АНАЛИЗ ФИШИНГОВЫХ АТАК

ANALYSIS OF PHISHING ATTACKS

УДК 004.424

Прокопайло Александр Александрович, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Prokopailo A.A. aka2h@yandex.ru

Аннотация

В данной статье описана теория по фишинговым атакам сетевых ресурсов. Описан метод и пример таких атак на организацию. Пользователь, приходя на необходимую страницу перенаправляется на поддельную страницу, которая выглядит точно так же, где запрашиваются как новые, так и существующие пароли. Злоумышленник, наблюдая за страницей, перехватывает исходный пароль, чтобы получить доступ к защищенным областям университетской сети. Таким образом сам пользователь открывает все данные, необходимые злоумышленнику для дальнейших атак, как организации, так и самого пользователя.

Annotation

This article describes the theory behind phishing attacks on network resources. A method and an example of such attacks on an organization are described. The user arriving at the required page is redirected to a fake page that looks exactly the same, where both new and existing passwords are requested. An attacker, observing the page, intercepts the original password in order to gain access to protected areas of the

university network. Thus, the user himself opens all the data that the attacker needs for further attacks, both the organization and the user himself.

Ключевые слова: фишинг, атака, информационная безопасность, несанкционированный доступ, методы фишинга

Keywords: phishing, attack, information security, unauthorized access, phishing methods.

Фишинг — это тип атаки социальной инженерии, часто используемый для кражи пользовательских данных, включая учетные данные для входа и номера кредитных карт. Это происходит, когда злоумышленник, маскируясь под надежную организацию, обманом заставляет жертву открыть электронное письмо, мгновенное сообщение или текстовое сообщение. Затем получателя обманом заставляют щелкнуть вредоносную ссылку, что может привести к установке вредоносного ПО, зависанию системы в результате атаки программы-вымогателя или раскрытию конфиденциальной информации [1].

Атака может иметь разрушительные результаты. Для физических лиц это включает несанкционированные покупки, кражу денежных средств или кражу личных данных.

Организация, поддавшаяся атаке, обычно несет серьезные финансовые потери в дополнение к снижению доли рынка, репутации и доверия потребителей. В зависимости от масштаба попытка фишинга может перерасти в инцидент безопасности, от которого бизнесу будет сложно избавиться [2].

Примеры фишинговых атак

Поддельное электронное письмо якобы от myuniversity.edu массово рассылается как можно большему количеству преподавателей.

В электронном письме утверждается, что срок действия пароля пользователя скоро истечет. Даны инструкции перейти на myuniversity.edu/renewal, чтобы обновить свой пароль в течение 24 часов. При нажатии на ссылку может произойти несколько вещей. Например, пользователь перенаправляется на myuniversity.edurenewal.com, поддельную страницу, которая выглядит точно так

же, как настоящая страница продления, где запрашиваются как новые, так и существующие пароли. Злоумышленник, наблюдая за страницей, перехватывает исходный пароль, чтобы получить доступ к защищенным областям университетской сети [3].

Пользователь отправляется на страницу фактического обновления пароля. Однако во время перенаправления вредоносный сценарий активируется в фоновом режиме, чтобы захватить файл cookie сеанса пользователя.

Методы фишинга

Фишинговые рассылки по электронной почте

Электронный фишинг — это игра с числами. Злоумышленник, рассылающий тысячи мошеннических сообщений, может получить значительную информацию и денежные суммы, даже если лишь небольшой процент получателей попадется на мошенничество. Как было показано выше, злоумышленники используют несколько приемов для увеличения своей успешности.

Во-первых, они будут делать все возможное, создавая фишинговые сообщения, имитирующие настоящие электронные письма от поддельной организации. Использование одинаковых фраз, шрифтов, логотипов и подписей делает сообщения легитимными.

Кроме того, злоумышленники обычно пытаются подтолкнуть пользователей к действию, создавая ощущение срочности. Например, электронное письмо может угрожать истечению срока действия учетной записи и поставить получателя на таймер. Применение такого давления заставляет пользователя быть менее прилежным и более склонным к ошибкам.

Можно сделать вывод, о том, что ссылки внутри сообщений напоминают свои законные аналоги, но обычно содержат неправильное имя домена или дополнительные поддомены. В приведенном выше примере URL-адрес myuniversity.edu/renewal был изменен на myuniversity.edurenewal.com. Сходство между двумя адресами создает впечатление защищенного соединения, из-за чего получатель менее осведомлен о том, что происходит атака.

Защита от фишинговых атак требует принятия мер как пользователями, так и предприятиями.

Для пользователей бдительность является ключевым фактором. Поддельное сообщение часто содержит тонкие ошибки, которые раскрывают его истинную сущность. Они могут включать орфографические ошибки или изменения в доменных именах, как показано в предыдущем примере URL. Пользователи также должны остановиться и подумать о том, почему они вообще получают такое письмо.

Для предприятий может быть предпринят ряд шагов по смягчению как фишинговых, так и копейных фишинговых атак:

Двухфакторная аутентификация (2FA) является наиболее эффективным методом противодействия фишинговым атакам, поскольку она добавляет дополнительный уровень проверки при входе в чувствительные приложения. 2FA полагается на то, что у пользователей есть две вещи: что-то, что они знают, например, пароль и имя пользователя, и что-то, что у них есть, например, их смартфоны. Даже когда сотрудники скомпрометированы, 2FA предотвращает использование их скомпрометированных учетных данных, поскольку одних этих данных недостаточно для получения доступа.

В дополнение к использованию 2FA организации должны применять строгие политики управления паролями. Например, сотрудники должны быть обязаны часто менять свои пароли и не иметь права повторно использовать пароль для нескольких приложений.

Образовательные кампании также могут помочь уменьшить угрозу фишинговых атак, применяя безопасные методы, такие как отказ от внешних ссылок электронной почты.

Многие информационные системы по организации безопасности предлагают сочетание решений по управлению доступом и безопасности веб-приложений для противодействия попыткам фишинга, позволяющие развернуть защиту 2FA для URL-адресов на вашем веб-сайте или веб-приложении. Это включает в себя

адреса с параметрами URL или AJAX-страницы, где защита 2FA обычно сложнее реализовать. Решение может быть развернуто за считанные секунды всего несколькими щелчками мыши. Он не требует установки какого-либо оборудования или программного обеспечения и позволяет легко управлять ролями пользователей и привилегиями непосредственно с панели мониторинга. Работая в облакесистемы блокируют вредоносные запросы на границе сети. Это включает в себя предотвращение попыток внедрения вредоносных программ скомпрометированными инсайдерами в дополнение к отраженным атакам XSS, вытекающим из эпизода фишинга.

Литература

1. Морозов, М. Атакуют "шнельботы". Германские торпедные катера Второй Мировой / М. Морозов, С. Патянин. - М.: Яуза, 2007. - 110 с.
2. Сорокин, З. Идем в атаку / З. Сорокин. - М.: ДОСААФ, 2016. - 200 с.
3. Стайн, Р.Л. Атака мутанта / Р.Л. Стайн. - М.: Росмэн, 2016. - 107 с.
4. Фостер, Дж.С. Защита от взлома: сокеты, эксплойты, shell-код: выявление уязвимостей операционных систем и прикладных программ к атакам хакеров / Дж.С. Фостер. - М.: ДМК, 2009. - 784 с.
5. Чирилло, Д. Обнаружение хакерских атак / Д. Чирилло. - М.: СПб: Питер, 2010. - 864 с.
6. Якименко, А. В атаке - "Меч" / А. Якименко. - М.: ДОСААФ, 2010. - 240 с.

Literature

1. Morozov, M. Attack "snail boats". German torpedo boats of the Second World War / M. Morozov, S. Patyanin. - M .: Yauza, 2007 .-- 110 p.
2. Sorokin, Z. We go to the attack / Z. Sorokin. - M .: DOSAAF, 2016 .-- 200 p.
3. Stein, R.L. Attack of the mutant / R.L. Stein. - M .: Rosmen, 2016 .-- 107 p.
4. Foster, J.S. Protection against hacking: sockets, exploits, shell-code: identifying vulnerabilities of operating systems and applications to hacker attacks / J.S. Foster. - M .: DMK, 2009 .-- 784 p.

5. Cirillo, D. Detection of hacker attacks / D. Cirillo. - M .: SPb: Peter, 2010 .-- 864 p.
6. Yakimenko, A. In the attack - "Sword" / A. Yakimenko. - M .: DOSAAF, 2010.- 240 p.