Viry a malware

Malware

Výraz malware vznikl spojením anglického *malicious software* (v překladu zákeřný software). Jako malware se označuje software psaný za účelem škodit vlastníkovi. Mezi malware se řadí **počítačové viry, červi, spyware, adware, trojští koně, rootkity, backdoory** a další.

Virus

Za virus se označuje program, který je schopný se šířit bez vědomí uživatele. Neumí se šířit sám, šíření probíhá skrze soubor nakažený virem (hostitel). Virus se může přenést z jednoho počítače na druhý jen, když někdo přenese celého hostitele. Chová se tedy podobně, jako biologický virus. Svojí činností negativně ovlivňuje hostitelský počítač.

Dělení virů podle hostitele

Spustitelné soubory

EXE(dříve COM) - nejčastější způsob, virus se aktivuje spuštěním programu

Boot viry

Častý způsob nákazy před rozšířením internetu. Do boot sektoru diskety, jiného média, či pevného disku (Master boot sektor) je zaveden kód viru a ten se do počítače dostane okamžitě po zapnutí. Tím virus obejde operační systém a tedy i případný antivirus.

Makroviry

Přenášejí se v dokumentech (např. dokumenty MS Office). Virus je zde ve formě makra, které je schopno např. i spustit libovolný program, a to bez vědomí uživatele. V dnešní době se již nevyskytují tolik, protože většina kancelářských programů má již ochranu proti nepovolenému spouštění maker.

Dělení virů podle činnosti

Nerezidentní

V okamžiku spuštění hostitele se virus začne šířit do nalezených nenakažených souborů.

Rezidentní

V okamžiku spuštění hostitele se virus uloží do paměti PC, kde zůstane až do vypnutí, mezitím infikuje soubory, se kterými uživatel pracuje.

Stealth viry

Virus maskuje svoji přítomnost tím, že se zachytí na přerušení, kudy prochází veškeré požadavky na čtení dat ze souboru (tedy i požadavky antiviru). Vir si pak kontroluje, zda se požadavek týká i infikovaného souboru, v tomto případě pak vrátí aplikaci data původního neinfikovaného souboru. Obrana proti tomuto způsobu skrývání není složitá - antivirus si buď kontroluje, zda není adresa přerušení přepsána, případně na čtení používá přímo služby diskového řadiče. Tato maskovací technika se používala hlavně na MS-DOS, v dnešní době viry k podobným účelům používají rootkit.

Červ

Chová se podobně jako virus(také se proto občas mezi viry řadí), ale poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a dokáže se díky tomu šířit po síti bez zásahu uživatele.

Dělení červů podle způsobu šíření

E-mailoví červi

Ke svému šíření využívají elektronickou poštu. Poté, co infikují počítač se začnou rozesílat na e-mailové adresy získané buď z adresáře oběti, nebo z jiných souborů.

Internetoví červi

Ke svému rozšíření využívá všechny dostupné síťové prostředky. Pokud najde v síti počítač, který je zranitelný, provede útok, spustí škodlivý kód a nainstaluje se do jeho systému.

IM a IRC červi

Tito červi využívají komunikačních sítí. V prvním případě nejčastěji posílají odkazy na webové stránky, které jsou schopny infikovat počítač, v případě IRC zasílají škodlivý program ve formě souboru. Uživatel soubor tedy musí uložit a spustit.

Botnet

Botnet je síť složená z množství infikovaných počítačů. Červy je možné aktivovat na dálku a donutit je

k rozesílání spamu (pomocí e-mailových adres získaných od uživatele), nebo např. k útoku DDoS (příliš velkým množstvím požadavků se zahltí stránka a to způsobí její nefunkčnosti, či dokonce může vyústit v pád serveru).

Spyware

Spyware je program, který přes internet odesílá bez vědomí uživatele (nejčastěji soukromá) data, které nasbíral v počítači. Takto může odesílat např. hesla, historii prohlížených stránek, informace o datech, které jsou na počítači, nebo přímo celé dokumenty. Může také snímat veškerou aktivitu na klávesnici (keyLogger), nebo zobrazovat reklamy (adware).

Adware

Adware zneužívá počítač uživatele ke zobrazování reklam (např. v internetovém prohlížeči), vytváření reklamních zástupců na ploše, a jinému zobrazování nevyžádaného obsahu.

Trojský kůň

Jako trojský kůň se program, který se tváří neškodně, avšak skrývá část, která uživateli škodí. Trojský kůň je často přidáván do nelegálně poskytovaných aplikací, her, ale vyskytují se i např. u spořičů obrazovky. Trojský kůň nedokáže sám infikovat další počítače nebo programy svojí kopií. Existují ale červi, kteří dokáží vytvářet Trojské koně z programů, které najdou v napadeném počítači.

Rootkit

Rootkit umožňuje maskovat přítomnost zákeřného software v počítači, tak, aby přítomnost malwaru nebyla běžnými síťovými prostředky odhalitelná.

Backdoor

Backdoor (zadní vrátka) je metoda, která umožní v budoucnu snadnější přístup dalšího malwaru do počítače, protože jim dovoluje obcházet autentizační mechanizmy a dovoluje jim využívat skrytou metodu vstupu.

Metody hledání virů

Slovníkové hledání

Při kontrole souboru antivirus zjišťuje, jestli se některá jeho část neshoduje s kódem některého z již objevených virů, který má v databázi. Pokud antivirus najde shodu, typicky nabízí tři řešení:

1. vyléčit soubor - odstranění viru ze souboru
2. umístit soubor do karantény - virus se dále nemůže šířit, protože jej nelze používat
3. odstranit virus i se souborem

Pro aktivní ochranu je třeba mít neustále aktivní antivirus, aby program porovnával kód s nejnovější virovou databází.

Heuristická analýza

Antivirus sleduje činnost všech programů, a varuje uživatele, kdykoliv se některý program snaží provést něco podezřelého. Výhodou tohoto postupu je, že je schopný najít i naprosto nové viry, antivirový program může ale takto nahlásit i neškodné programy („false positive“), proto, že část jejich chování se podobá nějakému viru.