ПОВЕДІНКОВІ ІНДИКАТОРИ КОМПРОМЕНТАЦІЇ ТА МЕТОДИ ДЕТЕКЦІЇ ФІШИНГОВОЇ АТАКИ BRATA В СЕРЕДОВИЩІ ANDROID

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

Операційна система Android є однією з найпоширеніших платформ для мобільних пристроїв у світі. Її популярність обумовлена відкритістю, гнучкістю та широкими можливостями кастомізації, що сприяє активному використанню як у споживчому секторі, так і в корпоративному середовищі.

Але зростання популярності Android безпосередньо впливає на їх безпеку.

Найбільш поширеними загрозами є malware (трояни, spyware), фішингові атаки, перехоплення даних, несанкціонований доступ до пристрою, вразливості в застосунках [1, 2].

Фішингові атаки на мобільні пристрої використовують підроблені інтерфейси або повідомлення для отримання конфіденційних даних; близько 30–40% мобільних інцидентів пов'язані із соціальною інженерією. Зростання таких загроз зумовлене активним використанням смартфонів у фінансових операціях, а кількість атак щорічно зростає на 15-25% [3].

Особливу небезпеку становить шкідливе ПЗ класу Remote Access Trojan, зокрема BRATA, що поєднує фішинг і віддалене керування пристроєм та маскується під легітимні застосунки для прихованого перехоплення даних [4].

Метою дослідження є визначення поведінкових індикаторів компрометації BRATA та аналіз методів її виявлення на основі статичного, динамічного й мережевого аналізу.

Визначення поведінкових характеристик BRATA здійснювалося шляхом поєднання статичного, динамічного та мережевого аналізу відповідно до сучасних підходів, описаних у звітах ENISA та рекомендаціях OWASP Foundation.

Статичний аналіз дозволив дослідити структуру застосунку, перелік дозволів, виклики API та використання служб доступності. Динамічний аналіз у контрольованому середовищі забезпечив спостереження за реальною поведінкою програми під час виконання, включаючи взаємодію з інтерфейсом користувача та ініціювання мережевих з'єднань. Мережевий аналіз доповнив дослідження шляхом виявлення шаблонів взаємодії з командними серверами та інтенсивності передачі даних, що узгоджується з результатами досліджень ThreatFabric і Cleafy. Такий підхід допомагає сформувати повний профіль поведінки шкідливого застосунку.

Аналіз функціонування BRATA показує, що програма використовує приховування структури коду, динамічне завантаження компонентів і служби доступності Android для отримання контролю над інтерфейсом пристрою [5]. У шкідливих застосунках такі механізми застосовуються у 70-90% випадків, тоді як у легітимних - лише у 5-10%. Крім того, BRATA взаємодіє з командними серверами (C2) та передає зібрані дані.

Індикаторами компрометації є надмірна кількість дозволів (20-30 проти 8-15), використання служб доступності без необхідності, інтенсивна мережева активність (до 30-40 запитів за хвилину), приховування іконки та підвищена фонова активність.

Для оцінки ефективності виявлення зазначених ознак проведено порівняльний аналіз методів детекції (таблиця 1).

Таблиця 1 - Порівняльний аналіз методів детекції

Метод аналізу	Предмет аналізу	Виявлення ознак BRATA	Виявлення інших атак
Статичний	Код, структура APK, дозволи, API	Надмірна кількість дозволів, використання служб доступності, підозрілі компоненти	Банківські трояни, шпигунське ПЗ, рекламне ПЗ
Динамічний	Поведінка під час виконання	Фонова активність, взаємодія з UI, C2	RAT, шпигунське ПЗ, кейлогери
Мережевий	Трафік, домени, частота запитів	Інтенсивні запити, C2-з'єднання	Ботнети, шкідливе ПЗ для викрадення даних

Аналіз показав, що статичний метод є швидким і малоресурсним, але обмеженим через механізми приховування, динамічний - більш точним, проте ресурсоємним, тоді як мережевий дозволяє виявляти приховану активність, але ускладнюється при шифруванні трафіку.

У сукупності їх застосування забезпечує ефективну та універсальну основу для подальшого розвитку систем виявлення мобільних кіберзагроз.

Список літератури

1. Сєвєрінов, О. В., Федорченко, В. М., Перепадя, В. І., Северинов, А. В., Федорченко, В. Н., & Перепадя, В. И. (2016). Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків.

2. Сєвєрінов, О. В., Федоров, І. А., & Власов, А. В. Аналіз методів детектування шкідливого програмного забезпечення // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей чотирнадцятої міжн. наук.-техн. конф., 25 – 26 квітня 2024 року. - Баку – Харків – Жиліна – 2024

3. ENISA. Threat Landscape Report 2023. - 2023. - URL: https://www.enisa.europa.eu/

4. ThreatFabric. Brata: a tale of three families. - 2022. - URL: https://www.threatfabric.com/blogs/brata-a-tale-of-three-families

5. Cleafy. BRATA is evolving into an Advanced Persistent Threat. - 2021. - URL: https://www.cleafy.com/cleafy-labs/brata-is-evolving-into-an-advanced-persistent-threat