Секція 1

АНАЛІЗ ЗАГРОЗ СПРЯМОВАНИХ НА МОБІЛЬНІ ПРИСТРОЇ

Литвинов О. А.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В.Я.

Актуальність. На даний момент у світі прогресує кількість смартфонів у світі, люди все більше взаємодіють саме з смартфонами та планшетами на ОС IOS та android. Кількість можливостей, що надаються мобільними пристроями, набагато більша, ніж у традиційних мобільних телефонів: вони мають встановлену мобільну операційну систему (iOS, Android) і можуть працювати як з мережами мобільного зв'язку, так і з бездротовими технологіями Wi-Fi та Bluetooth, завдяки чому користувачі можуть завантажувати та запускати сторонні програми використовуючи мережу Інтернет. Серед інших особливостей мобільних пристроїв відзначається підтримка сервісу мультимедіа повідомлень (MMS) та наявність вбудованих датчиків: гіроскоп, приймач сигналів GPS, акселерометр, а також мікрофон, камера з великою роздільною здатністю та динамік. Через це все більше критично важливих застосунків з’являються на цих пристроях, такі як, мобільний банкінг, або «Дія» у якій знаходяться персональні дані користувача пристрою. Як наслідок, зацікавлені в розробці шкідливого ПО та подальшого зараження ним мобільного пристрою. А розробники антивірусів навпаки зацікавлені в запобіганні подібних інцидентів. Саме для цього треба спочатку проаналізувати можливі загрози спрямовані на мобільні пристрої.

Мета. Переглянути статистику за перші квартали 2021 року та 2022 року та проаналізувати зростання чи спадання популярності тих чи інших загроз та можливість залежності популярності тих чи інших зловмисних ПО від навколишніх обставин.

Основні положення. Шкідливе програмне забезпечення – це будь-який код, що може поставити під загрозу користувача, його дані чи пристрій. До шкідливого ПО належать, зокрема, потенційно шкідливі додатки, двійкові коди та модифікації фреймворків, серед яких можна виділити категорії троянських програм, фішингових і шпигунських додатків.[1] Ці типи зловмисного програмного забезпечення покладаються на використання конкретних мобільних операційних систем і технологій мобільних телефонів. Розробники шкідливого ПО для мобільних пристроїв, яких також називають кіберзлочинцями, можуть мати одну або кілька цілей,

зокрема викрадення даних, підписання користувачів на послуги та стягнення з них плати за послуги, на які вони не погоджувалися, або блокування пристрою чи даних і вимагання грошей за їх не оприлюднення. Додаток, двійковий код чи модифікація фреймворку можуть бути потенційно шкідливі, навіть якщо їх не розроблено як зловмисні програми. Причина полягає в тому, що функції додатків, двійкових кодів і модифікацій фреймворків відрізняються залежно від багатьох змінних параметрів. Тому поведінка, шкідлива для одного пристрою Android, може не становити загрози для іншого. Згідно зі звітом про глобальні ризики Всесвітнього економічного форуму за 2022 рік, 95% проблем кібербезпеки пов'язані з людською помилкою [2]. Це є тривожним сигналом для всіх організацій, особливо з переходом на віддалену та гібридну роботу, коли співробітники частіше використовують мобільні пристрої. Тепер ці пристрої мають доступ до конфіденційних даних компанії та пряме підключення до корпоративної мережі.

Висновки. Отже після аналізу статистики зараження мобільних пристроїв можна зробити висновок. Найпопулярніші типи зловмисних програм це RiskTool, AdWare, Trojan, та Trojan-Banker. Всі вони направлені на масового користувача, на якому можливо заробити, або показуючи йому рекламу, або скриваючи/погрожуючи видалити файли, але випадок с файлами все ж ситуативний не у всіх користувачів є щось дійсно важливе на телефоні що не можна відновити. Але наприклад майже у всіх користувачів є мобільний банкінг, що як раз є цілю Trojan-Banker. Тому на мою думку, в сегменті масового користувача, антивіруси повинні дуже сильно розвиватись у направленні цих чотирьох направленнях шкідливих програм.

Список літератури

1. Malware - Play Console Help. *Google Help.* URL: https://support.google.com/googleplay/android/developer/answer/9888380 (дата звернення: 23.11.2022);
2. Зловмисне ПЗ для мобільних пристроїв у 2022 році. *KO IT для бізнесу.* URL: https://ko.com.ua/zlovmisne_pz_dlya_mobilnih_pristroyiv_u_2022_roci_142676 (дата звернення: 23.11.2022).

Відомості про авторів

Литвинов Олександр Андрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-304-66-95, a.lytvynov@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu