ВИЯВЛЕННЯ ОБФУСКОВАНОГО МЕРЕЖЕВОГО ТРАФІКУ В NEXT-GEN SIEM-СИСТЕМАХ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімкий розвиток інформаційно-комунікаційних систем, мережевих технологій та глобальна цифровізація призвели до використання зловмисниками складних векторів атак, що включають використання обфускованих каналів передачі інформації для приховування командно-контрольної інфраструктури (C2) та ексфільтрації даних [1]. Традиційні системи глибокої інспекції пакетів (DPI) та сигнатурного аналізу втрачають ефективність проти сучасних протоколів обфускації, що здатні імітувати легітимний мережевий трафік та підміняти TLS-сертифікати популярних сервісів [2, 3].

Метою дослідження є експериментальна перевірка ефективності систем Next-Gen SIEM на базі Wazuh та Suricata NIDS щодо виявлення обфускованих каналів комунікації, які використовують імітацію легітимних протоколів і підміну TLS-сертифікатів.

У ході практичного експерименту в хмарному середовищі за допомогою стеку Xray було розгорнуто обфускований VPN-тунель із використанням протоколу VLESS та розширення XTLS-Reality. Після цього було налаштовано дзеркалювання трафіку для його подальшого аналізу. Тунель було сконфігуровано з параметрами uTLS: chrome і цільовим доменом google.com для маскування з'єднання. Аналіз метаданих потоку та відбитка TLS-рукостискання системою моніторингу дозволив зафіксувати аномалію: було згенеровано сповіщення «CRITICAL: Xray Reality Anomaly (Malformed TLS Record to google.com)», що відповідає техніці Protocol or Service Impersonation з бази знань MITRE ATT&CK (T1001.003). Це дало змогу виявити підроблений самопідписний TLS-сертифікат, який був згенерований і використаний під час підключення до віддаленого сервера Xray.

Таким чином, проведений експеримент показав, що використання глибокого аналізу метаданих у поєднанні з правилами кореляції Next-Gen SIEM-систем дає змогу частково ідентифікувати сучасні методи обфускації.

Список літератури

1. Сєвєрінов, О.В., Шевцов, В.О., Сокол-Кутиловська, А.С. (2017). Аналіз сучасних методів атак на електронні ресурси органів управління. Системи озброєння і військова техніка, (1), 65-68.

2. M. Fuentes-García, J. Camacho and G. Maciá-Fernández, «Present and Future of Network Security Monitoring». IEEE Access, vol. 9. pp. 112744-112760. 2021. DOI: 10.1109/ACCESS.2021.3067106.

3. Sina Ahmadi. «Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches». International journal of advanced computer science and applications (IJACSA), 15 (3). 2024. DOI: 10.14569/IJACSA.2024.0150301.