

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 proto probíhá skrze soubor nakažený virem (hostitel), který viru umožňuje vytvářet další a další kopie sebe sama. Z jednoho počítače na druhý lze virus přenést pouze přenesením celého hostitele. Chová se tedy podobně, jako biologický virus. Svoji činností negativně ovlivňuje hostitelský počítač (vede k zahlcení, zpomalení apod.).

Dělení virů podle hostitele

Spustitelné soubory

EXE (dříve COM) atd. - nejčastější způsob, virus se aktivuje spuštěním spustitelného souboru.

Boot viry

Častý způsob nákazy před rozšířením internetu, velmi nebezpečný. 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 dokonce i spustit libovolný program, a to bez vědomí uživatele. V dnešní době se již ovšem příliš nevyskytují, protože většina kancelářských programů má již ochranu proti nepovolenému spouštění maker.

E-mailové viry

Přenášejí se (vědomě, nikoli omylem) za pomoci e-mailových služeb (nejčastěji MS Outlook). Šíří se s odeslanými e-maily ve formě přílohy.

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 [rootkity](#). Viry se mohou pokusit skrýt například také zachováním data poslední úpravy, velikosti souboru.

Červ

Chová se velmi podobně jako virus, ale na rozdíl od viru v infikovaném systému převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci, čímž se dokáže šířit po síti – sám, bez zásahu uživatele. Díky této vlastnosti může i zdánlivě neškodný počítačový červ způsobit potíže zahlcováním sítě.

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 z adresáře oběti nebo z jiných souborů.

Internetoví červi

Ke svému rozšíření využívá všechny dostupné síťové prostředky k nalezení zranitelného počítače, provede útok, spustí škodlivý kód a bez vědomí či akce od uživatele se nainstaluje 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 převážně zasílají škodlivý program ve formě spustitelného souboru. Uživatel soubor tedy musí prvně uložit a spustit.

Botnet

Botnet je síť složená z velkého 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 zahltní internetová stránka či služba, což vede k její nefunkčnosti, dokonce až pádu celého 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 (tzv. adware). Tvůrci spyware se často brání tím, že data využívají za účelem zobrazení přesnějších reklam apod.

Adware

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

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 kopíí. Existují ale červi, kteří dokáží vytvářet trojské koně z programů, které najdou v napadeném počítači.

Rootkit

Rootkit umožňuje maskovat přítomnost malware v počítači tak, aby byla jeho přítomnost co nejhůře odhalitelná. Ukrytí mohou docílit skrytím běžících procesů, souborů a operačního systému tak, aby nebyl daný malware běžným uživatelem odhalitelný. Místo ukrývání mohou rootkity malware také chránit proti ukončení a odstranění.

Backdoor

Backdoor (zadní vrátka) je metoda, která umožní v budoucnu snadnější přístup dalšího malwaru do počítače, protože jim dovoluje obcházet autentizační mechanismy a dovoluje jim využívat skrytou metodu vstupu. Backdoor bývá často spojován s myšlenkou předinstalování backdoorů za účelem snadnějšího poskytnutí technické podpory.

Pravidla prevence

Abychom se vyhnuli malware, je třeba:

- pravidelně aktualizovat operační systém a nainstalovaný software, protože aktualizace mohou obsahovat bezpečnostní vylepšení;
- přemýšlet při stahování, sdílení, otevírání e-mailové přílohy, dávání administrátorských práv, dokonce i při klikání na internetové odkazy a zdánlivě nevěrohodné stránky například ani nenavštěvovat;
- nevěřit vyskakovacím oknům vyzývajícím ke stažení nějakého souboru;
- používat ochranný software (např. antivirus).

Roli při prevenci hraje i sám operační systém. Převážně kvůli svému rozšíření na trhu je totiž naprostá většina virů a malware určena pro Windows. Mac a Linux jsou v tomto ohledu tedy mnohem bezpečnější.

Antiviry

Antivirus je program určený k identifikaci a následnému odstranění a eliminaci počítačových virů. Po rozšíření ostatních druhů malware však začaly antiviry vztahovat svoji ochranu až na všechny malware.

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 odstraněním viru ze souboru, pokud to je technicky možné
2. umístit soubor do karantény - virus se dále nemůže šířit, protože jej nelze používat
3. smazat virus spolu s infikovaným souborem

Pro aktivní ochranu je třeba mít antivirus neustále aktivní a aktualizovaný, aby mohl porovnával kód s nejnovější virovou databází. I přesto mohou nastat potíže např. kvůli schopnosti některých virů šifrovat části svého kódu.

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 zmutované i naprosto nové viry, antivirový program může ale takto nahlásit i neškodné programy („false positive“), protože se část jejich chování či jejich kódu podobá nějakému viru.

From:

<http://wiki.gml.cz/> - **GMLWiki**

Permanent link:

<http://wiki.gml.cz/informatika:maturita:5a?rev=1506961300>

Last update: **02. 10. 2017, 18.21**

