Škodlivý kód, útok na aplikace

Ing. Miloslav Hub, Ph.D.

5. prosince 2007

Viry (1)

- Nejstarší forma škodlivého kódu.
- **Základní funkce:**
  - Šíření
  - Destrukce
- **Techniky šíření:**
  - Bootovací viry – z diskety
  - Souborové viry – ze souboru
  - Makroviry – v dokumentech Word, Excel, Lotus, AmiPro,..
- **Antivirové mechanismy**
  - Podle vzoru
  - Heuristiky

Viry (2)

- **Akce po nalezení viru:**
  - Vyléčení souboru
  - Virová karanténa
  - Smazání souboru
- **Techniky obrany virů před odhalením:**
  - Mnohostranné viry – útočí více způsoby
  - Skryté viry – skryjí se např. do operačního systému
  - Polymorfické viry – modifikují svůj vlastní kód
  - Šifrované viry – pokaždé jiný klíč, pokaždé vypadají jinak.

Viry (3)

- **Důvody tvorby virů:**
  - Pomsta programátora svému zaměstnavateli
  - Vytváří je mladí programátoři, kteří si chtějí vyzkoušet své schopnosti
  - Vytváří je (prý) programátoři antivirových firem
  - Vytvoření viru za účelem útoku (DoS, spam,…)

Hoax

- Nevyžádaná zpráva, která uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod.
- Většinou obsahuje i výzvu žádající další rozeslání, někdy se proto označuje také jako řetězový e-mail.
- **Druhy:**
  - Falešný poplach
  - Zábavné
  - Prosby
- **Důsledky:**
  - Obtěžování příjemců
  - Nebezpečné rady
  - Zbytečné zatěžování linek a serverů
  - Ztráta důvěryhodnosti
  - Prozrazení důvěrných informací

Logické bomby

- Škodlivý kód, který nakazí systém a je neaktivní, dokud nenastane nějaká událost nebo více podmínek, např.:
  - Datum a čas
  - Spuštění jiného programu
  - Otevření webové stránky
- Často vložené do programů samotnými autory, kteří vytvoří sebedestrukci software v případě, že jsou nečekaně propuštěni.

Trojské koně (1)

- Uživateli skrytá část programu nebo aplikace s funkcí, se kterou uživatel nesouhlasí (typicky je to činnost škodlivá).
- Může být také přidán do stávající aplikace.
- Rozdíl mezi počítačovým virem a trojským koněm je, že trojský kůň nedokáže sám infikovat další počítače nebo programy svojí kopií.
- Existují však počítačové červy, které na napadeném počítači instalují různé trojské koně nebo vytvářejí trojské koně z programů, které se v napadeném systému nacházejí.

Trojské koně (2)

- **Zadní vrátka** – síťová služba, kterou může útočník použít pro získání přístupu do systému přes počítačovou síť
- **Spam server** – rozesílání nevyžádané elektronické pošty
- **Souborový server** - nainstaluje souborový server - např. FTP,P2P
- **Security software disabler** - zablokuje software pro zabezpečení
- **Hijacker** - mění domovskou stránku
- **Denial-of-service** - účastní de DoS útoku
- **Dialer** - přesměrovává na dražší tarify
- **Adware** - obtěžují při práci na počítači reklamou
- **Spyware** - program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele (přehled navštívených stránek či nainstalovaných programů).
- **Sniffer** – odposlouchávání hesel, čísel kreditních karet
- **Keylogger** – sledování znaků zadávaných z klávesnice

Spyware

- Program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele.
- Může sledovat uživatele a jeho zvyklosti při surfování na Internetu a posílat o tom zprávy .
- Může zasílat informace o nainstalovaných programech.

Červi

- Červi se na rozdíl od virů šíří bez spolupráce člověka – v paketech, souborech.
- Nejčastěji se šíří e-mailem, kde využívají chyb e-mailových klientů.

Aktivní obsah

- Obsažen ve webových stránkách.
- Např. ActiveX, Java applety, Macromedia Flash.
- Současné prohlížeče umožňují zakázat aktivní obsah, nebo ho povolit jenom u důvěryhodných stránek.

Antivirové desatero

1. Provádějte pravidelný update svého antivirového programu.
2. Nikdy neotvírejte e-mailovou přílohu, kterou jste nepožadoval(a).
3. Mějte kontrolu nad svým počítačem a nad tím, kdo jej používá.
4. Instalujte včas všechny „záplaty“ na používaný software.
5. Vždy prověřujte diskety a CD média předtím, než je použijete.
6. S každým novým souborem (i z důvěryhodného zdroje) nakládejte s největší opatrností.
7. Využívejte více než jeden způsob antivirové ochrany.
8. Vytvořte si zaručeně „čistou“ bootovací disketu a pečlivě ji uložte na bezpečné místo.
9. Pravidelně zálohujte.
10. Nepodléhejte panice.