Инженерный вестник Дона, №3 (2025)
ivdon.ru/ru/magazine/archive/n3y2025/9946

Разбор проведения интернет-агрессором атаки целевого фишинга для дальнейшей эксплуатации чувствительных данных

И. Крепак

Финансовый университет при Правительстве РФ, Москва

Аннотация: Любая атака интернет-агрессии, целью которой является манипуляция файлами жертвы и её чувствительной информацией, начинается с разведки и получения несанкционированного доступа к учётной записи. Обычно, это делается с помощью целевого фишинга. В данной статье будет описан детальный процесс подготовки и проведения акта получения доступа к учётной записи цели. В качестве платформы, на которой будет объясняться последовательность проводимых манипуляции выбрана социальная сеть с формой на главной странице. Опасность данного метода характеризуется высокой доступностью технических мер и относительно низким порогом входа. Главной целью данной научной статьи является осведомить членов информационных сообществ о многоэтапной компьютерной атаке, которая существует как самостоятельно, так и служит первоначальном набором мер в рамках других, более масштабных атак и их комбинаций. Решается задача декомпозиции методики, которую применяет злоумышленник на первых этапах целенаправленного цифрового преследования.
Ключевые слова: интернет-агрессия, фишинг, кибератака, несанкционированный доступ, веб-форма, язык разметки, пользовательский интерфейс, хостинг, вредоносное программное обеспечение, фильтрация контента.

Введение

Процесс получения несанкционированного доступа выглядит следующим образом. Создаётся веб-проект, который в дальнейшем загружается на хостинг с анонимной учётной записью, к хостингу подключается домен (бесплатный или коммерческий), файлы фишинг-проекта загружаются в корневой каталог [1, 2]. В зависимости от уровня компьютерной грамотности жертвы, злоумышленник решает – использовать сервис по сокращению ссылок или нет. Когда цель не разбирается в сетевых доменах и не связана с информационными технологиями (ИТ), то сокращение ссылки может быть лишней для злоумышленника мерой. Далее, придерживаясь принципов социальной инженерии проводит манипуляции по передаче вредоносной формы и провоцирует ввод логина с паролем. После успешного входа в учётную запись, злоумышленником занимается сбором чувствительной информации, личных файлов и текстовых переписок.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

Создание веб-проекта

Для создания веб-проекта, который в дальнейшем будет загружен на хостинг необходимо применить HTML, CSS, JS и PHP. HTML – для основной разметки элементов на веб-странице, CSS для правильного позиционирования и дизайна [3]. С помощью этих двух языков злоумышленник сделает макет страницы, которая похожа на главный экран социальной сети. Воссоздание аналога веб-страницы онлайн платформы имеет два пути реализации. Согласно первому, повторяются только основные элементы, остальной дизайн становится похожим и имеет значительные для инженера информационной безопасности отличия. Для большинства людей, которые не связаны с информационными технологиями или информационной безопасностью, данные неточности тоже незаметны. Второй путь – создание очень похожего дубликата веб-страницы. Используются оригинальные элементы пользовательского интерфейса - шрифт, кнопки, фоновые изображения [4], ссылки на скачивание мобильной версии клиента на устройства с различными операционными системами и даже определяет какую версию демонстрировать пользователю в зависимости от устройства, через которое он переходит по ссылке.

В зависимости от ИТ грамотности жертвы принимается решение о применение JavaScript на фишинговом сайте. Если атакующий понимает, что его жертва хорошо разбирается в информационных технологиях, то JavaScript код обязательно применяется. JavaScript позволяет воссоздать анимации – успешный вход, сообщение об ошибке, поле для восстановления пароля и перехода на другие страницы. Чтобы сайт злоумышленника не блокировался, он создаёт и применяет SSL сертификат. На данном этапе интернет-агрессор легитимным способом избегает проверок со стороны браузера и даже межсетевых экранов.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

Загрузка веб-проекта на хостинг

После того, как веб-проект создан, начинается этап тестирования [5, 6]. Он происходит очень быстро, так как главная проверка направлена на изучение возможности перехвата пароля через форму. Главная задача заключается, чтобы форма записывала логин и пароль к нему. Обычно, после нажатия кнопки «Войти», срабатывает PHP-код, который копирует логин и пароль из двух полей в текстовой файл. Из-за того, что такой файл имеет цену одновременно перед обоими сторонами ИБ инцидента – хакером и инженером информационной безопасности, а точнее, список авторизационных данных для нескольких людей, его часто пересоздают, скрывают и делают резервные копии.

По завершению тестирования на анонимный почтовый адрес создаётся учётная запись хостинга. Обычно, это бесплатные хостинги. Часто злоумышленник не применяет в своих кибератаках платные альтернативы, потому что его задача требует минимального объёма памяти хранилища хостинга, обычно, качественный веб-проект фишинга занимает не более 30 мегабайт. На хостинг загружаются файлы проекта [7]. Каждой директории и файлам добавляются (или редактируются) права. У большинства файлов права только на чтение, у текстового файла, куда записываются логины и пароли – на чтение и редактирование (или, другими словами – полные права) [8]. Далее, злоумышленник получает бесплатный домен на этом же сервисе. Процесс соединения домена с хостингом происходит автоматически и очень быстро, не требуются усилия хакера или специфические знания о публикации ИТ проектов в продуктовую среду.

Тестирование веб-проекта на общедоступном домене

Затем, злоумышленник в адресной строке браузера вводит URL своего проекта, переходит по ссылке и видит свою фишинговую страницу. Для проверки работоспособности формы и механизма записи данных в файл, в

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

поля для логина и пароля пишет текст, нажимает кнопку «Войти» и проверяет текстовой файл веб-проекта. Здесь хакер может столкнуться с тем, что затруднительно, а в некоторых случаях занимает очень много времени, отслеживать изменения в сборе логинов и паролей. Он может упростить задачу и применить FTP-клиент, например «FileZilla» [9]. Через такое ПО можно наблюдать за файлами веб-проекта на хостинге точно так же, как происходили бы манипуляции с локальными и сетевыми дисками в системной утилите «Проводник». Тестовые логин и пароль записываются в текстовой документ. Хакер в обязательном порядке проводит это тестирование несколько раз. Это делается для того, чтобы перехват логина и пароля осуществлялся с первого раза и у жертвы не было времени подумать для того, чтобы отличить фишинг ресурс от легитимного.

Передача ссылки жертве и получение пары «логин-пароль»

Определив, а в некоторых случаях, предположив уровень ИТ грамотности жертвы принимается решение, пропускать ли ссылку через сервис для сокращения URL. Такой сервис применяется для маскировки ссылки под сокращенный URL без первоначального определения действительного адреса. Следующим этапом происходит отправка ссылки жертве дальнейшего акта интернет-агрессии. Ссылка может быть как явной, так и обработанной через сервис для сокращения, в виде кнопки или гиперссылки. В некоторых случаях сервис для сокращения URL с помощью искусственного интеллекта и системы рейтинга пользовательских ссылок может определить, что ссылка является фишинг ресурсом и применяется для сбора паролей. Ссылка направляется жертве, она на ссылку нажимается, веб-проект открывается в режиме просмотра. Жертва вводит логин с паролем, затем, нажимает кнопку «Войти». Происходит одно из трёх действий. Первое – имитация загрузки, то есть, нет анимации или всплывающих сообщений. Второе – сообщение об ошибке. Третье – передача логина и пароля на

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

легитимный веб-ресурс с дальнейшей успешной авторизацией. Информация, которую ввела жертва, записывается в текстовой файл. Это значит, что злоумышленник завладел логином и паролем к учётной записи своей жертвы.

Эксплуатация учётной записи, сбор текстовой информации и мультимедийных файлов

Сейчас большинство социальных сетей и известных интернет-форумов после успешного входа в аккаунт направляет его обладателю уведомление с точным временем и местоположением (определяет по IP-адресу клиента) успешного входа. Злоумышленник подбирает благоприятного для него время, чтобы зайти в учётную запись. Это необходимо, чтобы жертва пропустила или не обратила должного внимания на уведомление о входе в аккаунт. Хакер входит в учётную запись. Первая манипуляция, которую он проводит, это ищет письма «самому себе». В известных отечественных мессенджерах и социальных сетях это аналог облака, где важные письма и файлы направляются в собственный адрес для дальнейшего хранения.

Далее, злоумышленнику необходимо скачать все переписки жертвы на свой компьютер. Кроме текста хакер хочет загрузить файлы и мультимедиа, которые есть у жертвы в её личных и групповых переписках. Для этого используются плагины автоматизации, например «VkOpt». Подобные программы позволяют скопировать все переписки, представить их в виде отдельных HTML-файлов и скачать вложения в виде файлов (некоторые программы распределяют по папкам и архивам).

Затем, хакер пишет письма от имени своей жертвы её собеседникам, присылает компрометирующую информацию, в частности – реплаи сообщений, чувствительная информация, фотографии и видео. Данная информация становится достоянием общественности [10], и жертва очень быстро узнаёт об успешном инциденте информационной безопасности [11]. За это время хакер может распространить вредоносное ПО, незаконным путём

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

выманить денежные средства, навредить в личном кабинете учебного заведения жертвы, получить доступ к аккаунтам цели на других сервисах, сделать заведомо ложные заявления о терроризме и так далее.

Способы пассивного противодействия

Всего существует 2 направления противодействия – пассивное и активное. Активное применяется инженерами информационной безопасности, и обычно, вместе с пассивными мерами. К активным относится инспектирование кода, запуск подозрительных ссылок и программного обеспечения в песочнице, проверка сомнительного ПО через несколько сервисов (антивирус, облако с сигнатурами и онлайн платформы рейтинга файлов). Обычный же пользователь, не будет заниматься подобным. Он не имеет тех знаний и навыков, что есть у выпускников ИТ и ИБ специальностей, но в то же время, может применить пассивные меры, которые обеспечат должный уровень информационной безопасности, минируют риск несанкционированного доступа к учётным записям, краже персональных данных и распространению чувствительных файлов.

Первым этап – настройка 2ФА. Двухфакторная аутентификация сегодня есть во многих социальных сервисах. Второй фактор позволит вовремя узнать о попытке зайти в аккаунт и сделать успешную атаку подбора паролей безрезультатной.

Второй этап – включить уведомления безопасности. Даже если злоумышленник подобрал пароль и второй фактор, пользователь-жертва будет вовремя узнавать о манипуляциях хакера и сможет вовремя отреагировать.

Третий – создание сложного пароля. Чем длиннее и запутаннее пароль, тем сложнее его подобрать. Разнообразие символов и отсутствие логических связей с потенциальной жертвой позволит иметь сложный пароль, который сложно будет узнать способом подбора.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

Четвёртый – не хранить в заметах, почте и в диалогах пароли от других сервисов. Когда злоумышленник получит несанкционированный доступ к такой учётной записи, где хранится или обсуждается пароль, он может продолжить мероприятия по разведке и кибератакам более точечно [12].

Пятая мера – не хранить компрометирующие данные, файлы, фото и видео. Злоумышленник может опубликовать их в сети «Интернет», откуда из-за индексации и «Way Back Web Archive» в дальнейшем, даже если стереть данные со страниц социальных сетей, эту информацию будет невозможно полностью удалить.

Шестая – не авторизовываться с помощью личной почты на сервисах онлайн заметок и напоминаний. На таких сайтах пользователь часто хранит много персональных данных и личной информации. Если хакер получит несанкционированный доступ к почтовой учётной записи, с помощью которой создавался аккаунт на таких сервисах как «Evernote» или «YouGile», то восстановив пароль он увидит личные заметки, и возможно, даже файлы.

Седьмая – в обязательном порядке на каждом используемом устройстве иметь полную версию отечественного антивирусного программного обеспечения. С его помощью можно проводить сканирования и в режиме реального времени пресекать множество базовых кибератак.

Восьмой этап – установка антиспам ПО на смартфоне для того, чтобы фильтровались СМС. В частности те, где имеются ссылки. Например, телефонный антиспам от «Т-Банк» или «Kaspersky Who Calls». Девятый – установить на все устройства блокировщик рекламы. Такое ПО позволит избежать случайные и целенаправленные нажатия по рекламным баннерам, которые ведут на фишинговые страницы и скачивание вредоносного программного обеспечения. Десятый способ – даже если произошёл переход по фишинг ссылке и уже введён логин, то можно ввести неправильный пароль. Так можно будет понять, вредоносная ссылка или легитимная и попробовать

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

определить, с какого устройства и IP-адреса хакер пытается войти в учётную запись.

Заключение

Кибератака фишинг на первый взгляд может показаться лёгкой в митигации, но как правило началом другой, более комплексной компьютерной атаки. Её возможный вред недооценён и к сожалению, для человека, не связанного с информационной безопасность и информационными технологиями, фишинг в любом виде может быть незаметным. Интересная особенность заключается в том, что сама атака проводится исключительно с помощью легитимных технических инструментов и сервисов и не требует глубоких инженерных знаний. Пользователь, привыкший к комфорту, к сожалению, рискует не только предоставить злоумышленнику доступ к своим личным перепискам, но и способствует распространению чувствительных файлов. Защита от данной кибератаки, в основном, состоит из комбинации пассивных методов противодействия. Данные меры не так сложны в реализации и настройки, в результате которых обеспечивается сохранность персональных данных, личных файлов, значительно сужается поверхность атаки и сводится к нулю вероятность возникновения новых инцидентов информационной безопасности против пользователя.

Список литературы

1. Ермакова А.Л. Фишинг как распространённое киберпреступление современности // Закон и право. 2022. № 2. С. 149-151.
2. Dziatkovskii A., Hryneuski U. The possibilities of ensuring the security of the software product in the conditions of unauthorized access //Economic Annals-XXI/Ekonomìčnij Časopis-XXI. 2021. V. 189. №5-6(1). pp. 90-100.
3. Двуреченский И.О., Симонов И.Н., Гаев Л.В. Веб-приложения: основы, технологии и разработка // Инновационная наука. 2023. № 6. С. 35-37.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

4. Иконников М.А., Карманов И.Н. Меры и требования к защищённым веб-приложениям // Интерэкспо Гео-Сибирь. 2019. № 2. С. 13-19.

5. Вишневская Т.И. Тестирование программного обеспечения - как учебная дисциплина // Образовательные ресурсы и технологии. 2014. № 4. С. 83-39.

6. Zhang M., Belhadi A., Arcuri A. JavaScript instrumentation for search-based software testing: A study with RESTful APIs //2022 IEEE Conference on Software Testing, Verification and Validation (ICST). IEEE, 2022. pp. 105-115.

7. Антонова Т.С., Смирнов В.М. Фишинг как неизученное киберпреступление // СтудНет. 2021. № 6. С. 70-75.

8. Семенова З.В., Данилова О.Т., Ковшарь И.Р. Анализ безопасности стека технологий для разработки Web-ресурсов // Динамика систем, механизмов и машин. 2019. № 7. С. 39-48.

9. Стефанцов Д.А., Филимонов А.Е. Внедрение политик безопасности в компьютерные системы методами АОП на примере ftp-сервера Apache // Прикладная дискретная математика. 2010. № 7. С. 43-62.

10. Сагитова В.В., Васильев В.И. Применение метода экспертных оценок для автоматизации аудита информационных систем персональных данных // Вестник Уфимского государственного авиационного технического университета. 2017. № 73. С. 105-112.

11. Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Научный журнал Байкальского государственного университета. 2022. № 2. С. 36-44.

12. Давыдова О.Б. Защита персональных данных // Вестник науки и образования. 2018. № 1. С. 91-93.

References

1. Ermakova A.L. Zakon i pravo. 2022. № 2. pp. 149-151.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

2. Dziatkovskii A., Hryneuski U. Economic Annals-XXI/Ekonomìčnij Časopis-XXI. 2021. V. 189. №5-6(1). pp. 90-100.

3. Dvurechenskiy I.O., Simonov I.N., Gaev L.V. Innovatsionnaya nauka. 2023. № 6. pp. 35-37.

4. Ikonnikov M.A., Karmanov I.N. Interekspo Geo-Sibir'. 2019. № 2. pp. 13-19.

5. Vishnevskaya T.I. Obrazovatel'nye resursy i tekhnologii. 2014. № 4. pp. 83-39.

6. Zhang M., Belhadi A., Arcuri A. 2022 IEEE Conference on Software Testing, Verification and Validation (ICST). IEEE, 2022. pp. 105-115.

7. Antonova T.S., Smirnov V.M. StudNet. 2021. № 6. pp. 70-75.

8. Semenova Z.V., Danilova O.T., Kovshar' I.R. Dinamika sistem, mekhanizmov i mashin. 2019. № 7. pp. 39-48.

9. Stefantsov D.A., Filimonov A.E. Prikladnaya diskretnaya matematika. 2010. № 7. pp. 43-62.

10. Sagitova V.V., Vasil'ev V.I. Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2017. № 73. pp. 105-112.

11. Zav'yalov A.N. Nauchnyy zhurnal Baykal'skogo gosudarstvennogo universiteta. 2022. № 2. pp. 36-44.

12. Davydova O.B. Vestnik nauki i obrazovaniya. 2018. № 1. pp. 91-93.

Дата поступления: 24.01.2025

Дата публикации: 10.03.2025

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025