Львівський державний університет безпеки життєдіяльності

Кафедра управління проектами, інформаційних технологій та телекомунікацій

Лекція

з курсу:

" Безпека інформаційно-комунікаційних систем"

***на тему:* " Шкідливе програмне забезпечення."**

(для курсантів та студентів 5-го курсу спеціальності «Комп'ютерні науки»)

ПЛАН ЛЕКЦІЇ

1. Класифікація шкідливого програмного забезпечення
2. Програмні закладки
3. Комп'ютерні віруси
4. Мережеві хробаки.

ЛІТЕРАТУРА

1. **Богуш В.М., Кудін А.М.** Інформаційна безпека від А до Я. - К.: МОУ, 1999. – 456 с.

2. **Гайворонський М.В., Новіков О.М.** Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. іл.

3. **Eugene H. Spafford.** The Internet Worm Program: An Analysis // Purdue Technical Report CSD-TR-823 — Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-2004.

1. Класифікація шкідливого програмного забезпечення

Під терміном *шкідливе програмне забезпечення* (рос. — вредоносное программное обеспечение, англ. — malware) розуміють програмні засоби, що несанкціоновано впроваджують у комп'ютерну систему і які здатні викликати порушення політики безпеки, завдавати шкоди інформаційним ресурсам, а в окремих випадках — і апаратним ресурсам комп'ютерної системи. Деякі програми навіть можуть виконувати руйнівну функцію, тому їх називають *руйнівними програмними засобами* (рос. — разрушающие программные средства, англ. — destructive software). Хоча шкідливі програмні засоби, які не мають вбудованої руйнівної функції, теж не можна вважати безпечними для комп'ютерної системи. По-перше, вони витрачають ресурси системи, а по-друге, порушують її політику безпеки. Спільною ознакою шкідливого програмного забезпечення є те, що воно виготовлене з метою порушення політики безпеки.

Шкідливе програмне забезпечення класифікують за різними ознаками. Наприклад, у монографії його поділяють на дві категорії — таке, що виконує деструктивні функції, і таке, що їх не виконує. В інших джерелах виділяють як окремий клас шкідливого програмного забезпечення так звані програмні закладки. Іноді термін *програмні закладки* (рос. — программные закладки, англ. — program bug) застосовують майже до всього шкідливого програмного забезпечення, крім комп'ютерних вірусів. Протиставлення вірусів і програмних закладок є помилковим. Будь-який шкідливий програмний засіб може або встановлювати програмну закладку, або не робити цього. Програмна закладка працюватиме на комп'ютері деякий час, допоки її не буде виявлено або згідно із закладеним у неї алгоритмом. Натомість, деякі програмні засоби, скажімо, «троянські коні», можуть здійснювати руйнівні дії з катастрофічними наслідками (наприклад, форматування диска) безпосередньо під час своєї активації, не намагаючись залишити в системі свої компоненти.

Чи виконуватимуть шкідливі програмні засоби руйнівні функції, визначити складно. По-перше, як уже зазначалося, вони у будь-якому разі порушують політику безпеки. По-друге, навіть якщо розробник шкідливого засобу не передбачив у ньому руйнівних функцій, такий засіб може призвести до значних втрат — як через необхідність спрямування зусиль висококваліфікованих (і високооплачуваних) фахівців на виявлення, ідентифікацію, видалення шкідливого програмного засобу, так і через недоступність систем. Яскравий приклад — хробак Морріса, який не мав жодних руйнівних функцій, проте за дуже короткий час свого функціонування в Інтернеті (протягом однієї доби) завдав збитків, які було оцінено в понад 98 млн доларів.

Тому доцільно класифікувати шкідливе програмне забезпечення за двома головними ознаками:

- способом розповсюдження засобу — яким чином засіб потрапляє на комп'ютер і домагається своєї активізації;
- метою функціонування засобу — які саме шкідливі дії він здійснює.

Шкідливе програмне забезпечення завдає шкоди комп'ютеру під час запуску його коду на виконання. Тому шкідливі програмні засоби застосовують такі механізми розповсюдження, що дають їм змогу виконуватися на комп'ютері або взагалі без втручання користувача, або непомітно для нього. За механізмами розповсюдження виділяють такі шкідливі програмні засоби.

- Класичні комп'ютерні віруси:
    1. файлові віруси;
    2. завантажувальні віруси;
    3. макровіруси;
    4. скриптові віруси.
- Мережні хробаки:
    1. поштові хробаки;
    2. хробаки, що використовують інтернет-пейджери;
    3. хробаки в IRC-каналах;
    4. хробаки для файлообмінних мереж (Peer-to-Peer Network, P2P);
    5. інші мережні хробаки.

- «Троянські коні».
- Спеціальні хакерські утиліти.

Наведена класифікація розроблена на основі класифікації, запропонованої «Лабораторією Касперського».

Класичні комп'ютерні віруси — це програмні засоби, які здатні самостійно відтворюватися, тобто розмножуватися, і використовують як носій інший програмний код, який вони модифікують у такий спосіб, щоб впровадити в нього свою копію. У результаті замість програмного коду, запущеного користувачем на виконання, виконується код вірусу.

Класичні мережні хробаки здатні самотужки, без будь-якого втручання користувача, розповсюджуватися у комп'ютерній мережі, виконуючи щонайменше дві функції: передавання свого програмного коду на інший комп'ютер і запуск свого програмного коду на віддаленому комп'ютері. Для цього хробаки використовують уразливості комп'ютерних систем. На відміну від класичних вірусів хробаки, як правило, не використовують як носії коди інших програм, оскільки не мають на меті примусити користувача у такий спосіб запустити їх. Іноді хробаками називають ще такі програми, які не здатні самотужки запустити себе на виконання на віддаленій комп'ютерній системі, й відтак застосовують принцип «троянського коня».

Категорію «троянські коні» не поділяють на підкатегорії за способами їх розповсюдження. їх класифікують за тими діями, які вони здійснюють на зараженому комп'ютері (така класифікація значною мірою повторює класифікації програмних закладок). Щодо способу зараження комп'ютера, то про нього каже сама назва «троянський кінь». Ці програми, використовуючи різні методи соціальної інженерії, приваблюють довірливого користувача, який запускає їх на виконання, отримуючи зовсім не ті результати, на які розраховував (у деяких «троянських коней» шкідливі функції добре приховано, тому користувач може навіть не підозрювати, що його комп'ютер уже скомпрометовано).

До спеціальних засобів належать дуже небезпечні засоби, які не мають своїх механізмів розповсюдження і які користувачі свідомо запускають на виконання як звичайні програми. Такі засоби зловмисники застосовують, якщо мають певні повноваження в системі (можливо, отримані несанкціоновано). Деякі з цих засобів називають *експлойтами* (рос. — эксплойт, англ. — exploit), що підкреслює факт використання (експлуатації) ними деякої вразливості системи. Часто такі засоби призначені для атаки не того комп'ютера, на якому вони запущені, а інших комп'ютерів у мережі. Інколи зловмисники використовують ці засоби як інструментарій, а не безпосередньо для атак. Класифікація спеціальних засобів буде наведена відповідно до функцій, які вони виконують.

Цей перелік був би неповним без ще одного класу програмного забезпечення, використання якого може призвести не лише до порушення політики безпеки, але й до пошкодження програмного, а інколи навіть апаратного забезпечення комп'ютерної системи. Це технологічні програми, які використовують адміністратори системи або технічний обслуговуючий персонал, наприклад: засоби резервного копіювання і відновлення з резервних копій, форматування дисків, дефрагментації файлових систем, перепрограмування BIOS, перевірки та редагування реєстру Windows. Такі програми не належать до шкідливих чи руйнівних, тому в цьому розділі ми їх не розглядатимемо. Проте, оскільки їх використання зловмисниками чи просто некомпетентними користувачами може мати дуже серйозні наслідки, розробляючи політику безпеки системи, слід враховувати наявність таких програм і впроваджувати заходи, що запобігають їх використанню невповноваженими користувачами.

2. Програмні закладки

Програмні закладки — це програми або окремі функції програм, що тривалий час працюють у комп'ютерній системі, здійснюючи заходи, спрямовані на приховування свого існування від користувача. Програмні закладки можуть впроваджувати віруси, «троянські коні», мережні хробаки чи безпосередньо користувачі- зловмисники. Іноді програмні закладки впроваджують адміністратори з метою виявлення злочинної діяльності користувачів або для керування комп'ютерами користувачів. У таких випадках програмну закладку не слід вважати шкідливою програмою, хоча функціонально вона, напевно, буде абсолютно ідентичною

шкідливій програмі. Це ще одне підтвердження того, що програмні засоби в інформаційному середовищі часто відіграють роль зброї, шкода чи користь від застосування якої залежить лише від того, в чиїх вона руках (і від того, хто оцінюватиме наслідки її застосування).

2.1. Функції програмних закладок

Є різні, більш або менш деталізовані класифікації функцій програмних закладок. Нижче наведено класифікацію, яка враховує «новинки» розробників «троянських коней».

- Перехоплення і передавання інформації:
  - крадіжка паролів;
  - шпигунські програми.
- Порушення функціонування систем («логічні бомби»):
  - знищення інформації;
  - зловмисна модифікація інформації;
  - блокування системи.
- Модифікація програмного забезпечення:
  - утиліти віддаленого адміністрування (люки);
  - інтернет-клікери;
  - проксі-сервери;
  - дзвінки на платні ресурси;
  - організація DoS-і DDoS-атак.
- Психологічний тиск на користувача:
  - реклама;
  - лихі жарти і містифікації.

Як видно із класифікації, програмні закладки першої групи порушують конфіденційність, другої — цілісність і (або) доступність інформації. Функції, які виконують програмні закладки із третьої групи, характерні для «троянських коней», вірусів і хробаків; такі закладки порушують спостережність і керованість комп'ютерної системи. Нарешті, дії програмних закладок четвертої групи безпосередньо спрямовані на користувача системи. Більш детально типові програмні закладки буде розглянуто далі.

2.2. Шпигунські програми

Програмні закладки, що здійснюють пошук інформації на зараженому комп'ютері та передають її зловмиснику, розрізняють за типом інформації, яку вони збирають, за режимом і технологіями її передавання.

Окрему категорію складають програми, що збирають і надсилають паролі доступу до локальної системи і до мережних ресурсів, зокрема платних, а також до банківських систем і систем електронних платежів.

Шпигунські програми (Spyware) — ширша категорія, до якої належать програми різних типів. Деякі з них стежать за діями користувача зараженого комп'ютера, перехоплюючи інформацію, що вводиться з клавіатури, копії екрана, відомості про активні програми і про те, що користувач із ними робить. Інші здійснюють пошук інформації у файлах користувача за певними ознаками (наприклад, за ключовими словами). Є окремий різновид шпигунських програм, які цікавляться конфігурацією апаратних і програмних засобів на комп'ютері користувача, зокрема серійними номерами ліцензійних програм.

Програмні закладки цього типу здебільшого впроваджують віруси і «троянські коні», проте часто такі програмні модулі встановлюють «нормальні» програми, переважно з числа умовно-безкоштовних (Shareware) або безкоштовних (Freeware).

Головне, що їх цікавить, — це склад апаратних і програмних засобів комп'ютера та його територіальне розміщення (країна, локальна мова, часовий пояс). У такий спосіб розробники збирають статистичну інформацію про використання своєї програми, що в подальшому може стати у пригоді для розроблення її нових версій.

2.3 «Логічні бомби»

До категорії «логічних бомб» належать програмні закладки, які за певних умов здійснюють деякі, як правило, руйнівні дії. Іноді виокремлюють категорію «часові міни» — фактично, це окремий випадок «логічних бомб», де умовою запуску є настання певного

моменту часу. Наприклад, вірус, відомий як CIH, впроваджував часову міну, яка спрацьовувала під час завантаження комп'ютера 26 квітня, тобто у річницю Чорнобильської катастрофи (за що дістав назву «Чорнобиль», під якою він більш відомий у нашій країні). Результат діяльності цієї програми був катастрофічним для комп'ютера: вона модифікувала Flash-BIOS, після чого комп'ютер повністю втрачав роботоздатність. Як правило, для відновлення такого комп'ютера потрібно було замінювати системну плату.

2.4 Люки — утиліти віддаленого адміністрування

Програмні закладки цієї категорії є утилітами віддаленого адміністрування комп'ютерів у мережі. Функціонально вони подібні до систем адміністрування, що розробляють і розповсюджують відомі виробники програмних продуктів. Окрім спеціалізованих засобів таку функціональність мають модулі операційних систем, наприклад віддалений помічник у Windows XP Home Edition.

Єдине, що вирізняє з-поміж таких програм шкідливі програмні закладки, — це відсутність попереджень про їх інсталяцію і запуск. Користувач не отримує жодних повідомлень про дії програмної закладки в системі. Тим паче, що програмна закладка може бути прихованою і не відображатися у списку активних програм і процесів. І в той час, коли користувач навіть гадки не має про присутність у системі такої програми, його комп'ютер стає відкритим для віддаленого керування.

Можна констатувати, що програмні закладки цього типу є одними з найнебезпечніших, оскільки вони потенційно уможливлюють будь-які зловмисні дії. Програми, які впроваджують ці програмні закладки, також належать до найшкідливіших. Так само слід розуміти, що потенційну загрозу можуть нести абсолютно «легальні» утиліти віддаленого адміністрування, позаяк вони роблять комп'ютер уразливим для будь-яких дій ззовні. Єдине, що може захистити у разі їхнього використання, — це надійна автентифікація вузла і користувача, від якого надходять команди керування. Але ніхто не може гарантувати відсутність помилок, що відкривають доступ для сторонніх осіб (зловмисників), які через діючу систему віддаленого керування зможуть упровадити власну приховану систему.

Хоча шкідливих програм цієї категорії дуже багато, насамперед слід згадати «троянського коня» BackOrifice, який з'явився у 1998 році та набув надзвичайного на той час поширення. «Троянець» встановлював програмну закладку віддаленого адміністрування, якою міг скористатися будь-хто. Антивірусні засоби дуже швидко почали його виявляти, а зловмисники використовувати цей люк для проникнення в систему і встановлення свого, непоширеного і тому невідомого антивірусним засобам люка. Саме таким чином було «зламано» сайт Relcom- Україна: зловмисники, які сканували інтернет у пошуках комп'ютерів, уражених BackOrifice, виявили серед них машину в офісі Relcom, впровадили свою утиліту (суттєво доопрацьований BackOrifice), яка здійснювала перехоплення клавіатурного вводу, що дало їм змогу дізнатися про IP-адреси та паролі доступу до інших машин, зокрема до захищеного сервера.

Крім «агента» — люка, який впроваджувався на віддалених машинах, — і дотепної назви (яка, між іншим, ще й пародіювала розрекламований Microsoft Back Office), BackOrifice мав утиліту-менеджера з великими можливостями і зручним графічним інтерфейсом.

Слідом за BackOrifice з'явилися інші такі програми (NetBus, Phase), що зробили свій внесок у перетворення Інтернету на небезпечне та агресивне середовище.

У наш час використання програмних закладок віддаленого керування набуло характеру глобальної епідемії. Упровадження таких закладок здійснюється спеціалізованими мережними хробаками. У результаті їхньої діяльності формується величезна армія комп'ютерів, на яких впроваджено певну утиліту віддаленого керування (так званий бот). До таких мереж, якими централізовано керує зловмисник, застосовують термін ботнет (мережа ботів). Керування переважно здійснюють через певний IRC-канал, інколи використовують веб-сайт, на якому зловмисник розміщує команди для вражених машин, а в окремих випадках навіть організовують спеціальну P2P-мережу. Перші ботнети було сформовано у 2002 році, а потім відбувся їх стрімкий розвиток. Значною мірою цьому сприяли критичні вразливості в системах Windows: у 2003 році виявили вразливість у службі RPC DCOM Windows 2000/XP (яку використав хробак Lovesan), а у 2004 році - у службі LSASS (її використав хробак Sasser).

Окрім того, велику роль відіграв поштовий хробак Mydoom, виявлений у 2004 році. Згадані хробаки впроваджували програмні закладки віддаленого керування або інші програмні закладки роботи з мережею, причому деякі з них мали вразливості, що ними скористалися наступні покоління хробаків. Усі ці люки було використано зловмисниками для інсталяції на машинах своїх утиліт-ботів. Між різними групами зловмисників буквально спалахнула війна за машини-зомбі; скомпрометовані комп'ютери могли переходити «із рук у руки» по кілька разів на день, рано чи пізно стаючи одним із учасників деякого ботнета.

За оцінками, наведеними експертом компанії «Лабораторія Касперського» Олександром Гостевим, у 2005 році кількість уражених комп'ютерів, що входили до складу ботнетів, становила вже кілька мільйонів; і ця кількість щомісяця зростала на 300-350 тис. Ботнети активно використовують зловмисники: через них розсилають спам, організовують DDoS-атаки, розповсюджують нові версії шкідливих програм. Цілком імовірною є організація розподілених обчислень, наприклад, для зламу криптосистем. Як приклад DDoS-атаки, організованої з використанням ботнета, можна навести результат діяльності вже згаданого хробака Mydoom.A, який 1 лютого 2004 року надовго вивів із ладу сайт компанії SCO, виробника дистрибутивів UNIX.

2.5 Несанкціонована робота з мережею

Програмні закладки, які несанкціоновано працюють із мережею (надсилають або отримують повідомлення чи спеціальні пакети даних), становлять доволі численну групу. Ми вже згадували раніше ті з них, що надсилають шпигунську інформацію задля здобуття даних про користувача і його комп'ютер, а також ті, що отримують команди з мережі та виконують їх. Але є ще багато шкідливих програм, призначених для роботи з мережею, які здатні завдати значної шкоди користувачу. Розглянемо деякі з них.

Інтернет-клікери

До цієї категорії належать програми (здебільшого «троянські коні»), основна функція яких — організація несанкціонованих звернень до ресурсів Інтернету (переважно до веб-сторінок), для чого або надсилають відповідні команди браузеру, або замінюють системні файли, де вказано «стандартні» адреси ресурсів Інтернету. Такі дії зловмисники можуть здійснювати з метою:

- підвищення кількості відвідувань деяких сайтів;
- організації DoS-атаки на деякий ресурс (хоча значно ефективніше було б здійснити скоординовану атаку, організовану системою віддаленого керування);
- привернення потенційних жертв задля впровадження на їх комп'ютери вірусів або «троянських коней».

Проксі-сервери

Прихований від користувача проксі-сервер можна використовувати для будь-якої злочинної діяльності в мережі, надаючи зловмиснику можливість анонімного (точніше, від імені користувача, який нічого не підозрює) доступу до будь-яких ресурсів Інтернету. Проксі-сервери застосовують для сканування мереж, здійснення атак на інші комп'ютери, але здебільшого їх використовують для розсилання спаму.

Доступ до платних ресурсів

Є програми, що здійснюють доступ до платних ресурсів. В Інтернеті це, як правило, не становить реальної загрози (оскільки там діє принцип — «гроші наперед»), якщо така програма не передає автоматично платіжні реквізити користувача (наприклад, номер кредитної картки).

Інсталяція з мережі

Програмні модулі-інсталятори є в багатьох «троянських конях», хоча їх можна зустріти майже в усіх сучасних програмах. У «троянцях» ці модулі звичайно спрацьовують безпосередньо під час запуску програми і часто не використовують програмних закладок. Натомість, у легальних програмах такі модулі дуже часто оформлені у вигляді типових програмних закладок. І хоча програмні модулі-інсталятори не можна класифікувати як шкідливі програми, вони безперечно є потенційно небезпечними для комп'ютерної системи.

3. Комп'ютерні віруси

Свого часу серед руйнівних програмних засобів саме комп'ютерні віруси набули найбільшого розповсюдження, тому вірусами називають будь-яке шкідливе програмне забезпечення, несанкціоновано впроваджене в систему. Так само і від антивірусних засобів часто очікують захисту не лише від вірусів, а й від руйнівних програмних засобів інших видів; інколи такі сподівання виправдовуються, а інколи — ні. Насправді, часто мова йде не про вірус, а про «троянського коня», хробака чи навіть експлойт, який хтось впровадив у систему.

Є різні підходи до визначення комп'ютерних вірусів. Ми зазначимо дві головні властивості, характерні саме для вірусів. Перша — це їх здатність самостійно відтворюватися, тобто розмножуватися. У програмний код вірусу закладено функції копіювання самого себе. Друга — це спосіб, у який вірус потрапляє до системи і примушує користувача запустити його. Вірус використовує як носій інший *програмний код, який він модифікує таким* чином, щоб впровадити в нього свою копію (подібно звичайним вірусам, які нездатні існувати самостійно тривалий час — їм потрібні клітини іншого живого організму). У результаті замість необхідного користувачу програмного коду виконується код вірусу.

Комп'ютерні віруси розрізняють за такими ознаками.

За середовищем існування (системні області комп'ютера, ОС, прикладні програми, до певних компонентів яких впроваджують код вірусу):

- файлові віруси;
- завантажувальні віруси;
- макровіруси;
- скриптові віруси.

За способом зараження (різні методи впровадження вірусного коду в об'єкти, які він заражає; залежно від середовища існування віруси використовують різні способи зараження, тому універсальної класифікації за цією ознакою немає).

Віруси також класифікують (або надають їм додаткових ознак) за тими технологіями, які вони використовують для ускладнення їх виявлення і ліквідації.

3.1. Файлові віруси

Файлові віруси для свого розповсюдження використовують файлову систему. Найчастіше віруси цього типу як носій застосовують виконувані файли. За способом зараження їх поділяють на *віруси, що перезаписують* (Overwriting), і *паразитичні віруси* (Parasitic). Оскільки перші замінюють собою оригінальний файл, знищуючи його, то в результаті їхньої діяльності прикладні програми й операційна система дуже швидко перестають функціонувати. Другі модифікують оригінальний файл, зберігаючи його функціональність. Файлові віруси цього типу найпоширеніші, тому їх згодом буде розглянуто детальніше. Є також *компаньйон-віруси*, які створюють файли-двійники, а також *link-віруси,* що використовують особливості організації файлової системи.

Методи зараження файлів паразитичними вірусами

Тепер детальніше розглянемо, як діють паразитичні віруси. їхньою типовою ознакою є те, що вони обов'язково змінюють уміст файлів, залишаючи останні повністю або частково роботоздатними.

Свого часу їх поділяли на *exe-* та *com-віруси*, відповідно до двох форматів виконуваних файлів, що були в MS-DOS. Тепер такий розподіл неактуальний. Зараз характерною ознакою паразитичних вірусів є те, під керуванням якої операційної системи вони можуть функціонувати.

Сучасні ОС підтримують кілька альтернативних форматів виконуваних файлів. Ці доволі складні формати надають широкі можливості для вірусів, які впроваджують свій код без порушення функціональності програми. Є віруси, що записують себе на початку файлів (Prepending), у їх кінець (Appending) і в середину (Inserting). Впровадження вірусів у середину файлів також відбувається у різні способи — перенесенням частини файлу в його кінець або копіюванням свого коду в ті частини файлу, що не використовуються (Cavity-віруси). Основні способи зараження файлів вірусами показано на рис. 1. Докладніше про це можна прочитати у Вірусній енциклопедії «Лабораторії Касперського».

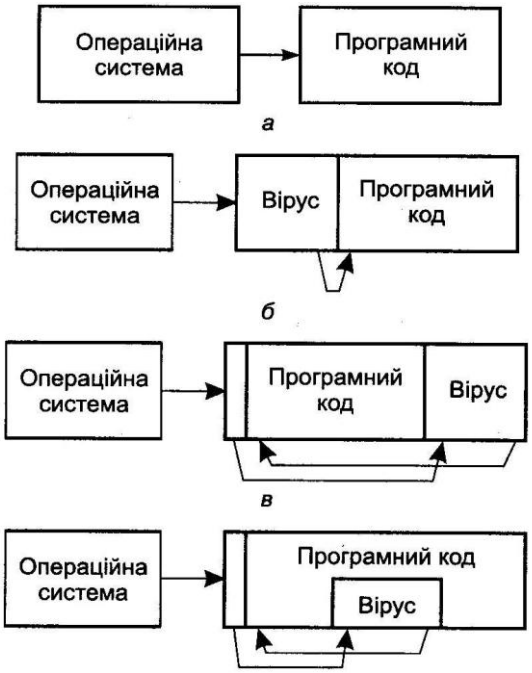

Рис.1. Основні способи зараження файлу вірусом: а — нормальне виконання незараженого файлу; *б* — програмний код вірусу розташовано на початку файлу, сам файл дописано в кінець вірусу (операційна система передає керування безпосередньо вірусу, а той після виконання своїх функцій передає керування файлу); в — програмний код вірусу дописано в кінець файлу (вірус коригує точку входження програми в заголовку оригінального файлу, щоб першим отримати керування); г — програмний код вірусу розташовано всередині оригінального файлу (вірус коригує точку входження програми, щоб першим отримати керування, або (на рисунку не показано) розміщує перехід на свій код будь-де у програмі, щоб отримати керування в певний момент)

Після того як вірус отримує керування, він виконує певні дії та передає керування програмі-носію. На цьому етапі вірус звичайно не здійснює руйнівних дій, а лише вживає заходів для свого розповсюдження (наприклад, «заражає» інші файли, тобто вбудовує в них свій код) і для отримання керування в подальшому (для чого впроваджує програмну закладку, за старою термінологією MS-DOS — резидентну частину). Часто вірус діє так швидко, що на тлі звичайної процедури запуску програми жоден користувач не зможе його помітити, навіть якщо контролюватиме час запуску із секундоміром.

3.2. Завантажувальні віруси

Завантажувальні, або бутові (англ. boot — початкове завантаження, специфічний комп'ютерний термін, скорочення від Bootstrap Loader — програма початкового завантаження), віруси активуються у момент завантаження системи. Для цього їм потрібно розташувати частину свого коду в службових структурах носія, з якого відбувається завантаження — жорсткого диска або дискети. Зараження дискети здійснюється записуванням коду вірусу замість оригінального коду boot-сектора дискети. Зараження жорсткого диска відбувається в один із трьох способів: вірус записує себе замість коду MBR (Master Boot Record — головний завантажувальний запис, таблиця у першому секторі завантажувального диска) чи замість коду boot-сектора завантажувального диска (у Windows — це, як правило, диск С) або модифікує адресу активного boot-сектора в таблиці розділів диска (Disk Partition Table), що знаходиться в MBR.

На жорсткому диску бутові віруси можуть вельми спокійно існувати і завдавати величезної шкоди інформаційним ресурсам. Вони також можуть дуже ефективно протидіяти антивірусним засобам, оскільки саме віруси стартують першими, ще до запуску операційної системи, і тому вони здатні залишити за собою керування критичними для їх існування ресурсами комп'ютера, зокрема, файловою системою. З іншого боку, для цього потрібно фактично утворити для ОС віртуальну машину, що для сучасних систем хоча і є можливим

(адже існують спеціальні програмні засоби, на кшталт vmware), але потребує великого обсягу програмного коду, що не дуже прийнятно для вірусу.

Великим і складним вірусам, розміщеним у завантажувальних секторах дисків (яким, наприклад, був OneHalf), для розповсюдження потрібен був інший носій, позаяк жорсткі диски переносять нечасто, а на дискетах не вистачало місця і для операційної системи, і для вірусу. Тому їх розповсюджували як звичайні файлові віруси, що після запуску намагалися заразити MBR. Поєднання характеристик бутових і файлових вірусів було типовим. Зараження бутовим вірусом особливо небезпечне. За деякими повідомленнями, той самий OneHalf, впроваджений у MBR, досить вільно існував у захищеному середовищі Windows NT Workstation 4.0.

У сучасних операційних системах модифікація MBR ретельно контролюється. її так само контролюють апаратні засоби деяких системних плат, тому такі віруси мають небагато шансів на успіх. Однак це твердження справедливе лише за умови правильного адміністрування і дотримання політики безпеки.

Сучасні знімні носії (наприклад, flash-накопичувачі, оптичні диски), що мають достатній об'єм, інколи використовують для завантаження операційної системи. Flash-накопичувачі для цього використовують рідко. Проте за всіма ознаками вони могли б стати підґрунтям для відродження бутових вірусів, якби завантаження з них було більш поширеною процедурою. Частіше завантаження здійснюють із дисків CD-ROM (або DVD-ROM), CD-R і CD-RW. Але запис на диски CD-R і CD-RW відбувається не так непомітно і швидко, як на жорсткий диск, тому оптичні диски не стали носіями для вірусів. Хоча, безумовно, «підхопити» вірус із піратського диска можна. Також відомі прецеденти, коли віруси містилися на дисках із презентаційними матеріалами, демоверсіями програмного забезпечення, комп'ютерними виданнями.

3.3. Макровіруси

Макровіруси — це віруси, які використовують прихований у файлах документів програмний код (так звані макроси). Ідея макросів виникла, коли програмістам під час роботи з документами доводилося багаторазово виконувати одні й ті самі рутинні операції редагування або певні, завжди однакові, послідовності дій. Природно було для виконання таких дій визначити процедуру, яка б виконувала певну послідовність операцій автоматично. Роль елементарних операцій у макросі виконують окремі команди з множини передбачених у програмі оброблення документа команд, або спеціально розроблені макрокоманди. Свої макромови мають графічні редактори, системи автоматизованого проектування, текстові та табличні процесори.

Макровіруси також написано макромовами. Передумови для макровірусів виникли, коли з'явилися вдосконалені системи, нові можливості яких використовують макроси: по-перше, можливість зберігання макросів у файлі документа, а по- друге, суттєве розширення доступних для макрокоманд функцій.

Наприклад, у 1995 році вийшла чергова версія Microsoft Office, де в текстовому процесорі Microsoft Word як мову макросів було використано досить розвинену мову Word Basic, а в табличному процесорі Excel — повноцінну об'єктно- орієнтовану мову програмування Visual Basic for Applications. Архітектура програм, з яких складається Microsoft Office, передбачає для кожної команди, яку можна викликати через меню або за допомогою кнопок на панелях інструментів, виконання вбудованих макросів. Наприклад, Microsoft Word для збереження файлу за командою File ► Save виконує макрос FileSave, для збереження файлу за командою File ► SaveAs — макрос FileSaveAs, для друкування документа — макрос FilePrint.

Макроси мають доступ не лише до документа, в якому вони містяться, а й до інших об'єктів, зокрема до файлової системи. Зберігатися вони можуть не лише в документах, а й у шаблонах документів, зокрема у шаблонах Normal, які використовуються за умовчанням у всіх документах програм пакета Microsoft Office. І найголовніше — передбачено автоматичне виконання визначених макросів під час відкривання документа чи застосування шаблону, причому шаблон Normal активізується автоматично під час старту відповідної програми (Word, Excel та інших програм пакета Microsoft Office).

3.4. Скриптові віруси

Програмний код можна впроваджувати і в документи інших видів, наприклад в HTML-сторінки, що завантажуються з мережі чи локально та відображаються на екрані за допомогою браузера. Наразі автоматично виконується програмний код сценаріїв, які ще називають скриптами (англ. script — сценарій) та інших елементів (ActiveX, Java). Програмний код сценаріїв може існувати й окремо, у спеціальних файлах. Деякі дуже розвинені мови сценаріїв можна вважати повноцінними мовами програмування. Наприклад, в операційних системах UNIX і Linux сценарії використовують як системні команди на рівних правах з бінарними виконуваними файлами. Далеко не всі користувачі знають, що вони запускають — скомпільовану програму чи сценарій. Сценарії можуть також мати встановлений атрибут SUID.

Скриптові віруси розглядають як підгрупу файлових вірусів. Такі віруси пишуть різними мовами сценаріїв (VBS,JS, BAT, PHP тощо). Вони можуть заражати інші програми-сценарії (командні та службові файли Windows або UNIX), бути компонентами багатокомпонентних вірусів, заражати файли інших форматів (наприклад, згаданий вище HTML), якщо вони підтримують виконання сценаріїв.

3.5. Захист від комп'ютерних вірусів

Найбільш поширені методи виявлення вірусів (та інших шкідливих програмних засобів) — це:

- пошук сигнатур;
- евристичний аналіз;
- контроль незмінності об'єктів.

Одним із основних методів виявлення вірусів був і залишається пошук характерних ознак відомих вірусів (сигнатур) у файлах і оперативній пам'яті комп'ютера. Деякий час великі надії покладали на евристичний аналіз, коли впровадження шкідливого коду виявлялося за наявністю підозрілих операцій (наприклад, відкриття для модифікації виконуваних файлів, перехоплення переривань тощо). Деякі засоби контролювали незмінність файлів, здебільшого виконуваних, що унеможливлювало впровадження в них коду вірусу. Сучасні антивірусні засоби поєднують у собі всі ці можливості, причому для виявлення відомих вірусів (а також хробаків, «троянських коней» та інших небезпечних програмних засобів) найефективнішим залишається саме пошук їхніх сигнатур. За режимом дії антивірусні засоби поділяють на:

- антивірусні сканери;
- антивірусні монітори;
- антивірусні фільтри.

Антивірусні сканери час від часу або за запитом здійснюють повне сканування файлової системи комп'ютера або вибіркове сканування заданих файлів чи каталогів.

Антивірусні монітори працюють безперервно, але вони здійснюють лише вибіркову перевірку і тому, як правило, не дуже уповільнюють роботу комп'ютера. Обов'язково перевіряються ті файли, над якими здійснюються будь-які операції (відкривання, читання, записування, переміщення файлу, запуск на виконання), а якщо таких операцій небагато, відбувається повільне вибіркове сканування файлової системи.

Антивірусні фільтри призначені для роботи здебільшого з тими потоками даних, що надходять із мережі. Вони ефективні для перевірки повідомлень, які надходять електронною поштою чи з каналів IRC, P2P-мереж та інших.

Віруси (а також хробаки і «троянські коні»), зі свого боку, протидіють антивірусним засобам у різні, часто досить вибагливі, способи.

Головним засобом проти пошуку сигнатур став так званий *поліморфізм* — модифікація коду вірусу від екземпляра до екземпляра. Для реалізації поліморфізму здійснюється переважно зашифровування коду з використанням різних ключів, а першим компонентом вірусу, який отримує керування, є розшифрувальник.

Деякі віруси досить ефективно приховують себе від програм, які контролюють розмір файлів (наприклад, на системний запит видають невірну інформацію про довжину файлу, дату його модифікації тощо). Подібні технології дістали назву *стелс* (Stealth).

4. Мережні хробаки

Основною ознакою мережного хробака є його здатність самостійно, без втручання користувача, розповсюджуватись у комп'ютерній мережі, забезпечуючи щонайменше дві функції: передавання свого програмного коду на інший комп'ютер і запуск свого програмного коду на віддаленому комп'ютері. Здебільшого мережні хробаки, як і комп'ютерні віруси, здатні розмножуватись, і тому їх часто розглядають як різновид вірусів. Однак на відміну від класичних комп'ютерних вірусів більшість хробаків не використовують як носій код іншої програми, оскільки не мають на меті примусити користувача у такий спосіб запустити їх.

Класичний мережний хробак використовує вразливості програмного забезпечення, яке реалізує ті чи інші мережні протоколи. Таке програмне забезпечення діє автоматично відповідно до вимог протоколу, а часом, через помилки розробників або завдяки їхньому специфічному погляду на деякі вимоги специфікацій протоколів, — і всупереч вимогам стандартних протоколів. Слід зазначити, що в переважній більшості ситуацій такі програми не покладаються на користувача, а часто інтерфейс взаємодії з користувачем локальної системи взагалі відсутній. Особливості програмного забезпечення, що обслуговує мережну взаємодію, буде докладно розглянуто в наступних лекціях, оскільки воно суттєво впливає і на можливості компрометації системи через мережу, і на методи її захисту.

4.1. Класифікація мережних хробаків

Основною ознакою, за якою хробаків поділяють на різні типи, є спосіб їх розповсюдження — яким чином хробак передає свою копію на віддалені комп'ютери. Іншими ознаками є способи запуску копії хробака на комп'ютері, методи його впровадження в систему та характеристики, притаманні різним видам шкідливого програмного забезпечення (вірусам і «троянським коням») — поліморфізм, прихованість тощо. Розглянемо такі типи хробаків (із наведенням позначень, які застосовує «Лабораторія Касперського»):

- поштові хробаки (Email-worm);
- хробаки, що використовують інтернет-пейджери (IM-worm);
- хробаки у IRC-каналах (IRC-worm);
- хробаки для файлообмінних мереж (P2P-worm);
- інші мережні хробаки (Net-worm).

Поштові хробаки

До цієї категорії належать хробаки, які для свого розповсюдження використовують електронну пошту. Хробак надсилає свою копію у вигляді вкладення (приєднаного файлу) в електронний лист або розміщує посилання (з URL-адресою) на свій файл на мережному ресурсі (наприклад, на скомпрометованому чи хакерському сайті). Як правило, код хробака активізується після втручання користувача: у першому випадку необхідно відкрити заражене вкладення, у другому — скористатися посиланням на заражений файл.

Поштові хробаки надсилають заражені повідомлення у різні способи:

- прямим підключенням до SMTP-сервера;
- використанням сервісів Microsoft Outlook;
- застосуванням функцій Windows MAPI.

Хробаки, що використовують інтернет-пейджери

Хробаки цього типу розсилають повідомлення, що містять URL-адресу файлу з кодом хробака, на контакти, отримані з контакт-листа інтернет-пейджера. Цей спосіб розсилки подібний до того, що використовують поштові хробаки.

Хробаки в IRC-каналах

Ці хробаки, як і поштові, розсилають URL-посилання на копію хробака або безпосередньо заражений файл, причому розсилання здійснюється по IRC-каналах. У другому варіанті користувач, якого атакують, має підтвердити отримання файлу, зберегти його на диску і відкрити.

Хробаки для файлообмінних мереж

Більшість із розглянутих типів мережних хробаків реалізують лише доставляння коду хробака на комп'ютер жертви. При цьому імітується отримання файлу з достовірних джерел (від відомих користувачу контактів), що й провокує користувача на запуск файлу.

Інші мережні хробаки

Це хробаки, які використовують інші способи зараження віддалених комп'ютерів. Серед них такі:

- копіювання хробака на мережні ресурси;
- проникнення в мережні ресурси публічного використання;
- проникнення на комп'ютер через уразливості в операційних системах і застосуваннях;
- паразитування на інших шкідливих програмах.

«Троянські коні»

Програми, які дістали назву «троянські коні» (іноді їх називають «троянськими програмами» і «троянами» або «троянцями»), — це програми, що мають привабливий зовнішній вигляд, але виконують шкідливі, дуже часто — руйнівні функції. У деяких «троянських коней» ці функції добре приховані, тож користувач може і не підозрювати, що його комп'ютер уже скомпрометований. Класичний «троянський кінь» не має функцій доставляння програми на комп'ютер-жертву, позаяк єдине його завдання — звернути на себе увагу користувача і змусити його запустити цю програму.

Яким чином «троянці» приваблюють користувачів? Методи введення користувачів в оману, що враховують особливості конкретної категорії осіб, називають *соціальною інженерією*. Для прикладу розглянемо одне з творінь, яке належить до категорії хробаків — позаяк активно розсилає себе, але для свого запуску потребує дій користувача (тобто має ознаки «троянського коня»). Цей хробак — перший хробак, розроблений для стільникових телефонів, що розповсюджується за допомогою MMS-повідомлень. «Лабораторія Касперського» присвоїла йому кодове ім'я Worm.SymbOS.Comwar.a (інші розробники антивірусного ПЗ використовують інші системи класифікації). Хробак працює на телефонах під керуванням ОС Symbian Series 60 і розповсюджується через Bluetooth і MMS.

Після запуску хробак ініціює пошук пристроїв, доступних через Bluetooth, і передає на них заражений SIS-архів із довільним ім'ям. Щоб його відкрити (і заразити телефон), потрібно кілька разів підтвердити приймання файлу. Цікавим є спосіб розповсюдження через MMS. Хробак розсилає себе по контактах адресної книги в MMS-повідомленнях, вставляючи тему і текст повідомлення, які мають зацікавити користувача і приспати його пильність (слід врахувати, що MMS надходить від особи, відомої потенційній жертві). Тема і текст повідомлень можуть бути такі:

- Norton Antivirus
  Released now for mobile, install it!
- 3DGame
  3DGame from me. It is FREE !
- Audio driver
  Live3D driver with polyphonic virtual speakers!
- Happy Birthday!
  Happy Birthday! It is present for you!
- Internet Accelerator
  Internet accelerator, SSL security update #7.
- Internet Cracker
  It is *EASY* to *CRACK* provider accounts!
  Matrix has you. Remove matrix!
- Nokia ringtoner
  Nokia RingtoneManager for all models.
- PocketPCemu
  PocketPC *REAL* emulator for Symbian OS! Nokia only.
- PowerSave Inspector

```
    Save you battery and *MONEY*!
```

- ```
  Symbian security update
    See security news at www.symbian.com
  ```
- ```
  SymbianOS update
    OS service pack #1 from Symbian inc.
  ```
- ```
  WWW Cracker
    Helps to *CRACK* WWW sites like hotmail.com
  ```

Як бачимо, типовими пропозиціями є безкоштовні програми — різні утиліти, зокрема, антивірусні програми, ігри, а також засоби безкоштовного доступу до платних ресурсів Інтернету.

2. Класифікація «троянських коней»

«Троянських коней» звичайно класифікують за тими діями, які вони здійснюють на зараженому комп'ютері (така класифікація значною мірою повторює класифікацію програмних закладок, розглянуту нами раніше). У цьому підрозділі наведено категорії «троянців», які використовують фахівці з «Лабораторії Каспер- ського»:

- шпигунські програми (Trojan-Spy);
- крадіжка паролів (Trojan-PSW);
- крадіжка кодів доступу до мережі AOL (America Online); ці «троянці» складають окрему групу через свою численність (Trojan-AOL);
- сповіщення про успішну атаку (Trojan-Notifier);
- троянські утиліти віддаленого адміністрування (Backdoor);
- інтернет-клікери (Troj an- Clicker);
- доставляння шкідливих програм (Trojan-Downloader);
- інсталяція шкідливих програм (Trojan-Dropper);
- троянські проксі-сервери (Trojan-Proxy);
- «бомби» в архівах (ArcBomb);
- інші троянські програми (Trojan).

Деяких пояснень потребує остання категорія. До неї належать ті «троянці», що здійснюють руйнування або зловмисну модифікацію даних, порушують роботу комп'ютера тощо. Такі дії можуть бути здійснені шляхом впровадження «логічної бомби» (тобто програмної закладки) або безпосередньо під час запуску «троянського коня». До цієї категорії також належать багатофункціональні «троянські коні», які, наприклад, надають зловмиснику доступ до зараженого комп'ютера або проксі-сервера і водночас стежать за діями локального користувача.

3. Шпигунські троянські програми

Численні «троянці» відразу після запуску «викрадають» із комп'ютера цінну інформацію і надсилають п зловмиснику за заданою в їхньому коді електронною адресою. Оскільки найчастіше такі програми «крадуть» паролі доступу до Інтернету (нерідко з відповідними номерами телефонів), за ними закріпилася назва Password-Stealing-Ware (PSW).

Деякі «троянці» передають також іншу інформацію про заражений комп'ютер, наприклад, про систему, тип поштового клієнта, IP-адресу, а іноді й реєстраційну інформацію до різного програмного забезпечення, коди доступу до мережних ігор тощо.

До окремої великої групи належать «троянці», які «крадуть» коди доступу до мережі AOL.

Також є категорія «троянців», які діють як складова багатокомпонентних наборів шкідливого програмного забезпечення. Завдання цих програм — сповістити розробника про зараження комп'ютера (інсталяцію програмної закладки). На адресу розробника надсилається, наприклад, IP-адреса комп'ютера, номер відкритого порту, адреса електронної пошти тощо. Повідомлення надсилають електронною поштою, через спеціальне звернення до веб-сторінки розробника та за допомогою ICQ.

4 Троянські інсталятори

Інсталятори поділяють на дві категорії — Downloader і Dropper. Перші здійснюють завантаження програм із мережі, а другі — містять програми для інсталяції у собі.
  ```

Програми класу Downloader часто використовують програмну закладку для здійснення періодичного оновлення версій шкідливих програм. Інколи такі програми здійснюють одноразове завантаження з мережі інших «троянців» або рекламних систем. Завантажені з Інтернету програми запускаються на виконання або реєструються на автозапуск відповідно до можливостей операційної системи. Усі ці дії відбуваються без відома користувача. Інформація про імена та розміщення програм, що завантажуються, закладена в код «троянця» або завантажується ним із «керуючого» ресурсу Інтернету (як правило, з веб-сторінки).

Троянські програми класу Dropper створено для приховування інсталяції інших програм (ясно, що шкідливих). Вони, як правило, мають таку структуру:

Основний код
Файл 1 _____
Файл 2 _____

За допомогою основного коду інші компоненти файлу (файл 1, файл 2,...) записуються на диск (у корінь диска C, у тимчасовий каталог, каталоги Windows) і запускаються на виконання. Це відбувається без жодних повідомлень або з хибними повідомленнями про помилку в архіві. При цьому щонайменше один із компонентів є «троянським конем», і щонайменше один компонент є «обманкою» (програмою-жартом, грою, картинкою тощо). «Обманка» відволікає користувача та імітує корисні дії програми, поки троянський компонент інсталюється в системі.

5 «Троянські бомби»

На відміну від «логічних бомб», які спрацьовують за певної умови, «бомби», закладені у «троянські коні», спрацьовують одразу після запуску такого «троянця». Напевно, це найкласичніший різновид «троянців», хоча останнім часом і не такий поширений. Не всі дії теперішніх зловмисників можна назвати «чистим» вандалізмом, навіть якщо їх ціллю є блокування деякої (але не будь-якої) системи або знищення інформації.

Функції такої «бомби» реалізують таким чином: використовують некоректний заголовок архіву, дані, що повторюються, чи однакові файли в архіві. Некоректний заголовок чи зіпсовані дані в архіві можуть призвести до збою в роботі архіватора або алгоритму розархівування. Дуже великий файл, який містить дані, що повторюються, можна заархівувати в архів невеликого розміру. Величезну кількість (десятки тисяч) однакових файлів спеціальними методами можна упакувати в невеликий архів (десятки кілобайтів). Розпакування таких архівів призводить до несподівано великих затрат ресурсів процесора, пам'яті та дискового простору.