Počítačové viry
známé a neznámé

1. díl – Úvod do problematiky & souborové viry

PETR NÁDENÍČEK

O počítačových virech se už dnes nemluví tolik jako tomu bylo dříve. Čas od času sice média informují o „nějakém novém hrozivém viru“ nebo třeba o tom, že „byl odhalen a zadržen virový pisálek XY“. Z globálního hlediska ale viry nejsou tak ožehavým tématem, jak tomu bylo na přelomu tisíciletí, kdy jsme byli svědky mnoha rozsáhlých epidemií e-mailových a síťových červů.

Nezaujatý pozorovatel tak může lehce získat dojem, že počítačové viry už nejsou tak palčivým problémem a potažmo se tedy může cítit v relativním bezpečí. Opak je ale pravdou. Počítačové viry stále žijí s námi, respektive s našimi počítači, jsou stále rafinovanější a hned tak nás na pokoji určitě nenechají. A hlavně – pořád nám mají co ukázat!

Jak šel čas…

Pokud se podíváme do historie, zjistíme, že první výskyty škodlivých kódů byly zaznamenány někdy kolem roku 1986. Tehdy šlo zejména o viry napadající zaváděcí sektory disket (a později pevných disků) a první parazitické souborové viry infikující spustitelné soubory. O něco později se s příchodem Windows 95 objevily první makroviry a 32bitové souborové viry. Všechny tyto škodlivé kódy byly při svém šíření odkázány hlavně na přirozenou výměnu dat mezi uživateli na fyzických médiích. Doba, kterou potřebovaly k propuknutí epidemie, tak byla velmi dlouhá – často až několik měsíců.

Kolem roku 2000 se začaly objevovat první e-mailoví a síťoví červi, kteří postupně zcela ovládli stále více se rozvíjející internet. Mnozí z nás ještě určitě mají v živé paměti první opravdu velkou epidemii e-mailového červa Iloveyou v roce 2001. V době své největší slávy představovali e-mailoví červi asi 90 % všech škodlivých kódů „In the Wild“ a přední stupínky statistik neopouštějí ani dnes.

V posledních několika letech pomyslné žezlo postupně přebírají další škodlivé kódy, označované jako spyware. Zdaleka však nejde o změnu revoluční, ale spíše o pozvolné prorůstání „stávající vládnoucí vrstvy s nově příchozími“. Běžně se tak nyní můžeme setkat s e-mailovým červem, který za účelem špehování uživatele nasazuje do infikovaného systému různé keyloggery nebo v něm otevírá zadní vrátka. Zcela aktuálním trendem jsou pak škodlivé kódy typu „BOT“, které z infikovaného počítače dělají poslušného vykonavatele příkazů vzdáleného útočníka – tzv. „zombie“. Takový počítač může být lehce zneužit k provádění DoS útoků nebo k šíření spamu či jiného nelegálního obsahu.

Asi největším hitem současnosti jsou potom mobilní viry, resp. mobilní červi, kteří si postupně prošlapávají cestu na chytré mobilní telefony. Podobně jako v počítačovém světě mají monopol viry pro MS Windows, v mobilním světě jsou to viry pro OS Symbian. Nutno ale říci, že nebýt vydatné pomoci uživatelů, neměly by viry ani zde valnou šanci na úspěch.

Pokud bychom si měli zahrát na proroky a odpovědět na otázku, jaké škodlivé kódy se objeví v blízké budoucnosti, mohli bychom parafrázovat památný výrok Járy Cimrmana a říci, že „budoucnost patří rootkitům!“ Škodlivé kódy na bázi tzv. nástrojů „rootkit“ se dokáží zavrtat do operačního systému velmi hluboko a dokonale se tak skrýt nejen před zraky uživatele, ale také (a o to jim především jde) před zraky antivirového programu. Již dnes se na virové scéně začínají objevovat první vlaštovky. Poněkud uklidnit nás ale může informace, že antivirové firmy o tomto trendu vědí a usilovně pracují na vývoji nástrojů, které nás před těmito škodlivými kódy v budoucnu ochrání.

A jak na tom jsme?

Podle oficiálních virových statistik, které zveřejňuje společnost F-Secure (přední světová antivirová firma), překročil v roce 2004 celkový počet různých exemplářů škodlivých kódů číslo 100 000. Pokud se podíváme na informace ostatních firem, zjistíme, že se příliš neliší. Odborníci zabývající se analýzou virů přitom každý den hlásí v průměru deset nových virů či jejich variant. V některých obdobích zvýšené aktivity pisatelů virů, jako byla třeba „válka červů“ v minulém roce, je tento počet ještě daleko vyšší.

Z hlediska schopností současných škodlivých kódů je situace ještě o něco hrozivější. Odborníci již zcela otevřeně hovoří o tom, že počítačové viry vstoupily do služeb organizovaného zločinu. Zatímco v minulosti byly škodlivé kódy vytvářeny převážně „pro zábavu“ nebo se jednalo o produkty mladistvé nerozvážnosti různých studentů a zneuznaných programátorů, dnes jsou tito lidé najímáni různými mafiemi a zločinnými gangy, které se specializují na nové formy „kybernetického zločinu“. Řada dnešních škodlivých kódů je tedy poměrně úzce zaměřena na různé činnosti, které těmto skupinám přinášejí nemalý ekonomický prospěch. Typickým příkladem je krádež hesel a jiných zneužitelných informací, ovládání infikovaných systémů s následným zneužíváním pro šíření spamu, nebo třeba phishingové útoky s cílem získat údaje ke kreditním kartám… Jak je tedy vidět, končí veškerá legrace…

Přijměte tedy pozvání na malý výlet do světa škodlivých kódů a vydejme se po stopách těch minulých, těch současných a možná i těch budoucích. Začneme přímo u samotných kořenů.

Souborový virus – druh na vymření

Jak jsme již uvedli v našem malém výletu do historie, souborové viry patří k prvním škodlivým kódům, které se kdy vůbec objevily. Typický souborový virus je definován jako škodlivý kód, který dokáže svoje programové instrukce přidat do hostitelské aplikace nebo souboru (infikovat ho) a tímto způsobem se dále šířit.

V praxi jsme se zprvu mohli setkat se souborovými viry pro operační systémy DOS. Typický virus fungoval tak, že se po spuštění infikované aplikace usídlil v paměti (jako rezidentní aplikace), případně se navázal na určité vektory přerušení a následně infikoval všechny vhodné soubory, ke kterým se dokázal nějakým způsobem dostat (spouštěné aplikace, soubory v určitém adresáři apod.).

Možná si pamatujete, jak před příchodem nové platformy Windows 95 představitelé Microsoftu proklamovali brzký konec virů, které neměly mít v novém operačním systému místo. Místo toho, aby nová technologie vzala autorům virů „vítr z plachet“, otevřela jim nové obzory. Ve stejném roce, kdy byly uvedeny nové Windows, jsme se mohli seznámit s makroviry, které přišly s novými kancelářskými programy balíku Office, jež nově obsahovaly makra. Do té doby relativně bezpečné formáty dokumentů se tak rázem staly potencionálním nositelem infekce, přičemž některé makroviry dokázaly infikovat i více než jeden typ dokumentů Office (tzv. cross-makroviry). I když to tehdy vypadalo, že tento typ virů čeká zářná budoucnost, postupem času téměř vymizely.

Autoři virů se však nehodlali smířit s tím, že by souborové viry neměly na nové platformě šanci uspět. Neuplynul ještě ani rok a světlo světa spatřily nové 32bitové viry pro Windows. Nové prostředí sice neumožňovalo využití starých metod, které fungovaly v prostředí DOSu, ale i s tím si tvůrci virů s úspěchem poradili. Typický souborový virus pro Windows se tedy v systému spouští jako služba, aby „všechno zpovzdálí sledoval a ve správnou chvíli se do věci vložil“, tzn. infikoval další vhodný soubor.

V současném světě škodlivých kódů jsou souborové viry opravdovou Popelkou. Je to zejména proto, že svým tvůrcům nemohou nabídnout tolik jako současní e-mailoví a síťoví červi, kteří se dokáží šířit daleko rychleji a jsou tedy daleko atraktivnější.

Důkazem toho je i skutečnost, že poslední známý „klasický“ souborový virus se objevil nedávno, takřka po dvouleté přestávce. Jedná se o Win32 parazitický virus Tanga, který se dokáže potají infiltrovat do spustitelných EXE souborů (přesněji Win32 PE EXE souborů), aniž by přitom jakýmkoliv způsobem narušil jejich funkčnost. Na rozdíl od svých naprosto „čistokrevných“ kolegů ale nespoléhá pouze na pro viry přirozený způsob šíření a snaží se za tímto účelem zneužívat jak lokální, tak i internetovou síť. Tento virus totiž rozesílá SYN pakety na náhodně generované IP adresy na TCP port 139 (služba NetBIOS) vzdáleného počítače, kde se snaží zneužívat nedostatečně zabezpečená systémová (IPC$), případně uživatelská sdílení a následně infikovat zde nalezené EXE soubory. Vzhledem k použitým metodám se ale zdá, že virus Tanga, stejně jako drtivá většina jeho soukmenovců, před sebou nemá žádnou významnější kariéru.

Tolik tedy k souborovým virům. Příště se podíváme na zoubek jejich rychlejším a perspektivním kolegům, a to sice e-mailovým červům.

5 0571/OK ❑

Terminologie počítačových virů

Počítačový virus versus škodlivý kód – Termín „počítačový virus“ bývá často používán jako označení všech druhů škodlivého softwaru (anglicky malware). Správněji bychom ale měli v této souvislosti používat termín „škodlivý kód“. Jednotlivé podskupiny potom můžeme označovat jako počítačový virus, trojský kůň, zadní vrátka, e-mailový červ, spyware atd. V praxi se však málokdy setkáme s „čistokrevným“ škodlivým kódem. Typický škodlivý kód v sobě většinou kombinuje dovednosti spadající do více podskupin (např. síťový červ kombinovaný s botem).

In the Wild – Termín označující, že se daný škodlivý kód vyskytl v běžné praxi, dokáže se tedy reálně šířit a nejedná se o tzv. „proof-of-concept“ virus.

E-mailový červ – Škodlivý kód, který se šíří prostřednictvím elektronické pošty v infikované e-mailové zprávě. K tomu, aby dokázal počítač infikovat, zpravidla potřebuje aktivní „spolupráci“ samotného uživatele.

Síťový červ – Naprosto samostatný škodlivý kód, který se většinou šíří pomocí určité bezpečnostní díry v cílovém systému a nepotřebuje žádnou spolupráci ze strany uživatele.

Root-kit – Škodlivý kód pracující na nízké úrovni operačního systému (kernel), který se dokáže ukrýt před uživatelem i před různými bezpečnostními programy. Původní root-kity pocházejí z unixových operačních systémů, kde sloužily k získání administrátorských (root) práv.

Keylogger – Škodlivý kód, který monitoruje a zaznamenává stisknuté klávesy. Může být zneužit třeba ke kompromitaci přihlašovacích údajů, hesel apod.

Zombie – Počítač infikovaný specializovaným škodlivým kódem typu BOT, který může být ovládán vzdáleným útočníkem a zneužíván k různým činnostem.

Bot – Škodlivý kód, který se soustředí zejména na ovládnutí infikovaného systému a jeho další využití. Může také např. vytvářet šifrovaný kanál pro komunikaci mezi útočníkem a infikovaným počítačem.