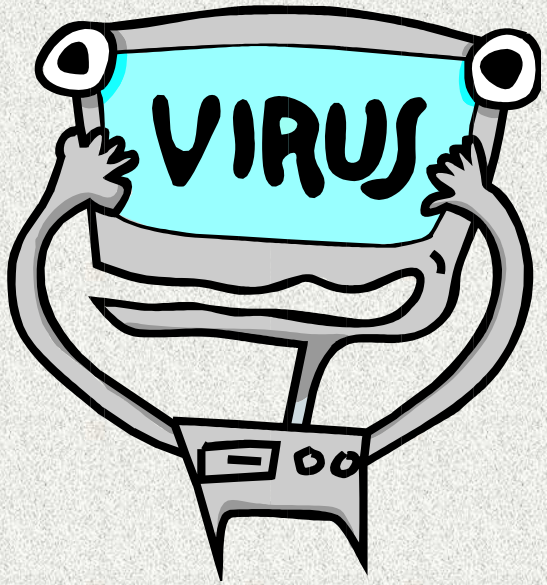
Viry a červi

Informatika v praxi

autor: Ing. Pavel Broža
Základní škola a Mateřská škola Kameničky
Další možnosti studia - nepovinné předměty CZ.1.07/1.1.28/02.0034

Předpokládaný čas: 2 vyučovací hodiny
Stupeň vzdělávání: druhý stupeň

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

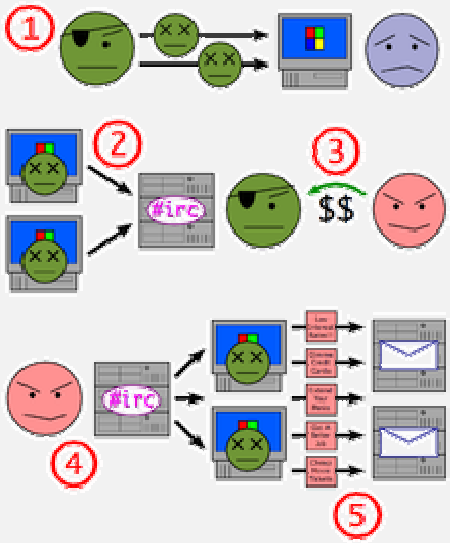


Co je to virus ?

Jako **virus** se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká *nakažení* či *infekce* a napadenému souboru *hostitel*.

Virus je typ programu, který se dokáže sám šířit tím, že vytváří (někdy upravené) kopie sebe sama. Hlavním kritériem pro posouzení programu jako viru je fakt, že k šíření využívá jiné soubory – hostitele. Virus se mezi dvěma počítači může přenést jedině tím, že někdo přenese celého hostitele, např. nějaký uživatel (obvykle neúmyslně) přenese soubor na CD-ROM, DVD-ROM, flashka nebo ho pošle prostřednictvím počítačové sítě.

Život viru



Život tzv. „ZOMBIE“:
(1) Autorovi viru se podaří infikovat uživatelské PC.
(2) Viry na napadených počítačích se průběžně přihlašují k IRC serveru a vytváří síť napadených počítačů (botnet).
(3) Spammer zaplatí autorovi viru za poskytnutí vzniklé sítě.
(4) Po IRC kanálu pošle spammer virům instrukce a
(5) napadené počítače slouží k rozesílání spamu.

Typy virů

• **cíleně ničivé** (např. mažou soubory na disku)

• **obtěžujících**

• **„logická bomba“** u některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů)

Dnes jsou klasické počítačové viry na jistém ústupu oproti červům, které se šíří prostřednictvím sítí a hlavně internetu.

Podle hostitele

- **Spustitelné soubory** – COM a EXE programy v prostředí DOSu EXE soubory ve Windowsu, ELF soubory v UNIXu atd
- **Boot sektory** disket a diskových oddílů
- **Maste boot sektor**(MBR) pevného disku
- **Dávkové soubory a skripty** – BAT v DOSu, shellovské scripy a UNIXeh
- **Dokumenty**, které mohou obsahovat makra – např. dokumenty programů Microsoft Office
- **Specializované skripty** některých konkrétních aplikací

Důvody vzniku virů

- Vytvářejí je programátoři velkých softwarových firem, kteří byli propuštěni ze zaměstnání.
- Vytvářejí je mladí programátoři, kteří si chtějí vyzkoušet své schopnosti.
- Programátoři softwarových firem, které vytvářejí antivirové programy.
- SPAM
- Cil zdiskreditovat platformu

Jak se chránit

- Používat antivirový program, není až tak důležité který.
- Pravidelně aktualizovat databázi virů i antivir samotný.
- Nikdy nespouštět nevyžádané programy, které přišly elektronickou poštou.
- Programy i dokumenty sdílené s jinými uživateli, které dostanete nebo vám přijdou elektronickou poštou, je potřeba zkontrolovat antivirovým programem.
- Pokud je to možné, nastavte si v prohlížeči vysokou úroveň zabezpečení, a pokud používáte MS Office, zapněte si antivirovou ochranu maker.

Princip antiviru

Porovnání s databází virů (skenování, scan)

Heuristická analýza – kód souborů známých virů

Sledování změn (kontrola integrity) – sledování změn v systému souborů

Rezidentní sledování – neustále spuštěn proces sledování změn

Počítačový červ

Počítačový červ je v informatice specifický počítačový program, který je schopen automatického rozesílání kopií sebe sama na jiné počítače. Poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a využívá je ke svému vlastnímu šíření.

Původně měli pomáhat a ne škodit

Činnost červů

Kromě svého vlastního šíření provádí další úkony:

- odstraňování souborů uložených v počítači
- šifrování souborů uživatele kryptováním k útokem jako nátlak k zaplacení poplatku, po kterém je přislíbena jejich opětovná dekrypce
- prohledávání počítače za účelem získání osobních dat, která mohou pro autora programu znamenat nějaký profit
- vytváření „zadních vrátek“ do systému (tzv. backdoor), která poté mohou být využita jako přímá cesta k infikování počítače dalšími nákazami
- jako důsledek jiné činnosti způsobují nestandardní chování systému.

+ dlaší vedlejší efekty: snížena rychlost průtoku dat

Typy červů

- **E-mailoví červi**
- **Internetoví červi**
- **IM a IRC červi**
- **Červi využívající sdíleného prostoru**

Jak se bránit?

- neotvírat přílohy e-mailů s neočekávaným typem přiložených souborů, jejichž obsah není přesně znám
- nespouštět odkazy na neznámé/podezřelé stránky a ani se po těchto webech nepohybovat
- nestahovat sdílený nelegální obsah
- používat antivirový a ideálně i antispywarový software, který je schopen nejen zastavit již probíhající infekci, ale v případě správné funkčnosti a nastavení rovněž předejít nakažení počítače
- používat firewall
- používat vždy nejaktuálnější verzi operačního systému (aktualizace) s instalovanými opravnými balíčky

Autor: Pavel Broža „rattle „

Čerpáno z: http://www.viry.cz, *cs.wikipedia.org/wiki/Virus*

Další možnosti studia - nepovinné předměty CZ.1.07/1.1.28/02.0034

evropský sociální fond v ČR | EVROPSKÁ UNIE | MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY | OP Vzdělávání pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ