УДК 304.44

Ивлева Анастасия Николаевна, *студентка 4-ого курса кафедры «Безопасность в цифровом мире», МГТУ им. Н. Э. Баумана, Москва, Российская Федерация*

e-mail: hanckhrom@yandex.ru

Каледина Полина Вадимовна, *студентка 4-ого курса кафедры «Безопасность в цифровом мире», МГТУ им. Н. Э. Баумана, Москва, Российская Федерация*

e-mail: p.kaledina@mail.ru

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ГОСУДАРСТВЕННЫХ ТЕХНИЧЕСКИХ СИСТЕМ ПО ПРОТИВОДЕЙСТВИЮ ФИШИНГУ

Аннотация: В статье рассматривается проблема фишинга и методы противодействия им. Обращается внимание на то, что фишинговые атаки - это один из наиболее распространенных и опасных видов киберпреступности. Ежедневно совершается более ста миллионов фишинговых атак, а в кризисные времена их количество только возрастает. Определенные слои населения, которые испытывают временные финансовые трудности, хотят улучшить свой качественный уровень жизни, воровством идентифицирующих знаков в банковских системах. Мошенники пользуются неразберихой в мире и маскируют свои вредоносные рассылки под письма из официальных источников, перенаправляя пользователей на мошеннические сайты, чтобы обманом побудить их ввести конфиденциальную информацию. Многообразие причин и схем фишинга обуславливает сложность борьбы с ним, ведь фишинг базируется на социальной инженерии, которую невозможно охватить машинными и программными алгоритмами защиты.

Ключевые слова: фишинговые атаки, сценарий DDL, ГосСОПКА, системы SIEM, цифровая среда, киберпреступния, социальная инженерия.

Annotation: The article discusses the problem of phishing and methods of countering it. Attention is drawn to the fact that phishing attacks are one of the most common and dangerous types of cybercrime. More than a hundred million phishing attacks are carried out daily, and in times of crisis their number only increases. Certain segments of the population who are experiencing temporary financial difficulties want to improve their quality of life by stealing identifying signs in banking systems. Scammers take advantage of the confusion in the world and disguise their malicious mailings as letters from official sources, redirecting users to fraudulent sites in order to trick them into entering confidential information. The variety of causes and schemes of phishing makes it difficult to combat it, because phishing is based on social engineering, which cannot be covered by machine and software protection algorithms.

Keywords: phishing attacks, DDL scenario, GosSOPKA, SIEM systems, digital environment, cybercriminal, social engineering.

Термин «фишинг» не имеет строго регламентированного определения, так как особенность данного явления сводится к характеризующему его методу возникновения и распространения внутри цифровой среды. Слово фишинг впервые было использовано в 1996 году в группе новостей Usenet под названием AOHell [4, с. 7]. Практиками в области исследования и противодействия фишингу постановляется, что это форма кражи личных данных, реализуемая, когда вредоносный веб-сайт выдает себя за законный, чтобы получить конфиденциальную информацию, такую как пароли, данные учетной записи или номера кредитных карт. Термин происходит от англоязычного «phishing», созвучного со словом fishing - «рыбалка». Фишинговая кампания всегда направлена на то, чтобы подтолкнуть жертву к действию: сообщение должно быть составлено таким образом, чтобы интерес к содержимому был обусловлен срочностью, беспокойством или корыстными побуждениями [7, с. 3].

Согласно исследованию Себастьяна Виу, директора по продуктам

кибербезопасности в Stormshield (европейский лидер в области безопасности цифровой инфраструктуры), киберпреступники чаще всего играют на эмоциях своих жертв. Вот почему этот тип атаки, функционирующий в основном на механизме социальной инженерии, так успешен [6].

Фактически, пользователь, не подразумевая о существующей угрозе, позволяет «поймать» себя на фальшивый домен, выдающий себя за подлинный, отчего и возникает ассоциация с ловлей на приманку [4, с. 7]. Замена латинской f на ph можно расценивать как отсылку к ранее актуальной форме хакерства - «фрикинг», заключающегося в оригинальном способе телефонного взлома («phreaking»).

Данный тип противоправного деяния использует комбинацию социальной инженерии и технологий для сбора конфиденциальной и личной информации, такой как пароли и данные кредитных карт, выдавая себя за заслуживающего доверия человека в электронном сообщении. Фишинг использует поддельные электронные письма, которые выглядят подлинными и якобы поступают из законных источников, таких как финансовые учреждения, сайты электронной коммерции и т.д., чтобы пользователи переходили на мошеннические веб-сайты по ссылкам, указанным в фишинговом письме [2, с. 3]. Мошеннические веб-сайты предназначены для имитации внешнего вида веб-страницы реальной компании.

Гуськова А. М. в своей работе рассматривает фишинг как основной метод социальной инженерии в схемах финансового мошенничества. Атаки с использованием методов социальной инженерии на текущий момент являются одним из самых опасных и распространенных видов атак, нацеленных на нарушение конфиденциальности и получения доступа, поскольку технически они ориентированы на психологические манипуляции [1, с. 2].

По данным Symantec, - американской компании - разработчика программного обеспечения в области кибербезопасности, каждое двухтысячное письмо является фишинговым [8]. То есть, ежедневно совершается больше ста миллионов атак, в кризисные времена их количество только возрастает.

Определенные слои населения, испытывающие временно непреодолимые финансовые трудности, которые также имеют специфичный навык работы с цифровой средой, стремятся повысить свой качественный уровень жизни посредством воровства идентифицирующих знаков в банковских системах. Мошенники пользуются хаосом и неразберихой, вызванными также спорными политическими и экономическими событиями, интригующими население. Это дает преступникам отличную возможность маскировать свои вредоносные рассылки под письма из официальных источников. Эти письма перенаправляют пользователей на мошеннические сайты, чтобы обманом побудить их ввести конфиденциальную информацию.

В период с 2019 по 2021 год Facebook, LinkedIn и WhatsApp были одними из наиболее часто атакуемых брендов. После волны Covid-19, бренды доставки также стали мишенью для фишинга в 2021 году [9, с. 49]. Компания Verizon Communications Inc, - один из мировых лидеров в коммуникациях, технологиях, информации и развлекательных сервисах, провела в 2020 году эксперимент, запустив среди сотрудников дочерней организации фишинговую атаку. Согласно исследованию Verizon, среднее время, необходимое первой жертве широкомасштабной фишинговой рассылки, чтобы открыть вредоносное письмо, составляет 16 минут, а на то, чтобы сообщить о фишинговой кампании в отдел информационной безопасности, обычно уходит вдвое больше времени - 33 минуты [3, с. 6]. Учитывая, что 91% киберпреступлений начинается именно с успешной фишинговой рассылки по электронной почте, эти 17 минут могут обернуться государственного органа катастрофой.

Обычно во время фишинговой атаки для обмана жертвы используется сразу несколько приемов. Чтобы обезопасить себя, злоумышленники зачастую копируют фирменный стиль банка, и меняют одну-две буквы в юридическом названии [6, с. 11].

Хотя на первый взгляд ссылка может выглядеть совсем как легитимный веб-сайт, можно визуально обнаружить небольшие несоответствия или нестыковки, раскрывающие истинную природу ссылки. Создание таких

мошеннических доменов, близких по написанию к известным сайтам, называется тайпсквоттингом [5, с. 10]. Злоумышленники могут получить доступ к этой информации, и, если жертва использует одно и то же имя пользователя и пароль на нескольких сайтах, под угрозой окажутся другие учетные записи в интернете. По состоянию на июль 2022 года в .fr было зарегистрировано более 1000 копирующих оригинальных доменов [4, с. 4].

Таким образом, можем прийти к выводу, что сложность борьбы с фишингом обуславливается многообразием его оснований для выделения прочих видов мошенничества, их комбинаций в отдельные преступные схемы и шаблоны. Подчеркнем, что техническая сторона взаимодействия с исследуемой цифровой средой является лишь универсальным инструментом в механизме совершения махинации, большая лишь функциональная значимость возлагается на личностных социальных навыках преступника.

Иногда вредоносное программное обеспечение включает программу-вымогатель, которая пробирается через сеть жертвы, шифруя и перемещая конфиденциальные данные для хранения с целью выкупа.

Фишинговая ссылка также может быть изменена и встроена в цепочку перенаправляющих ссылок, поэтому фишинговые фильтры не могут получить доступ к окончательному URL-адресу. Текст электронного письма также перерабатывается киберпреступниками и встроен в изображение, чтобы противодействовать обнаружению на основе текста.

Вначале для рассылок писем использовались взломанные серверы и скомпрометированные учетные записи, однако позже преступники начали регистрировать фишинговые домены и создавать для них самоподписанные сертификаты. Письма зачастую отправляются от имени банков, у которых не был настроен SPF, с арендованных серверов с подмененными заголовками. Во вложении письма содержались эксплоиты под MS Office Word с decoy документами. Помимо эксплоитов рассылались письма с вложенными CHM-файлами, запускающими Powershell-скрипты и JS-скрипты. Управление атакой и закрепление в системе проводит атаки с Linux-машины с использованием

утилиты WinExe (Linux аналог PSExec), которая может запускать программы на удаленном узле через SMB-протокол. После закрепления в системе троян устанавливает stager Meterpreter на зараженную систему. Meterpreter - это инструмент пост-эксплуатации, включающий динамически расширяемую нагрузку, которую можно распространять по сети во время выполнения. Инструмент заставляет целевую систему запускать внедренную DLL.

Распространение сценария DLL реализуется с использованием инструментов автоматизации фишинговых атак, такие как Gophish. Киберпреступники прибегают к готовым шаблонам для замаскированных страниц и шаблонов сообщений электронной почты.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак является территориально распределенной совокупностью центров (сил и средств), организованной по ведомственному и территориальному принципам, в числе которых — Национальный координационный центр по компьютерным инцидентам. Созданию такой системы послужил Указ Президента РФ от 15 января 2013 года № 31с «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 3 февраля 2012 г. №803).

Ряд организаций обязан использовать фиды поставляемые ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак) и ФинЦЕРТ (Автоматизированная система обработки инцидентов); в некоторых случаях эти данные могут помочь защититься от фишинговой атаки, однако эффективность тех сведений, которые содержатся в обновлениях специализированных продуктов выше. В рамках поддержания актуальной информации о зоне ответственности в отношении практики противодействия фишингу необходим сбор данных об инфраструктуре объекта, в том числе описание внешнего периметра организации и способов выхода в интернет, наличие информационных и

технологических «стыков» с другими объектами КИИ или прочими информационными системами [10]. Важным является также статус состояние установленных обновлений и патчей и возможные сроки установки корректирующих патчей.

Анализ статистических данных показал, что наиболее часто фишинговым атакам подвергаются официальные сайты Пенсионного фонда и Фонда социального страхования. Данный факт обусловлен тем, что на указанных сайтах установлено отсутствие нормативных правовых актов, позволяющих определять актуальные угрозы безопасности данных. С точки зрения конкретной организации, данная инвентаризационная информация не имеет существенного отношения к обеспечению информационной безопасности. При возникновении очередной массовой угрозы или уязвимости появляется возможность корректно оценить, какие именно объекты в состоянии самостоятельно и в штатном режиме устранить уязвимости, а в каких случаях необходимо более детальное информирование и особый порядок сопровождения конкретной задачи.

Зачастую злоумышленники используют скомпрометированные вычислительные ресурсы для атаки на другие инфраструктуры. В таком случае, если атака направлена на один из объектов гос. органа, при анализе технических индикаторов сможет выявить, что часть ботов использовали для атаки адреса одного из прочих объектов, и проинформирует ответственные службы об угрозе в инфраструктуре. В рамках отчетности по инцидентам происходит информирование вышестоящего центра ГосСОПКА о выявленных в своей инфраструктуре инцидентах со следующими ключевыми характеристиками: Техническая информация об атаке (адреса, инструменты, методы). Результаты реагирования и ликвидации последствий. Необходимость содействия со стороны вышестоящего центра.

Отметим, что в 2015 году член Комитета по безопасности и противодействию коррупции Илья Костунов заявлял о рассмотрении нового законопроекта антифишинговых систем. Суть его заключалась в том, что на

основе собранных данных о вызывающих подозрение фишинговой угрозе доменах, Роскомнадзор и Центробанк принимали решение о блокировке данных доменов в досудебном порядке. Данный законопроект не был реализован до конца по причине осложненного механизма обращения к уполномоченным органам, однако на сегодняшний день действует в тестовом режиме прототип автоматической системы поиска фишинговых сайтов. Оператором новой автоматической системы является межотраслевой научно-исследовательский институт «Интеграл», подведомственный Минцифры.

Задачи информационного взаимодействия в рамках разработанной государственной системы, охватывающей безопасность относительно киберугрозам, не являются простой отчетностью по инцидентам для накопления статистики. Модель построения ГосСОПКА, в которой ключевыми элементами системы являются ведомственные и корпоративные центры, призвана объединить специалистов реагирования и расследования компьютерных инцидентов в единое экспертное сообщество, обменивающегося обезличенной, но технически ценной информацией об угрозах безопасности. Данные об инцидентах могут передаваться и автоматизировано, и вручную. В последнем случае используются специальные кабинеты для отправки сведений, в первом – особым образом настроенные SIEM.

SIEM - (Security Information and Event Management) это решение, которое позволяет организациям обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб бизнесу. Сам термин был появился в 2005 году. Первоначально аббревиатура представляла собой комбинацию двух терминов, обозначающих область применения ПО: SIM (Security Information Management) — управление информационной безопасностью и SEM (Security Event Management) — управление событиями безопасности. SIEM-система должна собирать, анализировать и представлять информацию из сетевых устройств и устройств безопасности. Технология SIEM позволяет собирать данные журнала событий от различных источников, анализировать их в реальном времени, выявляя аномальные действия, и

принимать необходимые меры. Также в эту систему должны входить приложения для управления идентификацией и доступом, инструменты управления уязвимостями и базы данных и приложений [7, с. 14].

SIEM-системы обеспечивают возможность отправки предупреждений на основе предопределенных настроек, а также возможность просмотра данных на разных уровнях детализации, мониторинг подозрительного исходящего трафика и передаваемых по сети данных с использованием журналов брандмауэра, журналов веб-прокси и NetFlow [9, с. 28].

Внедрение и актуализация SIEM-систем в государственные органы представляет собой наиболее эффективный метод выявления угрозы фишинговых атак. Таким образом, механизм противодействие фишинговым атакам претерпевает позитивные изменения на государственном уровне. Продолжается модернизация нового программного обеспечения, снижающего шансы успешной атаки. Необходимо, чтобы тенденции по преследованию источников фишинговых угроз получили своё закрепление в законодательстве.

Библиографический список:

1. Гуськова, А. М. Фишинг как основной метод социальной инженерии в схемах финансового мошенничества / А. М. Гуськова. // Казань : Молодой ученый. - 2019. — С. 3-6.

2. Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения / А.Н. Завьялов. — DOI 10.17150/2411-6262.2022.13(2).36. — EDN SRVHGS // Baikal Research Journal. — 2022. — Т. 13, № 2. – С.20-26.

3. Юсупов М.Ю. Фишинг как угроза конфиденциальности в сети / М.Ю. Юсупов, А.О. Путилов. — EDN BSZNZY // E-Scio. — 2021. — № 10 (61). — С. 223-232.

4. Abbasi, A., Dobolyi, D. G., Vance, A., Zahedi, F. «The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites» // Information Systems Research (32). - 2021. - С. 410-436.

5. Belcic, I. Rootkits defined: what they do, how they work, and how to remove them // Avast Academy – 2020. - С. 7 -12.

6. Nguyen, C., Jensen, M., Day, E. «Learning Not to Take the Bait: A Longitudinal Examination of Digital Training Methods and Overlearning on Phishing Susceptibility» // European Journal of Information Systems. – 2021. - С. 1-25.

7. Roderic Broadhurst, Katie Skinner, Nick Sifniotis, Bryan Matamoros-Macias, Yuguang Ipsen. «Phishing and cybercrime risks in a university student community». / Criminology Research Advisory Council Grant: CRG 51/16–17. ISBN 978 1 92530426 8 // Australian Institute of Criminology - 2020 – С. 1 – 50.

8. Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy // Cardiff School of Technologies, United KingdomFront. Comput. Sci., - 2021 – С.15-43.

9. Yadav, S., Bohra, B.. A review on recent phishing attacks in Internet // International Conference on Green Computing and Internet of Things (ICGCIoT) - 2018 - IEEE – С. 1312-1315.

10. Cyber Media «ГосСОПКА: перспективы у цифрового щита России». 2022. Режим доступа: https://securitymedia.org/info/gossopka-kakie-perspektivy-u-tsifrovogo-shchita-rossii.html.