УДК 621.371
DOI: 10.31673/2409-7292.2018.035870

Зідан А.М.

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ЗАГРОЗ ПРОФІЛЮ FACEBOOK В КОМП'ЮТЕРНИХ ТА ТЕЛЕФОННИХ МЕРЕЖАХ

В даній статті проведено детальний аналіз можливих загроз інформації профілю Facebook як в комп'ютерних, так і в телефонних мережах. Наведені приклади заходів та засобів, що може використовувати зловмисник для реалізації атак. Розглянуті сучасні методи забезпечення захисту для інформації профілю Facebook.

Ключові слова: загрози, вразливість, профіль Facebook, Faitagram, Jenkins, Cross – Site Request Forgery, Graph API, клавіатурний шпигун, Phishing, SS7.

Вступ. Сьогодні Internet увійшов у всі сфери нашого життя: від відпочинку, хобі до роботи та особистого життя. Це неймовірний інструмент комунікації, що розширює межі можливого для кожного. Окреме місце займають соціальні мережі, так як це необмежена недорога можливість спілкування з людьми з різних точок світу з будь-яких приводів: як особистих, так і бізнес-сфери. Одним з беззаперечних лідерів є Facebook. Тому існує великий інтерес до інформації, що не є публічною.

Постановка задачі. Існує багато можливих методів досягнення інформації з обмеженим доступом профілю Facebook: збір необхідної інформації різними шляхами та реалізація різноманітних атак. Розглянемо можливі загрози інформації профілю Facebook, детально проаналізуймо їх та визначимо необхідні методи та засоби для забезпечення захисту інформації.

Основна частина. З метою реалізації атак профілю Facebook використовуються певні набори команд, написані на певних мовах програмування. Сьогодні існує велика кількість мов програмування, але є три, що набули найбільшого застування [1].

Java – це мова програмування, що використовується для створення кросплатформових додатків незалежно від пристроїв застосування (комп'ютер, телефон). В липні 2018р. Java була визнана найкращою відповідно індексу Tiobe, але набрала 45,3% під час опитуавння Stack Overflow і стала другою.

JavaScript – це динамічна мова програмування, що використовується в основному для надання сайтам інтерактивності. Відповідно до опитування Stack Overflow JavaScript займає перше місце серед усіх мов програмування вже шостий рік поспіль. Також найбільший веб - сервіс для хостінгу IT – проектів, GitHub, назвав JavaScript найпопулярнішим в 2018р.

Python – це мова програмування високого рівня, що використовується для аналізу даних та веб – розробок. Відповідно до опитування Stack Overflow Python набрала 38,8% і зайняла третє місце. А відповідно даних GitHub – друге місце серед найпопулярніших мов програмування. Але відповідно до Stack Overflow – молода мова програмування Python визнана таким, що найбільш швидко досягає популярність в 2018р.

Розглянемо знайдений в Internet експериментальний варіант атаки профілю Facebook шляхом використання мови програмування Python від липня 2018р.

Faitagram (Facebook, Twitter, Instagram) – це скрипт, написаний мовою програмування Python, що використовує STEM – проксі. Запускається при використанні Xvfb, pyvirtualdisplay на віртуальному дисплеї. Через наявність програми Selenium в скрипті, що запускає веб – браузер, є можливість не реалізації загрози. Розглянемо хід атаки. Для початку необхідно скопіювати сам скрипт з джерела. Для цього необхідно ввести наступне:

git clone https://github.com/Juniorn1003/Faitagram.git/

Faitagram складається з п’яти папок: License (ліцензія відкритого програмного забезпечення), Readme (інформація про скрипт), faitagram (головний файл), setup.by (установка залежностей), wlist (словник).

Наступним кроком має бути зміна права доступу, щоб ми могли використовувати скрипт. Для цього необхідно ввести команду:

chmod +x faitagram && chmod +x setup.py

Далі необхідно встановити необхідне для роботи скрипта, для цього необхідно ввести команду:

python.setup.by

Після встановлення стануть доступними команди для Facebook, Twitter та Instagram. Скрипт має велику базу паролів для захисту словників, але є можливість вводу нового паролю. Для цього необхідно ввести:

python faitagram –s service –u username –w wordlist –d delay ,

де необхідно вказати в:
service - facebook, twiter чи instagram;
username –ім’я користувача (профілю), на якого направлена атака;
wordlist – шлях до словника;
delay – проміжок часу між спробами набору паролю в секундах (є необов’язковим).

Для початку атаки Facebook необхідно ввести команду:

python faitagram –s facebook –u (email) –w (wordlist) –d (delay) ,

де необхідно вказати в:
email – електронну пошту користувача, на якого направлена атака;
wordlist – шлях до словника (за відсутності словника пишеться **«wlist»** замість **«wordlist»**);
delay – кількість секунд (необов’язково, за відсутності просто не пишеться «**d»**)

Ще раз зазначимо, що наведена атака є експериментальною та є велика ймовірність її не реалізації.

Також існує багато прикладів знаходження вразливостей Facebook, про які було попереджено адміністрацію всесвітньої соціальної мережі та, таким чином, захищено від можливих загроз для конфіденційності, цілісності та доступності інформації профілю Facebook за передбачену грошову винагороду. Одним із таких прикладів можна вважати наступний.

Вразливість Jenkins менш стандартного порту. Ця атака починається зі сканування портів доменів Facebook, що має сервіси на різних IP – адресах, за допомогою nmap.

Nmap – це вільна утіліта, що застосовується для різноманітного сканування IP – мереж з будь-якою кількістю об’єктів, визначення стану об’єктів сканованої мережі.

В ході сканування було виявлено на одному із портів Facebook Jenkins, що працював на стандартному порту.

Jenkins – це програмна система з відкритим вихідним кодом на мові програмування Java, що використовується для забезпечення процесу безперервної інтеграції програмного забезпечення.

При відкритті Jenkins стандартного порту в браузері з’явилося вікно базової аутентифікації. Але при подальшому повному скануванні портів було виявлено інший сервіс Jenkins, що працює на менш стандартному порту. При отриманні доступу до нього аутентифікація вже не вимагалась. Після був запущений Groovy – код через Jenkins Script Console, завдяки яким з’явилася можливість виконання команд на сервері від імені користувача Jenkins.

Groovy – це об'єктно орієнтована мова програмування, розроблена як доповнення для платформи мови програмування Java з можливостями мов програмування Python, Ruby та Smalltalk.

Таким чином було отримано можливість доступу до інформації та реалізації маніпуляцій. Наведемо приклад Groovy – коду для запуску команди **«who am I»**:

```
def command = """whoami"""
def proc = command.execute ()
proc.waitFor ()
println "stdout: $ {proc.in.txt}"
```

Також відомо, що за визначення та попередження цієї вразливості Facebook виплатив в якості винагороди $7500 через програму пошуку вразливостей («Bug Bounty»).

Розглянемо, ще декілька методів взлому профілю Facebook, що вже попереджені і більше не можуть бути реалізованими. Але завдяки цій інформації може скластися уявлення про можливий підхід до вирішення проблеми загроз інформації профілю Facebook.

Загроза методом підбору паролю. Зазначений метод часто називають методом «грубої сили».

Метод «грубої сили» - це повний перебір усіх можливих варіантів вирішення задач.

Зазначений недолік був виявлений в кінцевому пункті відновлення паролю до профілю Facebook. А саме мова йде про пункт, де користувач в процесі заміни (відновлення) паролю для отримання шестизначного коду надає номер свого телефону чи e-mail Цей пункт важливий для перевірки користувача - власника профілю. Зазначимо, що дуже важко підібрати шестизначний код введення для зміни паролю доступу профілю Facebook, так як надається всього 10 – 12 спроб для введення різних комбінацій коду підтвердження. А за відсутності правильного варіанта служба безпеки Facebook тимчасово заблокує профіль. Перевіривши субдомени «mbasic.facebook.com», «beta.facebook.com», виявилось, що вони не витримали перевірки методом «грубої сили». Це надало можливість підбору шестизначного коду за безмежною кількістю спроб та змінити пароль до профілю Facebook, тим самим надало можливість маніпуляції інформацією профілю на власний розсуд. Варіант запроса можна сформулювати наступним чином:

```
Post/recover/as/code/
Host: mbasic.facebook.com
n=<6_digit_code>&other_boring_parameters
```

Можливість нескінченного перебору варіантів параметру **n** (n=123456) надає можливість зловмиснику замінити пароль профілю на свій. Це може бути виконане будь-яким засобом для підбору паролю з Internet.

Зазначена вразливість вже виправлена. А фахівцю, що виявив це слабке місце та повідомив про неї Facebook, було виплачено винагороду в розмірі $15000 через програму пошуку вразливостей («Bug Bounty»).

Вразливість захисту профілю Facebook була виявлена методом підбору паролю іще в один спосіб. Розглянемо приклад запиту:

```
Post/recover/as/code/
Host: lookaside.facebook.com
n=<6_digit_code>&other_boring_parameters
```

Враховуючи вищезазначене ми можемо зробити висновок, що сценарій атаки такий самий, як і попередній, але відмінність є в імені домену. Фахівцю, що виявив цю вразливість

Facebook та попередив про її наявність виплатили винагороду в розмірі $10000 через програму пошуку вразливостей («Bug Bounty»).

Загроза методом Cross – Site Request Forgery. Метод Cross – Site Request Forgery є змішаним типом атаки заміщення, який використовує аутентифікацію та авторизацію користувача, проти якого направлена атака, при відправленні сфальшованого запиту на веб – сервер.

Цей метод вимагає, щоб користувач, проти якого направлена атака, відвідав посилання веб – сайта, щоб завершити реалізацію атаки зловмисника. Необхідною умовою є використання того ж браузера, що використовується для входу в Facebook.

Зазначена CSRF вразливість реалізується на останньому етапі за запитом електронної пошти Facebook. Виявилось, що коли користувач дає запит адреси електронної пошти, то перевірка адреси запиту користувача з боку сервера не проводиться. Таким чином, зазначена вразливість надає змогу робити запит електронного листа для будь-якого профілю Facebook. Перед створенням сторінки атаки CSRF необхідно отримати URL – адресу вимоги для зміни адреси електронної пошти. З цією метою спробуємо змінити адресу своєї електронної пошти на адресу електронної пошти, що вже використовується на іншому профілі Facebook. Потім буде запропоновано перевірити електронний лист. Далі вспливаюче вікно з запитом направить Вас на необхідну URL – адресу після натиску опції запиту. URL – адреса повинна виглядати наступним чином:

http://www.facebook.com/support/openid/accept_hotmail.php?appdata=%7B%22fbid%22%3A%22&code=<code>

Тепер є URL – адреса. Наступним кроком є створення сторінки для розміщення цієї URL – адреси в «iframe» та відправити її користувачу, проти якого направлена атака. Як тільки користувач перейде на відправлену йому сторінку – адреса необхідної електронної пошти буде прикріплена до його профілю Facebook. Після цього кроку зловмисник отримує можливість взлому профілю Facebook через опцію зброду паролю. Фахівець, що знайшов цю вразливість та попередив Facebook також отримав винагороду через програму пошуку вразливостей («Bug Bounty»).

Вразливість Facebook при використанні методу CSRF була знайдена іще одним шляхом. Цей варіант звичайно трохи схожий на попередній: користувачу, проти якого направлена атака, також необхідно відвідати сайт зловмисника для реалізації атаки. Зазначена вразливість була виявлена в кінцевій точці відправлення контактів під час процесу, коли користувач надає дозвіл Facebook отримати дозвіл для доступу до контактів в «Microsoft Outlook»: сервер робить запит і додає контакти до профілю Facebook. Атаку можна реалізувати наступним шляхом: вибрати «знайти контакти на Facebook» в профілі. Потім необхідно знайти запит, зроблений на сервер Facebook, при використанні перехвату проксі – сервера. Запит має наступний вигляд:

http://m.facebook.com/contact-importer/login?auth_token=

Такий самий запит може використовуватися і для атаки методом CSRF. Для реалізації цього необхідно ввести URL – адресу в «iframe» на сторінці атаки та поділитися неї із користувачем, проти якого направлена атака. Профіль Facebook користувача буде взломаний як тільки він відвідає цю сторінку. Про цю вразливість також було попереджено та виправлено.

Ще існує можливість атаки методом CSRF, за якої зловмисник отримує можливості повного контролю над профілем та виконувати будь-які дії анонімно не взламуючи. Вразливість була виявлена в останній стадії менеджеру об’яв Facebook. Запит CSRF може мати наступний вигляд:

Post/ads/manage/home/?show_dialog_uri=/settings/email/add/submit/?new_email=<attacker_email>

Наступним кроком є створення сторінки CSRF з прикріпленою формою в «iframe», що автоматично буде відправляти Post – запит, коли користувач відвідає цю сторінку. Електронна пошта зловмисника буде додана до профілю користувача, проти якого направлена атака, анонімно. Таким чином зловмисник отримує можливість зміни паролю профілю. Фахівцю, що виявив вразливість та попередив Facebook. Була виплачена винагорода в розмірі $15000 через програму пошуку вразливостей («Bug Bounty»).

Вразливість при використанні SMS. Для реалізації атаки шляхом використання sms необхідно знати активний номер користувача, проти якого направлена атака. Вразливість була виявлена на останньому етапі підтвердження номеру користувача. Необхідно відправити повідомлення наступного формату:

«FBOOK to 32665» (для США)

У відповідь буде наданий код. Наступним кроком буде запит на сервер Facebook з цільовим ідентифікатором користувача, отриманим кодом та декілька інших параметрів. Приклад запиту може мати наступний вигляд:

Post /ajax/settings/mobile/confirm_phone.php
Host: www.facebook.com
profile_id=<target_user_id>&code=<short_code>&other_boring_parameters

З цього етапу номер телефону, що в цьому випадку використовує зловмисник, буде прикріплений до профілю користувача Facebook, ідентифікатор якого був відправлений, після отримання відповіді сервера. Тепер є можливість направити запит на зміну паролю, використовуючи мобільний телефон, та отримати доступ до інформації профілю Facebook. Фахівцю, що виявив цю вразливість та попередив Facebook, було виплачено винагороду в розмірі $20000 через програму пошуку вразливостей («Bug Bounty»).

Вразливість без адміністрування. В цьому випадку вразливість була знайдена в крайній точці бізнес – менеджера, де визначається партнер. Зміна параметру ідентифікатора бізнес – активу партнера на ідентифікатор сторінки надає можливість взлому профілю Facebook. Запит можна сформулювати в наступному вигляді:

Post/business_share/asset_to_agency/
Host: business.facebook.com
parent_business_id=<business_id>&agency_id=<business_id>&asset_id=<target_page_id>

де,
Business ID - ідентифікатор зловмисника,
asset ID – замінюється цільовим ідентифікатором сторінки Facebook.

Після цього етапу цільова сторінка переходить в управління як бізнес – сторінка. У зловмисника виникає можливість видалити існуючих адміністраторів сторінки. Щоб повністю заволодіти управлінням сторінки. Фахівцю, що виявив вразливість та попередив про неї, виплатили винагороду в розмірі $16000 через програму пошуку вразливостей («Bug Bounty»).

Вразливість фотографій профілю Facebook. Реалізація атаки в цьому випадку досягається шляхом використання функції автоматичної синхронізації мобільного додатка Facebook та фотографій архіву мобільного пристрою. Ця функція завантажує фотографії з мобільного пристрою на сервер Facebook, але не публікує їх без рішення користувача –

власника профіля. Вразливість була виявлена в кінцевій точці при обробці приватних фото. Для реалізації цієї атаки необхідно, щоб сторонній додаток мав доступ до фотографій загального доступу. Тільки після цього стане можливим доступ цього додатка до фотографій з закритим доступом. Як приклад можна навести наступний вигляд запиту для доступу до приватних фотографій:

Get /me/vaultimages
Host: graph.facebook.com
access_token=<victim_access_token>

Відповідь, що надійде з кінцевої точки API, матиме URL – адреси для приватних фотографій користувача, проти якого направлена атака. Фахівцю, що виявив вразливість та попередив про неї, виплатили винагороду в розмірі $10000 через програму пошуку вразливостей («Bug Bounty»).

Існує іще вразливість фотографій профілю Facebook, використовуючи функцію сповіщення власника фотографії, якщо хтось бажає видалити її. Власник профілю отримує повідомлення та посилання видаленої фотографії. Якою власник колись поділився. Виявилось, що панель управління фотографіями не була належним чином перевірена з приводу правильної перевірки власника. Це дає можливість зловмиснику замінити параметр ідентифікатора власника на власний, щоб отримати напряму посилання на видалення фотографій. Після цього зловмисник отримає можливість видалити фотографію за допомогою отриманого посилання. При цьому власник фотографій не повідомляється про те, що в його профілі деякі фотографії видалені. Фахівцю, що виявив вразливість та попередив про неї, виплатили винагороду в розмірі $12500 через програму пошуку вразливостей («Bug Bounty»).

Вразливість Graph API профілю Facebook. Виявилось, що отримати доступ та управління фотографіями профілю Facebook можливо іще й наступним шляхом.

Graph API – це основний спосіб комунікації між сервером Facebook та додатками, створеними як своїми розробниками, так і сторонніми.

Вузол кінцевої точки Graph API виявився вразливим для небезпечного посилання на об’єкт, завдяки цьому і можливо отримати доступ та управління фотографіями профілю. Сам запит можливо представити в наступному вигляді:

Post/<album_id>
Host: www.facebook.com
access_token=<top_level_facebook_access_token>&method=delete

де,

Album ID – параметр, що вказує на певний альбом.

Фахівцю, що виявив цю вразливість та попередив про неї, виплатили винагороду в розмірі $12500 через програму пошуку вразливостей («Bug Bounty»).

Вразливість відеозаписів Facebook. Завдяки використанню функції Facebook, в якій можливе додавання відеозаписів в якості коментарів. А при видаленні коментаря з відеозаписом – можливе видалення першоджерела відео. Таким чином зловмиснику необхідно відредагувати існуючий коментар до повідомлення Facebook за допомогою Graph API – запиту, який має наступний вигляд:

Post/<post_id>/comments?attachment_id=<target_video_id>
Host: graph.facebook.com

Після виконання цього етапу певний відеозапис буде доданим до коментаря. Тепер зловмиснику необхідно видалити коментар, для видалення першоджерела відеозапису. За декілька секунд після видалення коментаря, видалиться і відеозапис. Фахівцю, що виявив

вразливість та попередив про неї, виплатили винагороду через програму пошуку вразливостей («Bug Bounty») [2, 3, 4].

Загроза інформації профілю Facebook через обнуління паролю. Реалізація даної загрози є однією із простіших, так як не вимагає спеціалізованих знань. Основним є перебування в списку друзів профілю користувача, проти якого направлена атака. Насамперед необхідно знати електронну пошту користувача, яка може бути зазначена в інформації анкети профілю Facebook. Спочатку необхідно вибрати сам профіль та вибрати функцію відновлення паролю. Для реалізації функції відновлення паролю буде запропоновано відправлення паролю на електронну пошту. Враховуючи те, що немає доступу до електронної пошти, необхідно вибрати альтернативні методи відновлення паролю, такі як введення адреси іншої електронної пошти, що не закріплена за жодним із профілей Facebook, але за умови надання відповіді на певне запитання. За відсутності інформації для надання відповіді на таке запитання, можливо піти іншим шляхом – через декількох друзів зі списку профіля. Для цього необхідно вибрати опцію «відновлення доступу через друзів», вибрати 3 – 5 друзів, яким буде надісланий код доступу. Можливо створити підставні профілі та попередньо увійти до с писку друзів профілю користувача, проти якого направлена атака, чи домовитися з існуючими.

Рис.1. Сторінка введення паролів, надісланих вибраним друзям.

Для реалізації захисту інформації профілю Facebook від зазначеної загрози перш за все необхідно використовувати унікальну електронну пошту при реєстрації. Інформація на запитання для перевірки автора не повинна бути якимось чином публічною. Необхідно заздалегідь вибрати 3 надійних друзів, яким може бути надісланий пароль доступу в разі необхідності, щоб не було випадкового вибору [5, 6].

Загроза інформації профілю Facebook через використання «клавіатурного шпигуна». Існують програмні та апаратні «клавіатурні шпигуни».

Програма «клавіатурний шпигун» - це додаток, що фіксує усі натискання клавіш та надсилає отриману інформацію на певну адресу електронної пошти. Перш а все необхідно встановити цей додаток на пристрій користувача, проти якого направлена атака, а після цього «клавіатурний шпигун» продовжує працювати в фоновому режимі, що є непомітним для користувача. Для реалізації цієї загрози можливо знайти безкоштовні додатки в Internet або створити власний на мові програмування С++.

Апаратний «клавіатурний шпигун» працює за тим же принципом, що і програмний. Різниця лише в тому, що в цьому випадку необхідно підключити до комп'ютера користувача USB – флешку з програмою, де буде зберігатися зібрана інформація. Для отримання цієї інформації необхідно буде забрати зазначену USB – флешку. Є декілька різновидів апаратних «клавіатурних шпигунів»:

- тип Keyllama - необхідне підключення до комп'ютера користувача та може працювати з будь-якою операційною системою. Для отримання інформації необхідний фізичний доступ до комп'ютера користувача.

- Тип «клавіатурного шпигуна» з підтримкою Wi-Fi. Отримана інформація надсилається на певну електронну пошту шляхом використання Wi-Fi.

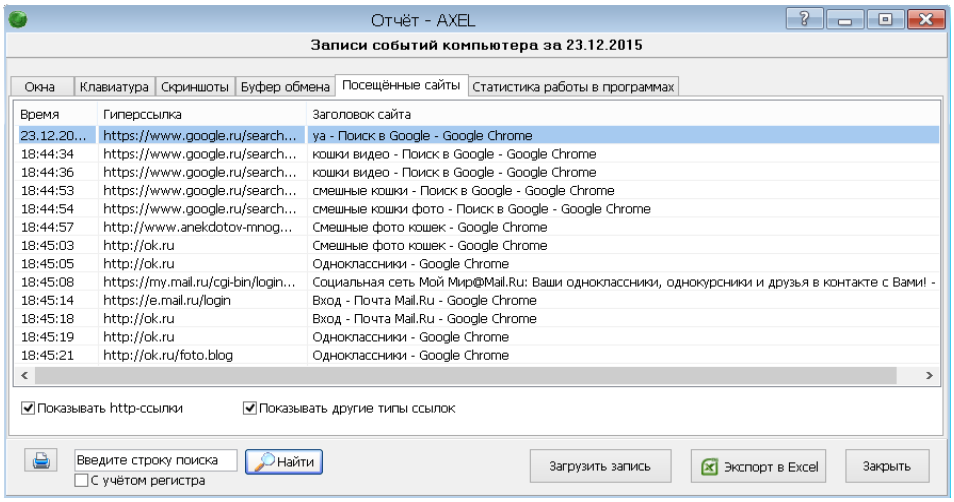

Рис.2, 3. Програма «клавіатурний шпигун» NeoSpy

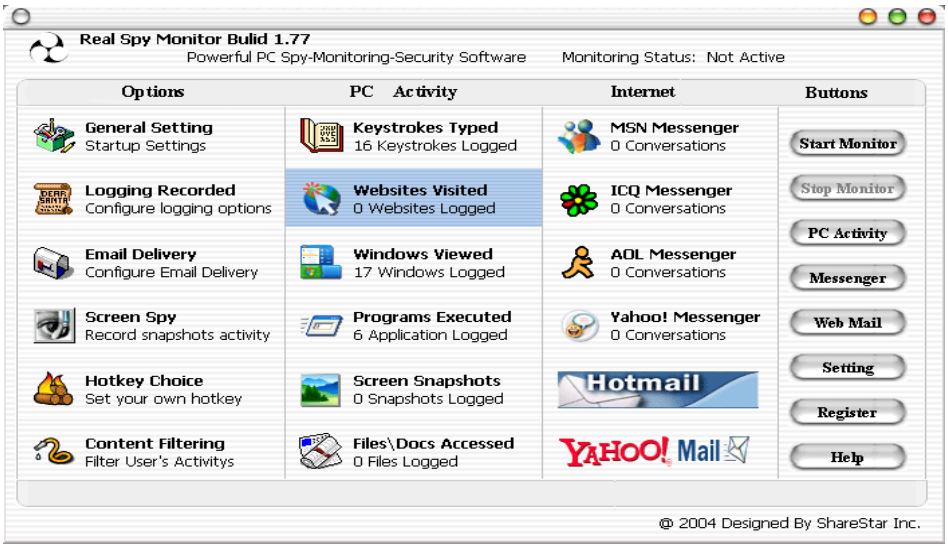

Рис.4. Програма «клавіатурний шпигун» Real Spy Monitor.

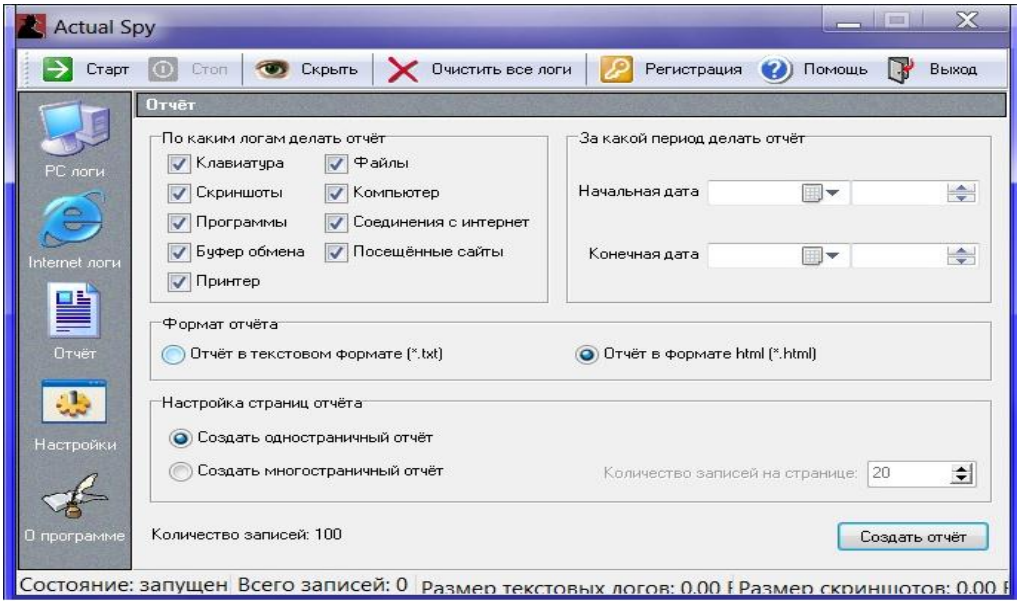

Рис.5. Програма «клавіатурний шпигун» Actual Spy

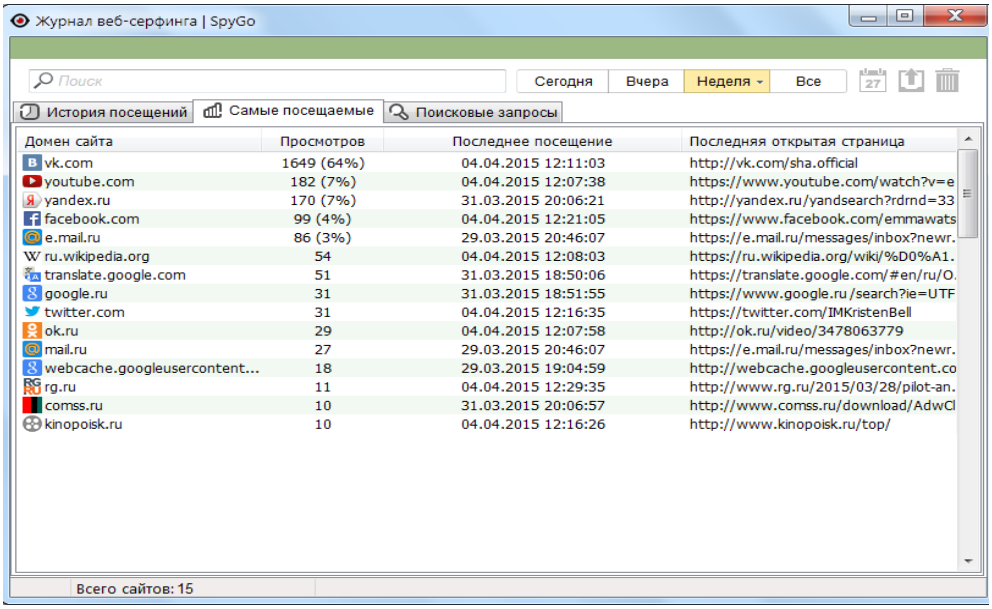

Рис.6. Програма «клавіатурний шпигун» SpyGo

Рис.7, 8. Апаратний «клавіатурний шпигун» PS/2 (KeeLog)

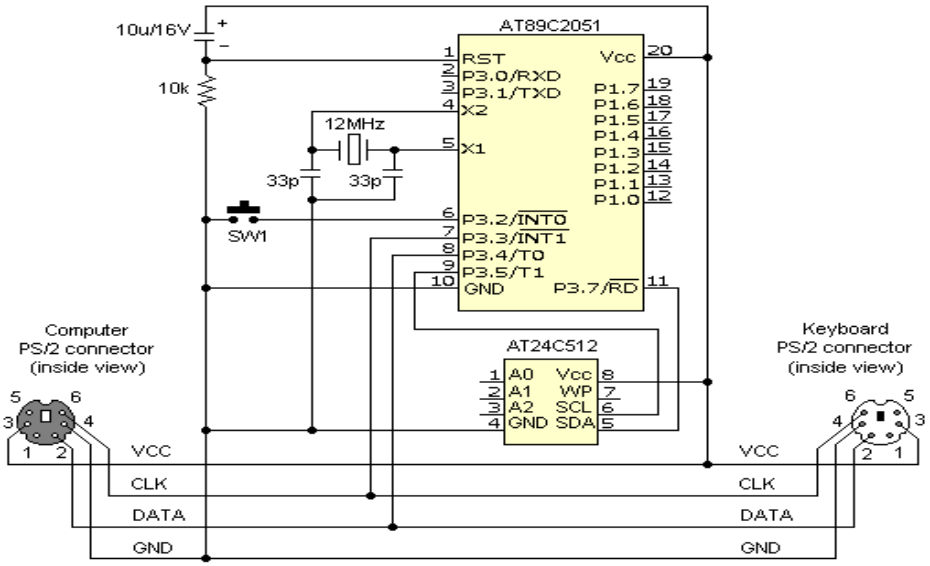

Рис.8. Схема апаратного «клавіатурного шпигуна» PS/2 (KeeLog).

Рис.9, 10. Апаратний «клавіатурний шпигун» USB.

Для реалізації захисту від зазначеної загрози необхідно використовувати Firewall, що буде перевіряти мережеву активність; менеджери паролів, що будуть вводити паролі без використання клавіатури; періодично оновлювати систему [7, 9, 10, 11].

Загроза інформації профілю Facebook шляхом реалізації методу Phishing. Зазначений метод пов'язаний із створенням підставної сторінки авторизації, візуально ідентичної до оригіналу, з подібною, але відмінною URL - адресою. Перш за все необхідно створити профіль на веб – хостінгу та підставну сторінку авторизації. Для цього можливо знайти інформацію з приводу клонування веб – сайтів. Потім створюється форма, за якою інформація, введена користувачем, зберігалася б. Для реалізації захисту від зазначеної загрози необхідно бути пильним та перевіряти URL – адресу сторінки. Також необхідно використовувати антивіруси та додатки, що захищають від веб – загроз, таких як Norton, McAfee.

Рис.11. Підставна сторінка авторизації (Phishing - сторінка)

Загроза інформації профілю Facebook шляхом реалізації атаки «людина посередині». Реалізація зазначеної загрози досягається шляхом створення клону бездротової мережі Wi-Fi, використовуючи утиліту Wi-Fi Pumpkin на основі бездротового мережевого адаптера та плати Raspberry Pi. Після підключення користувача, проти якого направлена атака, до бездротової мережі – клону є можливість виявити параметри підключення та підставити Fishing – сторінку. Для реалізації захисту від цієї загрози необхідно бути пильними при підключенні до відкритих Wi-Fi мереж.

Рис.12. Wi-Fi-Pumpkin v0.8.5

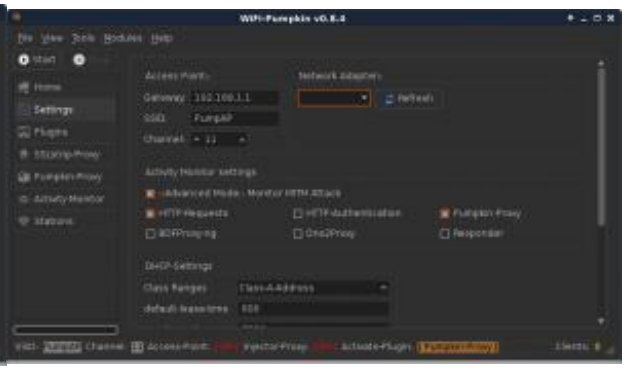

Рис.13. Wi-Fi-Pumpkin v0.8.4

Рис.14. Бездротовий мережевий адаптер Wi-Fi- MT 7601

Рис.15. Бездротовий мережевий адаптер Tenda U12

Рис.16. Материнська плата Raspberry Pi Compute Module I/O Board V3

Рис.17. Плата розширення портів вв/вив (GPIO) для Raspberry Pi

Загроза інформації профілю Facebook шляхом захвату паролю. Під поняттям «захвату паролю» мається на увазі метод взлому слабо захищеного сайту або його створення для отримання ім'я доступу та пароль, на якому також зареєстрований користувач, проти якого направлена атака. Реалізація загрози досягається шляхом взлому слабо захищеного сайту чи розміщення створеного сайту в мережі Internet, при реєстрації на якому і отримується інформація входу. Для реалізації захисту від цієї загрози необхідно не використовувати інформацію входу в профіль Facebook на інших сайтах [7, 12, 13, 14, 15].

Вразливість SS7 протоколу в Facebook Messenger. Реалізація загрози через використання вразливості SS7 протоколу досягається шляхом переносу інформації профілю користувача, проти якого направлена атака, на новий пристрій та загрузка архіву за рахунок перехвату сервісного sms - повідомлення Facebook з кодом верифікації.

SS7 – це система сигнальних протоколів для обміну інформацією та маршрутизації викликів.

Для реалізації перехвату sms - повідомлення для початку зловмиснику необхідно порушити доступність абонента (Dos). Для цього зловмисник надсилає в мережу користувача, проти якого направлена атака, повідомлення UpdateLocation (з адресою нового комутатора) від імені MSC (комутатор). Повідомлення відправляється на HLR (база даних абонентів). Після чого HLR в базі відв'язує дійсний комутатор та надає профіль абонента комутатору зловмисника. Таким чином абонент опиняється поза зоною мережі доки абонент не переміститься в зону дії іншого комутатора та перезавантажить пристрій, та виконає будь-яку вихідну дію (повідомлення, дзвінок), що відновить адресу комутатора абонента.

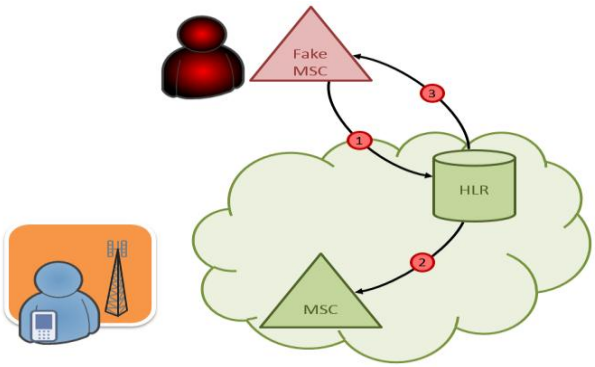

Рис.18. Порушення доступності абонента (Dos - атака)

Наступним кроком є ініціювання відправлення сервісного sms - повідомлення з Facebook для користувача, проти якого направлена атака. Сервісне sms - повідомлення надходить на комутатор, що обслуговує відправника. Потім відбувається направлення повідомлення на sms - центр (повідомлення MO-ForwardSM протоколу MAP). Далі направляється запит на адресу в HLR (повідомлення SendRoutingInfoForSM). Після Dos - атаки користувач опиняється поза доступом, а буде надана адреса зловмисника sms - центру. Таким чином повідомлення буде направлено зловмиснику в повідомленні MT - ForwardSM протоколу MAP.

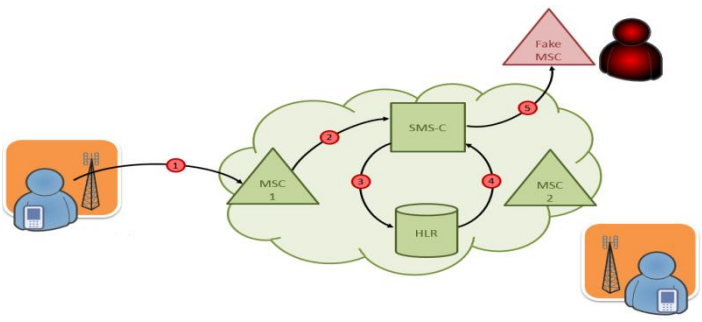

Рис.19. Перехват сервісного sms - повідомлення Facebook

Метод атаки SS7 протоколу працює в реальному часі без встановлення на пристрій користувача, проти якого направлена атака. Не має значення, на якому пристрої встановлений Facebook Messenger (смартфон, планшет, комп'ютер з операційною системою Android, Windows, iOS). Взлом Facebook Messenger може бути виконаний з будь-якого пристрою за умови наявності актуальних браузерів таких, як Opera, Google Chrome, Mozilla Firefox, Internet Explorer та за умови підключення до мережі. Взлом та скачування інформації користувача, проти якого направлена атака, відбувається максимум за 20 хвилин. Під час атаки протоколу SS7 та скачування інформації користувач не отримує жодних повідомлень, так як процес відбувається в фоновому режимі, і немає жодних впливів на роботу пристроїв. Процес не визначається жодним сканером, антивірусом. Заряд батареї пристрою витрачається як зазвичай, зайві процеси в диспетчері відсутні. Для реалізації захисту від цієї загрози полягає в обмеженому використанні номеру, зазначеного в Facebook [8, 16].

Висновки. Відповідно до вищезазначеного можемо побачити, що загроз для інформації профілю Facebook є дуже багато. Та невід'ємною частиною атаки є збір певної необхідної інформації про користувача, на профіль Facebook якого направлена атака. Тому, перш за все, необхідно використовувати унікальні контактні дані для профілю. Не треба нехтувати такими профілактичними методами захисту як періодичне оновлення системи, встановлення вдосконалених антивірусних програм, обмеження стороннього доступу до своїх пристроїв, які використовуються для входу до профілю Facebook.

Список використаних джерел:

1. Самойдюк А. Три самых популярных языка программирования в 2018 году, 2018р. [Електронний ресурс] – Режим доступу: www.rb.ru/story/top-3-programming-languages;
2. HelpUAdmin. Взлом паролей от аккаунтов Фейсбука, Инстаграма и Твиттера путем брутфорса, 2018р. [Електронний ресурс] – Режим доступу: www.helpugroup.ru/vzlom-parolej-ot-akkauntov-fejsbuka-instagrama-i-tvittera-putem-brutforsa;
3. Как я взломал Facebook, 2014р. [Електронний ресурс] – Режим доступу: www.habr.com/post/245961;
4. Мірошниченко М. Методи взлому хакерами облікового запису Facebook і способи захисту від них, 2018р. [Електронний ресурс] – Режим доступу: www.hetmanrecovery.com/ru/recovery_news/methods-of-hacking-a-facebook-account-and-ways-to-protect-against-them.htm$;
5. Як дістати чужий пароль к Фейсбук [Електронний ресурс] – Режим доступу: www.ru.wikihow.com;
6. Взлом Фейсбук [Електронний ресурс] – Режим доступу: www.hackmarket.info/vzlom_facebook.html;
7. Nelson Aguilar. 4 метода получения чужих паролей в Facebook [Електронний ресурс] – Режим доступу: www.securitylab.ru/analytics/492396.php;
8. Онлайн взлом FB Messenger через SS7 эксплойт [Електронний ресурс] – Режим доступу: www.appmsr.net/vzlom-fbmessenger;
9. Анохин Р. Программа шпион для компьютера: 5 лучших утилит, 2017р. [Електронний ресурс] – Режим доступу: www.geek-nose.com/programma-shpion-dlya-kompyutera-kak-soxranit-kontrol;
10. Аппаратный кейлоггер Open Source [Електронний ресурс] – Режим доступу: www.keelog.com/ru/diy.html;
11. Кейлогер — что это такое и как оградить себя от кражи пароля? [Електронний ресурс] – Режим доступу: www.no-viruses.ru/blog/kejloger-chto-eto-takoe-i-kak-ogradit-sebya-ot-krazhi-parolya.html;
12. Solid Team. Бездротовий мережевий адаптер Wi-Fi- MT 76 [Електронний ресурс] – Режим доступу: www.sdtm.com.ua/uk/katalog/setevoe-oborudovanie/wi-fi-oborudovanie/440;
13. МобіМанія. Tenda Бездротовий мережевий адаптер U12 [Електронний ресурс] – Режим доступу: www.mobimania.ua/computer/network/89-Bezdrotovyj-merezhevyj-adapter-U12_.html;
14. Chipdip. Raspberry Pi Compute Module I/O, Материнская плата для удобной отладки Raspberry Pi Compute Module 3 / 3 Lite [Електронний ресурс] – Режим доступу: https://www.chipdip.ru/product/raspberry-pi-compute-module-i-o;
15. Chipdip.Плата. Расширения портов ввода/вывода (GPIO) для Raspberry Pi [Електронний ресурс] – Режим доступу: www.chipdip.ru/product/gertboard-for-raspberry-pi;

PhoenixGruppe. Взлом мобильной связи через SS7: перехват SMS, слежка и прочее, 2017р. [Електронний ресурс] – Режим доступу: www.graph.io/Vzlom-mobilnoj-svyazi-cherez-SS7-perehvat-SMS-slezhka-i-prochee-08-19.

Надійшла: 27.07.2018 Рецензент: к.т.н. Курченко О.А.