Sedm znaků ďábla

VIR, NEBO SYSTÉMOVÁ CHYBA? Je velmi těžké rozpoznat, zda je počítač infikován, nebo zda se „jen chová divně“. Chip vám ukáže sedm typických znaků, které provázejí útoky virů, a také vám prozradí, jak problémy vyřešit…

CLAUDIO MÜLLER

Miliony uživatelů berou bezpečnost svého počítače na lehkou váhu. Nevěříte? Typickým příkladem je skutečnost, že už od konce minulého roku útočí na miliony počítačů červ Conficker, a to i přesto, že Microsoft příslušnou bezpečnostní mezeru (kterou červ zneužívá) uzavřel prostřednictvím aktualizace již v říjnu 2008! Celá řada uživatelů spoléhá na jediný nainstalovaný produkt (například na bezpečnostní balík), který však bez pravidelné aktualizace systému a virových databází může nakonec škůdcům podlehnout. Jak se tedy efektivně chránit před viry? Více informací najdete v rámečku Tipy pro prevenci (strana 106).

Jestliže škůdce vstoupil do vašeho počítače poprvé, může se před virovým skenerem maskovat pomocí rootkitu, nebo může dokonce paralyzovat ochranné mechanismy (antispywarový nástroj, firewall, ochranu registrů…). Spyware má potom dobrou příležitost zasílat hackerovi jakékoliv množství dat nebo stahovat ze sítě jiné škůdce. Náznaky virového útoku jsou v tomto případě víceméně nenápadné – pomalý počítač, neobvyklá vyskakovací okna, změny v prohlížeči, neustálé pády systému.

Smutné ale je, že podobné problémy mohou způsobovat samotná Windows, a dokonce i neškodný a na první pohled dokonalý software. Vysvětlíme vám, co stojí za největšími obtížemi, a poradíme vám, jak zjistit skutečnou příčinu: tedy zda je na vině vir, nebo Windows či jiný software. Všechny potřebné nástroje opět najdete na našem DVD.

A co dělat, když skutečně objevíte vir? Poradí vám naše „Tipy pro případ nouze“, které najdete straně 107.

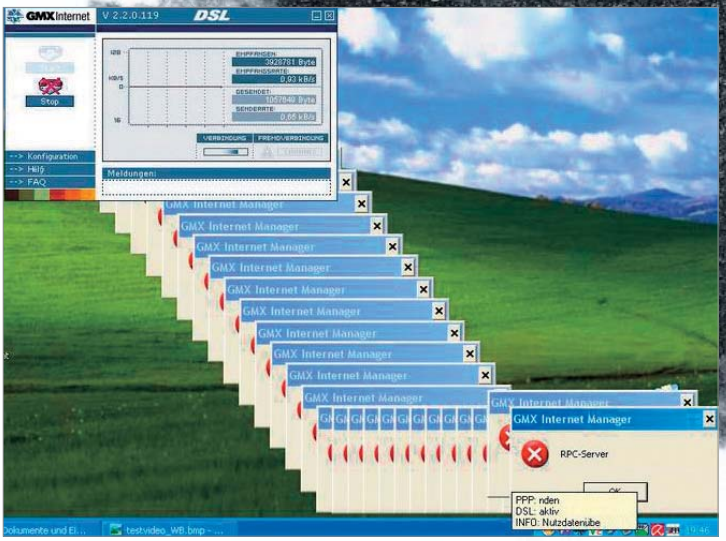
1 Windows se neustále hroutí…

Systémové chyby dostávají s větší či menší krutostí Windows stále „na kolena“. Důsledky: objevují se zprávy o chybějících či poškozených souborech, systém zamrzává nebo – což je obzvláště nepříjemné – se počítač neustále restartuje. Důvodem těchto problémů může být špatně naprogramovaný malware, který způsobuje konflikty v souborovém systému. To se stává proto, že někteří tvůrci virů nemají dost času a prostředků na testování svých „produktů“ v praxi. Za problematickým chováním škůdce často ani není žádný záměr – nakonec malware funguje nejefektivněji skrytě. Smutným faktem nicméně je, že i běžné aplikace mohou být naprogramovány problematicky, a tudíž způsobovat havárie. Další možnou příčinou mohou být i hardwarové problémy: především modré obrazovky a automatický restart počítače jsou často příznakem přehřátého nebo poškozeného procesoru, grafických karet či paměťových modulů.

VIR, NEBO WINDOWS? Abyste vyloučili hardwarové problémy, měli byste nejprve otevřít počítač a odstranit veškerý prach. Poté zkontrolujte, zda všechny „konektory“ jsou pevně propojeny a zda se větráky točí bez zbytečného odporu. V nástroji Správce zařízení (najdete ho v nabídce »Start | Nastavení | Ovládací panely | Systém | Hardware«) můžete vidět, zda v systému dochází k hardwarovým konfliktům, které je možné opravit pomocí reinstalace ovladačů. Pro obecný monitoring systému jsou vhodné analytické

ILUSTRACE: JAMES ALLRED

Zmatenost: Na firewall integrovaný ve Windows uživatelé rychle zanevřou – jeho varování jsou zmatená a firewall se často snaží blokovat i neškodné programy…



Strašák pro Windows: Pokud se plocha Windows pokryje okny s chybovými zprávami, může být viníkem malware.

nástroje, jako třeba SiSoft Sandra Lite. Tento nástroj například ukáže, zda se komponenta přehřívá. Možná jste nedávno nainstalovali nový program, který by mohl být příčinou vašich problémů. Jednoduché odinstalování však nemusí být vždy dostatečné, protože na disku častokrát zůstávají zbytky instalačních souborů a „mrtvé" zápisy v registrech. Zde vám pomůže čisticí nástroj CCleaner nebo obnova systému do stavu před instalací systému pochybného programu.

2 Neobvyklý datový provoz

Vždy je únavné, když vás firewall zahlcuje varovnými hláškami. O dost podivnější bývá zmiňovaná situace v případě, že nesurfujete. Ano, firewall vás může zahltit varovnými zprávami o datovém toku směrem z internetu nebo na internet, ačkoliv nemáte spuštěný prohlížeč ani jiný program pro komunikaci s přáteli (IM, Skype…). Jak zjistit více? Základní informace o těchto aktivitách lze najít ve Správci úloh v záložce Sítě.

Poměrně často zasílají špionážní programy svým tvůrcům citlivá uživatelská data, stahují z internetu další škůdce nebo z vašeho počítače rozesílají spam. Například spyware KeyProwler nahrává vaše „stisky kláves", posílá je hackerovi, a tak se vaše přihlašovací údaje mohou dostat do „špatných rukou". Za neidentifikovaný „síťový provoz" mohou být ale zodpovědné i běžné programy nebo samotná Windows – například když aktualizační rutiny stahují na pozadí nejnovější verze programů.

VIR, NEBO WINDOWS? Malý nástroj CurrPorts listuje všemi službami, které vytvářejí internetové spojení. V něm si nejprve pomocí klávesové zkratky CTRL+F6 skryjte všechny systémové služby Windows. Pokud poté mezi zbývajícími procesy uvidíte něco jiného než svůj prohlížeč nebo aktivní komunikační program, našli jste pravděpodobně viníka velkého datového provozu. Chcete-li mít stoprocentní jistotu, podívejte se do sekce „Remote address". Pomocí služby na adrese **http://network-tools.com** snadno zjistíte, kdo se skrývá za nalezeným připojením…

3 Počítač je pomalý

Fenomén, který už zná mnoho uživatelů Windows: s přibývajícími měsíci počítač „ztrácí" rychlost. Bootování trvá stále delší dobu a Windows při startu nahrávají čím dál tím více malých programů. Počítač se poté stává natolik pomalým, že ke spouštění programů a načítání dat vyžaduje mnohonásobně více času. Jedna věc je jistá: každý aktivní malware vyžaduje sys-

NAJDETE NA CHIP DVD

Nástroje na ochranu proti malwaru

CCleaner ► čistí disk a registry Windows

CurrPorts ► analyzuje systémový provoz a hledá špiony

DriveImage XML ► vytváří zálohy pro záchranu dat

Gmer ► hledá a odstraňuje rootkity

HijackThis ► chrání prohlížeč před útoky

NoScript ► blokuje nebezpečné javascripty

Recuva ► obnovuje smazaná data

SiSoft Sandra Lite ► nástroj na analýzu systému

Spamihilator ► třídí e-maily a odstraňuje spam

Spybot Search & Destroy ► efektivní lovec spywaru

System Explorer ► výborný správce procesů

Wise Registry Cleaner ► čistí registry

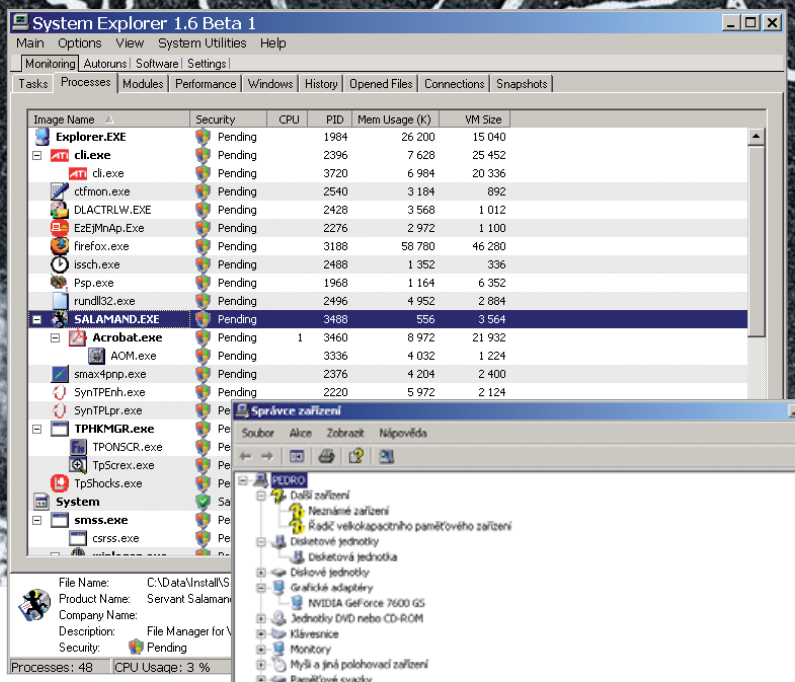
► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **MALWARE**.

INFO

Tipy pro prevenci

Stoprocentní ochrana proti virům a špionážním programům neexistuje. Nicméně budete-li dodržovat následující základní pravidla, můžete snížit potenciální riziko na minimum:

- aktivujte automatické aktualizace u svého virového skeneru;
- pravidelně kontrolujte svůj systém několika různými bezpečnostními nástroji;
- nevypínejte rezidentní antivirovou kontrolu;
- pravidelně aktualizujte Windows a všechny důležité programy;
- nezapomínejte zálohovat;
- vytvořte si záchranné DVD pro případ havárie Windows;
- neotvírejte podezřelé přílohy (nejen od uživatelů, které neznáte) a nesurfujte po rizikových stránkách.



V utajení: Pomocí nástroje System Explorer lze odhalit procesy, které se tajně spouští na vašem počítači.

Problematický hardware: V nástroji Správce zařízení lze vidět, zda v systému dochází k hardwarovým konfliktům.

témové zdroje a zatěžuje systém. U některých uživatelů se však na počítači po několika měsících práce nakupí na disku velké množství programů, které systém zpomalí i bez zásahu malwaru. Programy „zavalí“ registry, fragmentují disk a zaplní složku pro automatický start se systémem.

VIR, NEBO WINDOWS? Pro první pokus objevit systémové brzdy a nežádoucí návštěvníky můžete použít Správce úloh systému Windows. My vám však doporučujeme nástroj System explorer, který nabídne více informací než jeho kolega z Windows. Pod kartou »Autoruns | Startups« najdete všechny programy, které se aktivují při startu Windows, zatímco v nabídce »Monitoring | Processes« najdete přehled všech aktivních procesů. Položky označené „safe“ jsou obvykle důležité systémové služby Windows. Ale pozor – jako služby Windows se maskují i někteří škůdci! Například Netsky.AB se maskuje pod názvem „csrss.exe“. Rozdíl: Červ se skrývá ve složce C:\Windows, zatímco originální služba pracuje ve složce C:\Windows\System32. Poté, co v přehledu nástroje System explorer kliknutím označíte neznámý či podezřelý proces, zobrazí se jeho zdrojový adresář. Pomocí nabídky »File Check with | Upload to VirusTotal.com« (která se objeví po kliknutí pravým tlačítkem) si také můžete dát zkontrolovat libovolný soubor. Nikdy byste neměli ukončit proces před jeho analýzou – mohlo by jít o důležitou systémovou službu.

4 Prohlížeč zešílel

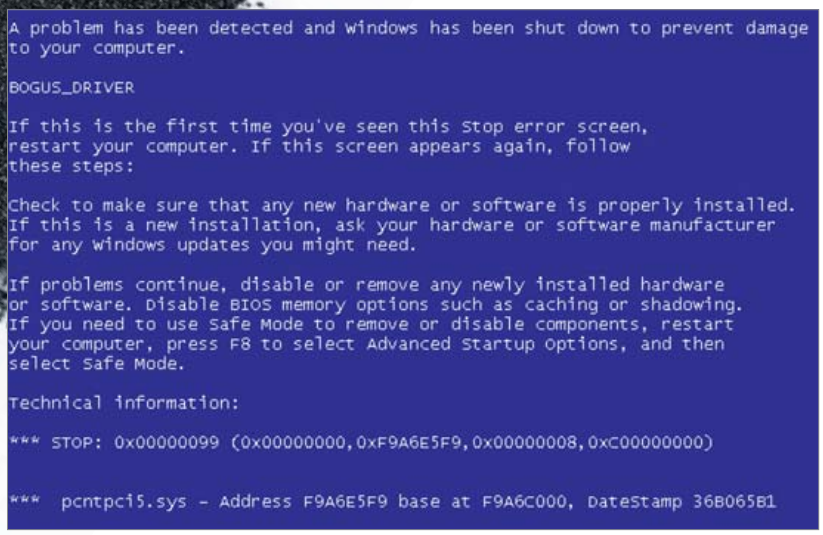
Je nepříjemné, když se chcete podívat na internet a prohlížeč nedělá to, co se od něj očekává: zčista jasna otevře jinou startovní stránku, mezi ovládacími prvky se objeví nové lišty s tlačítky a na obrazovce nepřetržitě vyskakují nová a nová okna. Použitím těchto metod se malware pokouší dostat uživatele na zmanipulované stránky, aby jim odcizil soukromá data a do počítače propašoval další malware. Adware MyCentria například instaluje do prohlížeče speciální lištu, která zadržuje vyhledávací dotazy uživatele a zobrazuje zmanipulované vyhledávací výsledky. Podobné lišty však bývají často integrovány i do neškodných programů. Pokud při instalaci softwaru nedáváte pozor a nevšimnete si nenápadných zatržítek (například „Chcete do vašeho prohlížeče přidat úžasného pomocníka Surfujeme s vámi?“), zjistíte, že do vašeho prohlížeče přibylo několik nových prvků.

VIR, NEBO WINDOWS? Většinou vůbec nemá smysl pokoušet se změnit „špatnou“ startovní stránku na původní volbu, protože „únosci“ svá nastavení znovu a znovu obnovují. Mnohem užitečnější bude pohled do registrů (například pomocí příkazu Regedit). V registrech totiž pod klíčem »HKEY_LOCAL_MACHINE/Software/Microsoft/InternetExplorer/Main« můžete najít zmiňovanou startovní stránku a dozvědět se více. Pokud ve zmiňované položce najdete neznámé adresy, počítejte s tím, že je na vašem počítači skryt adware a jakékoliv pokusy o úpravu prohlížeče jsou do jeho odstranění zbytečné. Většinu podobných útočníků dokáže odhalit nástroj HijackThis. Pro tento účel vytvoří soubor se záznamem, který můžete nechat zdarma automaticky zkontrolovat na celé řadě stránek (například na **www.hijackthis.cz**, **www.hijackthis.de/cz**). Na velkém množství stránek také najdete diskusní fóra, kde se můžete poradit s experty, kteří vám pomohou interpretovat data a poradí vám, zda máte skutečně v počítači škůdce a které položky je nutné odstranit (doporučujeme web **www.viry.cz/forum/**).

5 Podivné aktivity disku

Většina uživatelů to určitě zná: počítač náhle začne vibrovat, kontrolka disku začne zuřivě blikat, ačkoliv vy na počítači nic neděláte a neběží ani žádný náročný program. Je možné, že se náhle zaktivoval vir, hledá na disku přístupové údaje a soukromá data, nebo si možná útočník z webu stahuje další posily a instaluje jiný malware.

Tyto aktivity však mohou mít i neškodné příčiny. Windows i jiné programy často využívají „nečinné fáze“ počítače pro náročné



Strašení: Vir Blusod se snaží uživatele vyděsit tzv. modrými obrazovkami smrti. Jde však jen o neškodné padělky…

Malware často dokáže paralyzovat virový skener

služby, jako jsou defragmentace disku, indexování souborů nebo zálohování vybraných dat. V tuto dobu také může váš virový skener spustit běžnou kontrolu systému.

VIR, NEBO WINDOWS? Přes malou ikonu v systémové liště otevřete antivirový program a podívejte se, zda skener kontroluje systém. V Ovládacích panelech pod ikonou »Naplánované úlohy« (ve Windows XP) nebo »Systém a údržba | Plánovat úkoly« (ve Windows Vista) zjistíte, zda je ve svolené době aktivní nějaká služba Windows. Zde také uvidíte, kdy budou spuštěny standardní „údržbářské služby". Automatické aktualizace jiných programů můžete najít například pomocí programu System explorer (konkrétně v sekci Autoruns | Startups).

6 Poruchový virový skener

Každý den se objeví 30 tisíc nových virů. To znamená, že je opravdovým hazardem pracovat bez nejnovějších signatur virů. Mnoho uživatelů však ani nezaregistruje, když si virový skener neinstaluje aktualizace, nebo se dokonce ani nespustí. To totiž obvykle nejsou bezvýznamné problémy, ale spíše velmi dobře mířené útoky některých virů na ochranné mechanismy počítače. Malware často dokáže paralyzovat virový skener nebo zachytávat přístup k aktualizačním severům. Někteří škůdci jdou ještě dále: detekují vyhledávací dotazy (třeba přes Google) například na klíčová slova „ochrana", „virus" nebo „antivir" a blokují či manipulují výsledky vyhledávání. Příčinou podobných problémů však mohou být dokonce i špatně přenesené soubory při aktualizaci nebo výpadky aktualizačního severu.

VIR, NEBO WINDOWS? Nejprve byste se měli pokusit spustit aktualizaci manuálně. Ve většině bezpečnostních nástrojů je tato volba obvykle k dispozici pod nabídkou „Update" nebo „Options". Výrobci antivirů také obvykle na svých stránkách zveřejňují informace o možných problémech s programem nebo haváriích aktualizačních serverů. Čím déle si však neaktualizujete bezpečnostní program, tím více stoupá riziko infekce.

Pokud se vám i nadále nedaří spustit aktualizaci nebo samotný virový skener, vyzkoušejte alespoň jeho internetovou alternativu. Pro rychlou kontrolu doporučujeme například nástroj od Esetu, který najdete na adrese **www.eset.cz/online-skener**. Tato a podobné služby zkontrolují váš počítač od RAM až po bootovací sektor, výhodou je také použití nejnovějších signatur.

7 Změněné uživatelské rozhraní

Falešné chybové hlášení s „legračními řádky", změněnými ikonami, zmatkem znaků na monitoru – ne každý vir musí nutně ničit nebo špehovat. Někteří autoři virů chtějí jen uživatele otravovat nebo demonstrovat svou sílu. Například vir Blusod generuje falešné „modré obrazovky" a tím pravidelně uživatele straší. Začnete-li panikařit a spustíte obnovu ze zálohy nebo reinstalujete Windows, způsobujete si zbytečné problémy.

VIR, NEBO WINDOWS? Viry se sice podobným způsobem chovat mohou, sotva však způsobí stálé poškození počítače. Pravda totiž je, že v zájmu skutečně nebezpečných virů je zůstat v utajení co možná nejdelší dobu. Další výhodou je, že podobní otravní škůdci se obvykle nezavrtávají příliš hluboko do systému, takže si s nimi bezpečnostní nástroje dokáží velmi rychle poradit. Pro jejich odstranění také často stačí bezplatný nebo internetový antivirový skener.

Nemůžete však samozřejmě počítat s tím, že všechny viry jsou neškodné. Pokud se nechcete stát snadnou kořistí internetových zločinců, vždy se ujistěte, že váš počítač má kvalitní ochranu.

AUTOR@CHIP.CZ

INFO

Tipy pro případ nouze

Co dělat, pokud se skutečně ukáže, že se na vašem počítači skrývá škůdce? Nepatříte-li mezi zkušené uživatele, můžete při mazání složek a souborů nadělat více škody než samotný škůdce. Nabízíme vám sedm tipů, jak se při odstraňování malwaru vyhnout totální destrukci systému:

- žádné unáhlené akce;
- nainstalujte/aktualizujte virový skener;
- odpojte se od internetu (odpojte síťový kabel) – poté již škůdce nemůže odesílat žádná data nebo instalovat další malware;
- vypněte a zapněte počítač – některé viry se skrývají v paměti RAM, která se při vypnutí „vyčistí";
- důležitá data zazálohujte na prázdné datové nosiče (ideálně na DVD), protože stávající zálohy mohou být malwarem poškozené;
- spusťte antivirový nástroj a eliminujte co nejvíce škůdců;
- nainstalujte si dodatečný bezpečnostní nástroj (například Gmer z našeho DVD) a opět zkuste najít a odstranit co nejvíce malwaru.