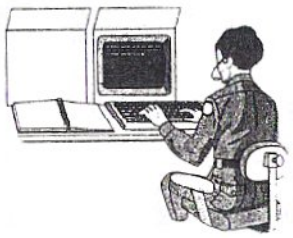
Počítačové viry

Ti, kteří si pod pojmem počítačový vir představují zákeřnou bakterii okusující mikroprocesor, budou zklamáni. Počítačový vir není nic jiného než „pouhý" program. Na rozdíl od většiny programů, které se snaží uživatelům zjednodušovat a ulehčovat práci, počítačový vir se snaží o opak – zmást uživatele, způsobit nefunkčnost vybraných programů a v tom nejhorším případě smazat cenná data nebo rovnou celý disk.

HISTORIE VIRŮ



Historie počítačových virů začíná na počátku osmdesátých let, což je ve výpočetní technice poměrně dávná minulost. V roce 1983 sestrojil Dr. Frederick Cohen první samomnožící program, který se začal označovat jako vir. Jednalo se o neškodný kód, jenž se uměl pouze sám množit.
První „škodlivý" vir s názvem Brain naprogramovali v roce 1986 bratři Basid a Amjad Farooq Alvi. Tím odstartovali boom nepopulárních programů – počítačových virů. Brain byl oproti některým dnešním virům pouhým pohlazením, protože autoři virů znají a předávají si mezi sebou moderní techniky, které umožňují virům měnit svůj vlastní kód, ukrývají se před antivirovými programy a disponují spoustou dalších „triků".

Počítačový vir je program, který je schopen se bez vědomí uživatele množit a provádět nežádoucí operace. Protože z každého zavirovaného programu může být nakaženo mnoho dalších programů, připomíná množení viru řetězovou reakci. Každý vir, ať už se jedná o jakýkoliv typ, je svým způsobem nebezpečný a pochopitelně v počítači nežádoucí. K jeho zlikvidování existují takzvané antivirové programy, které vir dokáží vyhledat a odstranit.
Je jasné, že žádný antivirový program není a ani nemůže být dokonalý tak, aby nalezl všechny viry, které v daném okamžiku existují. Každý antivirový program je za novými viry pozadu, protože aby mohla existovat antivirová ochrana, musí vir nejprve vzniknout a rozšířit se. V současné době lze říci, že zatím na každý vir byla nalezena metoda jak jej odstranit.

JAK SE VIRY ŠÍŘÍ

Pro své šíření potřebuje vir jednak prostředí, které zná - operační systém - a pak takové typy souborů, které mu šíření dovolují – většinou spustitelné programy. Viry se mohou šířit prostřednictvím následujících souborů:

- **Spustitelné soubory (programy)** – bezesporu jeden z nejčastějších případů šíření virů. Vir se při spuštění programu nahraje do paměti a poté provádí svou „nekalou" činnost (šíří se a ničí). Nákaza hrozí u souborů s koncovkou EXE, COM, SYS.
- **Dokumenty** – v poslední době bohužel zažívá velký rozmach relativně nová oblast virů – makroviry. Vir se uloží přímo do dokumentu, který může obsahovat makra (např. Word nebo Excel).
- **Elektronická pošta (e-mail)** – velmi moderní a v poslední době bohužel častý případ virových „invazí". Vir je přenášen jako samospustitelná příloha e-mailu, takže jakmile dojde nová zpráva, stačí ji pouze otevřít a vir se aktivuje.
- **Systémové oblasti** – cílem viru v tomto případě je Boot sektor nebo Partition tabulka. Jedná se o oblasti, do kterých za normálních okolností nemá uživatel přístup a které slouží pouze systému.

TYPY VIRŮ

Podle toho, jakým způsobem viry pracují a jak se projevují, je lze rozčlenit na bootviry, souborové viry, multipartitní viry a makroviry.

SOUBOROVÉ VIRY

Souborové viry napadají pouze soubory. Jedná se o kapitolu virů, které se projevují nejrozmanitějším způsobem. Podle toho se dále dělí:

- **Přepisující vir** - přepíše část programu, který napadl vlastním kódem. Díky tomu je velmi nápadný, a proto nemá mnoho šancí se rozmnožit.
- **Link vir** – „přilepí" se (přilinkuje) k napadenému souboru, což umožní chod programu a zároveň činnost viru.

- **Doprovodný vir** – zkopíruje napadený soubor do souboru se stejným jménem, ale typu COM, a k tomu se připojí (vzniknou dva soubory, kde COM je nakažený). Vir využívá vlastnosti MS-DOSu, jenž nejprve spouští COM soubory.
- **Vir přímé akce** – provede destrukční akci a tím skončí. Například smaže celý disk a tím „zabije" i sám sebe.
- **Rezidentní vir** – načte se a drží v paměti a tím snadno napadne soubory, se kterými se pracuje.
- **Stealth vir** – vir s touto vlastností se umí načíst do paměti a kontroluje činnost systému. Pokud antivirový program kontroluje zavirovaný soubor, pak mu vir s touto vlastností vrátí kód před infekcí. Pro antivirové programy, jež nejsou vybaveny anti-stealth kontrolou, je vir prakticky nezjistitelný.
- **Zakódovaný vir** – je zakódován určitým proměnným algoritmem, takže jeho tělo je pokaždé jiné. Stejná je pouze dekódovací instrukce.
- **Polymorfní vir** – podobný jako předchozí – pro každý napadený soubor se kóduje jinak a vytváří i jinou dekódovací funkci. Takový vir nemá v žádném okamžiku v žádném z napadených souborů stejnou sekvenci svého kódu.
- **Fast infektor** – šíří se extrémně rychle díky tomu, že napadá soubory při spuštění i při jakékoliv manipulaci s nimi. Snadno se rozšíří a tím na sebe upozorní.
- **Slow infektor** – na rozdíl od předchozího se šíří velmi pomalu a opatrně.

BOOTVIRY

Jak již sám název kategorie virů napovídá, jedná se o viry, které mají spojitost se zaváděním systému (bootováním). Vir napadne boot sektor nebo partition tabulku pevného disku či diskety. Při zavádění systému je pak pohodlně aktivován a převezme kontrolu nad funkcemi systému. Jestliže vir obsadil partition tabulku, následně její obsah bezpečně uloží a vzhledem k systému, resp. požadavkům softwaru se partition tabulka jeví v pořádku.
Vir se šíří prostřednictvím boot sektoru disket. Aby byl počítač takovým virem napaden, musí se z nakažené diskety nabootovat (např. necháme-li v disketové mechanice nakaženou disketu a počítač spustíme).

MULTIPARTITNÍ VIRY

Boot viry se aktivují ihned při zavádění systému, ale k infekci se musí nabootovat z nakažené diskety, což jejich šíření omezuje. Souborové viry se šíří prostřednictvím souborů, což je pro jejich šíření výhodné, ale potřebují být aktivovány spuštěním. Kombinací a výhod obou typů virů využívají tzv. multipartitní viry. Infikují partition tabulku i soubory.

MAKROVIRY

Makroviry se objevily až s příchodem makrojazyků především v textových editorech a tabulkových procesorech. Zákeřnost makroviru spočívá v tom, že vir je přenášen a uložen v dokumentu. Opatrní uživatelé mohou omezeně kopírovat soubory a programy a dávat pozor na diskety. Kopírovat dokumenty je ale nucen téměř každý.
Nebezpečí makroviru spočívá v tom, že ovládne program i šablony a poté při určité operaci (například uložení souboru) bude spuštěno makro s destrukčními účinky (např. vymazání dokumentů). Zatímco s masovým příchodem operačního systému Windows ubývá rezidentních a souborových virů, makroviry představují v oblasti virů nastupující hrozbu.

JAK SE VIRY PRAKTICKY PROJEVUJÍ

Počítačový vir je program a jako takový se projevuje podle toho, jak byl naprogramován. Existují stovky způsobů, jak se viry projevují, počínaje výpisem nejrůznějších humorných hlášení na obrazovku (např."chybí olej v procesoru") až po destrukční viry.
Obecně můžeme projevy virů rozdělit na:

Obtěžující

Příznaky obtěžujících virů spočívají například ve výpisech nesmyslných hlášení na obrazovku, která se zpočátku mohou zdát humorná, ale pokud každých 5 minut počítač napíše, že je unavený, pak uživatel asi dlouho s nervy nevydrží. Viry mohou obtěžovat také záměnou kláves na klávesnici, takže něco jiného píšete a něco jiného se zobrazuje na obrazovce. Některé obtěžující viry zjistí, že je k počítači připojen modem, a klidně zavolají třeba na číslo 0609.... Při placení účtu se nepřestanete divit.
Fantazie programátorů takových typů virů je prakticky neomezená.

Destrukční

Destrukční viry vzbuzují určitý respekt již při vyslovení této kategorie. Základním úkolem takových virů je zlikvidovat data. Chytré viry pracují tak, že nezničí všechna data na disku, ale postupně zaměňují pouze určité byty nebo řetězce. Uživatel takový vir těžko odhalí a při dlouhodobém působení nakazí i záložní kopie. Jednoduché viry zničí okamžitě po napadení například obsah disku a tím vlastně zničí samy sebe.
Destrukční viry, stejně jako obtěžující, mohou být naprogramovány na určitou dobu (například pátek třináctého) nebo v souvislosti s určitou akcí v počítači.

Ostatní

Sem se řadí ostatní typy virů. Často se stává, že viry nejsou kvalitně napsané a že se dostávají do kolizí s jinými programy. Pak se z původně neškodného viru klidně může stát destrukční – a to vlastně náhodou.

ANTIVIROVÉ PROGRAMY

Proti virům je třeba se bránit. V dnešní době si již nemůže být jistý žádný uživatel počítače, který datově komunikuje alespoň částečně se svým okolím. Kromě opatrnosti jsou silným prostředkem proti virům antivirové programy. Dokáží nejen najít vir, ale většinou i „vyléčit" nakažený soubor tak, že po zásahu antivirového programu funguje správně a nemusí být celý smazán.

JAK PRACUJÍ ANTIVIROVÉ PROGRAMY

Současné antivirové programy používají různé techniky. Asi nejstarší a nejznámější je technika vyhledávání prostřednictvím vyhledávací sekvence. Většina virů má určitou specifickou sekvenci, podle které lze vir jednoznačně specifikovat (A1 00 10 B5 C2 00). Vir prohledává celý disk a soubory s takovou instrukcí označí za napadené. Při tvorbě antivirových programů je velmi obtížné najít takovou sekvenci viru, která zároveň není obsažena v žádném programu v počítači, protože by docházelo k falešným odhalením – antivirový program by mohl „falešně" považovat čistý program za vir.

Bohužel, programátoři virů znají antivirové techniky a snaží se vyhledávací metodu obejít. Velmi obtížné je hledání tzv. polymorfního viru, který mění svůj vlastní kód. První polymorfní viry se samy kódovaly, ale měly alespoň krátkou dekódovací instrukci, podle níž je bylo možné vyhledávací metodou odstranit. Dnešní polymorfní viry již umí průběžně měnit i dekódovací instrukci, takže jejich tělo může být v počítači několikrát, ale pokaždé vypadají jinak. Takové viry jsou pak prostřednictvím vyhledávací instrukce nezjistitelné.
I tuto lest programátoři antivirových programů zvládli. Antivirový program v sobě obsahuje emulátor strojového kódu, který dokáže rozbalit zakódovaný vir. Naprogramovat takovou instrukci je velmi obtížné, zvlášť když je vir pokaždé zakryptován jinak.

Každým rokem na světě vzniknou stovky nových virů. Od vzniku viru po vydání aktuálního antivirového programu uběhne poměrně dlouhá cesta – vir se musí rozšířit, tvůrci antivirového programu jej musí analyzovat a začlenit do nové verze, ta musí být vyrobena a distribuována k zákazníkům, zákazníci ji musí nainstalovat a teprve v tomto okamžiku ji použijí. Od vzniku viru uběhla spousta času a v okamžiku instalace již mohou existovat desítky dalších nových virů. Proto antivirové programy disponují funkcí tzv. **heuristické analýzy**.
Na rozdíl od pouhé detekce viru heuristická analýza sleduje programy tak, že emuluje (nahrazuje) instrukce programu, resp. zjišťuje, co sledovaný program s počítačem provádí, a na základě zjištění vyhodnotí, zda je to v pořádku, či nikoliv („spustí program pod svou kontrolou"). Napsat takový emulátor je velmi obtížné, ale pokud je naprogramován skutečně dobře, dokáže najít 70% nových neznámých virů.

Jednou z dalších technik antivirových programů je tzv. **kontrola integrity**. Antivirový program s testem integrity hlídá změny v systému, adresářích a systémových oblastech disku a na základě změn detekuje vir. Tato metoda je velmi spolehlivá, ale neumí zjistit konkrétní vir, pouze změnu v systému.

Každá technika má své silné a slabé stránky. Antivirové programy proto většinou používají kombinaci technik a tím zvyšují svou účinnost.

Zajímavost: Několikrát se stalo, že autor viru jej záměrně nechal nenápadně rozšířit a záhy nato začal prodávat antivirový program, kterým si finančně významně přilepšil – fantazie virových pisatelů je skutečně neomezená.

ANTIVIROVÉ PROGRAMY

Na softwarovém poli působí poměrně velké množství antivirových programů. V České republice se mezi nejznámější řadí **AVG**, AVP, AVAST nebo F-PROT. Antivirový program by měl používat každý, kdo je alespoň částečně nucen komunikovat prostřednictvím disket nebo jiného typu média s daty na jiných počítačích. Antivirovou kontrolu by měl uživatel provádět v pravidelných intervalech.

ESET SMART SECURITY, NOD 32, Avira, Kaspersky

INTERNET – NOVÝ DRUH VIROVÉHO NEBEZPEČÍ

V souvislosti s největší počítačovou sítí na světě - internetem - je možné obávat se napadení virem dvěma způsoby:

Stáhnutím nakaženého programu či souboru

Internet je kromě obrovské spousty informací i velkým zdrojem virů. Nikdy nemůžete vědět, zda program nebo soubor uložený na internetu není nakažen virem. Pokud stahujete z internetu program, před spuštěním jej v každém případě zkontrolujte antivirovým programem!

Před stahováním zejména programů do počítače je dobré ověřit, z jakého serveru je soubor stahován. Je pochopitelné, že servery velkých a „ověřených" firem si těžko dovolí dát na své stránky zavirovaný soubor. Naopak neznámé a freewarové servery se obvykle viry jen hemží.

Infikovaný e-mail

Bohužel, v poslední době se forma nakažených e-mailů stává jedním z nejnebezpečnějších typů virů vůbec. „Kvalitní" e-mailový vir je zákeřný v tom, že ani nemusíte vědět, kdy a že vůbec jste jej dostali. Přijde „zabalený" v běžné zprávě (e-mailu) a už pouhým otevřením takové zprávy dojde k aktivaci viru a infikaci počítače. Problém je v tom, že nemáte možnost poznat, zda je právě tato zpráva zavirovaná, či nikoliv, protože jediným vodítkem je odesílatel a předmět zprávy. Obvykle když zprávu otevřete, abyste zjistili její obsah, pak - pokud se jedná o vir - je okamžitě po otevření rozeslán na všechny další adresy, které nalezl v seznamu adres (například v Outlooku) – tím nechtěně zavirujete e-maily i všem, se kterými jste dosud komunikovali elektronickou poštou.

Reklamní a nevyžádané e-maily

(spam)

Pokud budete v budoucnu alespoň trochu používat e-mail, zcela jistě se setkáte s nevyžádanými e-maily. Jedná se většinou o e-maily nabízející určitý produkt nebo reklamu na nějaké internetové stránky. Takové e-maily vám přišly, i když jste si je nevyžádali a chodit vám budou i nadále. Je velmi pravděpodobné, že pokud takových e-mailů budete dostávat týdně či dokonce denně několik, budou vás časem určitě obtěžovat.

JAK BOJOVAT PROTI VIRŮM

- Každou neznámou disketu, kterou vkládáte do svého počítače, nejprve otestujte antivirovým programem.
- Nepouštějte ke svému počítači žádnou cizí osobu, zvláště pak ne náruživého hráče s balíčkem disket v ruce.
- Pravidelně zálohujte svá data. Pokud totiž vir zlikviduje celý disk, nic až tak vážného se nestane, jestliže máte důležitá data zálohována.
- Používejte antivirové programy. Pokud používáte antivirové programy, pravidelně je aktualizujte, protože stárnou rychleji než kterýkoliv jiný software.
- Buďte obezřetní. Většina virů se nějak projevuje. Ať je to delším zaváděním systému, podezřelým padáním programů, nebo jiným „neobvyklým" chováním.
- Soubory stažené z internetu před spuštěním zkontrolujte antivirovým programem.
- Podezřelou či nevyžádanou e-mailovou poštu z internetu ani neotevírejte a ihned mažte.
- Otevřete-li e-mail a zjistíte, že obsahuje soubor, který by tam být neměl nebo má „divný" název či koncovku, zavřete tento e-mail a smažte jej.