ОБХІД МОБІЛЬНИХ СИСТЕМ ВИЯВЛЕННЯ ЧЕРЕЗ ІМІТАЦІЮ ПОВЕДІНКИ ЛЕГІТИМНИХ ДОДАТКІВ

Стеблина Олександр Станіславович
студент групи ІАСм -1-24-1.4д,
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Мельник І.Ю.

Сьогодні мобільні пристрої стають основною ціллю для зловмисників, і кількість атак на них стрімко зростає. За даними дослідників, лише протягом 2024 року засоби безпеки заблокували понад 33 мільйони випадків мобільного шкідливого програмного забезпечення [1]. На цьому тлі особливо актуальною є проблема обходу систем виявлення шкідливим ПЗ. Сучасні мобільні трояни та віруси дедалі частіше використовують маскування під легітимні додатки, щоб залишатися непоміченими для антивірусів і захисних механізмів. Зловмисні програми імітують вигляд і поведінку справжніх застосунків – наприклад, банківських або соціальних – та розповсюджуються поза офіційними магазином Google Play

Мобільні пристрої активно атакуються шкідливим ПЗ, яке часто маскується під легітимні додатки для обходу захисних систем. Основні техніки включають:

Трояни: створення майже ідентичних копій легітимних додатків із прихованим шкідливим кодом. Це особливо актуально для популярних додатків з відкритим чи умовно-відкритим кодом. Один з прикладів - нещодавно хвиля клонів месенджерів Telegram з буцім-то додатковим функціоналом [2]. Ці додатки таргетувалися на дітей і підлітків і рекламувалися через популярні соціальні мережі.

Накладення елементів: демонстрація підроблених інтерфейсів поверх справжніх додатків чи інтернет-сторінок для викрадення даних або використання їх як стілеру для вводів користувача. Наприклад, банківський троян Anubis демонструє форму логіну, коли жертва відкриває справжній банківський додаток: поверх з’являється підроблена форма входу, в яку користувач вводить облікові дані, що одразу пересилаються хакерам [3].

Використання бренду: застосування офіційних іконок та назв відомих програм, або введення користувача в оману з їх допомогою. Найбільше це актуально для сфери криптовалют і казино та найчастіше виражається у використанні айдентики компаній без ліцензій [4].

Шкідливе ПЗ також активно використовує Android API та системні виклики, щоб імітувати звичайну поведінку додатків, вводячи в оману антивіруси та захисні механізми. Воно може активно викликати ті ж системні функції, що й типовий легітимний додаток, щоб його поведінковий профіль не викликав підозр. Наприклад, шкідливий застосунок, маскуючись під сервіс геолокації, буде регулярно викликати LocationManager для отримання координат користувача, як це роблять карти або погодні додатки. Якщо троян видає себе за месенджер або соцмережу, він може використовувати NotificationManager для постійної генерації спливаючих повідомлень “нових

повідомлень", підтримуючи ілюзію активної легітимної діяльності. Вся справжня шкідлива функціональність при цьому прихована глибше в коді і маскується під ці звичайні виклики API. Крім того, зловмисники можуть використовувати системні дозволи: наприклад, доступ до Accessibility Service дозволяє програмі автоматично натискати кнопки, вводити текст або читати вміст екрану – усе це з легітимними цілями на кшталт сервісів для людей з інвалідністю, але водночас відкриває можливості для прихованого керування пристроєм [5].

У цьому дослідженні я розглянув техніку імітації поведінки як засіб обходу систем виявлення на Android. Основний висновок полягає в тому, що маскування під легітимні додатки є надзвичайно ефективною стратегією для зловмисників. Шкідливе ПЗ, яке вміло копіює поведінку, інтерфейс та взаємодію справжніх програм, може довгий час залишатися непоміченим: воно не видає себе ані дивними діями, ані зовнішнім виглядом. Такі трояни, як Anubis, SharkBot, XLoader та інші, на практиці продемонстрували, що навіть офіційні маркети й захисні сервіси можуть бути обійдені, якщо шкідливе програмне забезпечення добре замасковано і динамічно приховує шкідливі функції. Проведений аналіз вказує на те, що протидія таким витонченим загрозам потребує вдосконалення підходів до детекції: впровадження поведінкового аналізу з використанням ML, аналіз послідовностей API-викликів та дій, поліпшення sandbox-тестування та валідації легітимності інтеграцій.

ДЖЕРЕЛА

1. Mandvi. 33.3 Million Cyber Attacks Targeted Mobile Devices in 2024 Amid Rising Threats. Cyber Security News. URL: https://cyberpress.org/33-3-million-cyber-attacks-targeted-mobile-devices/ (date of access: 04.04.2025).

2. Inside FireScam : An Information Stealer with Spyware Capabilities - CYFIRMA. CYFIRMA. URL: https://www.cyfirma.com/research/inside-firescam-an-information-stealer-with-spyware-capabilities/ (date of access: 04.04.2025).

3. Toulas B. Anubis Android malware returns to target 394 financial apps. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/anubis-android-malware-returns-to-target-394-financial-apps/ (date of access: 04.04.2025).

4. Rao A. Illegal gambling websites are phishing Google Play users - Eydle Scam Protection Platform. Eydle Scam Protection Platform. URL: https://www.eydle.com/illegal-gambling-scamming-google-play-users/ (date of access: 04.04.2025).

5. Бондарчук, А. П., Складанний, П. М., Жебка, В. В., & Стражніков, А. А. (2024). Оптимізація системи зарядки електромобілів на основі методів дослідження операцій. Телекомунікаційні та інформаційні технології, 84(3), 86-93.