Житомирська політехніка	Міністерство освіти і науки України Державний університет «Житомирська політехніка»

ЛЕКЦІЯ №10

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ЗАХИСТ ВІД НЬОГО

План лекції:

- КЛАСИФІКАЦІЯ ШКІДЛИВОГО ПРОГРАМНОГО
- ЗАБЕЗПЕЧЕННЯ ТА СПОСОБИ ЙОГО РОЗПОВСЮДЖЕННЯ.
- ПРОГРАМНІ ЗАКЛАДКИ. УТИЛІТИ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ.
- КОМП'ЮТЕРНІ ВІРУСИ.
- СПЕЦІАЛЬНІ ХАКЕРСЬКІ УТИЛІТИ.
- ЗАХОДИ ЩОДО ЗАХИСТУ ТА ПРОТИДІЇ.

ПИТАННЯ №1

КЛАСИФІКАЦІЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА СПОСОБИ ЙОГО РОЗПОВСЮДЖЕННЯ

КЛЮЧОВІ ТЕРМІНИ

Під терміном ***шкідливе програмне забезпечення*** (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*** (англ. – destructive software).

КЛАСИФІКАЦІЯ ШКІДЛИВОГО ПЗ

Шкідливе програмне забезпечення класифікують за різними ознаками.

Програмні закладки (англ. – program bug) застосовують майже до всього шкідливого програмного забезпечення, крім комп'ютерних вірусів. 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.

КЛАСИФІКАЦІЯ ШКІДЛИВОГО ПЗ

Класифікація шкідливого програмного забезпечення:

1. ***За способом розповсюдження засобу*** – яким чином засіб потрапляє на комп'ютер і домагається своєї активізації;
2. ***За метою функціонування засобу*** – які саме шкідливі дії він здійснює.

За механізмами розповсюдження виділяють такі шкідливі програмні засоби:

1. ***Класичні комп'ютерні віруси***:

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

2. ***Мережні хробаки***:

- поштові хробаки;
- хробаки, що використовують інтернет–пейджери;
- хробаки в IRC-каналах;
- хробаки для файлообмінних мереж (Peer-to-Peer Network, P2P);
- інші мережні хробаки.

3. ***«Троянські коні»***.
4. ***Спеціальні хакерські утиліти***.

КЛАСИФІКАЦІЯ ШКІДЛИВОГО ПЗ

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.

КЛАСИФІКАЦІЯ ШКІДЛИВОГО ПЗ

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).

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*** (англ. – exploit), що підкреслює факт використання (експлуатації) ними деякої вразливості системи.

ПИТАННЯ №2

ПРОГРАМНІ ЗАКЛАДКИ

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.

ФУНКЦІЇ ПРОГРАМНИХ ЗАКЛАДОК

До функцій програмних закладок відносять наступні:

1. ***Перехоплення і передавання інформації***:

- крадіжка паролів;
- шпигунські програми.

2. ***Порушення функціонування систем («логічні бомби»)***:

- знищення інформації;
- зловмисна модифікація інформації;
- блокування системи.

3. ***Модифікація програмного забезпечення***:

- утиліти віддаленого адміністрування (люки);
- інтернет-клікери;
- проксі-сервери;
- дзвінки на платні ресурси;
- організація DoS- і DDoS-атак.

4. ***Психологічний тиск на користувача***:

- реклама;
- лихі жарти і містифікації.

ШПИГУНСЬКІ ПРОГРАМИ

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 зокрема серійними номерами ліцензійних програм.

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

«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.

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.

Єдине, що вирізняє з-поміж таких програм шкідливі програмні закладки, – **це відсутність попереджень про їх інсталяцію і запуск**.

Можна констатувати, що програмні закладки цього типу є одними з найнебезпечніших, оскільки вони потенційно уможливлюють будь-які зловмисні дії.

ЛЮКИ – УТИЛІТИ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ

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.

Бекдо́р (від англ. back door, чорний хід) – в комп'ютерній системі (криптосистемі або алгоритмі) – це метод обходу стандартних процедур автентифікації, несанкціонований віддалений доступ до комп'ютера, отримання доступу до відкритого тексту, і так далі, залишаючись при цьому непоміченим. Бекдор може приймати форму встановленої програми (наприклад, «троянський кінь» Back Orifice) або може проникнути у систему через руткіт.

Початкові паролі можуть функціювати як бекдори, якщо вони не змінені користувачем. Деякі функції налагодження можуть також виступати як бекдори, якщо вони не будуть видалені в остаточній версії програми.

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 та 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. Далі 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 вони 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-СЕРВЕР ТА ДОСТУП ДО ПЛАТНИХ РЕСУРСІВ

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.

ІНСТАЛЯЦІЯ З МЕРЕЖІ

Майже в усіх сучасних програмних продуктах передбачено можливість звернення до веб-сайту розробника та пошуку оновлень (це відбувається автоматично і переважно не потребує підтвердження користувача), а також завантаження інсталяційних пакетів із мережі (за підтвердженням користувача). Однак слід визнати, що не всі користувачі (а тим паче адміністратори корпоративних систем) у захваті від того, що програмні засоби з їхніх комп'ютерів самостійно виходять в Інтернет. Це зумовлено тим, що під час інсталяції програмного забезпечення користувачів не завжди попереджають про наявність модулів-інсталяторів і не надають їм можливості відмовитися від інсталяції таких програм. Часто встановлені модулі складно відключити. Для цього досвідченим користувачам доводиться вручну редагувати системний реєстр.

РЕКЛАМНІ МОДУЛІ (ADWARE)

Рекламні модулі – це тип шкідливого програмного забезпечення, яке спрямоване на відображення реклами на комп'ютері або мобільному пристрої користувача без його згоди або знання. **Ось деякі характеристики та наслідки рекламних модулів:**

- ***Помітна реклама***: Рекламні модулі можуть відображати рекламні банери, вікна, анімацію і навіть автоматично відкривати веб-сторінки з рекламним контентом.
- ***Порушення приватності***: Деякі рекламні модулі можуть збирати особисту інформацію про користувача, таку як переглянуті веб-сторінки і введені дані, та передавати цю інформацію третім сторонам без згоди користувача.
- ***Сповільнення пристрою***: Велика кількість рекламних елементів може сповільнювати роботу комп'ютера або мобільного пристрою і викликати нестабільність.
- ***Потенційна загроза безпеці***: Деякі рекламні модулі можуть бути використані зловмисниками для розповсюдження інших шкідливих програм або для викрадення даних.

ЛИХІ ЖАРТИ

Лихі жарти відносяться до програмного забезпечення або дій, які призводять до різного роду неприємностей або розваги, але без шкоди для даних або пристрою користувача. **Ось деякі приклади лихих жартів:**

- ***Скріншоти робочого столу***: Програми, які автоматично створюють скріншот робочого столу і роблять його фоном, можуть створювати смішні ситуації на комп'ютері користувача.
- ***Звуки і фонові мелодії***: Лихі жарти можуть включати нудні звуки, які неперервно відтворюються або змінюються на пристрої користувача.
- ***Фальшиві повідомлення і сповіщення***: Програми можуть відправляти фальшиві повідомлення, щоб зіграти над користувачем жарт.
- ***Зміна налаштувань***: Лихі жарти можуть внести зміни в налаштування пристрою, такі як зміна фону робочого столу, розташування піктограм або мови інтерфейсу.

Важливо розрізняти лихі жарти від справжніх загроз для безпеки. Лихі жарти призначені для розваги і можуть бути надокучливими, але вони не завдають шкоди пристрою чи даним користувача.

ПИТАННЯ №3

КОМП'ЮТЕРНІ ВІРУСИ

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. **Комп'ютерні віруси розрізняють за такими ознаками:**

1. ***За середовищем існування*** (системні області комп'ютера, ОС, прикладні програми, до певних компонентів яких впроваджують код вірусу):
   - файлові віруси;
   - завантажувальні віруси;
   - макровіруси;
   - скриптові віруси.
2. ***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***.

МЕРЕЖЕВІ ВІРУСИ

Мережеві віруси в якості середовища існування використовують глобальну або локальні комп'ютерні мережі. Вони не зберігають свій код на жорсткому диску комп'ютера, а проникають безпосередньо в оперативну пам'ять ПК. Віруси цього типу мають здатність обчислювати мережеві адреси інших машин, перебуваючи в пам'яті комп'ютера, і самостійно розсилати за цими адресами свої копії. Їх називають мережними хробаками. Такий вірус може знаходитися одночасно в пам'яті кількох комп'ютерів. Мережеві віруси виявити складніше, ніж файлові. Мережеві віруси поширюються з великою швидкістю і можуть сильно уповільнити роботу апаратного забезпечення комп'ютерної мережі.

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. Такепрограмне 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.

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: поштові хробаки (Email-worm); хробаки у IRC-каналах (IRC-worm); хробаки для файлообмінних мереж (P2P-worm); інші мережні хробаки (Net-worm).

ПОШТОВІ ХТОБАКИ

Поштові хробаки надсилають заражені повідомлення у різні способи:

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

Для пошуку поштових адрес, на які розсилатимуться заражені листи, також використовують різні методи:

- хробак розсилає себе на всі адреси, що було знайдено в адресній книзі Microsoft Outlook;
- адреси зчитуються з адресної бази WAB;
- хробак сканує «придатні» файли у файловій системі та позначає в них рядки, що є адресами електронної пошти;
- хробак вибирає адреси з листів, що містяться у поштовій скриньці (при цьому деякі хробаки можуть «відповідати» на знайдені у скриньці листи).

ХРОБАКИ В IRC-КАНАЛАХ. ХРОБАКИ ДЛЯ ФАЙЛООБМІННИХ МЕРЕЖ ТА ІН.

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. Файлообмінні мережі беруть на себе левову частку роботи з доставки файлу, тому хробаку достатньо скопіювати себе в каталог обміну файлами, що розташований на локальній машині.

Інші мережні хробаки. Це хробаки, які використовують інші способи зараження віддалених комп'ютерів. **Серед цих способів можна виділити наступні:**

- 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.

ХРОБАК МОРРІСА

Насамперед розглянемо відомий хробак Морріса або, як його іноді називають, вірус Морріса. Інцидент із хробаком Морріса стався у листопаді 1988 року.

Хробак Морріса – досить складний пакет програм, який реалізував (або намагався реалізувати) **такі функції**:

- пошук цілей для атаки;
- проникнення на віддалені цілі;
- завантаження через мережу основного програмного коду, його компіляцію і запуск на виконання;
- сповіщення про зараження чергової машини;
- заходи щодо приховування свого існування;
- перевірку на зараженість локальної та віддалених машин для запобігання повторному зараженню.

ХРОБАК МОРРІСА. ПОШУК ЦІЛЕЙ ДЛЯ АТАКИ

Для здійснення пошуку було передбачено низку процедур:

- сканування таблиці маршрутів і виявлення всіх адрес доступних шлюзів;
- обирання номеру підмережі з-поміж усіх мережних адрес локальної машини (оскільки атаковано було переважно шлюзи, більшість атакованих машин мали кілька мережних інтерфейсів і кілька адрес) з подальшим перебиранням адрес у цих підмережах (за жодної процедури не робилося повного перебирання; крім того, після першої успішної атаки процедура завершувалася);
- вибирання адрес зі списку з файлу /etc/hosts.equiv;
- вибирання адрес із персональних файлів користувачів .forward; ці адреси було використано для спроб застосувати підібрані паролі користувачів.

ХРОБАК МОРРІСА. ПРОНИКНЕННЯ НА ВІДДАЛЕНІ ЦІЛІ

Хробак застосовував кілька стратегій проникнення, використання деяких із них залежало від того, яким чином була отримана адреса цілі. Метою проникнення було виконання на віддаленому комп'ютері команди від імені легального користувача, що давало змогу встановити з'єднання з атакуючим комп'ютером і завантажити з нього основний програмний код хробака.

Хробак, всупереч розрахункам творця, буквально наповнив собою увесь мережевий трафік ARPANET.

При скануванні комп'ютера хробак визначав, чи інфікований вже комп'ютер чи ні, і випадковим чином обирав, чи перезаписати існуючу копію, щоб убезпечитися від трюку з підробленою копією, внесеної системними адміністраторами. З певною періодичністю програма так чи інакше перезаписувала свою копію. Занадто маленьке число, задане Робертом Моррісом для опису періодичності, і послужило причиною першої в світі епідемії мережевого хробака.

ХРОБАК МОРРІСА. ПРОНИКНЕННЯ НА ВІДДАЛЕНІ ЦІЛІ

Незначна логічна помилка в коді програми призвела до руйнівних наслідків. Комп'ютери багаторазово заражалися хробаком, і кожен додатковий примірник уповільнював роботу комп'ютера до стану відмови обслуговування, вщент вичерпуючи ресурси комп'ютера.

Хробак використовував давно відомі вразливості в поштовому сервері Sendmail, сервісах Finger, rsh/rexec з підбором паролів по словнику (брутфорсинг). Словник був невеликий – усього лише десь 400 ключових слів, але якщо врахувати, що в кінці 1980-х про комп'ютерну безпеку мало хто замислювався та ім'я облікового запису (зазвичай реальне ім'я користувача) часто збігалося з паролем, то цього було достатньо.

Хробак використовував також маскування, щоб приховати свою присутність в комп'ютері: він видаляв свій файл, який виконував, перейменовував свій процес в sh і кожні три хвилини розгалужувався.

За задумом автора хробак повинен був інфікувати тільки VAX-комп'ютери з операційними системами 4BSD і Sun 3. Однак кросплатформний С-код дав хробакові можливість запускатися і на інших комп'ютерах.

ХРОБАК МОРРІСА. НАСЛІДКИ

Збиток від хробака Моріса був оцінений приблизно в 96,5 мільйонів доларів.

Сам Моріс добре замаскував код програми, і навряд чи хто міг довести його причетність. Проте його батько, комп'ютерний експерт Агентства Національної Безпеки, вирішив, що синові краще у всьому зізнатися.

На суді Роберту Морісу загрожувало до п'яти років позбавлення волі та штраф у розмірі 250 тисяч доларів, проте, беручи до уваги пом'якшувальні обставини, його засудили до трьох років умовно, 10 тисяч доларів штрафу і 400 годин громадських робіт.

Масове ураження комп'ютерів показало, наскільки небезпечно беззастережно довіряти комп'ютерним мережам. Згодом були вироблені нові посилені норми комп'ютерної безпеки, що стосуються безпеки коду програм, адміністрування мережевих вузлів і вибору захищених паролів.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

Після Морріса протягом багатьох років ніхто не спромігся створити щось подібне. Те, що називали (і називають) хробаками, фактично наполовину було «троянськими кіньми», оскільки автоматично реалізовувало лише технологію доставлення на комп'ютер-жертву свого програмного коду або посилання на мережний ресурс, де цей код містився. Запуск шкідливого коду на комп'ютері-жертві здійснювався через необережні дії користувачів. Але згодом почали з'являтися справжні хробаки.

У грудні 1997 року з'явилися повідомлення про появу принципово нового типу мережних хробаків, що використовують канали IRC (Internet Relay Chat – система діалогового спілкування через Інтернет). Як виявилося, найпопулярніша утиліта для роботи з IRC-mIRC – мала небезпечну ваду захисту: файл налаштувань script.ini знаходився в каталозі, який одночасно застосовувався для зберігання файлів, завантажених через IRC.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

Таким чином, після того як файл з ім'ям script.ini, що містив програмний код хробака, потрапляв на віддалений комп'ютер, він автоматично замінював оригінальний файл налаштувань. Разом із mIRC запускався й хробак, який, у свою чергу, розсилав себе іншим користувачам. Про соціальну інженерію і технології «троянських коней» тут не йдеться – здійснювався запуск звичайної програми.

У наступні роки переважна більшість хробаків використовувала різні вразливості у програмних продуктах корпорації Майкрософт, які давали їм можливість розповсюджуватися без активного сприяння некомпетентних користувачів. Продукти Майкрософт завжди приваблювали зловмисників, по-перше, через свою надзвичайну розповсюдженість, по-друге, завдяки наявності докладної документації та оснащення для розроблення програм (бібліотек, ресурсів, середовищ розроблення, засобів налагодження тощо), а по-третє, через велику кількість критичних помилок.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

Такі помилки було виявлено у програмі Microsoft Outlook (під час глобальної епідемії **хробака Happy99**, також відомого як Ska), у поштовом клієнті Outlook Express, у браузері Internet Explorer. Незважаючи на те що Майкрософт, як правило, дуже швидко випускає виправлення (патчі), в Інтернеті завжди залишається безліч хостів, де ці виправлення не встановлено. Є багато прикладів глобальних епідемій хробаків, що використовували вразливості, виправлення для яких уже не один рік були доступними на сайті Майкрософт.

Безумовним лідером у 2002 році за кількістю інцидентів став **хробак Klez**. Його модифікації щонайменше два роки посідали «призові» місця у списках найбільш поширених загроз.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

Упродовж 2002 року кожні 6 із 10 зареєстрованих випадків зараження було викликано Klez. І Klez, і його найближчий конкурент за кількістю викликаних інцидентів – **хробак Lentin**, а також хробаки **Tanatos** і **Bad-Trans** використовували для свого розповсюдження вразливість IFRAME в системі безпеки Internet Explorer. Загалом на них припало більше 85 % усіх інцидентів. **Класичними мережними хробаками є представники сімейства Net-Worm.Win32.Sasser**. Ці хробаки використовують уразливість в службі LSASS Microsoft Windows. При розмноженні, хробак запускає FTP-службу на TCP-порту 5554, після чого вибирає IP-адресу для атаки і відсилає запит на порт 445 по цій адресі, перевіряючи, чи запущена служба LSASS. Якщо атакується комп'ютер відповідає на запит, хробак посилає на цей же порт експлойт уразливості в службі LSASS, в результаті успішного виконання якого на віддаленому комп'ютері запускається командна оболонка на TCP-порту 9996. Через цю оболонку хробак віддалено виконує завантаження копії хробака по протоколу FTP із запущеного раніше сервера й віддалено ж запускає себе, завершуючи процес проникнення і активації.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

Як приклад **поштового хробака** можна розглянути **Email-Worm.Win32.Zafi.d**. Заражене повідомлення включає в себе обрані з деякого списку тему і текст, змістом яких є привітання зі святом (велика частина – з Різдвом) і пропозицію ознайомитися з вітальною листівкою у вкладенні. Поздоровлення можуть бути на різних мовах. Ім'я перебуває у вкладенні файлу хробака складається з слова postcard мовою, відповідного привітання, і довільного набору символів. Розширення файлу хробака випадковим чином вибирається з списку .BAT, .COM, .EXE, .PIF, .ZIP. Для розсилки хробак використовує адреси електронної пошти, знайдені на зараженому комп'ютері. Щоб отримати управління, хробак повинен бути запущений користувачем.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

IRC-Worm.Win32.Golember.a є, як випливає з назви IRC-хробаком. При запуску він зберігає себе в каталозі Windows під ім'ям trlmsn.exe і додає в розділ автозапуску реєстру Windows параметр з рядком запуску цього файлу. Крім цього хробак зберігає на диск свою копію у вигляді архіву Janey2002.zip і зображення Janey.jpg. Потім хробак підключається до довільних IRC-каналах під різними іменами і починає слати певні текстові рядки, імітуючи активність звичайного користувача. Паралельно всім користувачам цих каналів відсилається заархівована копія хробака.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

Функціональністю поширення через P2P-канали мають багато мережних і поштових хробаків. Наприклад, **Email-Worm.Win32.Netsky.q** для розмноження через файлообмінні мережі шукає на локальному диску каталоги, що містять назви найбільш популярних мереж або ж слово «shared», після чого кладе в ці каталоги свої копії під різними назвами.

IM-хробаки рідко пересилають заражені файли безпосередньо між клієнтами. Замість цього вони розсилають посилання на заражені веб-сторінки. Так хробак **IM-Worm.Win32.Kelvir.k** посилає через MSN Messenger повідомлення можуть містити текст «its you» і посилання «http://www.malignancy.us//pictures.php?Email\u003d», за вказаною в якій адресою розташований файл хробака. Сьогодні найбільш численну групу складають поштові хробаки. Мережеві хробаки також є помітним явищем, але не стільки через кількість, скільки через якість: епідемії, викликані мережними хробаками найчастіше відрізняються високою швидкістю поширення і великими масштабами. IRC-, P2P- і IM-хробаки зустрічаються досить рідко, частіше IRC, P2P і IM служать альтернативними каналами поширення для поштових і мережевих хробаків.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

На етапі активації хробаки діляться на дві великі групи, що відрізняються як за технологіями, так і за термінами існування:

1. Для активації необхідно активна участь користувача.
2. Для активації участь користувача не потрібна зовсім або досить лише пасивної участі.

Під пасивною участю користувача в другій групі розуміється, наприклад, перегляд листів в поштовому клієнті, При якому користувач не відкриває вкладені файли, але його комп'ютер, проте, виявляється зараженим.

СУЧАСНІ МЕРЕЖНІ ХРОБАКИ

Emotet. Emotet був одним із найпоширеніших та небезпечних банкінг-троянів, який використовувався для поширення інших видів шкідливого програмного забезпечення. У вересені 2021 року правоохоронні органи спільно з інтернаціональними партнерами змогли вивести Emotet з ладу.

Ryuk. Це викуповий троян, який вимагає викуп за розшифрування зашифрованих даних. Він поширюється через вище зазначений Emotet та інші вектори.

TrickBot. TrickBot – це інший банкінг-троян, який також використовувався для розповсюдження різних видів шкідливого програмного забезпечення, включаючи Ryuk. Цей хробак був асоційований з багатьма кіберзлочинними групами.

QakBot (Qbot). QakBot – це інша загроза, яка спеціалізується на викраденні паролів та конфіденційних даних з комп'ютерів і мереж.

Dridex. Це інший банкінг-троян, який був активний в останні роки. Він спрямований на викрадення фінансової інформації.

SolarWinds (Sunburst). Хоча не справжній хробак, Sunburst став однією з найбільших кібератак у 2020 році. Зловмисники вдарили в мережу популярного постачальника програмного забезпечення SolarWinds, інфікувавши тисячі комп'ютерів.

Clop. Clop – це шифруючий рансомвірус, який шифрує файли на комп'ютері і вимагає викуп за їх розшифрування. Цей вид загрози став популярним у 2021 році.

«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 доставки програми на комп'ютер-жертву, через це має наступне завдання – звернути на себе увагу користувача і змусити його запустити цю програму.

СОЦІАЛЬНА ІНЖЕНЕРІЯ

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 – так як активно розсилає себе, але для свого запуску потребує дій користувача (тобто має ознаки «троянського коня»). Цей хробак – перший хробак, розроблений для стільникових телефонів, що розповсюджувався за допомогою MMS-повідомлень. Йому присвоїли кодове ім'я **Worm.SymbOS.Comwar.a** (інші розробники антивірусного ПЗ використовують інші системи класифікації). Хробак працював на телефонах під керуванням ОС Symbian Series 60 і розповсюджувався через Bluetooth і MMS.

СОЦІАЛЬНА ІНЖЕНЕРІЯ

Після запуску хробак ініціював пошук пристроїв, доступних через Bluetooth, і передає на них заражений SIS-архів із довільним ім'ям. Щоб його відкрити (і заразити телефон), потрібно було кілька разів підтвердити приймання файлу. Цікавим є спосіб розповсюдження через MMS. Хробак розсилав 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 надходило від особи, відомої потенційній жертві).

КЛАСИФІКАЦІЯ «ТРОЯНСЬКИХ КОНЕЙ»

«Троянських коней» **зазвичай класифікують за тими діями, які вони здійснюють на зараженому комп'ютері**:

- 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 (Trojan–Clicker);
- доставляння шкідливих програм (Trojan–Downloader);
- інсталяція шкідливих програм (Trojan–Dropper);
- троянські проксі-сервери (Trojan–Proxy);
- «бомби» в архівах (ArcBomb);
- інші троянські програми (Trojan).

ШПИГУНСЬКІ ТРОЯНСЬКІ ПРОГРАМИ

Численні «троянці» відразу після запуску «викрадають» із комп'ютера цінну інформацію і надсилають її 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.

ШПИГУНСЬКІ ТРОЯНСЬКІ ПРОГРАМИ

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 месенджерів.

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 ІНСТАЛЯТОРИ

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
…

ТРОЯНСЬКІ ІНСТАЛЯТОРИ

За допомогою основного коду інші компоненти файлу (файл 1, файл 2,...) записуються на диск (у корінь диска С, 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.

Програми цього класу дають змогу, по-перше, здійснити приховану інсталяцію «троянських коней» або вірусів, а по-друге, обійти деякі антивірусні програми за допомогою архівування і шифрування файлів-компонентів, що не дасть виявити в них відомі сигнатури. Часто ці програми створюють лише задля того, щоб уже відомий «троянець» потрапив до комп'ютера та інсталювався на ньому і щоб їх не виявили ще на підступах до комп'ютера-жертви (на сервері провайдера, на маршрутизаторі або брандмауері тощо).

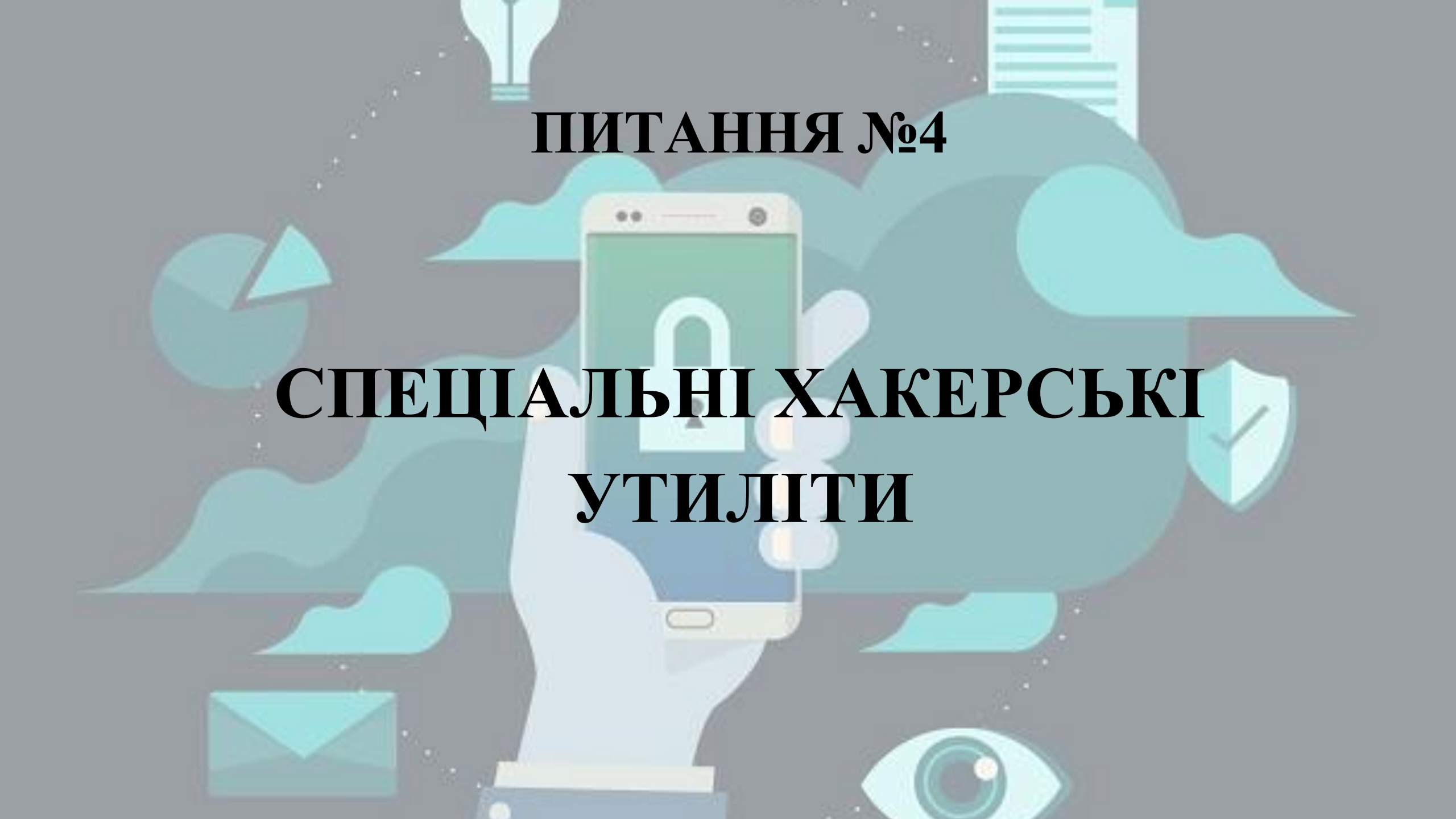
«ТРОЯНСЬКІ БОМБИ»

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.

«ТРОЯНСЬКІ БОМБИ»

Розглянемо різновид «троянців», які здійснюють блокування систем, – **«бомби в архівах» (ArcBomb)**. Це архіви, спеціально створені для того, щоб викликати нештатну поведінку архіваторів під час спроби розархівувати дані. Результатом може бути зависання або значне уповільнення роботи комп'ютера чи заповнення диска «порожніми» даними. «Архівні бомби» особливо небезпечні для файлових і поштових серверів, якщо вони підтримують будь-яку систему автоматичної обробки вхідної інформації, – «архівна бомба» може взагалі зупинити роботу сервера. На небезпеку наражаються також антивірусні програми, які автоматично розпаковують архіви для їх перевірки.

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.



ПИТАННЯ №4

СПЕЦІАЛЬНІ ХАКЕРСЬКІ УТИЛІТИ

СПЕЦІАЛЬНІ ХАКЕРСЬКІ УТИЛІТИ

Тепер розглянемо шкідливі засоби, які використовують цілком свідомо (питання про їхню шкідливість не має однозначної відповіді – все залежить від того, хто і з якою метою їх застосовує), ***хакерські утиліти***. Це програми, створені для того, щоб досліджувати системи чи програми та підготовлювати і здійснювати атаки.

Є також великий клас програм, що не належать до шкідливих і про які не можна сказати, що вони адресовані зловмисникам, але які також можуть порушувати політику безпеки будь-якої комп'ютерної системи. Це перш за все ***утиліти адміністрування системи***, які вже було згадано раніше. Крім того, до них можна віднести ***засоби розроблення і налагодження програм***, зокрема, ***налагоджувач*** (англ. – debugger) і ***дизасемблер*** (англ. – disassembler), без яких не може обійтися жодний тестувальник програмного коду. Є функціональні особливості, які роблять одні продукти привабливішими за інші. Але чи можна розмежувати звичайний і хакерський дизасемблери? Тому ці засоби ми тут не розглядатимемо, крім тих, що входять до єдиного пакета хакерських утиліт.

КЛАСИФІКАЦІЯ СПЕЦІАЛЬНИХ ХАКЕРСЬКИХ УТИЛІТ

Спеціальні хакерські утиліти можна класифікувати наступним чином:

1. ***Засоби здійснення віддалених атак:***

- проникнення на віддалені комп'ютери;
- засоби віддалених DoS- і DDoS-атак;
- фатальні мережні атаки;
- генератори «мережного сміття».

2. ***Засоби створення шкідливого програмного забезпечення:***

- конструктори вірусів і «троянських коней»;
- приховування від антивірусних програм;
- поліморфні генератори;
- конструктори атак (експлойтів).

ЗАСОБИ ПРОНИКНЕННЯ НА ВІДДАЛЕНІ КОМП'ЮТЕРИ

Ці засоби є інструментами безпосереднього здійснення атаки. У хакера немає часу вручну досліджувати віддалений комп'ютер і випробовувати ті чи інші методи зламу. Тому майже всі атаки здійснюються за допомогою спеціально написаних програм. Хоча для їх створення використовують різні мови програмування (навіть Visual Basic), найпопулярнішою серед сучасних хакерів є мова Perl. Будь-який засіб атаки називають ***інструментом зламу*** (англ. – hack tool). Засіб або модуль, який використовує певну вразливість атакованої системи, називають ***експлойтом*** (англ. – exploit).

ЗАСОБИ ПРОНИКНЕННЯ НА ВІДДАЛЕНІ КОМП'ЮТЕРИ

Також популярними є хакерські інструменти **rootkit**. Ця назва прийшла із системи UNIX, де її використовували для позначення набору інструментів, що застосовували для отримання прав суперкористувача root. До такого набору обов'язково входили засоби, що давали змогу впроваджувати люк і приховувати його присутність у системі. Сьогодні інструменти типу rootkit використовують і на інших ОС, переважно на Microsoft Windows, а значення терміну «rootkit» суттєво змінилося. Тепер цю назву використовують для програмного коду або технології, спрямованої на приховування присутності в системі заданих об'єктів (процесів, файлів, ключів реєстру тощо).

ЗАСОБИ ВІДДАЛЕНИХ DOS- І DDOS-АТАК

Програми цього типу реалізують атаки на віддалені сервери. Одним зі шляхів здійснення атаки на відмову в обслуговуванні (Denial of Service, DoS) є організація так званих ***штормів*** (англ. – flooding) або міні-штормів запитів. Шторм запитів полягає в тому, що на сервер надсилають так багато запитів, скільки можуть дозволити ресурси зловмисника. Мета буде досягнута за умови, якщо ресурси зловмисника і пропускна здатність каналів зв'язку перевищують можливості сервера, який атакують, тобто сервер не встигає обробляти всі запити, що надходять. Міні-шторм запитів, по-перше, спрямований на конкретний сервіс (порт), а по-друге, передбачає формування спеціальних запитів (наприклад, напіввідкритих TCP-з'єднань), які, незважаючи на їхню порівняно невелику кількість, можуть зупинити атакований сервіс (наприклад, через переповнення черги запитів у буфері).

ЗАСОБИ ВІДДАЛЕНИХ DOS- І DDOS-АТАК

Завдяки засобам протидії атакам можна легко виявити DoS-атаку через надзвичайно велику кількість запитів або через відому їм «шкідливу» форму запитів, що надходять з одного вузла. DDoS-атаку (Distributed DoS) можна реалізувати з кількох (багатьох) комп'ютерів одночасно, тому з точки зору системи виявлення атак це виглядає не як атака, а як надзвичайно підвищена активність у мережі. Але ресурси всіх комп'ютерів, задіяних у такій атаці, разом гарантовано значно перевищують ресурси будь-якого сервера, тому DDoS-атака має великі шанси на успіх. Це було підтверджено успішними DDoS-атаками на сайт президента США у 2001 році (організатор – **мережний хробак CodeRed**), а також атаками на сайт компанії SCO у 2004 році (організатор – **мережний хробак Mydoom.A**).

ЗАСОБИ ВІДДАЛЕНИХ DOS- І DDOS-АТАК

DoS-програми реалізують атаку з одного комп'ютера з відома користувача. ***DDoS-програми*** реалізують розподілені атаки з багатьох комп'ютерів часто без відома користувачів (там працюють програмні закладки), але, як правило, з відома, а можливо, й під керівництвом розробника програми.

Як дивно б це не звучало, але засоби DoS-атак можуть (і мусять!) входити не лише до інструментів зловмисників, але й до інструментів системних адміністраторів – для перевірки стійкості мережі та виявлення слабких місць у захисті.

ФАТАЛЬНІ МЕРЕЖНІ АТАКИ

Такі мережні атаки здійснюють засоби, які дістали назву ***нюкер*** (Nuke – ядерна зброя). Утиліти надсилають спеціально оформлені мережні запити на віддалені комп'ютери. Ці запити, використовуючи вразливості в ОС і прикладних програмах, викликають критичну помилку, внаслідок чого система, яку атакують, припиняє роботу. Нюкери відрізняються від експлойтів тим, що їх застосування викликає аварійне завершення роботи віддаленого комп'ютера або його перезавантаження, тоді як застосування експлойта спричиняє проникнення на віддалений комп'ютер, тобто надає можливість виконати на ньому довільну команду.

ГЕНЕРАТОРИ МЕРЕЖНОГО СМІТТЯ

Ще один різновид програм, призначених для порушення роботи систем комунікації, – ***генератори мережного сміття*** (Flooder). Ці утиліти використовують для заповнення непотрібними повідомленнями каналів Інтернету (IRC-каналів, комп'ютерних мереж, електронної пошти тощо). Ці атаки можуть призвести до недоступності системи або сервісу, що їх викликали.

ГЕНЕРАТОРИ МЕРЕЖНОГО СМІТТЯ

Ось кілька основних видів флудерів:

- ***Синтаксичний флуд (Syntax Flooding):*** В цьому виді атаки зловмисники надсилають запити, які не відповідають синтаксичним правилам для обробки. Наприклад, вони можуть надсилати запити, що містять невірні команди або параметри.
- ***Ping флуд (Ping Flooding):*** Ця атака використовує ICMP (Internet Control Message Protocol) пакети для надсилання великої кількості "ping" запитів до сервера або мережі. Це може перевантажити мережу і призвести до зниження її продуктивності.
- ***UDP флуд (UDP Flooding):*** Зловмисники надсилають велику кількість UDP-пакетів на цільовий сервер чи мережу. UDP (User Datagram Protocol) не вимагає встановлення з'єднання, і він може легко бути використаний для атак на перевантаження.
- ***HTTP флуд (HTTP Flooding):*** У цьому виді атаки зловмисники надсилають велику кількість HTTP запитів до веб-сервера. Це може призвести до перевантаження сервера та зниження доступності веб-сайту.
- ***SYN-флуд (SYN Flooding):*** SYN-флуд використовується для атак на TCP/IP з'єднання. Зловмисники надсилають велику кількість SYN-пакетів, але не завершують їх. Це може перевантажити сервер і призвести до відмови в обслуговуванні.
- ***ICMP флуд (ICMP Flooding):*** У цьому виді атаки зловмисники надсилають велику кількість ICMP-пакетів, таких як "ping" або "echo" запити, для перевантаження мережі чи сервера.

ЗАСОБИ СТВОРЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Утиліти, призначені для полегшення написання комп'ютерних вірусів і для їх вивчення із зловмисною метою (дають змогу розібратися, як вірус працює, і зробити свій – кращий), дістали назву ***VirTool***.

Є спеціальні **утиліти-конструктори**, за допомогою яких із заготовлених блоків (із заданих функцій) можна складати нові комп'ютерні віруси і «троянців». Відомі конструктори вірусів для DOS і Windows і такі, що допомагають створювати макровіруси. За допомогою таких конструкторів можна згенерувати вихідні тексти вірусів, об'єктні модулі та безпосередньо заражені файли.

ЗАСОБИ СТВОРЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Деякі конструктори мають віконний інтерфейс, в якому за допомогою меню можна обрати: тип вірусу та тип об'єктів, які цей вірус намагатиметься вразити; протидію налагодженню; наявність поліморфізму; внутрішні текстові рядки; ефекти, що супроводжуватимуть роботу вірусу тощо. Інші конструктори не мають такого інтерфейсу і зчитують інформацію про тип вірусу з конфігураційного файлу.

Є також **утиліти, які забезпечують реалізацію окремих функцій вірусів.** Наприклад, програми, що використовують для шифрування інших шкідливих програм, щоб приховати їхній вміст від антивірусної перевірки (FileCryptor або PoIy-Cryptor). Є ще **поліморфні генератори** (PolyEngine), основна функція яких – шифрування тіла вірусу іта генерування відповідного розшифрувальника.

СТВОРЕННЯ ЗАСОБІВ АТАК

Останнім часом спостерігається тенденція розвитку систем, призначених для спрощення та прискорення процесу розроблення експлойтів і середовищ їх тестування та моделювання. Поява таких систем привела до значного скорочення часу між випуском повідомлення про вразливість і появою відповідного експлойта. Розглянемо одну з таких систем – **Metasploit Framework (MSF)**. Ця система з відкритим вихідним кодом являє собою середовище для створення, тестування і використання експлойтів, що дає змогу тестувати системи на проникнення, розробляти shell-код і досліджувати вразливості.

ПИТАННЯ №5

ЗАХОДИ ЩОДО ЗАХИСТУ ТА ПРОТИДІЇ

МОНІТОРИНГОВІ ПРОГРАМНІ ПРОДУКТИ

Моніторингові програмні продукти – це програмні продукти (модулі), призначені для забезпечення спостережуваності обчислювальних систем, а також такі, що дозволяють фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів – з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

МОНІТОРИНГОВІ ПРОГРАМНІ ПРОДУКТИ

Види інформації, які можуть контролюватися:

1. ***Контроль подій:***

- натиснення клавіш на клавіатурі;
- натиснення клавіш миші;
- Logon та Logoff користувача;
- ім'я поточного користувача.

2. ***Скріншоти екрану:***

- десктоп (desktop capturing);
- активне вікно (active windows capturing);
- розрізання скріншоту і склеювання в пам’яті;
- скріншот навколо місця кліків клавіш миші.

3. ***Email:***

- вихідна пошта;
- вхідна пошта;
- двосторонній контроль web-пошти.

МОНІТОРИНГОВІ ПРОГРАМНІ ПРОДУКТИ

Види інформації, які можуть контролюватися(продовження):

4. ***Час і дата:***
- завантаження системи і ім'я поточного користувача;
- прикладних програм, що запускаються;
- перемикання між завданнями.

5. ***Буфер обміну:***
- вміст.

6. ***Інтернет:***
- URL.

7. ***Тексти, що набирають:***
- графічні вікна;
- консольні вікна.

8. ***Активність:***
- файлова;
- системного реєстру.

МОНІТОРИНГОВІ ПРОГРАМНІ ПРОДУКТИ

Види інформації, які можуть контролюватися(продовження):

9. Черга завдань:

- принтер.

10. Перехват певних файлів:

- по назві;
- по розширенню;
- по ключовому слову.

11. Меседжери:

- двосторонній контроль ICQ, IRC, AIM і т.д.

12. Віддалене адміністрування.

13. Відео інформація.

14. Аудіо інформація.

МОНІТОРИНГОВІ ПРОГРАМНІ ПРОДУКТИ

Види інформації, які можуть контролюватися(продовження):

15. ***За місцем зберігання Log-файлу:***

- твердий диск;
- пам’ять;
- реєстр;
- розшарений, тобто загальнодоступний (shared) мережевий диск;
- сервер в мережі Internet.

16. ***За методом відправки Log-файлу:***

- e-mail;
- ftp;
- http (https);
- будь-який варіант бездротового зв'язку (радіодіапазон, інфрачервоний діапазон, Bluetooth, Wifi і тому подібне).

17. ***За методом застосування:***

- санкціоноване застосування;
- несанкціоноване застосування;

18. ***За наявністю сигнатури в базах:***

- відомі моніторингові програмні продукти;
- невідомі моніторингові програмні продукти.

НЕСАНКЦІОНОВАНЕ ЗАСТОСУВАННЯ

Тільки **метод застосування моніторингових програмних продуктів дозволяє побачити грань між керування безпекою і порушенням безпеки**.

Несанкціоноване застосування – встановлення моніторингових програмних продуктів відбувається без відома власника (адміністратора безпеки) автоматизованої системи або без відома власника конкретного персонального комп'ютера. Несанкціоновано вживані моніторингові програмні продукти називаються **шпигунськими програмними продуктами**. Несанкціоноване застосування, як правило, пов'язане з незаконною діяльністю (illegal activity). Як правило, несанкціоновано встановлені шпигунські програмні продукти мають можливість конфігурації і отримання «скомплектованого» виконуваного файлу, який при інсталяції не виводить ніяких повідомлень і не створює вікон на екрані; такі продукти також мають вбудовані засоби доставки і дистанційного встановлення зконфігурованого модуля на комп'ютер користувача, тобто процес інсталяції не потребує безпосереднього фізичного доступу до комп'ютера користувача і часто не вимагає наявності прав адміністратора системи.

САНКЦІОНОВАНЕ ЗАСТОСУВАННЯ

Санкціоноване застосування – встановлення моніторингових програмних продуктів відбувається з відома власника (адміністратора безпеки) автоматизованої системи або з відома власника конкретного персонального комп'ютера. Моніторингові програмні продукти, що вживаються санкціоновано (англ. employee monitoring software, parental control software, access control software, personnel security programs) зазвичай вимагають або фізичного доступу до комп'ютера користувача, або обов'язкової наявності прав адміністратора системи для конфігурації і інсталяції цих програм.

ВІДОМІ МОНІТОРИНГОВІ ПРОГРАМНІ ПРОДУКТИ

Відомі моніторингові програмні продукти. До даної категорії відносяться моніторингові програмні продукти, сигнатура яких (на будь-якій підставі) включена до сигнатурних баз відомих фірм-виробників анти-шпигунських основни продуктів і/або антивірусних програмних х програмних продуктів.

НЕВІДОМІ МОНІТОРИНГОВІ ПРОГРАМНІ ПРОДУКТИ

Невідомі мотіторингові програмні продукти. До даної категорії відносяться моніторингові програмні продукти, сигнатура яких не включена до сигнатурних баз основних відомих фірм-виробників анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів і, ймовірно, **ніколи не буде в них включена з різних причин, а саме:**

- ***моніторингові програмні продукти (модулі), що розробляються під егідою різних урядових організацій***;
- ***шпигунські програмні продукти, які розроблені в обмеженій кількості*** (часто тільки в одній або декількох копіях) ***для вирішення конкретного завдання, пов'язаного з викраданням критичної інформації з комп'ютера користувача*** (наприклад, програмні продукти, що вживаються зловмисниками-професіоналами). Дані програмні продукти можуть бути трохи видозміненими відкритими початковими кодами моніторингових програмних продуктів, що взяті з мережі Інтернет та скомпільовані самим зловмисником, що дозволяє змінити сигнатуру моніторингового програмного продукту;

НЕВІДОМІ МОНІТОРИНГОВІ ПРОГРАМНІ ПРОДУКТИ

- ***комерційні моніторингові програмні продукти, які дуже рідко вносяться до сигнатурних баз відомих фірм-виробників анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів.*** Це призводить до того, що публікація зловмисниками в мережі Інтернет повнофункціональної версії даного комерційного моніторингового програмного продукту може перетворити останній на шпигунський програмний продукт, який не виявляється анти-шпигунськими програмними продуктами і/або антивірусними програмними продуктами;
- ***шпигунські програмні продукти, що включаються до складу програм-вірусів.*** До моменту внесення сигнатурних даних до вірусної бази ці шпигунські програмні продукти є невідомими. Приклад – всесвітньо відомі віруси, що натворили багато бід в останні роки, мають в своєму складі модуль перехоплення натискань клавіш клавіатури і відправки отриманої інформації в мережу Інтернет.

ЗАПОБІЖНІ ЗАХОДИ ЗАХИСТУ ВІД ВІРУСНИХ АТАК

Щоб захистити себе від нападів хакерів через віруси, необов'язково встановлювати на комп'ютері купу спеціальних захисних програм. Досить дотримуватися **запобіжних заходів в мережі**, тоді жоден шкідливий файл не потрапить на пристрій:

- Якщо на електронну пошту прийшло важливе повідомлення з вкладенням, не варто поспішати його відкривати. Спочатку необхідно зберегти вкладення на диск, а потім запустити його, використовуючи будь-який браузер. Можливо, замість текстового документа або фотографії на комп'ютер надійшов виконуваний файл.
- Ні в якому разі не можна запускати будь-яку програму, яка надійшла на електронну пошту з незнайомої адреси. Швидше за все, на пристрій прийшов хакерський файл.

ЗАПОБІЖНІ ЗАХОДИ ЗАХИСТУ ВІД ВІРУСНИХ АТАК

- Навіть якщо вкладення прийшло з уже знайомого e-mail, не варто поспішати його відкривати. Перш за все, необхідно просканувати його антивірусом. Не виключено, що електронна адреса, з якої надійшов лист, вже заражений шкідливим ПЗ і тепер просто відправляє розсилку по всіх збережених контактів.
- Ознакою того, що в надісланому вкладенні буде вірус, може послужити будь-яка сенсаційна новина в повідомленні. Це просто приманка для того, щоб користувач зацікавився вмістом і з цікавості відкрив заражений файл.

ЦІЛІ(НАПРЯМКИ) ЗАСТОСУВАННЯ ЗАХОДІВ ЗАХИСТУ ВІД ШКІДЛИВОГО ПЗ

Санкціоноване застосування моніторингових програмних продуктів дозволяє власникові (адміністраторові безпеки) автоматизованої системи:

- визначити (локалізувати) всі випадки спроб несанкціонованого доступу до конфіденційної інформації з точним визначенням часу і мережевого робочого місця, з якого така спроба здійснювалася;
- локалізувати всі випадки спотворення (знищення) інформації;
- визначити факти несанкціонованого встановлення програмного забезпечення;
- проконтролювати можливість використання персональних комп'ютерів в неробочий час і виявити мету такого використання;
- визначити всі випадки несанкціонованого використання модемів в локальній мережі шляхом аналізу фактів запуску несанкціоновано встановлених спеціалізованих прикладних програм;
- визначити всі випадки набору на клавіатурі критичних слів і словосполучень, підготовки будь-яких критичних документів, передача яких третім особам призведе до матеріального збитку;

ЦІЛІ(НАПРЯМКИ) ЗАСТОСУВАННЯ ЗАХОДІВ ЗАХИСТУ ВІД ШКІДЛИВОГО ПЗ

Санкціоноване застосування моніторингових програмних продуктів дозволяє власникові (адміністраторові безпеки) автоматизованої системи(продовження):

- визначити факти нецільового використання персональних комп'ютерів;
- отримати достовірну інформацію, на підставі якої розроблятиметься політика інформаційної безпеки підприємства;
- контролювати доступ до серверів та персональних комп'ютерів;
- проводити інформаційний аудит;
- проводити дослідження комп'ютерних інцидентів;
- проводити наукові дослідження, пов'язані з визначенням точності, оперативності і адекватності реагування персоналу на зовнішні дії;
- визначити завантаження комп'ютерних робочих місць;
- визначити завантаження персоналу підприємства;
- відновити критичну інформацію після збоїв комп'ютерних систем;
- забезпечити спостережуваність обчислювальної системи. Саме ця властивість, залежно від якості її реалізації, дозволяє в тій або іншій мірі контролювати дотримання співробітниками підприємства встановлених правил безпечної роботи на комп'ютерах і політики безпеки.

ЦІЛІ(НАПРЯМКИ) ЗАСТОСУВАННЯ ЗАХОДІВ ЗАХИСТУ ВІД ШКІДЛИВОГО ПЗ

Санкціоноване застосування моніторингових програмних продуктів дозволяє батькам:

- контролювати контакти неповнолітніх дітей в мережі Інтернет;
- протидіяти негативній дії на неповнолітніх дітей спеціалізованих сайтів, які показують дитячу порнографію або інші незаконні сексуальні дії (збочення), пропагують насильство, пропагують дискримінацію за ознакою раси, статі, релігійних переконань, національності, інвалідності, сексуальної орієнтації, зросту, пропагують протизаконні дії, порушують права інтелектуальної власності, порушують закони країни розміщення сайту або будь-які інші закони.

Несанкціоноване застосування моніторингових програмних продуктів дозволяє зловмисникові:

- дістати практично повний доступ до комп'ютера та інформації, що зберігається на ньому.

МЕТОДИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНО ВСТАНОВЛЕНИХ МОНІТОРИНГОВИХ ПРОГРАМНИХ ПРОДУКТІВ

Захист від «відомих» несанкціоновано встановлених моніторингових програмних продуктів включає в себе:

- використання анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів відомих виробників, з автоматичним оновленням сигнатурних баз.

Захист від «невідомих» несанкціоновано встановлених моніторингових програмних продуктів включає в себе:

- використання анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів відомих виробників, які для протидії шпигунським програмним продуктам використовують так звані евристичні (поведінкові) аналізатори, тобто не вимагають сигнатурної бази.

МЕТОДИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНО ВСТАНОВЛЕНИХ МОНІТОРИНГОВИХ ПРОГРАМНИХ ПРОДУКТІВ

Захист від «відомих» і «невідомих» несанкціоновано встановлених моніторингових програмних продуктів включає використання анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів відомих виробників, які для протидії шпигунським програмним продуктам використовують:

- сигнатурні бази шпигунських програмних продуктів, що постійно оновлюються;
- евристичні (поведінкові) аналізатори, що не вимагають наявності сигнатурної бази.

ЗАХОДИ ЗАХИСТУ ВІД ШПИГУНСЬКОГО ПЗ

Отже, серед заходів захисту від шпигунського програмного забезпечення можна виділити наступні:

- ***Встановлення надійного антивірусного та антишпигунського програмного забезпечення:*** Використовуйте довірені антивірусні та антишпигунські програми, які регулярно оновлюються. Вони допоможуть виявляти і видаляти шпигунське програмне забезпечення.
- ***Регулярні оновлення програмного забезпечення:*** Регулярно оновлюйте операційну систему, браузери, антивірусне програмне забезпечення та інші програми. Багато шпигунських програм використовують вразливості у застарілих версіях програм для вторгнення в систему.
- ***Обережність при завантаженні:*** Уникайте завантаження програм або файлів з ненадійних джерел. Використовуйте лише офіційні магазини додатків для мобільних пристроїв і джерела програм для комп'ютерів.
- ***Перевірка дозволів:*** Перевіряйте, які дозволи запитує програма перед її встановленням. Надайте лише необхідні дозволи і відмовте в доступі до особистої інформації, якщо це необхідно.

ЗАХОДИ ЗАХИСТУ ВІД ШПИГУНСЬКОГО ПЗ

Отже, серед заходів захисту від шпигунського програмного забезпечення можна виділити наступні(продовження):

- ***Використання антифішингових інструментів:*** Використовуйте антифішингові інструменти в браузерах та антивірусних програмах, які допомагають виявляти інтернет-сайти та повідомлення, які намагаються вас обманути.
- ***Захист електронної пошти:*** Будьте обережні з електронною поштою. Уникайте відкриття вкладень та переходів на посилання в сумнівних повідомленнях.
- ***Використання VPN:*** Використовуйте віртуальні приватні мережі (VPN), щоб шифрувати ваш інтернет-трафік і захищати свою приватність в мережі.
- ***Моніторинг активності:*** Регулярно перевіряйте активність вашого антивірусного програмного забезпечення та виявляйте підозрілі процеси або додатки.
- ***Безпечні паролі:*** Використовуйте сильні та унікальні паролі для різних облікових записів. Парольний менеджер може допомогти вам в керуванні паролями.
- ***Свідомість користувача:*** Постійно підвищуйте свідомість про потенційні загрози та вчіться розпізнавати підозрілі ситуації в інтернеті.

ДЯКУЮ ЗА УВАГУ!