Počítačové viry

Jednou z oblastí výpočetní techniky, která doznala značnou změnu s nástupem internetu, je oblast počítačových virů. Klasické viry stylu první poloviny devadesátých let minulého století, kterým trvalo týdny i měsíce než se rozšířily po celém světě, ustoupily do pozadí. Pokud tehdy uživatelé vůbec měli antivirové programy, stačilo, když je aktualizovali jednou měsíčně. Místo virů se stále více objevují červi, kteří dokážou zaplavit svět pomocí internetu během několika hodin, a které mají pro své škodlivé působení právě jen hodiny, maximálně dny, protože jsou jim „v patách“ antivirové programy, které uživatelé mohou také díky internetu velmi snadno aktualizovat. Na místo „geniálních“ programátorů, hledajících slabá místa v technickém a programovém vybavení počítačů pro své většinou nekalé záměry, nastupují programátoři často jen průměrní, kteří se zaměřují nejen na slabá místa operačních systémů, především síťových, ale také na jiný slabý článek informačních systémů – člověka – a nastupuje tak nová technika útoku – sociální inženýrství - zneužívající především nepozornosti, nedůslednosti uživatele a také klamu a podvodu, nejen za účelem poškozování cenných dat, ale také pro jejich získání pro nelegální účely.

Ačkoliv v dalším textu budou popsány i jiné formy škodlivého kódu, které navíc stále více nabývají na významu než klasické viry, bude užíván díky „tradici“ pojem **počítačový virus,** který zde bude chápán v širším významu, jako veškerá forma škodlivého kódu.

Viry a jejich třídění

Viry jsou programy, které představují nejznámější a nejčastější formu počítačové infiltrace. **Počítačová infiltrace** je jakýkoli neoprávněný vstup do počítačového systému, do jeho souborů, programů apod.

Třídění virů

Viry se obvykle dělí podle několika hledisek. Znalost rozdělení virů přispívá k celkové informovanosti uživatele o virech a k jeho schopnosti napadení viry očekávat a předvídání možných důsledků činnosti virů, i když konkrétní virus či jeho mutaci nezná. V dalším textu půjde také o úplnost, takže budou popsány i technologie dnes už také poněkud exotické.

podle způsobu šíření

Počítačový virus

Viry se vyznačují tím, že:

- Svou **činnost** obvykle provádějí **bez vědomí** nebo přání uživatele.

- Mají schopnost **replikace (množení)**. To probíhá tak, že zapisují svůj kód nebo jeho funkční část do jiných programů nebo určitých míst na paměťovém médiu. Virus je schopen zapisovat svoji kopii nebo odvozenou kopii a tato kopie je schopna infikovat další části systému podobným mechanismem, jako její originál.
- Velká skupina virů v sobě obsahuje **rutiny s nějakou destruktivní činností.** Škála destruktivních činnosti je široká a závisí na typu viru a jeho mutaci. Typické ničivé akce jsou vymazávání souborů, přeformátování disku, modifikace dat, přepis tabulky rozdělení disku, zničení této tabulky, označování sektorů za vadné, přepsání boot sektoru aj.
- Viry obsahují techniky, které mají za cíl umožnit viru setrvat v systému co nejdéle. Z nichž základní je **sebeidentifikace.** Viry někdy obsahují rutiny pro rozpoznání, zda soubor jím již byl napaden. Viry jsou koncipovány tak, aby již napadené soubory znovu neinfikovaly, protože by tak způsobovaly neúnosný růst délky souboru a tak upozornily na změny v souboru a usnadnily své odhalení.

Virus lze tedy definovat (s určitým zjednodušením):

Počítačový virus je spustitelný nebo interpretovatelný program, který je schopen sám sebe připojovat k jiným programům a dále se z nich (bez vědomí uživatele) šířit.

Zatím známe tyto objekty, které **mohou být napadeny virem**:

1. **Spustitelné soubory – programy.** Obvykle mají přípony .EXE, .COM nebo .SYS. Jsou to však třeba i překryvné moduly (.OVL) nebo šetřiče obrazovky (.SCR).
2. **Systémové oblasti** - Partition tabulka nebo boot sektor pevného disku a boot sektor diskety. Tyto systémové oblasti obsahují kód, který je vykonáván při startu počítače.
3. **Dokumenty, které mohou obsahovat makra** – zejména texty napsané v Microsoft Wordu, tabulky z Excelu, prezentace vytvoření PowerPointem, databáze z Accesu aj.

Objekty, ve kterých se **viry nešíří** (i když to třeba i některé časopisecké články tvrdí):

- **CMOS paměť.** Tato paměť slouží k uchování informací o konfiguraci počítače. Virus může tuto paměť smazat nebo v ní změnit některé údaje, ale nemůže ji použít pro umístění svého kódu. Brání tomu nejen její malá velikost, ale hlavně to, že nemůže obsahovat spustitelný kód.
- **Datový soubor.** Samozřejmě, že viry se mohou usídlit v libovolném souboru, ale např. v obrázku by byly snadno odhalitelné a ztratily by schopnost se šířit, protože by se nemohly spustit. Výjimkou jsou už zmíněné dokumenty, které obsahují makra.

Trojský kůň

Jsou programy, které mají účinky podobné virům**.** Tyto programy se obvykle tváří neškodně. Během určité doby se rozšíří (např. kopírováním programů, záměrným rozšiřováním elektronickou poštou apod.). Programy jimi napadené lze normálně používat. Škodlivou akci provedou viry jen při splnění určitých podmínek. Často se aktivují podle určitého systémového času (např. pátek třináctého). V tu dobu provedou nějakou nebezpečnou akci. Některé z nich jsou určeny přímo proti některým programům, mohou např. měnit jejich konfiguraci. Velmi nebezpečnou skupinou troj-

ských koňů jsou programy, které vykrádají hesla či umožňují vzdálenou kontrolu počítače.

Backdoor (zadní dvířka)

Backdoory jsou aplikace, které počítač „otvírají“ útočníkům. Spíše než typ je to vlastnost softwaru. „Čistokrevné“ backdoory jsou vzácné, většinou existují v kombinaci s jinými aplikacemi – zejména s trojskými koni či počítačovými viry.

Síťový červ

Jde o novou skupinu programů ještě nebezpečnějších než viry. Zatímco viry se množí uvnitř počítače, červ je v počítači často v jediném exempláři, avšak usiluje o šíření po síti prostřednictvím síťových médií, především elektronické pošty. Jeho nebezpečnost je v ohromné rychlosti šíření. Červ se může rozšířit po celém světě za 24 hodin. Zatímco vir potřebuje pro své šíření hostitelské aplikace (s výjimkou doprovodných virů – viz dále), červ je zpravidla škodlivým kódem sám o sobě.

Žertovný prográmek

Toto není vir, nemá jeho znaky - zejména replikaci. Přesto žertovné prográmky mohou mít určitě obtěžující chování a jejich účinek někdy způsobí nutnost restartu počítače, což u některých systémů může způsobovat problémy, proto i na tyto programy se zaměřují antivirové programy.

Podle času projevu

Viry aktivující se okamžitě

Jak již bylo uvedeno, vzhledem k možnosti poměrně rychle aktualizovat antivirový program mají viry krátkou dobu na svou činnost. Proto se dnes většina virů aktivuje ihned po vstupu do počítače.

Viry aktivující se k určitému datu

Takovéto viry byly charakteristické právě začátkem 90. let 20. stol., kdy antiviry teprve začínaly a viry se aktivovaly často s nějakým datem. Doba mezi vytvořením viru a dnem aktivace byla přiměřeně dlouhá, aby se vir stačil rozšířit a přiměřeně krátká, aby tvůrci antivirů nestačili zareagovat.

Viry aktivující se při nějakém úkonu

Některé viry se aktivovaly např. při osmém restartu nebo při stisku určité kombinace kláves.

Podle nebezpečnosti

Viry nedestruktivní

Do této skupiny patří většina dnešních škodlivých kódů. Vzhledem ke změněným podmínkám šíření virů nemají tvůrci škodlivých kódů zájem na přítomnost svého programu v počítači upozorňovat nějakým nápadným upozorněním a už vůbec ne

na celkové destrukci operačního systému a dat v počítači, protože to znamená „vyklizení dobytých pozic“.

Viry destruktivní

Jsou viry s určitou destruktivní rutinou v jádře (mazání souborů, poškozování dat apod.). Je možné je rozdělit na viry s destrukcí záměrnou a nezáměrnou (např. pro chyby v kódu), uživateli jsou však vzhledem k důsledku působení viru původní záměry tvůrce celkem lhostejné.

Podle napadených oblastí

Boot viry

Napadají pouze systémové oblasti. Infikují boot sektor disket a většinou také tabulku rozdělení pevného disku nebo jeho boot sektor. Po své aktivizaci většinou infikují boot sektor každé diskety zasunuté do počítače. Šíří se pouze při pokusu o nastartování systému z této diskety. Není však podmínkou, aby tato disketa byla systémová, stačí pouze tuto disketu zapomenout v mechanice A. Doporučuje se proto nastavit BIOS Setup tak, aby nejprve byl prováděn pokus o boot z pevného disku a teprve potom z diskety.

V boot sektoru není obvykle celé tělo viru, je zde jen spouštěcí mechanismus (příkaz skoku na výkonnou část viru). Boot virus se instaluje do paměti jako rezidentní a začne infikovat boot sektor disket, které nejsou chráněny proti zápisu. Boot sektor viry, které se zaměřují na infikování systémového disku, infikují disk hned při zavedení z diskety nebo později při prvním přístupu na disk.

Bootových virů bylo sice asi dvacetkrát méně než souborových, přesto se s nimi uživatel setkal častěji než se souborovými, protože disketa je médium, které si uživatelé často vyměňovali. Operační systém DOS byl pro tyto viry vhodným hostitelem, protože základní systémové služby se používaly velmi často. V podmínkách 32bitových operačních systémech jsou podmínky pro šíření boot virů mnohem horší, protože boot virus je většině případů při startu systému ihned odhalen.

Souborové viry

Napadají spustitelné programové soubory s tím, aby spuštěním hostitelského programu se aktivoval virus. Podle toho jak zacházejí se se svou „obětí“ tedy hostitelským programem je můžeme dělit dále na:

- **Viry přepisující,** které svým zásahem zničí či poškodí hostitelský program. Když je takový program spuštěn, je aktivován virus a program sám není schopen činnosti, což je podezřelé i nezkušenému uživateli. Díky tomu je možnost šíření těchto virů krajně nepravděpodobná. Viry proto svoji „aktivitu“ maskují nějakým (více či méně nejapným) chybovým hlášením, které má „vysvětlit“ neschopnost spuštění hostitelského programu.
- **Nepřepisující (**též **link) viry** hostitelský program neničí. Tyto soubory se připíší k hostitelskému souboru (vzácně i do jiné oblasti disku). Protože hostitelský program nebyl zničen, vykonává svoji obvyklou funkci, proto se často uživatel o viru dozví, až když se projeví nějakým destruktivním nebo propagandistickým (zpráva na obrazovce) způsobem. Protože tyto viry svou přítomností prodlužují hostitelské programy, mívají některé „schopnější“ viry vlastnost sebeidentifikace, která brání opakovanému napadání hostitelského programu a neúměrnému zvětšování hostitelského souboru.

- **Duplikující (množivé** též **doprovodné) viry** napadají soubor s příponou .EXE tak, že vytvoří nový soubor se stejným jménem, avšak s příponou .COM a do něj umístí svoje tělo. Protože operační systém při shodě jmen spouští nejprve programy s příponou .COM, spouští virus a nikoli původní program. Doprovodný virus je často generován fágem.
- **Fágy** - pro jejich název se odborníci inspirovali skutečnými fágy, které nahrazují infikované buňky svým vlastním genetickým kódem. Počítačové fágy nahradí spustitelné soubory svým vlastním kódem a často generují doprovodný kód. Fágy jsou silně destruktivní viry, protože ničí každý napadený soubor.
- **Mezerové viry** využívají volných míst hostitelských programů, do kterých se zapisují, aniž by měnily celkovou délku hostitelských souborů.
- **Clusterové viry** nezapisují své kódy do datové oblasti disku, a místo toho modifikují pouze odkazy adresářové struktury, tak aby ukazovaly na kopii těla viru umístěnou např. na konci disku.

Makroviry

Jsou sice historicky nejmladší, představují však velkou hrozbu**.** Jejich vznik byl inspirován tím, že když už někdo testuje na viry, tak testuje spustitelné soubory a nikoli data. A dále, že uživatelé vědí, že spustitelné programy jsou nebezpečně, proto je obvykle volně nešíří, avšak data kolují pro firmách zcela normálně, neboť je to pro chod firem nezbytné. Makroviry napadají všechna prostředí, kde lze spustit MS Word, Excel, PowerPoint či Access. Jsou to programové kódy napsané v makrojazyce dané aplikace. Oproti normálním makrům obsahují však samospouštěcí rutiny, které způsobují, že makra se chovají stejně jako viry. Jejich nebezpečí je to o větší, že jsou často nezávislé na platformě a operačním systému.

Podle umístění v paměti

Rezidentní viry

Tyto viry se při spuštění infikovaného programu většinou nelegálně nebo pomocí služeb operačního systému umístí jako běžné rezidentní programy do paměti. Poté jsou schopny napadat každý nově spuštěný program. Souborový virus se usídlí v paměti po prvním spuštění souboru. Boot virus se zavede do paměti při prvním zavedení z infikovaného boot sektoru. Virus zůstává v paměti, dokud není počítač vypnut.

Rezidentní viry byly těžko detekovatelné. Po zapnutí počítače jsou okamžitě schopny infekce souborů či boot sektoru nebo tabulky rozdělení disku. Velkou výhodou rezidentního viru je, že si nemusí sám hledat programy vhodné k napadení. Stačí mu sledovat, se kterými soubory uživatel pracuje a může na ně pak útočit.

V podmínkách 32bitových systémů závisí schopnost jejich přežití v operační paměti závisí na jejich kódu. Obecně platí, že čím je virus sofistikovanější a čím neobvyklejší příkazy používá, tím je jeho šance na přežití v paměti při startu 32bitového operačního systému menší.

Nerezidentní viry

Nepotřebují být trvale přítomny v paměti. Aktivují se spuštěním hostitelského programu. Pak převezmou řízení jako první, provedou svoji činnost (obvykle replikaci) a pak vrátí řízení hostitelskému programu. Jsou to vždy souborové viry.

Podle způsobu chování

Stealth viry

Pokud jsou aktivní, jsou schopny ovlivnit chování celého systému tak, aby co nejdůkladněji za maskovaly svou činnost v počítači. Využívají pro to několik způsobů. Například pokud je takový virus rezidentní v paměti, vrací při pokusech o zjištění délky souboru jeho délku před infikováním. Jiný způsob zamaskování své činnosti je schopnost viru dočasně odstranit infikovanou část a tím zabránit správné identifikaci antivirovým programem. Jako stealth vir se může projevovat i bootsektorový vir, který dokáže původní obsah tabulky uložit do některého volného sektoru a při pokusu o čtení tabulky (např. antivirovým programem) zajistí, aby nebyla čtena skutečná tabulka, ale její původní obsah.

Polymorfní viry

Polymorfismem mohou být vybaveny i starší viry. Zatímco klasické viry zachovávají ve všech kopiích vždy stejný kód, polymorfní vir nemusí mít stejný ani jeden bajt, protože v souboru se zakóduje. Před spuštěním polymorfního viru se nejprve aktivuje jeho část, která obsahuje algoritmus pro dekódování zbylé části. Detekce těchto virů je obtížná, protože nelze užít skenovacích programů, které vyhledávají v souborech řetězec, který je charakteristický pro určitý vir. Antivirové programy proto spíš vyhledávají určité instrukce, které jsou charakteristické pro chování virů. Starší zakódované viry měly pouze jednu stále stejnou dekryptovací funkci u polymorfních virů si vir pro každý napadený soubor vytváří zcela jinou dekryptovací funkci. Také makroviry mohou být polymorfní.

Retroviry (odvetné viry)

Speciální případem jsou viry, které se řídí heslem, že „nejlepší obrana je útok“. Zaměřují se proto na znemožnění činnosti některých konkrétních antivirových programů či na znemožnění některých obecných funkcí antivirů. Napadají soubory antivirových programů, vypínají rezidentní hlídače virů apod.

Tunelující viry

Vyhledávají původní vektory přerušení a volají je přímo, čímž odcházejí aktivitu monitorujících programů, které v systému detekují pokusy o volání vektorů přerušení. Tuto techniku však používají i některé antivirové programy, aby obešly neznámé a neidentifikovatelné viry, které mohou aktivní v době jejich spuštění.

Některé rozšířené omyly

Mezi **rozšířené omyly** patří zejména:

- **Virus může zničit i hardware.** Některá starší zařízení skutečně bylo možno ovlivňovat softwarovými prostředky, takže docházelo k poškození (např. nastavování nesmyslných synchronizačních frekvencí monitorů, které mohlo vést k tepelnému přetížení). U nových zařízení toto nebezpečí nehrozí. Trochu škodolibě se říká, že zařízení, které se takto nechá zničit, si ani nic jiného nezaslouží a pak si lze těžko představit ladění takovéhoto viru, asi by bylo pro programátora dost nákladné.

- **Virus přežije v paměti i reset počítače.** Stisk kláves Ctrl-Alt-Del může virus přežít, avšak restart tlačítkem na panelu softwarově ošetřit nelze.
- **Virus z napadené diskety zaútočí i při pouhém pohledu na ni (např. příkazem DIR).** Není to pravda, virus se aktivuje spuštěním infikovaného souboru nebo pokusem o zavedení systému z infikované diskety (např. ze zapomenuté v mechanice A: při startu počítače). Výjimkou jsou makroviry, kterým stačí načtení infikovaného dokumentu do příslušného programu (např. Wordu).
- **Virus napadne i disketu chráněnou proti zápisu.** Viry jsou zde bezmocné a proto drze žádají uživatele, aby zápis na disketu povolil. Autoři virů spoléhají na to, že těch nezkušených uživatelů, kteří to udělají, bude dost.

Při provozu počítačů se lze setkat i s **následujícími problémy:**

- **Programátorské chyby,** které způsobí nefunkčnost programu, která může připomínat působení viru.
- **Kolize softwaru či hardwaru.** I přes proklamace tvůrců zajistit stoprocentní kompatibilitu lze jen těžko, takže může docházet ke kolizím, které evokují působení virů.
- **Poruchy hardwaru,** svými projevy připomínají působení virů. Při provozu počítače lze zaregistrovat poruchu pevného disku. Pokud dochází k podivnostem na obrazovce, může za to virus, ale také závada grafické karty.
- **Poškození softwaru** mohou způsobit viry, ale také např. nekorektní ukončení programu.
- **Falešné poplachy,** i když autoři antivirových programů se snaží jejich výskyt minimalizovat, přesto je nelze zcela vyloučit.

Působení virů

- **Efekty.** Autoři virů na straně jedné usilují o maximální utajení činnosti viru, na straně druhé se chtějí „zviditelnit“ a proto viry většinou přinášejí různě „duchaplné“ efekty, jejichž start je buď vázán na určité datum nebo na nějaký spíše náhodný stav. Efekty nemají za cíl přímou destrukci a ani většinou ani uživatele příliš neobtěžují, spíše překvapují.
- **Obtěžující chování.** Některé viry např. převezmou kontrolu nad klávesnicí a obtěžují uživatele různými záměrnými překlepy. Vážná situace nastává, když vir manipuluje s modemem a přesměrovává hovory na různá čísla – např. na tísňové volání či do některých exotických zemí, což může výrazně negativně ovlivňovat výši poplatků za telefon.
- **Přímá záměrná destrukce,** která může být razantní – např. přepsání celých oblastí disku nesmysly, což při kvalitním zálohování nebývá až taková tragédie – či nenápadná, kdy uživatel dlouho nepozoruje žádné změnu ve svých souborech. Např. makroviry zaměřené na tabulky v nich mění některé položky.
- **Něco je špatně.** Viry ač nemají prvoplánově nějakou přímou destrukci, se dostávají do konfliktů s programy výsledkem je různé neobvyklé chování počítače (např. „tuhnutí“). Ze všech neobvyklých projevů počítače však nelze vinit viry, často to způsobuje různá softwarová a hardwarová nekompatibilita uvnitř počítače.

Sociální inženýrství a počítačové viry

Zatímco v počátku existence virů vyžadovala jejich tvorba hluboké znalosti informačních technologií a hardwaru, dnes je situace už trochu jiná, viry lze tvořit při podstatně nižší úrovni znalostí, neboť existují jejich generátory a na internetu je řada „tipů a triků“. Protože už existuje na počítačích řada zabezpečení, nastává úkol pro tvůrce virů přijít na to, jak přimět uživatele, aby přestal být opatrný, a to je úloha soci-

álního inženýrství. Sociální inženýrství působí na uživatele nejrůznějšími metodami – např. poukazem na peněžní částku neexistující objednávky, přesvědčováním uživatele, že pro správný chod programu je nutno vypnout antivirové testování nebo zasíláním zdánlivě důvěryhodných automatických odpovědí na e-maily apod.

Hoax

Hoax je smyšlená zpráva, která „varuje“ před neexistujícím virem a nutí uživatele ji šířit dál a tím zatěžovat síť, což ve svých důsledcích je někdy horší než působení samotného viru. Mezi obvyklé znaky patří: varování před novým virem, který je vždy destruktivní, je neznámý a není proti němu ochrany; důvěryhodnost má zvýšit jméno některé známé počítačové firmy, neobsahuje však kontakt na antivirovou firmu a pokud vůbec nějaký kontakt obsahuje je to zpravidla nějaké telefonní číslo v zahraničí, kam běžný uživatel stejně nezavolá; samotná manipulace s e-mailem je už nebezpečná; zpráva vždy obsahuje výzvu k dalšímu šíření.

Literatura:

[1] Počítačové viry a Vy – součást manuálu programu AVG
[2] Bezpečnost dat – příloha Softwarových novin č 1/2001
[3] Přibyl, Tomáš a kol.: Počítačové viry v roce 200x, příloha PC WORLD (ročníky 2002, 2003 a 2004)