Комп'ютерні віруси

Виконав

Учень 9-А

Для інформатики

Комп'ютерний вірус

- ***Комп'ютерний вірус*** *(англ. computer virus)* — комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Необізнані користувачі ПК помилково відносять до комп'ютерних вірусів також інші види зловмисного ПЗ — програм-шпигунів чи навіть спам. За створення та поширення шкідливих програм (в тому числі вірусів) у багатьох країнах передбачена кримінальна відповідальність. Зокрема, в Україні поширення комп'ютерних вірусів переслідується і карається відповідно до Кримінального кодексу (статті 361, 362, 363). Приклади вірусів: Neshta, Staog,Archiveus.

Історія створення вірусів

- Назва програми «комп'ютерний вірус» походить від однойменного терміну з біології за її здатність до саморозмноження. Саме поняття «комп'ютерного вірусу» з'явилося на початку 1970-тих і використовувалося у програмуванні та літературі, зокрема, у фантастичному оповіданні «Людина в рубцях» Грегорі Белфорда. Проте, автором терміну вважається Фред Коен, який у 1984 році опублікував одну з перших академічних статей, що були присвячені вірусам, де і було використано цю назву.

- Історія свідчить, що ідею створення комп'ютерних вірусів окреслив письменник-фантаст Т. Дж. Райн, котрий в одній із своїх книжок, написаній в США в 1977 р., описав епідемію, що за короткий час охопила біля 7000 комп'ютерів. Причиною епідемії став комп'ютерний вірус, котрий передавався від одного комп'ютера до другого, прокрадався в їхні операційні системи і виводив комп'ютери з-під контролю людини.

- В 70-х роках, коли вийшла книжка Т.Дж. Райна, описані в ній факти здавалися фантастикою, і мало хто міг передбачати, що вже в кінці 80-х років проблема комп'ютерних вірусів стане великою дійсністю, хоч і не смертельною для людства в єдиноборстві з комп'ютером, але такою, що призвела до деяких соціальних і матеріальних втрат. Під час досліджень, проведених однією з американських асоціацій з боротьби з комп'ютерними вірусами, за сім місяців 1988 р. комп'ютери, які належали фірмам-членам асоціації, піддавались дії 300 масових вірусних атак, які знищили близько 300 тис. комп'ютерних систем, на відтворення яких було затрачено багато часу і матеріальних затрат. В кінці 1989 р. в пресі з'явилося повідомлення про знаходження в Японії нового, надзвичайно підступного і руйнівного віруса (його назвали хробаком), за короткий час він знищив дані на великій кількості машин, під'єднаних до комунікаційних ліній. Переповзаючи від комп'ютера до комп'ютера, через з'єднувальні комунікації, «хробак» знищував вміст пам'яті, не залишаючи ніяких надій на відновлення даних.

- У 1992 році з'явився перший конструктор вірусів для PC — Virus Creation Laboratory (для Amiga конструктори існували і раніше), а також готові поліморфні модулі (MtE, DAME і TPE) і модулі шифрування для вбудовування в нові віруси. У кілька наступних років було остаточно відточено стелс і поліморфні технології (SMEG.Pathogen, SMEG.Queeg, OneHalf, 1994; NightFall, Nostradamus, Nutcracker, 1995), а також випробувано самі незвичайні способи проникнення в систему і зараження файлів (Dir II — 1991, PMBS, Shadowgard, Cruncher — 1993). Крім того, з'явилися віруси, що заражають об'єктні файли (Shifter, 1994) і вихідні тексти програм (SrcVir, 1994).

- З поширенням пакету Microsoft Office набули поширення макровіруси (Concept, 1995). У 1996 році з'явився перший вірус для Windows 95 — Win95.Boza, а в грудні того ж року — перший резидентний вірус для неї — Win95.Punch. З поширенням мереж та Інтернету файлові віруси все більше орієнтуються на них як на основний канал роботи (ShareFun, 1997 — макровірус MS Word, що використовує MS-Mail для поширення, Win32.HLLP.DeTroie, 1998 — сімейство вірусів-шпигунів, Melissa, 1999 — макровірус і мережевий черв'як, який побив усі рекорди за швидкістю поширення). Еру розквіту «троянських коней» відкриває утиліта прихованого віддаленого адміністрування BackOrifice (1998) і пішли за нею аналоги (NetBus, Phase). Вірус Win95.CIH досяг апогею в застосуванні незвичайних методів, переписуючи Flash Bios заражених машин (епідемія в червні 1998 вважається найбільш руйнівною за попередні роки).

- В кінці 1990-х — на початку 2000-х з ускладненням ПЗ та системного оточення, масовим переходом на порівняно захищені Windows сімейства NT, утвердженням мереж як основного каналу обміну даними, а також успіхами антивірусних технологій у виявленні вірусів, побудованих за складними алгоритмами, останні стали все більше замінювати впровадження у файли на впровадження в операційну систему (незвичайний автозапуск, руткіти) і підміняти поліморфізм величезною кількістю видів (число відомих вірусів зростає експоненціально).

- Разом з тим, виявлення в Windows та іншому поширеному програмному забезпеченні численних вразливих місць відкрило дорогу черв'якам-експлоїтам. У 2004 р. безпрецедентні за масштабами епідемії викликають MsBlast (більше 16 млн систем за даними Microsoft [15]), Sasser і Mydoom (оціночні збитки 500 млн. дол і 4 млрд дол. відповідно). Крім того, монолітні віруси в значній мірі поступаються місцем комплексам шкідливого ПЗ з поділом ролей і допоміжними засобами (троянські програми, завантажувачі / дропери, фішингові сайти, спам-боти і павуки).

- Також розквітають соціальні технології — спам і фішинг — як засіб зараження в обхід механізмів захисту ПЗ. Спочатку на основі троянських програм, а з розвитком технологій p2p-мереж— і самостійно — набирає обертів найсучасніший вид вірусів — хробаки-ботнети (Rustock, 2006, бл. 150 тис. ботів; Conficker, 2008–2009, понад 7 млн ботів; Kraken, 2009, бл. 500 тис. ботів).
- Віруси у складі іншого зловмисного ПЗ остаточно оформляються як засіб кіберзлочинності.

Суспільний аспект

- Для одних віруси є бізнесом. Причому не тільки для їхніх авторів, але і для тих, хто з цими вірусами бореться. Бо процвітання компаній, які випускають антивірусні програми не є несподіванкою ні для кого. Для інших — це хобі. Хобі — збирання вірусних колекцій і хобі — написання вірусів. Ще інші — створюють віруси для прояву власної зухвалості і незалежності, у деяких колах подібна діяльність просто необхідна для піднятя свого престижу. Є й такі, для кого віруси це витвір мистецтва; зустрічаються лікарі за покликанням, отже, може бути і комп'ютерний лікар за покликанням. Для деяких віруси служать приводом пофілософствувати на теми створення і розвитку комп'ютерного життя. Для інших віруси — це також стаття кримінального кодексу. Але для більшості користувачів комп'ютерів віруси — це щоденний головний біль і турбота, причина збоїв у роботі комп'ютера і ворог номер один.

Класифікація

- Не існує єдиної системи класифікації та іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO в 1991 році).
- Прийнято розділяти віруси за:
- об'єктами, які вражаються (файлові віруси, завантажувальні віруси, анти-антивірусні віруси, скриптові віруси, макро-віруси, мережеві черв'яки).
- способом зараження (перезаписуючі віруси, віруси-компаньйони, файлові хробаки, віруси-ланки, паразитичні віруси, віруси, що вражають вихідний код программ)
- операційними системами і платформами, які вражаються (DOS, Microsoft Windows, Unix, Linux, інші)
- активністю (резидентні віруси, нерезидентні віруси)
- технологіями, які використовуються вірусом (нешифровані/шифровані віруси, поліморфні віруси, стелс-віруси (руткіт і буткіт))
- деструктивними можливостями (нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси)
- мовою, якою написаний вірус (асемблер, високорівнева мова програмування, скриптова мова, інші).

Ознаки зараження вірусом

- Зменшення вільної пам'яті
- Уповільнення роботи комп'ютера
- Затримки при виконанні програм
- Незрозумілі зміни в файлах
- Зміна дати модифікації файлів без причини
- Незрозумілі помилки Write-protection
- Помилки при інсталяції і запуску ОС
- Відключення 32-розрядного допуску до диску
- Неспроможність зберігати документи Word в інші каталоги, крім Template

- Погана робота дисків
- Файли невідомого походження
- Ранні ознаки зараження дуже тяжко виявити, але коли вірус переходить в активну фазу, тоді легко помітити такі зміни:
- Зникнення файлів
- Форматування HDD
- Неспроможність завантажити комп'ютер
- Неспроможність завантажити файли
- Незрозумілі системні повідомлення, звукові ефекти і т. д.
- Здебільшого, все це в минулому. Зараз основні ознаки — самовільне відкривання браузером деяких сайтів (рекламного характеру), підозріло підвищений інтернет-трафік та повідомлення від друзів, що ваші листи електронної пошти до них містили вірус.