Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Что такое «социальная инженерия»**
- **Обнаружение /остановка атак социальной инженерии**

Социальная Инженерия

Обзор

Самым большим заблуждением многих людей является то, что кибер преступники атакуют учётные записи пользователей только с помощью продвинутых инструментов и техник. Но это совсем не так. Кибер преступники поняли, что часто простейшим способом кражи вашей информации, взлома ваших учётных записей или заражения ваших систем является введение вас в заблуждение, вынуждающее вас совершить ошибку. В этом выпуске мы поговорим о таком виде атак, называемых социальная инженерия, как они работают и как от них защититься.

Об авторе
Джеймс Лин (**@jameslyne**) – сертифицированный инструктор Института SANS и руководитель глобального отдела исследований компании Sophos. Он анализирует и декомпилирует новейшие и сложнейшие изобретения киберпреступников. Джеймс является автором курсов Института SANS: Metasploit (SEC580) и Социальная Инженерия (SEC567).

Что такое «социальная инженерия»

Социальная инженерия – это психологическая атака, где с помощью обмана вас вынуждают сделать то, что вы не должны. Концепция данных атак совсем не новая, ей уже тысячи лет. Вспомните «воров на доверие» или мошенников – у них подобные приёмы. Современные технологии позволяют обманывать людей более эффективно, так как вы не можете их видеть, следовательно, они могут выдавать себя за что угодно или кого угодно, обманывая миллионы людей, включая вас. Кроме того, с помощью социальной инженерии можно преодолеть многие технологии безопасности. Рассмотрим два примера атак, чтобы легче понять, как они происходят и как защитить себя от них.

Вам звонят и представляются службой поддержки компьютерной компании, вашего интернет провайдера или даже службой поддержки Microsoft. Человек, который звонит, сообщает, что ваш компьютер подозрительно активен в Интернете, это означает, что он заражен вирусом и предлагает помощь в поиске и обезвреживании вируса. Затем, используя большое количество компьютерных терминов, убеждает вас в том, что компьютер действительно заражён. Например, может попросить вас проверить наличие определенных файлов в компьютере, пошагово объяснив, где их искать. После того, ваш собеседник сообщает, что это и есть вирусы, хотя на самом деле это обычные

Социальная Инженерия

системные файлы, которые есть на любом компьютере в мире. Но если у мошенников получится убедить вас, что это вирусы, то они предложат купить антивирус или разрешить удалённый доступ к компьютеру для его установки. В любом случае вы получите вирус. Только в первом случае вы ещё и заплатите деньги за вредоносную программу. Если вы разрешите им удалённый доступ к компьютеру, то кроме установки вируса, они ещё и украдут ваши данные, будут требовать за них выкуп или будут использовать их в своих целях.

здравый смысл – ваша лучшая защита для обнаружения и прекращения большинства атак социальной инженерии.

Второй пример атаки по электронной почте, которая называется Афёра «Руководитель» (CEO Fraud) чаще всего может случится на работе. Кибер мошенники отправляют вам письмо от имени начальника или коллеги. В письме требуются немедленные действия, например, срочный перевод средств или конфиденциальных данных сотрудника. Чаще всего в письме требуют нарушить некоторые процедуры безопасности по причине срочности, например, оправить конфиденциальную информацию на личную почту @gmail.com. Такого рода атаки наиболее опасные, так как преступники тщательно их разрабатывают. В этом случае технологии безопасности, антивирусы или файрволлы, не могут обнаружить или остановить атаку, так как не задействованы вредоносные программы или ссылки.

Помните, что атаки с помощью социальной инженерии происходят не только по телефону или по электронной почте, а могут быть по любым текстовым сообщениям, в социальных сетях и даже лично. Вот ключевые моменты, которые следует знать, чтобы защитить себя.

Обнаружение/остановка атак социальной инженерии

К счастью, легко обнаружить такие атаки можно с помощью здравого смысла – это и есть лучшая защита. Если что-то вам кажется слишком подозрительным или неправильным, то это и есть атака. Вот примеры наиболее популярных атак социальной инженерии:

Социальная Инженерия

- Кто-то создаёт ситуацию срочности, пытаясь вынудить вас совершить ошибку.
- Кто-то запрашивает информацию, которую им либо не положено знать либо они уже должны знать её, например, номера банковских счётов.
- Кто-то спрашивает ваш пароль. Ни одна легальная организация не в праве этого делать.
- Кто-то заставляет вас нарушить или игнорировать процедуры безопасности, принятые в вашей компании.
- Что-то слишком прекрасно, чтобы быть правдой. Например, вам сообщают, что вы выиграли в лотерею или получили призовой iPad, хотя никогда не участвовали в розыгрыше.
- Если вы получили письмо от коллеги, написанное в необычном стиле, и создается впечатление, что письмо написано другим человеком. Возможно, учётную запись коллеги взломали и пытаются вас обмануть. Чтобы это проверить, свяжитесь с этим человеком другим способом, например, по телефону или поговорите с ним лично.

Если вам кажется, что кто-то пытается вас обмануть, сразу прекратите с ним общаться. Если атака происходит на рабочем месте, немедленно сообщите в Службу Поддержки или в отдел Информационной Безопасности.

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 securingthehuman.sans.org/ouch/archives.

Ресурсы

Фишинг:	https://securingthehuman.sans.org/ouch/2015#december2015
Афера «Руководитель»:	https://securingthehuman.sans.org/ouch/2016#july2016
Программы-вымогатели:	https://securingthehuman.sans.org/ouch/2016#august2016
Архив OUCH!:	https://securingthehuman.sans.org/ouch/archives

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

