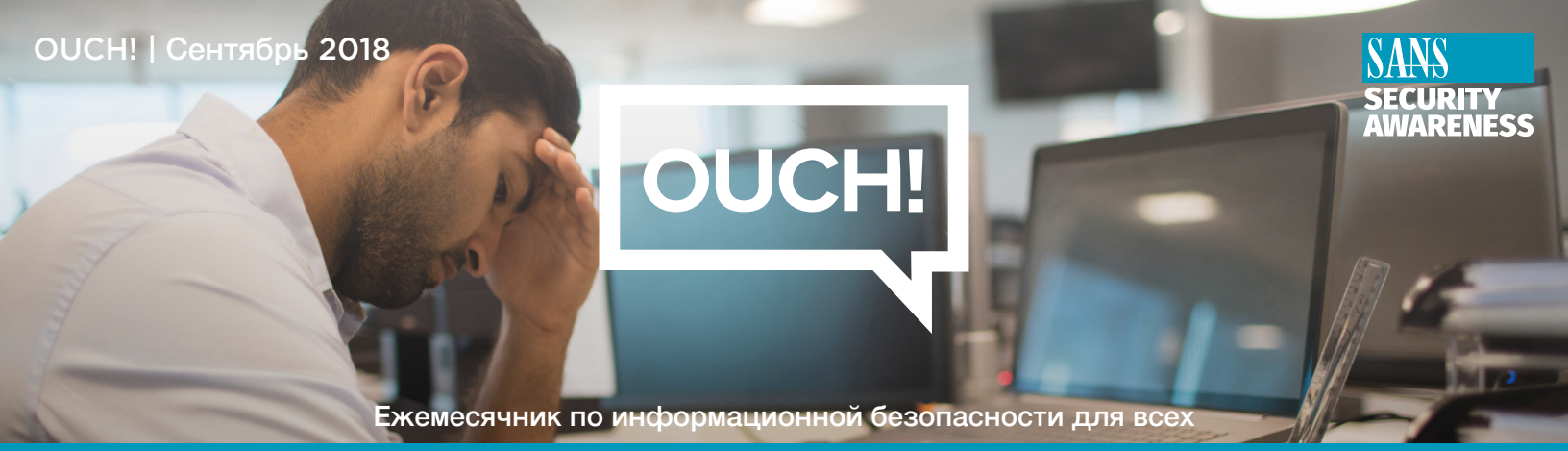

SANS SECURITY AWARENESS

OUCH!

Ежемесячник по информационной безопасности для всех

Афера «Руководитель»

Что такое Афера «Руководитель» и Скомпрометированная Деловая Переписка?

Кибер преступники продолжают совершенствовать атаки через электронную почту. Одними из наиболее изощрённых и опасных типов атак являются Афера «Руководитель» (CEO Fraud) и Скомпрометированная Деловая Переписка (Business Email Compromise - BEC). Это целевые атаки, использующие электронную почту, которые обманным путем заставляют жертв сделать что-то, что они не должны делать. В большинстве случаев присутствует финансовая мотивация. Эти атаки особенно опасны тем, что атакующая сторона тщательно изучает своих жертв перед началом атаки. Эти атаки очень сложно предотвратить техническими средствами, так как они не используют инфицированные вложения или ссылки в сообщениях электронной почты, которые можно было бы обнаружить. Приведем краткое описание механизма атаки.

Кибер преступник использует интернет для изучения своих потенциальных жертв и людей, с которыми они общаются. Например, если они взяли вас на прицел, они могут искать данные о вашем руководителе или риэлторе, с которым вы имеете дело. Кибер преступник затем составляет сообщение электронной почты, выдавая себя за одного из этих людей и посылает это сообщение вам. Это срочное сообщение, требующее от вас какого-либо незамедлительного действия, например, оплаты счёта, изменения платёжных реквизитов получателя или отправки конфиденциальной документации. Это сообщение вынуждает вас сделать то, что нужно преступникам. Приведём два примера таких атак.

Перевод денег: Кибер преступник пытается завладеть вашими деньгами. Они изучают компанию, в которой вы работаете, например выясняют имена сотрудников отдела платежей или операторов, занимающихся переводом денег. Преступник затем сочиняет и отправляет сообщения этим сотрудникам, выдавая себя за их начальника или руководителя компании. В сообщении говорится о каких-либо чрезвычайных обстоятельствах и необходимости немедленно перевести деньги на новый банковский счёт. Сообщение вынуждает их совершить ошибку; на самом деле, они посылают деньги преступникам.

Налоговое мошенничество: Кибер преступники охотятся за персональными данными людей, чтобы использовать их для налогового мошенничества. Один из наиболее эффективных способов получить эту информацию – украсть информацию о всех сотрудниках компании. Преступники выясняют, имена сотрудников отдела кадров. Затем они высылают этим сотрудникам сообщения электронной почты, выдавая себя за одного из руководителей компании или сотрудника юридического отдела. Эти сообщения требуют срочной отправки налоговой информации всех сотрудников компании. Сотрудники отдела кадров думают, что они посылают конфиденциальные документы руководству компании; в действительности же, они высылают их кибер преступникам.

Как защитить себя

Что вы можете сделать, чтобы защитить себя? Здравый смысл – ваша лучшая защита. Приведём несколько признаков, позволяющих распознать подобные атаки.

Сообщение очень короткое и срочное (часто, всего пара предложений) и подпись говорит, что сообщение было отправлено с мобильного устройства.

Чрезвычайная срочность ситуации, вынуждающая вас проигнорировать или обойти стандартные политики и процедуры вашей организации. Всегда соблюдайте корпоративные политики и процедуры, даже если сообщение выглядит так, будто его отправил ваш начальник или даже президент компании.

Сообщение служебное, но отправлено с личного адреса электронной почты, такого как @gmail.com или @hotmail.com.

Сообщение подписано вашим руководителем, коллегой или поставщиком, с которым вы работаете, но тон и стиль сообщения не похож на их стиль.

Предоставлены платёжные инструкции, отличающиеся от стандартных инструкций; например, требование срочного платежа на другой банковский счёт.

Если вы подозреваете, что стали объектом такой атаки на работе, прекратите все коммуникации с атакующей стороной и сообщите об этом своему руководителю. Если за вами охотятся дома или вы уже стали жертвой и перевели деньги преступникам, немедленно сообщите об этом в свой банк, затем в полицию.

Об авторе

Дон Кэвендер *– бывший специальный агент ФБР, имеющий более 22 лет опыта в области компьютерной форенсики и расследования киберпреступлений. Дон проводит тренинги и занимается исследовательской работой. Контакты Дона:* @don_cavender *и* https://www.linkedin.com/in/donald-cavender

Ресурсы

Социальная Инженерия: https://www.sans.org/u/HE3
Осторожно, фишинг!: https://www.sans.org/u/HE8
Защита от вирусов: https://www.sans.org/u/HEd
Надёжная защита вашего аккаунта: https://www.sans.org/u/HEi
BEC-аферы приводят к серьезным экономическим потерям для предприятий:
http://club.cnews.ru/blogs/entry/becafery_privodyat_k_sereznym_ekonomicheskim_poteryam_dlya_predpriyatij