DOI: 10.59647/978-617-520-936-3/1

Вплив комп’ютерних вірусів на інформаційну безпеку: аналіз сучасних загроз та методів захисту

Дем'ян Виноградов студент[1] [i] (ORCID: 0009-0004-7364-8374)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

Стаття присвячена загрозам, які представляють комп'ютерні віруси, та методам їх уникнення для забезпечення інформаційної безпеки. У ній розглядається історія розвитку комп'ютерних вірусів, починаючи з перших прикладів, таких як "Creeper system" та "Brain", і до сучасних загроз. Основна увага приділяється видам шкоди, яку можуть завдавати віруси, зокрема втраті даних, знищенню системних файлів, уповільненню роботи комп'ютерів та поширенню шкідливих програм. У статті також розглядаються основні шляхи проникнення вірусів, серед яких відкриття заражених файлів, завантаження з неперевірених джерел та відкриття підозрілих посилань. На завершення пропонуються рекомендації щодо запобігання вірусним атакам, включаючи використання антивірусів, оновлення операційних систем та роботу з обмеженими правами адміністратора.

Ключові слова: комп'ютерний вірус, інформаційна безпека, захист систем, вірусна атака, несанкціонований доступ.

1. ВСТУП

У сучасному цифровому світі, де інформація є одним з найцінніших ресурсів, комп'ютерні віруси представляють серйозну загрозу для інформаційної безпеки. Комп'ютерний вірус — це шкідлива програма, яка може розповсюджуватися через інші програми і файли, порушуючи роботу систем і завдаючи шкоди даним. Віруси еволюціонують разом із розвитком технологій, що робить їх атаки все більш складними і небезпечними. У цій презентації ми проаналізуємо сучасні загрози, які представляють віруси, розглянемо основні методи їх проникнення, а також ефективні способи захисту. Розуміння цих аспектів є ключовим для забезпечення надійної інформаційної безпеки та захисту цифрових систем від можливих атак.

2. ІСТОРІЯ КОМП’ЮТЕРНИХ ВІРУСІВ

Комп'ютерні віруси існують вже досить давно, і майже всі вони поширюються через Інтернет або його попередники. Більшість вірусів були розроблені для крадіжки інформації користувача, управління живленням або одночасного вимкнення системи. Віруси не стали масовими загрозами одразу. Як і інше зловмисне програмне забезпечення, вони стикалися з проблемами у розповсюдженні. Наприклад, заразити комп’ютери в межах університету було відносно легко, але це було значно складніше зробити в інших місцях. До широкого розповсюдження Інтернету віруси поширювалися через дискети разом з іншими програмами. Перший реально шкідливий комп'ютерний вірус був під назвою «Creeper system» був експериментальним самовідтворюваним вірусом, випущеним у 1971 році. Він заповнював жорсткий диск до тих пір, поки комп'ютер не міг більше працювати. Цей вірус був створений компанією BBN Technologies у США. Перший комп'ютерний вірус для персонального комп’ютера, що виклика глобальну епідемію називався «Brain» і був випущений у 1986 році. Він замінював завантажувальний сектор на дискетах і не давав комп'ютеру завантажитися. Він був написаний двома братами з Пакистану і спочатку розроблявся як захист від копіювання. У 2000-х роках, після розповсюдження інтернету, віруси стали поширеними по всьому світу. Тоді люди почали називати будь-яке зловмисне програмне забезпечення вірусами. Персональна кібербезпека на той момент ще не була розвинута. Слабкий внутрішній контроль над комп'ютерними системами та відсутність автоматизованих інструментів для виявлення і видалення загроз, разом із розповсюдженням піратського ПЗ і використанням торрентів як основних джерел програмного забезпечення замість офіційного придбання, призвели до того, що заражений комп’ютер став майже нормою. Ці обставини стали основою для розвитку ринку антивірусного програмного забезпечення, якого ми знаємо сьогодні.

3. ЗАГРОЗИ ВІД ВІРУСА

Комп’ютерний вірус класифікують на файлові: вірус що має здатність до самопоширення в ваших файлів; завантажувальні: комп’ютерний вірус що записується на завантажувальний сектор дискет, флеш накопичувача, твердого дисках і активується під час активації комп’ютера; Макровірус: комп’ютерний вірус який вбудовується в файли певних типів, для яких передбачені можливості автоматичного виконання .

Основні загрози, які виникають внаслідок зараження вірусами, включають: втрата даних: один з найпоширеніших видів загроз. Вірус може видаляти або пошкоджувати файли, що призводить до втрати важливої інформації без можливості відновлення. Знищення системних файлів: деякі віруси намагаються пошкодити критично важливі системні файли операційної системи. Це може призвести до системних збоїв і потреби в переустановленні ОС. Зниження продуктивності: віруси можуть істотно уповільнити роботу комп'ютера, використовуючи ресурси системи, такі як процесорний час і оперативну пам'ять, для виконання своїх шкідливих функцій. Розподіл шкідливих програм: віруси можуть використовувати заражені комп'ютери для розповсюдження інших шкідливих програм, таких як трояни або черв'яки, що збільшує масштаби атаки. Інші загрози: сюди відносяться крадіжка конфіденційної інформації, несанкціонований доступ до системи, і поширення шкідливих програм на інші комп’ютери.

4. СПОСОБИ ПРОНИКНЕННЯ ВІРУСІВ

Основні способи проникнення вірусів до комп'ютера:

Відкриття заражених вкладок або файлів: один з найпоширеніших способів зараження — це відкриття вкладок або файлів, що містять шкідливі програми: під час відкриття таких вкладок або файлів може завантажитися на ваш комп'ютер шкідливий файл або програма, яка автоматично інсталюється і починає діяти, наприклад, троянський вірус. Завантаження з неперевірених джерел: встановлення програмного забезпечення з неперевірених або сумнівних джерел є ще однією причиною зараження. Завантажені файли можуть містити віруси, які автоматично інсталюються разом із програмами. Відкриття посилань у електронних листах від невідомих відправників:спам електронною поштою вже став класикою розповсюдження вірусів, шахраї надсилають електронні листи, які змушують користувачів натиснути посилання або відкрити вкладений файл, що б там не було, ви отримаєте щось небезпечне на свій ПК після виконання зловмисного сценарію. Зловмисні інтернет-реклами: в світі технологій часто називають "шкідливими повідомленнями", є вірусами, що передаються через натискання на спливаючі оголошення.

5. УНИКНЕННЯ ВІРУСА

Дуже часто для уникнення зараження користувачам рекомендують не запускати підозрілих файлів, не клікати на підозрілі лінки та не вставляти в комп’ютер підозрілих флешок. Проблема в тому, що в реальному житті на файлі чи на посиланні не написано, що вони "підозрілі". Тому варто зосередитися не питанні "як має бути налаштований комп’ютер”, щоби мінімізувати ризик зараження". Оновлювати операційну систему оскільки у будь-якій оперативній системі час від часу знаходять вразливості, які дозволяють зловмисникам атакувати вас, тому розробники програмного забезпечення регулярно випускають оновлення безпеки, які закривають відомі вразливості. На комп’ютері має бути завантажений антивірус, оскільки він захищає від масового поширення вірусів. Сучасні антивіруси майже не впливають на швидкість роботи комп’ютера, але час від часу необхідно запускати повне сканування щоб забеспечити максимальну безпеку для комп’ютера. Працювати під обліковим записом без прав адміністратора у Windows то му що у цій оперативній системі є два типи облікових записів: Стандартний і Адміністратор. Стандартний користувач може виконувати базові завдання, такі як запуск програм, створення і видалення файлів, але для установки програм або зміни системних налаштувань потрібні права адміністратора. На відміну від цього, в MacOS і Linux користувачі за замовчуванням працюють без адміністративних прав і повинні вводити пароль адміністратора для змін в системі чи установлення програм. У Windows для досягнення подібного рівня безпеки потрібно налаштувати обліковий запис вручну.

Щоб перевірити, чи ваш комп'ютер заражений вірусом, звертайте увагу на підозрілі файли, проблеми з доступом до файлів ,несподівані перезавантаження або зависання, уповільнення роботи системи та якщо антивірусне програмне забезпечення перестає працювати. Такі ознаки можуть свідчити про проникнення шкідливого коду, який може пошкоджувати або видаляти файли та красти конфіденційні дані. Якщо ви помітили будь-які з цих ознак, спробуйте провести повне сканування системи за допомогою антивірусного програмного забезпечення та видаліть заражений файл, або переустановіть програмне забезпечення, це особливо ефективно якщо вірус не розповсюджується на інші частини комп’ютера.

6. ВИСНОВОК

Комп’ютерні віруси представляють серйозну загрозу для інформаційної безпеки, порушуючи нормальну роботу систем і завдаючи шкоди даним. Розуміння основних загроз і методів проникнення вірусів дозволяє вжити ефективні заходи для їх уникнення та захисту систем. Надійний захист і уважність при роботі з інформаційними системами є ключовими для підтримки інформаційної безпеки.

Список літератури:

[1] Як убеспечитися від зараження комп’ютерним вірусом? Поради.Інститут масової інформації.2020, Україна URL: https://imi.org.ua/advices/yak-ubezpechytysya-vid-zarazhennya-komp-yuternym-virusom-porady-i31434

[2] Alex Uhde. A short history of computer viruses. Sentrian. 2017. URL: https://www.sentrian.com.au/blog/a-short-history-of-computer-viruses

[3]Комп’ютерний вірус.2023. URL: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81

[4] 5 Common Ways of Getting a Computer Virus. Geeks on Wheels. Geek’s Blog. URL: https://geeksonwheels.co.nz/security-safety/five-common-ways-of-getting-a-computer-virus/

[5] Що таке комп’ютерний вірус? Історія, типи, приклади , та інше. URL: https://gridinsoft.ua/virus

[i] *Робота виконана під керівництвом к. т. н., доц. Євгенії Шабали*