Краткая сводка

Взлом «операционной системы» человека

Радж Самани (Raj Samani), главный технический директор компании McAfee в регионе EMEA

Чарльз Макфарланд (Charles McFarland), старший инженер-исследователь McAfee Threat Intelligence Service

intel Security

Одной из составляющих многих кибератак являются методы социотехники («социальной инженерии»). С их помощью злоумышленники пытаются убедить человека, выбранного ими в качестве объекта кибератаки, совершить то или иное действие, приводящее к заражению системы или раскрытию ценной информации.

Несмотря на то, что при устранении последствий атаки основное внимание уделяется устранению технических проблем, наличие человеческой составляющей приводит к тому, что в случившемся начинают винить того, кто стал объектом атаки, а от остальных сотрудников начинают требовать большей осторожности в вопросах безопасности. Проблема, однако, в том, что в большинстве организаций мало что предпринимается для выяснения того, почему злоумышленникам удалось успешно атаковать выбранный ими объект и, что более важно, что (помимо требований о большей осторожности) следует делать для снижения риска новых атак.

Термину «социотехника» можно дать следующее определение:

> *Намеренное использование методов, нацеленных на то, чтобы обманным путем подтолкнуть человека к раскрытию информации или совершению действий, которые могут привести к раскрытию информации.*

В ходе социотехнической атаки объект атаки не осознает, что его действия являются вредоносными. Методы социотехники основаны на злоупотреблении доверчивостью объекта атаки, а не на использовании его преступных инстинктов. Атаки можно разделить на две категории:

- «охота», предполагающая получение информации при минимальном взаимодействии с объектов атаки. При таком подходе взаимодействие, как правило, сводится к одиночному контакту атакующего с атакуемым, и после получения информации атакующий сразу прекращает общение с атакуемым;
- «животноводство», предполагающее установление продолжительных отношений с объектом атаки с целью его «доения» (т. е. получения информации) на протяжении длительного периода времени.

Социотехнические атаки с использованием электронной почты в качестве средства связи чаще всего носят характер «охоты». Конечно, есть исключения вроде «нигерийских писем», в которых делаются попытки продлить контакт с целью извлечения большего количества денег. Социотехнические атаки в категориях «охота» и «животноводство» проводятся, как правило, в четыре этапа:

1. Сбор информации. Цель этого необязательного этапа — сбор информации об объекте атаки. На этом этапе злоумышленник собирает информацию, которая поможет «зацепить» объект атаки: информацию о его увлечениях, месте работы, поставщике финансовых услуг и т. п.
2. «Зацепка». Цель «зацепки» — успешно «развести» объект атаки, вступив с ним в контакт и создав повод для взаимодействия. Психолог Роберт Чалдини (Robert Cialdini) описал шесть рычагов влияния на подсознание объекта атаки:
   - взаимность: получив что-либо, люди чувствуют себя обязанными и стремятся дать что-нибудь взамен;
   - дефицит: люди склонны выполнять просьбу, если считают, что речь идет о чем-то редком;
   - последовательность: если объект атаки пообещал что-то сделать, то он будет стремиться выполнить данное обещание, чтобы не казаться неблагонадежным;
   - симпатия: объект атаки охотнее выполняет просьбу, если злоумышленник ему симпатичен;

  - власть: люди склонны выполнять просьбы, поступающие от представителей власти;
  - социальное доказательство: склонность выполнять просьбу, если другие делают то же самое.

3. «Разводка». Выполнение основной части атаки. Это может быть раскрытие информации, переход по ссылке, перечисление денежных средств и т. д.
4. Выход. Завершение взаимодействия. Во многих атаках, относящихся к категории «животноводство», злоумышленнику выгодно выходить из игры так, чтобы не вызывать подозрений. Однако это не всегда необходимо. Например, когда злоумышленнику удается убедить объект атаки раскрыть данные платежной карты, он, как правило, не хочет вызывать подозрений, чтобы объект атаки не заблокировал свою карту, объявив ее потерянной или украденной. Однако, если злоумышленнику удалось украсть исходный код или личную информацию, то объект атаки не сможет восстановить украденные данные даже в том случае, если у него возникли подозрения.

Попытки применения методов социотехники не всегда линейны: та или иная отдельная атака может быть частью более крупной кампании по сбору взаимосвязанных данных. Например, злоумышленники могут провести одну атаку, получить необходимую информацию и исчезнуть. Или же они могут провести ряд атак, относящихся к категории «охота», а затем, используя собранную информацию, инициировать атаку, относящуюся к категории «животноводство».

Каналы атаки

Для проведения атак злоумышленники-социотехники могут использовать разные каналы.

- Веб-сайты. В качестве канала для социотехнических атак нередко используются вредоносные веб-сайты. Согласно отчету компании Verizon о расследовании утечек данных за 2014 год (2014 Verizon Data Breach Investigations Report) «в 20 % атак, проводимых с целью шпионажа, для доставки вредоносного ПО используются механизмы стратегического взлома веб-сайтов».
- Электронная почта. Самыми распространенными видами социотехнических атак с использованием электронной почты являются фишинг вообще и целенаправленный фишинг в частности. Рассылка электронных почтовых сообщений является эффективным методом проведения атак, поскольку согласно отчету Verizon «по ссылкам в фишинговых электронных сообщениях переходит 18 % пользователей».
- Телефон. Этот канал связи пользуется популярностью у информационных посредников.
- Личная встреча. Встретившись с сотрудником компании лично, злоумышленники могут принудительно или обманным путем заставить его предоставить информацию.
- Почтовая служба. Хотя этот канал и не столь популярен, как другие, но он тоже присутствует в общей статистике по атакам.
- Факс. Примером атаки по факсу может быть поддельное сообщение от системы электронных платежей.

Защита от социотехнических атак

Ниже перечислены средства, которые можно использовать для уменьшения опасности социотехнических атак. Эти средства разделены на три категории: люди, процессы и технологии. Данный список не является исчерпывающим и применим не ко всем организациям.

Люди

- Устанавливайте четкие границы. Все сотрудники должны быть ознакомлены с принятыми в организации правилами раскрытия информации и иерархическим порядком обработки запросов, выходящих за пределы их полномочий.
- Постоянное обучение. Должна быть разработана и внедрена программа повышения осведомленности сотрудников в вопросах безопасности, предполагающая постоянное обучение сотрудников. Для привлечения внимания сотрудников к распространенным тактикам проведения атак используйте такие инструменты, как специальный тест McAfee на умение распознавать фишинг.

- Разрешение на проверку. Сделайте так, чтобы ваши сотрудники не боялись сомневаться даже в самых безобидных на вид запросах. Например, сотрудник должен не бояться расспросить человека, пытающегося вслед за ним пройти в служебное помещение.
- Объясняйте важность информации. Даже самая незначительная на вид информация, такая как номера телефонов (информация, дающая новые возможности), может быть использована для проведения атаки.
- Не занимайтесь поиском виновных. Объекты социотехнических атак являются жертвами. Наказывая отдельных сотрудников, ставших жертвами обмана, вы создадите атмосферу, в которой сотрудники будут менее готовы признаваться в разглашении информации. Будучи один раз обманутыми, они могут попасть под контроль злоумышленника, который затем может начать их шантажировать.

Процессы

- Отчеты о подозрительных звонках. При обнаружении подозрительных действий сотрудники должны составлять отчеты с указанием всех подробностей. Это помогает расследовать инциденты.
- Информативные блокирующие страницы. При переходе сотрудника на вредоносную веб-страницу у него должна отобразиться блокирующая страница с информацией о причинах блокирования. Это заставит их задуматься о своих предыдущих действиях и поможет выявить источники атаки.
- Оповещение клиентов. Когда организация отказывает звонящим в предоставлении информации, она должна сообщить им об этом и проверить, имеет ли звонящий право на получение запрашиваемой информации. Кроме того, организациям следует установить порядок обмена информацией с клиентами. Например, PayPal предоставляет пользователям следующую инструкцию по проверке подлинности получаемых электронных сообщений: «в своих электронных письмах мы никогда не запрашиваем информацию следующего типа: номера банковских карт, номера банковских счетов, номера водительских удостоверений, адреса электронной почты, пароли, ваше полное имя».
- Иерархический порядок. Для персонала, непосредственно работающего с клиентами, должен быть разработан простой порядок передачи потенциально мошеннических сообщений на рассмотрение в вышестоящие инстанции.
- Оперативная проверка готовности персонала. Регулярно проводите проверки на уязвимость сотрудников к социотехническим атакам с использованием разных каналов связи. Такие проверки позволяют оценить эффективность программ обучения.

Технологии

- Запись телефонных разговоров. Регулярно записывайте входящие телефонные звонки — это помогает расследовать инциденты.
- Линии для подозрительных звонков. Перенаправляйте подозрительные звонки на контролируемый номер.
- Фильтрация электронной почты. Удаляйте мошеннические электронные сообщения, содержащие известные и неизвестные вредоносные программы.
- Фильтрация веб-трафика. Блокируйте доступ к вредоносным веб-сайтам и обнаруживайте вредоносные программы в процессе предоставления доступа в Интернет.
- Строгая проверка подлинности. Не устраняя полностью риск того, что в результате социотехнической атаки пользователи могут раскрыть злоумышленникам свои учетные данные, многофакторная проверка подлинности, однако, значительно усложняет злоумышленникам задачу получения учетных данных.

Подпишитесь на
McAfee Labs

Выводы

Опасность социотехнических атак очень серьезна. С их помощью киберпреступники незаконно получают доступ к информации, используемой ими затем в различных вредоносных целях. Для эффективной борьбы с этой проблемой необходимо понимать природу социотехнических атак. Это значит, что необходимо уметь выявлять наиболее вероятных действующих лиц, используемые ими методы проведения атак и имеющиеся у них ресурсы, а затем принимать соответствующие меры по снижению уровня риска, связанного с такими атаками.

Полный текст отчета см. на странице **www.mcafee.com/hacking-human-os.**

Twitter@Raj_Samani

Twitter@CGMcFarland

1. **http://www.verizonenterprise.com/DBIR/2014/**
2. **https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ**

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com