Аналіз захищеності системи Android для використання в корпоративному сегменті

Костянтин Нечволод[1], Олександр Сєвєрінов[2]

1. Кафедра безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, УКРАИНА, г. Харьков, пр. Науки, 14, E-mail: kostiantyn.nechvolod@nure.

2. Кафедра безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, УКРАИНА, г. Харьков, пр. Науки, 14, E-mail: oleksandr.sievierinov@nure.ua

Краткая аннотация – Android adoption has increased rapidly over the last few years, becoming the go-to OS for many organisations the world over. Due to the diversity of the platform and flexibility of form factor, application and budget, Android is making a huge impact on how employees undertake their daily responsibilities.

Ключевые слова –android, google play protect, google, mdm, безпека.

I. Вступ

Android – це надійна операційна система, яка встановлена на дуже велику кількість пристроїв, починаючи від мобільних телефонів і закінчуючи головними пристроями в автомобілі. Вона базується на таких основах, як відокремлення системних процесів, архітектурі довіреної ОС, а також вона використовує потужний аналізатор загроз який використовує машинне навчання та хмарні обчислення для визначення загроз за допомогою великої бази знань компанії Google.

Враховуючи ці фактори, підприємствам слід звернути увагу на операційну систему Android при впроваджені концепцій MDM та BYOD.

II. Вирішення проблеми та результати

Багато підприємств скоро розширять кількість мобільних пристроїв, які будуть використовуватися в корпоративній сфері за допомогою сучасних підходів та концепцій як MDM або BYOD. [1]

Але, незважаючи на те, що мобільність підприємств зростає, безпека даних залишається головною перешкодою на шляху впровадження нових технологій використання мобільних пристроїв.

Зараз одними з найпоширеніших загроз для мобільних пристроїв є:

– використання для доступу до глобальної мережі через незахищені точки доступу Wi-Fi, в яких можлива атака MITM(людина посередині);

– можливість крадіжки або втрати пристрою, яка дозволить зловмиснику отримати повний фізичний доступ до пристрою;

– шкідливе програмне забезпечення, яке може бути встановлено не навмисно самим користувачем і яке буде тихо збирати усю потрібну зловмиснику інформацію та навіть робити фото, відео та аудіо фіксацію усього, що трапляється навколо пристрою.[2]

Однак остання загроза є найменш вірогідною через сам принцип побудови системи Android, де кожен додаток виконується відокремлено від інших та отримати доступ до даних іншої програми без отримання прав root неможливо.

Сама думка про те, що доступ до конфіденційної інформації може бути не в корпоративній мережі викликає дуже багато сумнівів щодо доцільності використання подібних систем у фахівців з IT-безпеки. Тому перш за все, перед початком впровадження системи необхідно зважити всі переваги та ризики для бізнесу і вже потім приймати подальші рішення.[4]

Принести власний пристрій (BYOD) є поширеною концепцією у більшості підприємств, наприклад 84% опитаних компанією IDC в США заявили, що вони дозволяють хоча б певний ступінь використання персональних пристроїв на робочому місці. Використання персональних пристроїв на робочому місці - це тенденція, яка торкається більшості IT-підрозділів[3]. Хоча BYOD допомагає підприємствам скоротити витрати і може покращити задоволеність працівників, це також може бути проблемою безпеки.

За даними IDC, у підприємств з великим процентом використання BYOD виникли частіші проблеми з безпекою. Серед організацій с переважно більшим розгортанням BYOD, інциденти з мобільною безпекою були на 10-12% частішими. Серед фірм, що обмежують або забороняють BYOD, рівень відповідей на питання безпеки був нижчим за середній на 7%. Розмита межа робочих / особистих технології поширюється за межі пристроїв на додатки та хмарні послуги. Користувачі зазвичай залучають до роботи особисті або бажані мобільні додатки, хмарне сховище, програми SaaS та інші технології, які, на їх думку, роблять їх більш продуктивними. Відповідно до опитування менеджерів IT Mobile Mobile IDC за 2017 рік (спонсор Google) більше 70% підприємств США та Європи допускають певну тіньову IT у своїх організаціях. Ці фірми розуміють, що все дозволений, але пильний підхід до некорпоративних хмарних та програмних технологій, які використовують працівники, може сприяти підвищенню продуктивності та підвищити задоволеність користувачів. Незважаючи на те, що пристрої під керуванням операційної системи Android мають потужні основи безпеки, цілий ряд хмарних сервісів підтримує пристрої Android для подальшого покращення та забезпечення загальної безпеки платформи. Google Mobile Services (GMS) - це пакет програм, що ліцензуються Google сторонніми виробниками програмного забезпечення та партнерів Android, що дозволяє легко контролювати попередню інсталяцію таких програм, як Gmail, Карти, YouTube, Google Play Store та інші [2]. Менш очевидним для користувачів Android є основні можливості безпеки, які поставляються із GMS. Будь-який пристрій, що має ліцензію на GMS, також має функції сканування програмного забезпечення на основі пристроє та хмарно заснованих засобів для безпеки, а саме базовий набір послуг та функцій, який називається Google Play Protect. Вони варіюються від сканування на пристрої для використання потенційно небезпечних додатків (PHA) та експлуатування додатків, до програми Find My Device (раніше «Диспетчер пристроїв Android»)

для пошуку втрачених чи вкрадених пристроїв та виявлення наявності прав рут.

Google Play Protect включає набір API, які взаємодіють та обробляють інформацію між додатками на пристроях за допомогою вбудованих функцій захисту пристроїв та хмарні служби безпеки. У 2017 році Google Play Protect автоматично відключив PHA з приблизно 1 мільйона пристроїв. Google рецензує всі додатки, перш ніж публікувати їх у магазині Google Play. Окрім перегляду програм, поданих у Google Play, його хмарні системи шукають додатки у загальнодоступних джерелах. Google Play Protect також розглядає програми, які знаходить поза Google Play для PHA. Google Play Protect охоплює всі засоби безпеки, які роками захищають безпеку пристроїв користувачів Android. Наприклад, служба Verify Apps у Google Play Protect сканує програми для PHA, перш ніж користувачі встановлять їх, незалежно від їх походження.[2] Послуга Verify Apps виконує періодичну перевірку на всьому пристрої, яка інспектує додатки перед встановленням та виконує регулярні сканування всіх встановлених програм. Якщо PHA знайдено, сповіщення просить користувача видалити його. У випадках, коли PHA не надає можливих переваг користувачам, Google Play Protect може видалити PHA з уражених пристроїв та заблокувати майбутні встановлення.

AutoScan - це ще одна послуга, яка щодня перевіряє пристрої Android на предмет наявності PHA та інших ознак підробки. (Цей сервіс минулого року сканував майже 800 мільйонів пристроїв на день таких, як смартфони, планшети та телевізори з ОС Android.) AutoScan працює разом з Verify Apps як частина багатошарового підходу сканування Google до програмного забезпечення та безпеки Android. Якщо AutoScan виявить PHA або інші індикатори ризику на пристрої, це може викликати додаткове локальне сканування програм для подальшого вивчення проблеми. Хоча архітектура безпеки пристрою / хмари, що базується на хмарі, забезпечує надійний захист, вона значною мірою працює поза зони видимості для кінцевих користувачів. Google Play Protect був представлений у травні 2017 року, щоб розкрити цю функціональність та допомогти користувачам зрозуміти «стан здоров'я» своїх пристроїв. Google Play Protect забезпечує активні сповіщення користувачів Android про те, коли відбувається сканування на пристрої, стан безпеки кожного додатка, який переглядають або завантажують із магазину Google Play, та загальний стан додатків на пристрою. Швидке поширення оновлень програмного забезпечення є проблемою в такій різноманітній екосистемі, як Android. Google розповсюджує критичні оновлення безпеки через GMS, коли ця служба працює незалежно від оператора або версії програмного забезпечення Android.[3] Це може відправити нове програмне забезпечення, як тільки виявляться нові загрози. Крім критичних оновлень, часті оновлення ОС також забезпечують безпеку та продуктивність користувачів. З цією метою Google запустив Project Treble у 2017 році, щоб зробити його основні служби ОС більш модульними та однорідними, що дозволяє легше впроваджувати оновлення програмного забезпечення для операторів та виробників пристроїв. Treble змінює фреймворк для взаємодії компонентів операційної системи Android та компонентів постачальника пристроїв (чіпи від Qualcomm, MediaTek тощо).[3]

Це вирішує проблему швидких оновлень шляхом впорядкування процесу, коли виробники девайсів працюють з виробниками чіпів для перевірки нових оновлень ОС Android. Treble створює стандарт інтерфейсу постачальника для компонентів нижчого рівня для взаємовії з ОС. Виробники пристроїв та виробники чіпів більше не повинні переробляти низькорівневий код при кожному випуску, прискорюючи час оновлення.

Це посилює безпеку, оскільки знімається потреба у пряму доступу до драйверів ядра, які керують відтворенням медіа, що забезпечує більш надійну «пісочницю» та ускладнює скомпроментуваня фреймворку для використання ядра. (Однак підприємства можуть також навмисно затримувати оновлення ОС на пристроях, які рекомендовано програмою Android Enterprise, щоб дозволити IT-командам тестувати та оновлювати додатки для роботи на останній версії Android.).

Висновки

Операційна система Android вже давно лишилась старих проблем з безпекою. На сьогоднішній день безпеці цієї ОС приділяють багато часу та уваги, що безумовно грає велику роль в використанні пристроїв на базі Android не лише в приватній сфері, а ще і в корпоративному сегменті. Окрім вбудованих засобів безпеки, що працюють на рівні ядра системи, використання хмарних сервісів для постійного сканування системи на наявність потенційно небезпечного ПЗ, виявлення загроз ще на етапі завантаження додатків до магазину Google Play, наявність сервісу для пошуку втраченого пристрою та постійний випуск патчей безпеки для ОС дозволяють зробити висновки, що базовий варіант системи Android є досить безпечним для використання навіть в корпоративному сегменті.

Література

[1] Нечволод К.В. Аналіз безпеки даних в EMM системах / К.В. Нечволод, О.В. Сєвєрінов, А.В. Власов // Системи управління, навігації та зв'язку. – Полтава: ПНТУ. - 2019. – Вип. 3(55). – С. 131-134

[2] Android Enterprise [Электронный ресурс]. – режим доступа к журн.: https://www.android.com/enterprise/

[3] .IDS. Mobile Security at Enterprise Scale, 2019.

[4] Нечволод К.В. Аналіз безпеки даних на основі платформи Samsung Knox / К.В. Нечволод, О.В. Сєвєрінов // Комп'ютерні та інформаційні системи і технології. Третя міжнародна науково-технічна конференція. Збірник наукових праць. Х: ХНУРЕ, 2019.– С. 80-81.