Malware

škodlivý obsah

Základní rozdělení Malware

- Počítačový vir
- Trojský kůň
- Backdoor
- Spyware
- Dialer
- Hoax
- Spam
- Počítačový červ (worm)

Počítačový vir

- program, který se připojuje k jiným programům a dále se z nich (bez vědomí uživatele) šíří
- kromě programů (EXE, COM, SYS, SCR) dochází k napadení dalších aktivních objektů
- systémové oblasti disku - boot [bůt] sektor, partition [partyšn] tabulka
- dokumenty s makry (skupny příkazů VB) - texty DOC, tabulky XLS, prezentace PPT, databáze MDB
- aktivní internetové moduly - Java applety, VB Scripty a JScripty obsažené na HTML stránkách
- napadené objekty nefungují vůbec nebo jen omezeně a dále podporují šíření viru
- postupně dochází k blokování OS a k narušení nebo mazání dat na disku
- v datových souborech (bez maker) se viry nešíří, např. obrázky BMP, JPG jsou bezpečné
- Zavirovat lze každý systém včetně Linuxu a mobilních telefonů

Trojský kůň

- jednoduchý program předstírající užitečnou činnost
- po spuštění vykoná jednorázově destrukční činnost, např. smaže soubory na HD, přepíše CMOS a pod
- nemá schopnost šíření a proto jej nelze řadit k počítačovým virům

Backdoor [bekdůr]

- program, který po spuštění umožní průnik viru nebo zpřístupní data po Internetu
- zdrojem jsou www stránky nabízející cokoliv nainstalovat do PC

Spyware [spajvér]

- špionážní program, který zasílá na určitou adresu citlivé informace
  - osobní
  - o nainstalovaných programech
  - o navštívených www stránkách
  - o zaslaných emailech
  - o přístpových heslech
- existuje celá řada aplikací, kterými lze sledovat, co uživatel dělá
- mívají i podobu tzv. Cookies - malých souborů
- automaticky a nevědomky se stahují s Internetu

Dialer [dajler]

- Kvůli charakteru připojení není dnes častý
- při prohlížení www stránek se může do počítače dostat škodlivý program
- po spuštění dialeru dojde k zablokování původního připojení a přesměrování na placenou linku

Spam

- zahlcuje poštovní schránku obtěžuje
- nevyžádaná reklamní pošta, každý den miliardy zpráv od několika málo uživatelů, např. nabídky levného softwaru, léků, sexuálních služeb apod.
- útoky na emailové servery - využívání seznamu jmen
- obrana - prevence a filtrování
- e-mail v bezpečné podobě na osobních a firemních stránkách

Hoax [houks]

- poplašná zpráva - e-mail upozorňující např na nový vir atd

Počítačový červ (worm)

- škodlivý kód, který se zapisuje do registrů Windows a mění zde důležité informace
- v poslední době nejčastější varianta napadení PC
- antivirový program worm detekuje, ale neumí provést léčení
- k odstranění wormů je nutno použít specializovaný remover a určitý postup

Prevence, ochrana

- samotný antivirový program je pro ochranu PC nedostatečný
- nutnost jej kombinovat s tzv. firewallem (zabraňuje průniku škodlivých kódů do PC)

Hackeři

- podrobné útoky jako viry

Kategorie hackerů:

1. nabourávají se do systému, aby získali nové vědomosti a zkušenosti s hackováním
2. snaží se být „in“ /obvykle děti/ Tzn. že shání programy na hackování a náhodně se kamsi hackují a nevědomě tím mohou napáchat i velkou škodu
3. jde jim o získání citlivých údajů, v podstatě špióni
4. zneužití počítače k nekalým aktivitám