Počítačové vírusy

Informatika

OBSAH

Počítačové vírusy

I. Čo je to vírus ?

Vírus je program, ktorý môže nainfikovať iný program a spôsobiť tak problémy v systéme.

Pripájajú sa na iné programy a zneužívajú ich na ďalšie šírenie v počítači.

Niektoré vírusy nepotrebujú ani hostiteľský program, sú sami o sebe deštrukčné.

Počítačové vírusy

2. Rozdelenie vírusov

1. Podľa umiestnenie v pamäti
   1. Rezidentné
   2. Nerezidetné
2. Podľa cieľa infekcie
   1. Bootovacie
   2. Súborové
3. Podľa spôsobu infekcie
   1. Predlžujúce
   2. Prepisujúce
   3. Adresárové
   4. kombinované
4. Podľa funkcie
   1. Deštruktívne
   2. Nedeštruktívne
5. Podľa správania a možnosti detekcie
   1. Polymorfné
   2. Stealth
   3. Tunelujúce

Počítačové vírusy

2. Rozdelenie vírusov

Rezidentné – po spustení napadnutého súboru sa natrvalo usadia v operačnej pamäti PC, napadnuty program sleduje činnosť užívateľa a keď spustí ešte nenakazený súbor tak ho infikuje.

Nerezidentné- spôsobia nákazu len po spustení napadnutého súboru aj to spravidla v danom adresáry.

Bootovacie – sú umiestnené v systémovej oblasti disku, aktivuje sa po štarte systému. Potom napáda aj ostatné prídavné disky.

Súborový – pripája sa alebo prepisuje spustiteľné súbory (com, exe, bat, bin). Ak spustíme napadnutý program ten napadne aj ostatné a vykonáva záškodnícku činnosť.

Počítačové vírusy

2. Rozdelenie vírusov

Polymorfné – modifikujú sami svoj kód a ďalej sa šíria

Adresárové - *adresárové vírusy* infikujú spustiteľné programy, a to tak, že zmenia nie kód programu, ale jeho ukazovateľ v adresárovej položke disku

Stealth- dokážu sa ukryť pre antivírusmi

Tunelujúce – dokážu oklamať bezpečnostné prvky BIOSu a získajú tak kontrolu nad hardvérom

Deštruktívne – prepisujú náhodne vybraté sektory a formatujú pevný disk

Nedeštruktívne – ich aktivita sa prejaví vizuálne napr. zobrazovanie textových správ.

Počítačové vírusy

3. Typy vírusov a ich popis

Trójsky kôň

Navonok pôsobí neškodne a dáva dojem, že je užitočný. Na pozadí programu však vykonáva určitý druh deštrukcie údajov. Nereprodukujú sa a sú málo rozšírené. Vystupuje pod spustiteľným súborom exe, a neobsahuje nič len telo trojského koňa. Neparazituje na žiadnom programe a dá sa odstrániť len zmazaním dotyčného súboru.

Trojan Telefoon, ktorý sa vydával za komprimačný program RAR 3.0 alebo trójsky kôň vydávajúci sa za užitočný antivírusový program McAfee VirusScan, v skutočnosti likvidujúci súbory na pevnom disku

Počítačové vírusy

3. Typy vírusov a ich popis

Backdoory

Formou sa podobajú trójskym koňom. Poskytujú informácie prostredníctvom internetu. Tento vírus môže ovládať váš počítač, kradnúť dáta alebo ich modifikovať. Predovšetkým ide o neautorizovaný vstup do PC. Ide napríklad o komerčné produkty ako PC AnyWhere, VNC, Remote Administrator, ktoré fungujú na báze klient – server.

Bakdoor IRC, ktoré komunikujú s útočníkom cez kanál v sieti IRC (vírus Anarxy,). Vhodnou a účinou obranou sú firewally. Vírusy sú schopné sa šíriť aj po sieťovo zdielaných diskoch.

Počítačové vírusy

3. Typy vírusov a ich popis

Email HOAX

Ide o email, ktorý obsahuje poplašnú správu alebo inštrukcie ako odstrániť fiktívny vír, pričom užívateľ znemožní napr. opätovné spustenie PC. Užívatelia tieto emaily rozposielajú vzájomne v domienke dobrého úmyslu. Zahlcujú internet.

Od septembra má ICQ stáť 50 centov! Postav sa proti tomu a pošli tento text aspoň 15 ľudom z tvojich kontaktov. Keď si to urobil/a tak stlač F1 a tvoja kvetinka bude modrá. To znamená, že nemusíš nič platiť. Takto pomôž že icq bude ešte stále zadarmo! To nie je žiaden vtip!!!

Počítačové vírusy

3. Typy vírusov a ich popis

Žartovný program JOKE

Je určený skôr pre pobavenie ako na záškodnú činnosť. Pôsobí ako vírus, teda navodzuje napríklad deštrukciu ale v skutočnosti je úplne neškodný a nijako sa nereprodukuje.

Počítačové vírusy

3. Typy vírusov a ich popis

Červy WORMS

Sú najrozšírenejšie vírusy. Šíria sa najmä internetom ako príloha v e-maily. E-maily sú automaticky generované a pod vašim menom rozoslané tým, ktorých mailové adresy máte v PC. Samotný červ má aj sekundárnu činnosť ako napr. padanie systému, odstraňovanie súborov, šifrovanie a kryptovanie súborov, ktoré budú opäť dostupné po zaplatení poplatku, prehľadávanie PC za účelom získania osobných údajov, využitie ako cestu k ďalšiemu infikovaniu súborov.

Počítačové vírusy

3. Typy vírusov a ich popis

ADWARE

Sú to programy, ktoré sťahujú automaticky reklamy, propagačné materiály v PC bez vedomia užívateľa. Príznakom sú vyskakujúce okna pop-up. Nebezpečenstvo spočíva v tom, že integrované reklamné systémy sú často Spywarom.

Počítačové vírusy

Informatika

3. Typy vírusov a ich popis

SPYWARE

Program, ktorý využíva internet na posielanie rozličných údajov o používateľovi bez jeho vedomia inému užívateľovi. Informáciu môžu byť napríklad zoznam e-mailových adries, najčastejšie navštevovaných stránok, keylogery, ktoré zaznamenávajú všetky stlačené klávesy. Takto sa dajú získať prístupové heslá do systému, kreditných kariet, registračné kľúče. Spywarom môžu byť aj programy, ktoré sa vydávajú za odstraňovače Spywaru.

Malware wipe, Pest Trap, SpyAxe, AntiVirus Gold, SpywareStrike, WinFixer, SpySheriff, AlfaCleaner, Spyware Stromer,, Spy Wiper

Počítačové vírusy

4. Čo spôsobujú vírusy ?

- Nezvyčajné správanie sa programu
- Zmena veľkosti alebo obsahu súborov
- Poškodenie dokumentov
- Chybové hlásenia počas behu programov
- Spomalenie a nestabilitu systému
- Napádajú a ničia spustiteľné systémové súbory
- Ničia údaje z databáz, textových súborov
- Môžu zablokovať, prekódovať, naformátovať disk
- Modifikujú údaje bez iných vedľajších príznakov
- Ničia hardvér počítača

Počítačové vírusy

4. Funkcie vírusov

- Rozmnožovanie
- Škodenie
- Maskovanie
- Prežitie
- Spomalenie a nestabilita systému

Počítačové vírusy

6. Ako sa chrániť pred vírusmi (prevencia)

1. **Inteligencia** môžeme uplatniť najmä v prichádzajúcich e-mailoch. Koho by potom napadlo spustiť prílohu e-mailu, ktorý je napríklad napísaný po anglicky, a nevieme od koho prichádza. Alebo tiež kliknúť na odkaz e-mailu, u ktorého tiež nevieme od koho pochádza.

2. **Informovanosť** Ide tu najmä o sledovanie webových stránok antivírových spoločností, ktorých produkty užívateľ vlastní, to by malo byť na dennom poriadku, tak isto sledovanie nezávislých stránok a článkov čo sa týkajú tematiky škodlivých kódov.

3. **Zodpovednosť** Ide tu hlavne o zodpovednosť používateľa počítača pri vkladaní svojich CD alebo DVD nosičov a USB-čiek do iných cudzích počítačov alebo vkladaní si cudzích nosičov do svojho počítača.. Pretože ak sa v danom cudzom počítači nachádza infiltrácia možno ju ľahko preniesť do svojho a tým si zavíriť celý systém. Zodpovednosť úzko súvisí s inteligenciou a informovanosťou. Pretože len inteligentný a dobre informovaný užívateľ vie ako správne a zodpovedne narábať so svojimi CD, DVD a USB. A to hlavne v dnešnej dobe, v ktorej asi na každom kroku nájdeme nejaký druh počítačovej infiltrácie.

4. **Aktuálne verzie softvéru** Pripadnú infekciu počítača môžeme významne obmedziť pravidelným sťahovaním aktuálnych verzií software (hlavne sťahovanie aktualizácií pre antivírusové systémy) a to bez ohľadu na to o akú platformu ide. Nás zaujíma hlavne Microsoft Windows, kde okrem aktualizácií pre samotný systém existujú aj veľmi dôležité aktualizácie pre aplikáciu Internet Explorer. Šírenie veľa vírusov prostredníctvom aplikácie Microsoft Internet Explorer, by sa dalo obmedziť v prípade, že by takú aktualizáciu vykonával pravidelne každý užívateľ. Realita je však iná.

Počítačové vírusy

7. Antivírová ochrana

Antivírusový softvér

NOD 32, Norton Antivirus, AVAST, AVG Antivirus, Panda Antivirus, Mcafee, Avira Antivir,

Antispywarový softvér

Spyware Doctor, Spyware Terminator, Ad – Aware, Spybot Search and Destroy, HijackThis

Počítačové vírusy

Ďakujem za pozornosť

Pripravil : Mgr. Miloš Hadbavný

miloshadbavny@azet.sk