознакомится с новыми правилами банка, которые находятся по указанной ссылке или вложении.

**Паутина.** Я выделил его как отдельный самостоятельный метод, хотя он является частью фишинга. Метод назван мной «Паутина», так как принцип действия данного метода похож на действия паука, который плетет свою паутину и расширяет «свое влияние». В паутину или сеть попадается все больше и больше жертв и паук имеет контроль не только над своим объектом, но и над контактами объекта, на друзьями друзей жертвы, и далее по цепочке. Как на практике выглядит подобный метод?

Большинство руководителей крупного звена чаще всего в личных целях никогда не используют корпоративную почту. Большинство по старинке пользуются обычными почтовыми серверами. Личная почта - это богатый кладезь информации о человеке, - на почте хранятся все логины и пароли к различным информационным ресурсам, сайтам, где зарегистрирован пользователь, начиная от сайта знакомств и заканчивая различными биржами, торговыми площадками. Как правило, на личных почтовых ящиках, человек ведет не только личную переписку, но и высылает партнерам различные проекты, рабочие материалы, деловые предложения. Подделать вход в корпоративную почту достаточно проблематично, а вот создать фейк известного почтового сервиса достаточно просто. Хотя такие фейки долго не живут, и обычно банятся. Главная задача социального инженера методом фишинга - это проникновение в почту жертвы, и рассылка подобных фейков всем его значимым контактам. А далее по цепочке,- в вашу паутину вовлекаются контакты контактов объекта, и устанавливается тотальная слежка над всей этой цепочкой людей.



Как уже писал выше, что паутина - это подвид фишинга, который я выделил в отдельный метод атаки. Как самый действенный вариант можно использовать следующую схему работы по методу паутина. В связи с тем, что в отличие от социальных сетей на почтовых серверах не отмечается когда человек в последний раз заходил на свою страницу, то определить что кроме самого хозяина на почту еще кто-то заходит достаточно сложно. Проверить кто еще сидит на почте можно только если зайти в разделы безопасности и посмотреть с каких айпи адресов были произведены входы. Но обычно люди редко интересуются проверками своей безопасности и уверены в сложности своего пароля. Задача хакера получать постоянную информацию об объекте и его действиях, а также информацию о действиях всех его контактов. Для того чтобы получить логин и пароль жертве на его почтовый сервер высылается какое-то важное письмо с подменным адресом, например от известного делового партнера, или с адреса его банка. Объект идет по ссылке в письме или открывает вложенный файл и ему кажется, что произошел какой то глюк и что его выкинуло из почты. Он попадает на страницу опять же его сервера почтового, где он разлонгинен, и ему по новой надо ввести логин и пароль к своей почте. А на самом деле и де факто он попадает на фейк почтового сервера.

Как гипотетический пример, я продемонстрирую ниже, что видит объект, при открытии ссылки в письме. Предположим, что у вашей жертвы есть почта на mail.ru, и соответственно, нам нужно создать фейковую страницу, точно такую же, но с похожим адресом. В адресную строку редко кто вглядывается. Такие домены как «nail.ru» как в нашем гипотетическом примере давно заняты разными хакерами и пример скорее учебный, чем рабочий. Доменный адрес по факту может быть не настолько похож.

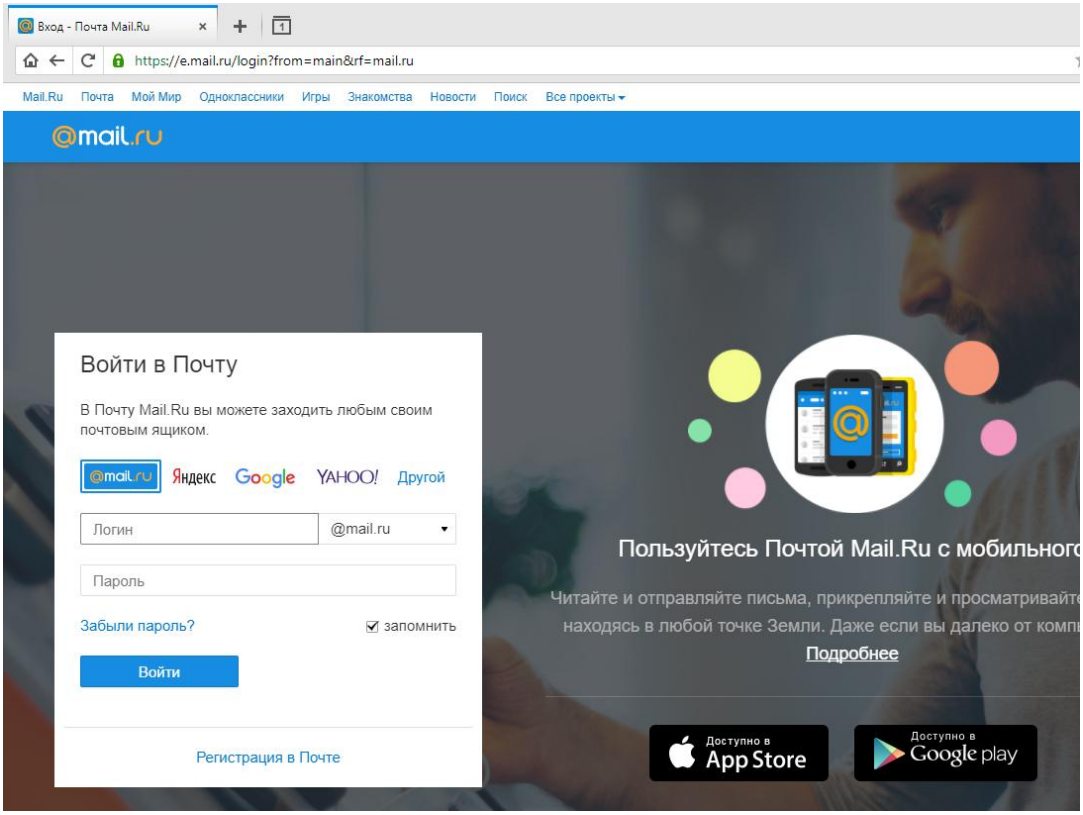



*Рис.1 реальная страница домена mail.ru*



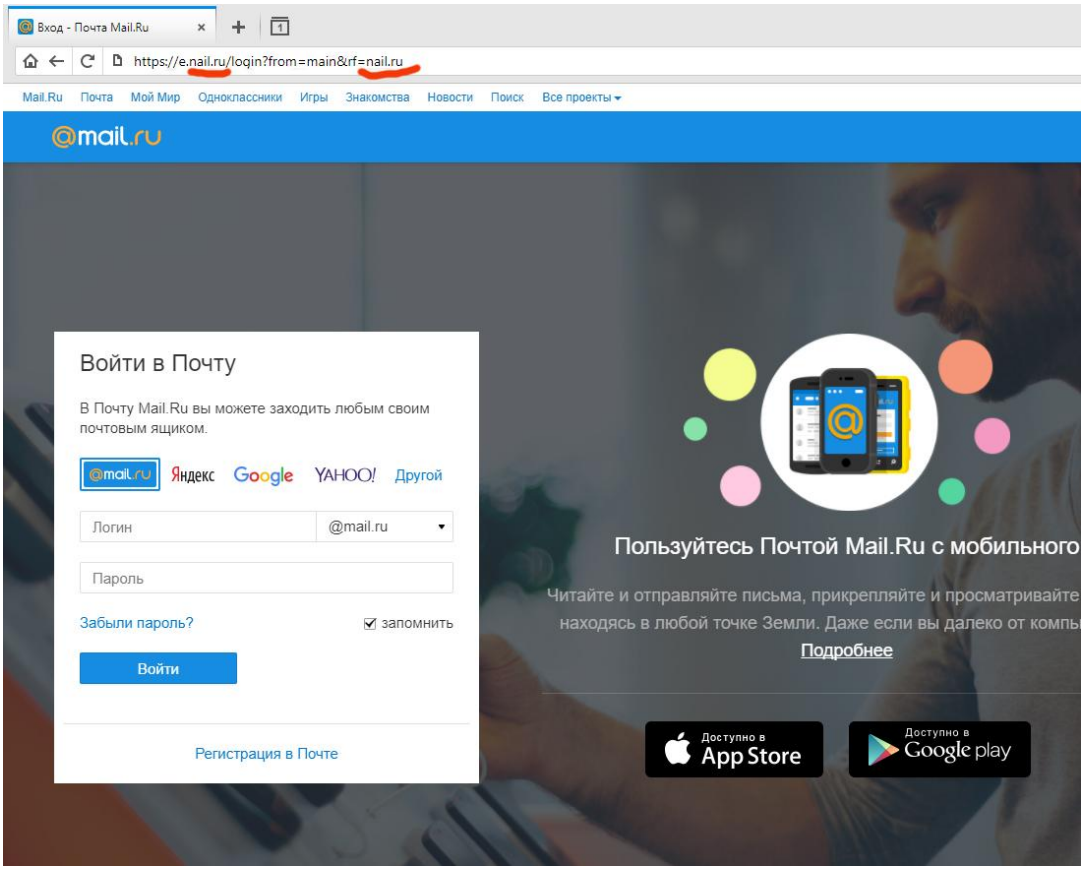



*Рис.2 фейковая страница, куда попадает жертва, когда ему «кажется» что что то глюкнуло и он «вылетел» из своей почты.*

Логин и пароль к почте отправляются хакеру. Он получает доступ к ящику объекта и начинает плести паутину. Подобные фейки рассылаются всем его контактам и контактам контактов, когда они попадут на удочку. Вероятность попадания на удочку где то 10-20 процентов на практике. Если с первого раза не получилось, то вероятнее всего жертва просто не открыла письмо. Такие атаки можно повторить. Далее, когда создана целая паутина объектов, устанавливается контроль над всей цепочкой людей, что они пишут, что делают, что рассылают, где регистрируются.

Социальный хакер должен огромное значение придавать контактами объекта, так как порой именно контакты объекта, а не сам объект являются бесценным источником информации об интересующей вас личности. Когда идет сбор информации об объекте в социальных сетях, необходимо прошерстить весь список друзей объекта и друзей друзей объекта и по принципу «Шести рукопожатий» (что любой человек на планете знаком с другим человеком как максимум через 6 человек), – найдется даже куча ваших общих знакомых, иногда самых неожиданных.

Бывают очень бдительные объекты, о которых практически невозможно собрать никакой информации. Приведу в пример нашумевшую историю недавнюю о Дерипаске и девушке с пониженной социальной ответственностью некой Анастасии Рыбки. Именно она выложила в социальных сетях компрометирующие фото Дерипаски. Хотя сам олигарх вел себя достаточно осторожно в социальных сетях, чем и воспользовался Навальный. Приведу еще один известный пример. Один из известных и самых разыскиваемых наркоторговцев попался потому, что его девушка в социальной сети поставила статус « Круто, когда у тебя парень наркодилер». Уделяйте внимание контактам объекта, и золотой ключик ваш. Какой бы он не был закрытый или осторожный, опять же главный риск и человека тоже человек, а точнее глупость его окружения. Хочу привести еще один пример атаки «Паутина» в мессенджере Телеграмм. Как известно, в мессенджере Телеграмм, аккаунты обитателей имеют так называемые линки, или ссылки на страницы пользователей, чисто гипотетически сами линки и ID- номер являются эквивалентом достоверности и аутентичности аккаунта, и как следствие самого человека. Подделать линк можно двумя способами.



1. К примеру, линк вашей жертвы @leonardo, по русски говоря, линк читается как Леонардо, по задумке жертвы. Что происходит далее. Вместо буквы Л используется буква I (i) которая позиционируется как буква l (L), визуально их практически невозможно отличить, но для особо внимательных и они, естественно, отличимые. Также 0 (ноль) и о (буква) тоже могут быть схожи, но, конечно же, не так выражено как L-уязвимость.
2. Вы подбираете похожий линк, заменив к примеру одну букву или цифру, чем длиннее линк вашей жертвы и многообразен, тем лучше для вас. Пример: ваша жертва использует линк @NikoLayGazprom821. Подделать линк вашей жертвы можно так: @NikolauGazprom821 или например, @NukolayGazprom821, все зависит лишь от вашей изобретательности.

   Подделать ID номер, насколько мне известно, невозможно, вы можете лишь использовать один из мультиаккаунтов с похожим ID номером, или же оставить все как есть. В основном жертва не обращает внимание на эту информацию, а некоторые клиент-приложения телеграмм вовсе не пишут ID номера человека, указывая только его линк. Естественно, что подделать остальную информацию не составляет труда.

**Дорожное яблоко.** При помощи этого приема была остановлена работа целого предприятия, внутренняя сеть которого не имела связи с внешним миром. Злоумышленник оставил красивую, крупную и привлекающую флеш карту на парковке для сотрудников , один из которых заметил и

подобрал ее. Естественно, это было утром перед началом рабочего дня. Любопытство взяло вверх, и сотрудник решил проверить ее содержимое прямо на рабочем месте. Как вы понимаете, на ней был вирус, который быстро распространился по внутренней сети. К дорожному яблоку можно отнести также такие методы как подкидывание флешки к квартире жертвы, на лестничную площадку, для того чтобы создалось впечатление, что какой то сосед случайно обронил свою вещь. Человеческая глупость и любопытство не имеют предела. В желании получить какую-нибудь «клубничку» на соседа, а вдруг там на флешке у соседа домашнее порно, человек сам своими руками в ажиотаже вставляет флешку в свой компьютер. Хакеру только остается сидеть дома и ждать звоночка уведомления в программе.

**Плечевой серфинг (англ. *shoulder surfing*).** Данный метод включает в себя наблюдение личной информации жертвы через её плечо. Этот тип атаки распространён в общественных местах, таких как кафе, торговые центры, аэропорты, вокзалы, а также в общественном транспорте.

Опрос ИТ-специалистов в о безопасности показал, что:

- 85 % опрошенных признались, что видели конфиденциальную информацию, которую им не положено было знать;
- 82 % признались, что информацию, отображаемую на их экране, могли бы видеть посторонние лица;
- 82 % слабо уверены в том, что в их организации кто-либо будет защищать свой экран от посторонних лиц.



**Квид про Кво(услуга за услугу)**. Данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

**Обратная социальная инженерия.** Данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте с злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

**Телефонный фрикинг (англ. phreaking)** . Это термин, описывающий эксперименты и взлом телефонных систем с помощью звуковых манипуляций с тоновым набором. Эта техника появилась в конце 50-х в Америке. Телефонная корпорация Bell, которая тогда покрывала практически всю территорию США, использовала тоновый набор для передачи различных служебных сигналов. Энтузиасты, попытавшиеся повторить некоторые из этих сигналов, получали возможность бесплатно звонить, организовывать телефонные конференции и администрировать телефонную сеть.

**Фарминг.** В классическом фишинге злоумышленник распространяет письма электронной почты среди пользователей социальных сетей, онлайн-банкинга, почтовых веб-сервисов, заманивая на поддельные сайты пользователей, ставших жертвой обмана, с целью получения их логинов и

паролей. Многие пользователи, активно использующие современные веб-сервисы, не раз сталкивались с подобными случаями фишинга и проявляют осторожность к подозрительным сообщениям. В схеме классического фишинга основным "слабым" звеном, определяющим эффективность всей схемы, является зависимость от пользователя – поверит он фишеру или нет. При этом с течением времени повышается информированность пользователей о фишинговых атаках. Банки, социальные сети, прочие веб-службы предупреждают о разнообразных мошеннических приемах с использованием методов социальной инженерии. Все это снижает количество откликов в фишинговой схеме – все меньше пользователей удается завлечь обманным путём на поддельный сайт.

Поэтому злоумышленники придумали механизм скрытого перенаправления пользователей на фишинговые сайты, получивший название фарминга ("pharming" – производное от слов "phishing" и англ. "farming" – занятие сельским хозяйством, животноводством). Злоумышленник распространяет на компьютеры пользователей специальные вредоносные программы, которые после запуска на компьютере перенаправляют обращения к заданным сайтам на поддельные сайты. Таким образом, обеспечивается высокая скрытность атаки, а участие пользователя сведено к минимуму – достаточно дождаться, когда пользователь решит посетить интересующие злоумышленника сайты. Вредоносные программы, реализующие фарминг-атаку, используют два основных приема для скрытного перенаправления на поддельные сайты – манипулирование файлом HOSTS или изменением информации DNS.

**Рейдерские атаки.** Рейдеры - это захватчики предприятий. Соответственно рейдерская атака - это атака по захвату предприятия. Классическая схема рейдерской атаки выглядит следующим образом.



1 этап. Сбор информации о захватываемом предприятии.

Как всегда, в любом виде деятельности, сбор информации – самый важный подготовительный этап. На этом этапе собирается и анализируется вся информация о предприятии: финансовая ситуация на предприятии, список контрагентов, список клиентов, список аукционеров, информация о слабых и сильных сторонах предприятия, о вредных привычках руководства и сотрудников, кто и с кем и против кого дружит на предприятии, информация о маркетинговых планах и прочее, прочее. На первом этапе в большинстве своем работают методы социальной инженерии, с помощью которых, как мы уже говорили ранее, собирать информацию легче всего. Как правило, этот этап занимает от одного до трех месяцев в зависимости от масштабов предприятия и сложности добывания нужной информации. Самое важное для рейдера на этом этапе получить тем или иным способом копию реестра аукционеров.

2 этап. Начало атаки.

Началом атаки можно считать тот момент, когда рейдер начинает скупку акций у миноритарных аукционеров. Миноритарии, как правило, с акциями расстаются легко, так как реально ощутимых дивидендов по ним практически не получают, а рейдеры предлагают за акции суммы в размере годового оклада. Миноритарные аукционеры - это акционеры с небольшим количеством акций. К примеру, в начале 90-х годов в разгул приватизации очень нередко, когда почти каждый работник какого-то большого предприятия с несколькими тысячами человек сотрудников имел по две-три акции. Вот такие аукционеры и называются миноритарными.

Параллельно со скупкой акций у миноритариев проходит работа по «закошмариванию предприятия», если выражаться на рейдерском языке. Основная цель «закошмаривания»- дезорганизация работы предприятия. Кроме этого достигается также побочная цель: колеблющимся аукционерам демонстрируется, что на предприятии имеются большие проблемы, после чего они со своими акциями расстаются гораздо охотнее. Второй этап для предприятия это действительно кошмар, лучше слово сложно придумать: руководству вчиняются иски от имени аукционеров по поводу нарушения различных операций с акциями, нарушении порядка проведения сделок, о чем рейдер узнает на первом этапе. В отношении руководства и сотрудников предприятия возбуждаются уголовные дела, неважно по реальным поводам или нет, - главная цель это издергать людей. Инициируются проверки деятельности предприятия различными службами, налоговой, инспекцией, санэпидемстанцией, противопожарной службой, природоохранной прокуратурой и чем больше, тем лучше. Для парализации работы предприятия устраивается классическая DDoS – атака (отказ от обслуживания) на социальном уровне. Как правило, при «закошмаривании» предприятия основную роль играют именно социальные хакеры, которые используют в своей работе методы социальной инженерии и программирования. Руководство предприятия видя, что стало объектом рейдерской атаки, обычно начинает идти на увольнение сотрудников, продающих свои акции, с целью устрашения тех, кто еще свои акции не продал. Иногда это дает результат, иногда нет. Кроме того, акции компании переводятся на доверительное управление или передаются в залог какой-нибудь конторе, подконтрольной предприятию. После этого руководством почти всегда проводится дополнительная эмиссия акций и организуется контр-скупка акций.



3 этап. Внесение раскола в состав руководства предприятия.

Для того чтобы заполучить предприятие практически легально, рейдерам достаточно 30% плюс одна акция. Однако в настоящее время ситуация такова, что управление предприятия держит в своих руках от 70% и более акций, -так называемый консолидированный пакет. Поэтому рейдеру необходимо внести раскол между членами управляющего органа предприятия, для чего рейдер пытается расколоть управляющий орган, сыграв на различных внутренних противоречиях между управленцами предприятия. Об их внутренних противоречиях также узнается на первом этапе.

По сути 3-й этап - это этап «плетения интриг» между руководством предприятия и этап скупки акций у основных держателей, которым делаются различные «интересные предложения». Кроме того на этом этапе формируется оппозиция из недовольных миноритарных аукционеров, для того чтобы под флагом этой оппозиции рейдеры могли проникнуть на предприятие. Руководство предприятия на этом этапе, обычно делает два шага:

1. Пытается теми или иными способами смягчить конфликт между управленцами предприятия;
2. Идет на уступки миноритарным аукционерам с целью смягчения давления оппозиции.

4 этап. Работа с активами предприятия.

На этом этапе руководство предприятия пытается сделать так, чтобы захват предприятия потерял для рейдеров смысл. Для этого руководству нужно либо вывести активы предприятия, либо каким либо образом их обременить. Рейдеры же, естественно, пытаются этого не допустить.

5 этап. Вход на предприятие.

Теперь рейдеру нужно легальным образом зайти на предприятие. Основная цель: внеочередное собрание аукционеров и переизбрание совета директоров. Делается это примерно следующим образом.

Если у рейдера имеется 30% плюс одна акция, то в действующий орган управления предприятия посылается требование о созыве внеочередного собрания аукционеров. После того, как основное собрание проигнорирует требование, рейдеры имеют право провести такое собрание самостоятельно. Как правило, подобные собрания проводятся скрытно, чтобы на нем могли присутствовать только подконтрольные рейдеру аукционеры. Известно немало случаев, когда подобные собрания проводились в воинских частях. Таким образом, рейдеры делают все, чтобы «ненужные» аукционеры не попали на собрание. Известны случаи, когда рейдеры для этой цели разыгрывали целые спектакли. Например, перед входом в здание, где должно проходить собрание аукционеров, представители рейдера на входе в здание перехватывали ненужных участников собрания и вели их в другой зал этого же здания, где перед ними разыгрывался спектакль под названием «собрание аукционеров». В это же самое время на настоящем собрании в другом зале рейдерская партия большинством голосов переизбирала совет директоров. Иногда применяется обратный подход, при котором, наоборот, оппоненты допускаются на собрание для того, чтобы всему миру показать, что все законно, что на собрании были не только подконтрольные рейдеру оппоненты, но и представители противоположной стороны. Только при этом акции оппонента каким-либо образом «блокируются» т.е делается так, чтобы оппонент временно не может воспользоваться своими акциями, что на него заведено уголовное дело на предмет того, что когда-то он добыл эти акции незаконным путем.



На первом собрании 30% плюс одна акция не является достаточным кворумом для принятия решения, поэтому на первом собрании констатируется отсутствие кворума, эта констатация заносится в протокол собрания, и все расходятся. Изюминка в том, что если собрать собрание повторно,30% плюс одна акция уже будет кворумом, и решения принимаются большинством голосов. Решения и принимаются: прекратить полномочия прежнего совета директоров и избрать новый совет директоров. Таким образом создается параллельный орган управления. Умные рейдеры, чаще всего, делают еще один остроумный шаг. Они делают так, что один из участников собрания… направляет в суд претензию к проведению собрания и просит признать суд собрание недействительным. Казалось бы зачем рейдерам это надо? Это же нелогично. На самом деле все логично. Повод для претензии выбирается очень формальный, и желательно какой-то вздорный, обычно такой, который суд не признает значимым. Суд и не признает и отказывает в удовлетворении иска. А поскольку заседание суда прошло, то у рейдера появляется документ о том, что фактически суд признал собрание легитимным - это называется преюдиция. Документ этот, естественно, очень ценный. После того как прошло собрание аукционеров с переизбранием совета директоров, по сути предприятие в руках рейдеров, и параллельный орган управления берет на себя контроль над деятельностью предприятия.

Дальнейшее развитие событий зависит от того, какую цель ставили перед собой рейдеры, захватывая предприятие. Если они захватывали предприятие с целью наживы, то после захвата быстро реализуется цепочка по продаже предприятия. Нередко, что в результате реализации этой цепочки предприятие попадает к добросовестному хозяину. Если же целью рейдеров был бизнес предприятия, то после захвата начинается этап «ликвидации последствий военных действий»: начинаются выплаты зарплат сотрудникам, делаются перечисления в бюджет и прочее. Нередки случаи, когда прежние руководители предприятия переквалифицировывались в рейдеров и

начинали отбирать у захватчиков свое бывшее родное предприятие по всем правилам рейдерской атаки.

Естественно подробное описание всех этапов рейдерской атаки выходит за рамки нашего курса, но нам это и не особо важною. Для нас важно прежде всего то, что на многих этапах этой атаки используются приемы социальной инженерии и социального программирования.

Где же применяются социальная инженерия и социальное программирование при организации рейдерских атак?

Социальная инженерия в классическом виде применяется в основном на первом этапе, то есть тогда, когда собирается информация об организации. А как мы говорили ранее, собирать информацию проще всего методами социальной инженерии. На втором этапе к методам социальной инженерии добавляются методы социального программирования, поскольку второй этап это начало рейдерской атаки, это уже не сбор информации, а работа по дестабилизации деятельности предприятия. И на этом этапе лучше подходят различные методы социального программирования, один из которых – устройство предприятию атаки «отказ от обслуживания». Методы же социальной инженерии на втором этапе тоже могут применятся, к примеру, для дискредитации компании в сети Интернет. Для этого обычно используются форумы, на сайте компании и прочие инструменты, посредством которых представители компании общаются в Интернете с посетителями своего сайта. Ну и конечно на третьем этапе, интриг и разговоров без социального программирования тоже никуда, конечно в области его отрицательного применения. Резюмируя вышесказанное, можно отметить, что основные и значимые этапы «рейдерского наезда» - это социальное хакерство в чистом виде.



Почему социальное хакерство и социальное программирование популярный инструмент для рейдерских атак?

Дело в том, что основная концепция социального программирования состоит в том, что многие поступки людей и групп людей предсказуемы и подчиняются определенным законам. Простой и банальный пример. Если на предприятии стало плохо, то люди с него побегут. Совершенно понятная вещь. А ведь это социальное программирование в чистом виде. Сотрудники предприятия – это одна большая социальная группа. А сказав фразу «если на предприятии стало плохо, то люди с него побегут» мы, по сути, сказали, что разработали метод воздействия на большую социальную группу, в которой в данном случае является многотысячная армия сотрудников предприятия. Таким образом мы предсказали как будет вести себя данная социальная группа под воздействием некой внешней силы. Внешняя сила здесь - это ухудшение обстановки на предприятии, а прогнозируемый нами способ поведения – это констатация факта, что при ухудшении условий сотрудники покинут предприятие. На примере этого мы увидели, что даже большой социальной группой можно вполне осознанно управлять, так как ее действия вполне прогнозируемы.

Как определить начало рейдерской атаки?

То, что на вас начата атака можно определить по нескольким признакам.

- Начались проверки предприятия различными ведомствами и инстанциями: налоговой полицией, санэпидемстанцией, МЧС, МВД, различными надзорными организациями и

прочее. Причем проверяющие просят предоставить копии документов, в которых указаны сведения о активах фирмы, о кредиторской задолженности, об акционерах.

- В средствах массовой информации, СМИ, интернете появляются негативные статьи о предприятии, его руководстве, да и вообще неожиданно ни с того ни с сего СМИ стали проявлять повышенную активность, в отношении предприятия. Особенно этот пункт должен вас насторожить, если в СМИ появляются сообщения об ущемлении прав миноритарных аукционеров.
- Аукционеры вдруг получили заказные письма с уведомлением о вручении, в которых находится, к примеру, поздравление с ближайшим праздником. Или вообще ничего не находится. Или находится просто чистый лист бумаги. Не важно. Главное, что таким образом те, кто собрался вас атаковать имитируют формальность, так как согласно закону перед созывом внеочередного собрания аукционеров нужно им направить предложение о созыве такого собрания. Вот и направили. А потом в суде атакующие скажут, что аукционерам было направлено предложение о внеочередном собрании аукционеров. Судья попросит предъявить доказательства, того какие письма были направлены. Этим доказательством будет уведомление о вручении письма. А то что, противоположная сторона будет говорить, мол, не правда, там лежали открытки, так на это всегда можно сказать, что там лежали, реальные документы, а про открытки это все наглая ложь.
- Миноритарные аукционеры начинают проявлять интерес к деятельности предприятия, чего за ними никогда не наблюдалось. Особенно надо насторожится в том случае, когда действуют не они сами, а по генеральной доверенности от их имени действуют какие-то родственники, которые, как нельзя кстати, являются большими специалистами в корпоративном праве.
- Вам часто стали поступать предложения о продаже ваших акций или их доли.



Таким образом, любой вид социальной инженерии практически всегда используется со злым умыслом. Некоторые люди, конечно, говорят о ее пользе, указывая на то, что с ее помощью можно разрешать социальные проблемы, сохранять социальную активность и даже адаптировать социальные институты к меняющимся условиям. Но, несмотря на это, успешнее всего ее применяют для:

- Обмана людей и получения конфиденциальной информации;
- Манипулирования и шантажа людей;
- Дестабилизации работы компаний для последующего их разрушения;
- Воровства баз данных;
- Финансовых махинаций;
- Конкурентной разведки.
- Рейдерские атаки

Естественно, это не могло остаться незамеченным, и появились методы противодействия социальной инженерии.

**Защита от социальной инженерии**

Сегодня в крупных компаниях систематически проводят всевозможные тесты на сопротивляемость социальной инженерии. Почти никогда действия людей, подпавших под атаку социальных хакеров, не носят умышленного характера. Но тем они и опасны, ведь если от внешней угрозы защититься сравнительно легко, то от внутренней – намного сложнее.

Чтобы повысить безопасность, руководство компаний проводит специализированные тренинги, контролирует уровень знаний своих сотрудников, а также само инициирует внутренние диверсии, что позволяет установить степень подготовленности людей к атакам социальных хакеров, их реакцию, добросовестность и честность. Так, на E-Mail могут присылать «зараженные» письма, вступать в контакт в Skype или соцсетях.

Сама же защита от социальной инженерии может быть как антропогенной, так и технической. В первом случае привлекается внимание людей к вопросам безопасности, доносится суть серьезности данной проблемы и принимаются меры по привитию политики безопасности, изучаются и внедряются методы и действия, повышающие защиту информационного обеспечения. Но у всего этого есть один недостаток – все эти способы пассивны, и многие люди просто пренебрегают предупреждениями.

Что же касается технической защиты, то сюда относятся средства, затрудняющие доступ к информации и ее использованию. Учитывая то, что самыми «популярными» атаками социальных хакеров в Интернете стали электронные письма и сообщения, программисты создают особое ПО, фильтрующее все поступающие данные, и это касается как частных почтовых ящиков, так и внутренней почты. Фильтры анализируют тексты входящих и исходящих сообщений. Но здесь есть трудность – такое программное обеспечение загружает серверы, что может тормозить и сбивать работу системы. К тому же невозможно предусмотреть все вариации написания потенциально опасных сообщений. Однако технологии совершенствуются.



А если говорить конкретно о средствах, препятствующих использованию полученных данных, они делятся на:

- Блокирующие использование информации везде, кроме рабочего места пользователя (аутентификационные данные привязываются к электронным подписям и серийным номерам комплектующих ПК, физическим и IP-адресам);
- Блокирующие автоматическое использование информации (сюда относится всем нам знакомая Captcha, где паролем служит картинка или ее искаженная часть).

Оба этих способа блокируют возможность автоматизации и смещают баланс между ценностью сведений и работой по их получению в сторону работы. Поэтому даже при наличии всех данных, выданных ничего не подозревающими пользователями, социальные хакеры сталкиваются с серьезными трудностями в их практическом применении.

А любому обычному человеку для защиты от социальной инженерии мы советуем просто сохранять бдительность. Получая на электронную почту письмо, обязательно внимательно читайте текст и ссылки, старайтесь понять, что находится в письме, от кого оно пришло и зачем. Не забывайте пользоваться антивирусами. Если же неизвестные звонят по телефону с незнакомого номера, никогда не называйте своих личных данных, тем более тех, которые касаются ваших финансов.

**Лабораторные задания к 4 уроку.**

Самостоятельно найти в интернете реальные кейсы, по одному кейсу на каждый вид атаки.

Проанализируйте каждую атаку и составьте приблизительный вывод по каждой атаке согласно схеме:

- Сбор информации об объекте. Какая информация была собрана, или возможно была собрана для проведения данного вида атаки, какую цель преследовал социальный инженер.
- Внедрение. Каким образом было осуществлено внедрение, какие методы и подходы применялись.
- Аттракция. Как была применена непосредственная атака.
- Итог. Каким образом атака получила успех.