Шкідливе програмне забезпечення на мобільних пристроях та підходи до його дослідження

Євген Панов

головний судовий експерт сектору
комп'ютерно-технічних та телекомунікаційних досліджень,
Сумський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України,
м. Суми, Україна, e-mail: exp.peo@gmail.com

Розглянуто сучасні операційні системи на мобільних пристроях, шкідливе програмне забезпечення та підходи до його дослідження.

Ключові слова: *мобільні віруси; шкідливі програми; android, iOS.*

Malware on Mobile Devices and Approaches to Its Research

Yevhen Panov

This work examines modern operating systems on mobile devices, malicious software and approaches to its research.

Keywords: *mobile viruses, malware, android, iOS.*

Дослідження шкідливого програмного забезпечення на мобільних пристроях дуже важливе завдання в галузі кібербезпеки. Мобільні застосунки стають все більш популярними у користувачів, вони містять велику кількість особистої інформації, що може бути викрадена зловмисниками.

Станом на сьогодні найпопулярнішими операційними системами для мобільних пристроїв є *Android* та *iOS*.

Android — це операційна система, яка була розроблена компанією *Google*. Вона безкоштовна та відкрита для користування, тому вона стала дуже популярною у виробників смартфонів, планшетів та інших ґаджетів. Більшість мобільних пристроїв, що випускаються сьогодні, працюють на операційній системі *Android*.

iOS — це операційна система, яка була розроблена компанією *Apple*. Вона пропріетарна та доступна тільки для користування на пристроях *Apple*, таких як *iPhone* та *iPad*. Проте завдяки своїй популярності та інноваційним можливостям *iOS* також стала дуже популярною в користувачів смартфонів.

Інші операційні системи для мобільних пристроїв, такі як *Windows Phone*, *BlackBerry* та *Symbian OS*, були популярні в минулому, але сьогодні користування ними дуже обмежене.

Мобільне шкідливе програмне забезпечення (mobile malware) — це програми або модулі, які роблять небажані / шкідливі дії на смартфоні: крадуть дані, шпигують, вимагають викуп, показують рекламу, дають віддалений доступ тощо. У 2023—2025 роках відбувається значне зростання складних атак (стелс-*spyware*, *stealer*'и, dropper'и)

та активність проти як *Android*, так і *iOS* екосистем.

Основні типи мобільного malware:

1) трояни-дроппери *(dropper)*: доставляють і установлюють інші модулі;
2) *Banking trojans / stealers*: перехоплюють вхідні дані, *SMS*-коди, скріншоти;
3) *Spyware / mercenary spyware* (програмне забезпечення для стеження): дуже потужні, часто експлуатують *0-day* в ОС;
4) *Stalkerware / stalker-apps*: простіші «шпигуни» для стеження за користувачем;
5) *Ransomware*: шифрують або блокують пристрій / файли;
6) *Adware / PUA (Potentially Unwanted Apps)*: агресивна реклама, збір аналітики;
7) *Malware* із *OCR* / скриншот-крадіжкою (нові приклади на *iOS* у 2024).

Як заражають мобільні пристрої (поширені вектори):

1) шкідливі або перепаковані додатки (у *Google Play* / сторонніх магазинах / репозитаріях);
2) фішингові повідомлення / підробні оновлення / *SMS (smishing)*;
3) експлойти в уразливостях ОС (застосовують в *mercenary spyware*);
4) зловмисний сайт *(drive-by)*, компрометація довірених *SDK* або *ads-network*.

Підходи до дослідження мобільного шкідливого ПЗ:

1) ізоляція та безпека — дослідження тільки в ізольованому середовищі (виртуалка / лабораторний девайс), відключити особисті акаунти, мережу або проксувати через контрольований *VPN/mitm*;
2) збирання зразка та первинна розвідка *(triage)*. Для *Android*: отримати APK; перевірити підписи, *manifest.xml*, список дозволів, *certificate*. Для *iOS*: *IPA* / файли бандлу, бінарні файли;
3) статичний аналіз (швидкий, без виконання):
   - *APK — apktool* (ресурси, *manifest*), *jadx* (декамп), strings, перегляд *native-libs (.so)* в *Ghidra/IDA*;
   - шукати *hardcoded URL*, *API*-ключі, родичі доменів, права доступу, методи обходу безпеки *(reflection/ obfuscation)*;
4) динамічний аналіз *(run-time)*:
   - запуск в емуляторі або на інструментованому девайсі; інструменти: *Frida* (динамічні хуки), *Xposed* / реплей інструменти для *Android*, *LLDB/Frida* для *iOS*. Логування системних викликів, файлових операцій, *IPC*, мережі;
   - захоплення трафіку через *mitmproxy/Burp* (можливо, треба обійти *SSL-pinning* через *Frida*);
5) аналізування нативного коду та експлойтів. Дослідити *.so* або *Mach-O* бінарі на предмет експлойтів, уразливих викликів, *shellcode*. Застосовують *Ghidra/ IDA/objdump*;

6) пам'ять та форензика. Можна взяти дані пам'яті процеса, шукати ключі / токени / розшифровані рядки; для *iOS* корисні інструменти *Corellium* (або реальний *device + jailbreak*);
7) автоматизація і *sandboxing*. Застосовують *sandboxes* / автоматичні платформи (*Cuckoo-like* або спеціальні мобільні *sandboxes*) для виконання великої кількості зразків і побудови ознак поведінки. Гібридні підходи *(static + dynamic)* дають кращу точність;
8) *IOC / threat intelligence* — зібрані індикатори (хеші, домени, *IP*, *URL*, юніт-поведінки) оформлюють та корелюють з публічними базами *(VirusTotal, ThreatIntel feeds)*;
9) класифікація / машинне навчання (опціонально) — ознаки (*permissions*, *API*-виклики, графи викликів) подають у моделі для автоматичної класифікації / кластеризації.

Корисні інструменти для дослідження:

1) статичний: *apktool, jadx, dex2jar, strings, Ghidra, IDA*;
2) динамічний / інструментування: *Frida*, *Objection (Android/iOS)*, *Xposed* (де потрібно), *adb*, *lldb*;
3) мережа / форензика: *mitmproxy, Burp Suite, tcpdump, Wireshark*;
4) *Sandbox* / платформи: *Corellium*, мобільні *sandboxes* (дослідницькі проєкти та комерційні рішення).

Практичні поради й типові пастки:

1) *Obfuscation / packing*: автори *malware* маскують код *(proguard, custom packers, native loaders)*. Поєднувати статичний і динамічний аналіз;
2) *Anti-emulator / anti-instrumentation*: зразки перевіряють оточення і «сплять» за виявлення емулятора — потрібні інструменти для емуляції реальної поведінки або дослідження на інструментованому реальному пристрої;
3) юридичні / етичні обмеження: не запускати шкідливі зразки в мережі, де є реальні користувачі; пам'ятати про приватність і закони про зберігання / оброблення даних;
4) оновлення середовища: слідкувати за *CVE* й оновленнями операційної системи: багато атак експлуатують відомі дірки (оновлення пристрою — важливий захист).