Počítačové viry a ostatní škodlivé programové kódy

(vir, červ, malware, spyware, ransomware)

Škodlivé programy

- je program, který někdo vytvořil za účelem:
  - získání dat z vašeho počítače
  - získání kontroly na vaším počítačem
  - využití zdrojů počítače
  - zničení vaší práce na počítači
  - znepřístupnění počítače a dat za účelem vydírání
- vše je děláno ze snahy okrást majitele počítače o data, hesla, počítačové zdroje a v konečném důsledku o peníze

Počítačový virus

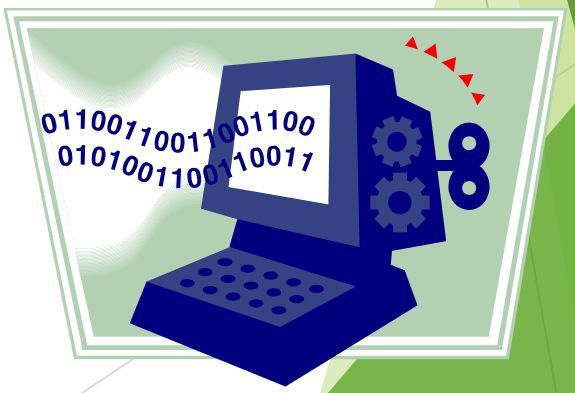
- **Virus:**
  - malý programový kód, který je vložen (infikuje) do spustitelného souboru (programu)
  - spuštěním infikovaného programu tedy nevědomky spustíme i virus, který napadne další programy
  - zavirovaný soubor léčíme
- **Makrovirus:**
  - virus, který není součástí nějakého programu, ale dokumentu, který může obsahovat makra – v dokumentu vložené programové kódy

Počítačový červ (Worm)

- **Červ:**
  - program, který má vlastní soubor a většinou se snaží přimět uživatele počítače, aby ho spustil, případně využívá bezpečnostní chybu a snaží se spustit sám
  - některé internetové červy využívají chyby v zabezpečení síťového připojení a šíří se přímo v paketech síťového protokolu
  - jsou velmi nebezpečné protože je nestačí zachytit antivirový program a ke svému spuštění nevyžadují aktivitu uživatele, obranou je firewall
  - červy neléčíme, ale mažeme

Rootkit

- **Rootkit:**
  - škodlivý kód, který běží v jádru operačního systému s právy administrátora počítače
  - špatně se detekuje a odstraňuje
  - protože je součástí jádra operačního systému, může se skrýt před běžným antivirovým programem



Malware a Spyware

- **Malware:**
  - shrnující označení pro škodlivé kódy
  - malicious – zákeřný
- **Spyware:**
  - program, který sleduje činnost uživatele a předává o ní někomu zprávy (špehuje)
  - prohledává obsah počítače a někoho o něm informuje
  - často se instaluje spolu s nějakým programem nebo pomocí aktivního obsahu webových stránek
- **Adware:**
  - sleduje aktivitu uživatele na Internetu a cíleně mu zobrazuje reklamu, nemusí to být škodlivý kód

Ransomware

- je druh malwaru, bránící přístupu k počítači, který je infikován
- některé formy ransomware šifrují soubory na pevném disku, jiné jen zamknou systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení (vyděračský software)

Činnost Malware

- Škodlivý kód, který přijde na váš počítač, ihned nemusíte poznat
- většinou se nějakou dobu jen šíří, případně infikuje další soubory v počítači, rozesílá se na emailové adresy uživatele
- teprve po určité době provede nějakou nepříjemnou činnost:
  - **ovládnutí počítače:**
    - program typu **backdoor** otevře některé porty počítače a naslouchá na nich povelům zvenčí
    - umožní tak získat útočníkovi přístup do počítače a pracovat s ním

Činnost Malware

- teprve po určité době provede nějakou nepříjemnou činnost:
  - **odcizení obsahu počítače:**
    - vzdálený útočník si může zkopírovat soubory napadeného počítače
    - může použít program typu **keylogger** ke sledování kláves (při vyplňování formulářů)
    - může použít program typu **dataminder**, který shromažďuje data o činnosti uživatele počítače

Činnost Malware

- teprve po určité době provede nějakou nepříjemnou činnost:
  - **využití počítače pro nelegální činnost:**
    - často se stane, že policie při zásahu proti rozesílatelům spamu nebo držitelům nelegálních souborů zasáhne u překvapeného majitele počítače, který o jeho nelegální funkci neměl tušení
    - vzdálený útočník přeměnil nezabezpečený počítač v server rozesílající spam nebo poskytující nelegální obsah

Metody útoku přes web a poštu

- 60% škodlivých kódů se dnes šíří přes internet
- autoři nakažených webů využívají širokou škálu technologií:
  - **umístění zavirovaného souboru** do jinak užitečného programu
    - obvykle na webech s nelegálním obsahem
    - uživatel si stáhne program, spustí ho a tím infikuje počítač
  - **umístění zavirovaného souboru** na zcela důvěryhodný web, který byl předtím napaden

Metody útoku přes web a poštu

- pokračování:
  - **umístění skriptu (programu)** do kódu webové stránky
    - pokud prohlížeč tento kód spustí, nahraje do OS škodlivý kód
    - prohlížeče ale obsahují zabudované ochrany, takže se to většinou podaří jen s využitím bezpečnostní chyby
    - rozšířeným útokem je nabídka falešné antivirové kontroly počítače – webová stránka upozorní na nalezení viru v počítači a nabídne jeho odstranění, stačí pouze spustit nabízený „antivir…“ uživatel tím odmítne bezpečnostní varování prohlížeče a vir spustí

Metody útoku přes web a poštu

- autoři nakažených webů využívají širokou škálu technologií:
  - **vytvoření zavirovaného doplňku** (plug-inu) pro webový prohlížeč
    - uživatel si s doplňkem nainstaluje i škodlivý kód
  - **vytvoření podvržené stránky**
    - uživatel je přesměrován na falešnou stránku, napodobující originál (bankovní web), kde vyplní své přihlašovací údaje a tím je poskytne útočníkovi
  - **další způsoby** propašování viru do systému se stále vyvíjejí, je proto důležité sledovat odborné weby: www.viry.cz, www.zive.cz, www.lupa.cz, www.root.cz

Útoky přes elektronickou poštu

- v minulosti fungovala elektronická pošta jako hlavní nosič virů
- typickým je e-mailová zpráva s přílohou, ve které je umístěn Malware
- většina e-mailových serverů má dnes integrovaný antivirový program
- zavirované zprávy jsou většinou odstraněny dříve, než si je stáhnete na počítač
- útočníci proto používají zprávy s odkazem na zavirované webové stránky

Cvičení

- Zjistěte aktuální statistiky rozšíření Malware a počty nakažených počítačů
- Najděte hodnocení bezpečnosti současných operačních systémů pro osobní počítače
- Proč se většina Malware zaměřuje na systémy Microsoft Windows?
- Je váš mobilní telefon, televize imunní proti útoku škodlivých kódů?