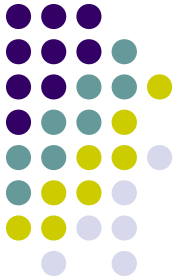
OP Vzdělávání
pro konkurenceschopnost

INVESTICE
DO ROZVOJE
VZDĚLÁVÁNÍ



Střední průmyslová škola a Vyšší odborná škola technická Brno, Sokolská 1

Šablona: Inovace a zkvalitnění výuky prostřednictvím ICT

Název: Základy výpočetní techniky

Téma: Počítačové viry

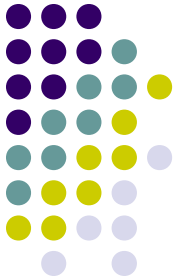
Autor: Ing. Jakab Barnabáš

Číslo: VY_32_INOVACE_28–18

Anotace: *Materiál uvádí základní rozdělení počítačových virů.*
Je určen pro žáky 1. ročníku oboru strojírenství.
Vytvořeno: prosinec 2013

Podpora digitalizace a využití ICT na SPŠ CZ.1.07/1.5.00/34.0632

Počítačové viry



- **Počítačový virus** je spustitelný nebo interpretovaný program, který je schopen sám sebe připojovat k jiným programům a dále se z nich šířit.
- Skutečným počátkem existence počítačových virů je rok 1986, kdy se narodil **Brain** – první virus pro osobní počítače PC.

Projevy zavirovaných počítačů

- Blokování místa
- Zpomalení práce systému
- Nestabilita systému
- Grafické a zvukové projevy
- Krádež dat
- Šifrování dat
- Zničení dat

Jak se viry šíří

Objekty, které mohou být napadeny viry:

- **Spustitelné soubory** (programy) – soubory s příponami EXE, COM, SYS, nebo s jinou příponou, např. OVL, SCR, BIN, …
- **Systémové oblasti** – partition tabulka nebo Boot sektor pevného disku
- **Dokumenty** – datové soubory, které mohou obsahovat makra, např. DOC, XLS, PPT, …
- **Ostatní objekty** – VBScripty a JScripty obsažené v HTML stránkách nebo Java applety

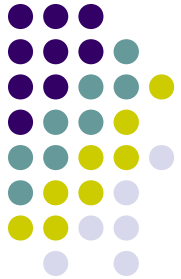
Základní dělení virů

- **Bootviry** – napadají pouze systémové oblasti.
  - Vlastní infekce disku spočívá v tom, že se virus zapíše do Partition tabulky pevného disku a její původní obsah odklidí na nějaké bezpečné místo.
  - Při každém startu je zaveden do OS a stává se aktivním.
  - Převezme kontrolu diskových služeb a poté spustí správný zaváděcí kód.

Základní dělení virů

- **Souborové viry** – napadají pouze soubory.
  - **Přepisující virus** – při napadení přepíše část těla oběti vlastním kódem. Takto napadené programy jsou nenávratně zničeny a nejsou kromě dalšího šíření viru schopny žádné jiné činnosti.
  - **Doprovodný virus** – vytváří stínový soubor stejného jména s příponou COM.
  - **Link virus** – virus se připojí k tělu oběti a může tak zachovat původní funkci programu.

Základní dělení virů



- **Multipartitní viry** – napadají soubory i systémové oblasti. Tyto viry kombinují „výhody“ bootviru a souborového viru. Jeden z nejrozšířenějších multipartitních virů byl *One_Half*.

- **Makroviry** – napadají dokumenty. Psaní makrovirů umožňuje jazyk VBA.

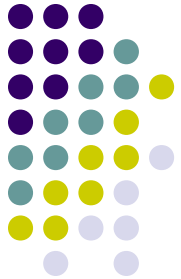
Speciální vlastnosti

- **Virus přímé akce** – jakmile je spuštěn, tak vykoná vše co chtěl a skončí.
- **Rezidentní virus** – je přítomen v paměti a může tak neustále ovlivňovat činnost počítače.
- **Stealth virus** – převezme kontrolu funkcí OS a při pokusu o čtení infikovaných objektů vrací stav před infekcí.
- **Polymorfní virus** – pro každý napadený soubor vytváří zcela jinou dekryptovací funkci (žádné sekvence stejného kódu).

Trojský kůň

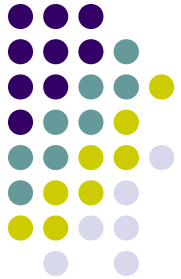
- Trojský kůň je škodlivý program, který je často zaměňován za počítačový virus.
- Jsou to jednoduché programy předstírající nějakou užitečnou činnost,
  - které místo toho smažou soubory,
  - přepíšou konfiguraci počítače v CMOS,
  - nebo provedou jinou destruktivní akci.

Spyware



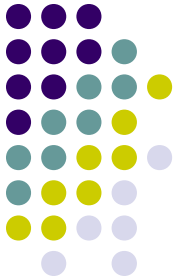
- odesílá z počítače data další osobě,
- jedná se pouze o data statistická, např. přehled navštívených stránek, počet a typ nainstalovaných programů ...,
- tyto informace bývají často zneužívány pro cílenou reklamu.

Adware



- jsou to programy, které znepříjemňují práci nějakou reklamní aplikací,
- mohou mít různou úroveň agresivity
  - běžné bannery
  - neustále vyskakující pop-up okna
  - ikony v oznamovací oblasti…

Hoax



- je poplašná zpráva, která důrazně varuje před nebezpečným virem, který ve skutečnosti vůbec neexistuje,
- není škodlivý, ale obtěžuje uživatele.

Použité zdroje

- Kocman, R., Lohniský, J. *Jak se bránit virům, spamu a spyware.* Computer press, 2005
- http://www.viry.cz [cit. 2013-12-04].