Аннотация – В документе представлен анализ патента US11483343B2, который относится к системе обнаружения фишинга и способу её использования. В ходе анализа будут рассмотрены различные аспекты патента, включая его технологическую основу, новизну изобретения, потенциальные области применения, а также выделены ключевые элементы, придающие ему значимость в области кибербезопасности.

Анализ полезен специалистам по безопасности, ИТ-экспертам и заинтересованным сторонам в различных отраслях, поскольку даёт им полное представление о сути патента и его полезности для усиления мер кибербезопасности. Он служит ценным ресурсом для понимания вклада запатентованной технологии в текущие усилия по борьбе с фишингом и другими киберугрозами.

I. Введение

Патент US11483343B2 "Phishing Detection System and Method of Use" посвящён усовершенствованной системе и методологии выявления фишинговых атак и смягчения их последствий. В патенте предлагается особая архитектура системы обнаружения фишинга, которая сканирует сообщения на наличие подозрительных URL-адресов и анализирует соответствующие веб-страницы для выявления попыток фишинга.

II. Область применения

Система и метод обнаружения фишинга применимы в широком спектре отраслей, которые полагаются на цифровые коммуникации и уязвимы для фишинговых атак:

A. Технологический сектор:

- Технологические компании, особенно те, которые предоставляют программное обеспечение, облачные сервисы, платформы социальных сетей и электронную коммерцию, являются основными целями фишинговых атак с целью получения пользовательских данных и учётных данных.
- Технологический сектор выигрывает от улучшения обнаружения фишинга для защиты своих платформ, клиентов и репутации.

B. Финансовый сектор:

- Финансовые учреждения, такие как банки, инвестиционные фирмы, страховые компании и финтех-стартапы, обрабатывают конфиденциальные финансовые данные и транзакции.
- Фишинговые атаки часто выдают себя за финансовые службы для кражи учётных данных учётной записи, платёжных реквизитов и совершения мошенничества.
- Финансовый сектор остро нуждается в эффективном обнаружении фишинга для обеспечения безопасности учётных записей клиентов и соблюдения нормативных требований.

C. Сектор здравоохранения:

- Организации здравоохранения, такие как больницы, поликлиники, страховые и фармацевтические компании, хранят личную медицинскую информацию и данные о страховании / платежах.
- Фишинговые атаки могут быть направлены на кражу данных пациента, мошенничество со страховкой или нарушение работы.
- Защита от фишинга имеет решающее значение для соблюдения требований HIPAA и доверия пациентов к сектору здравоохранения.

D. Образовательный сектор:

- Образовательные учреждения, от школ до университетов, перевели многие сервисы в онлайн-режим и хранят личные и финансовые данные учащихся.
- Фишинговые атаки могут быть нацелены на студентов, преподавателей и персонал с целью кражи академических записей, личных или исследовательских данных.
- Школы и университеты нуждаются в мерах по борьбе с фишингом для защиты образовательных данных и интеллектуальной собственности.

E. Государственный сектор:

- Правительственные учреждения на федеральном, местном уровне становятся мишенью атакующих, стремящихся получить конфиденциальные данные или нарушить работу сервисов.
- Улучшенное обнаружение фишинга может помочь обезопасить системы и данные госсектора.

III. Предлагаемое решение

Патент предлагает многоступенчатую систему обнаружения фишинга, которая сканирует сообщения, разрешает встроенные URL-адреса, извлекает функции веб-страниц и применяет машинное обучение для выявления

попыток фишинга. Хотя он предлагает более упреждающий и всеобъемлющий охват, чем традиционные методы, он может столкнуться с проблемами производительности и точности в меняющемся ландшафте фишинговых атак. Тем не менее, это представляет собой значительный шаг на пути к автоматизированному обнаружению и предотвращению фишинга в режиме реального времени.

Система и метод выявляют попытки фишинга в электронных сообщениях и направлены на упреждающее обнаружение и блокирование таких вредоносных сообщений.

A. Ключевые компоненты предлагаемого решения:

Детектор фишинга: основным компонентом является модуль детектора фишинга, который анализирует сообщения на предмет подозрительного содержания. Он состоит из двух основных подкомпонентов:

- **Механизм сканирования**: сканирует текст сообщения и вложения, чтобы идентифицировать любые присутствующие URL (веб-адреса) и извлекает эти URL для дальнейшего анализа.
- **Компонент Fetcher**: принимает URL-адреса, найденные механизмом сканирования, и преобразует их в реальные веб-страницы, на которые они указывают. Извлекает исходный HTML-код этих веб-страниц.

Механизмы извлечения: затем детектор фишинга извлекает два типа функций из полученных веб-страниц:

- **Извлечение на основе URL-адресов**: анализирует структуру и компоненты самого URL-адреса, такие как длина, специальные символы, использование IP-адреса и т.д. Подозрительные шаблоны могут указывать на попытку фишинга.
- **Извлечение на основе гиперссылок**: проверяет гиперссылки, присутствующие в исходном коде веб-страницы. Проверяет целевые URL-адреса, якорный текст и другие атрибуты ссылок на наличие признаков обмана.

Модели машинного обучения:

- **Гибридный принцип**: функции URL и гиперссылки объединены в гибридный набор функций, представляющий каждую веб-страницу что даёт характеристику подозрительности страницы.
- **Модели машинного обучения**: гибридные наборы функций используются для обучения классификаторов машинного обучения различать фишинговые и легитимные веб-страницы. Модели обучаются на больших наборах данных известных фишинговых и неопасных примеров.

B. Способ применения:

- **Сканирование сообщений**: при поступлении нового сообщения механизм сканирования детектора фишинга идентифицирует все URL-адреса, присутствующие в контенте.
- **Получение содержимого URL-адресов**: компонент fetcher преобразует найденные URL-адреса в целевые веб-страницы и извлекает исходный код страницы.
- **Механизм извлечения**: функции на основе URL-адресов и гиперссылок извлекаются с каждой веб-страницы.
- **Классификация**: предварительно подготовленные модели машинного обучения применяются к извлеченному набору функций. Модели классифицируют веб-страницу как фишинговую или легитимную.
- **Реализация действия**: если веб-страница считается попыткой фишинга, исходное сообщение может быть помещено в карантин или заблокировано. Для администраторов или предполагаемого получателя могут быть сформированы предупреждения.

IV. Технологический процесс

Основной технологический процесс включает в себя механизм сканирования, извлекающий URL-адреса из сообщений, средство выборки преобразует эти URL-адреса в веб-страницы, анализирует характеристики URL-адресов и гиперссылок на этих страницах и применяет модели ML для обнаружения попыток фишинга, что приводит к автоматическому удалению фишинговых сообщений. Многоступенчатый анализ позволяет осуществлять упреждающую фильтрацию фишингового контента в режиме реального времени на основе характеристик целевой веб-страницы, выходя за рамки традиционных методов фильтрации по URL или контенту.

Технологический процесс охватывает полный жизненный цикл предлагаемого решения и фокусируется на требуемых аспектах:

A. Механизм сканирования и выборки:

- Модуль сканирования проверяет входящие сообщения, чтобы идентифицировать и извлекать любые URL-адреса, присутствующие в тексте сообщения или вложениях.
- Затем компонент fetcher преобразует извлечённые URL-адреса в реальные веб-страницы, на которые они указывают, и извлекает исходный HTML-код этих веб-страниц.

B. Обнаружение и получение содержимого URL-адресов:

- Механизм сканирования отвечает за обнаружение URL-адресов, встроенных в сообщения. Он сканирует содержимое сообщений и вложения для идентификации строк URL-адресов.
- Как только URL-адреса обнаружены, компонент fetcher преобразует их в целевые веб-страницы. Это включает в себя следующие перенаправления и

получение конечной веб-страницы, на которую в итоге указывает URL-адрес.

- Программа выборки извлекает полный исходный HTML-код разрешённой веб-страницы для дальнейшего анализа.

C. Анализ веб-страницы:

- Полученный HTML-код веб-страницы анализируется для извлечения двух типов функций:
  - **Извлечение на основе URL**: анализ самой строки URL на наличие подозрительных шаблонов, таких как длина, специальные символы, использование IP-адреса и т.д.
  - **Извлечение на основе гиперссылок**: проверка гиперссылок в источнике веб-страницы, поиск целевых URL-адресов, текста привязки и атрибутов ссылки.
- Функции URL и гиперссылки объединены в гибридный набор функций, отражающий подозрительность веб-страницы.
- К набору функций применяются предварительно подготовленные модели машинного обучения, позволяющие классифицировать веб-страницу как фишинговую или легитимную.

D. Критерии обнаружения фишинга:

- Ключевыми критериями обнаружения фишинга являются URL-адрес и гиперссылки, извлечённые из веб-страницы.
- Подозрительные шаблоны URL-адресов могут включать чрезмерную длину, случайные символьные строки, IP-адреса, средства сокращения URL-адресов и т.д.
- Признаки гиперссылки, такие как несоответствие целевых URL-адресов, подозрительный якорный текст или ссылки на известные вредоносные сайты, могут указывать на фишинг.
- Модели машинного обучения совершенствуются на наборах данных известных фишинговых и законных веб-страниц для изучения отличительных паттернов.
- Веб-страница классифицируется как фишинговая, если модель определяет, что её URL-адрес и характеристики гиперссылок соответствуют изученным шаблонам вредоносных страниц.

E. Удаление сообщения:

- Если веб-страница, ссылка на которую содержится в сообщении, будет признана попыткой фишинга, исходное сообщение может быть помещено в карантин или удалено автоматически.
- Это предотвращает взаимодействие пользователя с вредоносным контентом и потенциальную компрометацию его информации.
- Удаление сообщения может произойти сразу после определения факта фишинга, до того, как сообщение попадёт во входящие пользователя.
- В качестве альтернативы подозрительные сообщения могут быть помечены для проверки перед удалением на случай потенциальных ложных срабатываний.

V. Преимущества, недостатки и значимость предлагаемого решения

A. Преимущества

Ключевыми преимуществами этой системы обнаружения фишинга являются её способность автоматически удалять фишинговые сообщения, избегать использования потенциально устаревших внешних чёрных списков, повышать точность обнаружения за счёт машинного обучения, предотвращать фишинг в режиме реального времени до того, как сообщения попадут в почтовые ящики, и интеграция с существующей инфраструктурой электронной почты для многоуровневой защиты. Эти возможности представляют собой значительный прогресс по сравнению с традиционными методами предотвращения фишинга.

1) Автоматическое удаление сообщений о фишинге:

- Если веб-страница, ссылка на которую содержится в сообщении, будет признана попыткой фишинга, исходное сообщение может быть автоматически помещено в карантин или удалено
- Это предотвращает взаимодействие пользователя с вредоносным контентом и потенциальную компрометацию его информации
- Удаление сообщения может произойти сразу после определения факта фишинга, до того, как сообщение попадёт во входящие пользователя

2) Снижение зависимости от внешних чёрных списков:

- Система позволяет избежать зависимости от внешних чёрных списков или баз данных, которые могут устареть
- Используются только функции на основе URL-адресов и гиперссылок, извлечённые из самого исходного кода веб-страницы, не полагаясь на сторонние сервисы
- Это позволяет ему обнаруживать новые и развивающиеся попытки фишинга, которые, возможно, ещё не внесены в чёрные списки

3) Повышена точность обнаружения фишинга:

- Объединение анализа URL-адресов и гиперссылок обеспечивает более полный охват и точность по сравнению с традиционными методами
- Модели машинного обучения совершенствуются на больших наборах данных известных примеров фишинга и вредоносных программ для изучения отличительных паттернов

- Это обеспечивает гибкую автоматизированную классификацию и снижает количество ложноположительных результатов по сравнению с подходами, основанными на правилах

4) Предотвращение фишинга в режиме реального времени:

- Система обнаруживает фишинг, анализируя целевые веб-страницы, а не только содержимое сообщений
- URL-адреса разрешаются, а веб-страницы анализируются в режиме реального времени по мере поступления сообщений
- Это позволяет блокировать попытки фишинга до того, как они попадут в почтовый ящик пользователя, предотвращая взаимодействие с вредоносным контентом

5) Интеграция с агентами передачи почты или клиентским программным обеспечением:

- Система обнаружения фишинга может быть интегрирована в агенты передачи почты (MTAS) или программное обеспечение почтового клиента
- Интеграция с MTA позволяет сканировать и блокировать фишинговые сообщения в процессе доставки электронной почты
- Интеграция с почтовыми клиентами обеспечивает защиту последней мили на уровне устройства пользователя
- Это обеспечивает многоуровневую защиту как на сервере, так и на конечной точке

B. Ограничения

Несмотря на то, что система предлагает улучшения по сравнению с традиционными методами, она по-прежнему сталкивается с проблемами с точки зрения вычислительной эффективности, адаптируемости к новым угрозам, компромиссов в отношении точности, зависимости от внешних факторов, языкового охвата и поведения пользователя. Устранение этих ограничений будет ключом к обеспечению надёжной защиты от фишинга в режиме реального времени перед лицом постоянно развивающихся атак..

1) Вычислительные затраты и масштабируемость:

- Разрешение URL-адресов и масштабный анализ веб-страниц могут быть дорогостоящими с точки зрения вычислений
- Системе необходимо обрабатывать большой объем сообщений и URL-адресов, что может повлиять на производительность и масштабируемость
- Возможные задержки в доставке сообщений из-за процесса сканирования могут повлиять на работу пользователя

2) Постоянная гонка вооружений:

- Атакующие постоянно совершенствуют свои методы, чтобы избежать обнаружения, что приводит к продолжающейся гонке вооружений
- Системе может быть трудно справляться с новыми моделями фишинга и атаками нулевого дня
- Злоумышленники могут найти способы скрыть фишинговый контент или имитировать безопасные страницы, чтобы обойти обнаружение

3) Обработка ложноположительных и отрицательных результатов:

- Система может выдавать ложноположительные результаты, ошибочно помечая законные сообщения как фишинговые
- Ложноотрицательные сообщения, при которых попытки фишинга остаются незамеченными, также представляют опасность
- Балансировка точности и минимизация ложноположительных / отрицательных результатов является сложной задачей и влияет на доверие пользователей

4) Зависимость от внешних источников данных:

- Система использует данные сторонних производителей, такие как записи WHOIS, PageRank и т.д. для анализа веб-страниц
- Изменения или сбои в работе этих внешних источников данных могут повлиять на точность и надёжность системы

5) Язык и интернационализация:

- Попытки фишинга на разных языках или в определённых регионах может быть сложнее обнаружить
- Системе может потребоваться адаптация и обучение для обеспечения многоязычного и международного охвата

6) Поведение пользователей и социальная инженерия:

- Ни одно техническое решение не может полностью уберечь пользователей от хорошо продуманных попыток социальной инженерии
- Любопытство, рассеянность или недостаточная осторожность пользователя могут привести к переходам по фишинговым ссылкам, несмотря на предупреждения
- Непрерывное обучение и осведомлённость пользователей по-прежнему необходимы в дополнение к любой технической системе обнаружения

7) Потенциальные проблемы с конфиденциальностью:

- Анализ сообщений пользователей и активности в Интернете на предмет обнаружения фишинга может вызвать вопросы конфиденциальности

- Необходимо учитывать баланс между конфиденциальностью пользователей и эффективным обнаружением угроз

8) Опережать возникающие угрозы:

- По мере развития фишинговых тактик система обнаружения нуждается в постоянном обновлении и переподготовке
- Адаптация к новым моделям фишинга и векторам атак требует постоянных усилий и ресурсов

C. Значимость

Ключевым значением системы обнаружения фишинга является её способность повышать точность обнаружения с помощью машинного обучения, предотвращать фишинг в режиме реального времени до того, как сообщения попадут в почтовые ящики, автоматическое удаление фишинговых сообщений, избегание использования устаревших чёрных списков и интеграции с существующей инфраструктурой электронной почты для комплексной многоуровневой защиты. Эти возможности представляют собой значительный прогресс по сравнению с традиционными методами предотвращения фишинга в продолжающейся борьбе со все более изощренными фишинговыми атаками.

1) Повышение точность обнаружения фишинга:

- Объединение анализа URL-адресов и гиперссылок обеспечивает более полный охват и точность по сравнению с традиционными методами
- Модели машинного обучения совершенствуются на больших наборах данных известных примеров фишинга и вредоносных программ для изучения отличительных паттернов, что обеспечивает адаптируемую автоматическую классификацию и сокращает количество ложных срабатываний

2) Предотвращение фишинга в режиме реального времени:

- Система активно обнаруживает фишинг, анализируя веб-страницы назначения, а не только содержимое сообщений, в режиме реального времени по мере поступления сообщений
- Это позволяет блокировать попытки фишинга до того, как они попадут в почтовые ящики пользователей, предотвращая взаимодействие с вредоносным контентом

3) Автоматическое удаление сообщений:

- Если веб-страница, ссылка на которую содержится в сообщении, будет признана попыткой фишинга, исходное сообщение может быть автоматически помещено в карантин или удалено до того, как оно попадёт в почтовый ящик пользователя
- Это предотвращает взаимодействие пользователей с вредоносным контентом и потенциальную компрометацию их информации

4) Снижение зависимости от внешних чёрных списков:

- Система позволяет избежать зависимости от потенциально устаревших внешних чёрных списков, используя только функции URL и гиперссылок, извлечённые из самого исходного кода веб-страницы
- Это позволяет ему обнаруживать новые и развивающиеся попытки фишинга, которые, возможно, ещё не внесены в чёрные списки

5) Интеграция с инфраструктурой электронной почты:

- Система обнаружения фишинга может быть интегрирована в агенты передачи почты или программное обеспечение почтового клиента для сканирования на стороне сервера или защиты конечных точек последней мили
- Это обеспечивает многоуровневую защиту как на уровне доставки электронной почты, так и на уровне пользовательского устройства