УДК 004.05

Олександр Вадимович ПИЛИПЕНКО,
судовий експерт відділу комп'ютерно-технічних та телекомунікаційних досліджень
Харківського науково-дослідного експертно-криміналістичного центру МВС України

ІНФОРМАЦІЙНА БЕЗПЕКА СМАРТФОНІВ

За останнє десятиліття смартфони стали невід'ємною частиною повсякденного життя сучасної людини. Безумовно, велику роль в цьому грає інформатизація у всіх сферах людської діяльності. Зараз дуже важко представити собі банк без онлайн банкінгу в смартфоні, онлайн магазин без мобільного додатку або вебсайту, оптимізованого під перегляд на мобільних пристроях, навіть для повсякденного онлайн спілкування все менше використовують стаціонарні комп'ютери або ноутбуки – усі популярні сервіси для онлайн спілкування давно є в смартфонах. І це не дивно, адже смартфон завжди під рукою, і не просто смартфон, а смартфон із доступом до мережі інтернет.

Приїжджаючи в інше місто або іншу країну, не знаючи місцевості, не маючи змоги спитати про місцезнаходження найближчого готелю, банкомату або необхідної автозаправної станції потрібно лише відкрити карту на своєму смартфоні і ситуація відразу змінюється. Зовсім нещодавно важко було уявити віддалену роботу та роботу в офісному програмному забезпеченні без ноутбука з доступом до мережі інтернет, проте і тут смартфон стає в нагоді – все офісне програмне забезпечення зараз адаптоване під мобільні платформи, а розміри дисплеїв дозволяють досить комфортно працювати з документами, вести листування електронною поштою та мессенджерами.

За допомогою смартфонів сучасна людина спілкується, працює, відпочиває, грає, вчиться, слідкує за своїм здоров'ям, проводить різноманітні оплати, за допомогою смартфону створює та зберігає фото та відео, як особисті, так і комерційного характеру, зберігає багато приватних даних, наприклад, логіни, паролі або PIN коди банківських карток. Багато користувачів не задумуються про інформаційну безпеку своїх пристроїв та навіть не знають, що багато цінної інформації може бути викрадено в результаті використання відкритої мережі Wi-Fi в улюбленому кафе.

Також користувач не завжди використовує парольний, графічний або біометричний захист, використання таких мір безпеки значно підвищує шанс на збереження особистих даних, хоча це і не панацея, дуже часто в авторитетних виданнях можна зустріти інформацію про те, що в мобільних телефонах тієї чи іншої компанії виявлено чергову помилку в операційній системі, через яку зловмисники можуть з легкістю отримати повний доступ до інформації в смартфоні.

Почнемо з того, що означає термін "вразливість нульового дня". Вразливістю нульового дня (англ. Zero day, 0day) називають вразливість програмного забезпечення, на виправлення якої у розробників було нуль днів, тобто до моменту випуску виробником патчу безпеки дана вразливість стає публічно відомою [1]. Нижче буде розглянуто деякі найбільш відомі останні проблеми в безпеці смартфонів.

Наприкінці 2019 року компанія Google зробила заяву, що знайшла докази того, що вразлива версія їх операційної системи Android, в якій знайшли вразливість нульового дня, наразі використовується у світі [2]. Вразливість знаходиться на рівні коду ядра операційної системи і може використовуватись зловмисниками для отримання root-доступу до смартфону (під root-доступом розуміють отримання привілей суперкористувача, власник яких може виконувати всі без винятку операції та має доступ до всіх даних на пристрої). Компанія протестувала дану вразливість на деяких своїх смартфонах Google Pixel та на деяких смартфонах компаній Samsung, Xiaomi, Huawei, Oppo, Motorola. Також дослідники Google заявили, що дана вразливість не потребує індивідуальних налаштувань під кожен пристрій, що може означати дієздатність даної вразливості на великій кількості пристроїв. Для потенційної експлуатації даної вразливості користувач лише повинен встановити шкідливий додаток.

Багато користувачів мобільних телефонів компанії Apple вважають, що їх смартфони не схильні по атака зловмисників. Проте таке твердження досить помилкове. Наприкінці літа 2019 року група спеціалістів Project Zero (група спеціалістів безпеки Google, яка займається пошуком вразливостей нульового дня) опублікувала статтю [3], в якій публікується про масштабну атаку на iOS пристрої, яка тривала щонайменше два роки. Користувачу треба було лише відвідати зламаний вебсайт, як мобільний пристрій відразу атакувався сервером експлойтів (від слова «експлуатувати» - послідовність команд, які використовують

вразливості програмного забезпечення) для подальшого моніторингу за мобільним пристроєм. Такий вебсайт був не один, і щотижня їх відвідувало тисячі користувачів. Зловмисники могли впровадити в систему код, який дозволяв обходити систему keychain, яка зберігає та захищає конфіденційну інформацію - логіни, паролі, дані банківських карток і так далі. Слід відмітити, що за допомогою обходу даного захисту зловмисники могли отримувати доступ до будь-яких даних в системі, навіть до баз даних месенджерів с шифруванням даних. Загалом дослідники компанії Google знайшли 14 вразливостей та 5 ланок експлойтів, за допомогою яких можна було отримати доступ до операційної системи iOS від десятої до останньої (на той час 12) версій.

Слід завжди брати до уваги той факт, що людина завжди є найслабшою ланкою в інформаційній безпеці. Це твердження справедливо як до людей які створюють програмне забезпечення, так і до звичайних користувачів. Коли людина пише код програми, вона допускала, допускає і завжди буде допускати помилки, а коли їх знайде зловмисник – це лише питання часу. Завжди треба давати звіт своїм діям як звичайного користувача – не встановлювати додатки з ненадійних джерел, не переходити по підозрілим посиланням, не відповідати на підозрілі SMS повідомлення, не зберігати паролі в нотатках та на фотографіях, використовувати лише надійні та різні паролі.

Список бібліографічних посилань

1. Вразливість нульового дня // Вікіпедія : віл. енцикл. URL: https://uk.wikipedia.org/wiki/вразливість_нульового_дня (дата звернення: 23.04.2020).
2. Cimpanu C. Google finds Android zero-day impacting Pixel, Samsung, Huawei, Xiaomi devices // ZDNet. 04.10.2019. URL: https://www.zdnet.com/article/google-finds-android-zero-day-impacting-pixel-samsung-huawei-xiaomi-devices/ (дата звернення: 23.04.2020).
3. Beer I. A very deep dive into iOS Exploit chains found in the wild // Project Zero team at Google. 29.08.2019. URL: https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html (дата звернення: 24.04.2020).

Одержано 25.04.2020