Bezpečnost

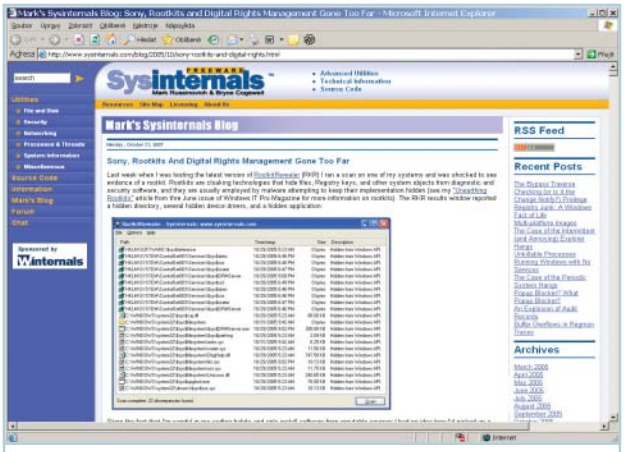
Rootkit od Sony

# Nebezpečné kompaktní disky

**Koncem října se na webu Sysinternals objevil zajímavý článek, ve kterém Mark Russinovič podrobně popisoval, jak na svém počítači zcela náhodou objevil program typu rootkit. Tyto programy, o kterých jsme podrobněji psali v červencovém čísle Chipu, používají stealth techniky a v systému skrývají jak činnost svoji, tak i činnost dalších škodlivých programů, které jsou s nimi spojeny.**

**Text: Pavel Baudiš, Alwil Software**

Standardními prostředky nelze jejich aktivitu zjistit. Mark je velmi zkušeným a opatrným uživatelem počítače, a tak byl přítomností takového programu dost zaskočen. Podrobně zkoumal, jak se program chová a co všechno dělá, a ke svému velkému překvapení zjistil, že se jedná o produkt firmy First 4 Internet a že je součástí DRM (Digital Rights Manager – systém ochrany proti kopírování), který používá firma Sony na některých hudebních CD, prodávaných v USA. Rootkit se automaticky instaluje na počítačích, do kterých je takto chráněný CD vložen, a jeho úkolem je skrýt přítomnost dalších ovladačů, které brání kopírování CD na daném počítači. Přesně tímto způsobem se rootkit dostal i do Markova počítače – koupil si totiž album „Get Right with the Man“ od bratrů Van Zantů, které si následně v počítači přehrál. V EULA (licenční ujednání) nebylo o tomto typu ochrany ani slovo, rootkit a příslušné drivery nebylo možné žádným způsobem odinstalovat. Po jejich ručním smazání zmizela jednotka CD-ROM z počítače a Markovi dalo spoustu práce, aby ji dostal zpět. Navíc zjistil, že při každém přehrání CD na počítači, který je připojen k internetu, se tato informace odesílá firmě Sony, údajně proto, aby se zjistilo, zda k CD nejsou na webu nějaké nové informace. Nicméně i o tomto chování EULA mlčí.




**Tady to začalo:** Blog Marka Russinoviče o nalezeném rootkitu *(www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html)*

## Odkud vane vítr

Brzy vyšlo najevo, že podobně chráněné CD se v Americe prodávají už od dubna 2005. První reakce firem Sony a First 4 Internet byly odmítavé, podle jejich názoru přítomnost rootkitu neznamená pro uživatele žádné riziko. Nicméně případu se brzy chopila média a ta vyvinula na obě firmy poměrně velký tlak, takže po několika dnech se na webu firmy Sony objevil program, který umí rootkit odinstalovat a pro DRM →

ochranu nepoužívá takto agresivní a nebezpečné metody. Samotné nalezení odinstalačního programu na stránkách Sony však není jednoduché, uživatel se musí identifikovat a link obdrží e-mailem s označením Confidential. Ozvaly se samozřejmě i antivirové firmy a také firma Microsoft, která ohlásila, že tento rootkit bude detekován jejím programem Windows Defender (původně MS AntiSpyware) v příští aktualizaci. Firmě Sony navíc hrozí několik žalob od organizací, které chrání soukromí uživatelů, a možná i další soudní procesy – generální prokurátor státu Texas například ohlásil, že požaduje 100 000 dolarů pro každého poškozeného. Takové požadavky jsou možná nadsazené, nicméně firma Sony zcela jistě svojí ochranou zákon porušila a měla by být nějakým způsobem potrestána. Určitě se v tomto případě jedná o precedens, který by měl určit, jak daleko mohou firmy při ochraně svých produktů zajít. Dnes Sony stahuje chráněné CD z trhu.

### Nejen ochrana CD

V čem tkví hlavní nebezpečí takto koncipované ochrany vlastních programů? Instalace jakéhokoli rootkitu je pro systém velkým rizikem. Umožňuje totiž skrývání nejen původních programů, ale i všech dalších, které funkčnost rootkitu využijí. V tomto konkrétním případě rootkit v systému skrýval před uživatelem i systémem veškeré soubory a adresáře, jejichž jméno začíná na $sy$. Bylo jasné, že se brzy objeví škodlivý kód, který se bude snažit tuto bezpečnostní díru zneužít. A opravdu to netrvalo dlouho – po několika dnech se objevil trojský kůň, který se do systému instaloval právě pod jménem $sys$xp.exe, jehož přítomnost je rootkitem maskována; a následovalo několik dalších. Uživatel, který si někdy na svém počítači přehrál legálně koupený CD s ochranou firmy Sony, nemá příliš šancí zjistit, že se mu trojský kůň v počítači usadil. Komerční programy by zkrátka takové metody používat rozhodně neměly. To však firma Sony dodnes pravděpodobně nechápe, jinak by prezident obchodní divize Thomes Hesse nikdy nemohl pronést větu: „Většina lidí nechápe, co rootkit je, tak proč by se o něj měli starat?“ Je škoda, že to nechápe ani pan Hesse. Kdyby to chápal, ušetřil by spoustě lidí velkou řadu problémů a vlastní firmě spoustu peněz!

Phishing

## Počet podvodných mailů klesá

Pozorovatelé Anti-Phishing Working Group zaznamenali obrat trendu: počet rozeslaných phishingových zpráv klesá – z 15 050 případů hlášených v červnu na 13 376 případů hlášených v srpnu. Počet odhalených phishingových webových stránek se však naproti tomu zdvojnásobil. V lednu 2005 jich bylo 2560, v srpnu už 5259.

Důvod tohoto nárůstu je zřejmý – phishingoví „rybáři“ nastražují pro jeden útok více webových stránek.
**Info:** *www.antiphishing.org*


Exploit

## Staré ohrožení

Na *www.computerterrorism.com/research/ie/ct21-11-2005* byl uvolněn exploit (vzorový kód) již dříve oznámené chyby WWW prohlížeče MS Internet Explorer. Umožňuje útočníkovi spouštět na cílovém stroji libovolný kód. Chyba, kterou exploit zneužívá, nastane při zpracování speciálně upravené HTML stránky se zákeřně upraveným javascriptovým voláním objektů „window()“ a událostí „onload“, při kterých dojde k porušení paměťové struktury.

Pokud útočník přesvědčí uživatele, aby navštívil takto upravenou stránku, může mu kompletně zkompromitovat celý systém. Oprava není dosud k dispozici, jako prozatímní obrana se uvádí vypnutí skriptování v IE.
**Info:** *zpravy.actinet.cz*

Antivirové prostředky

# Bezpečnostní soupravy jako bezpečnostní riziko

**Hackeři neúnavně hledají nové cesty, jak proniknout do cizích počítačů – a nyní je nacházejí tam, kde by se to dalo očekávat nejméně: bohaté portfolio možností jim v říjnu nabídl právě bezpečnostní software.**

Ošklivou chybu musel odstraňovat Symantec. Také jeho antivirové jádro poskytovalo hackerům teoretickou možnost spouštět prostřednictvím „buffer overflow" vlastní kód na cizích počítačích. Díky Live Update však byla rychle rozšířena příslušná záplata, takže k závažným následkům nedošlo.

Tato mezera ale jen potvrzuje nový trend: bezpečnostní software je čím dál tím méně bezpečný. Experti firmy Secunia *(www.secunia.com)* zaznamenali v roce 2005 v produktech Symantecu už dvanáct softwarových chyb. Od začátku roku 2004 do prvního čtvrtletí 2005 napočítala Yankee Group celkem 77 chyb; vychází jí tak jejich padesátiprocentní nárůst ve všech bezpečnostních produktech.

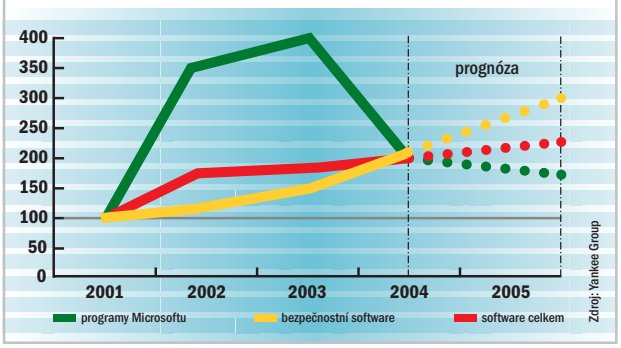
Slabiny Symantecu jsou pro jeho konkurenci samozřejmě vítaným zranitelným místem. A tak společnost GData ihned svou akcí „Norton v nouzi" dopomohla uživatelům Norton Internet Security k přestupu na GData Internet Security. Trapná byla jen taková maličkost, že ani ne o deset dnů později sama přiznala vlastní chybu. Její „antivirový kit" způsoboval s některými personálními firewally havárie systému. Ke škodlibosti nemá konkurence žádný důvod. V říjnu musel Kaspersky doznat, že přes zmanipulované CAB archivy se mohl útočník dostat do systému – tato mezera však mezitím byla odstraněna.

Každopádně si výrobci se záplatami dokážou pospíšit. A tak vzdor mezerám v bezpečnostním softwaru by měl každý uživatel svůj počítač vhodnými nástroji chránit.

**Info:** *www.secunia.com*

### »BEZPEČNOSTNÍ MEZERY V SOFTWARU

Od uvolnění Service Packu 2 klesá množství odhalených bezpečnostních chyb v programech Microsoftu, v bezpečnostních nástrojích naopak stoupá.




Denial of Service

## Problém ve Win2000

Společnost Microsoft vydala oznámení *(www.microsoft.com/technet/security/advisory/911052.mspx)* o chybě v systémech MS Windows 2000 Service Pack 4 a MS Windows XP Service Pack 1. Jedná se o chybu ve zpracování speciálně upraveného UPnP (Universal Plug and Play) požadavku „GetDeviceList" přes RPC (Remote Procedure Call), kterou může vzdálený útočník zneužít a odčerpat značnou část systémových prostředků. Oprava dosud nebyla zveřejněna a výrobce ve svém oznámení doporučuje blokovat na firewallu spojení s RPC. Proof of Concept kód je již k dispozici, a je tedy asi jen otázkou času, kdy se objeví první nástroj zneužívající tuto chybu.

**Zdroj:** *zpravy.actinet.cz*

Malware

## Jednotné názvy virů

Jeden červ, spousta názvů – až dosud pojmenovával každý lovec virů své úlovky vlastními názvy. A tak se tentýž škůdce jmenoval u firmy Kaspersky „Zotob" a u firmy McAfee „Bozori". To už by se však mělo změnit. Iniciativa „Common Malware Enumeration" (CME) bude napříště každému záškodnickému kódu náhodným výběrem přidělovat identifikační čísla ve tvaru „CME-123" nebo „M-123". Ta se pak budou připojovat za jméno, např. „Červ.A!M-123". Díky číslům budou škůdci navzájem porovnatelní. Iniciativa zatím sdružuje firmy McAfee, Microsoft, Sophos, Symantec, KasperskyLabs a další softwarové firmy.

**Info:** *http://cme.mitre.org*

Herní konzole

## Trojský kůň ničí PSP a Nintendo

Šrot v hodnotě 130 eur za sebou zanechá jistý škůdce, jeli spuštěn na konzoli Nintendo DS. Trojan se šíří převážně prostřednictvím pirátských kopií her a napadá jen přístroje, na něž byl předem nahrán změněný software. Také majitelé PlayStation Portable by se měli mít na pozoru. Pod názvem PSPBrick je v oběhu zfalšovaná záplata firmwaru, která konzoli přemění v „lepší těžítko" – už se ji nepodaří nabootovat, ale v obchodě ji lze samozřejmě vyměnit. Nebezpečí odstraňuje teprve nová verze firmwaru pro PlayStation Portable od Sony.

**Info:** *www.darkfader.net*

## KRÁTCE

**→ Červ místo třídní fotky**

Pod nadpisem „Třídní fotografie" se šíří Sober-O. Poštovní červ s německým textem se pokouší přimět uživatele, aby spustil EXE soubor v přiloženém zazipovaném souboru – údajně třídní fotografii. Novější virové aktualizace už škůdce dokážou odhalit.

**Info:** *www.sophos.com*

**VIROVÝ TOP TEN – ZÁŘÍ**

| | |
|---|---|
| 1 | *W32/Netsky-P* |
| 2 | *W32/Mytob-BE* |
| 3 | *W32/Mytob-AS* |
| 4 | *W32/Zafi-D* |
| 5 | *W32/ Netsky-D* |
| 6 | *W32/ Mytob-CX* |
| 7 | *W32/ Mytob-EP* |
| 8 | *W32/ Mytob-CJ* |
| 9 | *W32/ Mytob-C* |
| 10 | *W32/ Mytob-BN* |

**Déleslouží:** **Nikým neohrožován vládne Netsky-P.**

**→ Záplata od Microsoftu s následky**

Patch pro Windows vyloučí uživatele z počítače, pokud byla změněna oprávnění složky Windows. Záplata by přesto měla být nainstalována, neboť zaceluje jednu nebezpečnou mezeru.

**Info:** *www.microsoft.com*

**→ Největší hrozby**

SANS (SysAdmin, Audit, Network, Security) Institute zveřejnil aktualizovaný seznam *(www.sans.org/top20/)* dvaceti nejkritičtějších bezpečnostních chyb za rok 2005. Vedle tradičních cílů útočníků, jako jsou operační systémy (MS Windows, Unix), webové servery a mailové servery, se do popředí zájmu dostávají čím dál tím více multiplatformní aplikace (mediaplayery, zálohovací software, antiviry, databáze apod.). Další hrozbu představují chyby síťových zařízení.

**Info:** *zpravy.actinet.cz*

## NOVÉ BEZPEČNOSTNÍ MEZERY

### Windows

**Winrar 3.5**

**V komprimačním programu byly odhaleny dvě středně závažné mezery. Útočníci je mohou využít ke spuštění cizího kódu na počítači.**

➜ Ve verzi 3.51 se už bezpečnostní mezera nevyskytuje.

**Info:** *www.rarlabs.com/download.htm*

**AbiWord do verze 2.4.0**

**Několik chyb v textovém editoru může vyvolat přetečení bufferu a umožnit tak přístup do systému.**

➜ Nahrajte si aktuální verzi 2.4.1.

**Info:** *www.abisource.com*

### Linux

**Thunderbird a Firefox**

**Při předávání URL přes shell se projevila závažná bezpečnostní mezera: pomocí speciálních adres si útočníci mohou zjednat přístup do systému i zvenčí.**

➜ Thunderbird i Firefox ve verzi 1.0.7 už nejsou napadnutelné

**Info:** *www.mozilla.org/security/*

**Opera**

**Útočník může vytvořit zákeřný odkaz, který pokud je otevřen z externí aplikace a standardně otevíraným prohlížečem je Opera, může být použit k vykonání libovolných příkazů na napadeném počítači.**

**Info:** *http://secunia.com/secunia_research/2005-57/advisory*

Denial of service

# Děravý firewall

Společnost Kerio vydala novou verzi svého produktu WinRoute Firewall. Verze 6.1.3 opravuje některé bezpečnostní chyby, které mohou způsobit útok typu Denial of Service nebo neautorizovaný přístup. Pád aplikace nastane při zpracování streamu z některých RSTP serverů. Druhé bezpečnostní riziko spočívá v neautorizovaném přístupu uživatelů s vypnutým účtem. Další podrobnosti bohužel nebyly zveřejněny.

**Info:** *zpravy.actinet.cz*

Nové bezpečnostní díry

# Multimediální problémy

Společnost RealNetworks oznámila uvolnění záplat pro své produkty RealPlayer a Helix Player. Postižené jsou verze RealPlayer 8, 10, 10.5, RealOne Player v1 a v2, Helix Player 10 a RealPlayer Enterprise od verze 1.1 do verze 1.7. Zranitelná místa jsou celkem tři. První chybou je přetečení zásobníku. Tato chyba nastane při navštívení zákeřně upravené stránky se speciálně upraveným .rm souborem. Druhou chybu způsobí přetečení haldy v knihovně „DUNZIP32.DLL“, která nesprávně zpracuje zákeřně upravené skiny (.rjs) pro RealPlayer. Poslední je nespecifikovaná chyba typu přetečení zásobníku při zpracování skinu. Informace o záplatách naleznete v původním ohlášení *http://service.real.com/help/faq/security/051110_player/EN/*.