Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Что такое «Афера Руководитель»?
- Как себя защитить

Афера «Руководитель»

Что такое «Афера Руководитель»?

Кибер преступники очень изворотливы: они постоянно находят новые способы достижения своих целей. Они знают, что самое слабое звено любой организации - это неосведомленные люди. Но они не учитывают тот факт, что люди, обладающие знаниями в сфере компьютерной безопасности, такие, как читатели OUCH!, являются самой лучшей защитой компании.

Об авторе

Анжела Паппас руководит отделом тренингов по информационной безопасности компании Thomson Reuters. Анжела отвечает за обучение сотрудников защите от фишинга и координирует программу eLearning.

Кибер мошенники разработали новый вид атаки – «Афера Руководитель» (CEO Fraud), также известную как «Скомпрометированная деловая переписка» (Business Email Compromise – BEC). При подобных атаках, кибер мошенники выдают себя за директора или другого высокопоставленного руководителя вашей компании. Преступники рассылают письма сотрудникам компании, пытаясь обманным путем заставить сделать то, чего делать не следует. Этот вид атак необычайно эффективен, потому что мошенники проводят тщательную подготовку. Они подробно изучают сайт организации, её местонахождение, имена руководителей и партнеров компании. Кибер преступники тщательно собирают всю информацию сотрудников компании с сайтов социальных сетей, например, LinkedIn, Facebook или Twitter. После тщательного изучения структуры компании, преступники выбирают сотрудников, которых будут атаковать. Их выбор зависит от поставленной цели. Если целью является получение денег, то атака будет направлена на сотрудников финансовой службы. Если мошенников интересует налоговая информация, то будет сформирована атака на отдел персонала. Если они хотят получить доступ к базам данных, то будет атакован сотрудник службы IT.

Определившись со своими желаниями и выбором жертвы, преступники начинают готовить атаку. Часто такие атаки называют целевым фишингом. Под фишингом подразумевается рассылка писем миллионам людей, с целью их обмануть и вынудить к действию, например, загрузке инфицированного документа или переходу по ссылке на вредоносный сайт. Целевой фишинг похож по своей сути, только письма рассылаются не миллионам людей, а только некоторым, тщательно отобранным людям. Причем письма целевой атаки выглядят очень

Афера «Руководитель»

правдоподобно и их сложно распознать. Они могут быть от имени вашего коллеги или даже начальника. Содержания писем тоже очень правдоподобно, они могут содержать профессиональный жаргон, который используют коллеги, логотип компании или даже подпись руководителя. Содержание этих писем создает ощущение срочности, необходимости немедленных действий с вашей стороны и запрета на обмен этой информацией с коллегами. Цель мошенников - создать ситуацию срочности и вынудить вас совершить ошибку. Три наиболее распространённых сценария:

Целевые атаки «Руководитель» очень опасны и могут обойти большинство средств защиты безопасности. Но именно вы являетесь самой надежной защитой от них.

- **Денежный перевод**: в данном случае целью является получение денег. Жертвой выбирается сотрудник, совершающий денежные переводы или отдел, отвечающий за финансовые дела компании. Злоумышленники тщательно готовят письмо от имени руководства, в котором требуется совершить срочный перевод денег на указанный счет.

- **Налоговое мошенничество**: в этом случае преступников интересуют личные данные сотрудников компании, поэтому они могут представиться коллегой, проводящим расследование о мошенничестве с налогами. Жертвой выбирают людей, владеющих нужной информацией, например, сотрудников отдела персонала. Выбрав жертву, преступники отправляют письмо от имени высшего руководства или юриста компании с требованием немедленно прислать нужные им документы.

- **Выдать себя за адвоката**: не все целевые атаки проводятся по электронной почте. Злоумышленники могут использовать и телефон. В этом случае, как и в электронном письме, злоумышленник представляется начальником и предупреждает, что вам позвонит адвокат для обсуждения срочного вопроса. Мошенник затем звонит вам, выдавая себя за адвоката. Преступник нагнетает обстановку, требуя конфиденциальности и срочности выполнения указания. Эта ситуация срочности и есть способ заставить вас совершить ошибку.

Афера «Руководитель»

Как себя защитить

Что можно сделать, чтобы защитить себя и свою организацию? Здравый смысл – вот лучшая защита. Если вы получили подозрительное письмо от начальника или коллеги, будьте начеку, это может являться атакой. Ключом к разгадке может являться ситуация срочности, непривычная подпись или само неожиданное содержание письма, необычное обращение к вам от коллег. Другим подозрительным моментом может стать использование необычного электронного адреса отправки письма или незнакомого номера телефона, или использование адреса электроной почты, очень похожего на настоящий адрес вашего руководителя, но слегка отличающегося от него. Если есть хоть малейшие сомнения, свяжитесь с коллегой по проверенному номеру телефона или встретьтесь лично, чтобы подтвердить отправку письма (не следует писать ответ на адрес отправителя). Никогда не нарушайте политики и процедуры безопасности. Скорее всего, в вашей компании существуют процедуры подтверждения денежных переводов или запроса конфиденциальных данных. Требования нарушить данные процедуры должны вас насторожить, независимо от того, кто это требует, в любом случае следует провести процедуру авторизации перед любым действием. Если вы получили подобный запрос, посоветуйтесь со своим руководителем или немедленно свяжитесь со службой Информационной Безопасности или отделом поддержки департамента IT.

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

Социальная инженерия:	https://securingthehuman.sans.org/ouch/2014#november2014
Фишинг:	https://securingthehuman.sans.org//ouch/2015#december2015
Что такое вредоносные программы:	https://securingthehuman.sans.org/ouch/2016#march2016
Двухступенчатая верификация:	https://securingthehuman.sans.org/ouch/2015#september2015
Ежедневные советы Института SANS:	https://www.sans.org/tip-of-the-day

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

