АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД ФІШИНГ-АТАКИ BRATA

Логінова А.О., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах, коли кількість мобільних користувачів та обсяг переданих даних стрімко зростають, зловмисники активно використовують вразливості у популярних застосунках для реалізації фішингових атак [1, 2]. Це створює додаткові ризики для фінансових установ і кінцевих користувачів, оскільки атака може відбутися без їхньої активної участі. Прикладом є BRATA (Brazilian Remote Access Tool for Android), яке використовувало критичну вразливість віддаленого виконання коду (RCE) CVE-2019-3568 у WhatsApp та у подальшому інтегрувало інші функції зловмисного контролю над пристроями [3].

Метою дослідження є аналіз використання CVE-2019-3568 у рамках атак BRATA та оцінка ефективності методів захисту шляхом моніторингу VoIP-трафіку і системних журналів, а також визначення можливостей прогнозування подібних атак.

Вразливість CVE-2019-3568 у VoIP-стеку WhatsApp являла собою переповнення буфера, що дозволяло віддалене виконання коду через спеціально сформовані RTCP-пакети.

Вона охоплювала кілька платформ, включаючи Android, iOS, Windows Phone та Tizen. За даними NVD, її рівень небезпеки становив 9.8 (CVSS 3.x, критичний) та 7.5 (CVSS 2.0, високий) [4].

Проведені дослідження підтвердили, що аналіз часових рядів є ефективним для вивчення динаміки фішингових атак. Виявлена наявність довготривалої пам'яті у поведінці атак відкриває можливість прогнозування пікових періодів їх активності.

Встановлено, що середнє добове зростання кількості підтверджених атак становить 3–5%, тоді як у фазах підвищеної активності сплески сягали понад 20% від середнього рівня.

Такі результати свідчать про циклічність та кореляцію у часових інтервалах і створюють підґрунтя для побудови адекватних прогнозних моделей.

На основі цих висновків вводяться практичні заходи протидії: своєчасне оновлення ПЗ до захищених версій та застосування систем аналізу VoIP-трафіку із журналами подій.

Сучасні наукові підходи демонструють ефективність поєднання методів аналізу трафіку з алгоритмами машинного навчання для створення багаторівневих систем захисту.

Щоб зменшити навантаження на сервери, інференс організують каскадно: легкі правила/моделі працюють на всьому потоці, а ресурсоємні CNN або XGBoost застосовуються лише до підозрілих подій (орієнтовно 5–15% у звичайному режимі та 30–40% під час піків завдяки автоскейлінгу). Такий підхід зберігає точність понад 99% і знижує рівень хибнопозитивних

спрацювань до 1–2%, скорочуючи середній час виявлення на 30–40% порівняно з класичними сигнатурними методами.

Додаткову економію забезпечують батчинг і черги для важких перевірок та адаптивне підвищення частоти семплювання на основі журналів VoIP-трафіку.

У тестових середовищах це підвищувало ймовірність раннього виявлення атак до 95% і знижувало ризик компрометації критичних систем на 40–50% [5].

Отримані результати свідчать, що вразливість CVE-2019-3568 є прикладом критичної проблеми безпеки, яка трансформує природу фішингових атак. Запропонований підхід, що базується на поєднанні оновлення ПЗ, моніторингу журналів, прогнозних моделей та гнучких механізмів захисту (каскадні ML-системи та інспекції «рухомого заслону»), одночасно підвищують рівень кіберзахисту та оптимізує використання серверних ресурсів.

Одночасна реєстрація аномальних RTCP-пакетів, відхилень у структурі викликів чи спроб несанкціонованих з'єднань у журналах дозволяє виявляти атаку на ранніх етапах та своєчасно реагувати.

Відповідно до проведених досліджень можна зробити висновок, що з міркувань економії серверних ресурсів доцільно реалізувати не «монолітну стіну», а «рухомий заслін» перевірок: динамічно змінювати глибину інспекції й частку вибіркового аналізу залежно від прогнозованої активності (наприклад, 5–10% семплювання у між-пікові години та 60–80% — у «вікна ризику»), автоматично масштабуючи модулі аналізу і вмикаючи повну перевірку лише під час очікуваних сплесків.

Це доводить доцільність комплексної багаторівневої стратегії, яка поєднує превентивні й реактивні заходи та дозволяє ефективніше протидіяти новітнім фішинговим атакам.

Список літератури

1. Сєвєрінов, О. В., Хрєнов, А. Г., & Поляков, А. О. (2015). Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. Системи обробки інформації, (9), 101-104.

2. 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.

3. McAfee. Beware of BRATA: How to Avoid Android Malware Attack. – 2023. – URL: https://www.mcafee.com/learn/beware-of-brata-how-to-avoid-android-malware-attack/

4. NVD. CVE-2019-3568. - URL: https://nvd.nist.gov/vuln/detail/CVE-2019-3568

5. Дейнеко Ж., Драз Д. Дослідження динаміки фішингових атак методом вейвлет-аналізу // Тези доповідей 4-ї Міжнародної науково-технічної конференції «Інформаційні системи та технології» (ICT-2018), Харків, ХНУРЕ, 2018. - Секція «Захист інформації. Інформаційна безпека». - С. 396–397.