СЕКЦІЯ 7. SECURITY. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Кондрашов Д. А.,
Криворізький національний університет
Кузнєцов Д. І.
к.т.н., доцент, Криворізький національний університет

ОГЛЯД СУЧАСНОЇ ПРОБЛЕМАТИКИ ІТ-БЕЗПЕКИ

Розглянуто актуальні вірусні вразливості в ОС сімейства Microsoft Windows. Наведено теоретичні відомості класифікації вірусів та шкідливого ПЗ. Дано рекомендації з покращення рівня захисту комп'ютера від вірусного ПЗ.

Вірус (Virus) є найвідомішою формою malware. Часто термін «комп'ютерний вірус» використовується взаємозамінно з терміном «шкідливе ПЗ». Насправді, ці поняття відрізняються одне від одного. Термін malware означає будь-яке шкідливе програмне забезпечення, включаючи комп'ютерний вірус. Відмінною рисою вірусу є те, що він здатний копіювати себе та поширюватися шляхом приєднання до файлів звичайних програм.

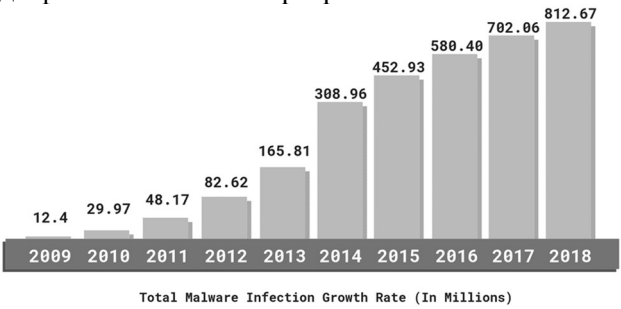

Рис. 1. Загальний темп зростання зараження вірусами комп'ютерів

Майже всі сучасні віруси та шкідливі програми створюються зловмисниками, які мають на меті отримати конфіденційні дані користувача або використовувати його комп'ютер для особистої вигоди. Вирізняють такі види:

Черв'як (Worm) – програма, яка здатна до самовідтворення. Її шкода полягає в захаращенні комп'ютера, через що він починає працювати повільніше. Черв'як не може стати частиною іншої нешкідливої програми, тобто є незалежним процесом.

Троян (Trojan) – шкідливе програмне забезпечення, що потрапляє на комп'ютер під виглядом корисної програми. Trojan встановлюється на ПК разом з потрібною програмою через майстер установки та використовується для крадіжки конфіденційних даних, збору інформації, розсилки спаму або порушення загальної працездатності ПК.

Drive-by Download – вид шкідливого ПЗ, що автоматично завантажується на комп'ютер користувача під час відвідування ненадійних веб-сайтів. Drive-by складається з невеликих фрагментів коду, які часто залишаються непоміченими слабкими засобами захисту. Після впровадження заражений код використовує вразливості операційних систем, веб-браузерів і модулів, що підключаються до них, таких як Java, Adobe Reader, Adobe Flash.

Шпигунське програмне забезпечення (Spyware) – це будь-яке програмне забезпечення, яке збирає конфіденційну інформацію з ПК і надсилає її віддаленим користувачам.

Рекламне програмне забезпечення (Adware) призначене для відображення реклами, працює через налаштування браузера або мережі. Не завдає шкоди пристроям, але може уповільнити їхню роботу.

Руткіт (Rootkit) – набір програмного забезпечення, що використовується для отримання адміністративного доступу до роботи ОС з метою повного контролю. Використовуються для приховування шкідливої активності.

Здирники (Ransomware) – це програми, що шифрують всю інформацію на комп'ютері, а потім вимагають оплати для її розшифровки.

У 2021 році найяскравіше виділилися декілька небезпечних вразливостей в ОС сімейства Microsoft Windows різних версій. Дослідники безпеки виявили цілу низку вразливостей у браузерах, серед яких можна виділити такі CVE (Common Vulnerabilities and Exposures):

CVE-2021-28310 – вразливість типу out-of-bounds (OOB) write у бібліотеці Microsoft DWM Core, яка використовується в Desktop

Window Manager. Через недостатню перевірку в коді роботи з масивами даних непривілейований користувач, що використовує DirectComposition API, може записати власні дані в контрольовані ним ділянки пам'яті. В результаті може відбутися псування даних реальних об'єктів, що, в свою чергу, може призвести до виконання довільного коду.

CVE-2021-33742 – помилка в браузерному двигуні Microsoft, що дозволяє записувати дані за межі пам'яті оперованих об'єктів.

Вразливості в браузері Google Chrome, що експлуатують помилки в різних компонентах браузера: CVE-2021-30551, що полягає в неправильній інтерпретації типів даних у скриптовому двигуні v8, CVE-2021-30554 – вразливість типу use-after-free в компоненті Web -2021-21220 – вразливість, що викликає ушкодження купи (heap corruption).

Вразливості у браузерному двигуні WebKit, який використовується переважно у продуктах Apple (наприклад, у браузері Safari). CVE-2021-30661 – вразливість типу use-after-free, CVE-2021-30665 - вразливість, що викликає пошкодження пам'яті, і CVE-2021-30663 – вразливість, що викликає переповнення цілочислової змінної.

Усі перераховані вразливості дозволяють зловмиснику непомітно атакувати систему користувача, якщо той відкриє шкідливий сайт у невчасно оновленому браузері.

Але головною темою кварталу стали критичні вразливості CVE-2021-1675 та CVE-2021-34527 у службі Print Spooler ОС Microsoft Windows, причому як у серверних, так і клієнтських редакціях. Їх виявлення, разом з виявленням Proof-of-Concept експлойту, викликало шум як серед фахівців, так і в ЗМІ, які дали одній з вразливостей назву PrintNightmare. Експлуатація цих вразливостей досить тривіальна, оскільки служба Print Spooler включена в Windows за промовчанням, а методи, за допомогою яких здійснюється компрометація, доступні навіть непривілейованим користувачам, у тому числі віддаленим. У разі для компрометації може використовуватися механізм RPC. В результаті зловмисник з низьким рівнем доступу може заволодіти не тільки локальною машиною, а й контролером домену, якщо ці системи не були вчасно оновлені або на них не були застосовані наявні методи зниження ризиків, пов'язаних із вразливістю.

Для того, щоб убезпечити свої дані, рекомендується користуватися антивірусним програмним забезпеченням, таким як Dr.Web, Kaspersky, ESET NOD32 і Avast. При виборі антивірусного ПЗ варто звернути увагу на такі функції:

Фаєрвол, тобто захист комп'ютера від атак хакерів. Його суть полягає у перевірці інформації, яку користувач переглядає, завантажує чи відкриває.

Веб-захист. Це одні із способів блокування потенційно небезпечних сайтів. У її функції також входить захист від фішингу.

Антиспам – сервіс, що блокує поштові листи із сумнівним чи шкідливим змістом;

Пісочниця (Sandbox). Програма створює «ізольоване середовище», яке слугує для відкриття програм. Після закриття пісочниці, усі зміни скасовуються і не впливають на подальшу роботу комп'ютера.

Варто пам’ятати, що через швидкий розвиток вірусів, жоден антивірус не може гарантувати 100% безпеки, а тому потрібно регулярно робити резервні копії важливої інформації.

ВИСНОВКИ

Таким чином, віруси є важливою проблемою, яка потребує негайного реагування та передчасної профілактики. Для попередження вірусних інфекцій необхідно завантажувати лише ліцензійне ПЗ з офіційних сайтів та своєчасно його оновлювати, адже актуальні версії програм мають найбільш досконалі системи контролю безпеки для захисту користувача, а використання антивірусних програм є обов’язковим.

ЛІТЕРАТУРА

1. 2021 Cyber Security Statistics. URL: https://purplesec.us/resources/cyber-security-statistics/ (дата звернення 16.02.2022).
2. Розвиток інформаційних загроз у другому кварталі 2021 року. Статистика з ПК. URL: https://securelist.ru/it-threat-evolution-in-q2-2021-pc-statistics/103374/ (16.02.2022).
3. Шкідливі програми та віруси: у чому різниця? URL: https://cutt.ly/5Pzjvfu (дата звернення 15.02.2022).