

Ochrana počítače před viry

01 - Počítačové viry Antivirové programy

Viry

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.

Historie virů

Historie počítačových virů začíná na počátku 80. let 20. stol., 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 pohazením, protože autoři virů znají a předávají si mezi sebou moderní techniky, které virům umožňují měnit svůj vlastní kód, ukrywají 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 tzv. antivirové programy, které vir dokáží vyhledat a odstranit.

Je jasné, že žádný antivirový program není a ani nemůže být tak dokonalý, aby našel 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.

Jak se viry šíří (a jak tomuto šíření předejít)

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 mimo jiné následujícími způsoby:

- **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**.

Prevence: Nikdy nespouštějte program, o kterém nevíte, co je zač a z jakého zdroje pochází. Pokud je program součástí ověřeného CD ze seriózní firmy, nemusíte se obávat. Pokud ale dostanete např. disketu od kamaráda, rozhodně ji nejprve otestujte antivirovým programem. Už vůbec nespouštějte programy stažené z „pochybných“ serverů z internetu - pokud program spustit chcete, pak opět výhradně po ověření antivirovým programem.

- **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). Pokud pak „nevinně“ otevřete např. dopis od kamaráda, spustí se i vir, který v počítači začne páchat spoustu „nekalostí“ bez vašeho vědomí.

Prevence: V programech, které používáte pro editaci dokumentů či tabulek, zakazte automatické spouštění maker. V takovém případě se po otevření nakaženého souboru program (např. Word a Excel) obvykle zeptá, zda si opravdu přejete otevřít tento soubor, i když obsahuje makra. Už v této fázi by vám to mělo být podezřelé - soubor raději neotevírejte. Viry jsou totiž tak chytré, že stačí pouze první otevření nakaženého souboru a vir si zajistí, že program se již podruhé ptát nebude. Proto pozor na neuvážené spouštění souborů s makry!

- **Elektronická pošta (e-mail)** – v poslední době bohužel nejčastější případ virových invazí. Vir je přenášen jako samospustitelná příloha e-mailu, takže jakmile dojde nová

Ochrana počítače před viry

01 - Počítačové viry Antivirové programy

zpráva, stačí ji pouze otevřít a vir se aktivuje. Viry tohoto typu jsou zákeřné, často přicházejí pod zajímavým názvem (předmětem) ze zfalšované adresy. Například z adresy Microsoft Support (podpora Microsoftu) přijde e-mail, že si máte upgradovat váš počítač. Pokud tak učiníte, svůj počítač nakazíte.

Prevence: Tento nový druh virů je opravdu velmi zákeřný. Obranou proti nim je pouze stálá a velká opatrnost. V žádném případě neotvírejte e-maily, které obsahují přílohu a jsou poslány z vám neznámé adresy, ihned je smažte (pozor, nejen vyhodte do koše, ale opravdu smažte). Rovněž neotvírejte e-maily, které sice přišly z vám známé adresy, ale obsahují podezřelé přípony. Většina moderních antivirových programů již obsahuje i tzv. *mail scan*, tj. v reálném čase se každý právě přichozí e-mail okamžitě zkontroluje a v případě, že je nakažen, ihned to ohlásí uživateli a nabídne smazání takového e-mailu.

- **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.

Prevence: Nikdy nebootujte (nezavádějte operační systém) z vám neznámé diskety. Právě tímto způsobem se viry šíří. Tento typ viru byl populární hlavně v dobách kralování operačního systému MS-DOS, dnes se již nevyskytuje tak často.

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 kapitoly 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-DOS, jenž nejprve spouští **COM** soubory.
- **Vir přímé akce** – provede destrukční akci a tím skončí. Například smaže celý disk a tím 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 dekodovací instrukce.
- **Fast infector** – 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.
- **Polymorfní vir** – podobný jako předchozí. Pro každý napadený soubor se kóduje jinak a vytváří i jinou dekodovací funkci. Takový vir nemá v žádném okamžiku v žádném z napadených souborů stejnou sekvenci svého kódu.
- **Slow infector** – na rozdíl od předchozího viru se šíří velmi pomalu a opatrně.

Ochrana počítače před viry

01 - Počítačové viry Antivirové programy

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. 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. necháte-li v disketové mechanice nakaženou disketu a počítač spustíte).

Multipartitní viry

Bootviry 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 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**. Poté při určité operaci (např. uložení souboru) bude spuštěno makro s destruktivními 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 destruktivní viry. Obecně můžeme projevy virů rozdělit na:

Obtěžující

Příznaky obtěžujících virů spočívají např. 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 škodlivé kódy a skripty (tzv. **dialery**) zjistí, že je k počítači připojen modem, a klidně zavolají třeba na číslo 0609... Při placení účtu se nestačíte divit. Fantazie programátorů takových typů virů je prakticky neomezená.

Destrukční

Destrukční viry vzbuzují určitý respekt již při vyslovení této kategorie. Jejich základním úkolem 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. Při dlouhodobém působení se nakazí i záložní kopie. Jednoduché viry zničí okamžitě po napadení např. obsah disku a tím vlastně zničí samy sebe. Destrukční viry, stejně jako obtěžující, mohou být naprogramovány na určitou dobu (např. 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 vir destruktivní – a to vlastně náhodou.

Ochrana počítače před viry

01 - Počítačové viry Antivirové programy

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, zvláště pak prostřednictvím e-mailu. Kromě opatrnosti jsou silným prostředkem proti virům antivirové programy. Dokáží nejen najít vir, ale většinou i „vyléčit“ nakažený soubor tak, že poté 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). Antivir 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. Jinak by mohlo dojít k falešným odhalením – antivirový program by mohl „falešně“ považovat čistý program za vir.

Programátoři virů bohužel 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, zvláště 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 uběhne 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.

Antivirové programy

Na softwarovém poli působí poměrně velké množství antivirových programů. V České republice se mezi nejznámější řadí **AVG, Kaspersky Antivirus, AVAST, Norton Antivirus, NOD32** nebo **F-SECURE**.

- ! Antivirovou kontrolu by měl uživatel provádět v pravidelných intervalech a je nutné pamatovat na pravidelnou aktualizaci virové databáze u instalovaného antiviru, nejlépe
- aktualizací po internetu ze serveru výrobce antiviru.