**Počítačové viry**

Pojem vir je v dnešní době ustálený výraz, který slouží k označení jakéhokoliv napadení PC. Všeobecně je řadíme do větší skupiny, kterou nazýváme pojmem **infiltrace**.

**Počítačovou infiltrací** nazveme jakýkoliv neoprávněný vstup do počítačového systému, a tím i do jeho souborů, programů atd.

**Mezi infiltrace řadíme:**

* hackerství
* trojské koně
* červy
* sparing
* viry

**Hackerství**

Jedná se v podstatě o zakázané přihlášení se (login) do počítače a jeho neoprávněné použití, často spojené se zcizením informací. Velmi nebezpečné jsou tzv. průniky do počítačových bankovních systémů, počítačových sítí telefonních ústředen, databank apod., nejčastěji za účelem finančního zisku. S touto činností souvisí tzv. backdoors (zadní vrátka) – napadený soubor čeká na aktivaci útočníkem prostřednictvím sítě internet, který může jeho prostřednictvím ovládat hostitelský PC.

**Trojské koně**

Nejsnáze odhalitelná forma infiltrace. Trojský kůň je většinou program, který se na první pohled chová jako zcela legální program, ve skutečnosti však tajně provádí škodlivé operace. Důležitou skutečností je, že trojský kůň není narozdíl od viru schopen replikace (množení) a nepřipojuje se k hostiteli - souboru. Jeho odstranění se provádí velmi jednoduše – smazáním.

**Červy**

Červ je na rozdíl od trojského koně sebereplikující program. Je soběstačný, samostatný, nevyžaduje žádný hostitelský program, je schopen šířit své funkční kopie nebo jejich části do jiných počítačových systémů. Program typu červ sám vytváří své kopie a způsobuje, že jsou spuštěny. Červi ke svému šíření využívají nejčastěji síťových služeb, například elektronickou poštu.

**Spamming**

Jedná se o šíření nevyžádaných mailů, k nimž patří i poplašné zprávy zvané hoaxy. Tyto důrazně varují před nebezpečnou počítačovou infekcí, která však ve skutečnosti neexistuje.

Text hoaxu obsahuje většinou tyto body:

* Charakteristika vymyšleného viru, zvláště pak údajný způsob šíření.
* Popis ničivých účinků viru.
* Varování pochází z důvěryhodných zdrojů.
* Výzva k dalšímu rozeslání. Mnoho nezkušených uživatelů velmi ochotně na výzvu reaguje. Nepravdivé informace se pak šíří po síti geometrickou řadou.

**Phishing**

Je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku. Tato stránka může například napodobovat přihlašovací okno internetového bankovnictví a uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze. Existuje několik úrovní boje s phishingem: na uživatelské úrovni zejména osvěta a dodržování bezpečnostních pravidel, na softwarové úrovni je možno používat specializované nástroje, které phishingové útoky umožňují detekovat a upozorňovat na ně.

## Rozdělení virů

### Klasifikace podle způsobu umístění do paměti

* rezidentní viry – umístěn natrvalo v paměti, při prvním spuštění infikovaného souboru nebo při jeho zavedení z boot sektoru se stává rezidentní a provádí svou škodlivou činnost
* nerezidentní viry – nejsou umístěny v trvale paměti, stačí , když jsou aktivovány společně s hostitelským programem. Pak přebírají řízení jako první, provedou svoji činnost, nejčastěji replikaci a předají řízení zpět hostitelskému programu (replikací zde většinou rozumíme například napadení všech vhodných souborů). Nerezidentní viry jsou většinou souborové viry

### Klasifikace podle napadených oblastí

* bootové viry - jsou to viry, které infikují proveditelný kód nacházející se v určitých systémových oblastech disku
* souborové viry – jde o viry, které napadají soubory.
  + prodlužující viry - při infekci změní (většinou prodlouží) obsah cílového souboru. Nepoškodí obsah cílového souboru (narozdíl od přepisujících virů). Nejčastěji se tyto viry připojují na konec souboru.
  + přepisující viry (virony) - souborové viry, které přepíší obsah cílového spustitelného souboru vlastním kódem (tělem), a tak zníčí původní obsah souboru Takto infikovaný soubor je již nefunkční a nemůže být opraven. Po jeho spuštění dojde pouze k aktivaci viru, který se ve většině případů rozmnoží do dalších spustitelných souborů.
  + duplikující viry - napadají soubor typu exe tak, že vytvoří nový soubor se stejným jménem, ale s příponou .com, do kterého umístí své tělo. Při volání původního souboru se podle dosovských priorit dává přednost com-souboru - dojde ke spuštění viru a ten spustí původní program. Dnes se téměř nevyskytují.
  + multiparitní viry - viry, které se chovají jako bootové i jako viry souborové
  + retroviry - cílem je obejít či znemožnit činnost konkrétního antivirového programu
  + makroviry – patří k rozšířené skupině virů, která ke svému šíření využívá maker. Makra jsou programy, které si uživatel může sám vytvořit pro usnadnění práce v některých aplikacích; typickou aplikací může být například Microsoft Word, či Microsoft Excel

## Typy makrovirů

* **Stealth -** tyto makroviry maskují svoje makra, aby se tak bránily proti snadnému odhalení.
* **Polymorfní -** tyto makroviry dokážou modifikovat strukturu vlastního těla. Polymorfní makroviry pak nelze detekovat podle sekvencí, či podle klasických kontrolních součtů (CRC).
* **Multipartitní -** tato skupina makrovirů se dokáže šířit několika způsoby. Například makrovirus Shiver je napsán tak, že se dokáže šířit jak v programu Word, tak i v programu Excel.
* **Multiplatformní -** některé makroviry se dokážou šířit pod různými systémy, kde se některé produkty používají.

**Použitá literatura:**

HÁK, Igor. *Moderní počítačové viry* [online]. [cit. 2013-02-03]. Dostupné z: <http://www.cmsps.cz/~marlib/bezpecnost/viry/velka_kniha_o_virech.pdf>

*Počítačové viry* [online]. [cit. 2013-02-03]. Dostupné z: <http://www1.osu.cz/~klimesc/public/files/Pocitacove%20systemy/Prednasky/08_-_Pocitacove_viry.pdf>

*Počítačové viry, antivirová ochrana a bezpečnost na internetu* [online]. [cit. 2013-02-03]. Dostupné z: http://www.ped.muni.cz/wtech/old2012/u3v/iepp/05.pdf