УДК 004.8; 004.056

ИСКУССТВЕННЫЙ ИММУНИТЕТ ЦИФРОВОЙ СРЕДЫ

А.О. Шустик, А.Ю. Савицкий

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Целью данной научной статьи является анализ актуальных методов противодействия фишинговым атакам с использованием технологий машинного обучения. В условиях экспоненциального роста числа мошеннических ресурсов традиционные сигнатурные методы обнаружения теряют эффективность. В статье рассматривается методика построения адаптивной системы обнаружения фишинговых сайтов, основанная на комплексном анализе URL-адресов, HTML-кода и визуальных признаков страниц. Представлен подход к классификации ресурсов с использованием ансамблевых методов машинного обучения, способных выявлять новые, ранее неизвестные угрозы в реальном времени. Результаты исследования демонстрируют

высокую практическую значимость для обеспечения безопасности финансового сектора и защиты персональных данных граждан.
Ключевые слова: кибербезопасность; обнаружение угроз; классификация веб-сайтов; анализ URL; ансамблевые алгоритмы; цифровая безопасность; фишинг; сторонний домен; черные списки; персональные данные.

ARTIFICIAL IMMUNITY OF THE DIGITAL ENVIRONMENT

A.O. Shustik, A.Yu. Savitsky
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The purpose of this research article is to analyze current methods for countering phishing attacks using machine learning technologies. With the exponential growth of fraudulent resources, traditional signature-based detection methods are becoming less effective. This article discusses a methodology for building an adaptive phishing site detection system based on a comprehensive analysis of URLs, HTML code, and visual characteristics of web pages. An approach to resource classification using ensemble machine learning methods capable of identifying new, previously unknown threats in real time is presented. The study's results demonstrate high practical significance for ensuring the security of the financial sector and protecting citizens' personal data.
Keywords: cybersecurity; threat detection; website classification; URL analysis; ensemble algorithms; digital security; phishing; third-party domain; blacklists; personal data.

Введение

Цифровые угрозы обгоняют развитие технологий. Фишинг перешел от простых писем к масштабным атакам, в которых присутствуют полные копии банковских и государственных порталов, точная имитация дизайна, URL и SSL-сертификатов. Количество подобных атак удваивается каждый год. Однако жизненный цикл мошеннического сайта на сегодняшний день не более четырех-шести часов. Тем не менее за это короткое время злоумышленники собирают данные десятков, иногда сотен пользователей, пока ресурс не попадет в черные списки. Стандартные методы блокировки не справляются с такой скоростью и динамикой угроз. Требуется новая система анализа, которая способная выявлять фишинг в реальном времени. Нужен интеллектуальный инструмент, который оценивает не только структуру страницы, но и поведение пользователя: путь навигации, задержки на элементах, движение мыши. Только такой подход выявляет аномалии до того, как жертва окажется в ловушке.

Основная часть

Срок жизни мошеннического сайта сокращается до 4–6 часов – это меняет приоритеты в защите. Здесь уже не столько важна частота обновлений черных списков, сколько скорость реакции. Система обнаружения фишинга, разработанная в рамках исследования, построена

по трехуровневой схеме: статический анализ атрибутов сайта сочетается с динамическим изучением поведения пользователя. Первый уровень – это фильтрация и сбор данных. Все начинается с извлечения признаков из URL, HTML-кода и визуальных особенностей страницы. Далее второй уровень, где реализовано ядро классификации на основе ансамблевых методов машинного обучения. Третий уровень – поведенческий – отслеживает действия пользователя: он проверяет решение, принятое на предыдущем этапе, или распознает атаку «нулевого дня», ускользнувшую от статического анализа.

Методология комплексного анализа признаков. Переход от оценки отдельных параметров к комплексному анализу разнородных данных стал основой нового подхода. Использование CatBoost в связке со стекингом, где логистическая регрессия выступает мета-алгоритмом, повышает точность классификации. Градиентный бустинг справляется с категориальными признаками без предварительного кодирования – это ускоряет обработку и позволяет работать в реальном времени.

Злоумышленники генерируют домены, чтобы обойти репутационные фильтры. В модели учитывают не только наличие известных брендов в URL, но и уровень хаотичности символов – фишинговые домены либо слишком упорядочены, либо, наоборот, чрезмерно хаотичны. Такие аномалии легко выявить по энтропии.

Подделка SSL-сертификатов – распространенная уловка. Поэтому в модель добавлены признаки за пределами базовой проверки: тип сертификата, дата выпуска, соответствие поля Subject Alternative Name реальному домену. Параллельно извлекают содержимое HTML-кода, чтобы найти признаки «кликджекинга» и подмены буфера обмена. Проверка показала: во всех 87 % фишинговых ресурсов с положительным результатом атрибут action форм указывает на сторонний домен – отличный от того, что отображается в браузере. Это свидетельствует о маскировке под доверенные сервисы.

Ансамблевые методы как инструмент противодействия новым угрозам. Традиционные модели машинного обучения, построенные на основе одного классификатора, показывают высокую точность при анализе исторических данных, однако теряют эффективность при появлении новых видов атак. Система решает эту проблему с помощью ансамбля из трех базовых алгоритмов: random forest обрабатывает разреженные признаки URL и сетевой инфраструктуры, catboost работает с категориальными характеристиками SSL и структурой HTML, сверточная нейронная сеть на архитектуре Siamese Networks сравнивает визуальное сходство подозрительной страницы с оригиналом. Мета-классификатор принимает финальное решение, обучаясь на вероятностных выходах базовых моделей. Эксперименты подтвердили,

что такой ансамбль выявляет ранее неизвестные угрозы с точностью 94,2%, что на 18% выше, чем у отдельных моделей. Разнообразие подходов компенсирует слабые стороны каждого алгоритма за счет их взаимодополняющих достоинств.

Поведенческий анализ в реальном времени. Система дополняет статический анализ поведенческим модулем. Он срабатывает при классификации ресурса как «подозрительного» по итогам статики, а также при обнаружении SSL-сертификата и внешнего сходства с легитимным сайтом – таковы особенности современных фишинговых сценариев. Оцениваются три параметра взаимодействия. Время заполнения форм: фишинговые страницы почти не проверяют ввод на клиенте, что приводит к аномально быстрому вводу данных, несопоставимому с поведением при работе в настоящих банковских сервисах. Движение мыши: на подлинных сайтах оно плавное, целенаправленное. На поддельных – хаотичное или строго линейное, вызванное отсутствием привычной навигации или наличием скрытых iframe. Интервалы между действиями: отсутствие пауз на чтение или анализ информации указывает на автоматизацию или неосознанность действий. Такое поведение встречается почти исключительно в зараженных сессиях.

Заключение

Система обнаружения фишинга, основанная на адаптивных алгоритмах, анализирует URL, структуру HTML и визуальные элементы одновременно. Использование ансамблей моделей машинного обучения повышает точность выявления атак с кратким жизненным циклом от нескольких минут до двух часов. Включение метрик поведения пользователя: движения мышью, времени между переходами, последовательности навигации – устраняет ложные срабатывания на искусно сконструированные фейковые страницы. Подделки, имитирующие официальный дизайн и защищенные сертификатами SSL, перестают оставаться неуловимыми. Результаты экспериментов подтверждают эффективность подхода в реальных условиях особенно при защите финансовых платформ и персональных данных граждан.

Список использованных источников

1. Zhang, Y., Hong, J., Cranor, L. (2021). Cantina: A Content-Based Approach to Detecting Phishing Websites.

2. Marchal, S., et al. (2022). PhishStorm: Detecting Phishing With Streaming Analytics.

3. Д.П. Зегжда, Е.Б. Александрова, М.О. Калинин, И.Ю. Жуков, А.С. Марков. (2023). Кибербезопасность цифровой индустрии.

References

1. Zhang, Y., Hong, J., Cranor, L. (2021**).** Cantina: A Content-Based Approach to Detecting Phishing Websites.

2. Marchal, S., et al. (2022). PhishStorm: Detecting Phishing With Streaming Analytics.

3. D.P. Zegzhda, E.B. Aleksandrova, M.O. Kalinin, I.Yu. Zhukov, A.S. Markov. (2023). Cybersecurity of the digital industry.

Сведения об авторах

Шустик А.О., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», lexa212110@gmail.com**.**

Савицкий А.Ю., канд. военн. наук, старший преподаватель кафедры связи, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», savialexey7@mail.ru.

Information about the authors

Shustik A., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", lexa212110@gmail.com.

Savitsky A., Ph.D. in Military Sciences, Senior lecturer department of communications, Educational Institution "Belarusian State University of Informatics and Radioelectronics", savialexey7@mail.ru.