УДК 621.391

КОМПЛЕКСНЕ ВИКОРИСТАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Р.Д. Капуста, К.О. Горяінова
Харківський національний університет радіоелектроніки

Abstract *– The article analyzes the main types of social engineering attacks and their classification. An overview of the instruments for detecting and counteracting social engineering as a method of accessing confidential information is provided, and key tools for counteracting such attacks are proposed. Experiments are conducted to demonstrate the effectiveness of each tool in different types of attacks. Particular attention is paid to software tools that help minimize the risks and losses from social engineering attacks. A system of integrated use of security tools has been developed that provides almost complete protection of the information system from such threats. The use of the WAZUH SIEM system in combination with the VirusTotal module provides opportunities to detect and counteract most types of attacks, including social engineering. For its part, integrating the Mozilla Firefox browser with the Startpage Privacy Protection application guarantees anonymous web browsing. The effectiveness of the protection methods has been confirmed experimentally. The proposed system was tested by modeling attacks, which proved its effectiveness. It was found that the integrated use of all modules provides the maximum level of protection of information resources. At the same time, the absence of any module reduces the overall security level.*

Анотація – У статті аналізуються основні види соціоінженерних атак та їхня класифікація. Здійснено огляд засобів виявлення та протидії соціальній інженерії як методу доступу до конфіденційної інформації, запропоновано ключові інструменти для протидії таким атакам. Проведено експерименти для демонстрації ефективності кожного з інструментів у різних типах атак. Особлива увага приділяється програмним засобам, що допомагають мінімізувати ризики та втрати від соціоінженерних атак. Розроблено систему комплексного використання засобів захисту, яка забезпечує майже повний захист інформаційної системи від подібних загроз. Використання SIEM системи WAZUH у поєднанні з модулем VirusTotal надає можливості для виявлення та протидії більшості видів атак, включаючи соціальну інженерію. Зі свого боку інтеграція браузера Mozilla Firefox з додатком Startpage Privacy Protection гарантує анонімність перегляду вебсторінок. Ефективність методів захисту підтверджена експериментально. Проведено тестування запропонованої системи шляхом моделювання атак, що дозволило підтвердити її дієвість. Виявлено, що комплексне використання всіх модулів забезпечує максимальний рівень захисту інформаційних ресурсів. Водночас відсутність будь-якого модуля знижує загальний рівень безпеки.

Вступ

На сьогоднішній день соціальна інженерія дозволяє зловмиснику отримати майже повний доступ до інформаційної системи, лише підібравши правильний підхід до співробітників будь-якої організаційної структури. Невичерпний потенціал подібних атак спонукає кіберзлочинця до вдосконалення методів атаки на потенційну жертву, проводити попередню розвідку, відшукувати особисті дані та слабкі місця співробітника для обрання найбільш дієвого вектора атаки. За статистичними даними основною загрозою інформаційній безпеці підприємства є людський фактор. Слабкі

сторони людини, які можуть бути використані зловмисником, описуються як вразливості, доступ до інформації та довіра, якими маніпулює атакуючий. Людина може несвідомо надати зловмиснику доступ до інформаційних ресурсів, чим той і користується, розраховуючи на помилки персоналу.

Таким чином, задача щодо забезпечення захисту інформації кінцевих користувачів від атак соціальної інженерії представляє значний практичний інтерес. Водночас метою роботи є розробка системи комплексного використання засобів захисту від атак соціальної інженерії, які матимуть можливість мінімізувати ризики, а також запобігти виконанню подібних атак у майбутньому.

I. Аналіз і класифікація соціоінженерних атак

У сучасному світі неможливо уявити собі підприємство, яке б не мало у своєму розпорядженні співробітників та інформаційних ресурсів, з якими б вони взаємодіяли. Кожен має своє робоче місце, свій унікальний ідентифікатор тощо. Проте не кожен співробітник замислюється над тим, наскільки важлива інформація, якою він володіє, та до яких наслідків може призвести заволодіння цієї інформацією зловмисником. На жаль, існує безліч методик, які допомагають атакуючому отримати інформацію від потенційної жертви. Серед прийомів безпосереднього впливу на свідомість людини (обману, шантажу, легендування) слід зазначити те, що всі ці методи перейшли у цифровий формат. Адже з розвитком ери інформаційних технологій з'явилися відповідні інструменти, які домагають шахраям довести свою «істину» до необхідного користувача. Повний комплекс шкідливих дій, спрямований на заволодіння особистими даними або отримання доступу до інформаційної системи через необачність користувача, отримав назву соціальної інженерії.

Насамперед необхідно визначити основні атаки соціальної інженерії. Існує величезна кількість різноманітних способів обману людини, а також методів впливу на свідомість, які можуть буди використані потенційним зловмисником для отримання інформації. За статистичними даними компанії IBM на 2022 рік [1] саме через соціоінженерні атаки відбуваються найбільші фінансові втрати у світі. Найбільші фінансові втрати, які сягають мільйонів доларів, спричиняються саме фішинговими атаками. На рис. 1 приведено діаграму світових фінансових втрат через найбільш популярні атаки на інформаційні ресурси [1] .

Методи соціальної інженерії можуть застосовуватися не лише через засоби зв'язку, але й безпосередньо серед співробітників, шляхом проникнення до установи, де планується атака. Серед різноманіття таких методів можна виділити основні, які найчастіше використовуються зловмисниками. Їх перелік наведено на рис. 2 [1, 2].

Рис. 1. Щорічні втрати компаній, розподілені по атаках

Рис. 2. Класифікація атак соціальної інженерії

II. Побудова системи комплексного використання засобів захисту інформаційних ресурсів від атак соціальної інженерії

Спираючись на глобальну проблему захисту інформації від впливу атак соціальної інженерії, було проведено дослідження різноманітних механізмів захисту та визначено компоненти для побудови комплексної системи протидії атакам соціальної інженерії, яка матиме на меті автоматичне блокування та протидію вчинкам зловмисника через запобігання розповсюдження шкідливого впливу на інформаційні ресурси користувачів [3 – 8]. Слід зазначити те, що всі інструменти, які були використані для побудови системи протидії та захисту інформації, мають виключно ліцензію з відритим доступом. До того ж всі обрані інструменти захисту мають чітку та структуровану документацію, яка також міститься у вільному доступі. Це дозволить створити

власну систему захисту від подібних атак для будь-якої організації незалежно від бюджету та рівня підготовленості спеціалістів з інформаційної безпеки. Завдяки мультиплатформенній основі всі зазначені механізми захисту можуть бути використані для різноманітних пристроїв незалежно від місця знаходження користувача.

Для підключення до корпоративної мережі захисту, в якій розгорнуто SIEM систему WAZUH, користувачу достатньо завантажити агент на свій домашній або робочий комп'ютер та ввести верифікаційний токен корпоративного сервера [3]. Тобто у будь-якому кутку планети при справному мережному підключенню до мережі інтернет, співробітник зможе приєднатися до корпоративного сервера SIEM системи WAZUH та отримати надійний захист та аудит власного інформаційного простору.

Браузер Mozilla Firefox і вебзастосунок Startpage Privacy Protection можуть бути завантажені та встановлені самостійно на будь-який пристрій. Навіть без додаткового налаштування цих програмних засобів користувач отримає надійний захист за замовчуванням від кібератак.

VirusTotal є безперервно доступним вебресурсом, що може надавати послуги з перевірки надісланих посилань або програмних файлів, які можуть передаватися від невідомих користувачів і бути шкідливими.

Спираючись на отримані результати дослідження, було побудовано структурну схему для наочної демонстрації переваг використання запропонованих засобів захисту від атак соціальної інженерії. Запропонована система приведена на рис. 3.

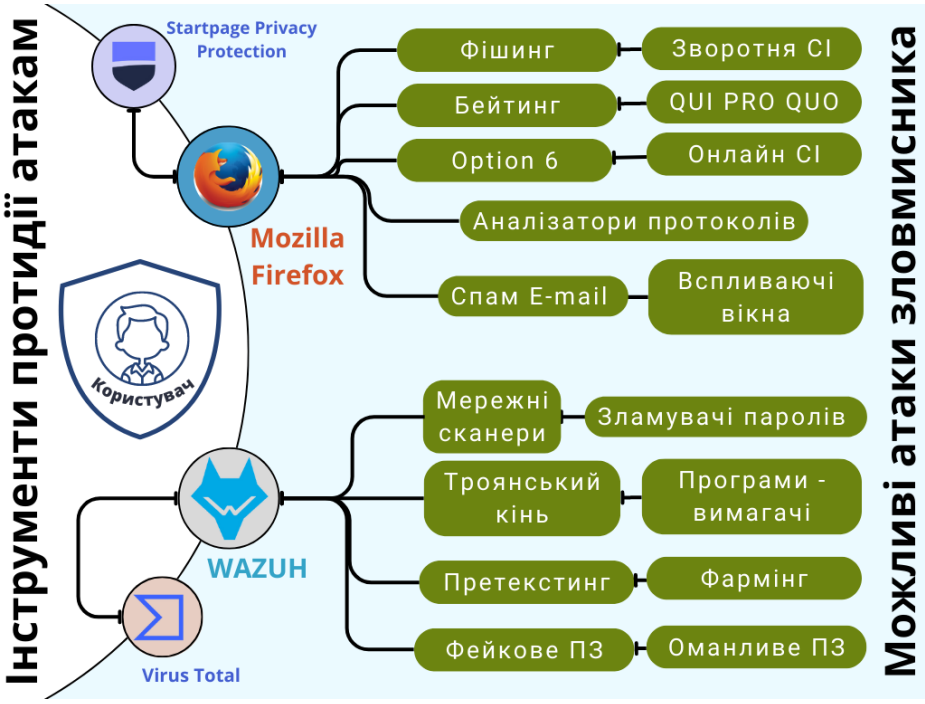

Рис. 3. Класифікація атак соціальної інженерії

На схемі відображено розглянуті методи протидії атакам соціальної інженерії, проте слід зазначити, що обрані інструменти можуть надати розширений захист і від

інших розповсюджених атак, які можуть використати зловмисники. Біля символу користувача ми маємо відображення основних інструментів безпеки та інтегровані в них модулі. На іншій стороні схеми відображено актуальні атаки соціальної інженерії, а також інші атаки, які можуть бути заблоковані обраними механізмами захисту.

III. Оцінка ефективності використання SIEM системи WAZUH

Основним компонентом захисту та виявлення атак можна визначити саме SIEM систему WAZUH. Цей інструмент дозволяє провести захист майже від будь-якої атаки з використанням соціальної інженерії при наявності відповідної конфігурації. Проте для більшої ефективності необхідно використовувати додаткові модулі, що можуть бути інтегровані у систему [4]. Окрім цього, SIEM система WAZUH виконує функцію аудиту та аналізу подій безпеки, які відбуваються на пристроях користувачів. Для визначення доцільності та необхідності використання цього інструменту проведемо дослідження загальної ефективності SIEM системи WAZUH протягом одного року використання. Результати дослідження приведено на рисунку 4.

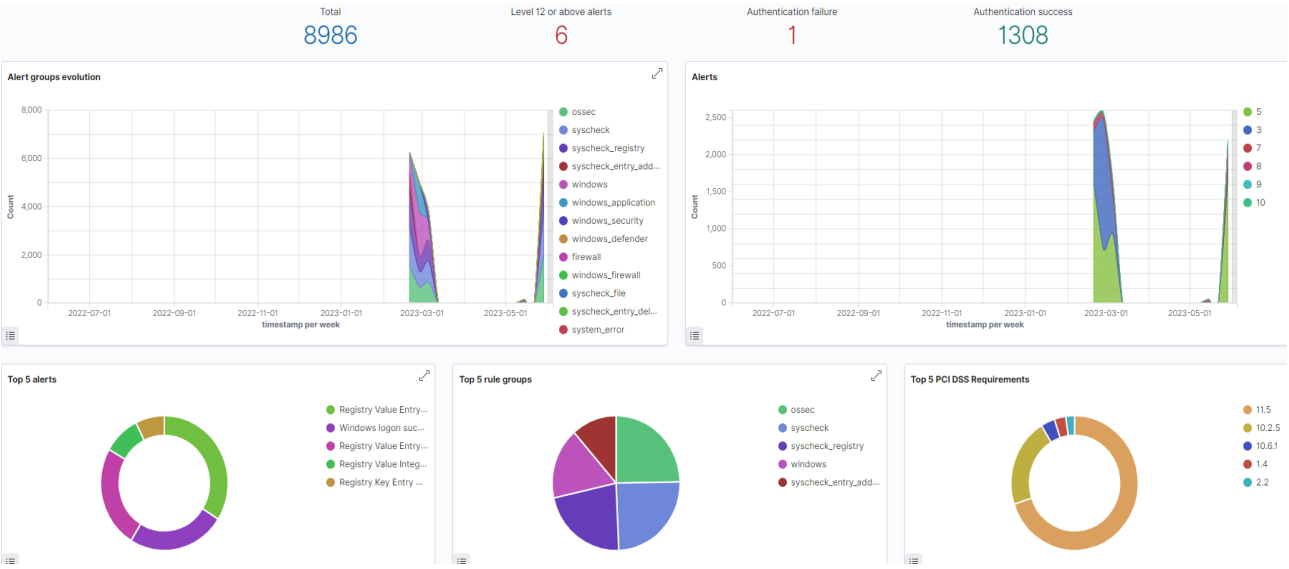

Рис. 4. Результати дослідження ефективності впровадження SIEM системи WAZUH

Виконаємо аналіз отриманих результатів. Перед цим слід зазначити, що дані для дослідження було отримано шляхом постійних експериментів з використанням різних операційних систем і підключених агентів до них.

Протягом аналізу було виявлено п'ять найчастіших типів сповіщення, тобто реагування системи на певні види порушень вказаних політик безпеки. Цей параметр дозволить виявити найбільш слабкі місця у системі безпеки, а також визнати, на що саме необхідно звернути особливу увагу співробітнику з інформаційної безпеки підприємства для запобігання та вчасного реагування на вказані інциденти.

Також системою було виділено п'ять найбільш актуальних груп політик безпеки, що мали найбільше сповіщень безпеки. Цей параметр дозволить краще структурувати групи політик безпеки для підвищення швидкості реагування на інциденти, використовуючи виключно ті політики безпеки, які впроваджені у даній групі політик.

Окрім цього, SIEM система WAZUH має вбудований модуль перевірки платіжних карток за стандартом PCI DSS. В даному випадку модуль перевіряв наявність ідентифікаційного номеру користувача та встановивши його приналежність до системи звіряв рівень захисту облікових даних за вказаним стандартом. Цей модуль може бути особливо корисним при здійсненні платіжних операцій користувачів в інтернеті. Операція захисту відбувається під час відправки облікових даних на вебресурсах.

Загалом системою було знайдено приблизно дев'ять тисяч порушень безпеки за рік використання системи. Дванадцять із них були критичними для системи захисту персонального комп'ютера користувача. Також було зафіксовано порушення автентифікації у системі.

Таким чином, можна визначити те, що SIEM система WAZUH має величезний потенціал для підвищення рівня інформаційної безпеки. Спираючись на отримані дані, можна визначити те, що при розгортанні даної системи можливо здійснювати повний аудит подій інформаційної безпеки на підприємстві та автоматизувати систему сповіщень при виявленні кіберінцидентів. Можливості SIEM системи WAZUH допоможуть значно підвищити потенціал спротиву майже від усіх можливих кібератак зокрема із застосуванням методів соціальної інженерії.

IV. Оцінка ефективності використання VirusTotal API

Наступним компонентом захисту є VirusTotal API, який було вдало інтегровано у SIEM систему WAZUH [5]. VirusTotal дозволяє автоматично перевіряти всі файли та програмні компоненти системи, які наявні в операційній системі користувача. Саме завдяки цьому модулю кожен підключений агент має змогу отримати повний захист від порушення цілісності файлів у власній системі. Також безперервне сканування програмного засобу допоможе виявити вразливості програмних продуктів, що встановлені на персональному комп'ютері.

Для визначення доцільності та необхідності використання цього інструменту проведемо дослідження ефективності виявлення змін параметрів реєстру операційної системи Windows 10 за допомогою VirusTotal API протягом одного місяця використання. Результат дослідження приведено на рис. 5.

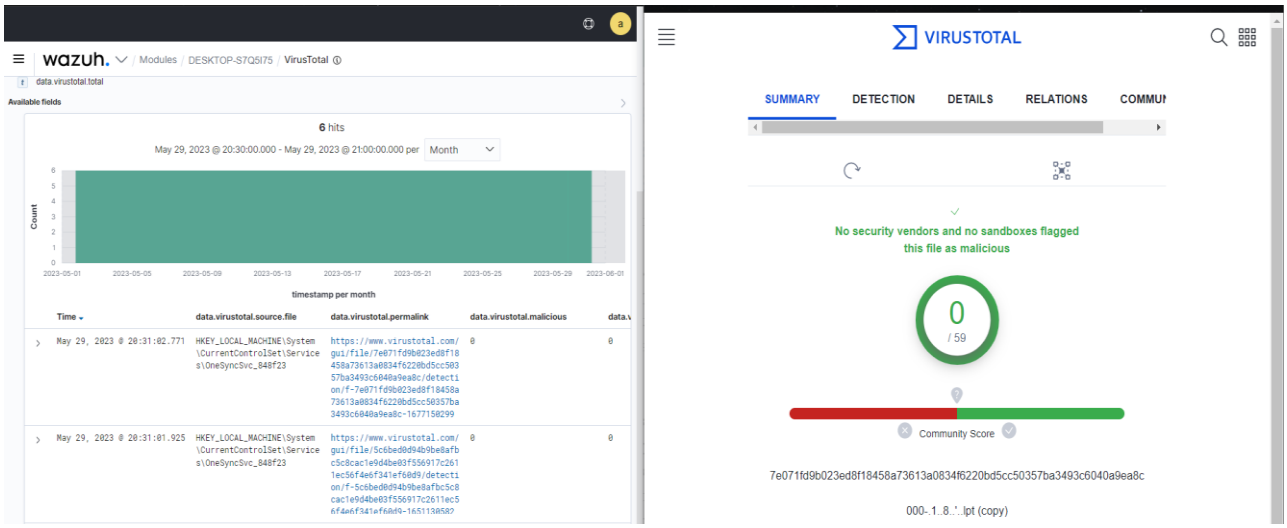

Рис. 5. Результати дослідження ефективності використання VirusTotal

Проведемо аналіз отриманих результатів. Попередньо зазначимо, що дані для проведення дослідження були отримані під час використання віртуальної машини з розгорнутою операційною системою Windows 10, тобто досліджувана система навмисно використовувалась не часто та не була основною системою для роботи користувача, що дозволило зібрати об'єктивні дані з ефективності використання модуля VirusTotal.

Цим модулем було знайдено зміни у параметрах розділу реєстру, який відповідає за зміни у політиках нашарування Bluetooth з'єднання. Це означає, що цей розділ реєстру було модифіковано без прямого дозволу користувача. Також дана модифікація отримала відповідний номер у базі даних VirusTotal, а системою було сформовано гіперпосилання, перейшовши на яке користувач має змогу детальніше ознайомитись із звітом. Отже, у даному випадку відбулося звичайне оновлення драйверу, проте система відреагувала з попередженням про те, що вказані зміни все ж відбулись у реєстрі.

Спираючись на отримані результати досліджень, можна дійти висновків, що VirusTotal є досить універсальним інструментом захисту, який допоможе виявити та запобігти не тільки модифікації файлів користувача, а також відслідкує зміни у системних файлах ОС, що дозволить значно підвищити відмовостійкість та збереження працездатності системи навіть під час здійснення кібератак зловмисником. VirusTotal має свою окрему базу даних вразливостей, яка автоматично оновлюється. Окрім цього, модуль VirusTotal формує простий та зрозумілий звіт, який допоможе пришвидшити оцінку виявленої загрози після чого оцінити необхідність у прийнятті відповідних заходів щодо їх усунення.

V. Оцінка ефективності використання Mozilla Firefox

Наступним елементом захисту є браузер Mozilla Firefox, який має особливий модуль захисту від фішингових посилань і шкідливих вебресурсів [6, 7]. Mozilla Firefox

надає можливість користувача власноруч проводити налаштування безпеки та самостійно визначати параметри захисту, що дозволяє проводити тонкі налаштування, які б відповідали політикам безпеки підприємства. Також ядро браузеру має можливість інтегрувати велику кількість сторонніх модулів і додатків, що дозволяє провести інтеграцію усіх необхідних інструментів безпеки та аудиту перегляду вебсторінок користувачів. Більше того, браузер має змогу проводити автоматичний аудит переглянутих сайтів і визначає їхній рівень безпеки для користувача. Для визначення доцільності та необхідності використання цього інструменту проведемо дослідження загальної ефективності браузера Mozilla Firefox та його вбудованого модуля детекції для виявлення потенційно небезпечного сайту. Результат роботи приведено на рисунку 6.

Проведемо аналіз отриманих результатів. Попередньо зазначимо, що дані для проведення дослідження були отримані при використанні небезпечного вебресурсу, який замаскований під сайт банку «Бумб». Одразу після відкриття сайту браузером було зупинено подальші дії за використаним гіперпосиланням. Користувач отримав попередження про те, що цей ресурс є небезпечним і що працювати з ним заборонено. До того ж було виведено технічну інформацію, яка містить у собі IP-адресу небезпечного сайту, порт та навіть ім'я домену. Також користувачу було надано підказку щодо необхідності передачі інформації на ресурс CERT-UA, що допоможе фахівцям з інформаційної безпеки державного рівня прийняти відповідні заходи щодо перевірки та подальшого блокування цього ресурсу. Згідно з аудитом безпеки та за даними звіту, який було автоматично сформовано, даний ресурс отримав найвищій третій рівень небезпеки, про що було підтверджено відпрацюванням самого браузеру.

Спираючись на результати попередніх досліджень можемо визначити, що саме веббраузер Mozilla Firefox може стати плацдармом для захисту користувача від небезпечних вебсторінок і фішингових сайтів. Завдяки вбудованому модулю захисту, спеціаліст з інформаційної безпеки має можливість провести налаштування, які б відповідали встановленим політикам безпеки на підприємстві. Окрім того, модель безпеки запобігає виконанню шкідливих посилань і надає звіт з причини унеможливлення роботи з ресурсом. Також автоматизований зв'язок з ресурсом CERT-UA надає можливість оперативного сповіщення про потенційно небезпечний сайт, а також спонукає до надання переваги цьому браузеру для його використання на підприємствах та в організаціях України.

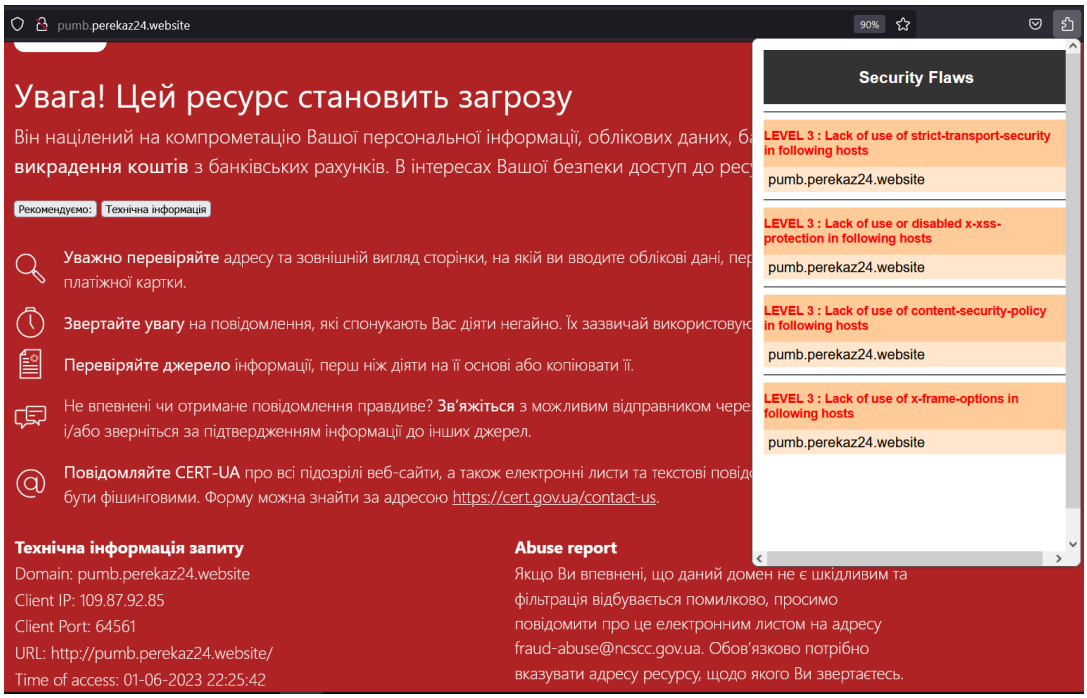

Рис. 6. Результати дослідження ефективності використання Mozilla Firefox

VI. Оцінка ефективності використання Startpage Privacy Protection та аналіз отриманих результатів

Останній модуль, який було обрано для захисту та запобігання атакам, це Startpage Privacy Protection [8]. Цей вебзастосунок було успішно інтегровано у браузер Mozilla Firefox та використано для дослідження можливостей захисту конфіденційності користувача, який переглядає вебсторінки. Цей застосунок має можливість автоматичного блокування, які можуть містити у собі персональні дані користувача. Також програмний засіб проводить оцінку захищеності з'єднання з сервером і проводить аудит заблокованих даних. Для визначення доцільності та необхідності використання цього інструменту проведемо дослідження загальної ефективності вебзастосунку Startpage Privacy Protection протягом одного дня використання цього сервісу. Результат виконання дії приведено на рис. 7.

Проведемо аналіз отриманих результатів. Проте перед цим слід зазначити, що дані для проведення дослідження отримано при звичайному режимі роботи користувача, що являє собою використання пошукових запитів для отримання інформації з різних сайтів мережі Інтернет без додаткових засобів захисту. При активному стані роботи застосунку відбувається зміна графічного оточення браузера, це необхідно для сповіщення користувача про те, що застосунок наразі є активованим. Окрім цього, всі сайти з результату пошуку отримали позначки про те, що користувач буде працювати з ними у режимі «інкогніто».

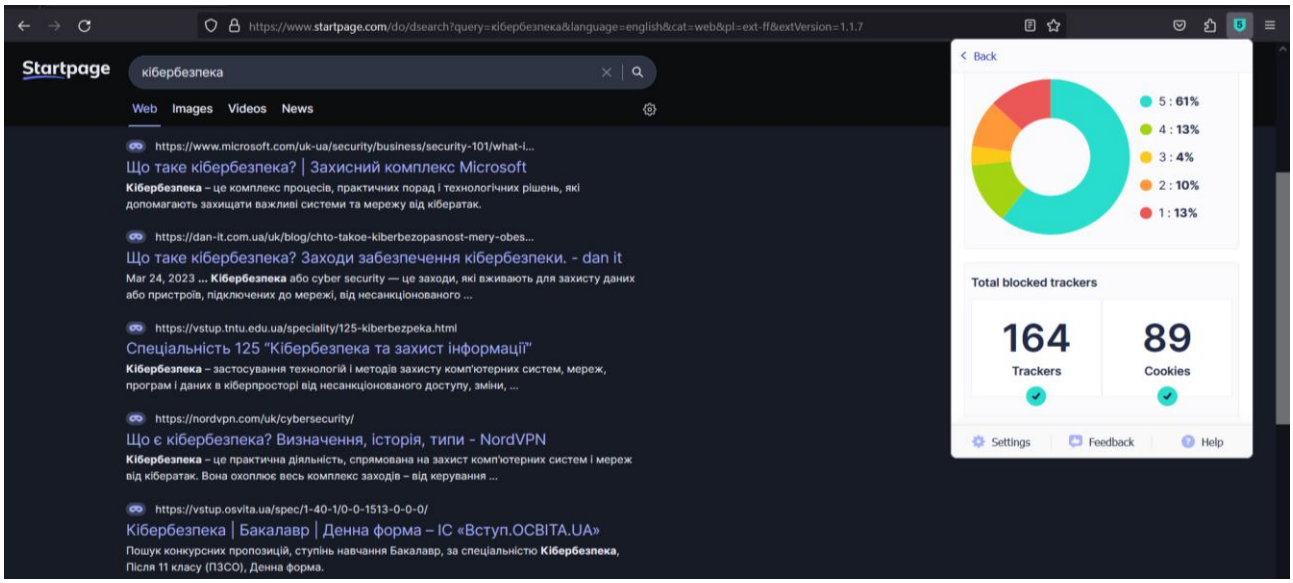

Рис. 7. Результати дослідження ефективності використання Startpage Privacy Protection

Загалом після активної роботи з браузером протягом одного дня було заблоковано низку застосунків відстеження та збору конфіденційної інформації про користувача. Також системою було динамічно створено діаграму відсотків безпечності переглянутих сайтів. Відповідно до цього можемо визначити, що близько шістдесяти відсотків переглянутих ресурсів мали найвищій рівень безпеки та лише тринадцять відсотків мали критичний рівень безпеки.

Спираючись на результати попередніх досліджень можемо визначити, що веб-застосунок Startpage Privacy Protection може бути використаний для підвищення рівня конфіденційності перегляду вебсайтів користувачів. Ці властивості надають можливість приховати особисті дані користувачів від потенційного зловмисника, унеможливлюючи проведення цілої низки атак, які спираються на попередній збір інформації.

VII. Підготовка до тестування запропонованої комплексної системи протидії атакам соціальної інженерії

Для підтвердження працездатності та доцільності використання розробленої системи захисту від атак соціальної інженерії було змодельовано три найбільш популярні атаки на проникнення, а саме:

- оманливе програмне забезпечення, яке буде реалізовано за допомогою програмного засобу MSFvenom Payload Creator;
- фішинг, імплементований з використанням програмного забезпечення Zphishe;
- email фішинг, виконаний за допомогою додатку Phish Mailer.

Тестування на проникнення було здійснено у середовищі віртуалізації VMware зі встановленою операційною системою Kali Linux. Всі використані програмні засоби під час тестування були заздалегідь завантажені та налаштовані. Для розгортання віртуальної машини було виділено наступні фізичні ресурси, а саме:

– 4 Гбайта оперативної пам'яті для оптимальної швидкості обчислень;
– 2 ядра основного процесора з частотою 1.33 ГГц;
– 512 Мбайт відео пам'яті для підтримки графічного інтерфейсу;
– 10 Гбайт виділеної пам'яті жорсткого диску;
– широкосмугове підключення до мережі Інтернет через порт Ethernet.

Обрані фізичні параметри системи сприяли оптимальній роботі операційної системи та надавали змогу динамічно відслідковувати результати проведення тесту. Під час підготовки до проведення тестування на проникнення заздалегідь було вимкнено інші засоби захисту персонального комп'ютера, окрім тих, які були запропоновані у схемі захисту від атак соціальної інженерії. Всі змодельовані атаки проводились в умовах, наближених до реальних; користувач, який приймав участь у тестуванні, не знав про те, які саме отримані дані мають шкідливий характер. Деякі персональні дані користувача, що приймав участь у тестуванні, були видалені з міркувань безпеки.

VIII. Результати тестування з використанням MSFvenom Payload Creator

Першим кроком проводимо дослідження захисту за допомогою моделювання атаки оманливого програмного забезпечення, що матиме можливість передачі корисного навантаження від тестувальника до потенційної жертви, тобто програмний засіб, який виконує команди атакуючого у віддаленому режимі. Для цього можливе використання програмного засобу MSFvenom Payload Creator (MSFPC) [9], який проводить автоматичне генерування шкідливого програмного засобу, що містить у собі корисне навантаження для тестувальника. Шкідливі програмні засоби можна створювати для різних операційних систем, що дозволить проводити тестування різноманітних пристроїв. Для створення атакуючому достатньо лише вказати свою IP-адресу та порт підключення, за яким буде налаштований канал віддаленого доступу, після цього MSFPC самостійно генерує необхідні файли та запаковує їх у файл відповідного формату, в даному випадку це файл з розширенням .exe. Результат створення та активації шкідливого програмного засобу приведено на рис. 8.

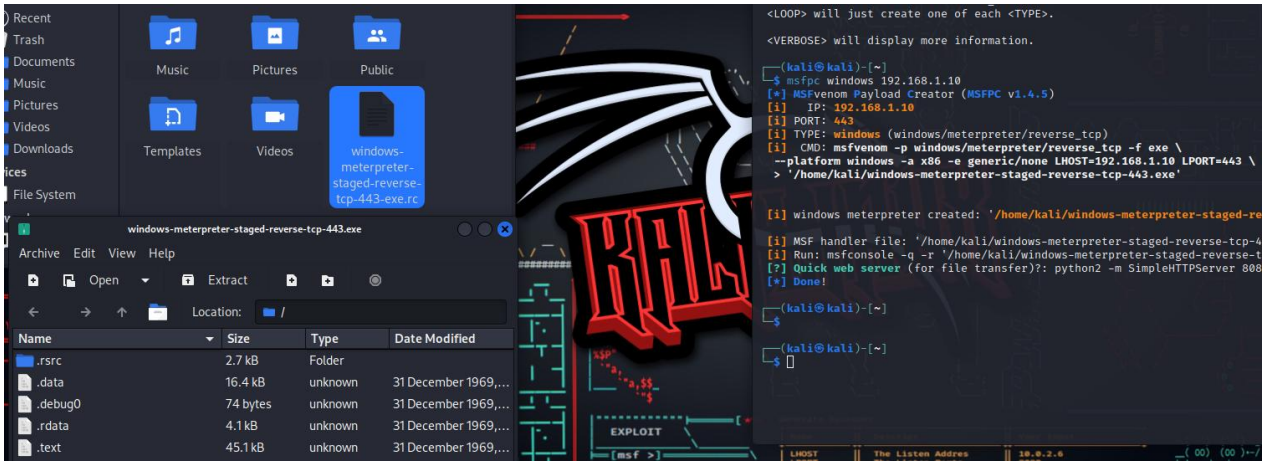

Рис. 8. Виконання роботи програмного засобу MSFPC

Після створення шкідливого програмного засобу проводимо його відправку зо допомогою месенджеру Telegram на адресу потенційної жертви та активуємо його на робочому комп'ютері. Ця діє моделює поведінку звичайного співробітника, який може отримати програмний файл від свого колеги по роботі. На наступному кроці спостерігаємо за роботою SIEM системи WAZUH разом з інтегрованою оболонкою VirusTotal API. Результат виконання блокування програмного засобу за допомогою механізмів SIEM системи WAZUH приведено на рис. 9.

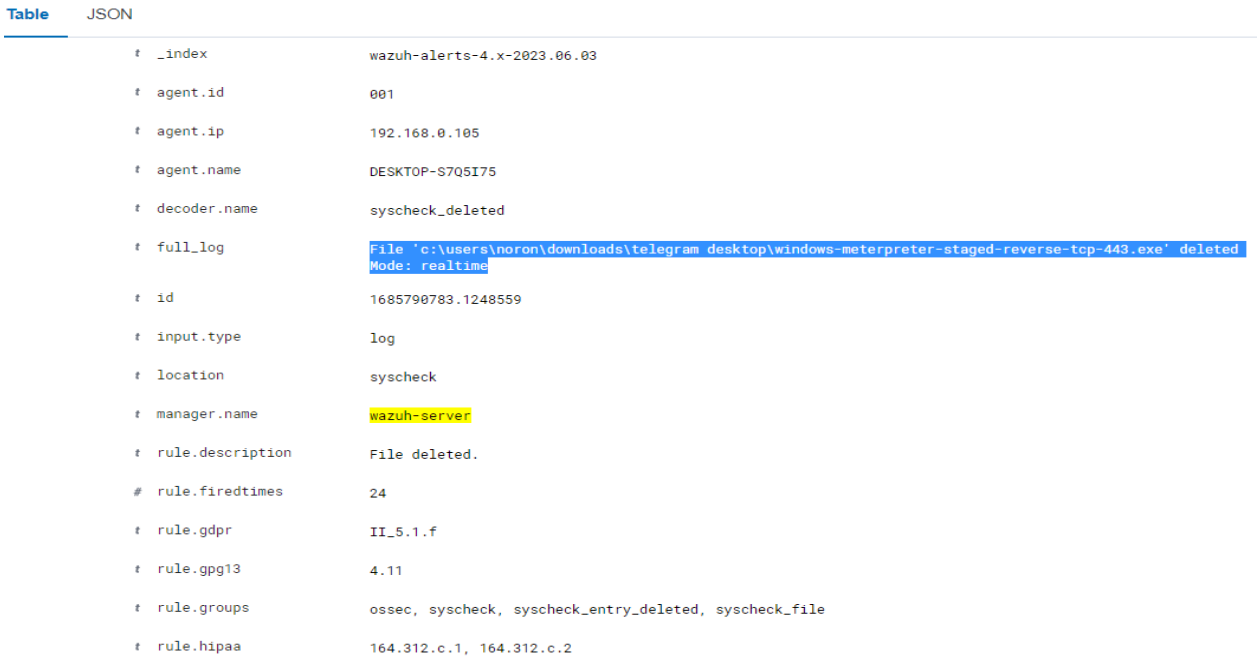

Table JSON

_index	wazuh-alerts-4.x-2023.06.03
agent.id	001
agent.ip	192.168.0.105
agent.name	DESKTOP-S7Q5I75
decoder.name	syscheck_deleted
full_log	File 'c:\users\noron\downloads\telegram desktop\windows-meterpreter-staged-reverse-tcp-443.exe' deleted Mode: realtime
id	1685790783.1248559
input.type	log
location	syscheck
manager.name	wazuh-server
rule.description	File deleted.
rule.firedtimes	24
rule.gdpr	II_5.1.f
rule.gpg13	4.11
rule.groups	ossec, syscheck, syscheck_entry_deleted, syscheck_file
rule.hipaa	164.312.c.1, 164.312.c.2

Рис. 9. Реакція SIEM системи WAZUH на шкідливий програмний засіб, створений MSFPC

Після завантаження шкідливого програмного засобу SIEM системою WAZUH було виявлено та автоматично видалено цей файл, який порушував заздалегідь налаштовані політики безпеки групи користувачів, до якої відносився підключений агент. Це допоможе ідентифікувати комп'ютер та обліковий запис співробітника, який виконав завантаження шкідливого програмного засобу. Виявлення потенційного співробітника та його робочого комп'ютера відбувається через підключеного до системи ідентифікатора агента, який містить у собі інформацію про ім'я комп'ютера його IP-адресу, а також ім'я облікового запису користувача. Також було зафіксовано час та дату цього інциденту. Таким чином, завдяки роботі SIEM системи WAZUH було попереджено атаку за допомогою шкідливого програмного засобу, а також ідентифіковано користувача, яким було спричинено цей інцидент.

IX. Результати тестування з використанням Zphisher

Далі проводимо дослідження та моделювання атаки фішингу за допомогою створення шкідливого посилання на сайти. Переважна більшість атак із використан-

ням соціальної інженерії базується на зборі конфіденційних даних користувача. Найбільш розповсюджений спосіб – це маскування авторизайційних форм із транслюванням введених облікових даних атакуючому. Для створення подібного посилання можна використати програмний засіб Zphisher [10], який надає можливість тестувальнику створити підроблену вебсторінку, яка надасть можливість подивитись введені користувачем дані та виявити адресу пристрою, з якого ці дані було знято. Програмний засіб надає можливість створити підроблену сторінку за різними шаблонами популярних Інтернет ресурсів. Після цього розгортається сервер, який має змогу збирати введені облікові дані, а також IP-адресу пристроїв, з яких було відкрито дане посилання, після цього зібрані дані передаються тестувальнику. Для прикладу проводимо створення та активацію сторінки платіжної системи PayPal. Результат виконання створення посилання приведено на рисунку 10.

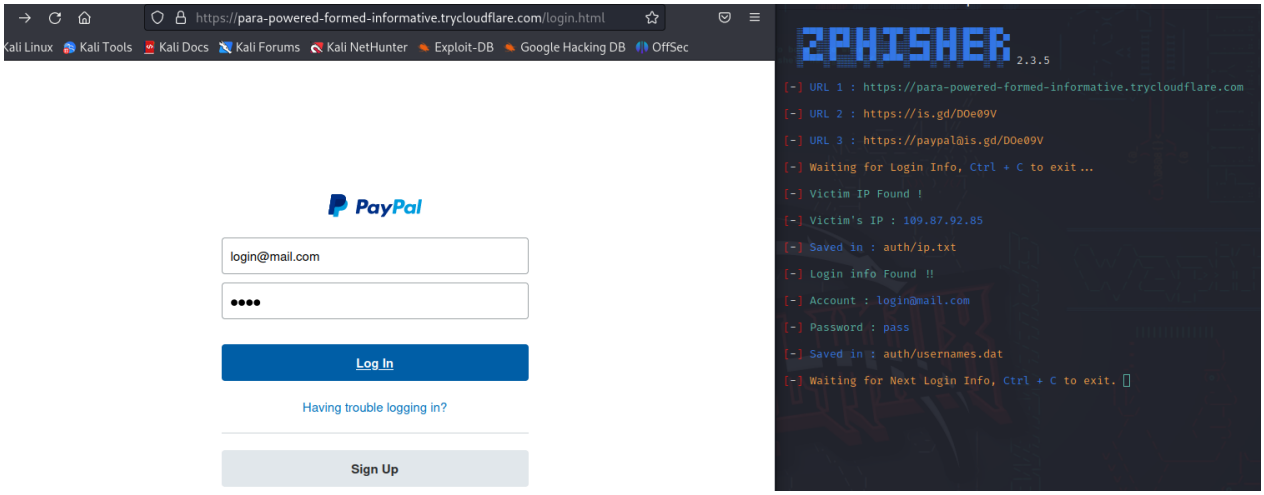

Рис. 10. Створення фішингового посилання

Після активації параметрів тестувальник отримав повноцінну вебсторінку авторизаційної форми сайту PayPal. Якщо користувач авторизується на цій сторінці, то всі його дані будуть передані атакуючому. Також атакуючий отримав IP-адресу пристрою, з якого було виконано роботу цього посилання. Таким чином, тестувальник має змогу ідентифікувати співробітника, який перейшов за цим шкідливим посиланням. Для захисту від цієї атаки проводимо активацію цього посилання за допомогою браузеру Mozilla Firefox зі встановленими параметрами безпеки та модуля захисту від фішингових атак. Результати експерименту приведено на рис. 11.

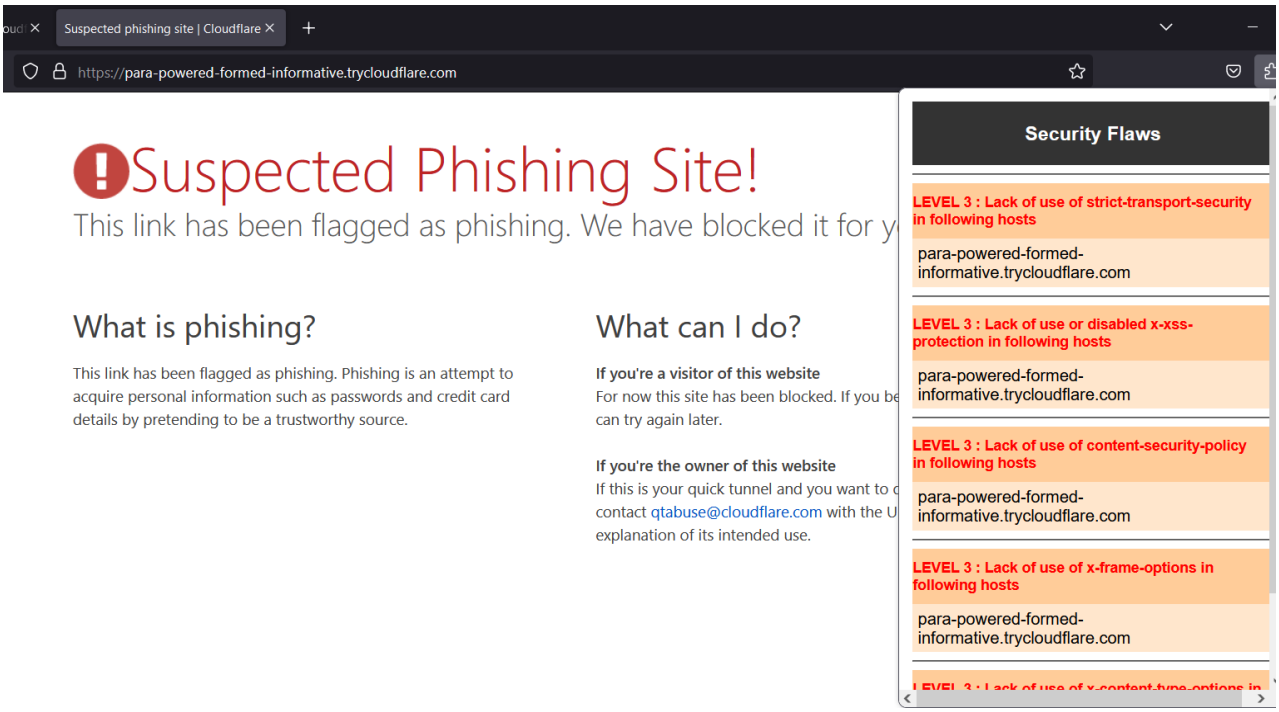

Рис. 11. Блокування фішингового посилання браузером Mozilla Firefox

В результаті аналізу отриманих результатів було виявлено, що браузер Mozilla Firefox успішно заблокував шкідливе посилання та відобразив попередження про те, що даний ресурс є небезпечним, а також заблокував подальшу роботу користувача на цьому сайті. Жодні подальші дії з цим посиланням не зможуть надати користувачу доступ до ресурсів цього сайту, шкідливе посилання було додано до бази даних браузеру та було автоматично заблоковано. Програмний засіб аудиту безпеки браузеру відобразив відповідне повідомлення, що цей сайт був заблокований та йому було присуджено третій, найвищий рівень небезпеки. Також програмним засобом було зафіксовано факт передачі даних з цієї сторінки на віддалену не перевірену адресу. Таким чином, під час тестування на проникнення фахівець з інформаційної безпеки має змогу перевірити надійність наявних систем захисту від подібних посилань, а також виявити осіб, що зазнали шкоди від подібного роду атак.

X. Результати тестування з використанням Phish Mailer

Проводимо дослідження та моделювання атаки email фішингу за допомогою створення шкідливого електронного листа. Слід відмітити, що кожен співробітник організації щоденно отримує велику кількість різноманітних листів на електронну адресу, тому email фішинг є досить популярною атакою за допомогою соціальної інженерії. Тому спеціаліст з тестування на проникнення може використати і цей вид атаки. Для створення фішингового листа не треба власноруч підроблювати оригінальний лист повідомлення. Можливо використати готові шаблони та програмні засоби, які можуть автоматично сформувати фішинговий лист та проводити збір конфіденційних даних потенційної жертви. Для прикладу розглянемо роботу програмного засобу

Phish Mailer [11], який надає можливість створити підроблений лист за певним переліком запропонованих шаблонів. Тестувальник має змогу налаштувати адресу відправника, ім'я адресата та інші параметри, які допоможуть замаскувати контент цього листа. Для прикладу створюємо сторінку, яка має вигляд листа від команди підтримки PayPal та свідчить про небезпечну автентифікацію облікового запису на іншому пристрої. Також на цьому листі присутня кнопка переходу на сайт відновлення пароля, проте тут приховано шкідливе посилання, яке було створено за аналогією з попереднім сценарієм. Результат створення фішингового листа приведено на рис. 12.

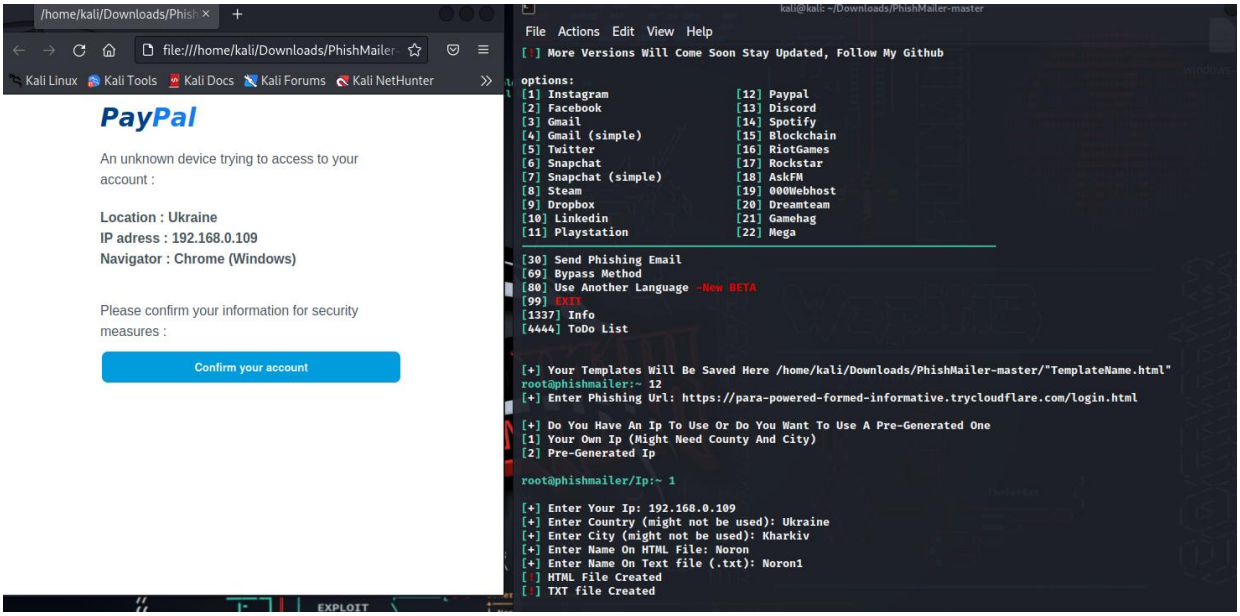

Рис. 12. Результат створення шкідливого листа

Отже, якщо користувач перейде за посиланням, то тестувальник отримає його IP-адресу та зможе виявити користувача, який перейшов за даним посиланням. Також тестувальник матиме змогу відтворити всі облікові дані користувача. Для захисту від подібних листів користувач може перевірити надане посилання за допомогою ресурсу VirusTotal. Скопіювати надане фішингове посилання можливо через кнопку, яка додана до листа, визвавши контекстне меню. Після переходу на офіційний сайт VirusTotal необхідно обрати відповідне меню перевірки гіперпосилань та вставити отриманий рядок. Після чого ресурс наддає відповідь з аналізом цього посилання, результат якого приведено на рис. 13.

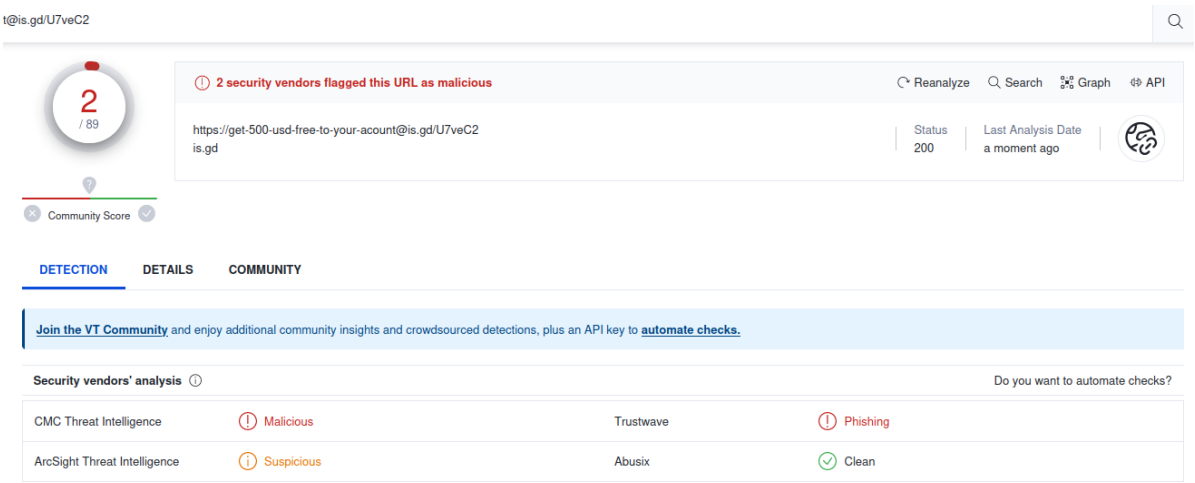

Рис. 13. Результат перевірки шкідливого посилання

Проводимо аналіз отриманих результатів. Ресурс VirusTotal, перевіривши це посилання за різноманітними базами та антивірусними програмними засобами, визначив, що дане посилання є фішинговим і небезпечним. Про це свідчать відповідь від антивірусного програмного засобу Trustware. Зі свого боку програмний модуль CMC Threat Intelligence визначив це посилання зловмисним, а модуль захисту ArcSight Threat Intelligence вказав на підозрілість цього посилання. Всі інші антивірусні програмні засоби, за якими ресурс VirusTotal проводив перевірку фішингового посилання, не виявили жодної загрози. Також було встановлено те, що дане посилання є активним та може прослуховуватись зловмисником – про це свідчить наявний статус «200», а також відповідь оболонки API про те, що останні запити були щойно надіслані.

Висновки

У роботі було проаналізовано основні види соціоінженерних атак та проведено їхню класифікацію, виконано огляд засобів виявлення та протидії соціальній інженерії як методу доступу до конфіденційної інформації. Запропоновано основні інструменти протидії атакам соціальної інженерії та проведено експерименти для наочної демонстрації роботи кожного з них для різних типів атак. Розглянуто програмні засоби, які допоможуть мінімізувати ризики та втрати, що можуть бути викликані атаками соціальної інженерії.

Спираючись на отримані результати було запропоновано систему комплексного використання засобів захисту від атак соціальної інженерії, що дозволяє забезпечити майже повний захист інформаційної системи від подібних атак. Окрім того, розгорнута SIEM система WAZUH разом з інтегрованим модулем VirusTotal надає можливості виявлення та протидії майже від усіх видів атак, включаючи атаки із застосуванням соціальної інженерії. Браузер Mozilla Firefox та інтегрований застосунок Startpage Privacy Protection надає повну анонімність перегляду вебсторінок користувачем без ризиків перехоплення персональних даних. Ефективність кожного із запропонованих методів захисту було експериментально підтверджено.

Наступним кроком, було протестовано запропоновану систему комплексного використання засобів захисту від атак соціальної інженерії шляхом проведення тестування на проникнення за допомогою атак соціальної інженерії. У межах експерименту використано певні програмні засоби та змодельовано три види атак для тестування захищеності інформаційних ресурсів, що в результаті дозволило довести ефективність використання запропонованої системи комплексного використання засобів захисту від досліджених атак.

Запропонована система комплексного захисту від атак соціальної інженерії найбільш ефективно працюватиме саме під час використання всіх запропонованих модулів захисту. Відсутність будь-якого з модулів системи знижує загальний рівень захисту інформаційних ресурсів. Експериментально доведено, що тільки у разі спільної роботи всіх модулів досягається захист від атак з використанням оманливого програмного засобу, фішингу, email фішингу та інших.

Список літератури

1. Cost of a data breach 2022 (2022), IBM. **URL**: https://www.ibm.com/reports/data-breach.
2. *Hadnagy C.* (2018), Social Engineering: The Science of Human Hacking. John Wiley & Sons, Inc. 320 p.
3. *Капуста Р. Д., Горяінова К. О.* (2023), Переваги використання SIEM системи WAZUH для підвищення стійкості інформаційної безпеки підприємства. «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем», ПРІТС 2023 : матеріали XV Міжнар. наук.-тех. конф. Київ, 2023. С. 362.
4. Windows Defender logs collection – Malware detection. Wazuh documentation. **URL**: https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/win-defender-logs-collection.html.
5. VirusTotal integration – Malware detection. Wazuh documentation. **URL**: https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/virus-total-integration.html.
6. Розширений захист від стеження у Firefox для комп'ютерів. Довідка Firefox. Mozilla Support. **URL**: https://support.mozilla.org/uk/kb/rozshirenij-zahist-vid-stezhennya-u-firefox-dlya-k?as=u&utm_source=inproduct
7. Яким чином працює вбудований захист від фішингу та шкідливих програм. Довідка Firefox. Mozilla Support. **URL**: https://support.mozilla.org /uk/kb/yakim-chinom-pracyuye-vbudovanij-zahist-vid-fishin.
8. Startpage Privacy Protection for Firefox. Firefox. **URL**: https://addons.mozilla.org/en-US/firefox/addon/startpage-privacy-protection/#:~:text=Startpage%20Privacy%20Protection%20is%20designed,your%20privacy%20and%20tracking%20settings.
9. Kali Linux Tools. Kali Linux. **URL**: https://www.kali.org/tools/msfpc/.
10. An automated phishing tool. GitHub. **URL**: https://github.com/htr-tech/zphisher.
11. Generate professional phishing emails fast and easy. GitHub. URL: https://github.com/BiZken/PhishMailer.