ПОРІВНЯННЯ СЕРВІСІВ ДЛЯ ВИЯВЛЕННЯ ФІШИНГОВИХ ДОМЕНІВ

Стецик Р.[1], Столик Д.[1], Мудрицький І.[1],
Мойко О.[1], Тімошин А.[1]

[1]*Харківський національний університет внутрішніх справ,*
romanstetsyk06@gmail.com, deni.s201811111111@gmail.com,
migor2k05@gmail.com,
Joker-moyko@ukr.net, timxxvii@gmail.com

У роботі аналізуються сучасні сервіси для виявлення фішингових доменів, такі як VirusTotal, Sucuri, Google Safe Browsing API, PhishTank та OpenPhish. Оцінюються їхні можливості та ефективність у боротьбі з кіберзагрозами.

Ключові слова: фішинг, виявлення фішингових доменів, кіберзагрози, VirusTotal, Sucuri, Google Safe Browsing API, PhishTank, OpenPhish

Загроза фішингу та необхідність виявлення фішингових доменів

Фішинг є однією з найбільших загроз, що полягає в шахрайських спробах отримати конфіденційну інформацію, зокрема паролі, номери кредитних карток чи інші особисті дані, через підроблені вебсайти або електронні листи [1]. Такий вид атак може завдати значної шкоди як окремим користувачам, так і організаціям. З огляду на зростаючу загрозу фішингу, виявлення фішингових доменів стало важливим кроком у боротьбі з кіберзлочинністю. Для цього були розроблені спеціалізовані сервіси, що значно підвищують ефективність боротьби з фішинговими атаками, адже дають змогу оперативно виявляти підозрілі сайти та мінімізувати їхній вплив. Використання технологій збору і аналізу даних у реальному часі сприяє значному зниженню ризиків для кінцевих користувачів та організацій. За допомогою пошукової системи Google були знайдені наступні сервіси для виявлення фішингових

доменів: VirusTotal, Sucuri, Google Safe Browsing API, PhishTank, OpenPhish. Ці платформи використовують різні підходи до збору та аналізу даних, включаючи автоматизовані системи сканування, краудсорсинг та інтеграцію з іншими засобами безпеки. Вони дозволяють оперативно виявляти фішингові домени, що допомагає знижувати ризики для користувачів і організацій, а також активно протидіяти фішинговим атакам на глобальному рівні.

Огляд сучасних сервісів для виявлення фішингових доменів

VirusTotal [2] здійснює перевірку об’єктів за допомогою більше ніж 70 антивірусних сканерів та сервісів блокування URL/доменів, а також низки інструментів для збору сигналів із досліджуваного контенту.[3]. На даний момент сервіс користується великою популярністю, станом на серпень 2024 року, VirusTotal щоденно аналізує в середньому 1,2 мільйона унікальних нових файлів, які раніше не були представлені на платформі [4]. VirusTotal використовує кілька потужних інструментів для виявлення фішингових доменів. Система URL/Domain Scanner перевіряє домени за допомогою різних антивірусних та безпекових движків, що дозволяє ефективно виявляти фішингові ресурси. Інтерактивна платформа VirusTotal Graph дозволяє візуалізувати зв'язки між доменами, IP-адресами, файлами та сертифікатами SSL, що дає можливість досліджувати інфраструктуру фішингових кампаній. Крім того, зберігання історії DNS-записів у Passive DNS дає змогу виявляти фішингові домени, що використовують однакові IP-адреси або хостинги. Також підтримка кастомних правил через Livehunt/YARA Rules дозволяє ефективно виявляти фішингові шаблони, такі як підроблені сторінки входу до популярних сервісів, наприклад, PayPal, Google чи Microsoft.

Sucuri – це комплексна хмарна платформа для забезпечення безпеки вебсайтів, яка спеціалізується на виявленні та запобіганні різним видам кіберзагроз, включаючи фішинг [5]. Платформа забезпечує постійний

моніторинг сайтів, аналізуючи вебсторінки на наявність шкідливих скриптів, редиректів, підозрілих форм та інших фішингових елементів. Sucuri пропонує комплексний набір інструментів, спрямованих на виявлення фішингових загроз і забезпечення безпеки вебресурсів. Одним з основних компонентів є SiteCheck Scanner – безкоштовний онлайн-інструмент, який здійснює зовнішній аналіз вебсайтів на наявність шкідливого коду. Він перевіряє вихідний HTML-код, виявляє приховані iFrame, обфускований JavaScript та інші ознаки потенційної компрометації, включаючи фішингові сторінки. Інструмент Website Blacklist Monitoring дозволяє визначити, чи потрапив сайт до чорних списків основних пошукових систем або антивірусних платформ, таких як Google Safe Browsing, PhishTank та інші, що часто сигналізує про наявність фішингового контенту. Окрім клієнтського сканування, Sucuri надає Server-Side Scanner, який виконує поглиблену перевірку на серверному рівні, аналізуючи файли, бази даних та конфігураційні параметри на предмет фішингових елементів, шкідливого ПЗ, бекдорів тощо. Для розробників доступний Scanning API, що дозволяє інтегрувати функціонал сканування до власних систем або додатків, автоматизуючи виявлення фішингових посилань і отримання звітів у реальному часі. Завдяки поєднанню клієнтського, серверного аналізу та API-інтеграції, Sucuri є ефективним рішенням для проактивного виявлення фішингових загроз.

Google Safe Browsing API [6] – це сервіс від компанії Google, призначений для виявлення небезпечних вебресурсів, зокрема фішингових сайтів, сторінок із шкідливим або небажаним програмним забезпеченням. Цей API дозволяє інтегрувати функцію перевірки URL-адрес у клієнтські додатки та сервіси, підвищуючи рівень безпеки користувачів в онлайн-середовищі. Основними компонентами є Lookup API та Update API. Lookup API (v4) дозволяє надсилати URL-адреси на сервери Google для перевірки в реальному часі без необхідності зберігати локальні списки небезпечних сайтів. Цей варіант простий у реалізації, однак має певні обмеження щодо

продуктивності та конфіденційності, оскільки кожен запит надсилається безпосередньо. Натомість Update API (v4) дозволяє клієнтським додаткам завантажувати зашифровані списки небезпечних ресурсів і виконувати перевірку локально. Це підвищує ефективність і забезпечує кращий захист приватності, оскільки URL-адреси хешуються перед обробкою. Обидва інтерфейси активно використовуються в безпекових рішеннях для проактивного виявлення фішингових загроз.

PhishTank [7] – це платформа, яка дозволяє користувачам надсилати підозрілі URL-адреси, що, на їхню думку, є фішинговими. Ці URL перевіряються як автоматизованими системами, так і спільнотою користувачів, що сприяє оперативному виявленню шкідливих ресурсів. Після підтвердження фішингової природи, домен додається до загальнодоступної бази, яку можуть використовувати антивірусні програми, пошукові системи та інші системи безпеки для блокування таких загроз. PhishTank надає низку інструментів для ефективного виявлення фішингових посилань. Основою є спільнота користувачів, які надсилають підозрілі URL-адреси, а також голосують за їхню фішингову природу, сприяючи колективному аналізу загроз. Сервіс також пропонує відкрите API, що дозволяє розробникам інтегрувати перевірку URL-адрес у свої системи безпеки. API підтримує HTTP POST-запити, завдяки чому можна оперативно перевіряти статус підозрілих ресурсів у базі PhishTank. Крім того, доступні завантажувані бази даних з фішинговими доменами у різних форматах, які оновлюються щогодини, забезпечуючи постійний доступ до актуальної інформації для масових перевірок.

OpenPhish [8] автоматично збирає фішингові URL-адреси з різних джерел, аналізує їх за допомогою власних алгоритмів, а також класифікує тип загрози. Сервіс надає доступ до безкоштовного відкритого фіду з оновленням кожні кілька годин, а також комерційний API із розширеним набором даних і метаінформацією, що дозволяє інтегрувати його у системи безпеки для автоматизованого виявлення фішингових атак.

OpenPhish використовує автоматизовані системи виявлення, які на основі внутрішньої структури знань автономно визначають ймовірність того, що URL є фішинговим, що дозволяє забезпечити оперативне реагування без участі людини. Сервіс підтримує постійно оновлювану базу даних фішингових сайтів, яка включає такі параметри, як хостнейми, шляхи, мови сторінок, SSL-метадані, IP-адреси, ASN, країни походження та бренди, що імітуються. Крім того, OpenPhish пропонує спеціалізовані фіди фішингової розвідки з даними про URL-адреси, цільові бренди, географію атак і пов'язані індикатори, що допомагає дослідникам і системам безпеки ефективно відстежувати та аналізувати фішингові загрози.

Висновки

Отже, проаналізовані сервіси – VirusTotal, Sucuri, Google Safe Browsing API, PhishTank, OpenPhish, – демонструють високу ефективність у виявленні фішингових доменів завдяки різним підходам до аналізу, серед яких: краудсорсинг, автоматизоване сканування, API-інтеграція та багаторівневий моніторинг. Усі платформи мають свої переваги й можуть бути корисними залежно від конкретних потреб. Наприклад, PhishTank вирізняється активною участю спільноти, Google Safe Browsing API — простотою інтеграції, а Sucuri — глибоким аналізом вебресурсів. Проте серед усіх рішень найбільш універсальним і функціональним можна вважати VirusTotal, оскільки він поєднує потужні антивірусні сканери, інтерактивну візуалізацію, історичні дані DNS та можливість використання кастомних правил, що робить його незамінним інструментом у сучасній боротьбі з фішингом.

Список використаних джерел

1. Що таке фішинг? Захисний комплекс Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (дата звернення 06.04.2024).

2. VirusTotal. URL: https://www.virustotal.com/gui/home/url (дата звернення 06.04.2024).

3. How it works. URL: https://docs.virustotal.com/docs/how-it-works (дата звернення 06.04.2024).

4. Scaling Up Malware Analysis with Gemini 1.5 Flash. Google Cloud Blog. URL: https://cloud.google.com/blog/topics/threat-intelligence/scaling-up-malware-analysis-with-gemini (дата звернення 06.04.2024).

5. Sucuri – Complete Website Security, Protection; Monitoring. Sucuri. URL: https://sucuri.net (дата звернення 06.04.2024).

6. Overview;| Safe Browsing APIs (v4);| Google for Developers. URL: https://developers.google.com/safe-browsing/v4 (дата звернення 06.04.2024).

7. PhishTank. Join the fight against phishing. URL: https://phishtank.org/ (дата звернення 06.04.2024).

8. OpenPhish – Phishing Intelligence. URL: https://openphish.com/ (дата звернення 06.04.2024).