Научная статья

Original article

УДК 004.424

ФИШИНГ НА КОНКРЕТНОГО ПОЛЬЗОВАТЕЛЯ

PHISHING TO A SPECIFIC USER

Гнутова Ольга Викторовна студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), ol.gnutova@mail.ru

Мотуз Николай Сергеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), motuz0nik@yandex.ru

Gnutova Olga Viktorovna bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), ol.gnutova@mail.ru

Motuz Nikolay Sergeevich bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), motuz0nik@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.

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.

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

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

Собрав даже небольшое количество информации о жертве, злоумышленник может создать персонализированное и правдоподобное электронное письмо. Этих фишеров тоже нелегко поймать, так как большинство из них могут скрывать местонахождение своих серверов и работать почти полностью анонимно. Даже пользователь с отличным программным обеспечением безопасности может стать жертвой фишинговой атаки, потому что по большей части они полностью зависят от информации, введенной в форму, а не от заражения компьютера вредоносным ПО. Однако существует множество способов защиты от попыток фишинга. В этой статье мы обсудим три разных подхода, каждый из которых используется на разных этапах атаки. Атака может быть обнаружена до того, как она достигнет пользователя после того, как пользователь достиг фишингового сайта, или пользователь может быть обучен, чтобы знать об атаке. Используя эти подходы вместе, можно создать безопасную и безопасную среду для пользователя. Мы также рассмотрим современные методы фишинга, используемые для обмана своих жертв, и то, насколько он изменился за эти годы. А успехи в целенаправленных фишинговых атаках — и то, как легко они могут находить данные, просто просматривая общедоступные источники, — поражают. Предыстория Фишинг — одно из самых организованных преступлений 21-го века. Он определяется как тип вредоносного ПО или термин, обозначающий, когда кто-то отправляет поддельное электронное письмо случайным жертвам, чтобы попытаться получить личную информацию о них. В частности, в вычислительной технике фишинг — это преступная деятельность с использованием методов социальной инженерии для получения мошенническим путем конфиденциальной информации, такой как имена пользователей и пароли, путем попытки обмануть пользователей

популярных веб-сайтов, отправив им по электронной почте поддельные версии веб-сайта для предоставления их учетных данных. to.Этого может показаться легко избежать, но успехи фишингового сообщества делают фишинговые мошенничества все труднее и труднее идентифицировать с точки зрения жертв.

Термин «фишинг» превратился из почти плохо сконструированной атаки обмена мгновенными сообщениями в спуфинг целых веб-сайтов, чтобы обманом заставить пользователей предоставить личную информацию.

Для этой статьи мы провели обзор литературы, чтобы изучить текущее состояние фишинга и существующие решения. Чтобы учесть многие новые разработки в области фишинга, такие как целевой фишинг, фарминг и социальный фишинг, а также то, как фишеры разрабатывают все более и более убедительные сайты, и электронные письма для обмана пользователей, мы разработали трехэтапный подход к предотвращать и контролировать фишинг. На основе предложенной схемы решения по фишингу атака может быть остановлена до того, как она достигнет пользователя, как только пользователь окажется на фишинговом сайте, или путем обучения пользователей избегать ее самостоятельно. Цель этой статьи — дать четкий анализ текущего состояния фишинга и порекомендовать практические решения. В следующих разделах дается описание фишинга в целом, история фишинга и общие проблемы, связанные с его практикой, отравление DNS-кэша и т. д.

«Фишинг долгое время был серьезной проблемой для безопасности без решения. Проблема с фишингом заключается в том, что комплексного решения, надежно защищающего пользователей от фишинга, не существует. По мере развития средств защиты от фишинга менялись и современные методы фишинга. В результате важна потребность в более совершенных методах безопасности для выявления фишинговых атак. Обзор литературы «Фишинг и фарминг — смертельный дуэт». с течением времени.

Цели большинства фишинговых атак определяются как широкие или персонализированные. В современном обществе все находится в сети, и

безопасность личных учетных данных находится под угрозой. Фишинг можно рассматривать как один из самых старых и простых способов кражи информации у людей, и он используется для получения широкого спектра личных данных. Он также имеет довольно простой подход — отправить электронное письмо, само электронное письмо отправляет жертву на сайт, сайт крадет информацию.

Разбор фишингового процесса поэтапно описывается, что помогает создать представление о типичной фишинговой атаке. Мы можем визуализировать пагубные последствия фишинга для жертв с трех разных точек зрения: предприятия, клиента и государственного органа. Еще один вредоносный тип массового фишинга — фарминг. В статье рассматривается процесс фарминга и его отличия от фишинга. Фарминг использует вредоносный код, такой как вирусы, черви, трояны и программы-шпионы, для проведения изощренных атак, включая модификацию хост-файлов, отравление кэша DNS и т. д., о чем пользователь не узнает. Существует несколько решений, которые предлагаются для предотвращения фишинговых атак. «Онлайн-мошенничество в банках с фишингом»: здесь представлен более подробный анализ последствий фишингового мошенничества в онлайн-банкинге. Это исследование объясняет наиболее распространенные случаи мошенничества с онлайн-банками и то, как они связаны с фишингом. Здесь описано множество различных определений, которые можно использовать для фишинга. Кроме того, в этой работе описываются различные методы фишинга, которые могут использовать злоумышленники. В этом документе описываются причины увеличения распространенности фишинговых атак и приводится несколько примеров реальных организаций, пострадавших от этих злонамеренных действий. В нем представлен подробный план действий по борьбе с банковским мошенничеством путем фишинга. Различные таблицы данных включают лучшие методы хостинга для фишинговых сайтов и количество сообщений об атаках, количество которых увеличивается с годами. «Текущее состояние фишинговых атак». В этой работе автор

анализирует состояние фишинговых атак. атаки будут обманывать жертв с помощью нескольких типов вредоносных программ. Анатомия фишинговой атаки объясняется с помощью концепций поддельных фишинговых писем, создания поддельных веб-сайтов и монетизации украденной информации. Кратко объясняется психология, лежащая в основе того, почему фишинговые атаки работают. Фишинг наносит ущерб организациям и ежегодно стоит больших денег. Приведены рекомендации по контрмерам с различными подходами, чтобы не дать кому-либо стать жертвой фишинговых атак. «Классификация фишинговой электронной почты с использованием метода машинного обучения случайного леса». Основное внимание в этой исследовательской работе уделяется применению машинного обучения для выявления фишинга. электронной почты.

Во-первых, в нем вводится понятие фишинга и связанных с ним проблем. Также описывается концепция машинного обучения для ее использования при обнаружении фишинговых писем. Большинство методов фильтрации электронной почты не развивались вместе с методами фишинга, поэтому важно машинное обучение для обнаружения шаблонов в фишинговых электронных письмах. Классификация фишинговых писем, используемая в системе обнаружения машинного обучения, описана на основе набора правил. Он подходит к фишингу, используя эксперимент, основанный на алгоритме обнаружения фишинговых писем. Результаты для этого метода были обнадеживающими, с небольшим количеством ложных срабатываний. «Целевой фишинг: как обнаружить и смягчить угрозу». создать точку входа в организацию.6 Эта статья в основном посвящена концепции целевого фишинга и тому, чем он отличается от обычного фишинга. В нем рассказывается, как фишинг влияет на жертв и что получает злоумышленник, используя эти методы. Также приводится краткое описание того, как избежать целевого фишинга. «Социальный фишинг». В этой статье авторы определяют фишинг с точки зрения подходов социальных сетей7. Множество способов, которыми можно добывать и использовать личную информацию жертвы. с

использованием данных, которые можно легко найти в Интернете. Злоумышленник может использовать различные сайты социальных сетей для целенаправленной и гораздо более эффективной тактики фишинга. В документе описывается исследование, которое было проведено путем просмотра и документирования отношений, находящихся в свободном доступе для общественности на таких сайтах, и использования этой информации для запуска имитации фишинговой атаки на их субъектов. Во время этой процедуры авторы описывают методы социальных фишинговых атак, которые используются для кражи учетных данных пользователей. Наконец, в документе обсуждаются результаты эксперимента и демографические данные субъектов, подвергшихся атакам.

«Защита людей от фишинга: разработка и оценка встроенной обучающей системы электронной почты»: в этой работе обсуждается возможный форма предотвращения фишинга в формате системы электронной почты.8 Вместо того, чтобы сосредоточиться на автоматизированной системе веб-браузера или алгоритмах, которые обнаруживают фишинговые атаки, это исследование было сосредоточено на подходе с точки зрения пользовательского интерфейса. Авторы разработали встроенную обучающую систему в свои почтовые серверы, чтобы обучать пользователей тому, как идентифицировать себя и защищаться от попыток фишинга с помощью основных рассуждений и простых советов. В ходе исследования пользователям почтового сервера отправляли ложные фишинговые электронные письма со встроенными ссылками, по которым при нажатии на них они попадали на страницу.

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.

References

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.

© Гнутова О.В., Мотуз Н.С., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Гнутова О.В., Мотуз Н.С. ФИШИНГ НА КОНКРЕТНОГО ПОЛЬЗОВАТЕЛЯ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.