УДК 004.056.5
Світличний Віталій Анатолійович
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0003-3381-3350

ДЕЯКІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, РЕАЛІЗОВАНІ В МОБІЛЬНІЙ ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID 11

У міру того, як смартфони стають швидше і розумніші, вони грають все більш важливу роль в нашому житті, виступаючи в якості нашої розширеної пам'яті, нашої зв'язку зі світом в цілому і часто будучи основним інтерфейсом для спілкування з друзями, родиною, різними соціальними мережами. Цілком природно, що в рамках цієї еволюції ми стали довіряти нашим телефонами свої персональні дані, конфіденційну інформацію і в багатьох відносинах ставитися до них як до розширення нашої цифрової та фізичної ідентичності.

Мобільна операційна система (ОС) Android відносно молода платформа, яка постійно привертає підвищену увагу кіберзлочинців. Як відомо, Android – це ОС, яка заробила свою репутацію за відносну відкритість в порівнянні з iOS. Вона дозволяє завантажувати APK файли (англ. Android Package – додатки для ОС Android) з будь–яких джерел. Користувач може налаштувати root–доступ на пристрої і встановити іншу систему на базі Android [1]. При цьому, чим більше активно модифікується ОС, тим більша ймовірність завдати шкоди вашому пристрою, ніж можуть з успіхом скористатися кіберзлочинці.

Однак, в останні роки розробниками були представлені досить ефективні поліпшення безпеки системи, наприклад, вбудований антивірус Google Play Захист. Тому резонно постає питання: чи потрібно встановлювати сторонній антивірус? Однозначно 15–20 років тому наявність додаткового засоби захисту було життєвою необхідністю, зараз часи змінилися, і сучасні операційні системи стали в значній мірі самодостатніми з точки зору безпеки.

Компанія Google в 2017 році представила систему безпеки Play Захист, яка використовує технології машинного навчання для сканування магазину

додатків Google Play на предмет шкідливих додатків. Google Play Захист також вміє аналізувати додатки локально на конкретному смартфоні. Користувач може активований перевірку вручну – для цього потрібно перейти в додаток Play Маркет> Мої додатки та ігри> Оновлення та натиснути іконку поновлення у верхній частині екрану [2]. Google Play Захист вбудована в сервіс Play Маркет, і за словами розробників «допомагає вам зберегти ваш пристрій в безпеки і недоторканності». Google Play Захист, по суті є пакетом програм безпеки, який не тільки сканує на предмет зараження вірусами і іншим шкідливим софтом додатки, завантажувані з Play Маркета, але також досліджує ваші вже встановлені додатки і ваш пристрій в комплексі.

За багато років Android перетворився в досить надійну ОС. Google Play Захист – це в цілому відмінна функція захисту, але вона не гарантує абсолютну безпеку. Іноді буває, що деякі шкідливі програми залишаються в магазині Play Маркет протягом півроку. Так, наприклад, в минулому році на майданчику були виявлені будильники і сканери QR кодів, які містили троян AsiaHitGroup – на той момент їх встигли завантажити кілька десятків тисяч користувачів. Цей троян виконував корисне навантаження з метою отримати повний доступ до пристрою і контроль над персональними даними користувача. Нове «що не видаляється» шкідливе програмне забезпечення xHelper заразило 45 000 Android пристроїв. Раніше в минулому році дослідники з компанії Trend Micro (це світовий лідер в області рішень для захисту корпоративних даних і кібербезпеки для бізнесу, центрів обробки даних) виявили в Google Play 36 фальшивих антивірусів, які встановлювали шкідливе програмне забезпечення на пристроях, викликали неправдиві попередження і показували рекламу. Ці додатки також схильні запитувати невиправдано велике число дозволів доступу з метою крадіжки персональних даних [3]. Також варто брати до уваги швидкість і фрагментацію процесу оновлення Android. У той час як пристрої на чистому Android (без надбудов) отримують оновлення безпеки відразу після виходу, відомо, що виробники деяких пристроїв з модифікованими версіями системи затримують вихід патчів на кілька днів або навіть тижнів.

Так само, як і Apple в своїй iOS 14, Google попрацювала над безпекою в своїй системі. Головні зміни стосуються сховища. Відтепер сторонні додатки не можуть отримувати доступ до папок Android/obb/ і Android/data/. Таке обмеження може, наприклад, ускладнити установку сторонніх програм з кешем. Крім цього, дозвіл на доступ до сховища перейменовано: тепер запитується доступ до файлів і медіа. Важливі зміни торкнулися і механізму дозволів. Так, в Android 11 користувач може надати одноразовий доступ додатки до місця розташування, мікрофона або камері. В системі з'явився автоматичне скидання деяких дозволів. Він відбувається, якщо конкретним додатком не користуватися кілька місяців. А кнопка «Відхилити» в діалоговому вікні дозволів на увазі під собою дію «Не питати знову». Крім того, APK додатків в Android 11 можна видавати одноразовий доступ до мікрофона, камери або даних про місцезнаходження [4]. Наступного разу, коли з додатком знадобиться доступ, воно запросить його знову. Якщо користувач давно запускав програму з раніше виданими набором дозволів операційна система автоматично їх відкличе, повідомивши про це. Зрозуміло, при необхідності права доступу можна буде відновити в будь-який момент.

Компанія Google ще в 10 версії Android змінила підхід до поширення оновлень в рамках Project Mainline. В останній Android 11 додані 12 додаткових модулів оновлення системи через Google Play. Таким чином, безпосередньо через магазин Play Маркет надходитиме більше виправлень, що стосуються безпеки та конфіденційності операційної системи. Крім того, вони будуть виходити частіше, і користувачеві не доведеться чекати виходу повного оновлення ОС.

Інша справа, якщо користувач завантажує APK додатки зі сторонніх джерел. В цьому випадку, вбудований в Android антивірус Google Play Захист вже не може допомогти. Якщо немає впевненості в надійності джерела додатки, то необхідно задуматися про встановлення антивірусу для Android, щоб дозволить забезпечити додатковий захист. Звідси випливає дуже проста порада – не завантажуйте додатки, якщо ви не впевнені в їх надійності та безпеки.

Шкідливе програмне забезпечення – це найсерйозніша загроза для безпеки Android, тому слід завжди перевіряти легітимність додатки до його завантаження.

Список використаних джерел

1. Как работает антивирус Google Play и как его отключить // Trashbox : сайт. 15.08.2017. URL: https://trashbox.ru/topics/112068/kak-rabotaet-antivirus-google-play-i-kak-ego-otklyuchit (дата звернення: 19.11.2020).

2. Представляем Android 11 // Android : сайт. URL: https://www.android.com/intl/ru_ru/security-center/ (дата звернення: 19.11.2020).

3. i-Intelligence GmbH : сайт URL: http://www.i-intelligence.eu (дата звернення: 19.11.2020).

4. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення // CERT-UA: Computer Emergency Response Team of Ukraine : сайт. 21.07.2020. URL: https://cert.gov.ua/recommendation/2502 (дата звернення: 19.11.2020).

Одержано 21.11.2020

УДК 004.49

Семчук Андрій Олегович
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ
Світличний Віталій Анатолійович
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0003-3381-3350

ПОНЯТТЯ DDOS-АТАК ТА ЇХ КЛАСИФІКАЦІЯ

Атака на відмову в обслуговуванні (англ. Denial-of-Service attack – DoS attack. Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (англ. Distributed Denial-of-Service – DDoS). У розподіленій атаці на відмову одночасно можуть брати участь від кількох одиниць до кількох сотень тисяч, а іноді - кількох мільйонів хостів [1]. Мета атаки: зробити так, щоб система перестала працювати, і користувачі не могли отримати доступ до системних ресурсів. Щоб DDoS-атака була успішною, атакуючому потрібно посилати більше запитів, ніж може обробити сервер.