Шкідливе програмне забезпечення мобільних пристроїв і підходи до його дослідження

Євген Панов,
Сумський НДЕКЦ МВС України, м. Суми, Україна, e-mail: exp.peo@gmail.com

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

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

Mobile malware and approaches to its investigation

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 є дуже важливим завданням у галузі кібербезпеки. Мобільні додатки набувають усе більшої популярності в користувачів, вони містять безліч особистої інформації, яку можуть викрасти зловмисники.

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

Android — це операційна система, розроблена компанією *Google*. Вона є безкоштовною та відкритою для використання, тому дуже популярна у виробників смартфонів, планшетів та інших ґаджетів. Більшість мобільних пристроїв, які випускають сьогодні, працюють на операційній системі *Android*.

iOS — це операційна система, розроблена компанією *Apple*. Вона є пропрієтарною й доступна тільки для використання на пристроях *Apple* — *iPhone* та *iPad*. Проте (зокрема, завдяки інноваційним можливостям) *iOS* також дуже популярна у користувачів смартфонів.

Інші операційні системи для мобільних пристроїв (такі, як *Windows Phone, BlackBerry* та *Symbian OS*), популярні в минулому: сьогодні їх використання дуже обмежене.

Існує безліч різних вірусів, які можуть атакувати пристрої на платформі *Android*. Деякі з найпоширеніших програм-вірусів на *Android*:

- *Hummingbad* — шкідлива програма, установлювана без відома власника пристрою, яка відправляє спам і краде особисту інформацію;
- *Android/SMSSend* — вірус, який відправляє автоматичні текстові повідомлення на платні номери, що може збільшити рахунки за мобільний зв'язок;
- *Andr/Clickr-ad* — вірус, який відображає небажану рекламу на вашому телефоні та може сповільнити його роботу;
- *Android/FakeAV* — шкідлива програма, яка виглядає як антивірусна, але насправді вона, зокрема, краде особисту інформацію;
- *Android/Spy.Agent.SI* — вірус, який може відстежувати вашу активність на телефоні, красти особисту інформацію й надсилати її зловмиснику;
- *BankBot* — вірус, розроблений для крадіжки фінансових даних. Він може вивчити інформацію про банківські карти, паролі й інші фінансові дані користувача.

Інформаційні віруси (*malware*) для операційної системи *iOS* виявляють дуже рідко (через високу безпеку, яку надає сама операційна система). Водночас, хоча віруси на *iOS* не такі поширені, як на Android, вони все ще існують і можуть шкодити пристрою та даним користувача. Деякі з найпоширеніших шкідливих програм-вірусів на *iOS*:

- *XcodeGhost* — шкідлива програма, що потрапила в *App Store*, вона створює незвичайні запити до серверів зловмисників, які можуть призвести до витоку конфіденційної інформації користувачів;
- *WireLurker* — вірус може вплинути на *Mac*-комп'ютер і перенестися на ваш iOS-пристрій, використовуючи порт *USB*, що може надати зловмисникам доступ до вашого пристрою та конфіденційної інформації;
- *Masque Attack* — шкідлива програма, яка може проникнути у ваш пристрій через завантаження додатків із підозрілих джерел замість *App Store*. Цей вірус замінює легітимні додатки шкідливими копіями, що може

призвести до витоку конфіденційної інформації;

- *Pegasus* — програма-шпигун, здатна перехоплювати приватну інформацію, включно з паролями, повідомленнями та зображеннями. Його можуть установити на ваш пристрій через текстові повідомлення та незначні вразливості.

Дослідити віруси на мобільних додатках можна в різний спосіб, зокрема:

1) статичний аналіз — цей підхід використовують для дослідження коду додатка без запуску програми на мобільному пристрої. За допомогою статичного аналізу можна виявити потенційно небезпечні дії в коді (наприклад, використання не захищених каналів зв'язку, витік конфіденційної інформації та ін.);
2) динамічний аналіз — полягає в запуску додатка на мобільному пристрої з наступним моніторингом його поведінки. Динамічний аналіз дає змогу виявляти небезпечні дії, які додаток виконує в реальному часі (наприклад, відправлення *SMS*-повідомлень або створення підключення до віддаленого сервера);
3) реверс-інженерія — цей підхід використовують для аналізу збірки додатка, щоб отримати розуміння його внутрішньої структури та функцій. Реверс-інженерія дає змогу виявляти небезпечні функції (наприклад, виклики системних функцій, які можна використати для викрадення конфіденційної інформації);
4) аналіз мережевої діяльності — полягає в аналізі мережевого трафіку, що генерується додатком на мобільному пристрої. Аналіз мережевої діяльності дає змогу виявляти відправлення додатком конфіденційної інформації на зовнішні сервери або здійснення небезпечних дій.

Кожен із цих підходів має свої переваги й недоліки, тому для ефективного виявлення вірусів на мобільних додатках доцільно використовувати комбінацію цих підходів. Важливо зауважити, що досліджувати віруси на мобільних додатках слід із дотриманням законодавства та правил конфіденційності.

Перелік джерел посилання

1. Srinivasan S., Saravanan R. Mobile Malware and its Evolution. *International Journal of Computer Science and Mobile Computing*. 2015. Vol. 4. Is. 4. Pp. 258—265.
2. Alzahrani N. A Survey of Mobile Malware and Security Solutions. *Ibid*. Is. 2. Pp. 553—563.
3. Naik S. H., Bhatkar V. S. Mobile Malware: A Comprehensive Survey. *International Journal of Computer Applications*. 2014. Vol. 95. No. 16. Pp. 20—26.

Напрями удосконалення методики розслідування кримінальних правопорушень у сфері обліку військового майна

Ігор Папуша,
канд. юрид. наук, доцент, заслужений юрист України, Військова академія, м. Одеса, Україна

Досліджено актуальні проблеми удосконалення методики розслідування кримінальних правопорушень у сфері обліку військового майна. Обгрунтовоно, що практика протидії злочинності у сфері обліку військового майна зумовлює необхідність формування комплексної криміналістичної методики, що має спільний предмет посягання, подібну об'єктивну сторону їх вчинення та свою специфіку розслідування.

Ключові слова: методика розслідування; криміналістичні знання; кримінальні правопорушення у сфері обліку військового майна; тактичні операції; судові експертизи.

Directions for improving the methodology of investigating criminal offenses in the field of accounting for military property

Ihor Papusha

Significant issues for improving the methodology of investigating criminal offenses in the field of accounting for the military property are explored. It is well-founded that the practice of countering crime in the field of accounting for military property necessitates the formation of a complex forensic methodology that has a common object of encroachment, a similar objective aspect of their commission, and its own specificity of investigation.

Keywords: methodology of investigation, forensic knowledge, criminal offenses in the field of accounting for military property, tactical operations, forensic examinations.