Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Социальная инженерия**
- **Обнаружение и блокировка атак Социальной инженерии**
- **Предотвращение потенциальных атак Социальной инженерии**

Социальная инженерия

Обзор

Широко распространено ошибочное мнение, что кибер преступники используют только сложные хакерские инструменты и технологии для взлома компьютеров, мобильных устройств и учетных записей. Это далеко не так. Кибер преступники давно поняли, что один из простейших способов кражи вашей информации или атаки на ваш компьютер – просто поговорить с вами и ввести вас в заблуждение. В этом выпуске мы узнаем, как работают эти атаки «с человеческим лицом» (их называют атаками социальной инженерии) и как вы можете защитить себя от них.

Автор выпуска

Алисса Торрес – сертифицированный инструктор Института SANS. Она специализируется на расследованиях сложных компьютерных преступлений и реагирования на инциденты. У неё большой практический опыт обработки последствий инцидентов и расследования кибер преступлений. Алисса ведет свой блог в Twitter как **@sibertor**.

Социальная инженерия

Социальная инженерия – это тип психологической атаки, при которой нападающий вводит вас в заблуждение, в результате которого вы сделаете то, что им нужно. Социальная инженерия существует тысячи лет; идея мошенничества и манипуляций не нова. Однако, кибер преступники осознали, что использование этих манипуляций в Интернете чрезвычайно эффективно; миллионы людей могут стать потенциальными жертвами. Простейший способ понять, как работает социальная инженерия – рассмотреть типичный пример из реальной жизни.

Кто-то звонит вам и представляется сотрудником компании по сопровождению компьютеров, вашего интернет провайдера или Службы поддержки компании Microsoft. Звонящий объясняет, что они зафиксировали странное поведение вашего компьютера, такое как сканирование Интернета или рассылка спама, и они считают, что ваш компьютер заражен. В их обязанности входит расследование этой проблемы и помощь вам в обеспечении безопасности вашего компьютера. Затем они используют множество сложных технических терминов и помогают вам проделать непонятные операции и тесты с целью убедить вас, что ваш компьютер заражен.

Например, они могут попросить вас проверить наличие определенных файлов на вашем компьютере. Они любезно проинструктируют вас, как найти эти файлы. Когда вы обнаружите эти файлы, звонящий будет уверять вас, что наличие этих файлов является признаком заражения вашего компьютера. На самом деле, это обычные системные файлы, которые могут быть найдены на каждом компьютере. Как только они убедят

Социальная инженерия

вас в том, что ваш компьютер заражен, они будут настаивать, чтобы вы посетили определенный веб сайт и купили их приложение по обеспечению безопасности. Они могут попросить вас предоставить им удаленный доступ к вашему компьютеру для того, чтобы они могли удалить вредоносные программы с него. Однако, программа, которую они продают, на самом деле является вредоносной. Если вы купили и установили эту программу, то они не только одурачили вас и заразили ваш компьютер; вы ещё и заплатили им за это. Если вы предоставите им удаленный доступ к вашему компьютеру, они возьмут его под свой контроль и инфицируют его.

Имейте в виду, подобные атаки социальной инженерии не ограничены телефонными звонками; используются практически любые технологии, включая фишинговые атаки по электронной почте, СМС, сообщения в сети Facebook, посты в Twitter или интернет чат. Главное, знать, чего надо опасаться.

Знание способов предотвращения, обнаружения и блокировки атак социальной инженерии – один из наиболее эффективных методов защиты.

Обнаружение и блокировка атак Социальной инженерии

Простейший способ защиты от атак социальной инженерии – использование здравого смысла. Если что-то выглядит подозрительно, это может быть атака. Типичные признаки атаки социальной инженерии:

- Кто-то пытается создать ощущение крайней срочности. Если вас вынуждают принять решение очень быстро, будьте бдительны.
- Кто-то запрашивает у вас информацию, к которой не должен иметь доступа или должен владеть этими данными.
- Что-то выглядит слишком хорошо, чтобы быть правдой. Типичный пример: вас извещают о выигрыше в лотерею, даже если вы никогда не покупали лотерейных билетов.

Если у вас есть подозрение, что кто-то пытается сделать вас жертвой атаки социальной инженерии, больше не общайтесь с этим человеком. Если кто-то звонит вам, повесьте трубку. Если кто-то пишет вам в чате, просто закройте сессию. Если вас насторожило сообщение электронной почты, удалите его. Если атака как-то связана с вашей организацией, немедленно сообщите об этом в Службу поддержки или Отдел информационной безопасности вашей организации.

Предотвращение потенциальных атак Социальной инженерии

К счастью, существуют способы предотвращения потенциальных атак социальной инженерии.

Социальная инженерия

- **Никогда и никому не сообщайте свои пароли**. Ни одна организация никогда не будет спрашивать ваш пароль. Если кто-то все же спрашивает ваш пароль, это атака.

- **Не будьте слишком откровенны**. Чем больше преступники знают о вас, тем легче для них убедить вас сделать то, что им нужно. Когда вы делитесь даже небольшими деталями о себе, со временем эта информация может помочь создать ваш достаточно полный портрет. Чем меньше информации вы сообщаете о себе в общедоступных ресурсах, включая социальные сети, обзоры товаров или открытые форумы и группы рассылки, тем меньше вероятность, что вы будете атакованы.

- **Проверьте контактную информацию**. Время от времени ваш банк, оператор мобильной связи и другие организации могут позвонить вам на вполне законных основаниях. Если у вас есть какие-либо сомнения в правомерности запроса, спросите у звонящего его имя и номер телефона. Затем найдите номер телефона компании в каком-либо надёжном источнике, например, на обороте вашей кредитной карты, выписке из вашего банковского счета или номер на веб сайте компании (обязательно сами печатайте URL в адресном поле браузера). Таким образом, когда вы позвоните в организацию, вы будете уверены, что вы говорите именно с ними. Хотя это доставляет некоторые неудобства, защита ваших персональных данных стоит этих усилий.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Ресурсы

Фишинг: атаки по электронной почте: http://www.securingthehuman.org/ouch/2013#february2013

Безопасность в социальных сетях: http://www.securingthehuman.org/ouch/2013#march2013

Избегайте мошенничества: http://www.onguardonline.gov/topics/avoid-scams

Управление «К» предупреждает: http://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Upravlenie_K_preduprezhdaet

Что такое социальная инженерия?: http://www.microsoft.com/ru-ru/security/resources/socialengineering-whatis.aspx

Что такое ложный антивирус?: http://www.microsoft.com/ru-ru/security/pc-security/antivirus-rogue.aspx

Правила безопасности при использовании социальных сетей: http://www.microsoft.com/ru-ru/security/online-privacy/social-networking.aspx

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова

