УДК 343

КОМП'ЮТЕРНІ ВІРУСИ – ШКІДЛИВІ ПРОГРАМНІ ЗАСОБИ, РУШІЙНА СИЛА МОДИФІКАЦІЇ

Ричка Д.О., аспірант
Дніпровський національний університет імені Олеся Гончара

У статті розглянуто шкідливі програмні засоби, досліджено особливості комп'ютерних вірусів, розглянуто форми вірусів. Досліджено основні типи вірусних атак та проаналізовано вплив програм-вірусів, на підставі чого розроблено засоби захисту від вірусів.

Ключові слова: *шкідливі технічні засоби, програми-шпигуни, вірус (комп'ютерний вірус, програма-вірус), «троянський кінь», хакер, «хробаки», «логічні бомби», макроси (макровіруси), міжплатформні віруси, віруси-невидимки (стелс-віруси), поліморфні віруси, багатокомпонентні віруси, самооновлювані віруси, антивірусна програма (антивірус).*

В статье рассмотрены вредные программные средства, исследованы особенности компьютерных вирусов, рассмотрены формы вирусов. Исследованы основные типы вирусных атак и проанализировано влияние программ-вирусов, на основании чего разработаны средства защиты от вирусов.

Ключевые слова: *разрушительные технические средства, программы-шпионы, вирус (компьютерный вирус, программа-вирус), «троянский конь», хакер, «черви», «логические бомбы», макросы (макровирусы), платформах вирусы, вирусы-невидимки (стелс-вирусы), полиморфные вирусы, многокомпонентные вирусы, самообновляемые вирусы, антивирусная программа (антивирус).*

Rychka D.O. COMPUTER VIRUSES – HARMFUL SOFTWARE, ELECTRONIC POWER MODIFICATIONS

The article deals with malicious software tools, the features of computer viruses are investigated, forms of viruses are considered. The main types of virus attacks are investigated and the influence of programs-viruses on the basis of which the means of protection against viruses have been developed.

Key words: *malware, spyware, virus (computer virus, virus program), Trojan horse, hacker, worms, logical bombs, macros (macroversia), interplatform viruses, invisible viruses (stealth viruses), polymorphic viruses, multicomponent viruses, self-recovering viruses, antivirus software (antivirus).*

Постановка проблеми. Із розвитком інформаційних технологій (далі – ІТ) суспільство перейшло від індустріального до інформаційного етапу розвитку еволюції. Важко уявити людину XXI ст. без гаджетів, Інтернету, соціальних мереж та електронної пошти. ІТ стали невід'ємною частиною нашого життя і визнані передовою галуззю світу. Тепер доступ до електронних даних можуть отримувати не лише спеціальні служби, а й зацікавлені хакери. Одним із засобів отримання електронної конфіденційної інформації виступають віруси різної природи. Якісний аналіз впливу комп'ютерних вірусів на недоторканість приватного життя людини необхідний, аби дослідити основні тенденції ураження ЕОМ, мереж та інформації, що міститься на них, та розробити швидкі, прості та ефективні засоби захисту від вірусних атак, які стануть у пригоді кожному.

Ступінь розробленості проблеми. Дослідженню впливу шкідливих програм – комп'ютерних вірусів приділялася увага великої кількості видатних вчених, таких як Е. Авер'янова, Д. Азарова, А. Білоусов, С. Бородіна, В. Бутузова, В. Вєхова, Н. Гадіон, О. Гладуна, В. Голубєва, А. Гребєнькова, О. Григорьєва, Г. Долженкова, М. Журби, І. Карася, В. Кіютіна, І. Клепицький, О. Книженко, О. Користіна, Л. Краснова, В. Крачевський, С. Кузьміна, М. Литвинова, Ю. Ляпунова, С. Максимова, А. Музика, А. Новікова, П. Смагіна, М. Погорецький, М. Рудик, В. Шеломенцева, В. Хахановський, І. Юрченко та ін.

Метою наукової **статті** є дослідження особливостей комп'ютерних вірусів та, як наслідок, розроблення засобів захисту від них.

Досягнення поставленої мети забезпечується розв'язанням таких завдань дослідження:

1) ознайомлення зі шкідливим програмними засобами;

2) дослідження особливостей комп'ютерних вірусів;

3) розгляд найтиповіших форм вірусів;

4) виявлення місць, функціонально придатних для прихованого існування вірусів;

5) ознайомлення з основними типами вірусних атак;

6) аналіз наслідків, спричинених різними формами комп'ютерних вірусів;

7) розроблення дієвих засобів захисту інформації та систем ЕОМ від комп'ютерних вірусів.

Виклад основного матеріалу. Програмні засоби (комп'ютерні програми) є певним набором інструкцій у вигляді слів, цифр, кодів, схем, символів, виражених у формі, придатній для зчитування комп'ютером, який приводить цю програму в дію для досягнення певної мети. Як предмет злочину, передбаченого ст. 361-1 Кримінального кодексу України, комп'ютерні програми (програмні засоби) повинні бути шкідливими, тобто здатними забезпечити несанкціонований доступ до інформації, а також змінити, знищити, пошкодити, заблокувати комп'ютерну інформацію чи ту, яка передається мережами електрозв'язку [1, с. 464].

Шкідливі програмні та технічні засоби, операції з якими заборонені, можуть мати вигляд шкідливих комп'ютерних програм або ж технічних пристроїв, які працюють із використанням таких програм.

Найпоширенішими різновидами шкідливих програмних засобів є:

– комп'ютерні віруси – комп'ютерні програми, здатні після проникнення до операційної системи ЕОМ чи до автоматизованої системи (далі – АС) порушити нормальну роботу комп'ютера, АС чи комп'ютерної мережі, а також знищити, пошкодити чи змінити комп'ютерну інформацію;

– програми, призначені для нейтралізації паролів та інших засобів захисту комп'ютерних програм чи комп'ютерної інформації від несанкціонованого доступу;

– програми-шпигуни, які після їх проникнення до певної АС, комп'ютерної мережі, операційної системи ЕОМ чи окремої комп'ютерної програми забезпечують несанкціонований доступ сторонньої особи до інформації, яка зберігається у ЕОМ, АС, мережі чи програмі або ж непомітно для власника чи законного користувача здійснюють несанкціоновану передачу такої інформації сторонній особі [2].

Одним із різновидів шкідливих комп'ютерних програм є комп'ютерні віруси.

Програма-вірус – це спеціально створена програма, яка здатна сама приєднуватися до інших програм (тобто пристосовуватися і «заражати» їх) і у разі запуску спричиняти різні негативні наслідки (псування файлів і каталогів, перекручування інформації, у т. ч. результатів обчислення, засмічення чи спотворення пам'яті ЕОМ) та створювати інші перешкоди у роботі ЕОМ чи АС.

Шкідливі технічні засоби – це різного роду прилади, обладнання, устаткування тощо, за допомогою яких вчиняється несанкціонований доступ до ЕОМ чи АС. Такі засоби здатні призвести до витоку, втрати (знищення), підробки (фальсифікації), блокування інформації, спотворення процесу обробки інформації, що функціонує в ЕОМ, АС, комп'ютерних системах чи мережах електрозв'язку, або до порушення встановленого порядку її маршрутизації (ст. 361 КК) [1, с. 464–465].

Для створення шкідливих програм необхідні знання у сфері програмування. Сьогодні навчитися створювати віруси різної складності та різних галузей застосування, контролювати будь-який комп'ютер чи здобути паролі від систем, проводити махінації з метою отримання грошових коштів від жертви не складає труднощів. Ввівши у рядок пошуку потрібне запитання, можна легко знайти відповідь, тож, провівши такий експеримент, ми знайшли детальний посібник для застосування хакерами.

Можна створити як серйозний вірус, так і вірус-жарт. Найгірше, що можуть зробити віруси-жарти – це зламати систему, однак після перевстановлення системи ПК працюватиме без змін [3], тож вони не становлять високої суспільної небезпеки, перейдемо до більш серйозних шкідливих програм.

Комп'ютерний вірус є зловмисною комп'ютерною програмою, в якій міститься частина коду, що починає свою дію після запуску вірусу в комп'ютерній системі. Під час роботи вірус заражає інші програми копіями самого себе. Ефект дії вірусу може варіюватися від легкого роздратування користувача до повного знищення всіх даних у системі [4]. Однак деякі віруси можуть реплікувати самих себе і поширюватися в інші системи. Це ускладнює локалізацію вірусів і захист від них [5].

Щоб написати простий вірус, достатньо ввести кілька рядків програмного коду. Віруси можна передавати по лініях зв'язку або поширювати на інфікованих носіях, що значно ускладнює локалізацію творця вірусу. Деякі віруси можуть переховуватися усередині інших програм або проникати в операційну систему комп'ютера. До вірусних атак вразливі всі без винятку комп'ютерні операційні системи, однак деякі з них більш уразливі за інші. Віруси досить часто переховуються у комп'ютерних іграх, які завантажуються через Інтернет, також їх можна виявити в макросах, що використовуються в офісних інформаційних системах, або в компонентах, що завантажуються з Інтернету. Шляхи потрапляння вірусів у комп'ютери різні, але загальне в них одне – віруси входять до комп'ютерних систем виключно з зовнішніх джерел. Як тільки вірус входить у систему, він може почати свою руйнівну діяльність відразу або ж очікувати активації якоюсь подією, наприклад, отриманням певних даних або настанням заданої дати або часу.

Відомі кілька різних форм вірусів, які можуть вдертися до комп'ютерної системи.

«Троянський кінь» – це комп'ютерна програма, яка маскується або ховається в частині програми. На відміну від інших вірусів, троянці не реплікують самих себе в системі. Деякі форми «троянських коней» можуть бути запрограмовані на саморуйнування і не залишати жодних слідів, крім заподіяних ними руйнувань. Вони можуть використовуватися для отримання паролів і відсилання їх назад хакеру, для банківських шахрайств, коли невеликі суми грошей знімаються з законних рахунків і передаються на секретний [5].

В Інтернеті можна зустріти не тільки теоретичні аспекти хакерської діяльності, а й практику застосування. На одному з таких ресурсів були навіть проведені експерименти. За допомогою трояну можливо отримати доступ до чужої поштової скриньки. Для цього проводиться розсилання електронних листів із вбудованими вірусами. Лист містить лише посилання на вірус, зазвичай зміст листа має чимось «зачепити» користувача, він повинен бути таким, на який користувач не зможе не відреагувати. Прикладами троянів є: DarkComet RAT, SpyEye, Carberp та ін. Автор експерименту використовував модифіковану версію трояна ZeuS (на момент створення, 29 жовтня 2015 р., його не виявляв жоден антивірус, до того ж, у ньому була функція відключення процесів, серед яких є Dr.Web). На комп'ютері жертви був встановлений Comodo, що навіть полегшило проникнення вірусу. В якості жертви було обрано бухгалтера їх керуючої компанії. Як змусити запустити вірус? Якщо просто відправити посилання –

зрозуміло, що переходити за ним ніхто не буде, обіцяти золоті гори в листі – теж минуле століття, на таке користувачі вже не реагують, тому лист було відправлено нібито від податкової служби (тепер уже фіскальної).

Як і розраховувалося, жертва скачала програму і запустила інсталятор оновлення форми звітності (інсталятор зроблено за допомогою Inno Setup за 5 хвилин), саме він встановить і запустить троян, після чого можливий повний контроль над комп'ютером жертви, внаслідок чого можливо переглянути список процесів комп'ютера, в якому, до речі, не буде трояну. Можливо переглядати файлову систему та навіть дізнаватися список паролів (файли Cookies), які збережені у браузері [6]. Нескладні знання у сфері IT відчиняють широкі кордони для розвитку комп'ютерної злочинності.

«Хробаки» є програмами, які руйнують комп'ютерну систему, вони можуть проникати до програм обробки даних і підміняти або руйнувати дані. Вони подібні до «троянських коней», оскільки не можуть реплікувати самих себе. Як віруси, вони можуть завдавати великих руйнувань, якщо їх вчасно не виявити. Набагато простіше ліквідувати «хробака» або «троянського коня», якщо існує тільки єдина копія програми-руйнівника [5].

Ми легко знайшли в Інтернеті статтю, присвячену створенню «хробака» під назвою .bat вірус. Аби створити .bat-вірус, потрібен текстовий редактор, для цього підійде Блокнот. Створивши і відкривши новий текстовий документ, потрібно вписати туди той код (команди), які він повинен виконати, після чого за допомогою меню зберегти, задавши йому ім'я з розширенням .bat і вказавши тип файлу «Все файлы». Вікна командного рядка, які нескінченно і дуже швидко відкриваються, не дадуть користувачеві спокійно працювати. Закрити їх не встигне ніхто і дуже скоро вони заб'ють оперативну пам'ять комп'ютера, що загальмує його роботу аж до повного зависання [7].

«Логічні бомби» подібні до програм, що використовуються для «троянських коней», однак вони мають таймер, який підриває їх у задану дату і час. Наприклад, вірус Michelangelo має тригер, встановлений на день народження знаменитого художника Мікеланджело – 6 березня. Завдяки вбудованому механізму затримки «логічні бомби» активно використовуються для шантажу. Наприклад, шантажист може послати повідомлення, що, якщо йому буде виплачена певна сума грошей, він надасть інструкцію для відключення «логічної бомби».

Шляхи проникнення вірусів можуть бути найрізноманітнішими. Віруси потрапляють у вашу комп'ютерну систему з безлічі різноманітних джерел, виконуваних програм, програм і файлів, що передаються, програмного забезпечення, придбаного в архівованій формі.

Пропонуємо перейти до розгляду структури зберігання даних на гнучких дисках, із метою виявлення місць, функціонально придатних для прихованого існування вірусів.

Гнучкі диски можуть зберігати файли даних, програм і програмне забезпечення операційних систем. Вони виконують роль посередника у передачі файлів даних. Гнучкий диск складається з завантажувального сектора і даних, за необхідністю у ньому може зберігатися інформація, необхідна для завантаження комп'ютера, або інформація про розділи, завантаження, про розміщення файлів, тобто вони містять всю змістовну інформацію, яка зберігається на дискеті [5].

Улюбленим місцем розміщення вірусів є завантажувальні сектори і виконувані файли, що зберігаються на дискеті. Вміщені в завантажувальному секторі віруси можуть запускатися під час завантаження системи з дискети. Віруси, поміщені у виконувані файли, запускаються разом із зараженою програмою, після чого починають свою діяльність у комп'ютерній системі. Ті самі можливості перенесення вірусів забезпечують компакт-диски, що нині стали основним засобом перенесення файлів та інформації між комп'ютерами. У компакт-дисках міститься двоїчна цифрова інформація, яка записується на диск шляхом створення мікроскопічних ямок на поверхні диска. Інформація зчитується під час проходу по диску променя світла, що генерується лазером. Компакт-диски подібні до гнучких дисків тим, що для зберігання даних у них також використовується структура, що складається з завантажувального сектора і даних.

Інтернет надав користувачам нові можливості встановлення зв'язку, які збільшують потенційну небезпеку в системі захисту від вірусів. Технології Web, наприклад, для створення аплетів Java і ActiveX, полегшують користувачам взаємодію через Інтернет, але, з іншого боку, служать зручним засобом для поширення зловмисного програмного забезпечення. Користувачі робочої станції, встановленої на комп'ютері, для виконання своїх завдань використовують програмне забезпечення та файли даних. Вся ця інформація, включаючи операційну систему, зберігається на жорсткому диску комп'ютера.

Іншим місцем постійного зберігання інформації, необхідної для роботи комп'ютера, є незалежна пам'ять CMOS, що зберігає базову систему введення/виведення (BIOS) комп'ютера; процедури BIOS використовуються при завантаженні системи, тому їх зараження – серйозна небезпека [5].

Таким чином, у комп'ютері є два основних місця, здатних постійно зберігати і оновлювати інформацію – жорсткий диск і пам'ять CMOS. Ці компоненти комп'ютерної системи і є тим місцем, куди найчастіше потрапляють віруси у разі інфікування комп'ютера.

Вірусні атаки можна класифікувати за місцем їх розташування в комп'ютері. Відомі три основні типи вірусних атак:

– атака завантажувального сектора;
– інфікування файлу;
– атака з використанням макросів.

Віруси завантажувального сектора інфікують завантажувальний сектор або головний завантажувальний запис комп'ютерної системи. Коли комп'ютер завантажується, вірусна програма активується, такі віруси переміщають в інше місце або перезаписують вихідний завантажувальний код і заміщають його ін-

фікованим завантажувальним кодом. Інформація вихідного завантажувального сектора переноситься на інший сектор диска, який позначається як дефектна область диска і надалі не використовується. Оскільки завантажувальний сектор – перший елемент, що завантажується під час запуску комп'ютера, виявлення вірусів завантажувального сектора може виявитися нелегким завданням. Віруси завантажувального сектора – одні з найпопулярніших типів вірусів, вони можуть поширюватися шляхом використання інфікованих гнучких дисків при завантаженні комп'ютера. Це може легко статися, якщо при перезавантаженні комп'ютера гнучкий диск вставлено у дисковод.

Віруси, що інфікують файли, вражають виконувані файли. Вони можуть активуватися тільки за умови виконання файлу. Частіше за інших уражаються файли типів: COM, EXE, DLL, DRV, BIN, SYS і VXD. Віруси, що інфікують файли, можуть ставати резидентними і приєднуватися до інших виконуваних програм. Вони зазвичай заміняють інструкції завантаження програми виконуваного файлу власними інструкціями, після чого переносять початкову інструкцію завантаження програми в інший розділ файлу. Цей процес збільшує розмір файлу, що може допомогти виявити вірус [5].

Віруси, в основі яких лежать макроси (макровіруси), виконують непередбачувані дії шляхом використання макромови – додатків до свого розширення в інші документи. Вони можуть, наприклад, інфікувати файли .DOT і .DOC, додатки Microsoft Word, а також файли Microsoft Excel. Ці віруси належать до міжплатформних вірусів і можуть інфікувати як системи Macintosh, так і PC, інші віруси можуть мати риси одного або декількох описаних вище типів.

Віруси-невидимки (жаргонна назва – «стелс-віруси») намагаються сховатися як від операційної системи, так і від антивірусних програм. Щоб перехопити всі спроби використання операційної системи, вірус повинен міститися в пам'яті. Віруси-невидимки можуть приховувати всі зміни, які вони вносять у розміри файлів, структуру каталогів або інші розділи операційної системи, що значно ускладнює їх виявлення. Щоб блокувати віруси-невидимки, їх слід виявити, коли вони містяться в пам'яті [5].

Зашифровані віруси під час роботи шифрують свій вірусний код, що дозволяє їм уникнути виявлення і розпізнавання.

Поліморфні віруси можуть змінювати свій зовнішній вигляд під час кожного інфікування. З метою зміни зовнішнього вигляду і, як наслідок, ускладнення виявлення, вони використовують механізми мутацій. Ці віруси здатні набувати понад двох мільярдів різних форм, оскільки змінюють алгоритм шифрування.

Багатокомпонентні віруси інфікують як завантажувальні сектори, так і виконувані файли. Вони – одні з найскладніших для виявлення, оскільки можуть поєднувати деякі або всі методи приховування своєї діяльності, властиві вірусам-невидимкам і поліморфним вірусам.

Самооновлювані віруси, які з'явилися останнім часом, здатні таємно оновлюватися через Інтернет під час сеансів зв'язку.

Зустріч комп'ютера з вірусом може спричиняти такі наслідки:

– появу незвичайних системних повідомлень;

– зникнення файлів або збільшення їх розмірів;

– уповільнення роботи системи;

– раптову нестачу дискового простору;

– недоступність диска.

Важливим методом захисту від вірусів виступає розгортання антивірусних програм. Антивірусна програма повинна виконувати три основні завдання: виявлення вірусу, видалення вірусу та превентивний захист [5]. Проте антивірус не завжди може допомогти, адже принцип його дії побудовано на відстеженні коду вірусу, який прописано у його програмі. Якщо певного коду вірусу немає у такому переліку, то антивірус на його не відреагує. Це ж стосується і нових вірусів.

Висновок. Думка «Кому я потрібен, хто мене зламуватиме?» – хибна. Ми живемо у соціумі, тому і знайомі, і колеги, і конкуренти по бізнесу, і навіть сусіди можуть бути зацікавленими у вашому особистому житті та інформації, до якої ви маєте доступ.

Для користувачів-початківців найпростішими діями, спрямованими на захист електронної інформації, є:

– перезавантаження комп'ютера перед початком роботи, особливо, якщо за цим комп'ютером працювали інші користувачі;

– озброїтися останнім антивірусом, час від часу оновлюючи його, або краще кількома;

– застосовувати резервне копіювання інформації (створення копій файлів і системних областей жорстких дисків);

– не переходити на «дивні» сайти або, перебуваючи на них, не підтверджувати непотрібні вам операції;

– не відправляти власні дані (логін, пароль, номер телефону, номер картки і т. д.);

– не зберігати паролі автоматично, очищувати файли «cookie» (у цих файлах зберігаються логіни і паролі, які ви вводите на ПК);

– шифрувати інформацію – це чи не найнадійніший спосіб захисту від копіювання;

– здійснювати вимкнення комп'ютера з мережі (на час, коли ви ним не користуєтеся);

– будьте обачними і дотримуйтеся інформаційної гігієни.

Зламування можна розглядати і в якості рушійної сили для модифікації програмних продуктів і створення нового, надійного, функціонального рішення для подолання комп'ютерної злочинності. Світ розвивається, розвивається злочинна IT-сфера, тому час вдосконалити і «білих програмістів» – IT-фахівців із безпеки.

ЛІТЕРАТУРА:

1. Кримінальне право України: Особлива частина: підручник / за ред. В.В. Сташиса, В.Я. Тація. Х.: Право, 2010. 608 с.

2. Науково-практичний коментар до кримінального кодексу України. Законодавство України. URL: https://zakon.osmark.com.ua/кримінальний-кодекс-україни-комента-15.

3. Как создать вирус шутку с помощью Блокнота. URL: https://ru.wikihow.com/%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D1%82%D1%8C%D0%B2%D0%B8%D1%80%D1%83%D1%81%D1%88%D1%83%D1%82%D0%BA%D1%83%D1%81%D0%BF%D0%BE%D0%BC%D0%BE%D1%89%D1%8C%D1%8E%D0%91%D0%BB%D0%BE%D0%BA%D0%BD%D0%BE%D1%82%D0%B0.

4. Мішин А.В. Поняття комп'ютерного вірусу. Шляхи проникнення вірусів. Лекційне заняття. URL: http://om.net.ua/5/5_13/5_131653_ponyatie-kompyuternogo-virusa-puti-proniknoveniya-virusov.html.

5. Виды компьютерных вирусов, и способы борьбы с ними. Web 3.0. URL: http://comp.web-3.ru/virus/?act=full&id_article=1411.

6. 10 относительно честных способов взломать почту. Хабрахабр. URL: https://habrahabr.ru/company/cybersafe/blog/269829.

7. Как создать, написать компьютерный вирус? Немного про Windows. URL: http://about-windows.ru/virusy-i-xakery/pishem-virusy/sozdaem-virus.