Cíl zaměřen: Malware

S rostoucím počtem malwaru klesají i **DETEKČNÍ A DEZINFEKČNÍ SCHOPNOSTI KLASICKÝCH ANTIVIRŮ**. Jak tedy poznat, zda je váš počítač skutečně napaden, a jak se nákazy zbavit? Poradíme vám základní triky pro „přežití“.

PETR KRATOCHVÍL

Nástroje určené k boji proti malwaru ušly za poslední rok pěkný kus cesty. Minimalizace systémových nároků, pulzní updaty, cloud computing – na první pohled by se mohlo zdát, že navrch teď jednoznačně mají ti „dobří“. Bohužel, nespala ani temná část internetu a vývoj virů a malwaru je také o něco dále (více informací na toto téma najdete v článku o supervirech na straně 56). Pokud jsou tedy síly vyrovnané, rozhodují použité prostředky a především možnosti a schopnosti uživatele. Stejně jako v klasické válce patří i zde k nejdůležitějším bodům identifikace protivníka (v tomto případě malwaru). V minulém Chipu jsme vám ukázali základní identifikační znaky platící pro počítače napadené malwarem, konkrétní identifikace však chyběla. Jak tedy poznáte, kdo konkrétně na váš počítač zaútočil?

Obvyklá situace

Počítač oběti je zamořen malwarem. Spouští se desítky procesů, při pokusu o jejich odstranění jsou aktivovány nové a nové, navíc je připojení k internetu „čímsi“ zpomaleno. Ochranné prostředky Windows jsou odstraněny nebo blokovány, antivirové nástroje třetích stran se bezradně znovu a znovu pokoušejí počítač vyčistit. Marně. Cesta k řešení problému není jednoduchá. Prvním krokem by mělo být zjištění, kde a jak byl váš počítač napaden.

Programů, které dokáží zkontrolovat systém a najít škůdce, je celá řada. Už několikrát jsme se v Chipu zmiňovali o on-line skenerech, které dokáží z browseru prohledat počítač a najít (v některých případech i odstranit) vir či jinou hrozbu. Tento typ nástrojů má ale několik nevýhod: vyžaduje stabilní připojení k internetu a poradí si pouze s určitým typem hrozeb.

Vyhledej a znič

V některých situacích mohou být efektivnější nástroje označované jako systémové analyzátory, které se zaměří na nejčastěji napadané oblasti systému a ty prohledají. Nalezené položky roztřídí a označí, aby s nimi bylo možné dále pracovat. Obvyklá je i možnost exportu výsledků pro externí analýzu. Ve finále je možné podezřelé položky zablokovat nebo smazat.

HijackThis

Prvním z nástrojů, které dokáží zjistit, „co se děje“, a zároveň se postavit méně zkušeným záškodníkům, je program HijackThis. Tento praktický nástroj, vyvíjený nyní pod taktovkou firmy TrendMicro, najdete jak na našem DVD, tak i například na stránce **http://free.antivirus.com/hijackthis/**. A co HijackThis umí? Po jeho spuštění se objeví jednoduché okno s několika málo tlačítky. Většinu uživatelů ale bude zajímat jen jediné: »Do a system scan and save log file«. Po kliknutí na něj provede program hloubkovou prohlídku systému a vytvoří záznam s nejdůležitějšími údaji – záznamy z registrů, spuštěnými službami nebo programy spouštěnými při startu. Pokud máte podezření, že se na vašem počítači ukrývá záškodník, stačí tento záznam ukázat odborníkovi a ten vám prozradí, zda je tomu opravdu tak. Existuje také celá řada diskusních fór, kde vám po zveřejnění logu poradí zkušenější uživatelé (jako příklad lze uvést web **www.viry.cz/forum/**).

To nejlepší si jako obvykle necháme na konec – pomocí automatického analyzátoru můžete z logu programu HijackThis zís-

NAJDETE NA CHIP DVD

Kontrola systému a odstranění malwaru

Ultimate Process Manager ► detekuje a odstraňuje malware

HijackThis ► provádí kontrolu ohrožených částí Windows

ComboFix ► skenuje počítač a odstraňuje nebezpečný malware

WinSock Fix ► opravuje připojení k internetu „poškozené“ malwarem

ESET SysInspector ► kontroluje počítač a hledá malware

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

kat informace okamžitě. Stačí ho nahrát na web **www.hijackthis.de/cz**, a během několika sekund zjistíte, jak si „stojíte“. Jen je důležité zmínit, že jde o německou službu, která je částečně lokalizovaná. To znamená, že v některých případech je nutné ignorovat varování „Eventuálně špatný!“, protože v českých Windows se (na rozdíl od databáze této služby) programy neinstalují do složky „c:\programme\“...

Posledním krokem by mělo být označení nebezpečných položek v okně programu HijackThis a kliknutí na tlačítko »Fix checked«.

HODNOCENÍ: Jednoduchý program i pro méně zkušené uživatele, který boduje především možností automatické kontroly „logu“ a celou řadou „skrytých“ funkcí.

TIP PRO ZKUŠENĚJŠÍ UŽIVATELE: Pokud toho o počítačích víte více a chcete si log programu zkontrolovat sami, budete potřebovat informace o zkratkách a číselných kódech, které HijackThis používá. Ty najdete například na adrese **http://hjt-data.trendmicro.com/hjt/analyzethis/hijackthis-codes.htm**.

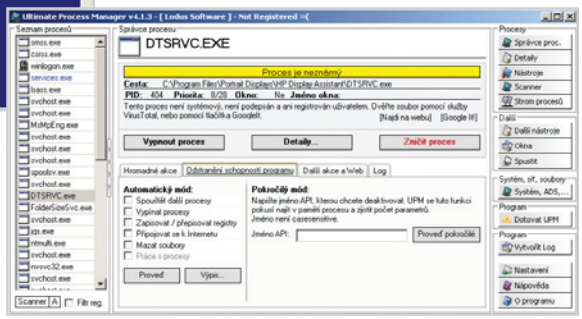
Ultimate Process Manager

Ačkoliv i nástroj HijackThis prochází neustálým vývojem, rozhodně v tomto směru nestačí tempu, které udržuje český nadšenec s přezdívkou Lodus, autor alternativního analyzátoru nazvaného Ultimate Process Manager. Tento profesionální nástroj toho nabízí mnohem více než HijackThis, běžný uživatel však patrně využije jen zlomek jeho schopností. Jak už z jeho názvu vyplývá, jeho dominantou je práce s procesy. O vybraném procesu nabídne zcela bezkonkurenční množství informací a navíc snadnou cestu ke zjištění dalších podrobností pomocí Googlu. Ve srovnání se Správcem úloh systému Windows však boduje ještě několika praktickými funkcemi. Jako nejdůležitější lze označit tu, která se skrývá pod tlačítkem „zničit proces“ – tato funkce totiž dokáže odstranit i obzvlášť nepříjemný proces včetně jeho „zdrojového“ souboru. Zkušenější uživatelé budou nadšeni sekcí „Odstranění schopností programu“, kde lze vybranému procesu zabránit ve spouštění dalších procesů, v mazání souborů nebo v přístupu k internetu. Ultimate Process Manager je zkrátka funkcemi nabitá zbraň pro pokročilé uživatele. Zklamáni ale nebudou ani začátečníci – ti ocení například „Scanner“, který prověří spuštěné procesy, a především vytváření „logů“, které lze předat k posouzení IT odborníkům. Logy lze nechat „prověřit“ na celé řadě míst. Kromě již zmiňovaného fóra serveru Viry.cz lze doporučit i návštěvu diskusního fóra slovenského bezpečnostního portálu SecIT (**http://secit.sk/forum/**), kde je možné „narazit“ i na autora programu. Na závěr lze už jen připojit varování: Zatímco v rukou zkušeného „virobijce“ se UPM může proměnit v ultimativní zbraň, nezkušený uživatel může jeho pomocí zničit svá Windows dřív, než řeknete „nová nátěrová barva“. Více než kdekoliv jinde zde tedy platí: „Klikejte“, jen když jste si zcela jisti...

HODNOCENÍ: Neznáme jiný program se stejně širokou nabídkou funkcí a s podobnými funkcemi. Zcela jednoznačné doporučení pro IT profesionály...

TIP PRO MÉNĚ ZKUŠENÉ UŽIVATELE: Popis všech funkcí a možností programu by zabral podstatnou část Chipu, a i shrnutí těch nejdůležitějších by zcela zaplnilo tento článek. Pokud ale chcete rychle odhalit základní „pracovní triky“, podívejte se na stránkách autora (**www.lodusweb.net**) na

Musíte důvěřovat: Z obsahu okna programu nelze odhadnout, co právě ComboFix dělá...



Bez konkurence: Ultimate Process Manager je funkcemi nabitá zbraň pro boj s malwarem určená pro pokročilé uživatele.

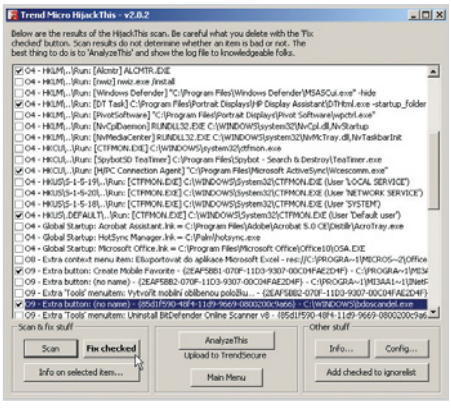
ukázková videa. Poradí vám, jak odrovnat i ty nejnebezpečnější škůdce.

ComboFix

Zatímco oba předchozí nástroje vyžadovaly „zkušenou ruku“, ComboFix je určen spíše začátečníkům. Tomu odpovídá i jeho taktika – po spuštění vytváří bod obnovy a během „práce“ nedává uživateli šanci cokoliv ovlivnit. Proskenuje systém, automaticky odstraní „nebezpečné soubory“ a vygeneruje log, který je opět možné zaslat k prozkoumání na celou řadu diskusních fór.

Zkušenějším uživatelům ale ComboFix nedoporučujeme – jeho metody pro ně budou příliš „znervózňující“. Vůbec totiž nelze odhadnout, co právě program dělá – na obrazovce vidíte v modrém okně jen hlášení „Dokončena fáze 20“, „Dokončena fáze 21“...

Poté nástroj automaticky smaže „nebezpečné“ soubory a zobrazí log. Během skenu vyžaduje vypnutí browseru a také deaktivuje přístup k některým komponentám Windows. Na testovacím počítači sice našel (a smazal) ukrytý malware BrilliantDigitals, zároveň ale odstranil i dll soubor z on-line skeneru BitDefenderu. Profesionálové zkrátka tímto nástrojem příliš nadšeni nebudou. Nástroj najdete jak na našem DVD, tak i na adrese **www.combofix.org**.



Snadná pomoc: Po kliknutí na tlačítko »Do a system scan...« provede program prohlídku systému a vytvoří záznam s nejdůležitějšími údaji.

HODNOCENÍ: Pomalejší nástroj na kontrolu počítače pro méně zkušené uživatele. Kontroverzní funkcí je automatické odstranění nebezpečných souborů.

TIP PRO ZKUŠENĚJŠÍ UŽIVATELE: Jednou z praktických „perliček“, které lze v logu programu ComboFix najít, jsou naposledy vytvořené soubory. Z nich lze poměrně snadno poznat, kde a jak malware řádil...

Bez virů a bez internetu

Některé typy malwaru jsou natolik zákeřné, že razantně modifikují nastavení připojení k síti. Pokud jsou v systému, obvykle připojení pouze zpomalují a omezují, po jejich odstranění však přestane připojení k internetu fungovat zcela.

Typickým příkladem je adware New.Net (někdy také označovaný jako Newdotnet). Ten se obvykle do počítače dostane „legálně“ s dalším softwarem – jeho autoři totiž počítají s tím, že většina uživatelů podmínky užívání jen „odkliká“ – a poté začne řádit. Nejprve se zpomalí internet, poté se začnou objevovat vyskakovací okna a lišty a končí to bizarními problémy typu „nefunguje kopírování do/ze schránky“. Pokud adware odstraníte klasickým antivirem, přestane fungovat připojení k internetu – obvykle se objeví hlášení „omezené nebo žádné připojení“. Na vině je adwarem modifikovaný Winsock, který nefunguje tak, jak by měl.

Řešení tohoto a podobných problémů je několik. Microsoft na svých stránkách nabízí poněkud komplikovanější návod, jak problémy s Winsockem řešit (**http://support.microsoft.com/kb/811259**).

Pro méně zkušené uživatele a operační systém Windows XP lze doporučit nástroj WinSock XP Fix (**www.snapfiles.com/get/winsockxpfix.html**), který dokáže pomoci při většině problémů.

Pokročilí uživatelé mohou využít program LSP Fix (najdete ho na **http://download.chip.eu/cz/download_cz_1520896.html**).

PETR.KRATOCHVÍL@CHIP.CZ

INFO

Postup při „čištění“ počítače

1| **Nepropadejte panice.**
2| **Připravte si na disk všechny důležité nástroje.**
3| **Spusťte HijackThis a jeho log si nechte automaticky zkontrolovat na webu. Odstraňte označený malware.**
4| **Spusťte Ultimate Process Manager, vytvořte log a nechte si ho zkontrolovat odborníky.**
5| **Odstraňte označený malware.**
6| **Nainstalujte kvalitní firewall (například Outpost z našeho DVD, rubrika Plné verze).**
7| **Zkontrolujte počítač pomocí on-line antiviru (například od Esetu).**
8| **Zbývajících škůdců se zbavte pomocí aplikací KillBox a Avenger (viz níže).**

KDYŽ JE ŠPÍNA ZAŽRANÁ

U některých zvláště odolných typů malwaru je úspěšnost klasického smazání poměrně nízká – obranné systémy škůdce ho dokáží neustále obnovovat. Zde tedy musí nastoupit specializované nástroje, které dokáží vybrané soubory odstranit při restartu počítače. K nim patří například již několikrát zmiňované programy Pocket Killbox a The Avenger. V jednodušším Killboxu stačí jen označit požadovaný soubor (či soubory) a zvolit metodu odstranění – doporučujeme »Delete on reboot« nebo »Replace on reboot (Use Dummy)«. Složitější Avenger vyžaduje vytvoření skriptu s popsáním požadovaných operací. Na rozdíl od svého jednodušího kolegy si ale poradí i s rootkity.

Potřebujete okamžitě smazat soubory, které si malware úzkostlivě chrání? Vyzkoušejte FileAssasin, který si poradí i s vícenásobným blokováním. Aktuální verzi najdete na adrese **www.malwarebytes.org/**fileassassin.php.

Poznámka: Všechny výše uvedené „operace“ zvládne i profesionální Ultimate Process Manager. Pravda ovšem je, že nalezení těchto funkcí a práce s nimi je podstatně složitější než u zmiňovaných „jednoúčelových“ nástrojů.

NEJSTE SI JISTI?

Je to malware, nebo neškodný systémový soubor? Toto dilema patří k nejčastějším problémům při čištění počítače od škůdců. V případě nejistoty doporučujeme využít on-line souborové virové skenery. Mezi nejlepší patří **www.virustotal.com** a **http://virscan.org/**.

Oba nástroje dokáží dilema „mazat, nebo nemazat“ jednoznačně vyřešit...

Nezapomeňte před jakoukoliv podobně rizikovou operací zazálohovat všechna důležitá data...