Pekelné počítačové nástroje

Malé děti se straší bubáky, starší školou a počítačová veřejnost je pravidelně strašena rootkity. **ĎÁBELSKÉ NÁSTROJE**, které nelze odhalit, jsou na žebříčku nebezpečí obvykle hodně vysoko. Také se bojíte?

PETR KRATOCHVÍL

Vzpomenete si, kdy se naposledy počítače v klasických médiích objevily v „pozitivním kontextu“? Kdy naposledy někdo zdůraznil, jak nám zjednodušují a zpříjemňují život? Většina počítačových příspěvků (především v TV) má nádech katastrofy, ve které jsou počítače tajně napadány viry, nebo dokonce slouží jako nástroje zločinců. Radikální názor důchodkyně Věry Pohlové (**cs.wikipedia.org/wiki/České_internetové_memy**) je pak téměř logický.

Ale abychom příliš neodbočili – nádech tajemna a záškodnictví do světa škůdců přinesly už v počátcích počítačů tzv. stealth viry. Ty dokázaly falšovat určité údaje a tím maskovat přítomnost záškodníků. Jenže zatímco v dobách minulých bylo hlavním cílem viru počítač infikovat a poté „poškodit“, moderní škůdci mají zcela jiné úkoly a jejich cílem je zůstat v utajení co nejdéle. A právě zde vstupují do hry rootkity.

Co je to rootkit

Ačkoliv to bude znít překvapivě, historie „rootkitů“ je už dlouhá několik desítek let. Dříve byl tento pojem spojen především se světem Unixu, kde označoval program maskující činnost „hackera“. Do světa Windows se rootkity dostaly až nedávno, přičemž tu pravou pozornost jim zajistila firma Sony BMG. Zjednodušeně lze tedy říci, že rootkit je program umožňující maskování činností v počítači. V praxi si to lze představit tak, že pokud například antivirový program zažádá o seznam spuštěných procesů nebo aplikací komunikujících s internetem, rootkit dokáže žádost zachytit a odpověď upravit tak, aby zakryl vybrané programy a aktivity.

Obvykle se rootkity ještě dělí na „kernel mode“ a „user mode“ (podle úrovně, na které rootkit pracuje). Druhá kategorie používá obvykle techniku „úpravy cest“, přičemž pracuje mezi aplikací a tzv. API funkcemi operačního systému. Díky tomu je lze pomocí specializovaných nástrojů relativně snadno odhalit. Jako zajímavost lze uvést, že populární „detektor“ Hijackthis tyto záškodníky nezjistí…

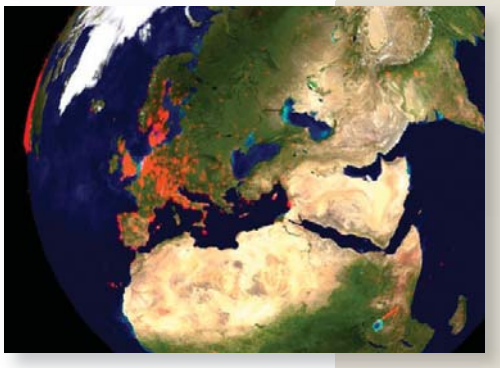
První kategorie rootkitů běží na úrovni kernelu (tzv. ring 0) a je z hlediska detekce mnohem obtížnější. Tyto rootkity totiž pracují s nejvyššími právy a zjednodušeně lze říci, že si mohou se systémem dělat cokoliv.

Zdroj informací: Jeden z mála webů s informacemi o rootkitech najdete na adrese www.rootkit.cz.

Zaujalo nás:

64bitová verze Windows Vista používá technologii Kernel Patch Protection (**http://blogs.msdn.com/windowsvistasecurity/archive/2006/08/11/695993.aspx**), která by měla zamezit cizím zásahům a manipulacím s jádrem systému – například nahrazení systémových služeb.

Rootkity lze také rozdělit na dvě kategorie podle toho, zda slouží pouze jako „plášť neviditelnosti“ pro ostatní škůdce, nebo zda vykonávají další činnost. A protože i v oblasti vytváření malwaru dochází k čím dál tím větší specializaci, přibývá především rootkitů první kategorie. Smutným paradoxem je, že zatímco všechny kategorie programů přibírají na objemu (výjimkou není ani ovladač tiskárny o velikosti



Planeta Sony: Víte, kde v Evropě znají rootkit z hudebních CD?

INFO

Rootkit na výsluní

Firmě Sony vděčíme za popularizaci walkmanů, herních konzolí… a rootkitů. Byl to právě případ firmy Sony, který vynesl rootkit do světel reflektorů a upozornil uživatele, jaké nebezpečí rootkity představují.

O co tedy šlo? Firma Sony BMG se (logicky) snaží chránit svá hudební CD před pirátskými aktivitami. Vzhledem k tomu, že většina běžných ochran je prolomena během několika dní, rozhodla se zřejmě nasadit „větší kalibr“. Tím byl program XCP, který se vetřel do počítače a začal tam „kouzlit“. Skrýval programy začínající na sys, zbytečně vytěžoval procesor a sbíral informace o přehrávaných CD a odesílal je (poněkud nešikovně) Sony. Jeden nadšenec dokázal tyto informace nádherně zobrazit přímo na mapě (**www.doxpara.com/?q=sony**). Stačí jen kliknout v dolní části stránky na odkaz (USA, Asia nebo Europe), a hned víte, kde jsou CD s ochranou XCP nejvíce rozšířena.

Na tento „první komerční rootkit“ přišel (pomocí programu Rootkit Revealer) jeden z největších odborníků na Windows Mark Russinovich ze Sysinternals (ano, asociace s programem Process Explorer je správná), který vše zveřejnil na svém blogu. Následovalo mediální peklo, ve kterém se firma Sony zpočátku divoce mrskala: „Většina lidí stejně neví, co rootkit je, tak proč by je to mělo zajímat.“ Až poté, co se objevily první žaloby (a škůdci využívající tento rootkit ke skrytí své činnosti), přiznala porážku a ustoupila. Celá věc měla ještě dohru, a to i proto, že kroky k nápravě byly zpočátku spíše laxní. Pro většinu uživatelů však byla důležitá především informace, jak rootkity fungují.

Pokud vás tento případ zaujal, pak vám doporučím k přečtení výborný článek na serveru CD-R (**www.cdr.cz/a/16233**), kde se dozvíte o zajímavé předehře a o tom, že Mark Russinovich nebyl až tak úplně první…

stovek MB), velikost většiny rootkitů je menší než 10 KB. To znamená, že je lze do počítače nenápadně propašovat jako přílohu mailu, na USB disku nebo jako součást malwaru (tak tomu bylo například u viru Sober.p).

Jak se nenakazit

I přes poněkud přehnanou pověst není zpočátku rootkit o nic nebezpečnější než obyčejný vir. Pokud navíc dodržujete několik jednoduchých zásad, nemusíte se rootkitu bát vůbec.

1) NEPRACUJTE S ADMINISTRÁTORSKÝMI PRÁVY

Staré, nicméně stále doporučeníhodné pravidlo. Pracujete-li na počítači jako „obyčejný“ uživatel, riziko instalace nebezpečného „kernel mode“ rootkitu zmenšíte na minimum...

2) NEINSTALUJTE NEZNÁMÉ PROGRAMY

Narazili jste na internetu na program, který vás zaujal? Zjistěte si, například pomocí Googlu, zda už si na něj někdo nestěžoval. Velké riziko hrozí především na pochybných stránkách, které nabízejí různé lišty a stahovače...

3) POUŽÍVEJTE ANTIVIR S AKTUÁLNÍMI DEFINICEMI

V první fázi může rootkit odhalit i obyčejný antivir. Pokud máte na svém počítači kvalitní antivir s aktuálními signaturami, měl by vás na rootkit upozornit už při jeho stahování. Jestliže antivir nemáte, zkuste alespoň zběžnou kontrolu (**http://virusscan.jotti.org/** – limit 10 MB na soubor).

Příznaky aneb Máte ho...

Odhalit samotný rootkit není zrovna jednoduché (i když námi nabízené nástroje to dokáží). Existuje však celá řada náznaků, které vám napoví, že máte v počítači nezvaného hosta. Jedním z dřívějších příznaků přítomnosti rootkitu byla nestabilita systému – ne všichni „vývojáři“ věnovali odladění těchto nástrojů dostatek času, což bylo ve výsledku znát. V dnešní době je podobná nestabilita víceméně výjimkou (a lze na ni narazit spíše u kernel mode varianty), pokud se však počítač začíná znenadání bezdůvodně „zakousávat“, lze kontrolu na přítomnost rootkitu doporučit. Dalšími příznaky jsou neobvyklé zatížení systému (i když Správce úloh mlčí) nebo zvětšený provoz směrem „na internet“ (nutné zjišťovat jinde než na PC – například u poskytovatele).

PETR.KRATOCHVIL@CHIP.CZ

Ne rootkitům: Pokud si nejste jisti staženým souborem, raději ho prověřte souborovým skenerem.

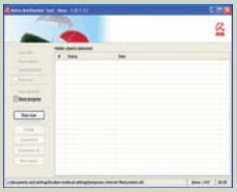
INFO

Detekční nástroje

Na internetu najdete celou řadu bezpečnostních nástrojů tvrdících, že odstraňují rootkity. V této oblasti bychom více než kdy jindy doporučili spoléhat se na osvědčené „koně“, obvykle v podobě renomovaných bezpečnostních firem. Většinu vhodných nástrojů najdete na Chip DVD, ale doporučujeme stáhnout si jejich aktuální varianty...

AVIRA ROOTKIT DETECTION

www.antirootkit.com/software/Avira-Rootkit-Detection.htm



Jako jediný z nástrojů vyžaduje instalaci a pro jeho odstranění musíte navštívit v Ovládacích panelech sekci Přidat / Odebrat programy. Nabízí poměrně rozsáhlé možnosti nastavení, včetně rychlého scanu.

F-SECURE BLACKLIGHT

www.f-secure.com/blacklight

Tento nástroj je k dispozici i v online scanneru (viz. Chip 4/2008). Jako samostatný nástroj je zdarma nabízený v Security centru firmy F-Secure. Po stažení stačí jen spustit exe soubor a jednou kliknout na tlačítko Scan. Kontrola počítače trvá přibližně o třetinu déle než u ostatních nástrojů.

MCAFEE ROOTKIT DETECTIVE

http://vil.nai.com/VIL/STINGER/RKSTINGER.ASPX

Detektiv rootkitů nabízí druhé nejrozsáhlejší možnosti nastavení a konfigurace skenu. Přehledné je také zobrazení výsledků a přepínání mezi zjištěnými a aktuálními informacemi.

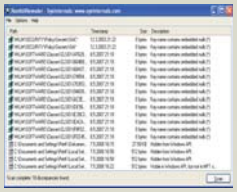
PANDA ANTI-ROOTKIT

http://research.pandasecurity.com/archive/Panda-AntiRootkit-Released.aspx

Pokud se vám na poněkud zmateném webu podaří najít soubor s detektorem rootkitů, pak máte vyhráno. Opět jde o jeden exe soubor, který po stažení stačí spustit. Jako jediný nástroj nabízí „in-depth scan“ (kontrolu po restartu systému).

ROOTKITREVEALER 1.71

http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx



Známý nástroj od Marka Russinoviche, nyní nabízený „pod hlavičkou“ Microsoftu. Jeden soubor, jedno tlačítko a spoustu (nepřehledných) výsledků. Ne nebojte se, položka „Key name contains embedded nulls (*)“ ještě nic neznamená...

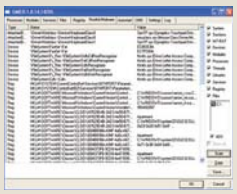
TREND MICRO ROOTKITBUSTER

http://www.trendmicro.com/download/rbuster.asp

Čtyři možnosti, jedno kliknutí a vše je hotovo. Ve srovnání s ostatními zde proběhl sken „kosmickou rychlostí“ (přibližně desetinu doby trvání ostatních). Předností je přehledné zobrazení výsledků.

GMER

www.gmer.net



Legenda nejen mezi detektory rootkitů. Nejširší možnosti a schopnosti. Je zkrátka nejrozsáhlejší – umí vše na co si vzpomenete. Doporučujeme především zkušenějším uživatelům, protože uživatelská přívětivost je zde neznámé slovní spojení...