DOI 10.37882/2223-2966.2024.4-2.26

МОДЕЛИРОВАНИЕ ПРИЗНАКОВ И ВЕСОВ ДЛЯ ПОСТРОЕНИЯ ДОСТУПНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ АТАК НА РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ, ОСНОВАННЫХ НА МЕТОДАХ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Наумова Ксения Денисовна
Национальный исследовательский ядерный университет МИФИ (Москва)
naumovaxe@mail.ru
Радыгин Виктор Юрьевич
к.т.н., доцент, Национальный исследовательский ядерный университет МИФИ (Москва)
VYRadygin@mephi.ru

Аннотация. С увеличением числа кибератак в цифровом пространстве растет потребность в качественной защите не только компаний, но и отдельных пользователей. Однако на текущий момент гражданам РФ доступен достаточно узкий ряд решений, большинство из которых не может выявлять и предотвращать атаки, основанные на методах социальной инженерии. Проведённый в данной работе обзор существующих инструментов (расширений для браузера) показал их неэффективность, использование устаревших технологий для обнаружения и предотвращения данного вида атак. Таким образом, работа посвящена формированию признакового пространства для доступного для всех использующих интернет граждан РФ программного решения для обнаружения и предотвращения атак, основанных на методах социальной инженерии.

Ключевые слова: социальная инженерия, кибератака, инструменты защиты от кибератак, браузер, расширение для браузера.

MODELING OF FEATURES AND THEIR WEIGHTS FOR AN ACCESSIBLE SYSTEM FOR DETECTING AND PREVENTING ATTACKS BASED ON SOCIAL ENGINEERING METHODS AIMED AT INTERNET USERS AND RELEVANT TO THE CURRENT SITUATION IN THE RUSSIAN FEDERATION

K. Naumova
V. Radygin

Summary. With the increasing number of cyber attacks in the digital space, there is a growing need for high-quality protection not only for companies, but also for individual users. However, at the moment, citizens of the Russian Federation have access to a fairly narrow range of solutions, most of which cannot detect and prevent attacks based on social engineering methods. The review of existing tools (browser extensions) carried out in this paper showed their inefficiency, the use of outdated technologies to detect and prevent this type of attack. Thus, the work is devoted to the formation of a feature space for a software solution for detecting and preventing attacks based on social engineering methods that is accessible to all citizens of the Russian Federation using the Internet.

Keywords: social engineering, cyber attack, cyber attack protection tools, browser, browser extension.

Введение

Возможность выхода ежедневно растущего количества пользователей в сеть влечет за собой спрос на удобство и качество разрабатываемых информационных технологий (ИТ), их стабильность и безопасность. В рамках безопасности ИТ можно использовать различные подходы к реагированию на атаки, основанные на методах социальной инженерии. Примером таких подходов являются инструменты, направленные на выявление и предотвращение атак. На мировом рынке ИТ существует множество широко известных решений антивирусной защиты, систем обнаружения вторжений и реагирования на них, но далеко не все сейчас доступны и могут использоваться на территории РФ. Среди функционирующих решений на сегодняшний день на отечественном рынке большинство направлены на защиту именно компаний. Для отдельных пользователей представлен узкий ряд инструментов, не обеспечивающих полную защиту [1].

Целью работы является моделирование признаков и их весов для доступной системы обнаружения и предотвращения атак, основанных на методах социальной инженерии, направленных на пользователей в Интернете и актуальных для современной ситуации в РФ.

1. Обзор существующих инструментов-расширений для обнаружения и предотвращения атак, основанных на методах социальной инженерии

Сегодня для доступа к веб-сайтам пользователи наиболее часто используют в качестве приложения веб-

браузер. В настоящее время самым популярным браузером в мире является Google Chrome с долей мирового рынка 65 % на всех устройствах. Доля российских пользователей, использующих указанный браузер, составляет 42 % на момент мая 2023 года [2]. Следующими по популярности в РФ являются браузеры «Яндекс» и «Safari».

Непосредственно сами браузеры не содержат встроенных механизмов защиты от атак социальной инженерии. Тем не менее допускается модификация функционала веб-браузера программными модуль в формате расширения для браузера [3]. Функционал расширений может включать: модификации пользовательского интерфейса, управление файлами cookie, блокировку рекламы, также настраиваемые сценарии и стили вебстраниц и т.д. Популярность механизма расширений (в Google Chrome их доступно порядка 200 000 [4]) и их использование ведущими ИБ-компаниями позволяет говорить о возможности построения системы защиты от атак социальной инженерии на данном принципе.

В работе [1] авторами предложена классификация, отражающая современные паттерны последовательности возможных атак, основанных на методах социальной инженерии. Среди ресурсов воздействия присутствуют целевые, подробно рассмотренные в работах [5–7], и нецелевые интернет-ресурсы, которые в свою очередь ведут за собой методы использования невербального психологического массового и целевого манипулирования пользователями в виде текстовых сообщений и визуального представления. Основным инструментом воздействия у этих ресурсов является интернет-адрес. О данном инструменте взаимодействия неоднократно упоминают авторы исследований [7–10]. В работе [1] выделен сценарий атак злоумышленника, основанных на методах социальной инженерии, для защиты от которых в настоящий момент может быть использовано решение, построенное, как расширение для браузера.

Анализ инструментов-расширений для Chrome-подобных браузеров доступных в интернет-магазине расширений Chrome усложнен отсутствует сортировки по количеству скачиваний расширения и специальным разделам с расширениями, связанными с защитой пользователя, что потребовала проведения их ручного исследования. В результате выявлено около 100 существующих расширений для проверки веб-сайтов и обнаружения фишинговых атак. Часть расширений устарела, разработчики обновляли их в интернет-магазине более трех лет назад, а около половины всех найденных расширений были скачаны менее 500 раз. Оставшиеся — составляют около 10 % всех инструментов, их разработчики крупные ИБ-компании, предоставляющие платные многофункциональные инструменты для защиты предприятий и организаций.

Авторами был выполнен детальный анализ каждого из выбранных 10 наиболее релевантных расширений, в том числе по количеству скачиваний пользователей, стране разработчика, дате последнего обновления в интернет-магазине, поддерживаемым языкам, версии или нескольким версиям «манифеста», по содержимому, а именно обфускации кода (если имеется), обнаруженным про анализе методам проверки веб-сайтов и URI-адресов и результату проверки детектирования расширением актуальных действующих фишинговых ресурсов, в том числе направленных на российского пользователя, в формате реального времени.

В результате проведенного анализа расширений сделано несколько выводов. Среди основных 10 компаний-разработчиков расширений 4 находятся в США, у 7 из 10 выбранных расширений есть поддержка русского языка, а российской из представленных компаний является только одна, занимающая в общем списке 5 место. Данной решение загружено чуть более чем у 100 000 пользователей. Далеко не каждая из компаний занимается регулярным обновлением своего расширения, в силу незаинтересованности в актуализации бесплатного продукта для пользователей, а значит такие расширения не могут эффективно обнаруживать атаки, с использованием методов социальной инженерии, в том числе новых фишинговых атак. Дополнительно, данный факт подтверждает наличие в открытом исходном коде некоторых расширений комментариев разработчиков, не предназначенных для чтения пользователям.

В процессе изучения программного кода расширений (скриптов) выявлено, что большинство содержат обфускацию для более сложного детального изучения открытого исходного кода с целью сохранить методы проверки веб-ресурсов от конкурентов. Среди обнаруженных методов проверки URI-адресов и веб-сайтов выделены: черный и белый списки, категории ресурсов, внедрение ChatGPT и некоторые другие частные признаки. Проверка по черному списку является самой неэффективной, поскольку такие списки быстро устаревают, а значит быстро теряют актуальность в обнаружении новых угроз. В то же время белые списки могут быть полезны для более быстрого «отсеивания» чистых ресурсов для вычислительной производительности обработки данных. Категории ресурсов не являются важным признаком для определения чистоты или вредоносности ресурса. Внедрение ChatGPT является хорошим методом, однако ИИ не имеет возможности получать доступ к веб-сайтам, а также из-за малого количества данных и сложности обфускации неизвестна основная роль данного ИИ в расширении.

Стоит отметить, что помимо выявленных методов на локальных серверах некоторых расширений могут использоваться дополнительные признаки для более

качественной обработки запроса, однако при проверке обнаружения пяти различных фишинговых российских веб-сайтов в формате реального времени только 3 расширения смогли обнаружить хотя бы одну угрозу.

Итогом обзора является подтверждение гипотезы об отсутствии доступного браузерного инструмента, способного обнаружить и предотвратить атаки, основанные на методах социальной инженерии, направленных на российских пользователей в сети Интернет.

2. Построение признакового пространства для разработки системы обнаружения и предотвращения атак социальной инженерии

На основании проведенного обзора исследований [5–13] об атаках, основанных на методах социальной инженерии, выделены следующие 10 признаков (включающих обобщенные и более точные), наличие которых позволяет классифицировать проверяемый веб-сайт как чистый или опасный для пользователя:

1. проверка по белым спискам — позволяет исключить известные легитимные ресурсы, для того чтобы не тратить время их проверки по другим признакам;
2. проверка даты регистрации домена — чем свежее доменное имя, тем более подозрительным является веб-сайт, расположенный на нем;
3. проверка инструментом whois внутренних полей — если внутри встречается автоматически сгенерированная пометка «REDACTED FOR PRIVACY», это является подозрительным признаком;
4. проверка доменной зоны (или зоны первого уровня) — в популярных зонах (например,: com, ru, org, net) встречается больше легитимных ресурсов, а соответственно больше доверия, чем к таким зонам как cyou, online, biz, xyz, в том числе из-за их более дешевой стоимости и возможными быть приобретенными большим числом пользователей;
5. проверка длины доменного имени и содержания в нем необычных последовательностей букв и цифр, несвойственных для легитимных ресурсов;
6. проверка кода (статуса), заголовков и длины тела ответа от сервера ресурса — при получении кодов ответов, отличных от часто встречающихся 200 («запрос успешно обработан»), 301 («перемещен на постоянной основе»), 302 («найден, но временно изменен»), а также при наличии заголовков перенаправления на другой веб-сайт и длины ответа, меньшей 100, высокий уровень подозрительности;
7. проверка популярности ресурса — поиск информации в Google Chrome и подсчет числа полученных результатов — чем меньше нашлось информации, тем подозрительнее ресурс;
8. Проверка DNS-записи MX, предназначенный для маршрутизации электронной почты с использованием протокола SMTP — ее отсутствие является подозрительным, поскольку большинство легитимных ресурсов добавляют данную запись;
9. проверка DNS-записи NS, предназначенной для связи адресов DNS-серверов, обслуживающих домен — если публичным DNS-сервером выступает cloudflare, publicdnsservice и другие популярные у атакующих дешевые сервера, то это считается подозрительным признаком;
10. проверка IP-адресов — подозрительно, если при проверке всех IP-адресов, на которые зарегистрировано доменное имя, обнаруживается большое число других подобных недавно созданных доменов.

Каждый из обобщенных признаков влияет на качественное обнаружение опасных ресурсов, распространяемых злоумышленниками в Интернете. Тем не менее, при проектировании браузерного инструмента для обнаружения и предотвращения атак, основанных на методах социальной инженерии, некоторые обобщенные признаки было необходимо разделить на более конкретные, а также отметить их веса. Для этого была сформирована определяющая выборка, содержащая опасные ресурсы, для которых была выполнена разметка наличия и отсутствия в них подозрительных признаков. Число рассматриваемых опасных ресурсов составило 20 адресов. На основании 10 приведенных ранее признаков проведена проверка 20 ресурсов, в результате которой был сделан вывод о частоте встречаемости признаков и присвоении каждому признаку определенного веса.

В результате была получена оценка весом признаков, приведенная в таблице 1 с новыми сформированными признаками и весами. С учетом небольшого размера выборки можно пренебречь небольшими отклонениями весов. Исходя из этого значения весов были округлены с условием значимости и опасности признака. Введем термин «идеальный вес». «Идеальным весом» считается 1, в случае рассмотренных ресурсов ставится 1, когда признак обнаружен у 20 из 20 ресурсов.

Таким образом, при разработке доступной системы обнаружения и предотвращения атак, основанных на методах социальной инженерии, веса помогут наиболее точно определить опасность ресурса для пользователя.

В целях улучшения методов обнаружения и предотвращения атак, основанных на методах социальной инженерии, направленных на пользователей в Интернете и актуальных для современной ситуации в РФ, был разработан прототип решения в формате плагина (расширения) для браузера. Его функционал заключается

Таблица 1.

Сформированные признаки и веса

№	Признак	Вес
1	Число дней с даты регистрации домена от 0 до 50	0.75
2	Число дней с даты регистрации домена от 51 до 150	0.25
3	Наличие в whois полей с содержимым «REDACTED FOR PRIVACY»	0.3
4	Наличие подозрительной доменной зоны	0.65
5	Аномальная последовательность цифр и букв в домене	0.25
6	Ответ сервера заголовка перенаправления на другой ресурс	0.35
7	Статус ответа, отличный от 200, 301 и 302	0.25
8	Длина тела ответа меньше 100	0.35
9	Количество найденных страниц в браузере при поиске домена менее или равно 500	0.8
10	Количество найденных страниц в браузере при поиске домена от 501 до 2000	0.2
11	Отсутствие DNS-записи MX	0.8
12	Наличие DNS-записи NS, связанной с публичными дешевыми DNS-серверами	0.2
13	Количество недавно зарегистрированных доменов на IP-адресах домена от 3 до 30	0.4
14	Количество недавно зарегистрированных доменов на IP-адресах домена от 30	0.8

в оперативной проверке сетевых ресурсов в Интернете, посещаемых пользователем в режиме реального времени, и выдаче предупреждения в случае обнаружения угрозы, способной нанести урон информационной системе (ИС) ПК, его персональным данным (ПДн) или активам.

Разрабатываемое расширение — кроссплатформенное, поддерживается всеми браузерами, построенными на основе свободного браузера Chromium и движка Blink для отображения веб-страниц. Архитектура разрабатываемого инструмента содержит плагин с функционалом извлечения домена и выдачей конечного результата, а также сервер с выполнением полной проверки домена. Плагин отправляет на сервер полученный домен. Далее домен анализируется с помощью выбранных признаков. На последнем шаге сервер направляет ответ обратно плагину. Такой вариант архитектуры был выбран на основе сравнения с другими по следующим критериям: используемый язык программирования (ЯП), реализация функционала всех выделенных признаков, возможность создания базы данных с накопленными знаниями (доменами и весами) и выдачи впоследствии более быстрого результата, безопасность, распределение нагрузки, скорость работы.

Для проверки точности и корректности обнаружения и предотвращения атак, основанных на методах социальной инженерии, разработанным решением необходимо было сформировать списки заранее известных легитимных ресурсов и фишинговых, а также вредоносных сайтов. Для формирования перечня чистых доменов используются сайты Интернет-магазинов, социальных сетей, новостных и образовательных ресурсов. Для того, чтобы составить перечень опасных доменов — небезопасных ресурсов были выбраны списки Банка России [14] и телеграм-канала «CyberSquatting RU Alerts» [15]. Стоит отметить, что выбранные ресурсы ориентированы именно на пользователей РФ, поскольку разработанное решение направлено на их защиту. Тестирование проводилось на равно распределенном количестве доменов для последующего заключения о результатах. Результат тестирования на 20 ресурсах показал 100 % правильное срабатывание для каждого домена из списка, на 100 ресурсах — 96 %.

Несмотря на имеющиеся недостатки со скоростью обработки сервером подаваемых на проверку ресурсов тестирование прототипа показывает хороший результат, решение верно определяет опасность данных на вход доменов. Данный результат позволяет говорить о качестве и эффективности разработанного решения с полученными признаками и их весами для обнаружения и предотвращения указанных атак.

Заключение

Для определения текущего уровня защищенности пользователей от атак методом социальной инженерии существующими популярными инструментами-расширениями проведен их обзор и анализ. В результате сравнения инструментов и выделения их преимуществ и недостатков выявлено практически полное отсутствие российских инструментов доступных для свободной загрузки пользователями РФ. Также для большинства рассмотренных расширений отмечены редкие обновления, а значит и минимальная актуализация данных, устаревшие манифесты и проверка по черным спискам, что показывает невозможность инструментами оперативного обнаружения новейших атак. Проверка расширений в режиме реального времени на опасных ресурсах доказала их неэффективность в обнаружении и предотвращении атак, основанных на методах социальной инженерии, направленных на российских пользователей в интернете.

На основе выявленных возможных сценариев действий злоумышленника при подготовке и реализации атак, а также с учетом недостатков рассмотренных расширений сформировано признаковое пространство. В зависимости от важности признака и частоты его выявления при проведении атак в исследуемых ресурсах, определены значения для весов предлагаемых признаков.

На основе представленной архитектуры прототипа системы обнаружения и предотвращения атак, основанных на методах социальной инженерии, выполнено проектирование и разработка программного решения. Данное решение представляет собой кроссбраузерный JavaScript-плагин и взаимодействующий с ним сервер с дополнительными модулями, библиотеками, а также функциями, реализующими определенные признаки с весами при проверке домена.

Для проверки точности и корректности определения обнаружения и предотвращения атак, основанных на методах социальной инженерии, разработанным решением, проведено его тестирование. Сформирован перечень безопасных и опасных доменов на основе данных из отчетов Банка России и вендоров решений по кибербезопасности в РФ. Тестирование прототипа показывает хороший результат, решение верно определяет опасность данных на вход доменов, что указывает на качество и эффективность разработанного прототипа.

Таким образом, полученные результаты свидетельствует о применимости разработанного прототипа системы и лежащего в её основе сформированного авторами признакового пространства, для обнаружения и предотвращения атак, основанных на методах социальной инженерии, направленных на пользователей в Интернете и актуальных для современной ситуации в РФ.

ЛИТЕРАТУРА

1. Исследование основных методов противодействия атакам, основанным на методах социальной инженерии, на предмет их эффективности и применимости к современной ситуации в РФ / К.Д. Наумова, В.Ю. Радыгин // Инновационные механизмы управления цифровой и региональной экономикой : Материалы V Международной студенческой научной конференции, Москва, 15–16 июня 2023 года. — Москва: Национальный исследовательский ядерный университет «МИФИ», 2023. — С. 145–158.
2. Браузер в России, Яндекс Радар. URL: https://radar.yandex.ru/browsers (дата обращения: 11.10.2023)
3. What are extensions, Mozilla. URL: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/What_are_WebExtensions (дата обращения: 11.10.2023)
4. Half of all Google Chrome extensions have fewer than 16 installs, ZdNet. URL: https://zdnet.com/article/half-of-all-google-chrome-extensions-have-fewer-than-16-installs/ (дата обращения: 11.10.2023)
5. ЖУРИН, Сергей И.; КОМАРКОВ, Дмитрий Е. ЗАЩИТА ВНЕШНЕГО ИНФОРМАЦИОННОГО ПЕРИМЕТРА ОРГАНИЗАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 95-107, 2018. ISSN 2074-7136. Доступно на: https://bit.mephi.ru/index.php/bit/article/ view/1164. Дата доступа: 26.10.2023. doi:http://dx.doi.org/10.26583/bit.2018.4.09.
6. SÜZEN A. A. EXAMINING THE SOCIAL ENGINEERING ATTACK VECTOR IN THE LINE OF DATA BREACH //Teknik Bilimler Dergisi. — 2023. — Т. 13. — №. 2. — С. 50–56. URL: https://dergipark.org.tr/en/download/article-file/3190558 (дата обращения: 27.10.2023).
7. Wang Z. et al. Social engineering in cybersecurity: a domain ontology and knowledge graph application examples //Cybersecurity. — 2021. — Т. 4. — С. 1–21. URL: https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00094-6 (дата обращения: 27.10.2023).
8. Lansley M. et al. SEADer++: social engineering attack detection in online environments using machine learning //Journal of Information and Telecommunication. — 2020. — Т. 4. — №. 3. — С. 346–362. URL: https://www.tandfonline.com/doi/full/10.1080/24751839.2020.1747001 (дата обращения: 27.10.2023).
9. Li T., Song C., Pang Q. Defending against social engineering attacks: A security pattern-based analysis framework //IET Information Security. — 2023. — Т. 17. — №. 4. — С. 703–726. URL: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/ise2.12125 (дата обращения: 27.10.2023).
10. Albladi S.M., Weir G.R.S. User characteristics that influence judgment of social engineering attacks in social networks //Human-centric Computing and Information Sciences. — 2018. — Т. 8. — №. 1. — С. 1–24. URL: https://hcis-journal.springeropen.com/articles/10.1186/s13673-018-0128-7 (дата обращения: 27.10.2023).
11. Oest A. et al. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale //29th {USENIX} Security Symposium ({USENIX} Security 20). — 2020. URL: https://www.usenix.org/system/files/sec20fall_oest_prepub.pdf (дата обращения: 26.10.2023)
12. Broadhurst R., Trivedi H. Malware in Spam Email: risks and trends in the Australian Spam Intelligence Data (SID)(January-September 2016). — 2019. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07194944/KSB_SpamPhishing_2015.pdf (дата обращения: 26.10.2023)
13. Szurdi J. et al. The long «taile» of typosquatting domain names //23rd {USENIX} Security Symposium ({USENIX} Security 14). — 2014. — С. 191–206. URL: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-szurdi.pdf (дата обращения: 26.10.2023)
14. Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке. Банк России. URL: https://www.cbr.ru/inside/warning-list/ (дата обращения: 03.12.2023)
15. Телеграм-канал CyberSquatting RU Alerts. URL: https://t.me/CyberSquattingChannel (дата обращения: 03.12.2023)

© Наумова Ксения Денисовна (naumovaxe@mail.ru); Радыгин Виктор Юрьевич (VYRadygin@mephi.ru)

Журнал «Современная наука: актуальные проблемы теории и практики»