вольными последовательностями, встает вопрос о выборе принципа применения этих алгоритмов к данной предметной области. Здесь существует два пути.

Первый подразумевает модификацию классических алгоритмов для обработки числовых (в т. ч. и комплексных) данных. Это самый очевидный путь. В то же время он довольно трудоемкий, требует глубокого и детального изучения математической базы и может повлечь за собой непредвиденные сложности в связи с дальнейшей оптимизацией.

Второй вариант кажется более затратным по времени и вычислительным мощностям, но, на мой взгляд, оправдывает себя простотой реализации. Он состоит в переводе числовой последовательности в некую эквивалентную ей последовательность символов, к которой затем можно применить классический алгоритм поиска без каких-либо дополнительных манипуляций с данными или модификаций самого алгоритма.

Список литературы:

1. Попов В.Н. и др. Подготовка набора данных для обучения нейронной сети, используемой в задачах сравнения аудиофайлов // Проблемы правовой и технической защиты информации. 2021. №. 9. С. 22-27.

2. Юрченко Н.Ю. Аудио- и видеоматериалы из интернета: трудности и возможности // Вестник УМЦ. 2017. № 15-2. URL: https://cyberleninka.ru/article/n/audio-i-videomaterialy-iz-interneta-trudnosti-i-vozmozhnosti (дата обращения: 15.01.2025).

3. Слепой ABX тест звучания аудиофайлов. URL: https://hamsterilla.ru/slepoj-abx-test-zvuchaniya-audiofajlov/ (дата обращения: 15.01.2025).

ДЕТЕКТИРОВАНИЕ ПРИЗНАКОВ ФИШИНГОВЫХ АТАК НА ОСНОВЕ ВСТРОЕННЫХ СРЕДСТВ ЗАЩИТЫ ПОЧТОВЫХ СЕРВИСОВ

Конанов О.И.

Российский экономический университет имени Г.В. Плеханова, Москва, e-mail: 2310.Oleg.Konanov@gmail.com

Статистические отчеты различных организаций показывают, что почтовый фишинг является одной из самых распространенных и эффективных техник кибератак, использующихся как при атаках на почтовую инфраструктуру организаций, так и на частные почтовые ящики. По данным отчета ФБР IC3 Report за 2021 год, на долю фишинговых атак приходится почти 22% всех случаев утечки данных, что подтверждает их позицию как одного из самых распространенных киберпреступлений. В отчете Verizon за 2022 год говорится, что 36% всех случаев утечки данных связаны с фишингом. По оценкам специалистов, к 2022 году атаки с использованием выкупа или фишинга будут происходить каждые 11 секунд [1].

Кроме того, несмотря на кажущуюся простоту почтового фишинга, данная техника непрерывно совершенствуется злоумышленниками. Исследования показывают, что более 80% фишинговых рассылок осуществляются с помощью специализированного программного обеспечения. Также злоумышленники стали активно применять технологии машинного обучения, например, получившие в последнее время широкое распространение языковые модели, для формирования правдоподобных фишинговых писем и обхода существующих средств защиты почтовых сервисов [2].

В статье рассмотрены актуальные техники фишинговых атак, в том числе предложены дополнительные фишинговые подтехники, не представленные в матрице Mitre Att&ck, выделены признаки того, что письмо является фишинговым, механизмы детектирования данных признаков, а также эффективность встроенных средств защиты почтовых сервисов по детектированию данных признаков.

Показано, что существующие встроенные средства защиты почтовых сервисов не детектируют все фишинговые признаки и требуют дальнейшего совершенствования.

Анализ техник фишинговых атак и их признаков

Почтовый фишинг может быть разделен на целевой (направленный на конкретного сотрудника, узкую группу сотрудников в рамках одной организации, частный почтовый ящик конкретного пользователя) и массовый (может быть направлен на всех сотрудников одной организации, сотрудников различных организаций, частные почтовые ящики широкого круга пользователей). В рамках настоящего исследования были рассмотрены целевые фишинговые атаки.

С точки зрения фреймворка Mitre Att&ck, фишинг входит в тактику Initial Access. Целью злоумышленника на данном шаге является получение несанкционированного доступа к ИС.

С точки зрения Mitre Att&ck, злоумышленник может выполнить поставленные задачи на данном шаге с помощью следующих подтехник, связанных с почтовым фишингом [3]:

1. Целевой фишинг с вложением – к письму прикрепляется вредоносное вложение, например, исполняемый файл, архив, документ Microsoft Office с вредоносным расширением и т.д.

2. Целевой фишинг с ссылкой – в текст письма помещается вредоносная ссылка, ведущая, например, на поддельный корпоративный ресурс (как правило с формой авторизации с целью получения логина и пароля сотрудника), загрузчик вредоносного ПО и т.д.

3. Целевой фишинг с помощью стороннего сервиса – данная подтехника зачастую комбинируется с подтехниками целевого фишин-

га с вложением или ссылкой и предполагает, что злоумышленник отправит письмо от имени авторитетного стороннего сервиса, например, подрядчика организации. При этом, злоумышленник может как подделать учетную запись, так и отправить письмо от имени авторитетного источника, в случае если учетная запись последнего была ранее скомпрометирована.

По мнению автора, отдельно следует выделить следующие фишинговые подтехники, не представленные в матрице Mitre Att&ck:

1. Целевой фишинг с введением в заблуждение – в рамках это подтехники злоумышленник может не прикреплять к письму вредоносное вложение или ссылку, но использовать социальную инженерию с целью склонения сотрудника к предоставлению какой-либо конфиденциальной информации. Данная подтехника может комбинироваться с целевым фишингом с помощью стороннего сервиса.

2. Целевой фишинг с целью повышения доверия – письмо, сформированное в соответствии с данной подтехникой, не содержит вредоносного содержимого и не склоняет сотрудника к передаче конфиденциальной информации, но направлено на повышение доверия сотрудника к злоумышленнику путем симуляции легитимной деловой переписки. Данная подтехника может предшествовать применению перечисленных выше подтехник.

Результаты анализа фишинговых подтехник позволяют сделать вывоу, что даже письмо, не содержащее вредоносного содержимого, может представлять потенциальную опасность для информационной безопасности предприятия или частного почтового ящика. Ввиду этого факта, в ходе настоящего исследования, был проведен анализ существующих фишинговых признаков.

Признаки, указывающие на то, что письмо является фишинговым можно разделить на 2 основные группы:

1. Признаки в почте отправителя – с точки зрения протокола SMTP располагаются в заголовках письма: Return-Path, Received, From, Sender, Reply-To, In-Reply-To и т.д.

2. Признаки в содержимом письма – с точки зрения протокола SMTP располагаются в теле письма.

Среди признаков (маркеров) почты отправителя, указывающих на то, что письмо может быть фишинговым, выделены следующие (в порядке убывания степени угрозы)[4,5]:

1. Применение Email spoofing, техники подделки адреса легитимного отправителя в электронных письмах. Наиболее распространенные виды email spoofing: спуфинг схожего домена (например, легитимный домен @example.com заменяется на домен @example.ru), спуфинг легитимного домена (подстановка в заголовок From реального домена организации), AD-спуфинг (указание поддельного адреса в качестве имени отправителя), подмена имени отправителя (в заголовках From и Reply-to содержится реальный адрес злоумышленника, а имя отправителя подделывается на легитимное), изменение значений From и Reply-to (подделывается как имя отправителя, так и поля From и Reply-to).

2. Плохая репутация домена отправителя. На нее могут указывать наличие домена в черных списках сервисов проверки доменов (например, Spamhaus или SORBS). Другим маркером подозрительного домена может выступать отсутствие служебных DNS-записей DMARC, SPF, DKIM.

3. Подозрительный адрес электронной почты. Адрес электронной почты можно считать подозрительным, если он не содержит какой-либо содержательной информации об отправителе или отправителем является лицо, получение письма от которого не связано с должностными обязанностями конкретного сотрудника.

4. Получение письма от отправителя впервые. В зависимости от рабочих задач конкретного сотрудника (например, если он не занимается коммуникацией с клиентами), факт получения письма от нового отправителя может являться признаком фишинга. С другой стороны, если почтовый сервис (или стороннее СЗИ) указывает на то, что письмо получено от отправителя впервые, но сотрудник ранее вел переписку с данным отправителем, это является признаком email spoofing и, следовательно, фишинга.

5. Адрес электронной почты был создан недавно. Данные, в том числе электронной почты, утекают очень часто. Это привело к тому, что некоторые организации, работающие в сфере интернет-продаж, проверяют электронный адрес покупателя на предмет его наличия в утечках электронных почтовых ящиков. Если электронный адрес когда-либо был подвергнут компрометации, то это может свидетельствовать о том, что адрес является легитимным. Подобная логика может быть применима и в области борьбы с фишингом [6].

6. Получение письма от внешнего источника. Если рабочие обязанности сотрудника не предусматривают взаимодействие с клиентами или подрядчиками, но только с другими сотрудниками организации (то есть, пользователями одного домена), то это может быть признаком фишинга.

Среди признаков содержимого письма, указывающих на то, что письмо может быть фишинговым, выделены следующие (в порядке убывания степени угрозы):

1. Вредоносное вложение. Ранее в качестве вредоносного вложения были распространены исполняемые файлы (.exe), но в последнее время вредоносный ПО, как правило, доставляется на устройство жертвы с помощью архивов (.rar, .zip и т.д.), офисных файлов (.docx, .xslx и т.д.),

PDF-файлов, картинок (.jpg, .pdf и т.д.) и прочих файлов, обмен которыми по почте распространен при выполнении бизнес-задач.

2. Вредоносная ссылка. Для маскировки и передачи вредоносных ссылок используется огромное число методов, например, размещение вредоносной ссылки под легитимной ссылкой с помощью html-кода, размещение вредоносной ссылки под картинкой, размещение вредоносной ссылки под текстом письма, размещение вредоносной ссылки в вложении (которое, при этом, не является вредоносным), передача вредоносной ссылки с помощью QR-кода. Как правило, вредоносные ссылки ведут на поддельный корпоративный веб-ресурс (с целью перехвата данных учетной записи пользователя) или на загрузчик вредоносного ПО. Зачастую, при формировании вредоносного URL-адреса, используются подходы, аналогичные email spoofing, например, использование схожего доменного имени (exampl.ru вместо легитимного example.ru), подмена домена (example.com вместо легитимного example.ru) и т.д.

3. Фишинговые паттерны. В существующем ландшафте угроз квалифицированный злоумышленник, как правило, проводит доскональную разведку организационной структуры предприятия и бизнес-задач отдельных сотрудников перед отправкой фишингового письма, чтобы симулировать легитимность письма. Однако в подавляющем большинстве фишинговых писем могут быть обнаружены следующие фишинговые паттерны: симуляция должностного положения (например, письмо отправлено сотруднику от имени вышестоящего руководителя), угроза (например, письмо отправлено от имени отдела ИБ с требованием сменить пароль), поощрение (например, предоставление информации о премии или повышении и т.д. Тоже справедливо и для частных почтовых ящиков. Все многочисленные фишинговые паттерны направлены на то, чтобы принудить жертву перейти по вредоносной ссылки, открыть вредоносное приложение или передать конфиденциальную информацию.

4. Замена символов. Зачастую злоумышленники, с целью обхода средств защиты электронной почты, используют омоглифы – символы, графически одинаковые или похожие друг на друга. Также распространена замена символов с помощью изменения кодировки [7]. Ввиду распространенности данного подхода при манипуляциях злоумышленника с HTML-кодом письма, выделено в отдельный признак.

5. Подозрительный HTML/CSS-код. Злоумышленники манипулируют с HTML/CSS-кодом письма, например, с целью сокрытия ссылок на фишинговые веб-страницы или загрузчики опасного ПО. Применяется огромное число техник, например, сокрытие ссылок под картинкой, применение упомянутых ранее омоглифов, стилизация письма под рассылки от авторитетных организаций и т.д.

6. Текст, сформированный с помощью языковых моделей. В последнее время получили широкое распространение большие языковые модели, используемые, среди прочего, для формирования фишинговых писем [8].

7. Текст, сформированный с помощью машинного перевода. Распространенный ранее фишинговый признак, обусловленный тем, что зачастую злоумышленник зачастую атакует иностранные почтовые ящики и не является носителем языка, на котором говорит жертва. Данный признак хоть и сохраняет свою актуальность, постепенно уходит в прошлое ввиду существенного развития алгоритмов машинного перевода.

8. Грамматические и орфографические ошибки. Еще один распространенный ранее признак фишинга, уходящий в прошлое ввиду распространения языковых моделей и более продвинутых алгоритмов машинного перевода.

9. Универсальные обращения. Один из выделенных отдельно фишинговых паттернов, ввиду его распространенности, при этом мало актуальный в текущем ландшафте угроз, в котором, как правило, злоумышленник знает ФИО жертвы. При этом, письма, начинающиеся с универсального обращения, например, “уважаемый коллега”, должны быть проверены на наличие других признаков фишинга.

Механизмы детектирования признаков фишинговой атаки

Из перечисленных выше фишинговых признаков, ключевыми являются: email spoofing, вредоносные вложения, вредоносные ссылки и фишинговые паттерны – данные признаки однозначно указывают на фишинговую природу письма. Остальные признаки с разной долей вероятности позволяют судить о фишинговой природе письма. Тем не менее, комплексный анализ письма на предмет фишинга требует анализа получаемых писем на все перечисленные выше фишинговые признаки, для детектирования которых применяются различные механизмы. Механизмы детектирования различных фишинговых признаков приведены в таблице 1. Правый столбец таблицы содержит фишинговые признаки, рассмотренные выше, а левый столбец содержит основные механизмы детектирования, применяемые как во встроенных в почтовые сервисы, так и в сторонних антифишинговых средствах защиты.

В ходе исследования было проведено тестирование наиболее распространенных почтовых сервисов на их возможность по детектированию фишинговых признаков. Проверка считалась успешной, если почтовый сервис блокировал получение письма с фишинговыми признаками или предупреждал получателя о их наличии в письме.

Таблица 1

Механизмы детектирования фишинговых признаков

Фишинговый признак	Механизмы детектирования
Применение Email spoofing	Фильтрация на основе репутации сервера-отправителя Фильтрация на основе проверок DNS-записей сервера отправителя Фильтрация на основе проверок DNS-записей домена отправителя из конверта письма Фильтрация на основе проверок SPF-записей Фильтрация на основе DKIM Фильтрация на основе DMARC
Плохая репутация домена отправителя	Фильтрация на основе данных сервисов репутации доменов Фильтрация на основе собственных черных списков доменов
Подозрительный адрес электронной почты	Фильтрация на основе данных сервисов репутации адресов электронной почты Фильтрация на основе собственных черных списков адресов электронной почты Фильтрация на основе механизмов машинного обучения
Получение письма от отправителя впервые	Детектирования с помощью встроенных механизмов почтовых сервисов
Адрес электронной почты был создан недавно	Фильтрация на основе данных сервисов, проверяющих наличие электронного адреса в утечках
Получение письма от внешнего источника	Детектирования с помощью встроенных механизмов почтовых сервисов
Вредоносное вложение	Эвристический анализ Сигнатурный анализ Анализ хэш-сумм Запуск в защищенной программной среде
Вредоносная ссылка	Фильтрация на основе репутации домена Фильтрация на основе содержимого URL-адреса Фильтрация на основе используемых протоколов Фильтрация на основе сетевого трафика
Фишинговые паттерны	Фильтрация на основе механизмов машинного обучения Фильтрация на основе bag of words
Замена символов	Фильтрация на основе анализа исходного html-кода
Подозрительный HTML/CSS-код	Парсинг исходного HTML-CSS кода на основе заданных правил Фильтрация на основе механизмов машинного обучения
Текст, сформированный с помощью языковых моделей	Фильтрация на основе механизмов машинного обучения
Текст, сформированный с помощью машинного перевода	Фильтрация на основе механизмов машинного обучения
Грамматические и орфографические ошибки	Фильтрация на основе механизмов машинного обучения
Универсальные обращения	Фильтрация на основе механизмов машинного обучения Фильтрация на основе bag of words

Для эксперимента были выбраны следующие почтовые сервисы: Gmail, Outlook, Mail.ru и Яндекс.Почта. В каждом почтовом сервисе были созданы тестовые учетные записи, принадлежащие автору настоящего исследования, на которые отправлялись письма с фишинговыми признаками. В результате тестирования были получены результаты, приведенные в таблице 2. В таблице «+» означает, что почтовый сервис детектировал фишинговый признак для всех проведенных экспериментов; «+/-» означает, что почтовый сервис не детектировал фишинговый паттерн в 1-2 экспериментах; «-» означает, что почтовый сервис не детектировал фишинговый паттерн в 3 и более экспериментах.

В рамках эксперимента отправлялись как письма, содержащие несколько фишинговых признаков одновременно, так и письма, содержащие только один признак. Для большинства признаков было проведено несколько экспериментов с разными входными данными, например, для вредоносных вложений использовались вложения разных видов в разных форматах.

Таблица 2

Результаты детектирования фишинговых признаков в почтовых сервисах

Фишинговый признак	Gmail	Outlook	Mail.ru	Яндекс.Почта
Применение Email spoofing	+	+	+	+
Плохая репутация домена отправителя	+	+	+	+
Подозрительный адрес электронной почты	-	+	-	+
Получение письма от отправителя впервые	+	-	-	+
Адрес электронной почты был создан недавно	-	-	-	-
Получение письма от внешнего источника	+	+	+	+
Вредоносное вложение	+/-	+/-	+/-	+/-
Вредоносная ссылка	+	+	+	+
Фишинговые паттерны	-	+	-	+
Замена символов	-	+	+	-
Подозрительный HTML/CSS-код	+/-	+/-	+/-	-
Текст, сформированный с помощью языковых моделей	-	-	-	-
Текст, сформированный с помощью машинного перевода	-	-	-	-
Грамматические и орфографические ошибки	-	-	-	-
Универсальные обращения	-	-	-	-

Полученные результаты

Таким образом, в ходе проведенного исследования, было продемонстрировано, что существующие средства защиты почтовых сервисов от спама и фишинга не совершены, несмотря на широкую распространенность фишинговых атак. В ходе исследования было продемонстрировано, что разработчики встроенных средств защиты концентрируют свое внимание на детектировании ключевых фишинговых признаков (плохая репутация домена, подозрительные ссылки) и большинство таких признаков детектируются системами защиты, но, например, некоторые вредоносные вложения не блокируются средствами защиты почтовых сервисов и их удается доставить до получателя. Из очевидных соображений, детали техник, которые позволили реализовать фишинговую атаку не афишируются в рамках настоящего исследования. Большинство фишинговых признаков, являющихся вторичными по отношению к основным признаками, но присущие части фишинговых писем не детектируются встроенными средствами защиты почтовых сервисов.

Заключение

В статье рассмотрены существующие подтехники почтового фишинга, признаки, присущие фишинговым письмам, перечислены механизмы детектирования фишинговых признаков, а также проведено исследования эффективности детектирования фишинговых признаков встроенными средствами защиты наиболее популярных почтовых сервисов. Обоснованы и предложены дополнительные фишинговые подтехники, не представленные в матрице Mitre Att&ck. Были сделаны выводы, что существующие средства защиты почтовых сервисов не совершены и что, учитывая распространенность фишинговых атак в текущем ландшафте киберугроз, требуется их дальнейшее совершенствование и использование дополнительных почтовых средств защиты.

Список литературы

1. 250+ статистика фишинга: виды, стоимость и многое другое // MarketSplash [электронный ресурс]. URL: https://marketsplash.com/ru/statistika-fishingha/ (дата обращения: 11.02.2025).

2. Фишинг в России // TADVISER [электронный ресурс]. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8 (дата обращения: 11.02.2025).

3. Phishing, Technique T1566 // MITRE ATT&CK [Электронный ресурс]. URL: https://attack.mitre.org/techniques/T1566/ (дата обращения: 11.02.2025).

4. Спуфинг почтового адреса: как злоумышленники выдают себя за других // SECURELIST [Электронный ресурс]. URL: https://securelist.ru/email-spoofing-types/101688/ (дата обращения: 11.02.2025).

5. А ваш почтовый сервер на в спам-листе? Как это проверить // Дневник сисадмина [Электронный ресурс]. URL: https://sysadmin-note.ru/article/a-vash-pochtovyi-server-ne-v-spam-liste-kak-eto-proverit/ (дата обращения: 11.02.2025).

6. Если тебя не взломали, то ты не бот // Habr [Электронный ресурс]. URL: https://habr.com/ru/articles/725146/ (дата обращения: 11.02.2025).

7. Омоглифы возвращаются: киберпреступники в 11 раз чаще стали использовать подмененные буквы во вредоносных письмах // F.A.C.C.T. [Электронный ресурс]. URL: https://www.facct.ru/media-center/press-releases/homoglyphs-comeback/ (дата обращения: 11.02.2025).

8. Хакеры начали использовать WormGPT для помощи в фишинговых атаках // Habr [Электронный ресурс]. URL: https://habr.com/ru/news/748304/ (дата обращения: 11.02.2025).