Фанг Дук Ан Туан, курсант,
Краснодарское высшее военное училище

Научный руководитель:
Сидельников Олег Васильевич, преподаватель,
Краснодарское высшее военное училище

ЭВОЛЮЦИЯ ТЕХНИК И ТАКТИК ФИШИНГОВОЙ АТАКИ

Аннотация. В настоящее время фишинговые атаки постепенно трансформировались из простых мошеннических писем по электронной почте в сложные высокотехнологичные кампании. В данной статье анализируются ключевые техники и тактики фишинга: от манипуляций с протоколами передачи данных и адресами ресурсов до использования технологий искусственного интеллекта (ИИ) для создания дипфейков (поддельных аудио- и видеоматериалов). На основе анализа таких технологий, как голосовой фишинг (вишинг) и текстовый фишинг (смишинг), предлагаются меры противодействия фишинговой атаке.

Ключевые слова: Фишинговая атака, техника фишинговой атаки, дипфейк, тактика фишинговой атаки, меры противодействия фишинговой атаке, вишинг, смишинг.

Фишинг (phishing) – это вид интернет-мошенничества, цель которого – кража конфиденциальных данных (паролей, номеров карт) через поддельные письма, сайты или сообщения, имитирующие известные бренды, банки или госорганы. Это метод социальной инженерии, заставляющий пользователей добровольно раскрыть личную информацию. Фишинг давно перестал быть новым понятием в сфере информационной безопасности, однако методы его реализации постоянно совершенствуются для преодоления существующих систем киберзащиты. На основе результатов исследований, проведенных специалистами «Лаборатории Касперского» и Сбербанка, атаки нацелены не только на кражу учетных данных, но и распространяются на мошенничество под видом оплаты государственных услуг (жилищно-коммунальное хозяйство), а также на глубокое проникновение в корпоративные сети [1-3].

Техники фишинговых атак

Основа фишинга базируется на создании технических компонентов:

- Манипуляции с адресами ресурсов и доменными именами: использование техники typosquatting (регистрация доменных имен, визуально схожих с оригинальными) или технического протокола Punycode (данный протокол применяется для преобразования символов Unicode в последовательность символов американского стандартного кода (ASCII) для обмена информацией, которая включает в себя только латинские буквы, цифры и дефисы). Это позволяет создавать символы, внешне практически идентичные латинице, что крайне затрудняет распознавание поддельного веб-сайта для пользователя.
- Техника подмены электронной почты (Email Spoofing): фальсификация данных протокола и заголовков электронного сообщения, позволяющая нарушители изменять поле отправителя («From») в заголовке простого протокола передачи почты (SMTP). Данная техника подмены создает иллюзию того, что электронное письмо было отправлено от лица авторитетной организации или администратора системы.
- Атаки через современные каналы связи: смещение фокуса с электронной почты на приложения для обмена мгновенными сообщениями (Telegram, WhatsApp) и социальные сети. В данном случае нарушители используют сокращенные ссылки и вредоносные вложения для получения несанкционированного доступа и захвата контроля над учетными записями пользователей.

Тактики фишинговых атак:

Одной из разновидностей тактик фишинговых атак является **голосовой фишинг (вишинг)**. Вишинг представляет собой значительный шаг вперед в области интеграции телекоммуникационных технологий и психологических методов воздействия:

- Подмена идентификатора вызывающего абонента, когда нарушители используют протокол передачи голоса через интернет (Voice over Internet Protocol – VoIP) для фальсификации номеров телефонов банковских учреждений или государственных органов.
- Сценарии манипулирования (скрипты): использование фактора ограниченного времени или угроз блокировки банковских счетов для принуждения жертвы к передаче одноразовых паролей или конфиденциальной информации о банковских картах [1,4].

Другая тактика фишинговых атак – это **текстовый фишинг (смишинг)**. Если традиционный фишинг обычно осуществляется через электронную почту, то текстовый фишинг атакует непосредственно через службу коротких сообщений. Нарушители обычно отправляют сообщение с крайне срочным или заманчивым содержанием, чтобы побудить пользователя к немедленному действию:

- Использование вредоносных ссылок. Направление пользователя на поддельный веб-сайт (визуально идентичный официальному сайту банка или сервису оплаты государственных услуг) для кражи данных учетной записи или одноразовых паролей. *Например, банковское уведомление: «Ваш счет заблокирован, войдите по ссылке [ссылка] для разблокировки».*
- Запрос на установку программного обеспечения: чаще всего это файлы формата расширения пакета приложения Андроид (Android Package Kit), содержащие вредоносный код для перехвата сообщений и захвата контроля над устройством.
- Использование подменных номеров отправителя: применение техники фальсификации имени отправителя текстового сообщения или использование номеров телефонов, выглядящих официально, для формирования доверия со стороны жертвы.

Почему текстовый фишинг (смишинг) является более опасным, чем традиционный фишинг?

- Отсутствие фильтров безопасности: в отличие от корпоративных систем электронной почты, оснащенных межсетевыми экранами и сложными алгоритмами фильтрации, стандартные приложения для обмена сообщениями на мобильных телефонах обычно обладают меньшими возможностями для автоматической блокировки вредоносных ссылок.
- Проверка мобильного интерфейса: на небольшом экране мобильного устройства пользователю гораздо сложнее проверить полный адрес ресурса (URL) или сертификат безопасности веб-сайта, чем при использовании персонального компьютера.

Применение ИИ для создания дипфейков: новый этап развития фишинга

Дипфейк (Deepfake) – это технология, использующая ИИ, особенно методы глубокого обучения (deep learning), для создания поддельного аудиовизуального контента с высокой степенью реалистичности, что затрудняет зрителям отличие подделки от реальности [5]. Современной вершиной фишинговых атак является использование ИИ для создания контента типа «дипфейк»:

- дипфейк аудио: на основе короткого образца речи искусственный интеллект способен синтезировать голос руководителя компании или родственника для совершения мошеннических звонков в рамках голосового фишинга.
- Видеоизображение с использованием технологии дипфейк: в ходе онлайн-конференций нарушители могут использовать подмену лиц в режиме реального времени для обмана сотрудников с целью совершения денежных переводов или иных противоправных действий.

- Использование искусственного интеллекта для генерации контента: технологии позволяют нарушителей создавать фишинговые письма без грамматических и орфографических ошибок, обеспечивая высокую степень персонализации и многоязычность. Это позволяет успешно обходить простые спам-фильтры, работающие на основе анализа ключевых слов.

Меры противодействия фишинговым атакам:

Для противодействия современным изощренным методам фишинга необходимо внедрение комплексных организационных и технических мер:

- Внедрение протоколов аутентификации электронной почты, таких как инфраструктура политики отправителя (Sender Policy Framework): при получении электронного сообщения сервер получателя проверяет, входит ли адрес межсетевого протокола (IP-адрес) отправителя в список разрешенных. В случае отсутствия адреса в списке письмо классифицируется как подозрительное. Также рекомендуется использование метода идентификации почты по доменным ключам (DomainKeys Identified Mail), который гарантирует неизменность содержания письма и подтверждает подлинность отправителя в процессе передачи данных.
- Применение многофакторной аутентификации (Multi-Factor Authentication), не основанной на использовании служб коротких сообщений: использование специализированных приложений для генерации кодов, таких как Google Authenticator или Microsoft Authenticator, а также аппаратных ключей защиты (YubiKey). В случае перехвата нарушителей текстового сообщения в рамках смишинг-атаки, он не сможет получить доступ к аккаунту без кода из приложения или физического ключа.
- Использование программного обеспечения для блокировки нежелательных вызовов и сообщений: установка приложений с актуальными базами данных мошеннических телефонных номеров, а также использование стандартных функций фильтрации спама в операционных системах Android и IOS.
- Проверка адресов ресурсов (Uniform Resource Locator): при необходимости перехода по ссылке следует внимательно изучать доменное имя. Необходимо проявлять бдительность в отношении доменов, использующих технический протокол Punycode или содержащих орфографические ошибки (например, sber-bank.ru вместо официального sberbank.ru).

Вывод: Фишинговые атаки трансформировались из простых методов фальсификации протоколов передачи данных в сложные операции с применением таких передовых технологий, как искусственный интеллект и дипфейки. Успех фишинга обусловлен не только техническим совершенством, но и эксплуатацией самого слабого звена в системе обеспечения безопасности – человеческого фактора. Сочетание современных технических средств фильтрации и блокировки с повышением уровня осведомленности общества является единственным ключом к минимизации рисков, исходящих от данных угроз в современных условиях.

Список литературы:

1. Касперский, Евгений Валентинович. Что такое вишинг: анализ схем атак и методы защиты / Евгений Валентинович Касперский. – Текст : электронный // Энциклопедия «Лаборатории Касперского». – 2024. – URL: https://encyclopedia.kaspersky.ru/glossary/vishing/.

2. Сбербанк России. Кибрарий: библиотека знаний по кибербезопасности. Фишинг в социальных сетях и мессенджерах. – Текст : электронный // Официальный сайт Сбербанка. – 2024. – URL: https://www.sberbank.ru/ru/person/kibrary/articles/fishing-v-socialnykh-setyakh-i-messendzherakh.

3. СберБизнес Live. Что такое фишинг и как бизнесу защищаться от интернет-угроз. – Москва : Издательство Сбербанка, 2024. – Текст : электронный. – URL: https://sberbusiness.live/publications/chto-takoe-fishing-i-kak-biznesu-zashchishchatsya-ot-internet-ugroz.

4. Малуэрбайтс. Основы кибербезопасности: что такое вишинг и как не стать жертвой мошенников. – Текст : электронный // Malwarebytes. – 2024. – URL: https://www.malwarebytes.com/ru/cybersecurity/basics/vishing.

5. iProov. Как дипфейки угрожают системам удаленной проверки личности / iProov. – Текст : электронный // iProov Blog. – 2024. – URL: https://www.iproov.com/vi/blog/deepfakes-threaten-remote-identity-verification-systems/.