Pohádky o Windows

Sněhurka a sedm trpaslíků, O Popelce nebo O Červené karkulce – kdo by neznal tyto klasické dětské pohádky? Pohádky však pronikly i do světa IT. Dospělí sice moc dobře vědí, že neexistují sudičky, víly ani ježibaby, ale povídačkám ze světa IT věří jako malé děti. Nejvíce těchto příběhů pak pojednává o Windows. Témat je celá řada – registry, hackeři, jádro systému i ovladače. Hezké je, že všechny tyto báchorky vznikly jako lidová slovesnost, což zároveň ukazuje, jak bohatou fantazii mají uživatelé počítačů. Kdyby Božena Němcová nebo Karel Jaromír Erben chtěli pohádky o Windows posbírat, určitě by jim to stačilo na hodně tlustou knížku.

A co vy, dokážete poznat, který příběh je pravdivý, a co je naopak jen pohádka? Není to úplně jednoduché, protože některé příběhy mají reálné jádro, ale informace k němu přidané jsou opravdu jen ze světa fantazie. Chip vám pomůže odkrýt pravdu. Chcete-li totiž skutečně optimalizovat chod svého systému, pomohou vám jen naše zaručené rady a odzkoušené nástroje z Chip DVD.

O čistých registrech

ÚKLID ZRYCHLÍ POČÍTAČ

Popelka měla velkou výhodu – když měla za úkol oddělit hrách od popela, pomohli jí holoubci. Kdo ale odstraní popel z registrů, aby byly krásně čisté?

Tato pohádka pochází ještě z dob, kdy počítačům vládl operační systém DOS. Tehdy byla paměť velmi drahá, a proto se ukládaly jen důležité informace a šetřilo se každým bajtem. A Windows dokážou místem pořádně plýtvat! Jádro této pohádky se tedy zakládá na pravdivém příběhu: každá operace totiž zanechává stopu v databázi registru a všechny programy si do něj zapisují, co je napadne. Registr tak bobtná a uchovává často zbytečné informace. Proto je třeba, podle příběhu této pohádky, sáhnout po nástroji, který registry vyčistí od nepotřebného balastu. Ale pozor, toto pravidlo platí pouze pro starší operační systémy, tedy po systém Windows 2000. XP a Vista jsou při správě registru mnohem inteligentnější než jejich předchůdci. V operační paměti si totiž drží jen ty části registru, které potřebují pro současnou činnost. Klíče z registru, které nejsou v danou chvíli potřeba, zůstávají na disku. Díky tomu je v paměti jen vybraná část registru a zbytek zůstává uložený na disku. Zmenšení registru proto žádné zrychlení systému nepřinese.

Čištění registru přesto doporučujeme, ale z úplně jiného důvodu. Mnoho programů i poté, co je odinstalujete, zanechá v registrech svoje záznamy. Pokud jich není mnoho, nic zásadního se neděje, ale pokud jsou v registrech přítomny stovky klíčů, které tam nemají co dělat, může jejich přítomnost vést k chybám systému – třeba ke špatnému vyhledání ovladače hardwarového zařízení. To může vést až k nestabilitě celého systému. Jestliže pravidelně testujete nějaké programy, instalujete je a pak je zase dáváte pryč, není špatné čas od času smazat neplatné klíče.

O otráveném počítači

WINDOWS SE V SÍTI INFIKUJÍ ZA PĚT MINUT

Sněhurce stačilo jen jedno sousto otráveného jablka, aby upadla do dlouhého spánku.

NAJDETE NA CHIP DVD

Mýty o Windows

Autoruns ► přehled programů spouštěných po startu
AVG 8.0 Chip Edition ► bezpečnostní balík
CCleaner ► čistí disk a registry
Erunt ► záloha a obnova registrů
HWINFO32 ► informace o hardwaru
Registry System Wizard ► čistí registry
TuneUp Utilities 2007 ► tuning systému
Sandboxie ► bezpečné surfování
Tweaking Utility ► úprava systému
Vispa ► úprava Visty
xpy ► úprava XP

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **POHÁDKY**.

Windows se mohou infikovat stejně rychle. Stačí, aby byl systém připojený k síti, a pokud nemá pořádnou obranu v podobě bezpečnostního balíku, bude do pěti minut infikován. Je to tak? Ne! Je to pohádka, kterou nám pravidelně předkládají testeři antivirových programů. Jejich představy o standardní práci uživatele jsou totiž značně zkreslené, navíc scénář okamžitého napadení počítače by platil pouze pro nahá XP, která jste instalovali tak před sedmi lety. Dnes máte XP vybavena Service Packem 2, který uzavřel velkou většinu bezpečnostních mezer, a navíc Microsoft přidal i celou řadu vylepšení, jako je třeba jednoduchý firewall, který zabrání tomu, aby se někdo zcela náhodně dostal do počítače. Díky těmto opatřením se razantně snižují i šance různých červů a infikovat počítač po síti není tak jednoduché. Kdo má tedy aktuální operační systém, nemusí se připojení k síti obávat. To samozřejmě neplatí v případě, kdy používáte rizikový software. Ten sám o sobě totiž otevírá bezpečnostní mezery, které jsou vstupenkou pro škůdce. V rubrice Bezpečnost pravidelně upozorňujeme na internetové prohlížeče, přehrávače multimédií a jiné programy, které jsou plné bezpečnostních mezer. I z toho důvodu doporučujeme používat bezpečnostní software, jako je například plná verze AVG 8.0, kterou pravidelně nacházíte na Chip DVD.

O začarovaném uživateli

MICROSOFT ŠPEHUJE UŽIVATELE

Zlá čarodějnice vidí ve své křišťálové kouli, co právě děláte. Stejně tak Microsoft kontroluje, co právě provádíte na svém počítači. Zdá se, že z této pasti není úniku: uživatel musí on-line potvrzovat pravost svého operačního systému, přičemž Internet Explorer posílá na servery Microsoftu informace o stránkách, na kterých surfujete, a přehrávač médií informuje svého stvořitele o tom, jakou hudbu posloucháte. Skutečnost však tak hrozivá není: Microsoft pouze ověřuje, zda používaný operační systém není kradený, a Windows Media Player si sahá na internet pro obrázek alba u hudby, kterou přehráváte. A mimochodem: Apple dělá s iTunes to samé, a Google si dokonce zaznamenává, jaké výrazy hledáte.

Často se také kritizují chybová hlášení, která se generují při pádu aplikace. Tato hlášení se totiž odesílají Microsoftu a obsahují celou řadu soukromých informací, především z problémové aplikace. Pokud si nepřejete Microsoftu nic odesílat, sáhněte na Chip DVD po nástrojích Vispa a xpy. Ty dokážou Windows držet na uzdě.

Ani dočasné soubory neznamenají problém. Běžnému uživateli zřejmě nijak vadit nebudou, ale pokud by se k nim dostala třetí osoba, může získat citlivé informace. O dokumentech, se kterými pracujete, o stránkách, které navštěvujete, a řadu dalších informací. Proto doporučujeme, abyste pravidelně mazali dočasné soubory. Perfektně to zvládne CCleaner.

Mac porazí všechny

XP JSOU POMALÁ A LÍNÁ

Pamatujete si na závod zajíce a želvy? Jen rychlost nestačí. Ačkoliv je zajíc rychlejší, do cíle se dostane později než želva. A podobné je to i s Mac OS X a XP. Mac je stále v kondici, naproti tomu XP dobíhají do cíle celá unavená. Je to tím, že podporují jakýkoliv hardware. Rozběhnou se na platformě AMD i XP, nepotřebují konkrétní typy hardwaru. Mac je přesně optimalizován na jeden druh počítače, což mu dává náskok.

Kdo používá PC, zná to moc dobře: Windows jsou zpočátku rychlá a výkonná, ale od určitého data se systém začne zpomalovat a pak je den ode dne pomalejší. Problém není v systému samotném, ale v přidružených aplikacích. Nafouklý software zpomaluje běh celého systému. Problémem jsou hlavně položky, které se spouští automaticky se systémem – jsou to desítky programů, které se musí po startu zavádět: messenger, poštovní klient, antivir, nástroje zvukové a grafické karty. Všechno jsou to brzdy, které obsazují paměť a užírají výkon.

Pokud chcete brzdy odstranit, je třeba odstranit všechny tyto programy. Pro program Autoruns to není žádný problém. Přehledně vám zobrazí všechny aplikace, které nabíhají spolu se systémem. Většinu ze spouštěných aplikací můžete odstranit – typicky jde o podpůrné aplikace kancelářských balíků, přehrávače apod. Rozhodně neodstraňujte bezpečnostní programy, rezidentní štíty atp.

Windows také pořádně zpomalí používání mnoha programů paralelně. Nejde ani tak o výkon procesoru, dnešní dvoujádrové procesory jsou opravdu hodně rychlé, ale hlavně o zabranou operační paměť. Pokud programy požadují více paměti, než kolik jí máte fyzicky v počítači, začne si ji operační systém odkládat na harddisk (swapuje). Pevný disk je samozřejmě mnohem pomalejší než paměť, a proto dojde k velmi výraznému zpomalení práce. Máte-li dostatečné množství paměti RAM, tedy aspoň 1, ideálně 2 GB, můžete swapování zcela deaktivovat. Zvolte »Start | Ovlá-

INFO

Jak se Vista chrání proti malwaru

Microsoft vybavil Vistu technologiemi, které ochrání uživatele před nebezpečným kódem. Tři z nich jsou klíčové.

KONTROLA OVLADAČŮ

Když už se škůdce dostane do jádra systému, je velmi těžké jej vysledovat a odstranit. Proto se mohou do jádra zapisovat jen prověřené kódy. Systém kontroluje ovladače, zda mají platný podpis a certifikát WHQL (Windows Hardware Quality Lab). Pokud ovladač podpis nemá, Vista jej označí jako nebezpečný a nedoporučuje jeho instalaci.

IMUNIZACE PAMĚTI

Technika pojmenovaná jako Address Space Layout Randomization (ASLR) zabraňuje přetečení bufferu, což je jeden z nejčastějších typů útoku hackerů. Windows při každém novém spuštění umístí kód a knihovny do jiné části paměti, takže i když dojde k přetečení bufferu, nespustí se škodlivý kód, který útočník do paměti připravil, ale ukazatel paměti se dostane do prázdného místa.

BLOKOVÁNÍ PROGRAMOVÉHO KÓDU

Funkce Data Execution Prevention (DEP) zabraňuje spuštění malwaru, který se vklíní do paměti mezi běžná data. Pokud by chtěl malware udělat nějakou nestandardní operaci, která je pro škodlivý kód typická, DEP jej jednoduše zablokuje. Tuto technologii zkoušel Microsoft už v XP, zde ale nefungovala příliš dobře.

dací panely | Systém | Upřesnit«, v části Výkon klikněte na »Nastavení | Upřesnit | Změnit« a deaktivujte virtuální paměť u všech disků. Upozornění: Po každé změně je třeba kliknout na tlačítko »Nastavit«, a změny se projeví až po novém spuštění počítače.

Oslíku, otřes se

VISTA JSOU DRUHÁ MILLENIUM EDITION

Ten, kdo vlastní oslíka „otřes se“, se nemusí starat o svoji budoucnost. Microsoft do svého oslíka investoval mnoho – tento operační systém měl největší marketingovou podporu v celé historii Microsoftu. Místo obrovských prodejních úspěchů je však Vista katastrofou – podobně jako Windows Millenium Edition. Ona paralela mezi ME a Vistou je docela patrná. Obě verze byly od začátku plné dětských nemocí, které Microsoft odstranil až pomocí aktualizací. Zároveň velkému množství uživatelů pil nový systém krev. A oba systémy měly potíže se starším hardwarem. Kdo by si nepamatoval problémy Visty, jako je pomalé kopírování, chybějící ovladače pro tiskárny nebo chyby při režimu spánku? Tyto potíže odstranil Microsoft až pomocí Service Packu 1, který je však dostupný už téměř rok.

Chybou zřejmě také bylo, že Microsoft oznámil, že za sedm let vývoje Visty je nový operační systém plný převratných funkcí, a Vistu prezentoval jako „Wow!“. Takové problémy, jaké měla Windows ME, však Vista nemá. A hlavně – Millenium Edition byl operační systém založený na MS-DOS, takže zde nebylo možné vůbec pracovat s uživatelskými právy, jako to umí Vista. Tím byl systém velmi nebezpečný, a pokud se do počítače dostal škodlivý kód, měl prakticky neomezené možnosti. Proti tomu už je Vista velmi dobře chráněná (podrobnosti v rámečku na straně 42). Nové funkce ve Vistě nejsou sice Wow!, ale přináší vyšší bezpečnost. Třeba povedené »Řízení uživatelských účtů«, to dělá práci se systémem mnohem bezpečnější.

Všichni na jednoho

WINDOWS JSOU HLAVNÍM CÍLEM HACKERŮ

Hloupý Honza v pohádkách většinou nachází velmi šikovná řešení – a hackeři jsou na tom podobně. Proto si za cíl svých útoků vybrali Windows – jsou nejrozšířenější, a proto stačí napsat pouze jeden vir, a ten napadne 95 % počítačů v síti. Pokud se jedná o červy, spustí řetězovou reakci, která ochromí tisíce počítačů. Jenže to, že jsou Windows jediným cílem hackerů, není tak úplně pravda. Současné operační systémy jsou již tak zabezpečené, že se do nich útočník jen sotva dostane. Proto se útočníci přestali orientovat na operační systém a využívají programy, které si uživatelé instalují. To je skutečný zdroj nebezpečí. Přitom nebezpečí jsou to opravdu vážná. Třeba v létě loňského roku byla objevena mezera v přehrávači Flashe ve verzi 9.0.115.0. Hacker se mohl dostat do systému a nahrát do něj libovolný kód v okamžiku, kdy uživatel přehrával Flash třeba na internetových stránkách. Velmi oblíbené jsou i podfuky, kdy hacker vytvoří stránku, která jakoby vyžaduje stažení kodeku. Pokud potvrdíte stažení, stáhne se kodek, který třeba přehraje nějaké video, ale zároveň do počítače nainstaluje malware.

Trend poslední doby je jasný: útočníci se na Windows nesoustřeďují. Novým cílem jsou aplikace s přímým přístupem do internetu, jako jsou prohlížeče, e-mailoví klienti, chatovací programy atd. Proto je nutné aktualizovat nejen operační systém, ale také aplikace.

O zlobivé Vistě

ŘÍZENÍ UŽIVATELSKÝCH ÚČTŮ JE ZBYTEČNÉ

Alenka v říši divů se musí postavit Královně srdcí, vládkyni říše divů. Uživatelé Visty se zase musí postavit Microsoftu, vždyť řízení uživatelských účtů je příšerné. Neustále na vás vyskakuje okno, které chce potvrdit kdejakou triviální operaci. Spuštění souboru, instalace, kontrola aktualizace – neustále vyskakují okna, se kterými musí uživatel bojovat.

Okno se zobrazuje jen v situacích, kdy se provádí nějaká důležitá operace, která by mohla ohrozit bezpečnost operačního systému. Takové kliknutí vám nervy pocuchá méně, než kdybyste měli později odvirovávat počítač nebo hledat data, o která jste přišli. Jestliže vás i přesto vyskakující okýnka obtěžují, můžete »UAC« zcela deaktivovat. Pokud to však provedete, přijdete o jednu z nejdůležitějších funkcí Visty, která vašemu systému přináší velmi účinné zabezpečení.

Nejlepšího zabezpečení dosáhnete, vytvoříte-li si speciální účet, prostřednictvím něhož budete přistupovat na internet a který nebude mít žádná práva. Pokud se vám škůdce dostane do systému, stejně nebude moci nic udělat. Administrátorský účet pak používejte jen pro nejnutnější případy, třeba když instalujete nový hardware nebo software. Řešením je také použití programu Sandboxie, což je nástroj, který izoluje internetový prohlížeč od ostatních částí operačního systému.

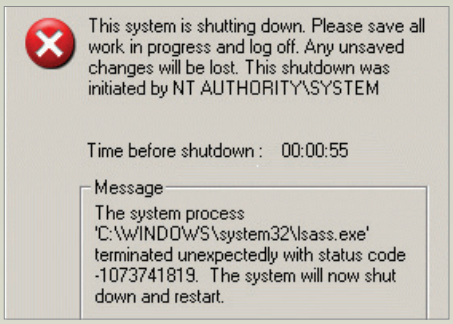
AUTOR@CHIP.CZ

INFO

Skutečné tragédie Windows

ČERV, KTERÝ KAŽDÉHO ZOTROČIL

Červ W.32.Sasser využíval zranitelnost služby Local Security Autority Subsystem (LSASS), která přiděluje přístupová práva uživatelským aplikací. Tento bezpečnostní prvek byl používán ve Windows 2000 a XP. V květnu roku 2004 naprogramoval 17letý student z Německa škodlivý kód, který vyhledával počítače na internetu. Jakmile našel počítač se správným systémem, poslal do něj červa. Červ je relativně neškodný, pouze vypne počítač, nekrade tedy žádné soubory nebo hesla. Sasser infikoval dva miliony počítačů po celém světě. Microsoft uzavřel bezpečnostní mezeru Service Packem 2.



Sasser: Toto hlášení zná většina uživatelů Windows. Má ho na svědomí červ Sasser.

ZOMBIE ÚTOČÍ

W32.Blaster (Lovesan/MSBlast) infikoval více počítačů než jakýkoliv jiný červ. Podle Microsoftu napadl devět milionů počítačů. Červ využíval slabé místo DCOM-RPC (Distributed Component Object Model/Remote Procedure Call). Upravoval registry a kopíroval do systému soubor MSBLAST.exe. Infikovaný počítač sloužil, mimo jiné, k DDoS útokům na jiné počítače. Záplata MS03-026 od Microsoftu bezpečnostní díru uzavřela.

DA VINCIHO OBRAZ

Útočníci zneužili slabého místa v grafickém modulu pro vykreslování souborů WMF. Na rozdíl od předchozích útoků, které se staly již v roce 2006, se grafika v Internet Exploreru normálně zobrazila. Útočníci ale spustili svůj kód, který třeba mohl v počítači sbírat hesla. Postiženy byly všechny systémy od Windows 98, tedy včetně systémů Server 2000 a 2003. Díru zavřela záplata MS06-001.

TROJSKÁ MYŠ

Obzvláště nebezpečný kód se objevil na počátku roku 2007. Využíval slabé místo v souborech s příponou .ani, což jsou soubory, které obsahují animace kurzorů myší (třeba známé přesýpací hodiny). Stačilo navštívit infikovanou webovou stránku, a před útokem nebylo obrany. Postiženy byly všechny operační systémy od roku 2000, tedy včetně nové Visty. Microsoft okamžitě reagoval kritickou záplatou s označením MS07-017.