

КАК СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ОТКРЫВАЕТ ХАКЕРУ ДВЕРИ В ВАШУ ОРГАНИЗАЦИЮ



СОДЕРЖАНИЕ

Введение 3

Как белые хакеры притворяются злоумышленниками 3

Сотрудники — невольные соучастники 5

Втереться в доверие 7

Тема письма решает 8

Позвони мне, позвони! 10

Или в Фейсбуке напиши 11

Заключение 12

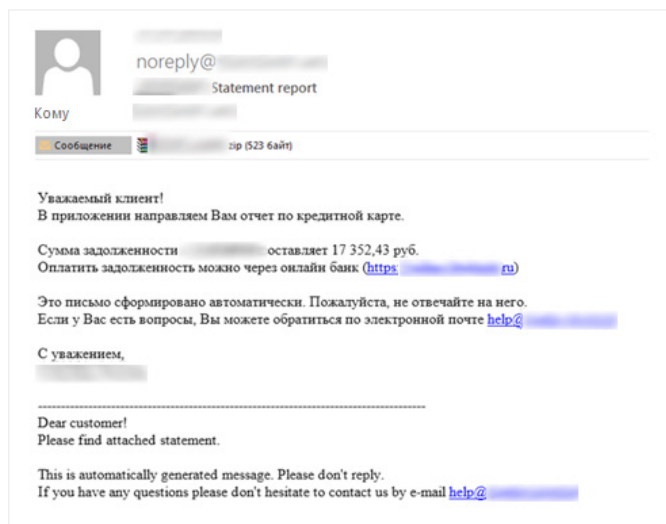
ВВЕДЕНИЕ

Киберпреступники все чаще используют методы социальной инженерии для проникновения в инфраструктуру организации при целевой атаке. Человеческий фактор по-прежнему остается слабым звеном в любой системе защиты, поэтому сегодня как никогда возрастает потребность в обучении сотрудников основам информационной безопасности. Продуктивный способ научиться противостоять кибермошенникам — реальная практика, которая предполагает воспроизведение действий потенциального нарушителя без ущерба корпоративной инфраструктуре.

Эксперты Positive Technologies регулярно выполняют работы по оценке осведомленности сотрудников в вопросах ИБ для крупнейших компаний в России и за рубежом. В этом исследовании представлена статистика и аналитические данные по результатам 10 наиболее показательных проектов за 2016 и 2017 годы, а также примеры успешных сценариев атак на сотрудников организаций. Такие работы основаны на использовании различных методов социальной инженерии и, как правило, связаны с рассылкой электронных писем, телефонным взаимодействием, а также общением через социальные сети.

КАК БЕЛЫЕ ХАКЕРЫ ПРИТВОРЯЮТСЯ ЗЛОУМЫШЛЕННИКАМИ

В ходе работ по оценке осведомленности сотрудников эксперты Positive Technologies проводят серию согласованных тестовых атак, имитирующих реальную деятельность злоумышленников, и отслеживают реакцию сотрудников на них. Специалисты отправляют письма, в которых содержится ссылка для перехода на специально созданный ресурс, где размещена форма для ввода учетных данных. Письма могут также содержать приложенный файл — как правило, это офисный документ с исполняемым вложением или некий архив.



Предварительно эксперты собирают адреса электронной почты сотрудников из открытых источников (как это и делают обычно злоумышленники), затем согласовывают полученный набор с компанией-заказчиком, которая уже либо удаляет лишние, либо добавляет другие электронные адреса, которые считает необходимыми. Рассылка проводится на адреса домена той организации, в отношении которой ведутся работы. Сотрудники, которым отправляются письма, разделены на фокус-группы, для каждой группы формируется отдельный сценарий. В результате мы можем корректно оценить, какой из сценариев будет успешнее при целевой атаке на организацию.

По результатам рассылок проводятся сбор статистики и оценка полученных данных: сколько потенциально опасных действий совершили пользователи — перешли

по ссылке, ввели свои учетные данные, загрузили и запустили файл или вступили в переписку. Так мы демонстрируем и оцениваем, какие данные мог бы получить потенциальный нарушитель и как злоумышленник мог бы распространить вредоносное ПО в инфраструктуре или проникнуть во внутреннюю сеть компании.

В данном исследовании оценка проводилась на основе 3332 отправленных писем, содержащих ссылки на веб-ресурсы, формы для ввода паролей и вложенные файлы. На диаграмме ниже видно, какие типы писем отправлялись и в какой пропорции.



Отметим, что при рассылке использовались безвредные файлы, а в ходе эксперимента фиксировался только запуск. Для киберпреступников часто достаточно, чтобы пользователь просто скачал и запустил файл, хотя иногда требуется разрешить установку ПО или внесение изменений от имени администратора.

Наши проверки показали, что в общей сложности 17% всех писем в реальной жизни могли бы привести к компрометации компьютера сотрудника, а впоследствии — и всей корпоративной инфраструктуры.

Ожидаемо наиболее успешным оказался метод социальной инженерии с применением фишинговой ссылки: 27% сотрудников перешли по ссылке. Пользователи невнимательно читают адрес ссылки или же просто, не глядя, кликают на него и переходят на поддельный ресурс. Когда же пользователю предлагается скачать файл, а затем запустить его, то с каждым дополнительным действием у него начинают закрадываться подозрения. Поэтому лишь 7% сотрудников оказались невнимательными и попались на удочку.

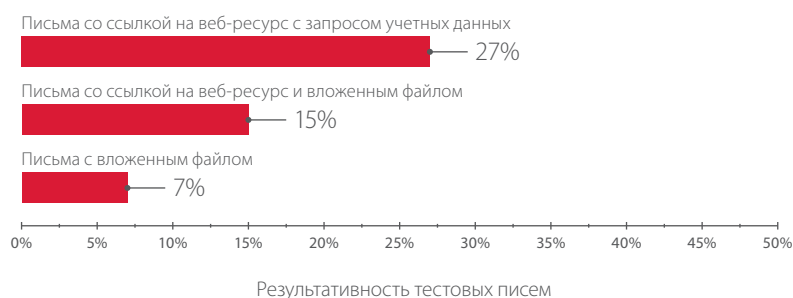
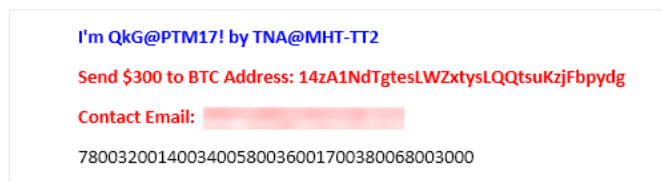


Схема реальной атаки может выглядеть следующим образом. Злоумышленник размещает на подконтрольном ресурсе набор эксплойтов под различные версии ПО. Ссылка на этот ресурс массово рассылается в фишинговых письмах. Сотрудник организации переходит по ссылке из письма, и после открытия страницы в браузере происходит эксплуатация уязвимостей, что может привести к заражению рабочей станции пользователя вредоносным ПО. Например, при использовании устаревшей версии браузера Internet Explorer может быть реализовано удаленное выполнение кода (CVE-2016-0189), ведущее к получению полного контроля над компьютером сотрудника. При этом сам сотрудник даже не заметит, что злоумышленник уже «поселился» в его компьютере. Приложенный к письму файл также может содержать сразу несколько эксплойтов, направленных на использование различных недостатков в ПО. Существует целый набор уязвимостей, которые могут быть

использованы нарушителем (CVE-2017-0037, CVE-2012-0158, CVE-2017-0199 и другие). Так, в ноябре 2017 года злоумышленники рассылали документы, содержащие в качестве вредоносной нагрузки шифровальщик qkG¹. В случае если пользователь скачивал полученный файл и разрешал выполнение макросов, то после закрытия такого документа на компьютере жертвы шифровалось содержимое всех документов, добавлялось текстовое сообщение с требованием выкупа, а шифровальщик мог распространяться дальше и вызвать эпидемию в инфраструктуре компании.

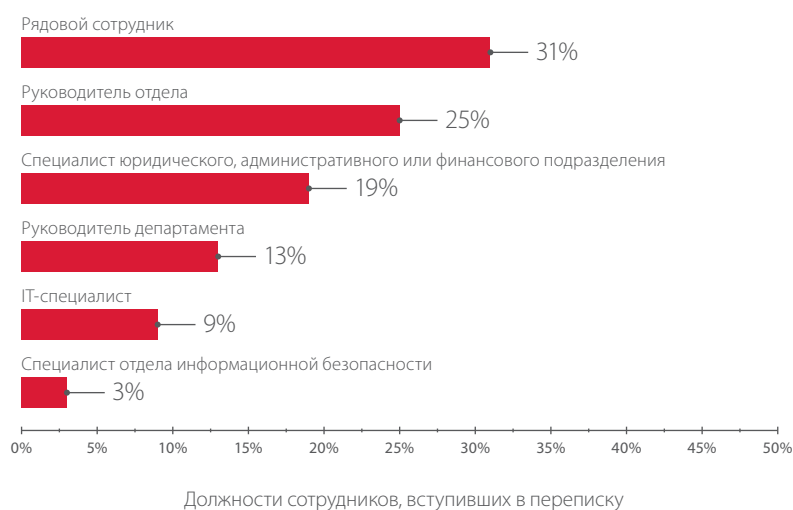


Для повышения эффективности злоумышленники часто сочетают различные способы атаки на пользователя. Фишинговое письмо может содержать одновременно вложение с набором вредоносных скриптов и ссылку на поддельный ресурс, где не только размещена связка эксплойтов, но и форма для ввода учетных данных. Даже если в инфраструктуре используется современное и обновленное ПО, а также соответствующие антивирусные средства, это не спасет ситуацию, если пользователь сам отдаст свой пароль в руки мошенников, введя их в некой форме на поддельном сайте.

СОТРУДНИКИ — НЕВОЛЬНЫЕ СОУЧАСТНИКИ

Если с переходом по ссылке, вводом своих учетных данных на поддельном сайте и запуском подозрительного файла все более-менее ясно, то почему же не стоит вступать в переписку со злоумышленником? Давайте посмотрим, в чем кроется опасность и кто обычно так поступает.

В 88% случаев в переписку вступают сотрудники компании, не являющиеся IT-специалистами (бухгалтеры, юристы, менеджеры и т. п.). Каждый четвертый сотрудник, вступавший в переписку, являлся руководителем отдела. Интересно, что среди вступивших в переписку были и специалисты по информационной безопасности, и хотя они были в меньшинстве (3%), это лишний раз показывает, что социальная инженерия — мощный инструмент в руках злоумышленников, и даже самые осведомленные в вопросах ИБ сотрудники могут ошибиться.

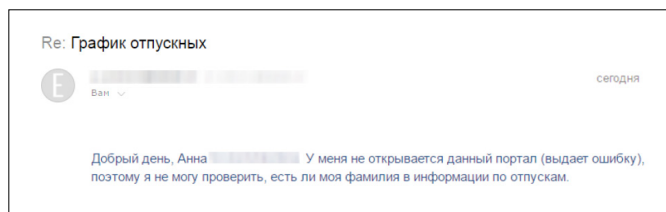


Что же обычно пишут сотрудники, когда получают необычное письмо?

Как правило, пользователи сообщают, что ссылка или вложение не открывается, после чего в журналах регистрации событий на используемом при тестировании сервере сбора информации можно обнаружить, как этот пользователь

¹ blog.trendmicro.com/trendlabs-security-intelligence/qkg-filecoder-self-replicating-document-encrypting-ransomware/

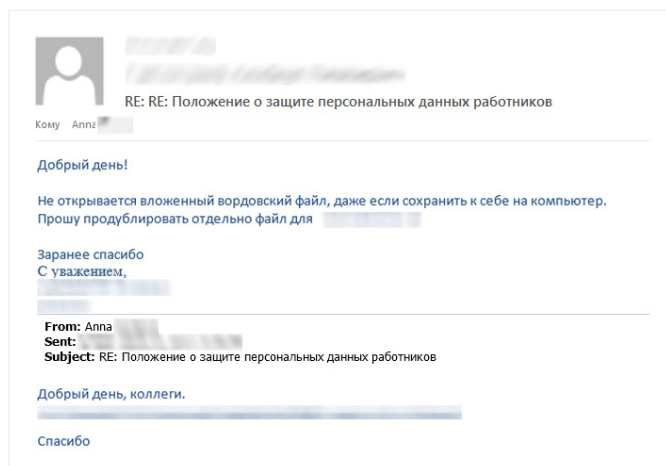
многократно переходил по фишинговой ссылке, вводил различные вариации своего пароля, а затем еще и пароли к другим ресурсам. В отдельных случаях это повторялось 30–40 раз!



Иногда сотрудники писали нам «вы ошиблись адресатом» и указывали, кому еще (по их мнению) следует направить данное письмо.

Чем это грозит? Как только злоумышленник убедился, что сотрудник принял его за коллегу или какое-то доверенное лицо, в ходе дальнейшей переписки он попытается получить нужную ему информацию, не вызывая подозрений. Так можно узнать версию используемого ПО, наличие антивируса на рабочем компьютере, электронную почту других сотрудников, номера мобильных телефонов, структуру компании. Все это представляет ценность и может использоваться при планировании и проведении последующих социотехнических атак.

Иногда бывает так, что сотрудники непреднамеренно помогают злоумышленнику в развитии атаки, пересылая зараженное письмо коллегам с просьбой открыть вложение или перейти по ссылке. В нашей практике такое тоже случается. Например, сотрудники компании-заказчика перенаправляли полученные письма в IT-департамент, требуя разобраться, почему у них не открывается файл «График_отпусков.xls»! Стоит отметить, что после этого специалисты IT-департамента открывали письмо и запускали файл уже у себя, видимо доверяя письму, полученному от коллеги, которого знают лично.



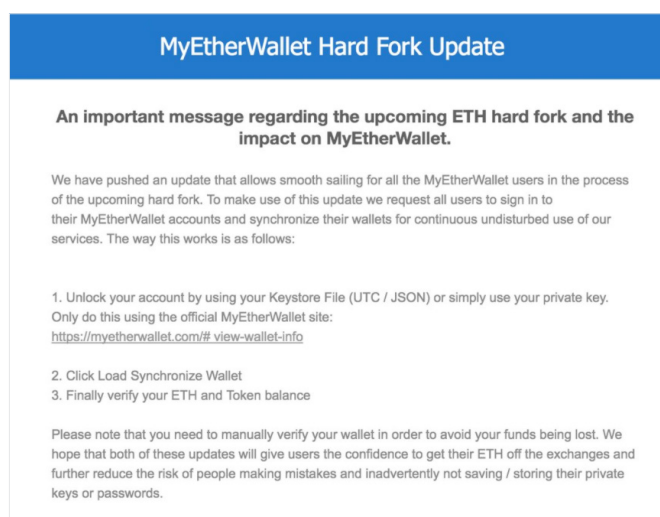
Так как перечень сотрудников, в отношении которых проводятся такие работы, согласуется и утверждается заранее, то довольно странно обнаружить, что скачивали и запускали рассылаемый файл совсем другие люди, не входящие в согласованные заранее фокус-группы. Именно так мы понимали, что сотрудники уже начали пересылать наше письмо своим коллегам самостоятельно. Таким образом письмо могло доходить до рабочих станций системных администраторов и специалистов по безопасности, о которых нам не было известно при изначальной рассылке.

Важный момент при проведении работ по анализу защищенности это реакция со стороны специалистов по ИБ. Что касается реагирования на фишинговые рассылки, то в тех случаях, когда работы проводились без уведомления специалистов подразделения ИБ, своевременное обнаружение подобных писем с последующей их фильтрацией и блокировкой фишингового ресурса встретилось лишь на двух проектах.

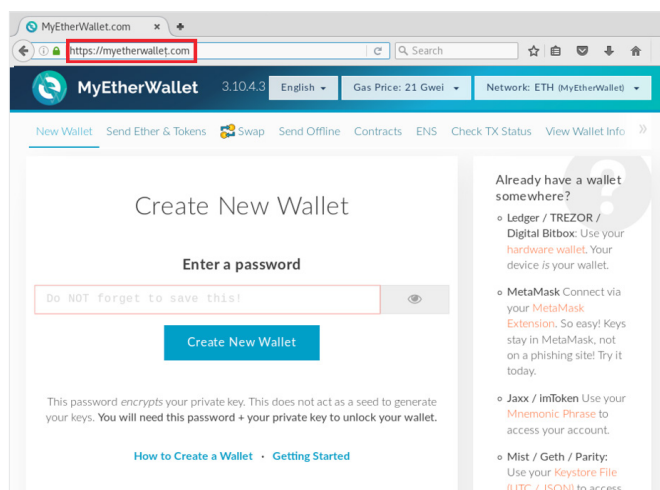
ВТЕРЕТЬСЯ В ДОВЕРИЕ

Для проведения работ эксперты Positive Technologies регистрируют домены, которые по написанию схожи с реальными доменами компаний-заказчиков. К этому трюку часто прибегают и реальные злоумышленники: не каждый сотрудник обратит внимание, что какая-то буква в названии написана неверно либо что к имени компании добавлена приставка или постфикс. При этом проверить принадлежность доменного имени к компании с помощью общедоступных интернет-сервисов могут, как правило, только разбирающиеся в информационных технологиях люди. Но одно дело — если распознать подделку действительно сложно, например когда используется настоящее доменное имя организации или доверенного партнера, и совсем другое — когда письмо пришло явно с поддельного доменного имени, например `admin@example.com`. В таких случаях речь идет о банальной невнимательности либо полном отсутствии знаний в вопросах ИБ.

В октябре 2017 года была осуществлена фишинговая рассылка² от имени администрации популярного онлайн-криптокошелька MyEtherWallet. В письме было указано, что сейчас якобы проводится обновление ПО и учетные записи заблокированы, а для их разблокировки и подтверждения баланса нужно перейти по ссылке.



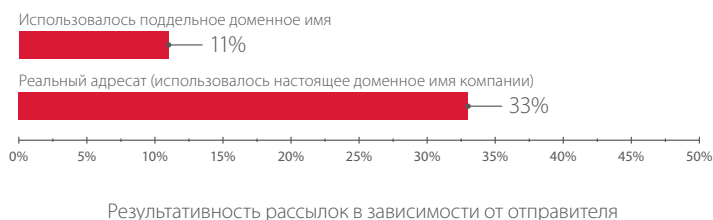
При переходе по ссылке открывался сайт, как две капли воды похожий на оригинальный `myetherwallet.com`. Разница была в том, что вместо последней буквы «t» использовался практически идентичный символ «ſ» в кодировке Unicode.



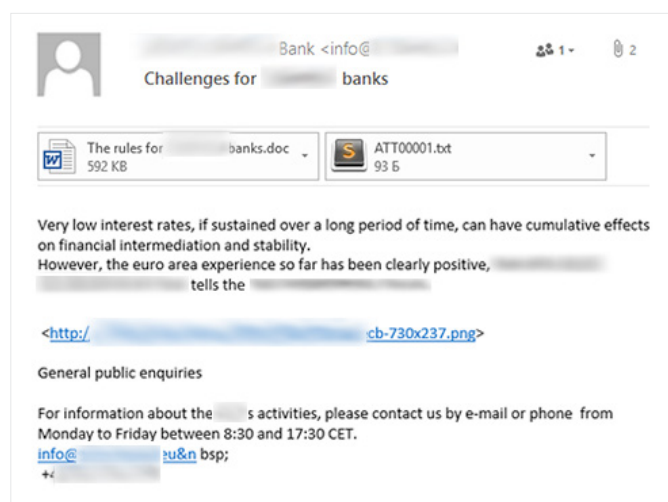
² dearbytes.com/blog/cryptocurrency-phishing/

На какие только ухищрения не идут злоумышленники — использование юникода, добавление дефиса к реальному имени домена, подмена похожих или созвучных букв, добавление приставок и постфиксов. Тем не менее мы считаем, что использование этой техники неминуемо будет сходиться на нет с повышением уровня осведомленности рядовых пользователей в вопросах информационной безопасности.

Наша практика подтверждает это: 33% пользователей совершали потенциально опасное действие, если письмо пришло от реального адресата (использовалось настоящее доменное имя какой-либо компании). В том случае, когда использовалось поддельное доменное имя, это происходило значительно реже: лишь 11% сотрудников поверили собеседнику.



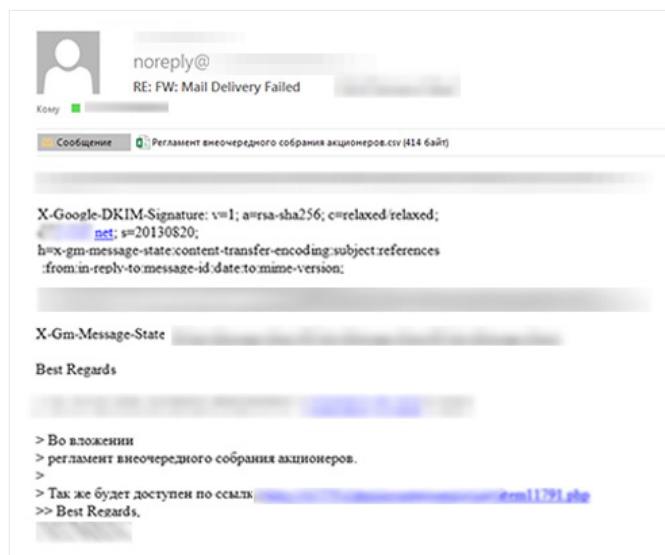
Вероятно, поэтому нарушители сегодня стали переходить к рассылке от имени контрагентов вместо использования поддельных доменов. Здесь можно вспомнить группировку Cobalt³, которая в качестве исходного вектора заражения инфраструктуры использовала фишинговые письма не только через поддельные доменные имена, но и от лица сотрудников реальных банков и компаний-интеграторов, инфраструктура которых была предварительно взломана для проведения подобных рассылок. Так как письма от коллег, контрагентов и партнеров обычно приходят в рабочее время, для большей достоверности злоумышленники проводили рассылку таким образом, чтобы письма доставлялись в рабочее время получателей.



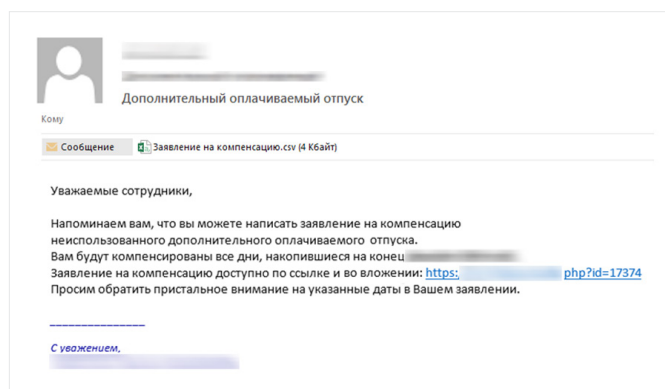
ТЕМА ПИСЬМА РЕШАЕТ

Злоумышленники часто опираются на страх, жадность, надежды, ожидания и другие эмоции, которые могут заставить пользователя поддаться сиюминутной слабости. Когда внезапно на почту приходит письмо «Недоставленное сообщение: список сотрудников на увольнение» — пользователь забывает об элементарных правилах техники кибербезопасности, он даже не задумывается, почему ему вообще пришло уведомление о «недоставленном сообщении».

³ ptsecurity.com/upload/corporate/ru-ru/analytics/Cobalt-Snatch-rus.pdf



Часто бывает так, что именно тема письма побуждает сотрудника открыть его, перейти по ссылке, скачать и запустить файл, не разбираясь — кто адресат и почему домен отправителя написан как-то странно. В ходе работ по оценке осведомленности сотрудников в каждом отдельном случае текст и тема письма тщательно прорабатываются экспертами.



Если недостаточно внимательно отнестись к прочтению такого письма, то подвох заметить непросто. Самые эффективные сценарии фишинга, используемые в наших рассылках, приведены на диаграмме ниже.



Предсказуемо страх увольнения или сокращения — достаточно мощный фактор, чтобы забыть о правилах информационной безопасности: почти 40% (!) тестовых фишинговых писем с такой темой побуждали пользователей совершить потенциально опасное действие. Высокий процент успеха показывают письма, где есть слова «премия», «поощрение», «повышение зарплаты»: каждое четвертое такое письмо обмануло сотрудника. Злоумышленник может также попытаться привязать тему рассылки к какому-то знаменательному событию (если располагает, например, сведениями о недавно прошедшем в компании корпоративе), профессиональным и государственным праздникам. В нашей практике 11% писем с подобной темой стали причиной совершения потенциально опасного действия.

ПОЗВОНИ МНЕ, ПОЗВОНИ!

Хотя электронная почта и является наиболее распространенным и эффективным инструментом социальной инженерии благодаря возможному охвату и простоте реализации, это далеко не единственный метод, который используют злоумышленники. Они могут позвонить по телефону, представляясь специалистом технической поддержки, и попытаться получить критически важные данные или обманом заставить сотрудника перейти по нужной ссылке, ввести пароль, скачать и запустить посторонний файл. Классический пример — звонок рано утром в воскресенье с просьбой срочно явиться на работу, но в ходе разговора выясняется, что можно просто предоставить свой пароль от компьютера, и тогда «специалисты» все сделают сами. Сотрудник сразу же сообщает свой пароль, да еще и благодарит звонившего за помощь.

Фишинговые рассылки можно делать быстро, массово и почти одномоментно, и телефонные звонки по этим параметрам проигрывают: необходима тщательная подготовка, разговор с каждым человеком требует определенного времени, да и массовый обзвон всех сотрудников компании вряд ли останется незамеченным. В наших работах, как правило, телефонное взаимодействие проводится в отношении сотрудников, которые вступили в переписку, а в их подписи либо есть контактные данные, либо их удалось получить в ходе переписки. Это позволяет провести обзвон точно, а пользователи практически готовы к общению и содействию в решении придуманной нарушителем «проблемы». В итоге эффективность такого вектора атаки достаточно высока. По результатам наших работ 44% сотрудников в результате телефонного взаимодействия выдавали свои пароли, рассказывали об установленном ПО, переходили по требуемой ссылке.

Как это выглядит на практике: после соответствующего согласования с руководством компании, где проводились работы, наши эксперты, представившись специалистами технической поддержки, позвонили сотруднику, ранее ответившему на фишинговое письмо. Под их диктовку пользователь зашел на поддельный корпоративный портал (было зарегистрировано доменное имя, содержащее дефис), а после того, как у него несколько раз не получилось ввести пароль, состоялся следующий диалог.



[Эксперт РТ]: давайте вы просто свой пароль скажете, мы все на портале сделаем сами.

[Сотрудник]: о, так даже лучше. Мой пароль 978654321#!

[Эксперт РТ]: хорошо, спасибо.

[Сотрудник]: вы только не меняйте мне его, он очень удобный!

В отдельных случаях сотрудники просили позвонившего назвать свои имя и фамилию, и наши специалисты называли свои настоящие имена. Наиболее бдительные сотрудники проверяли наличие такого сотрудника в компании, а не найдя — обрывали разговор. Стоит отметить, что злоумышленник может легко узнать необходимые данные заранее, используя социальные сети или другие источники, где сотрудники раскрывают свои должности и контактные данные. Вероятно, что результативность атаки после такой подготовки может быть значительно выше.

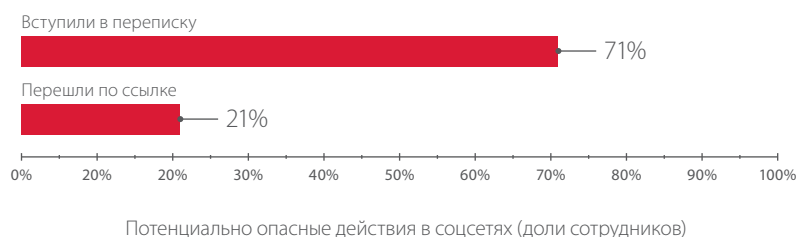
Причиной отказа выполнить требуемое действие иногда было нежелание делать что-то в нарушение установленного регламента: сотрудник напрямую говорил, что переходить по ссылке он не будет, потому что «так у нас не делается». Тут можно только похвалить подход к ИБ в организации и уровень ответственности отдельных сотрудников. В некоторых случаях пользователи спрашивали — а безопасно ли переходить по ссылке? Но потом все равно переходили и даже вводили свои учетные данные.

ИЛИ В ФЕЙСБУКЕ НАПИШИ

Злоумышленники не пренебрегают поиском сотрудников компаний в социальных сетях. Атака на профиль в социальной сети может быть достаточно эффективной. Например, можно заразить вредоносным ПО устройство сотрудника, с которого он впоследствии подключается к внутренней сети компании или проверяет корпоративную почту. Недостаточно осведомленные в вопросах ИБ пользователи могут обсуждать в социальных сетях рабочие вопросы, обмениваться конфиденциальными документами, которые представляют высокую ценность для нарушителя. В отдельных случаях сотрудники могут использовать одинаковые пароли для доступа к социальной и корпоративной сети либо незначительно изменять пароль, добавляя отдельные символы. Все полученные данные могут быть использованы злоумышленником при развитии атаки на инфраструктуру.

Сегодня так действуют и многие киберпреступники, например, группировка SongXY, которая в 2017 году принимала участие в атаках на промышленную отрасль и государственные учреждения стран СНГ. Злоумышленники искали профили сотрудников в социальных сетях и отправляли им сообщения. Кроме того, опасность заключается еще и в том, что сотрудники часто подключаются к социальным сетям с рабочих компьютеров, и тогда переход по ссылке, полученной от злоумышленника, может привести к прямому доступу к ЛВС организации.

Наши специалисты в ходе работ осуществляют тестовое взаимодействие с сотрудниками компании-заказчика через социальные сети. Отбирались сотрудники, у которых в профиле указано текущее место работы, а после того как перечень собран, чтобы исключить ложные аккаунты и тех, кто уже не работает в организации, список согласовывался с заказчиком. Таким образом, рассылка производилась только в отношении проверенных лиц, утвержденных самой компанией. В рамках таких работ используется простой логгер, который фиксирует лишь переход по ссылке на специально созданный ресурс. Более 70% сотрудников охотно вступали в переписку, а 21% перешли по предлагаемой ссылке.



При целевой атаке злоумышленники будут использовать все доступные средства — социальные сети, мессенджеры. Поэтому, если в профиле социальной сети сотрудник указал свое место работы, то он должен понимать свою ответственность за обеспечение ИБ и в нерабочее время.

ЗАКЛЮЧЕНИЕ

Злоумышленники всегда будут использовать фишинг как для атаки на рядовых пользователей, так и с целью проникновения в корпоративную инфраструктуру. Причиной тому относительная дешевизна и простота таких методов, а также высокая эффективность.

Для рядовых пользователей самый актуальный и действенный совет — всегда оставаться бдительными, проверять информацию об отправителе, прежде чем перейти по ссылке или скачать предлагаемый файл — убедиться, что это не вредоносный ресурс. Полученные файлы перед открытием необходимо проверить с помощью антивирусного ПО, а если у компании есть специальная «песочница», то отправить файл в нее. Стоит также удостовериться, что домен легитимный и реальный. В случае возникновения сомнений, рекомендуется проверить, действительно ли адресат отправлял данное письмо и является ли он настоящим владельцем домена и (или) электронного ящика, связавшись с ним каким-то альтернативным способом, например через мессенджер или по телефону. Если бы такую простую рекомендацию выполнили сотрудники при атаке со стороны группировки Cobalt, то это бы могло уберечь банки от многомиллионных потерь.

Что касается советов для IT- и ИБ-специалистов, то существует несколько простых технологий, позволяющих повысить защищенность от фишинговых атак по электронной почте. Настроенная SPF-запись защищает письма от подделки при отправке от имени вашего домена. Данная технология позволяет проверить подлинность сервера отправителя. Ее полезно использовать в сочетании с технологиями DKIM и DMARC. Первая позволяет настроить соответствующую подпись, которая подтверждает, что адрес, указанный в поле «От кого», действительный, а использование второй снижает количество фишинговых писем на основе правил и признаков идентификации почтовых доменов отправителя, заданных на сервере получателя. В качестве дополнительной меры защиты необходимо проверять PTR-запись для определения имени узла-адресата по его IP-адресу, а также наличие IP-адреса отправителя в спам-базах.

Рекомендуется заблокировать доставку вложений по почте с расширениями, которые используются для исполняемых (.exe, .src), системных (.dll, .sys), скриптовых (.bat, .js, .vbs) и других файлов (.js, .mht, .cmd). Файлы с такими расширениями могут содержать вредоносный код, используемый злоумышленником при фишинговой рассылке. С более детальным перечнем таких расширений можно ознакомиться в соответствующих исследованиях⁴. Рекомендуется внедрить в инфраструктуру систему выявления вредоносного ПО, в которую сотрудники могли бы в любой момент загрузить на проверку почтовое вложение или любой другой файл. Специализированное антивирусное ПО позволяет выявлять вредоносные ссылки и файлы в корпоративной электронной почте до момента их открытия. Стоит отметить, что если злоумышленники используют обфускацию⁵, то антивирусы могут не выявить вредоносное ПО сразу, поэтому стоит проводить анализ вложений не только перед открытием файла, но и ретроспективно. Это позволит как минимум выявить факт того, что корпоративная система была скомпрометирована, определить дату компрометации и источник заражения, локализовать инцидент и провести более детальное расследование. Своевременное выявление и пресечение атаки позволит избежать серьезных последствий. Всегда остается актуальным совет своевременно устанавливать обновления ПО и ОС: это предотвратит эксплуатацию соответствующих уязвимостей.

Что касается организационных мер, то начинать надо с разработки и внедрения программы повышения осведомленности сотрудников в области информационной безопасности. Наше исследование процессов обеспечения ИБ в российских компаниях показало, что 38% организаций вообще не проводят тренинги для сотрудников по вопросам ИБ, а 37% делают это формально, без какой-либо

⁴ blueteamer.blogspot.ru/2017/05/support.office.com/en-us/article/Blocked-attachments-in-Outlook-434752e1-02d3-4e90-9124-8b81e49a8519

⁵ Обфускация — процесс приведения исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.

проверки эффективности⁶. Хотя проводить периодическое обучение с контролем информированности каждого сотрудника крайне важно. При этом процесс повышения осведомленности должен в первую очередь быть направлен на практическую сторону обеспечения безопасности, а каждый сотрудник должен понимать свои обязанности и ответственность за обеспечение ИБ. Хорошая практика, когда сотрудники оповещают своих «безопасников» о том, что им пришло фишинговое письмо, особенно если заметно, что над рассылкой тщательно поработали. В таком случае, даже если заражение или утечка имели место, еще можно успеть оперативно отреагировать на атаку и принять контрмеры.

⁶ ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

Подробнее — на ptsecurity.com, facebook.com/PositiveTechnologies, facebook.com/PHDays