# 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. A nebo obecně cokoliv co škodí našemu počítači. 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. Svojí 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 (např. přes CD, DVD, flash disky atd.). Tím virus obejde operační systém a tedy i případný antivirus. Odstranit ho pak můžeme pomocí flash disku, CD atd. s antivirem.

#### Makroviry

Přenášejí se v dokumentech (např. dokumenty MS Office → .doc, .docx, .xls atd.). Virus je zde ve formě makra (tj. skripta), 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.

#### Multipartite virus

Hybrid Boot a Souborového viru. Infikuje program a jakmile je program spuštěn, virus infikuje boot oddíl. Když je pak spuštěn počítač, virus se načte z boot oddílu do paměti a začne infikovat ostatní soubory na disku.

#### Polymorfní virus

Virus tohoto typu umí zašifrovat vlastní kód tak, že v každé infekci se jeví jinak. Tyto viry jsou obtížné na detekci.

### 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 operační 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. Například „Whale virus„ přidá 9216 bytů infikováním souboru, pak odebere stejný počet bytů (9216) od velikosti zobrazující se v adresáři. 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 zahltí internetová stránka či služba, což vede k její nefunkčnosti, dokonce až pádu celého serveru).

# Neviry

Jsou to malwary, které se nešíří z počítače hostitele.

## 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

Většinou je spojen s freeware programem, aby programátoři mohli díky reklamám dále financovat svůj program. Někteří dávají i možnost odstranění adwaru po zaplacení. Mohou také být spojeny s shareware programy.

### Trojský kůň

Jako trojský kůň chápeme program, který se tváří neškodně, avšak skrývá část, která uživateli škodí. Může například posílat naše údaje autorovi (loginy + hesla, osobní údaje, čísla karet, mail atd.). Trojský kůň je často přidáván do nelegálně poskytovaných aplikací, her, ale vyskytují se i např. u spořičů obrazovky nebo i u jiných zdarma dostupných aplikací. 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 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

Nezdokumentovaný způsob přístupu k systému, obcházející normální mechanismy autentizace. Některá zadní vrátka jsou do softwaru umístěna předinstalováním backdooru za účelem snadnějšího poskytnutí technické podpory a jiná jsou umístěna do systému po napadení například virem nebo červem. Útočníci obvykle používají zadní vrátka pro snazší a trvalý přístup k systému poté, co byl napaden.

### Cryptominer

Software, který používá systémové prostředky oběti za účelem těžení kryptoměny pro útočníka. Způsobuje tak značné zpomalení počítače.

## Distribuční kanály pro malware

Malware má několik kanálů, kterými se může šířit:

- drive-by download - neúmyslné stažení softwaru z internetu;
- nevyžádaná pošta - nechtěné přílohy nebo vložené odkazy v emailu;
- fyzická média - integrovaná nebo vyměnitelná média např USB;
- vlastní šíření - software je schopný se šířit sám třeba infekce mezi počítači po síti.

## Pravidla prevence

Abychom se vyhnuli malware, je třeba:

- pravidelně aktualizovat operační systém a nainstalovaný software, protože aktualizace mohou obsahovat bezpečnostní vylepšení;
- použití nástrojů pro monitorování procesů;
- 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);
- dát si pozor na phishing, kontrolovat si jestli dávám své údaje správné stránce;

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 všechen malware.

## Hledání virů

### Virové slovníky/databáze

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

Pokud se program chová tak, že použije „samo-modifikační“ kód nebo se jeví jako virus (pokud například začne hledat další spustitelné soubory), můžeme předpokládat, že virus nakazil další spustitelné soubory. Nicméně i tato metoda může hlásit falešné pozitivní nálezy.

### Sandbox

Sandbox, napodobuje systém a spouští .exe soubory v jakési simulaci. Po ukončení programu software analyzuje sandbox, aby zjistil nějaké změny, ty mohou ukázat právě přítomnost virů. Tato metoda může taky selhat a to pokud jsou viry nedeterministické a výsledek nastane za různých akcí nebo akce nenastanou při běhu - to způsobí, že je nemožné detekovat virus pouze z jednoho spuštění.

## SELinux

SELinux (Security Enhanced Linux) je vylepšení zabezpečení systémů Linux, které uživatelům a správcům umožňuje větší kontrolu nad řízením přístupu. Lze omezit kteří uživatelé a aplikace mohou přistupovat ke kterým prostředkům. Tyto prostředky mohou mít například podobu souborů. Standardní ovládací prvky přístupu k systému Linux, například režimy souborů (-rwxr-xr-x), jsou modifikovatelné uživatelem a aplikacemi, které uživatel spouští. Naopak, řízení přístupu SELinux je určeno zásadou načtenou do systému, kterou neopatrní uživatelé nebo špatně fungující aplikace nemohou změnit. SELinux také přidává jemnější a podrobnější řízení přístupu. Například SELinux umožňuje určit, kdo může číst, zapisovat nebo spouštět soubor, a určit, kdo může použít unlink, připsat do souboru, přesunout soubor atd. SELinux umožňuje specifikovat přístup i k mnoha jiným zdrojům, než jsou soubory, například k síťovým prostředkům a meziprocesové komunikaci (IPC).