Demaskovaný spyware

Vlci v rouše beránčím – právě toto biblické přirovnání přesně charakterizuje nebezpečné nové „superviry". Jejich zdánlivě mírumilovnou masku se nám podařilo strhnout. *Valentin Pletzer, autor@chip.cz*

V tomto článku najdete

Svůj počítač nepochybně chráníte a systém pravidelně aktualizujete. Správně. A věříte, že jste tak imunní proti spywaru a trojským koním? To ale nemusí být zcela pravda!

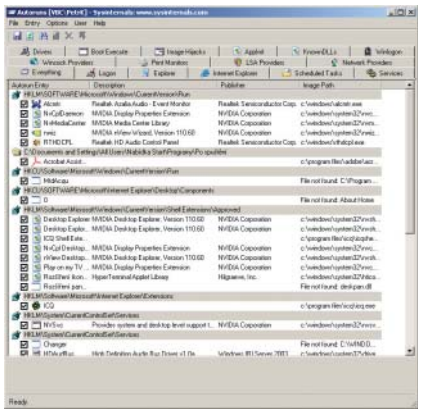
Kdo se spoléhá například na nějaký freewarový antivirový nástroj, jen se nechává ukolébat falešným pocitem bezpečnosti. Celá řada testů ukazuje, že tyto programy nic nezmohou právě proti té nejzákeřnější kategorii škůdců – spywaru. V boji proti moderním záškodníkům však pravidelně selhávají i komerční programy a speciální nástroje jako Spybot Search & Destroy a Ad-Aware.

Jak se tedy dá spyware odhalit, a hlavně – jak se jej zase zbavit? Abychom to vyzkoušeli, na našem testovacím počítači jsme „nainstalovali" tři nejrozšířenější škůdce. Výsledek pokusu byl téměř šokující: známé standardní nástroje je většinou nedokázaly odstranit. Nelze se však příliš divit, neboť tito špioni téměř denně mění svou tvář – tedy „krycí" jméno souboru a úkryt v systémovém registru. Dlouho nepomáhaly dokonce ani zkušenosti a vědomosti našeho „všemi mastmi mazaného" virového experta. „Já tu bestii snad nedostanu," bědoval na setkání týmu. Teprve krátce před uzávěrkou se přece jen podařilo spyware definitivně vymazat – pomocí následujících triků a nástrojů.

SPYSHERIFF

Důsledné odstranění falešného antispywaru

Jeden zvláště proradný trik používá SpySheriff: v převlečení za antispywarový nástroj (rogue antispyware) přiměje svou oběť k tomu, aby si tento malware dobrovolně nainstalovala. Kdo vábení podlehne, ten už se vetřelce nezbaví. Ale nejdrzejší fintu si SpySheriff nechává na konec: při předstírané kontrole objeví v počítači množství škodlivých programů – které samozřejmě neexistují. Ten, kdo se chce imaginárních záškodníků zbavit, má zaplatit – jak jinak než kreditní kartou.



AUTORUNS: Tento nástroj zná všechny úkryty v systémovém registru....

Jak poznat „záškodníka"

Malware SpySheriff poznáte podle toho, že vás trvale bombarduje varovnými zprávami typu „Tento počítač je infikován" a neustále vám připomíná, že si máte koupit plnou verzi. To však často bývá jen špička ledovce. Špion se případ od případu chová různě: někdy se nainstaluje jen falešná antispywarová komponenta, jindy navíc ještě trojský kůň. Jisté je jen jedno: proti skutečnému spywaru nástroj nepodnikne vůbec nic!

Jak odstranit SpySheriff

Překvapující je skutečnost, že pro SpySheriff existuje odinstalační rutina. Nenajdete ji sice v nabídce Start, ale určitě v Ovládacích panelech v sekci *Přidat nebo odebrat programy*. Využijte této příležitosti a odešlete SpySheriff do věčných lovišť – ale jenom na to se nespoléhejte. Kde se tento malware určitě pokaždé uhnízdí, to vidíte v našem „zatykači". Uvedené položky a soubory lze zcela normálně odstranit po- →

→ mocí Průzkumníka Windows a editoru registru.

Jistota je jistota

V našich testech se různé falešné antispywarové programy dařilo odstraňovat dodaným odinstalátorem. V příslušných internetových fórech (například na **www.viry.cz**) si však postižení neustále stěžují, že se toho v jejich počítačích uhnízdilo ještě více. Při podlých obchodních praktikách malwaru SpySheriff a spol. skutečně nelze vyloučit, že falešný antispyware s sebou zavlekl ještě další škůdce. Proto byste si pro jistotu měli osvojit také následující tipy, které používáme proti oběma zbývajícím diverzantům, a svůj systém důkladně prozkoumat pomocí nástrojů HijackThis, Autoruns a Blacklight.

Profil pachatele

Jméno
SpySheriff

Charakteristika
Vydává se za virový skener

Alias
Adware Sheriff, SpyAxe, SpywareQuake

Aktivní procesy
1950.exe, newdial.exe, spysheriff.exe, uninstall.exe, winstall.exe

Úkryty v systémovém registru
HKLM\SOFTWARE\spysheriff,
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\uninstall\spysheriff

Krycí názvy souborů
%ProgramFiles%\spysheriff,
1950.exe, Desktop.html, newdial.exe, spysheriff.exe, uninstall.exe, winstall.exe,
%UserProfile%\Desktop\SpySheriff.lnk

VUNDO

Jak se definitivně zbavit agresivních hijackerů

Druhý škůdce, na kterého jsme se zaměřili, je bezesporu nejagresivnější. Abychom jím nakazili náš testovací počítač, hledáme na Googlu „hacknuté“ sériové číslo. V těchto lákavých, nicméně ilegálních nabídkách se totiž často skrývají hijackery (spyware měnící domovskou stránku) a downloadery (stahovače). Google nás sice před potenciálně škodlivou stránkou varuje, jeho radu však ignorujeme a stránku otvíráme.

Nebezpečný podvod

Zdánlivě nevinná webová stránka skrývá jeden z nejzákeřnějších škodlivých programů: SpySheriff.

Profesionální logo a elegantní balení propůjčují malwaru zcela seriózní vzhled.

Tlačítko FREE SCAN však nespouští bezplatnou antivirovou kontrolu, nýbrž EXE soubor, který váš počítač infikuje spywarem SpySheriff.

Popis produktu působí dojmem, že jde o skutečný antispyware. Kdo program nezná, snadno padne do léčky.

NAJDETE NA CHIP DVD

Nástroje, které zlikvidují každý spyware

Jakmile se malware v počítači jednou usadí, lze se jej zbavit jen pomocí správných nástrojů. Ty nejlepší jsou pro vás připraveny na Chip DVD v sekci Servis pro PC.

HijackThis
Pomocí tohoto nástroje lze zvláště dobře najít a odstranit prohlížečové hijackery, ovšem jen tehdy, pokud znáte jejich silné i slabé stránky.
www.hijackthis.de/cz

Autoruns
Tento profesionální nástroj zná všechny úkryty v systémovém registru, které se dají využít jako platforma pro automatické spouštění. Domníváte-li se, že máte v počítači nějaký malware, s tímto programem máte dobrou šanci, že jej najdete a zabráníte jeho spuštění.
www.microsoft.com/technet/sysinternals/default.mspx

Process Explorer
Na vypátrání a zastavení spywarových procesů bohužel „palubní" prostředek Windows, Správce úloh, nestačí. Tento problém však zvládá Process Explorer, který kromě toho nabízí i řadu dalších funkcí.
www.microsoft.com/technet/sysinternals/default.mspx

Pocket KillBox
Metody spywarových záškodníků jsou čím dál tím neurvalejší. Sotva jeden proces ukončíte, nějaký jiný jej znovu spustí. S tím však KillBox definitivně skoncuje.
www.killbox.net

F-Secure BlackLight
Stále častěji se malware schovává pomocí techniky rootkitů. Tento nástroj firmy F-Secure škůdce v jejich úkrytu odhalí – nebo alespoň jejich většinu.
www.f-secure.com

Gmer
Samotný „antirootkit" na analýzu nestačí. Ne každý nástroj totiž zná všechny triky. Tento software se zvláště dobře hodí jako doplněk k nástroji BlackLight.
www.gmer.net

Pak už jde všechno velice rychle: „sestaví" se stránka, aktivuje se škodlivý kód, PC je infikován. Náš záškodník se jmenuje Vundo a patří mezi stahovače. To však zjišťujeme až později, když jistý podezřelý soubor necháváme zkontrolovat celkem 18 virovými skenery. Jen hrstka z nich však stahovač vůbec dokázala identifikovat. A jak už název typu malwaru naznačuje, náš nový přírůstek ihned začíná stahovat další softwarové bandity. V našem případě je to doplněk pro Internet Explorer, který nás okamžitě bombarduje reklamními „pop-upy" všeho druhu.

Profil pachatele

Jméno
Vundo

Charakteristika
Napadá virové skenery

Typ
Hijacker, stahovač a trojský kůň

Procesy
Dva pokaždé náhodně generované DLL soubory

Úkryty v systémovém registru
HCR\clsid\{EFCB1D95-FFF6-47BB-B6C9-61A523F04322},
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

Úkryt na pevném disku
C:\Windows\System32\

Abychom agresora zničili, instalujeme si freewarový Ad-Aware 2007. Tento nástroj sice Vundo rozpozná, avšak není schopen stahovač kompletně zlikvidovat – ten se v počítači po každém restartu znovu objeví. Ještě hůře jsme dopadli s nástrojem Spybot Search & Destroy: spouštíme setup, ale nemůžeme jej dokončit. Vundo pokaždé proces ukončí a znemožní tak úspěšnou instalaci svého protivníka. Nezbývá tedy než nasadit zbraně těžšího kalibru.

Rozpoznání škůdce

Dokud je třeba jen jediný proces záškodníka aktivní, nelze jej ze systému odstranit. Proto je nutné nejprve malware i všechny jeho úkryty identifikovat. Za tímto účelem si nainstalujte nástroj Autoruns (zdarma ke stažení na **www.sysinternals.com**).

Tento freeware koná v podstatě stejnou práci jako mezi lovci spywaru oblíbený program HijackThis. Na rozdíl od něj však vypisuje všechny položky automatického spuštění v systémovém registru, neboť – nikoli jako ještě před několika lety – dnes se malware už nezanáší jen pod „Run" nebo „RunOnce". Například právě Vundo se zahnízdí hned na třech různých místech.

Abyste je dokázali lokalizovat, spusťte Autoruns a nejprve zaškrtněte volby *Verify Code Signatures* a *Hide Microsoft Entries*. To má dobrý důvod: každý spustitelný soubor může být výrobcem opatřen jménem a digitální signaturou. Tak je tomu například také u každého originálního souboru od Microsoftu. Zmíněná nastavení tyto soubory odfiltrují a ušetříte si tak spoustu „rešeršní" práce.

Zbývající soubory musíte prověřit manuálně. I s tím vám pomůže Autoruns. Na zvolenou položku klikněte pravým tlačítkem myši a pak klikněte na *Search online...* Tak se začne název souboru hledat vyhledávačem Microsoftu Live.com. V některých případech se tak dají identifikovat soubory známých škůdců. Nakonec vám zbude seznam pochybných souborů a položek registru, které byste měli vymazat.

Deaktivace škůdců

Vundo je bohužel natolik agresivní, že nestačí pouhé odstranění jeho položek ze systémového registru. Aktivní komponenty drzého vetřelce je totiž ihned zase obnoví. Pomůže však jeden trik: ze stránky **www.sysinternals.com** si stáhněte Process Explorer a spusťte jej. Po krátkém prohledávání pak nástroj vypíše všechny aktivní procesy. Naše finta spočívá v tom, že soubory hijackeru nevymažeme z paměti, ale nejdříve je pouze pozastavíme. Klikněte proto pravým tlačítkem myši na podezřelý proces a zvolte *Suspend*. Tak proces pouze uspíte – a kontrolní rutina ostatních procesů →

F-SECURE BLACKLIGHT: Jeden z pomocníků v boji proti rootkitům.

→ hijackeru si toho nepovšimne. Teď už máte skoro vyhráno.

Odstranění hijackeru

Poté, co jste útočníka pomocí Process Exploreru zastavili, můžete jej pohodlně odstranit. Nejprve si poznamenejte názvy a cesty všech těch souborů, které jste mohli přiřadit vetřelci. Pak v Process Exploreru příkazem *Kill* ukončete všechny procesy, které jste předtím uspali příkazem *Suspend*.

V dalším kroku je třeba nástrojem Autoruns vymazat všechny položky, které se vám podařilo identifikovat. Klikněte proto pravým tlačítkem myši na podezřelou položku a zvolte *Delete*. Nyní už je nebezpečí téměř zažehnáno. V závěrečném kroku ještě odstraňte nebezpečné soubory, aby nemohly být vyvolány třeba nedopatřením. Po restartu by váš systém už měl být od záškodníků osvobozen. A znovu budou fungovat i Spybot Search & Destroy a Ad-Aware. Pomocí těchto nástrojů teď ještě zkontrolujte, zda jste opravdu nic nepřehlédli.

ZLOB

Spolehlivé odstranění nebezpečných videokodeků

Pomocí titulků jako „Nahá Paris Hilton“ či „Všechny filmy zdarma“ se vás snaží přilákat webové stránky, které mají jediný cíl: dostat pod kontrolu vaše pécéčko. Jejich trik je prostý: kdo si takto propagovaný film chce pustit, musí si zároveň nainstalovat nabízený kodek – a už má v počítači malware jménem Zlob. Z testovacích důvodů na falešnou hru přistupujeme, a náš počítač je také okamžitě infikován. Žádné napadení ovšem zpočátku nepozorujeme, neboť podvržený kodek má dokonce i oficiální odinstalační rutinu. To je samozřejmě podvod – takto se Zlob úplně odstranit nedá.

Odhalení škůdce

První známka toho, že něco není v pořádku, se objeví v síťových nastaveních. V domácí síti obvykle name servery přiděluje DHCP server. Znamená to, že o přiřazování adres se stará DSL router, a v počítači s Windows je nastavena volba *Získat adresu serveru DNS automaticky*. Falešný kodek však nainstaluje trojského koně DNS-Changer, který aktivuje vlastní servery. Jakmile je jednou nainstalován, může provozovatel serveru sledovat každý krok oběti, a dokonce jej i přesměrovat. Tuto modifikaci dokážou nástroje jako Spybot Search & Destroy rozpoznat a opravit. Jenomže příčina toho všeho, totiž rootkit, zůstává aktivní. A tak je po restartu počítače vše při starém – a tedy špatně.

Zviditelnění rootkitu

Aby sám sebe ochránil před nežádoucími přístupy, uchyluje se trojský kůň DNS-Changer ke zvláště vychytralému triku: požadavky na souborový systém nedostane ke zpracování přímo operační systém, ale nejprve jsou zmanipulovány v rootkitu. Bezpečnostní programy se o trojském koni vůbec nedozvědí, poněvadž ten sám sebe prostě vyškrtl ze seznamu. A právě na tom ztroskotají Spybot Search & Destroy, Ad-Aware a další antispyware. Tady pomůže jen „protirootkitový“ nástroj – bohužel však ne každý. Například Rootkit Revealer firmy Sysinternals vetřelce neodhalí. Dokáže to však Blacklight od firmy F-Secure. Pokud jím počítač proskenujete, nástroj najde EXE soubor, jehož název sestává z „kd“ a trojice dalších, náhodně zvolených písmen.

Odstranění škodlivého kódu

Program od firmy F-Secure nabízí funkci výmazu. Aktivujte ji a pak nezapomeňte ihned restartovat počítač, jinak bude v paměti trojský kůň i nadále aktivní a v nejhorším případě dokáže sám sebe obnovit. Po restartu ještě musíte ze systémového registru odstranit položku pod klíčem Winlogon (viz „profil pachatele“). Spusťte proto Autoruns a otevřete záložku *Logon*. Tam uvidíte položku, kterou byste měli po stisku pravého tlačítka myši volbou Delete vymazat. Jinak se může stát, že při příštím spuštění počítače bude z adresáře „System32“ zaveden stejnojmenný soubor. Případné zbytky malwaru už lze opět odstranit pomocí programů Spybot Search & Destroy nebo Ad-Aware. A pak bude s vetřelcem definitivně konec!

Valentin Pletzer

Profil pachatele

Jméno
Zlob

Charakteristika
Skrývá se pomocí rootkitu

Alias
DvdCodec, UseCodec, KeyCodec, EliteCodec, PerfectCodec, PornMagPass, QualityCodec, VCCodec, XPassword Generator, ZCodec, ZipCodec

Procesy
kd*.exe

Úkryt v systémovém registru
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\System

Úkryty na pevném disku
C:\Windows\System32\kd*.exe,
C:\Programme\PornoPlayer*.*

Jiné
Mění nastavení DNS serveru v síti