УДК 004.056.53
О. Семчишин; Р. Козак, к. т. н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДІВ АНАЛІЗУ ШКІДЛИВИХ ПОСИЛАНЬ ТА IP-АДРЕС У СЕРЕДОВИЩІ LINUX

UDC 004.056.53
O. Semchyshyn; R. Kozak, PhD., Assoc. Prof.

METHODS FOR ANALYZING MALICIOUS LINKS AND IP ADDRESSES IN THE LINUX ENVIRONMENT

Сучасні кіберзагрози активно використовують шкідливі URL-посилання та IP-адреси для організації фішингових кампаній, доставки шкідливого програмного забезпечення та підтримання взаємодії з командно-керувальними серверами. Тому важливим завданням є оперативний аналіз таких індикаторів компрометації (IoC) у середовищі Linux, яке широко застосовується для серверів, систем моніторингу та інструментів кіберзахисту[1].

Одним із базових методів є репутаційний аналіз URL та IP через зовнішні сервіси: VirusTotal, AbuseIPDB, URLScan. У середовищі Linux такі сервіси можуть бути інтегровані через API, що дозволяє автоматизувати масову перевірку індикаторів засобами Bash або Python. Використання інструментів curl, jq та системи черг дозволяє формувати конвеєр обробки, у якому кожен елемент проходить оцінку за рівнем ризику.

Другим важливим етапом є локальний динамічний аналіз, що не залежить від зовнішніх платформ. До нього належать інструменти:

- wget – для завантаження та аналізу HTML-вмісту;
- curl -I – для перевірки редиректів та статус-кодів;
- dig та nslookup – для аналізу DNS-структури домену;
- whois – для визначення реєстратора, AS-номеру та країни розміщення IP.

Такі інструменти дають змогу виявити підроблені домени, ознаки фішингу, нестандартні DNS-записи, а також домени– «одноразівки», реєстровані спеціально для атак [2, 3].

Третім етапом є статичний аналіз та зіставлення з існуючими IOC-базами. У Linux широко застосовуються yara, threatfox-cli, локальні списки IP-адрес та URL із MalwareBazaar, ThreatFox, OpenPhish. Це дозволяє створювати власні правила виявлення підозрілих структур, аналізувати шаблони вмісту та виявляти повторювані ознаки шкідливої активності[3].

Передбачається, що поєднання репутаційного, динамічного та статичного аналізу може забезпечити помітно вищу ефективність класифікації шкідливих URL та IP-адрес порівняно з використанням лише зовнішніх сервісів. Такий комплексний підхід, імовірно, дає змогу точніше виявляти підозрілу активність завдяки багаторівневій перевірці індикаторів. DLP системи захищають конфіденційні дані від витоків, контролюючи канали їх передачі та використання. Це дозволяє організаціям та бізнесу мінімізувати ризики фінансових втрат, репутаційних ударів і юридичних проблем.

Література

1. Almomani A., Gupta B., Atawneh S., Meulenberg A. The Scope of Phishing Attacks: A Comprehensive Study. IEEE Communications Surveys & Tutorials. 2013. 29 p.
2. Malicious URLs and IP Address Threat Analysis Report. Palo Alto Networks Unit 42. URL: https://www.content.shi.com/cms-content/accelerator/media/pdfs/palo-alto/palo-alto-122623-unit42-threat-report.pdf (дата звернення: 1.12.2025).
3. A Project from abuse.ch for Malware Samples and IOC Feeds. MalwareBazaar URL: https://bazaar.abuse.ch/statistics/ (дата звернення: 3.12.2024).