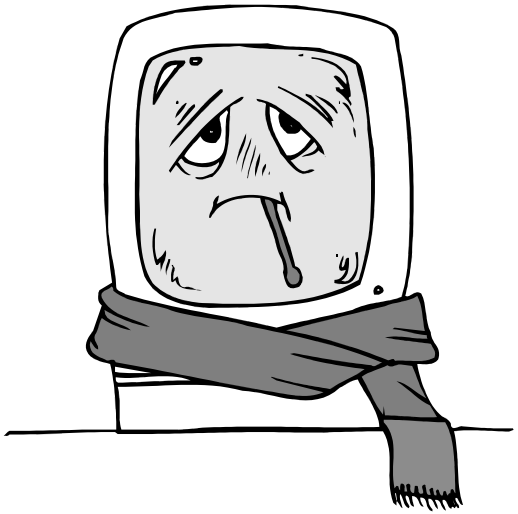
Viry
a další počítačová havěť

„Jak se rozmnožují počítačové viry?“
„Pučením.“
„???“
„Pučíš si flešku a už ho máš taky."

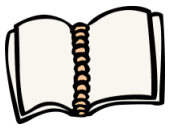
Ing. Simona Martínková
Masarykovo gymnázium, Plzeň

Obsah

Počítačová infiltrace



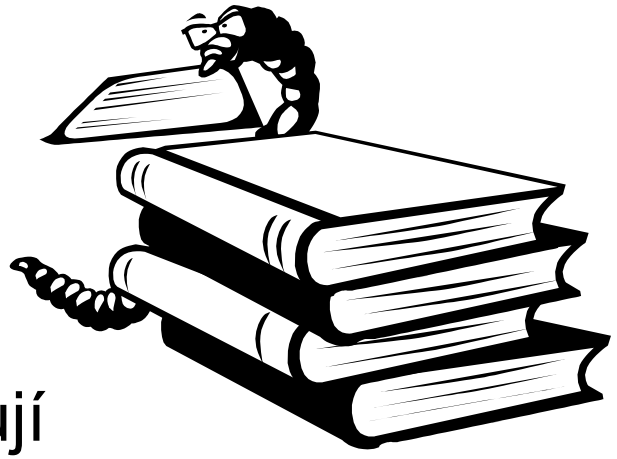
- Jakýkoliv neoprávněný vstup do počítačového systému.
- **Malware** – MALicious softWARE, škodlivý (zákeřný) software.
- Souhrnné označení pro počítačové viry, trojské koně, spyware, adware…
  = počítačová nečistota.



Počítačový virus

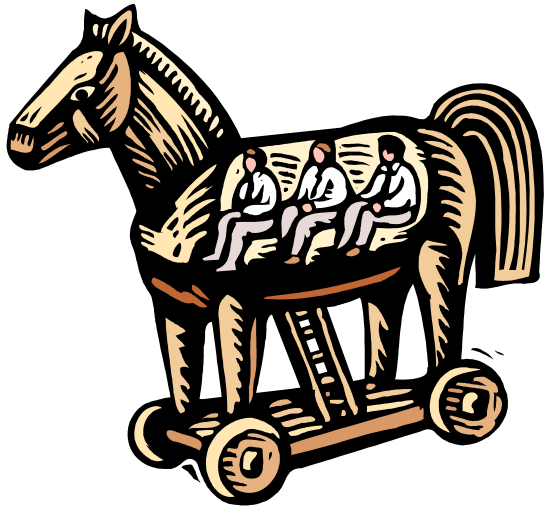
- Program **napadající** obvykle **spustitelné soubory** (EXE, COM, …) nebo systémové oblasti disku.
- Neexistuje jako samostatný soubor – připojuje svůj kód k jiným programům.
- Je schopen se množit a dál se bez vědomí uživatele šířit na další spustitelné soubory.

Makrovirus



- **Napadá dokumenty**, které obsahují tzv. makra (makro – program napsaný v programovacím jazyce, který je součástí příslušné aplikace).
- Úspěšné šíření makroviru vyžaduje několik podmínek:
  - Příslušná aplikace musí být široce používána (např. MS Word, Excel, PowerPoint, Outlook, ...).
  - Musí docházet k výměně dat mezi jednotlivými uživateli a počítači.

Trojský kůň



- Je **samostatně existující program**.
- Může se maskovat jako užitečný program a na pozadí provádět nějakou škodlivou činnost – například otevřít „zadní vrátka“ do našeho počítače a umožnit tak jeho vzdálenou správu.
- Nejčastěji jako spustitelný soubor typu EXE.

Červ (worm)

- Červ zneužívá konkrétní bezpečnostní díry v operačním systému.
- Šíří se prostřednictvím počítačové sítě.
  - např. rozesílá kopie sebe sama na e-mailové adresy nalezené v počítači.
- Vedlejším efektem může být kompletní zahlcení sítě.

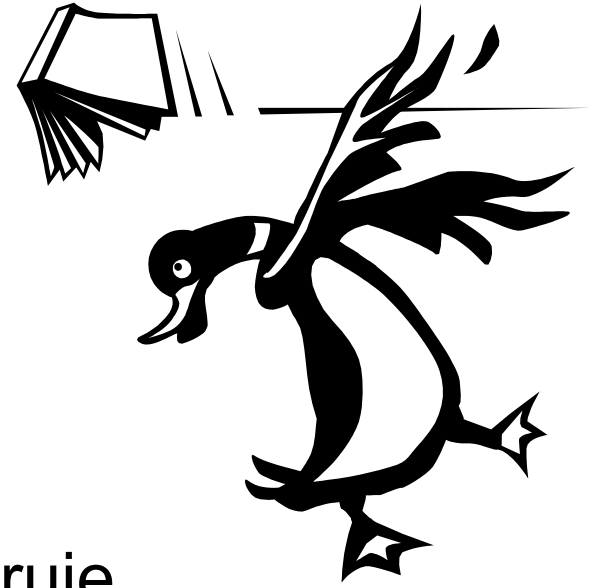
Spyware

- Je program, který využívá internetu k **odesílání dat z počítače bez vědomí jeho uživatele**.

Adware

- Program, který **znepříjemňuje práci s počítačem reklamou** (ADvertisement softWARE).
- Typickým příznakem jsou „vyskakující“ pop-up reklamní okna během surfování společně s vnucováním stránek, o které nemá uživatel zájem.
- Adware může být součástí některých, např. sharewarových programů.

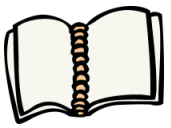
Hoax



- Označuje **poplašnou, lavinovitě se šířící zprávu**, která obvykle varuje před neexistujícím nebezpečím (např. nebezpečným virem).
- Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů (např. firmy IBM, Microsoft).
- Nechybí výzva k dalšímu rozeslání.
- Patří sem i tzv. **řetězové dopisy**.

Phishing

- **Podvodné e-maily** sloužící k získávání důvěrných údajů.
- Na první pohled vypadají jako informace od významné instituce (nejčastěji banky).
- Příjemce je informován o údajné nutnosti vyplnit údaje v připraveném formuláři (bývá uveden odkaz), jinak mu může být zablokován jeho účet, popřípadě může být jinak znevýhodněn.



Spam

- **Nevyžádané masově šířené obchodní sdělení** (reklama).
- V drtivé většině případů rozesílají roboti.
- Získání adresy – ochrana proti sběru adres.
  - Jednou z možností, jak se bránit, je uvádět e-mailovou adresu v „nečitelné“ podobě (obrázek, at, zavináč).
    Například: *novak@seznam.cz*
    novak (at) seznam (dot) cz
    novak(zavináč)seznam.cz

Jak se infiltrace šíří

- Síť internet (web, e-mail)
- Paměťové médium (autorun.inf)
- Čeho využívá k šíření:
  - Bezpečnostní chyby v operačním systému
  - Bezpečností chyby v programech (internetový prohlížeč, e-mail, icq, …)
  - Nezodpovědné chování uživatelů (vypínání firewallu, navštěvování nedůvěryhodných stránek – s cracky, keygeny, …)

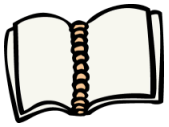
Prevence

- **Pravidelná aktualizace operačního systému.**
- **Pravidelná aktualizace „internetových“ programů** (prohlížečů, e-mailových klientů, chatovacích programů apod.) – odstranění bezpečnostních děr.
- **Originální software** – jednak neobsahuje virus od výrobce, jednak při napadení jej lze znovu nainstalovat z originálních médií.
- **Zálohování důležitých dat.**

Antivirové programy

- Poskytují kombinované služby
  - nalezení viru
  - odstranění viru
  - ochrana počítače
- Aktualizace programu
- Průběžná aktualizace virové databáze
- Plánované skenování počítače
  - program se spustí ve vhodné době
  - provede se kompletní prohlédnutí počítače

Některé antivirové programy



- ESET – program NOD32 – http://www.eset.cz/
- Grisoft – program AVG – http://www.grisoft.cz/ nebo http://free.avg.com/
- Alwil Software – program Avast! – http://www.alwil.com/
- MS Security Essentials – http://www.microsoft.com/security_essentials/
- Kaspersky Lab – program Kaspersky Antivirus http://www.kaspersky.cz/
- McAfee VirusScan – http://cz.mcafee.com/
- Symantec – program Norton Antivirus http://www.symantec.com/cs/cz/norton/index.jsp

Firewall

- Slouží k ochraně počítačů připojených k internetu před útoky „zvenčí“.
- Firewall kontroluje veškerý pohyb dat dovnitř a ven a podle nastavených pravidel tento pohyb dat řídí.
- Pokud je komunikace pro daný program povolena, propustí firewall data.
- Pokud je zakázána, tak firewall komunikaci nepovolí.

Používejte zdravý rozum

- Neklikat na vše co vidím.
- Nepotvrzovat dotazy, kterým nerozumím.
- Nenavštěvovat pochybné stránky.
- Nespouštět odkazy na neznámé/podezřelé stránky a ani se po těchto webech nepohybovat.
- Nestahovat sdílený nelegální obsah.
- Nespouštět podezřelé programy.
- Neotvírat přílohy e-mailů s neočekávaným typem přiložených souborů (pozor na dvojitou příponu, např. obrazek.jpg.exe, „bílé“ znaky, interní ikonu souboru).
- Používat antivirový a ideálně i antispamový software.
- Používat firewall.

První zmínka o počítačovém viru

- Rok 1972 – první zmínka v románu Davida Gerrolda „When H.A.R.L.I.E. Was One“
  - počítačový program nazvaný VIRUS, sám sebe kopíruje, šíří se, skrývá se a dovede ničit
  - je zničen programem VACCINE, tedy románovým předchůdcem antivirů

První virus

- Rok 1986 – vznik **prvního viru Brain**
  - Napsali ho dva bratři z Pakistánu (Asit a Amjat Farooq Alviovi).
  - Údajně ho dávali jako bonus cizincům, kteří si u nich v obchodě kupovali nelegální software (nedestruktivní, obsahoval pouze reklamu – v boot sektoru zanechal text, obsahující copyright týkající se viru a informace o jeho autorech).
  - Brain byl boot virus šířící se přes disketu zapomenutou při startu počítače v mechanice.
- Rok 1988 zahájil éru **antivirových programů** – jedním z nejstarších je McAfee VirusScan.

Jeden legendární virus

- Během roku 1994 se objevila jedna z virových legend, virus **One_Half**.3544.A.
  - One_Half postupně kódoval obsah pevného disku podle určitého klíče, který si s sebou nesl.
  - Pokud operační systém potřeboval zapsat nějaká data na disk, virus převzal kontrolu a tato data nejdříve svým algoritmem zašifroval a až poté je nechal zapsat na disk. Při požadavku ke čtení je naopak dešifroval a předal dál operačnímu systému.
  - Pokud byl One_Half neodborně odstraněn (včetně tohoto klíče), znamenalo to i ztrátu zakódované části dat.

Kdo jsou tvůrci virů?

- **Cíl uškodit** – naprostá většina dříve rozšířených virů pocházela právě od této skupiny lidí.
- Snaha o nalezení vzrušení a **získání uznání a slávy** v rámci hackerské komunity, překonání intelektuálních výzev – dnes už též v pozadí.
- **Pomsta** propuštěného programátora – poškodit zaměstnavatele, zničit svoji dřívější práci – snad.
- Dnes hlavně snaha **odcizit údaje** (soukromé i firemní) nebo **zneužít cizí počítač pro odesílání spamů**.

Hacker

- Dnes se toto označení obecně používá pro osoby nabourávající se (pronikající) do cizích počítačových systémů
  - za účelem vykrádání dat (například prostřednictvím trojského koně)
  - nebo jinak škodící (třeba zneužití vašeho počítače k útokům na jiné počítače, k rozesílání spamů apod.).

Heslo

- Diskrétní a soukromá věc – střežit jako oko v hlavně.
- Nepsat do mobilu nebo do volně přístupného dokumentu v počítači.
- Nepoužívat jedno heslo všude – používat tzv. **silná hesla** (malá i velká písmena, číslice, jiné znaky).
- Používat virtuální klávesnici (například na stránkách www.servis24.cz).

Užitečné adresy a zdroje informací

- Informování uživatelů o nástrahách el. pošty a mnohých dalších – http://www.hoax.cz
- Aktuální informace o virech a podobné havěti a o tom, co s tím – http://www.viry.cz
- Ukázky využití sociálního inženýrství – „oblbnutí" uživatele za využití přesvědčivě vypadající grafiky či textu