УДК 004.03142:004.056.5

ВРАЗЛИВОСТІ ПЛАТІЖНИХ ТА ІНФОРМАЦІЙНИХ ТЕРМІНАЛІВ

Автор: Колісніченко Дмитро Вадимович
Керівник – співавтор: Масальська Олена Олександрівна
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, SDKolisnichenko@gmail.com

На сьогоднішній час в більшості сфер IT-діяльності присутні платіжні термінали. Існують вразливості, до яких схильна велика кількість терміналів, такі як: виклик контекстного меню (Tap fuzzing); ведення некоректних даних, що призводить до появи на екрані стандартних елементів операційної системи (Data fuzzing); зовнішні посилання, стандартні елементи інтерфейсу.

Платіжні термінали – це інформаційні системи, що вимагають ретельного дослідження і сучасного захисту.

Ключові слова – термінальне обладнання, зовнішні посилання, інтерактивна графічна оболонка, вразливість, шкідливі додатки.

ВСТУП

У 21 столітті в більшості культурних, освітніх, розважальних місць присутні платіжні та інформаційні термінали. В цій доповіді, розглянемо термінальне обладнання, яке присутнє в більшості сфер діяльності:

1. Touch – термінали з оплатою різних послуг (квитки, мобільний рахунок, парковки, комунальні послуги, поповнення банківських карт);
2. Інформаційні термінали для пасажирів;
3. Термінальне обладнання в якому присутні «карти», побудова маршрутів.

Чим функціональніший пристрій, тим більше шанс наявності вразливостей в конфігураційній системі. Використання злочинцем термінального обладнанням в своїх цілях, безпосередньо витікають з особливостей.

- доступність;
- велика кількість термінального обладнання, що розташована в публічних місцях;
- обробка особистих даних користувачів;
- однакова структура, в рамках одного типу пристроїв.

У цій доповіді розглянемо деякі елементи, вразливості, недоліки платіжних та інформаційних терміналів [3].

ТЕХНОЛОГІЇ ВИХОДУ З ІНТЕРАКТИВНОЇ ГРАФІЧНОЇ ОБОЛОНКИ

Існує кілька типів вразливостей, до яких схильні дуже багато терміналів. Послідовність дій для виходу з графічної оболонки проілюстрована на рисунку 1.

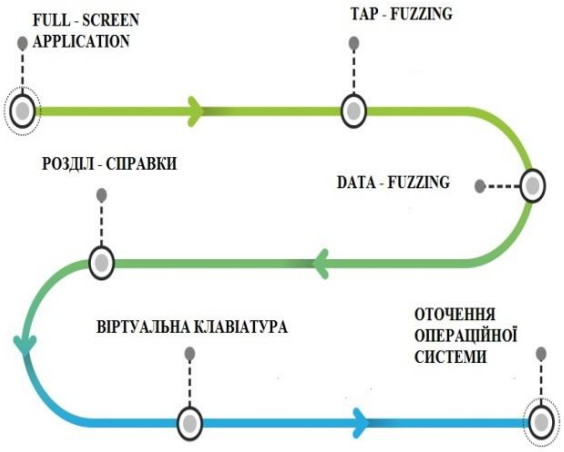

Рисунок 1. Основні дії для виходу з графічної оболонки

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ

В технічному сенсі все термінальне обладнання – це звичайні персональні комп'ютери з сенсорним екраном. Одна з основних відмінностей в них, це інтерактивна графічна оболонка, в якій присутня оплата послуг. Графічна оболонка перекриває первинні функції операційної системи. У деяких терміналів відсутній надійний захист від виходу з даного режиму, що тягне за собою повне отримання доступу і функціоналу операційної системи [2].

Розглянемо технологію «Tap fuzzing», що являє собою вихід з повноекранного додатка за рахунок некоректної обробки. Зловмисник намагається знайти в інтерактивній графічній оболонці вразливі місця, за допомогою тривалого натискання на них, за рахунок чого викликається контекстне меню операційної системи. При знаходженні даної уразливості зловмисник намагається відкрити командний рядок, за допомогою якого може заходити на жорсткий диск, встановлювати шкідливі програми, виходити в мережу [2].

Технологія «Data fuzzing» при вдалому використанні також призводить до появи на екрані елементів операційної системи. Зловмисник намагається спровокувати некоректну роботу термінального обладнання. Даний метод може спрацювати, якщо розробник не зміг налаштувати коректно фільтр на обмеження вводимих даних (наявність спеціальних символів, довжини рядка, розмір символу). Наприклад, зловмисник вніс некоректні дані в додаток, і ця помилка розробки призведе до відкриття вікна операційної системи [2].

Присутні інші способи виходу з інтерактивної графічної оболонки, на деяких терміналах фігурують зовнішні посилання (Facebook, Google +, Вконтакте).

Ще одним способом виходу за межі інтерактивної графічної оболонки можуть стати стандартні елементи інтерфейсу операційної системи. Якщо в даному терміналі встановлена операційна система сімейства Windows, є можливість, що зловмисник зможе викликати елементи управління діалоговим вікном, це дозволить залишити середу графічної оболонки [2].

Не можна забувати і про термінал в якому присутні карти. Деякі розробники в термінальне обладнання встановлюють карти від компанії «Google», при цьому «Google» має «віджет», у якому містяться такі елементи: «Повідомлення про помилку», «Конфіденційність», «Умови використання». Перехід по кожній з цих посилань гарантує попадання в браузер [1].

Розглянемо термінали, які обслуговують пасажирів. Важлива відмінність даного термінального обладнання в тому, що вони працюють з особистою інформацією клієнтів. В даних терміналах також присутня деяка подоба інтерактивної графічної оболонки. В більшості таких пристроїв використовується політика фільтрації веб-сайтів. Проте доступ і керування даною політикою відкритий, при бажанні зловмисник може видалити або додати будь-який сайт.

Наприклад, вільний доступ до фішингових сайтів, шкідливих сайтів.

Так само присутні вразливості перегляду бази даних. Якщо є можливість виходу з інтерактивної графічної оболонки, будь-який зловмисник може переглянути всю інформацію про клієнтів з їх логінами та паролями [3].

Вразливості термінального обладнання в параметрах друку також присутні. Після того, як користувач заповнив всі поля, він вводить реквізити і натискає кнопку "створити", термінал на обмежений час відкриває вікно друку, в якому присутні всі можливі параметри друку.

В такому випадку у зловмисника є обмежений час натиснути клавішу для зміни параметрів друку, після чого він зможе потрапити в довідковий розділ операційної системи. З даного розділу зловмисник може потрапити на панель керування або викликати віртуальну клавіатуру. За допомогою даної вразливості зловмисник зможе переглядати інформацію про вже роздрукованих раніше квитанції, запускати шкідливий код та інше [2].

ВИСНОВОК

Успішно проведена атака на термінальне обладнання може заподіяти прямі фінансові витрати його власнику. Зловмисник може використовувати "підлеглий" термінал для злому інших, адже вони часто об’єднані в мережу.

Для того що б мінімізувати шкідливу активність на публічних пристроях, потрібно використовувати такі методи:

- в інтерактивної графічній оболонці не повинно знаходитись зайвих функцій, які дозволять вийти за межі даної оболонки;
- додаток необхідно запускати за допомогою технології «пісочниця»;
- дані зберігати на сервері, якщо зловмисник видалив додаток з термінального обладнання, основна інформація про користування цим додатком залишиться на сервері;
- обмежити привілеї звичайного користувача – це утруднить встановлення нових додатків на сервері;
- для кожного пристрою повинен бути окремий логін і пароль, щоб не дозволити зловмиснику скомпрометувати один термінал, а потім використовувати отриманий пароль для всіх інших.

З кожним роком термінальна інфраструктура поступово поповнюється все новими пристроями, які пов’язані з іншими пристроями і системами. Термінальне обладнання – це окрема система, яка вимагає спеціального підходу та розробки ефективної системи захисту.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Денис Макрушин, Владимир Дащенко вразливості в платіжних та інформаційних терміналах [Електронний ресурс]. – Режим доступу: http://www.kaspe rsky.ru/about/news/virus/2016/fooling- the-smart-city, вільний;

2. Денис Макрушин, Владимир Дащенко розумне але не безпечне місто [Електронний ресурс]. Режим доступу: https://securelist.ru/analysis/obzor/29286/fooling-the-smart-city/, вільний;

3. Кенін А.М. Практичне керівництво системного адміністратора. – СПБХ. БХВ – Петербург, 2010. – 464 с.: ил. – (Системний адміністратор);