УДК 536.24

ЗАГРОЗИ КІБЕРБЕЗПЕКИ АВТОТРАНСПОРТНИХ ЗАСОБІВ, ПІДКЛЮЧЕНИХ ДО МЕРЕЖІ ІНТЕРНЕТ

Симбірський Г. Д.
Харківський національний університет радіоелектроніки

Протягом останніх кількох років набирає популярності концепція connected car – автомобілі з доступом в інтернет. Йдеться не тільки про інфо-мультимедіа системи (музика, карти, фільми на борту доступні на сучасних автомобілях преміум сегмента), а й про ключові як у прямому, так і в переносному сенсі системах автомобіля. За допомогою спеціалізованих мобільних програм можна отримати координати автомобіля, його маршрут, відкрити двері, запустити двигун, включити допоміжні пристрої. З одного боку, це надзвичайно корисні можливості, якими користуються вже мільйони людей, з іншого боку – опинися у викрадача доступ до мобільного пристрою жертви, на якому встановлено таку програму, хіба викрадення авто не стане дрібницею?

У пошуках відповіді на це питання у компанії KasperskyOS вирішили розібратися, що справді може зробити зловмисник, і як власники машин можуть уникнути можливих проблем.

Такі програми зараз популярні: аудиторія додатків найбільш популярних брендів коливається від кількох десятків тисяч до кількох мільйонів користувачів. Нижче для прикладу показано кілька додатків із кількістю їх установок.

Для експериментів було взято кілька додатків для керування різними марками автомобілів. Не розкриватимемо їх назви, але зазначимо, що в ході дослідження компанії розробників про його результати були сповіщені.

Кожна програма була розглянута з наступних позицій:

• чи містить програмний додаток потенційно небезпечні можливості, тобто чи можна за його допомогою викрасти автомобіль або вивести з ладу одну з його систем;

• чи використовували творці програми засоби, що ускладнюють реверс інжиніринг (обфускацію або упаковку). Якщо ні, то зловмиснику не важко прочитати код програми, знайти його вузькі місця і за їх допомогою пробитися до інфраструктури авто;

• чи є програма перевірка на наявність root-прав на пристрої (з подальшою відмовою від установки у разі позитивного результату). Адже якщо шкідливій програмі вдається заразити рутований пристрій, її можливості стають практично безмежними. У цьому випадку важливо зрозуміти, чи використовували творці збереження облікових даних користувача на пристрої у вигляді Plaintext;

• чи є програма перевірка, що після його запуску саме його інтерфейс показується користувачеві (захист від перекриття). Android дозволяє відстежувати який додаток в даний момент показується користувачеві, шкідлива програма може цю подію перехопити - показавши користувачеві вікно фішинга з ідентичним інтерфейсом - і вкрасти, наприклад, облікові дані користувача;

• чи є у додатку контроль цілісності, тобто. чи перевіряє воно себе щодо змін у коді. Від цього залежить, наприклад, чи зможе зловмисник взяти та впровадити свій код у додаток, а потім розмістити його в магазині додатків, зберігши при цьому функціональність та працездатність оригіналу.

Для дослідження було взято сім найбільш популярних програм від відомих брендів і перевірено на предмет слабких місць, якими можуть скористатися зловмисники для доступу до інфраструктури автомобіля.

Аналіз Додатка 1. Механізм реєстрації автомобіля в додатку зводиться до введення логіну та пароля користувача, а також VIN автомобіля. При цьому у додатку є PIN, який треба ввести в систему автомобіля штатними засобами для завершення прив’язки смартфона до машини. Тому лише VIN недостатньо для відкриття дверей авто.

Програма не перевіряє, чи є на пристрої root і при цьому зберігає логін від сервісу у відкритому вигляді у файлі accounts.xml разом з ним і VIN від авто. За наявності у троянця прав суперкористувача на прив’язаному смартфоні ці дані дуже легко вкрасти.

Додаток №1 легко декомпілювати, код можна розібрати. Крім того, воно ніяк не протидіє перекриття власного інтерфейсу, а

значить логін і пароль можна запровадити за допомогою фішингової програми, що складається з 50 рядків коду. Досить перевірити який додаток запущено в даний момент і якщо додаток з цільовим ім’ям пакета, то запустити своє Activity з аналогічним інтерфейсом.

У цьому випадку логін та пароль просто відобразяться на екрані телефону, і нічого не завадить вбудувати надсилання облікових даних на сервер зловмисників.

Відсутність перевірки на цілісність дозволяє будь-кому бажаючому взяти додаток, модифікувати його на свій розсуд і почати роздавати потенційним жертвам. Перевірки підпису не вистачає. Звичайно, така атака вимагатиме від зловмисника певних зусиль – потрібно змусити користувача завантажити модифіковану версію програми. Зате вона носить дуже прихований характер, користувач нічого не помітить, поки його машину не відведуть

З позитивного: програма викликає із собою сертифікати SSL і здійснює з’єднання з їх допомогою. Загалом це запобігає атаці типу Man-in-the-Middle.

Аналіз Додатка 2. Додаток пропонує зберегти облікові дані користувача, але рекомендує зробити шифрування всього пристрою на випадок крадіжки. Розумно, але ми красти телефон не збираємося - ми його "заразили". В результаті та ж загроза, що і в додатку №1 - зберігання логіна разом з паролем у відкритому вигляді у файлі prefs.{??????????}.xml

Таким чином, програма зберегла свою функціональність, але вказані нами при реєстрації логін і пароль були виведені на екран смартфона відразу після спроби входу в систему.

Аналіз Додатка 3. Автомобілі, що використовують цю програму, за бажанням замовника комплектуються модулем керування, який може запустити двигун та відкрити двері. Його встановлює дилер, при цьому кожен модуль комплектується стікером з кодом доступу, який видається на руки власнику машини. Тому прив’язати автомобіль, знаючи його VIN, до чужих облікових даних не вдасться.

Однак є інші можливості для атаки: по-перше, додаток дуже маленький, всього 180 кілобайт в APK-виді, по-друге, вся програма обкладена налагоджувальною печаткою в лог-файл, який зберігається на SD карту.

Аналіз Додатка 4. Додаток дозволяє підчепити існуючий VIN до будь-яких облікових даних, але сервіс обов'язково надійшле запит на бортовий комп'ютер автомобіля. Тому найпростіший крадіжка VIN не допоможе розкрити машину.

Проте досліджуваний додаток беззахисно перед перекриттям свого вікна, і якщо завдяки цьому у зловмисника виявляться логін та пароль від системи, він зможе відкрити авто.

Аналіз Додатка 5. Щоб прив'язати автомобіль до смартфона, на якому встановлено цю програму, потрібен PIN-код, який повідомить бортовий комп'ютер авто. Отже, як і у випадку з попереднім додатком, одного VIN недостатньо, потрібен доступ до автомобіля.

Додаток від російських розробників, який концептуально відрізняється від своїх аналогів тим, що в якості авторизації використовується номер телефону власника.

Такий підхід створює неабиякий ризик для власника автомобіля: для початку атаки потрібно виконати одну API функцію Android та отримати в результаті логін до системи.

Аналіз Додатка 6. З особливостей останнього розглянутого додатка варто відзначити зберігання логіну та пароля у відкритому вигляді у файлі credentials.xml.

Успішне зараження смартфона троянцем з правами суперкористувача дозволить без особливих зусиль вкрасти цей файл.

Теоретично, після крадіжки облікових даних зловмисник зможе отримати контроль над автомобілем, проте це не означає, що злочинець зможе просто його викрасти. Справа в тому, що для того, щоб рушити на авто обов'язково наявність ключа, тому, потрапивши всередину машини, викрадачі використовують блок програмування і записують в борт управління авто новий ключ. А тепер згадаємо, що майже всі описані програми дозволяють розблокувати двері, тобто. зняти машину із охоронної сигналізації. Таким чином зловмисник проробить всі необхідні для угону операції потай і швидко, не треба нічого ламати або свердлити.

Також не слід обмежувати ризики власника одним лише викраденням. Отримавши доступ до авто, його можна зіпсувати так, що жертва потрапить в аварію і може зазнати серйозних травм або загинути.

Жоден із розглянутих додатків немає повного захисту. Однак треба віддати належне розробникам додатків та сервісів – дуже добре, що для керування авто у жодному з описаних випадків не було використано голосових або SMS каналів. Однак саме такими засобами користуються виробники охоронних сигналізацій. З одного боку, нічого дивного в цьому немає, якість мобільного інтернету не завжди і не скрізь дозволяє авто бути онлайн, у той час як голосові дзвінки та SMS як базові функції будуть доступні. З іншого боку, це створює додаткові загрози безпеці авто, розглянемо які саме.

Голосове управління відбувається з допомогою про DTMF команд. Власнику потрібно в прямому значенні слова зателефонувати автомобілю, охоронна сигналізація відповість на вхідний дзвінок і приємним жіночим голосом повідомить статус автомобіля, після чого перейде в режим очікування команди від власника. Для того щоб змусити авто відкрити двері або запустити двигун, достатньо буде набрати відповідні цифри на клавіатурі телефону. Сигналізація розпізнає коди та виконає потрібну команду.

Творці таких систем подбали про безпеку та передбачили список дозволених номерів, яким дозволено керувати автомобілем. Проте, ніхто не подумав про ситуацію, коли телефон власника скомпрометований. Тобто зловмиснику достатньо заразити телефон жертви примітивним додатком, який від її імені дзвонитиме охоронної сигналізації. Якщо при цьому вимкнути звук динаміка та екран, можна керувати автомобілем повністю непомітно для жертви.

Звичайно, не все так просто. Наприклад, багато автолюбителів зберігають номер охоронної системи під вигаданим ім’ям, тобто. для успішної атаки необхідно, щоб жертва часто взаємодіяла з авто через дзвінки. Тільки так зловмисник, який викрав історію вихідних дзвінків, може знайти номер авто у списку контактів жертви.

Творці іншого методу управління охороною автомобіля - за допомогою SMS-команд - точно не читали жоден з наших оглядів з безпеки пристроїв на базі платформи Android. Справа в тому, що першими та найчисленнішими мобільними троянцями, з якими боролася компанія, були SMS-троянці. Тобто зловреди, що містять у своєму коді можливість прихованого надсилання SMS; причому таке відправлення здійснювалося як у ході штатної роботи троянця, так і

по віддаленій команді зловмисників. В результаті, для того, щоб відкрити двері авто жертви, господарям зловреда достатньо виконати три дії:

1. Перебрати SMS на смартфоні на предмет команд автомобілю.

2. У разі виявлення потрібних SMS, витягніть з них номер телефону та пароль доступу.

3. Надіслати на виявлений номер SMS із текстом, що відкриває двері авто.

Усі три операції троянець може зробити потай від жертви, єдина складність, з якою, утім, зловмисники вміють справлятися, — це зараження смартфона.

Автомобіль — річ дорога, і до безпеки потрібно підходити не менш ретельно, ніж до безпеки банківського рахунку. Зрозуміло, зрозуміла позиція автовиробників і розробників, які намагаються оперативно випускати на ринок програми з новими можливостями для зручності власників машин. Однак думаючи про безпеку connected car не варто обмежуватися безпекою інфраструктури (серверів управління), каналами взаємодії авто та інфраструктури. Варто також звернути увагу на бік клієнта, зокрема на програму, яка зараз знаходиться у користувачів. Зараз його дуже просто обернути проти його власника, і це, можливо, зараз найвужче місце, на яке можуть націлитися зловмисники.

Тут слід сказати, що поки ми не бачили жодного випадку атак на програми для керування авто, жоден з тисяч виявлених нами нових зловредів поки не містив код для завантаження файлів конфігурації таких додатків. Однак сучасні троянці дуже гнучкі, якщо сьогодні один такий троянець показує персистентну рекламу (яку користувач сам ніколи не зможе видалити), то завтра він за командою зловмисників завантажить на C&C конфігураційний файл автододатку. Або видалить його та поставить поверх інше – модифіковане. Як тільки це стане фінансово вигідно зловмисникам, нові можливості для звичайних мобільних троянців не забаряться.

Література

1. Https://securelist.ru/mobile-apps-and-stealing-a-connected-car/30188/.