Социальная инженерия. Угрозы и защита: литературный обзор

Статья переведена @N3M351DA (@in51d3) и @beh1ndy0urback

Предисловие

В этой статье рассматриваются аспекты социальной инженерии. На рынке существует множество приложений и оборудования для обеспечения безопасности, но все еще есть методы, которые используются для обхода защиты персональной или корпоративной информационной безопасности. Атаки с использованием социальной инженерии направлены на получение информации для кражи личных данных, паролей или осуществления атак другого типа. Угрозу представляют комбинации атак социальной инженерии с другими типами: фишингом, атакой на «водопое», от которых трудно защититься. Данное исследование направлено на изучение влияния

современных методов социальной инженерии на организации и частных лиц. Оно описывает категории социальной инженерии и каким образом злоумышленник использует в своих интересах человеческое поведение. Так же я хочу обсудить прямые и косвенные атаки социальной инженерии и способы защиты от них.

1. Введение

Социальная инженерия – это один из немногих типов атак, который в целом можно классифицировать как нетехнический тип, но в то же время он может эффективно сочетаться с техническими атаками, такими как шпионское ПО и троянские программы. Людьми можно очень легко манипулировать, заставляя предоставлять информацию или другие детали, которые могут быть полезны злоумышленнику. «Социальные инженеры не обязательно являются технически подкованными людьми, но они хитры и находчивы», – говорит главный операционный директор Social Engineer. Сегодня большинство компаний и банков используют интернет и смартфоны. Они тратят большие деньги на покупку программных и аппаратных средств для обеспечения безопасности, но в то же время наивный работник может предоставить всю информацию, необходимую злоумышленнику, не прибегая к взлому системы. Социальная инженерия использует человеческий фактор, который является самой слабой точкой в любом институте или организации. Людей легче взломать, чем компьютерные системы и сети. Большинство людей воспитаны добрыми и вежливыми, что заставляет их доверять другим. Концепция плохих людей, пользующихся добрыми и честными, не укладывается в понимание большинства людей. Социальные инженеры креативны и сообразительны, они используют различные методы для доставки вредоносного программного обеспечения, получения личной информации, для мошенничества или получения доступа к защищенным системам.

2. Категории социальной инженерии.

Существуют две основные категории, по которым можно классифицировать все методы социальной инженерии:

1) Методы, основанные на компьютерных или иных технологиях: заключаются в том, чтобы обмануть пользователя, заставив его поверить в то, что он взаимодействует с реальной компьютерной системой, и заставить его предоставить конфиденциальную информацию.

2) Метод, основанный на человеческом факторе: осуществляется путем обмана, используя невежество жертвы и естественную склонность человека понравиться и быть полезным.

3. Социальная инженерия и прорыв в области электроники

Социальная инженерия – это метод манипуляции, который используется, чтобы обмануть пользователей и получить доступ к компьютеру, определенной информации или базе данных. Её можно назвать самым опасным методом по следующим причинам:

1) Социальная инженерия является одной из самых успешных методов атак по сравнению с техническими.

2) Специалисты по информационной безопасности, а также пользователи компьютеров редко берут в расчет риск применения методов социальной инженерии.

3) Привычки и природа человека: люди склонны следовать определенным привычкам и действиям по умолчанию, не задумываясь и злоумышленник может использовать это в своих целях.

Основываясь на опросе, проведенном Dimension Research (2011) среди 850 специалистов в области ИТ и безопасности, проживающих в Соединенных Штатах, Канаде, Великобритании, Германии, Австралии и Новой Зеландии, в апреле 2016 года ФБР опубликовало последние статистические данные об инцидентах и потерях, связанных с компрометацией деловой электронной почты. В нем говорится, что:

1) Зафиксировано 17 642 случая компрометации деловой электронной почты в период с октября 2013 по февраль 2016 года.

2) Число выявленных жертв и потерь возросло на 270% с января 2015 года.

3) Глобальные потери от мошенничества в результате этих преступлений с октября 2013 года составляют примерно 2,3 млрд. долларов США.

Чтобы дополнить эти цифры, приведем некоторые убедительные статистические данные из Отчета о социальной инженерии за 2016 год:

1) 60% респондентов говорят, что социальная инженерия является одной из самых значительных угроз, с которыми они сталкиваются на сегодняшний день.

60% знают, что они были или могли быть жертвами атаки методом социальной инженерии в прошлом году.

2) 65% из тех, кто подвергся нападению, говорят, что учетные данные сотрудников были раскрыты в результате этих инцидентов.

4. Этапы социальной инженерии

Большинство хакеров следуют этим этапам осуществления атаки, чтобы безопасно и не вызывая подозений приблизиться к своей цели:

1. Сбор информации для социальной инженерии:

За последнее десятилетие одни из самых серьезных угроз безопасности исходят от использования социальных сетей. Быстрый рост этих технологий позволяет миллионам пользователей каждый день публиковать сообщения в Facebook, Twitter и многих других социальных сетях. Тип информации, которую они публикуют, может выглядеть маловажной, но это ключ для з апуска успешной атаки, например:

а) Личная информация.

б) Фотографии.

в) Информация о местоположении.

г) Информация о друзьях.

д) Деловая информация.

е) Предпочтения пользователя.

Опасность предоставления такой информации в том, что любопытный злоумышленник может собрать воедино эти источники и получить четкое представление о человеке или его делах. После того, как сообщение опубликовано, удалить его из интернета практически невозможно. Тем более, что оно, возможно, уже был передано другим пользователям и размещено заново. Имея эту информацию в руках, злоумышленник может использовать социальную инженерию, чтобы убедительно выдать себя за этого человека или получить прибыль от использования инсайдерской информации. Также много программ-червей распространяются через социальные сети. В большинстве случаев они используют приемы социальной инженерии для публикации заманчивых сообщений от имени зараженного пользователя. Социальные сети

могут быть интересными, но в то же время они могут значительно облегчить работу злоумышленника, основываясь на огромном объеме данных и личной информации, которая в них содержится.

2) Развитие доверительных отношений с жертвой.

Развитие доверительных отношений может осуществляться с помощью инсайдерской информации, которая обычно используется для того, чтобы выставить себя более опытным и авторитетным человеком. В человеской природе доверять другим, пока они не предадут доверие. Если кто-то говорит нам, что является кем либо, мы обычно принимаем это заявление. Если кто-то говорит нам, что является кем либо, мы обычно принимаем это заявление. Иногда мы боимся попасть в неприятности или ленимся выключить компьютер после окончания нашей работы. Опытный хакер всегда попытается использовать эту уязвимость, прежде чем тратить время и усилия на другие методы взлома паролей или получения доступа к системам.

3) Эксплуатация отношений:

На этом этапе злоумышленник сосредотачивается на поддержании ощущения соответствия образу, созданному на шаге 2. Манипулируя жертвой, он старается привести ее в определенное эмоциональное состояние, соответствующее плану. Атакующий должен изучить эмоциональное состояние своей жертвы и узнать, как использовать его в своих интересах. Эксплуатация может осуществляться путем разглашения, казалось бы, не важной информации или доступа, которым располагает злоумышленник. Примеры успешной эксплуатации включают в себя:

а) Персональную информацию: удержание открытой двери или иное проникновение злоумышленника внутрь помещения.

б) Предоставление социального доказательства: цель или какое-то доверенное лицо представляет социального инженера другим сотрудникам компании.

в) Разоблачение коммерческой тайны в разговоре с предполагаемым «собеседником».

4) Исполнение:

На этом этапе начинается настоящая атака без предупреждения. Лучше оставить у жертвы ощущение, что он сделал что-то хорошее – это позволит продолжить возможную эксплуатацию этого контакта в будущем.

5. Аспекты атак с применением социальной инженерии

Атака методом социальной инженерии может производиться на нескольких уровнях:

1) Сенсорный уровень: основное внимание уделяется местоположению и окружающей среде, в том числе:

а) Рабочим местам: злоумышленник под видом работника, подрядчика, уборщика или работника по техобслуживанию бродит по офисам и пытается собрать любую полезную информацию, чаще всего пароли.

б) Телефонам: наиболее уязвимыми для этого типа атак являются работники центров тех. поддержки. Например, злоумышленник может связаться с центром тех. поддержки, запросить некоторую техническую информацию и постепенно получив, например, пароли, использовать их для атаки на компьютеры корпоративного сектора.

в) Отходам: это один из самых популярных методов для атакующих, использующих социальную инженерию, поскольку злоумышленник, может не привлекая внимания собрать таким образом важную информацию, например, пароли, информацию о корпоративной структуре, номера и имена сотрудников, даты встреч, чеки и счета.

г) Интернет: обычно один и тот же пароль используется для нескольких сайтов, чтобы их было легче запомнить. Единожды скомпрометировав такой пароль, злоумышленник с легкостью проникнет во все приложения и аккаунты пользователя.

2) Психологический уровень: злоумышленник создает вокруг жертвы определенный психологический климат, атмосферу, которая поможет втереться в доверие к жертве и убедить ее, что злоумышленник – доверенное лицо и имеет полное право просматривать конфиденциальную информацию о своей цели или учреждении.

6. Методы социальной инженерии

Существует несколько методов атак с использованием социальной инженерии, в частности:

1) Искушение иметь что-то редкое: у людей зачастую есть желание владеть чем-то особенным, редким. Желание владеть возрастает, когда мы чувствуем, что

этот шанс может быть последним. Злоумышленник может использовать эту мысль, чтобы подтолкнуть жертву к попытке завладеть тем, что он желает, независимо от его стоимости.

2) Показать сходство с целью: люди имеют тенденцию чувствовать себя в безопасности среди людей одинаковой расы, цвета кожи, со схожими проблемами и природой. Наше чувство существования параллелей с кем-то делает нас менее осторожными при общении со «схожим» человеком.

3) Возврат долга: мы обычно хотим вернуть долг; это свойство прочно укоренилось в племенных и семейных общинах. Атакующий оказывает услугу цели, что заставляет ее чувствовать себя должником. Это чувство заставляет цель помогать атакующему, предоставляя ему некоторую информацию или позволяя ему использовать свое устройство.

4) Лесть: многие сотрудники и члены общества стремятся создать хорошее представление о себе, поэтому некоторые из них, не колеблясь, предоставят информацию, необходимую злоумышленнику, чтобы почувствовать себя хорошо. Обычно злоумышленники льстят жертве, которая имеет полномочия или связана с представителем власти в компании или учреждении, чтобы завоевать его доверие.

5) Движение по течению: в обществе принятно, что человек не должен идти против большинства и злоумышленники, зная об этом, нанесут удар, используя эту точку. Используя традиции общества, злоумышленники могут легко добраться до жертвы и заставить его дать информацию или совершить определенное действие.

6) Предлоги: это также известно в Великобритании как подначивание – это процесс создания и использования сценария для вовлечения жертвы таким образом, чтобы увеличить вероятность, что она разгласит информацию или выполнит действия, которые были бы маловероятными для нее в обычных обстоятельствах. Этот метод используется, чтобы обмануть какой-нибудь бизнес и заставить его сотрудников раскрыть информацию о клиентах, также он используется частными следователями для получения телефонных, служебных или банковских записей или другой информации непосредственно у представителей сервисной службы компании. Так же он может использоваться злоумышленником, чтобы выдать себя за коллегу, полициейского, сотрудника банка, налоговых органов или любым другим лицом.

7) Обратный социальный инжиниринг: это один из продвинутых способов завоевать доверие цели и затем получить информацию. Этот метод применяется путем создания позиции, которая показывает злоумышленника в форме человека с наличием административных или технических полномочий, так, что цель может начать просить помощи и получать инструкции у него. Злоумышленник может добиться этого, применив следующие действия:

а) Подделав идентификатор должности.

б) Представившись от имени человека, обладающего необходимыми знаниями или полномочиями, чтобы справиться с ситуацией.

в) Оказав реальную помощь.

8) Фишинг: это метод мошеннического получения частной информации. Согласно отчету Verizons о разглашении конфиденциальных данных за 2016 год, фишинг был связан с 9576 нарушениями, 916 из которых привели к подтвержденным утечкам данных. В последнем отчете Института непрерывности бизнеса (BCI) (2017) говорится что данный фишинг был частью 21 vishing (голосового фишинга), который использует поддельные данные идентификатора вызывающего абонента, чтобы создать впечатление, что звонки поступают из доверенной организации. SMS-фишинг использует текстовые сообщения, чтобы побудить людей разглашать свою личную информацию.

9) Целевой фишинг: это метод, который обманным путем получает личную информацию, отправляя сильно кастомизированное электронное письмо нескольким конечным пользователям. Это основное различие между фишинговыми атаками, потому что фишинговые кампании фокусируются на рассылке больших объемов обобщенных электронных писем, ожидая, что ответят лишь несколько человек. С другой стороны, фишинговые электронные письма требуют, чтобы злоумышленник провел дополнительное исследование своих целей, чтобы «обмануть» конечного пользователя. Уровень успешности целевых фишинг-атак значительно выше, чем обычных фишинг-атак.

10) Атака «на водопое»: термин «водопой» относится к началу атаки против целевых предприятий и организаций. Атакующий использует стратегию социальной инженерии, которая использует доверие пользователей к определенным веб-сайтам, которые они регулярно посещают. Целью этой атаки не является распространение вредоносного ПО как можно большему количеству систем, вместо этого злоумышленники используют эксплойты на известных и надежных сайтах, которые, вероятно, посетят их жертвы. Это делает технику

«водопоя» эффективной для доставки его предполагаемой полезной нагрузки. Эта стратегия была успешно использована для получения доступа к некоторым (предположительно) очень защищенным системам. Подготовка к этому типу атаки начинается со сбора информации, чтобы подтвердить, что цели посещают данные веб-сайты и что система разрешает такие посещения. Затем злоумышленник проверяет эти веб-сайты на наличие уязвимостей для внедрения кода, который может заразить систему жертвы вредоносным ПО. Как только жертвы посещают взломанный сайт, эксплойт использует уязвимости программного обеспечения для установки вредоносных программ. Установленное вредоносное ПО может быть представлено в форме трояна для удаленного доступа, который позволит злоумышленникам получить доступ к защищенной системе и конфиденциальные данные.

7. Защита от социальной инженерии

1) Организация может приобрести страховку от хакерских атак, но это требует четких и строго определенных политик безопасности, в которых описаны процедуры доступа к информации.

2) Не доверяйте никаким электронным письмам, которые запрашивают информацию вроде имени пользователя, пароля и номера кредитной карты, или просят вас перейти по ссылке и ввести такую информацию там, подлинные организации в Интернете не запрашивают личные данные в электронных письмах. Если электронное письмо не имеет цифровой подписи, вы не можете быть уверены, что оно не было подделано, потому что любой может отправить его от любого имени, следовательно, когда в письме говорится о чем-то важном, лучше проверить полные заголовки.

3) Постоянно проверяйте выписки по своим банковским, кредитным и дебетовым картам, чтобы убедиться, что все транзакции верны.

4) При обращении в финансовое учреждение используйте только официальный сайт, большинство из которых используют протокол https. Это хорошая защита от фишинговых атак.

5) Убедитесь, что ваш специалист по информационной безопасности знает, как обращаться с атаками методом социальной инженерии, поскольку каждая атака имеет свою сигнатуру и цель. Также используйте программную защиту, такую как антивирусы, брандмауэры и антишпионские программы, чтобы защититься от вирусов, троянских программ, шпионского и рекламного ПО.

6) Обучение пользователей и работодателей является важной частью системы безопасности. Тренеры должны сосредоточиться на различных сценариях атак социальной инженерии и на том, как пользователям на них реагировать.

8. Заключение

В этой статье описаны общие способы, используемые для современных атак методом социальной инженерии, и раскрыта растущая на сегодняшний день угрозу данных атак.

Подобные атака представляет большую опасность, так как может успешно сочетаться с техническими атаками типа шпионского, троянского ПО, фишинга; так же она нацелена на самое слабое звено в любой системе – на человека. Для такой атаки люди – самая легкая мишень, но также и самый лучший инструмент для защиты от нее.

Были рассмотрены уровни социальной инженерии и то, как злоумышленник может подобраться к цели и манипулировать ею. Увеличение числа людей, использующих социальные сети, облегчает работу для злоумышленника, поскольку большинство из пользователей непреднамеренно делятся в них личными и конфиденциальными данными. Также известно, что организация должна обеспечивать информирование своих сотрудников об угрозе социальной инженерии и убедиться, что её политика безопасности и процедуры доступа к данным выполняются должным образом.
