# ЗАГРОЗИ КІБЕРБЕЗПЕЦІ ТРАНСПОРТНИХ ЗАСОБІВ, ПІДКЛЮЧЕНИХ ДО ІНТЕРНЕТУ

***Дяченко Д.С.,*** Магістр
Науковий керівник – ***Біндюг С.А.,*** асистент
*Харківський національний автомобільно-дорожній університет*

Концепція connected car (автомобіль, який можна підключити до інтернету) стає все більш популярною протягом останніх кількох років. Це стосується не лише інформаційних та мультимедійних систем (сучасні автомобілі преміум-класу пропонують музику, карти та фільми в салоні), але й основних систем в автомобілі, як в прямому, так і в переносному сенсі. Спеціальні мобільні додатки дозволяють визначати координати автомобіля, прокладати маршрути, відчиняти та зачиняти двері, запускати двигун та вмикати допоміжне обладнання. З одного боку, це дуже корисні функції, якими вже користуються мільйони людей, але з іншого боку, чи була б крадіжка автомобіля тривіальною справою, якби викрадач мав доступ до мобільного пристрою жертви, яка встановила такий додаток?

Щоб знайти відповідь на це питання, KasperskyOS вирішив дослідити, що насправді можуть зробити хакери і як автовласники можуть уникнути можливих проблем.

Такі додатки наразі дуже популярні, а найпопулярніші бренди мають від десятків тисяч до мільйонів користувачів. Нижче наведені приклади додатків та кількість встановлень.

У нашому експерименті ми використовували кілька додатків для водіння автомобілів різних марок. Назви додатків не будуть опубліковані, але слід зазначити, що розробники були поінформовані про результати дослідження.

Кожен додаток було проаналізовано з точки зору

- Чи містить програма потенційно небезпечні функції;

- чи використовує творець програми інструменти, які ускладнюють зворотний інжиніринг (обфускація, пакування); і Якщо ні, то зловмиснику не важко прочитати код програми, знайти її вузьке місце і використати його для проникнення в інфраструктуру транспортного засобу;

- Чи перевіряє додаток root-дозволи пристрою. Адже якщо шкідливій програмі вдається заразити рутований пристрій, її можливості практично безмежні. У цьому випадку важливо розуміти, чи зберіг автор облікові дані користувача на пристрої у вигляді простого тексту;

- чи є перевірка того, що саме інтерфейс програми відображається користувачеві після запуску програми (захист від перекриття); Android може відстежувати, який додаток в даний момент відображається користувачеві, і шкідливе ПЗ може перехоплювати ці події;

- Чи має додаток засоби контролю цілісності, тобто чи перевіряє він зміни коду. Це визначає, наприклад, чи може зловмисник вставити свій код в додаток

і розмістити його в магазині додатків, зберігаючи при цьому функціональність і продуктивність оригінального додатка.

У дослідженні було взято сім найпопулярніших додатків відомих брендів і перевірено їх на наявність вразливостей, якими може скористатися зловмисник, щоб отримати доступ до інфраструктури автомобіля.

Аналіз додатків 1. Механізм реєстрації автомобіля в додатках обмежується введенням логіну, паролю та VIN-коду користувача. Водночас у додатку є PIN-код, який необхідно ввести в автомобільну систему штатними засобами для завершення з'єднання смартфона з автомобілем. Таким чином, один лише VIN-номер не може бути використаний для відчинення дверей автомобіля.

Додаток не перевіряє, чи є пристрій root, і при цьому зберігає логін сервісу разом з VIN-кодом з автомобіля у відкритому вигляді у файлі accounts.xml. Якщо троянець має права суперкористувача на підключеному смартфоні, вкрасти ці дані дуже легко. Додаток №1 легко декомпілюється, а його код можна розібрати. Крім того, оскільки не вжито жодних заходів для перекриття пропрієтарного інтерфейсу, для введення логінів і паролів може бути використана фішингова програма, що складається з 50 рядків коду. Достатньо перевірити, яка програма запущена в даний момент, і якщо це програма з назвою цільового пакета, запустити активність з подібним інтерфейсом. У цьому випадку логін і пароль просто відображаються на екрані телефону, що не заважає додатку надсилати облікові дані на сервер зловмисника.

Оскільки немає жодних перевірок цілісності, будь-хто може отримати додаток, змінити його на свій розсуд і почати розповсюджувати серед потенційних жертв. Також відсутня перевірка підпису. Звичайно, така атака вимагає зусиль з боку зловмисника - користувача потрібно змусити завантажити модифіковану версію програми. Однак це відбувається дуже непомітно, і користувач нічого не помітить, поки у нього не заберуть автомобіль.

Позитивним моментом є те, що програма запитує SSL-сертифікат і використовує його для встановлення з'єднання. Загалом, це запобігає атакам типу «людина посередині».

Аналіз додатку 2 Додаток пропонує зберігати облікові дані користувача, але рекомендує зашифрувати весь пристрій на випадок крадіжки. Хоча це розумно, ми не маємо наміру красти телефон. Як наслідок, ми стикаємося з тими ж загрозами, що і в Додатку 1. Логіни та паролі у відкритому вигляді у файлі prefs.{.}. Вони зберігаються в xml-файлі.

Таким чином, додаток зберіг свою функціональність, але логін та пароль, вказані при реєстрації, відображалися на екрані смартфона одразу після спроби входу в систему.

Аналіз Додатку 3 Автомобілі, що використовують додаток, мають додатковий модуль управління, який дозволяє запускати двигун та відчиняти і зачиняти двері. Цей модуль встановлюється дилером, і на кожному модулі є наклейка з кодом доступу, який видається власнику автомобіля. Тому, знаючи VIN-номер, неможливо прив'язати автомобіль до чужих облікових даних.

Однак є й інші можливості для атаки. По-перше, додаток дуже маленький, всього 180 кілобайт у форматі APK, а по-друге, вся програма запечатана налагоджувальною печаткою у лог-файлі, що зберігається на SD-карті.

Аналіз Додатку 4 Додаток дозволяє прив'язати існуючі VIN-коди до будь-якої автентифікаційної інформації, але цей сервіс обов'язково надсилає запит до бортового комп'ютера автомобіля. Тому найпростіша крадіжка VIN-коду не може розблокувати автомобіль.

Однак досліджуваний додаток має вразливість, яка блокує його вікно, що дозволяє зловмиснику відкрити автомобіль, отримавши логін та пароль для входу в систему.

Аналіз Додатку 5 Для того, щоб прив'язати автомобіль до смартфону зі встановленим додатком, потрібен PIN-код, який передається на бортовий комп'ютер автомобіля. Іншими словами, як і у випадку з попереднім додатком, VIN-коду недостатньо, потрібен доступ до автомобіля.

Цей додаток російського розробника відрізняється від подібних програм тим, що для автентифікації використовується номер телефону власника. Такий підхід створює значні ризики для власника автомобіля. Для здійснення атаки достатньо виконати одну функцію Android API та отримати логін для входу в систему.

Аналіз Додатку 6 Серед особливостей останнього досліджуваного додатку варто відзначити, що логіни та паролі зберігаються у відкритому вигляді у файлі credentials.xml.

Якщо їм вдасться заразити смартфон трояном з правами суперкористувача, вони зможуть без особливих труднощів викрасти цей файл.

Теоретично, після викрадення облікових даних зловмисник зможе отримати контроль над автомобілем, але це не означає, що злочинець може просто викрасти машину. Насправді, оскільки для керування автомобілем потрібен ключ, потрапивши всередину автомобіля, злодій за допомогою блоку програмування записує новий ключ в панель керування автомобіля.А

Тут слід пам'ятати, що майже всі описані програми дозволяють відчинити двері, тобто зняти автомобіль з охорони. Таким чином, зловмисник може виконати всі необхідні для викрадення операції таємно і швидко, нічого не ламаючи і не пробиваючи.

Ризик для власника також не повинен обмежуватися лише крадіжкою. Отримавши доступ до автомобіля, жертва може потрапити в аварію, яка може спричинити пошкодження, що можуть призвести до серйозних травм або навіть смерті.

Жоден додаток не є повністю безпечним. Однак розробників додатків і сервісів слід поважати. Дуже добре, що в жодному з наведених випадків не використовувалися голосові або SMS-канали для керування автомобілем. Однак саме ці засоби використовують виробники протиугінних сигналізацій. З одного боку, це не дивно. Адже якість мобільного інтернету не завжди дозволяє автомобілю постійно бути онлайн, а голосові дзвінки та SMS доступні в якості

базових функцій. З іншого боку, це створює нові загрози для безпеки автомобіля, тож давайте розглянемо їх.

Голосове керування здійснюється за допомогою DTMF-команд. Власник повинен буквально подзвонити в машину. Сигналізація відповідає на вхідний дзвінок, приємним жіночим голосом інформує власника про стан автомобіля і переходить в режим очікування команд від власника.

Щоб автомобіль відчинив двері або запустив двигун, достатньо набрати відповідний номер на клавіатурі телефону. Сигналізація розпізнає код і виконує потрібну команду.

Розробники таких систем дбали про безпеку і передбачили перелік номерів, яким дозволено керувати автомобілем. Однак ніхто не думав про те, що станеться, якщо телефон власника буде скомпрометований. Це означало, що зловмисники могли просто заразити мобільний телефон жертви примітивним додатком, який від її імені викликав би тривогу. Вимкнувши динамік та екран, зловмисники могли поїхати на своєму автомобілі абсолютно непомітно для жертви.

Звісно, не все так просто. Наприклад, багато автовласників зберігають номери своїх охоронних систем під псевдонімами. Це означає, що для успішної атаки жертва повинна часто виходити на зв’язок з автомобілем за допомогою дзвінків. Тільки так зловмисник, який викраде історію дзвінків, зможе знайти номер машини в списку контактів жертви.

Творець ще одного способу керування охороною автомобіля за допомогою SMS-команд не читав наш огляд про безпеку Android-пристроїв. Насправді, першим і найпоширенішим мобільним трояном, з яким боролася компанія, був SMS-троян. Тобто шкідливе програмне забезпечення, яке містить у своєму коді можливість таємно надсилати SMS-повідомлення. Такі передачі здійснювалися як під час нормальної роботи трояна, так і віддаленою командою зловмисника. В результаті, для того, щоб відкрити двері автомобіля жертви, власнику шкідливого програмного забезпечення необхідно виконати три дії:

1. Просканувати SMS на смартфоні, шукаючи команди до автомобіля.

2. Якщо потрібне SMS знайдено, витягти з нього номер телефону та пароль доступу.

3. Відправити на знайдений номер телефону SMS з текстом для відкриття дверей відправити жертві.

Троянський кінь може виконати всі три операції таємно від жертви.

Єдина складність, з якою можуть зіткнутися зловмисники - це зараження смартфонів.

Автомобілі коштують дорого, і про їхню безпеку потрібно дбати так само, як і про безпеку банківських рахунків. Звичайно, позиція автовиробників і розробників зрозуміла. Адже вони намагаються якнайшвидше випускати додатки з новими функціями для зручності автовласників. Однак, розглядаючи безпеку підключених автомобілів, не варто обмежуватися безпекою інфраструктури (сервера управління) і каналів взаємодії між автомобілем та інфраструктурою.

Варто також звернути увагу на клієнтську частину, зокрема на додатки, які наразі має користувач. Зараз дуже легко налаштувати цей додаток проти його власника, і це може бути найвужчим місцем, куди може націлитися зловмисник.

Важливо зазначити, що, хоча підтверджених атак на програми для керування автомобілем не було, жодна з тисяч нових шкідливих програм, які ми виявили, не містить коду для завантаження конфігураційних файлів таких додатків. Однак сучасні трояни дуже гнучкі. Сьогодні такий троянець може показувати постійну рекламу (яку користувач ніколи не зможе видалити), але завтра він завантажить файл конфігурації програми для самостійного водіння в C&C за командою зловмисника. Або ж видалить його і встановить замість нього іншу модифіковану версію. Якщо це стане фінансово вигідним для зловмисника, перед звичайними мобільними троянами відкриються нові можливості.

**Література**

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

## ТЕМАТИЧНА КЛАСИФІКАЦІЯ НАУКОВИХ ДОСЛІДЖЕНЬ В ГАЛУЗІ МАШИНОБУДУВАННЯ

***Васильченко Ю.В.,*** магістр
Науковий керівник – ***Шабанова-Хайрова Н.Ф.***
*Національний технічний університет*
*«Харківський політехнічний інститут»,*

У сучасну інформаційну епоху обсяг наукових публікацій у галузі машинобудування стрімко зростає. Збільшення кількості документів вимагає ефективних способів організації цієї інформації для легкого та швидкого доступу до неї. Тематична категоризація допомагає скоротити час пошуку та забезпечити точний і зручний доступ до необхідних даних. Актуальні дані та результати досліджень є важливими для успіху нових технологій та інновацій у машинобудуванні. Правильна організація та класифікація наукової інформації може оптимізувати дослідницький процес та підвищити продуктивність дослідницької команди.

Основною метою даного дослідження є створення ефективної системи, яка дозволить дослідникам, інженерам та іншим зацікавленим особам швидше і точніше здійснювати пошук наукових статей, пов’язаних з конкретними темами в галузі машинобудування.