УДК 004.056
Лізунов С.І.[1], Верещака М.П.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] асп. НУ «Запорізька політехніка»

ВІРУСИ В МАРШРУТИЗАТОРІ: ЧИМ НЕБЕЗПЕЧНІ, ЯК ЇХ ВИЯВИТИ ТА УСУНУТИ

У світі, де цифрові технології проникають в усі сфери життя, інформаційна безпека стає пріоритетом. Багато користувачів добре обізнані про віруси, які можуть потрапити в комп'ютери і ноутбуки, але далеко не всі знають, що вони можуть також вражати домашній маршрутизатор. Маршрутизатори, ключовий елемент сучасних мереж, дедалі частіше стає мішенню для кіберзлочинців.

Способів заразити маршрутизатор досить багато, але з найпоширеніших на практиці можна навести наступні:

Вразливості програмного забезпечення. Якщо маршрутизатор не оновлюється і використовує застаріле програмне забезпечення, зловмисники можуть скористатися вразливостями в цьому програмному забезпеченні, щоб отримати доступ до маршрутизатора і заразити його вірусом.

Пароль. Якщо пароль для маршрутизатора дуже простий, зловмисники можуть легко його підібрати і отримати доступ, всіляко налаштувавши його і завантаживши шкідливі програми. Це стосується не тільки мережевого пароля, але і пароля до панелі адміністратора маршрутизатора.

Фішинг. Зловмисники можуть надсилати фішингові електронні листи або повідомлення в соціальних мережах, які виглядають як справжні. У них користувачів просять надати свої дані для входу в різні сервіси, в тому числі у адміністративну панель маршрутизатора. Це може призвести до того, що зловмисники отримають доступ і заразять маршрутизатор вірусом.

Зараження маршрутизатора вірусом може призвести до серйозних наслідків. Ось деякі з них:

Витік персональних даних. Вірус може перехоплювати дані, що передаються через маршрутизатор, включаючи дані банківських карток, паролі, особисту інформацію тощо.

Спам. Заражений маршрутизатор може бути використаний зловмисниками для розсилки спаму.

Доступ до пристроїв у вашій мережі. Зловмисники можуть отримати доступ до пристроїв у вашій мережі, таких як комп'ютери, принтери та інші пристрої, і використовувати їх у своїх цілях.

Уповільнення роботи мережі. Заражений маршрутизатор може входити у масштабні ботнет-мережі для організації DDoS-атак. Використання значної

частини мережевих ресурсів призводить до уповільнення та погіршення якості інтернет-з'єднання.

Зазвичай користувач не відразу розуміє, що проблеми пов'язані з маршрутизатором. Однак є кілька ознак, які можуть вказувати на проблему:

Несподівано низька швидкість інтернету або проблеми зі з'єднанням. Ця ознака може мати інтервальний період, коли канал зв’язку зайнятий зловмисниками.

Поява незрозумілих повідомлень веб-браузера, таких як попередження про безпеку (недійсний сертифікат HTTPS), банерна реклама тощо.

Незвичайна активність на маршрутизаторі, наприклад, несподівана зміна налаштувань або поява нових пристроїв у списку підключених пристроїв до маршрутизатора.

Якщо ви помітили одну з цих ознак, негайно перевірте свій комп'ютер, ноутбук, телефон або інший пристрій, з якого ви виходите в інтернет, на наявність вірусів. Найчастіше проблема криється саме в пристрої. Якщо ви впевнені в "чистоті" свого пристрою, а "симптоми" вірусу з’являються на всіх інших гаджетах, то шкідливе програмне забезпечення, ймовірно, знаходиться в маршрутизаторі. Необхідно переходити до процесу його видалення.

Видалення вірусу з маршрутизатора може вимагати великих знань і досвіду, оскільки різні програми мають свої властивості та особливості. Ось кілька кроків, які допоможуть вам впоратися з більшістю випадків:

Скиньте маршрутизатор до заводських налаштувань за замовчуванням і необхідно налаштувати його заново. Зазвичай це робиться натисканням і утриманням клавіші Reset протягом 15 секунд.

Змініть пароль (як панелі адміністратора маршрутизатора, так і мережі) на більш складний і надійний.

Оновіть прошивку маршрутизатора до останньої версії. Універсальної інструкції не існує. Зазвичай, необхідно перейти на офіційну веб сторінку виробника маршрутизатора та завантажити останню версію програмного забезпечення для маршрутизатора.

Використовуйте антивірусне програмне забезпечення для перевірки мережі на наявність вірусів та інших шкідливих програм.

Найефективніший метод протидії будь-якому вірусу полягає у його своєчасній профілактиці. Розглянемо наступні кроки:

Регулярно оновлювати програмне забезпечення для маршрутизатора до останньої версії. Необхідно перевіряти знайдені CVE (Поширені вразливості та ризики) у останніх версіях програмних забезпечень і, у разі наявності, додавати додатковий захист від знайдених вразливостей якщо ці вразливості ще не закриті розробниками.

Використовуйте надійні паролі, які важко вгадати або підібрати. Перевіряйте у відкритих базах даних наявність відомих паролів та використовуйте складний пароль із цифрами, буквами в різному регістрі та іншими символами.

Не відповідайте на фішингові електронні листи та не надавайте особисту інформацію, якщо ви не впевнені, що це справжній запит. Завжди перевіряйте адреси та назви посилань.

Використовуйте антивірусне програмне забезпечення для захисту ваших пристроїв і мережі в цілому. Оновлюйте базу сигнатур до останньої версії

Встановіть файрвол. Файрвол — це програма або пристрій, що контролює вхід та вихід мережевого трафіку. Він може блокувати небажаний доступ до мережі та допомагати блокувати потенційно шкідливі підключення.

Відключити віддалений доступ до налаштувань маршрутизатора. Якщо за замовчуванням цей функціонал відкритий – його необхідно закрити, але в більшості сучасних маршрутизаторів віддалений доступ закритий від початку.

Використовуйте безпечні протоколи зв'язку для підключення по Wi-Fi. Замість застарілих протоколів, таких як WEP (Wired Equivalent Privacy), використовуйте більш безпечні протоколи, наприклад, WPA2 (Wi-Fi Protected Access 2) або WPA3. Вони забезпечують більшу захищеність мережі Wi-Fi.

Встановіть VPN (віртуальну приватну мережу). VPN шифрує ваш мережевий трафік і забезпечує конфіденційність та безпеку під час передачі даних через інтернет, навіть на відкритих мережах Wi-Fi.

Увімкніть двофакторну автентифікацію. Двофакторна автентифікація зміцнює безпеку вашої мережі, вимагаючи додаткового підтвердження, крім пароля, для входу в адміністративну панель маршрутизатора.

Перед підключенням до мережі перевірте всі підключені пристрої на наявність вірусів та інших шкідливих програм.

Додатково, важливо періодично проводити аудит безпеки мережі, щоб виявити можливі вразливості та вчасно їх усунути. Також слід регулярно резервувати дані, щоб у разі інциденту мати можливість відновлення інформації та налаштувань.

Захист вашого маршрутизатора від вірусів та інших кіберзагроз є важливою складовою забезпечення вашої інформаційної безпеки.