Тема 10-11. Поняття шкідливого програмного забезпечення. Основні типи та загальний огляд сучасних комп'ютерних вірусів.

Поняття шкідливого програмного забезпечення

Вірус - програма, здатна створювати свої копії (необов'язково співпадаючі з оригіналом) і впроваджувати їх у файли, системні області комп'ютера, комп'ютерних мереж, а також здійснювати інші деструктивні дії. При цьому копії зберігають здатність подальшого поширення. Комп'ютерний вірус відноситься до шкідливим програмам.

Ще одна проблема, пов'язана з визначенням комп'ютерного вірусу криється в тому, що сьогодні під вірусом найчастіше розуміється не "традиційний" вірус, а практично будь-яка шкідлива програма. Це призводить до плутанини в термінології, ускладненої ще й тим, що сьогодні практично будь антивірус здатний виявляти всі типи шкідливих програм, таким чином асоціація "шкідлива програма-вірус" стає все більш стійкою.

Шкідлива програма - комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в комп'ютерній системі (КС), або для прихованого нецільового використання ресурсів КС, або іншого впливу, що перешкоджає нормальному функціонуванню КС. До шкідливим програмам ставляться комп'ютерні віруси, трояни, мережні хробаки і інші.

Віруси

До вірусів відносяться:

– ***Завантажувальні віруси*** - віруси, що заражають завантажувальні сектори постійних і змінних носіїв;

– ***Файлові віруси*** - віруси, що заражають файли;

– ***Макровіруси*** - віруси, написані мовою макрокоманд і виконують у середовищі якого-небудь додатка. У переважній більшості випадків мова йде про макроси в документах Microsoft Office;

– ***Скрипт-віруси*** - віруси, що виконуються у середовищі певної командної оболонки: раніше - bat-файли в командній оболонці DOS, зараз частіше VBS-і Java-скрипти в командній оболонці Windows Scripting Host (WSH);

Окремо варто сказати пару слів про макровіруси. Більшість електронних документів створюються й обробляються у форматі MS Office, інструмент VBA (Visual Basic for Application), який можна використовувати для створення макровірусів поставляється разом з додатком MS Office. Такий стан речей призводить до того, що на сьогоднішній день макровіруси - найбільш розповсюджений тип вірусів. Однак боротьба з ними не викликає особливих проблем і зводиться до вивчення тіла шкідливого макросу за допомогою того ж VBA на предмет виконуваних операцій, контролю стартових макросів AutoOpen, AutoClose, AutoSave, глобальних макросів FileOpen, FileSaveAs, FileSave, FileClose і ряду стандартних операцій, таких як виклик API-функцій, виконання команд Shell і т. д. Процедура лікування макровірусів зводиться до видалення тіла макросу з документів і шаблонів MS Office.

Мережеві черв'яки

Черв'як (мережний черв'як) - тип шкідливих програм, що поширюються по мережних каналах, здатних до автономного подолання систем захисту автоматизованих і комп'ютерних систем, а також до створення й подальшого поширення своїх копій,

У залежності від шляхів проникнення в операційну систему чирви діляться на:

– *Поштові черв'яки* (Mail-Worm) - черв'яки, що поширюються у форматі повідомлень електронної пошти;

– *IM черв'яки* (IM-Worm) - черв'яки, що використовують Інтернет-пейджери;

– *P2P черв'яки* (P2P-Worm) - черв'яки, що розповсюджується за допомогою пірінгових (peer-to-peer) файлообмінних мереж;

– *Мережеві черв'яки* (Net-Worm) - інші мережеві черв'яки, серед яких має сенс додатково виділити Інтернет-хробаки і LAN-черв'яки.

Інтернет черв'яки - черв'яки, що використовують для поширення протоколи Інтернет. Переважно цей тип черв'яків поширюється з використанням неправильної обробки деякими додатками

базових пакетів стека протоколів TCP / IP.

LAN черв'яки - черв'яки, що поширюються по протоколах локальних мереж.

Трояни

– ***Троян*** (троянський кінь) - тип шкідливих програм, основною метою яких є шкідливий вплив стосовно комп'ютерної системи. Трояни відрізняються відсутністю механізму створення власних копій.

– Деякі трояни здатні до автономного подолання систем захисту КС, з метою проникнення й зараження системи. У загальному випадку, троян попадає в систему разом з вірусом або хробаком, у результаті необачних дій користувача або ж активних дій зловмисника. Найбільш поширені наступні види троянів:

– ***Клавіатурні шпигуни*** (Trojan-SPY) - трояни, що постійно перебувають у пам'яті і зберігають всі дані, що надходять від клавіатури з метою наступної передачі цих даних зловмисникові. Зазвичай в такий спосіб зловмисник намагається довідатися паролі або іншу конфіденційну інформацію.

– ***Викрадачі паролів*** (Trojan-PSW) - трояни, також призначені для одержання паролів, але не використають спостереження за клавіатурою. Зазвичай в таких троянах реалізовані способи добування паролів з файлів, в яких ці паролі зберігаються різними додатками.

– ***Утиліти віддаленого керування*** (Backdoor) - трояни, що забезпечують повний віддалений контроль над комп'ютером користувача. Існують легальні утиліти такої ж властивості, але вони відрізняються тим, що повідомляють про своє призначення при установці або ж постачаються з документацією, у якій описані їхні функції. Троянські утиліти вилученого керування ніяк не видають свого реального призначення, так що користувач і не підозрює про те, що його комп'ютер підконтрольний зловмисникові. Найбільш популярна утиліта віддаленого управління - Back Orifice.

– ***Анонімні smtp-сервери й проксі*** (Trojan-Proxy) - трояни, що виконують функції поштових серверів або проксі й, що використаються в першому випадку для спам-розсилок, а в другому для замітання слідів хакерами.

– ***Модифікатори настроювань браузера*** (Trojan-Cliker) - трояни, які міняють стартову сторінку в браузері, сторінку пошуку або ще які-небудь настроювання, для організації несанкціонованих звертань до Інтернет-ресурсів.

– ***Інсталятори інших шкідливих програм*** (Trojan-Dropper) - трояни, що представляють можливість зловмисникові здійснювати приховану установку інших програм.

– ***Завантажувачі шкідливих програм*** (Trojan Downloader) - трояни, призначені для завантаження на комп'ютер-жертву нових версій шкідливих програм, або рекламних систем.

– ***Повідомлювачі про успішну атаку*** (Trojan-Notifier) - трояни даного типу призначені для повідомлення своєму "господарю" про зараження комп'ютеру.

– ***"Бомби" в архівах*** (ARCBomb) - трояни, що представляють собою архіви, спеціально оформлені таким чином, щоб викликати нештатну поведінку архіваторів при спробі розархівувати дані - зависання або істотне уповільнення роботи комп'ютера, заповнення диска великою кількістю "порожніх" даних.

– ***Логічні бомби*** - частіше не стільки трояни, скільки троянські складові черв'яків і вірусів, суть роботи яких полягає в тому, щоб за певних умов (дата, час доби, дії користувача, команда ззовні) зробити певну дію: наприклад, знищення даних.

– ***Утиліти дозвону*** - порівняно новий тип троянів, що представляє собою утиліти dial-up доступу в Інтернет через платні поштові служби. Такі трояни прописуються в системі як утиліти дозвону за замовчуванням і спричиняють за собою великі рахунки за користування Інтернетом.

Життєвий цикл шкідливих програм

Процес розмноження вірусів може бути умовно розділений на кілька стадій:

- Активація вірусу.
- Пошук об'єктів для зараження.
- Підготовка вірусних копій.
- Впровадження вірусних копій.

Так само як для вірусів, життєвий цикл хробаків можна розділити на певні стадії:

- Проникнення в систему.
- Активація.
- Пошук "жертв".
- Підготовка копій.
- Поширення копій.

У троянів внаслідок відсутності функцій розмноження й поширення, їхній життєвий цикл менше ніж у вірусів - усього три стадії:

- Проникнення на комп'ютер.
- Активація.
- Виконання закладених функцій.

Це, само собою, не означає малого часу життя троянів. Навпаки, троян може непомітно перебувати в пам'яті комп'ютера тривалий час, ніяк не видаючи своєї присутності, до тих пір, поки не виконає свою шкідливу функцію.

Основні шляхи проникнення в систему і активації

Існує твердження - будь-яку шкідливу програму користувач може перемогти самостійно, тобто не вдаючись до використання антивірусних програм. Це дійсно так, за успішними діями будь-якої антивірусної програми стоїть праця вірусних аналітиків, які вручну розбираються з алгоритмами роботи нових вірусів, виділяють сигнатури, описують алгоритм роботи вірусу.

Сигнатура вірусу - в широкому сенсі, інформація, що дозволяє однозначно визначити наявність даного вірусу у файлі або іншому коді.

Прикладами сигнатур є: унікальна послідовність байт, присутня в даному вірусі і не зустрічається в інших програмах; контрольна сума такої послідовності

Таким чином, антивірусну програму можна розглядати як засіб автоматизації боротьби з вірусами. Слід зауважити, що аналіз вірусів потребує від користувача володіння більшим обсягом специфічних знань в області програмування, роботи операційних систем і т.д. Сучасні шкідливі програми використовують складні технології маскування і захисту своїх копій, які обумовлюють необхідність застосування спеціальних засобів для їх аналізу.

Процес підготовки шкідливою програмою своїх копій для поширення може істотно відрізнятися від простого копіювання. Автори найбільш складних у технологічному плані вірусів намагаються зробити різні копії максимально несхожими для ускладнення їх виявлення антивірусними засобами. Як наслідок, складання сигнатури для такого вірусу вкрай ускладнено.

При створенні копій для маскування можуть застосовуватися наступні технології:

Шифрування - вірус складається із двох функціональних блоків: власне вірусу і шифратора. Кожна копія вірусу складається із шифратора, випадкового ключа й вірусного блоку, зашифрованого цим ключем

Метаморфізм - створення різних копій вірусу шляхом заміни груп команд на еквівалентні, перестановки місцями блоків коду, вставки між значущими шматками коду "сміттєвих" команд, які практично нічого не роблять.

Поєднання цих двох технологій приводить до появи наступних типів вірусів.

Шифрований вірус - вірус, що використає просте шифрування з випадковим ключем і незмінний шифратор. Такі віруси легко виявляються по сигнатурі шифратора.

Метаморфний вірус - вірус, що застосовує метаморфізм до всього свого тіла для створення нових копій.

Поліморфний вірус - вірус, що використає метаморфний шифратор для шифрування основного

тіла вірусу з випадковим ключем. При цьому частина інформації, використовуваної для одержання нових копій шифратора також може бути зашифрована. Наприклад, вірус може реалізовувати кілька алгоритмів шифрування і при створенні нової копії міняти не тільки команди шифратора, але і сам алгоритм

Розглядаючи сучасні вірусні загрози необхідно відзначити, що більше 90% відсотків вірусних погроз останнім часом пов'язані з хробаками. Найбільш численну групу в цьому класі шкідливих програм становлять поштові черв'яки. Інтернет-черв'яки також є помітним явищем, але не стільки через кількість, скільки через якість: епідемії, викликані Інтернет-хробаками найчастіше відрізняються високою швидкістю розповсюдження і великими масштабами. IRC і P2P черв'яки зустрічаються досить рідко, частіше IRC та P2P служать альтернативними каналами поширення для поштових і Інтернет-черв'яків. Поширення через LAN також використовується переважно як додатковий спосіб поширення.

Крім того, на етапі активації хробаків можна розділити на дві великі групи, що відрізняються як за технологіями активації, так і по тривалістю життя:

Для активації необхідно активна участь користувача.

Для активації участь користувача не потрібна зовсім або досить лише пасивної участі.

Активація мережного хробака без участі користувача завжди означає, що хробак використовує пролом в безпеці програмного забезпеченні комп'ютера. Це призводить до дуже швидкого поширення хробака у середині корпоративної мережі з більшим числом станцій, істотно збільшує завантаження каналів зв'язку і може повністю паралізувати мережу. Саме цей метод активації використали черв'яки Lovesan і Sasser. Під пасивною участю користувача розуміється, наприклад, перегляд листів у поштовому клієнті, при якому користувач не відкриває вкладені файли, але його комп'ютер тим не менше виявляється зараженим.

Активна участь користувача в активації хробака означає, що користувач був уведений в оману методами соціальної інженерії. У більшості випадків основним фактором служить форма подачі інфікованого повідомлення: воно може імітувати лист від знайомої людини (включаючи електронну адресу, якщо знайомий уже заражений), службове повідомлення від поштової системи або ж що-небудь подібне, настільки ж часто зустрічається в потоці звичайної кореспонденції.

При зараженні комп'ютера хробаки зазвичай виробляють наступні дії:

Створюють виконуваний файл з розширенням .exe з довільним ім'ям або ім'ям дуже схожим на ім'я системних файлів Windows. У деяких черв'яках можуть використовуватися технології притаманні вірусам, в такому випадку черв'яки інфікують вже існуючий файл програми (наприклад WSOCK32.DLL) або замінюють його на свій файл (наприклад I-Worm.MTX записує одну зі своїх процедур в файл WSOCK32.DLL таким чином, що вона перехоплює відсилання даних в Інтернет (процедура send). Внаслідок черв'як в зараженій бібліотеці WSOCK32.DLL отримував управління кожен раз, коли дані відправляються в Інтернет).

Крім цього, разом з додаванням в систему виконуваних файлів, в ряді випадків черв'яки поміщають в систему файли бібліотек, які зазвичай виконують функції Backdoor компонентів (наприклад один з клонів хробака MyDoom - I-Worm.Mydoom.aa створював системному каталозі Windows файл tcp5424.dll , що є Backdoor-компонентом і реєстрував його в системному реєстрі: HKCR \ CLSID \ {E6FB5E20-DE35-11CF-9C87-00AA005127ED} \ InProcServer32 {Default} = "% SysDir% \ tcp5424.dll").

Шкідлива програма може вносити зміни в системні файли win.ini і system.ini. Наприклад Email-Worm.Win32.Toil при установці в заражаємо системі копіює себе в папку Windows з випадковим ім'ям і записує у файл system.ini наступні значення:

[Boot]

shell = Explorer.exe% ім'я хробака%

що забезпечує йому автозапуск при кожному перезавантаженні Windows (але тільки під Win9x/Me).

Email-Worm.Win32.Atak.h в процесі інсталяції копіює себе з ім'ям dec25.exe в системний каталог Windows і модифікує файл win.ini для свого подальшого запуску - додає повний шлях до файлу

dec25.exe в ключ run секції [windows]:

[Windows]

run =% SystemDir% \ dec25.exe)

Слід так само відзначити, що у файлі system.ini крім секції [boot] шкідливі програми можуть використовувати секцію [Drivers].

Шкідливі програми можуть вносити зміни в наступні гілки реєстру:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion в ключі Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce - для того щоб система запускала створені хробаком файли.

HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion в ключ Run.

Наприклад, Email-Worm.Win32.Bagle.ax після запуску копіює себе в системний каталог Windows, після чого реєструє в реєстрі скопійований файл: HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run "Sysformat" = "% System% \ sysformat. exe

HKEY_CLASSES_ROOT \ exefile \ shell \ open \ command

Крім вище перерахованих гілок і ключів реєстру шкідливі програми можуть вносити зміни і в інші гілки і ключі реєстру, наприклад:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ WOW \ boot
HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Drivers32
HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows NT \ CurrentVersion \ WinLogon
HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Active Setup \ Installed Components HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ AeDebug.

Усунення наслідків зараження

У зв'язку з тим що, що черв'яки практично не використовують технології шифрування і метаморфізму для маскування своїх копій, боротьба з ним вручну дещо спрощується і зводиться донаступного алгоритму дій:

1. Аналіз і виявлення за допомогою Диспетчера завдань Windows підозрілих процесів;
2. Аналіз відкритих портів за допомогою команди Netstat;
3. Вивантаження підозрілих процесів;
4. Аналіз реєстру за допомогою утиліти Regedit.exe в вище перерахованих гілках і ключах;
5. Відновлення та правка ключів реєстру;
6. Пошук інфікованих файлів по імені на основі даних аналізу процесів операційної системи і даних аналізу реєстру;
7. Видалення або заміна інфікованих файлів;
8. Перевантаження системи;
9. Контрольний аналіз процесів, ключів реєстру, відкритих портів.

Якщо підозрілих процесів не виявлено, ключі реєстру не змінилися, значить, процедуру дезинфекції комп'ютера можна вважати успішною, в іншому випадку алгоритм доведеться повторити.

Тим не менше, враховуючи той факт, що сучасні хробаки можуть використовувати технології притаманні вірусам, встановлювати backdoor-компоненти, ускладнюючи тим самим, процедуру аналізу та виявлення своїх файлів, для повної впевненості комп'ютер після дезінфекції вручну настійно рекомендується здійснити перевірку антивірусним засобом. Слід також зазначити, що боротися вручну з шкідливими програмами можна тільки постфактум - після того, як вони вразили комп'ютер, в той же час використання антивірусного програмного забезпечення в переважній більшості випадків не допустить активації шкідливої програми на комп'ютері

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається комп’ютерним вірусом?
2. Які існують основні групи вірусів?

3. Опишіть основні типи мережевих черв’яків.
4. Опишіть основні типи троянів.
5. Зробіть аналіз життєвого циклу шкідливих програм.
6. Які існують способи проникнення шкідливої програми на персональний комп’ютер?
7. Назвіть основні ознаки враження вірусом.
8. Поясніть у чому різниця між шифрованим і поліморфним вірусом?
9. Чи достатньо для захисту від зараження шкідливою програмою встановити файлам дозвіл тільки для читання? Обґрунтуйте відповідь.
10. Поясніть у чому відмінність понять вірус і шкідлива програма.