можливість перевірки коректності меж зон обслуговування і визначення нормативного часу доїзду до конкретного населеного пункту.

4. Розробити алгоритми сортування слабко-структурованих даних за визначеними критеріями.

5. Розробити алгоритми пошуку та відбору даних за певними класифікаційними ознаками.

6. Провести регресійних аналіз та визначити рівень впливу аналізованих даних на показник ймовірності виникнення надзвичайних подій.

Висновки. В результаті, аналітика великих масивів даних надасть можливість сформувати базу знань щодо прийняття оперативних рішень. Також це дозволить обгрунтувати потребу створення добровільних та місцевих пожежних команд.

ПЕРЕЛІК ПОСИЛАНЬ

1. Грицевич В. С. Статистичні ознаки та характеристики їхньої центральної тенденції: тексти лекцій / В. С. Грицевич. − Львів: Видавничий центр ЛНУ імені Івана Франка, 2008. − 52 с.

2. Гуліда Е.М. Завдання та методичні вказівки для виконання розрахунково-графічної роботи № 1 з дисципліни методологія та організація наукових досліджень для підготовки магістрів зі спеціальності 8.092801 «Пожежна безпека» / Е.М. Гуліда. – Львів: ЛДУ БЖД, 2013. – 19 с.

3. https://postgis.net/ Spatial and Geographic objects for PostgreSQL

УДК 004.46

Ю.А. Мілінчук[1], Р.С. Глушан[1]
[1]Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРИ АТАКАХ НА ПЛАТІЖНЕ ТЕРМІНАЛЬНЕ ОБЛАДНАННЯ

Анотація. Розглянуто основні види термінального обладнання та проаналізовано атаки на термінальне обладнання, що здійснюються шкідливими програмами Tyupkin та Skimer.

Ключові слова*: термінальне обладнання, Tyupkin, атаки на термінальне обладнання, ОС термінального обладнання* .

Вступ. Застосування термінального обладнання, яке включає в собі об’єднання різноманітних рішень, та сучасних технологій, забезпечує комфорт, зручність отримання послуг та раціональне споживання ресурсів для користувачів. Наразі інфраструктура термінального обладнання розвивається швидше, ніж засоби її захисту, що залишає великий простір для діяльності зловмисників, і це, в свою чергу, потребує пошуку нових засобів безпеки. На

сьогоднішній день люди все частіше використовують платіжне термінальне обладнання. Вносять свої персональні данні, банківські данні, і тому безпека такого обладнання являється важливим аспектом.

Постановка задачі. Для досягнення поставленої мети в роботі сформовані і вирішені такі завдання: досліджено термінальне обладнання; проаналізовані атаки на термінальне обладнання; виконано аналіз ПЗ при атаках на термінальне обладнання.

Термінальне обладнання – устаткування, що перетворює призначену для користувача інформацію в дані для передачі по лінії зв'язку і здійснює зворотне перетворення. Таке обладнання може бути як джерелом інформації так і одержувачем, або тим і іншим одночасно. Ці пристрої передають або приймають дані, за допомогою використання кінцевого обладнання лінії зв'язку і каналу зв'язку. До термінального обладнання відносяться: платіжні термінали (торгові і банківські термінали, термінали голосової авторизації) та контрольно – касові системи; інформаційні термінали.

Розберемо більш детально термінали.

Платіжний термінал – апаратно–програмний комплекс, що забезпечує прийом платежів від фізичних осіб в режимі самообслуговування. Для платіжного термінала характерна висока ступінь автономності його роботи. Контроль за роботою цих терміналів можна проводити через мережу Інтернет.

Технічний склад терміналу:

- метало-пластиковий корпус, в який вбудований комп'ютер;
- TFT – монітор з сенсорним екраном;
- пристрій безперебійного живлення;
- купюро – приймач;
- чековий принтер;
- GPRS модем;
- GSM антенна;
- сторожовий таймер.

Щоб збільшити кількість послуг, що надаються, в деякі платіжні термінали вбудовують:

- пристрій для роботи з пластиковими банківськими картами;
- сканер штрих-кодів;
- диспенсер, кардрідер;
- пін–пад клавіатури;
- додатковий TFT-монітор.

При роботі з терміналом, користувач виконує пошук послуг, вказує реквізити та інше за допомогою вбудованого екрану, на якому відображається меню. Після чого вже сам термінал перевіряє правильність введеної інформації, перевіряє існування даного рахунку і можливості його поповнення. Користувач вносить бажану суму готівки, купюро приймач розпізнає справжність готівки, їх номінал, і здійснює повернення купюр, які не пройшли перевірку на справжність. Після закінчення внесення готівкових коштів, термінал у відповідь роздруковує і видає користувачеві чек з інформацією цієї транзакції.

За допомогою GPRS – модему, термінальне обладнання пересилає інформацію про платіж серверу, який забезпечую обробку цього платежу. Після обробки даних серверне обладнання передає їх на шлюз сервера організації, після чого гроші поступають на рахунок одержувача.[1]

На сьогоднішній день існує велика кількість видів ОС, в кожній з яких різний рівень захисту, система управління, підтримка додатковий послуг. Але в основному використовуються наступні ОС:

1. Microsoft Windows Embedded (IoT)– це вбудована операційна система, яка використовується в спеціалізованих пристроях. Існує кілька категорій продуктів для створення широкого спектра пристроїв, починаючи від простих контролерів реального часу і закінчуючи POS – системами, такі як кіоск самообслуговування або касовий апарат та промисловими системами.

2. Microsoft Windows Embedded POSReady (Windows Embedded for Point of Service) - вбудована операційна система для POS-терміналів, кіосків, систем самообслуговування. Володіє перевагами вбудованих операційних систем Windows IoT, такими як фільтри захисту від запису, вибір компонентів для установки, блокування спливаючих вікон, приховування завантажувальних екранів, знижена вартість ліцензії, довгий термін доступності для замовлення . Однак, на відміну від Windows Iot), Windows Embedded POSReady не вимагає спеціальних навичок для установки та настройки, а також має можливість поставки без попередньо встановленого додатка. Також, як і Windows Embedded Standard, володіє 100% сумісністю з додатками, розробленими для Windows.

3. Windows Embedded 8 Standard – модульна операційна система. Виробник пристроїв має можливість самостійно обрати, які саме сервіси та можливості будуть включені в образ. В основі платформи лежить сучасна операційна система Windows 8. Windows Embedded 8 включає в себе стандартні функції і технології для створення багатофункціональних пристроїв з використанням «multitouch», а також додатковий функціонал, який зазвичай може бути включений тільки в рамках програм корпоративного ліцензування.[2]

Шкідлива програма, за допомогою якої були здійсненні найбільш відомі атаки на термінальне обладнання має назву Tyupkin. Вона являється актуальною для банкоматів, що випускаються одним з найбільших виробників подібних пристроїв, що працюють під керуванням 32-розрядної версії Microsoft Windows.

Щоб уникнути виявлення, шкідлива програма активна лише у певний час уночі. Крім того, для кожної сесії використовується ключ, що генерується з обраного випадковим чином числа. Без цього ключа взаємодія із зараженим банкоматом неможлива. При введенні правильного ключа шкідлива програма виводить на екран інформацію про кількість грошей, доступних у кожній касеті, і дозволяє зловмиснику, який має фізичний доступ до банкомату, отримати 40 купюр із обраної ним касети.

Більшість зразків цієї програми скомпільовано десь у березні 2014 року. Проте автори не стояли на місці. У її останньому варіанті (версії .d) у шкідливому коді реалізовано захист від аналізу, що здійснюється із застосуванням налагоджувачів та емуляторів. Крім того, ця версія відключає на зараженій системі захист McAfee Solidcore.

У процесі атаки злочинці копіювали на банкомат такі файли:

– C:\Windows\system32\ulssm.exe;

– %ALLUSERSPROFILE%\Start Menu\Programs\Startup\AptraDebug.lnk;

Після певних перевірок середовища, шкідлива програма видаляє файл з розширенням .lnk і створює у системному реєстрі наступний ключ:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

"AptraDebug" = "C:\Windows\system32\ulssm.exe".

Далі шкідлива програма взаємодіє з банкоматом, використовуючи стандартну бібліотеку MSXFS.dll – розширення фінансових сервісів (Extension for Financial Services – XFS).

Шкідлива програма запускає нескінченний цикл очікування введення користувача. Щоб ускладнити виявлення, Tyupkin приймає (за замовчуванням) команди лише вночі у неділю та понеділок.

Допустимі наступні команди:

XXXXXX – показати головне вікно;

XXXXXX – видалити зловмисну програму за допомогою пакетного файлу;

XXXXXX – продовжити період активності шкідливої програми;

XXXXXX – приховати головне вікно.

Після введення кожної команди оператор має натиснути клавішу Enter на цифровій панелі банкомату.

Крім того, Tyupkin використовує сесійні ключі, щоб унеможливити взаємодію з випадковими користувачами. Після введення команди "Показати головне вікно" шкідлива програма виводить повідомлення "ENTER SESSION KEY TO PROCEED!" (Для продовження введіть сесійний ключ). При цьому для кожної сесії ключ генерується обраного випадковим чином числа.

Оператор шкідливої програми повинен знати алгоритм, що дозволяє згенерувати сесійний ключ із показаного на екрані числа. Взаємодія із зараженим банкоматом можлива лише після успішного введення цього ключа.

Потім шкідлива програма виводить таке повідомлення:

CASH OPERATION PERMITTED. TO START DISPENSE OPERATION - ENTER CASSETTE NUMBER AND PRESS ENTER. (Касова операція дозволена. Щоб запустити операцію з видачі готівки – введіть номер касети та натисніть Enter).

Після вибору оператором номера касети банкомат видає 40 купюр з неї.

Також сьогодні здійснюють атаки за допомогою шкідливого програмного забезпечення Skimer. Після запуску шкідлива програма дізнається про тип файлової системи банкомату. У разі використання FAT32 вона копіює в папку System32 динамічну бібліотеку netmgr.dll. Якщо ж застосовується NTFS, то Skimer зберігає netmgr.dll в альтернативному потоці даних файлу SpiService.exe – компоненті банкоматів Diebold, який реалізує XFS, стандартну клієнт-серверну архітектуру для фінансових програм під Windows.

Встановивши бібліотеку, шкідлива програма додає у SpiService.exe виклик, що завантажує netmgr.dll, та перезапускає систему, в результаті чого отримує повний доступ до XFS та контроль над усіма можливостями пристрою.

Шкідливою програмою можна керувати за допомогою спеціальних карток з магнітною смугою, на другій доріжці якої записані інструкції для

Skimer. Інший тип карт дозволяє зловмисникам активувати одну з 21 відомих трояну команд, користуючись цифровою клавіатурою банкомату.

Зазвичай Skimer збирає дані банківських карток, вставлених у банкомат. За командою зловмисника він може роздрукувати накопичену інформацію або видати йому готівку. Крім того, у програмі передбачені команди для налагодження, оновлення та видалення.[3]

Висновки. 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. Той факт, що багато терміналів працюють під управлінням операційних систем з відомими вразливістю, а також без спеціалізованих захисних рішень – ще одна проблема, вирішення якої необхідно знайти якомога швидше.

ПЕРЕЛІК ПОСИЛАНЬ

1. Термінальне обладнання [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D1%82%D1%91%D0%B6%D0%BD%D1%8B%D0%B9_%D1%82%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB

2. Операційні системи терміналів [Електронний ресурс] – Режим доступу: https://www.depo.ru/article_a14913_r991.aspx;

3. Tyupkin, маніпулювання банкоматами за допомогою шкідливого програмного забезпечення [Електронний ресурс]: Режим доступу: https://securelist.ru/blog/issledovaniya/23950/tyupkin-manipulirovanie-bankomatami-s-pomoshhyu-vredonosnogo-po/.

УДК 004.048

А.А. Мартиненко[1]

[1]Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

ПРОБЛЕМИ СТВОРЕННЯ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ІДЕНТИФІКАЦІЇ КУЛЬТУРНИХ ЦІННОСТЕЙ

Анотація. Описано основні організаційні, нормативно-правові та матеріально-технічні проблеми процесу розробки та впровадження системи підтримки прийняття рішень для ідентифікації культурних цінностей. Наведено можливі шляхи вирішення зазначених проблем.

***Ключові слова**: системи підтримки прийняття рішень, ідентифікація культурних цінностей, архітектура систем.*

Вступ. Як зазначалось в роботах [1, 2] розробка та використання інтелектуальних систем підтримки прийняття рішень (ІСППР) при ідентифікації культурних цінностей (КЦ) є актуальним і перспективним. Також