ЦЕЛЕВОЙ ФИШИНГ

SPEAR PHISHING

УДК 004.424

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

Prokopailo A.A. aka2h@yandex.ru

Аннотация

Целевой фишинг представляет собой направленный на определенную цель атаку. Ключевым моментом для пользователей является бдительность. Злоумышленник при помощи поддельных сообщений, часто содержащих небольшие ошибки, пытается раскрыть сокрытые данные. В данной статье приведены примеры фишинга вовремя чемпионат мира по футболу FIFA, мошенничество с биллингом Netflix и другие.В статье описаны существующие способы для решения обеспечения безопасности электронной почты, архивирования и непрерывности работы, клиентам, помогающие обучать сотрудников и повышать осведомленность о фишинге, позволяя избегать самые слабые звенья в цепочке безопасности.

Annotation

Spear phishing is an attack directed at a specific target. Vigilance is key for users. An attacker uses fake messages, often containing small errors, to uncover hidden data. This article provides examples of phishing during the FIFA World Cup, Netflix billing scams, and more. This article describes existing ways to address email security,

archiving and business continuity, helping customers educate employees and raise awareness of phishing by avoiding the weakest links in the security chain.

Ключевые слова: фишинг, целевой фишинг, атака, информационная безопасность, мошенничество.

Keywords: phishing, target phishing, attack, information security, fraud.

Целевой фишинг нацелен на конкретного человека или предприятие, а не на случайных пользователей приложений. Это более глубокая версия фишинга, требующая специальных знаний об организации, включая ее структуру власти.

Целевые фишинговые угрозы-это повышенная форма фишинговых вирусных атак, которые используют социальную инженерию, чтобы заставить конкретного человека раскрыть конфиденциальную информацию. Целенаправленные фишинговые атаки достигают успеха, используя информацию, почерпнутую из социальных сетей и других источников, чтобы создать ощущение знакомства. Так, например, электронные письма, которые были присланы «жертве», могут упоминать общего друга, ссылаться на недавнюю покупку или включать информацию, которая, по-видимому, является надежным источником.

После того, как было установлено доверие, целевые фишинговые кампании просят получателя предоставить некоторую информацию или войти на веб-сайт, который оказывается фальшивым или зараженным вредоносными программами.

Чтобы предотвратить фишинговые атаки и целевые фишинговые атаки, организациям нужны мощные инструменты для выявления подозрительной электронной почты и предотвращения действий сотрудников по ним.

Атака может развиваться следующим образом:

Преступник исследует имена сотрудников в отделе маркетинга организации и получает доступ к последним счетам.

Выступая в роли директора по маркетингу, злоумышленник отправляет электронное письмо менеджеру проекта отдела, используя строку темы, которая

гласит: Обновленный счет для кампаний Q3. Текст, стиль и прилагаемый логотип дублируют стандартный шаблон электронной почты организации.

Ссылка в электронном письме перенаправляет на защищенный паролем внутренний документ, который на самом деле является поддельной версией украденного счета [1].

Далее просят войти в систему для просмотра документа. Злоумышленник крадет его учетные данные, получая полный доступ к конфиденциальным областям в сети организации. Целевой фишинг, предоставляющий злоумышленнику действительные учетные данные для входа.

Защита от фишинговых атак требует принятия мер как пользователями, так и предприятиями. Ключевым моментом для пользователей является бдительность. Поддельное сообщение часто содержит небольшие ошибки, раскрывающие его истинную сущность. Они могут включать орфографические ошибки или изменения доменных имен, как показано в предыдущем примере URL. Пользователи также должны остановиться и подумать, почему они вообще получают такое электронное письмо [2].

Для предприятий можно предпринять ряд шагов для смягчения как фишинговых, так и целевых фишинговых атак:

Двухфакторная аутентификация (2FA) - наиболее эффективный метод противодействия фишинговым атакам, поскольку он добавляет дополнительный уровень проверки при входе в уязвимые 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 их одних недостаточно для получения доступа.

Помимо использования двухфакторной аутентификации, организациям следует применять строгие политики управления паролями. Например, от сотрудников следует требовать, чтобы они часто меняли свои пароли, и им нельзя разрешать повторно использовать пароль для нескольких приложений.

Образовательные кампании также могут помочь снизить угрозу фишинговых атак, применяя безопасные методы, такие как запрет на переход по внешним ссылкам электронной почты [2-3].

Известные фишинговые атаки 2018 года.

В мае 2018 года свои учетные данные для входа и банковскую информацию.

1. Билеты на Чемпионат мира по футболу FIFA.

Мошенничество, связанное с текущими событиями, может быть более убедительным для пользователей, которые обычно опасаются получать нежелательные сообщения. Киберпреступники в полной мере воспользовались одним из крупнейших событий на планете - Чемпионатом мира по футболу FIFA 2018 - для проведения ряда фишинговых атак.

В преддверии турнира многие люди сообщали о получении электронных писем от спекулянтов, продающих билеты по завышенным ценам на мероприятия, которые в противном случае были распроданы. Был ряд фишинговых атак, направленных на заманивание жертв обещаниями дешевых туристических виз, авиабилетов и услуг по размещению [4-5].

2. Мошенничество с биллингом Netflix.

Имея более 130 миллионов подписчиков, Netflix пользуется популярностью не только среди киноманов и поклонников телешоу, но и у киберпреступников. В 2018 году Netflix распространил ряд фишинговых писем с призывом к получателям обновить свою платежную информацию, чтобы избежать блокировки их учетной записи. Ссылка в письме ведет на убедительно выглядящий веб-сайт, который крадет имя пользователя, пароль и платежную информацию цели [6].

3. Голосовой фишинг становится все более продвинутым.

Голосовой фишинг - практика выдачи себя за законное лицо по телефону для извлечения конфиденциальной информации - не новая концепция, но в последние годы она стала заметно более сложной. Благодаря достижениям в области автоматизации и распознавания голоса злоумышленники теперь могут

использовать сочетание роботов и людей, вызывающих звонки, для более эффективного ого контакта с целями.

Существует различные способы для решения обеспечения безопасности электронной почты, архивирования и непрерывности работы позволяют клиентам стать более устойчивыми к целенаправленным фишинговым атакам и многим другим угрозам, с которыми сталкивается корпоративная безопасность.

Одним из решений является облачные, предлагаемые как спектр решений безопасности электронной почты для предотвращения угроз, утечек данных и обеспечения безопасной связи. Также применяются динамические инструменты повышения осведомленности пользователей, которые помогают обучать сотрудников и повышать осведомленность о фишинге, позволяя им перестать быть самым слабым звеном в цепочке безопасности.

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.