Útoky internetových banditů

Ochrana počítače

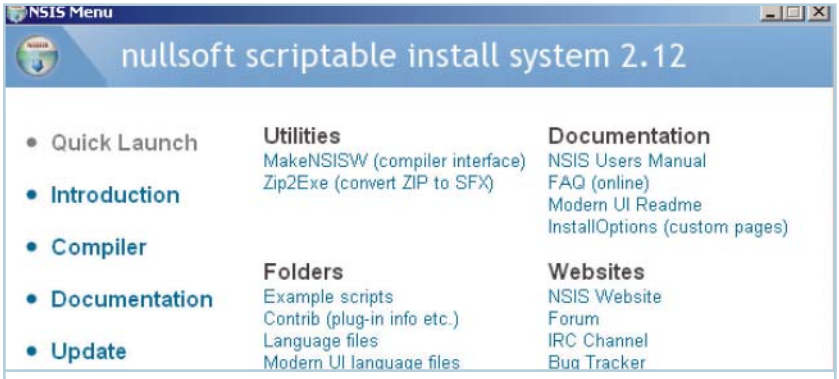
Tajně přenášet obsah harddisku, číst tajné dokumenty, odposlouchávat telefonáty – to vše je až hrozivě jednoduše možné. Simulovali jsme ty nejnebezpečnější útoky a nyní vám ukážeme, jak se bránit proti nejnovějším trikům hackerů.

Text: Valentin Pletzer

Chráníte si svůj systém pomocí firewallu, antivirového programu a service packu? To je dobře. Věříte, že takto zůstane váš počítač ochráněn před špionáží dat, hackery a internetovou mafií? Velký omyl!

Ten, kdo na svém počítači nemá nainstalovány nejnovější patche, samozřejmě ulehčuje práci útočníkům – a nemůže se takové nechtěné návštěvě vůbec divit. Ale i když jste si tyto nejnovější patche nainstalovali, neznamená to, že je váš počítač stoprocentně chráněn. S takzvaným 0-Day-Exploit využívají hackeři dosud neznámé a neopravené bezpečnostní „díry“ a pronikají do zdánlivě bezpečných ochranných „zdí“ během několika sekund. A jde to ještě dokonce jednodušeji: pomocí CD, který je správným způsobem zmanipulován, lze překonat i ty nejlepší firewally.

Chip udělal případovou studii a pomocí nových hackerských metod simuloval nejnebezpečnější internetové útoky – včetně přenosu dat z harddisku. Tyto pokusy dokonce „odneslo“ i pár kolegů. Výsledek byl děsivý: pokud to útočník myslí opravdu vážně, je pro něj velmi jednoduché získat kontrolu nad počítačem oběti. Ukážeme vám, jak vše funguje a pomocí jakých obranných opatření můžete svůj systém efektivně chránit. →



CD s trojským koněm během pěti minut: S volně dostupným setup-nástrojem „NSIS“ vytvoříme zdánlivě opravdový instalační demo CD, abychom mohli trojského koně přenést.

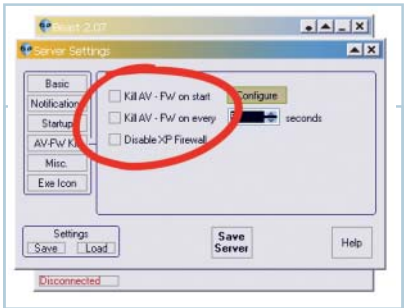
1 ŠPEHOVÁNÍ OBĚTI

Pravidlo číslo jedna úspěšného špiona zní: Znát dobře nepřítele. U webových prohlížečů je to snadné: stále ještě více než 90 % „surfařů“ používá Internet Explorer. A co je ještě zajímavější – především ve firmách jsou používány již předinstalované programy od Microsoftu. Hacker tedy musí svoji oběť přilákat na předem připravenou webovou stránku a poté využít slabin prohlížeče.

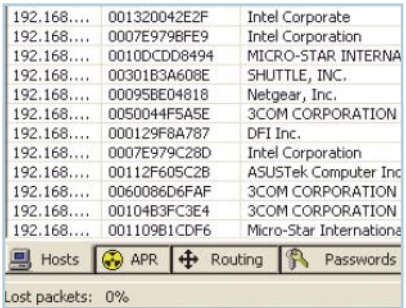
Útok: Plánujeme pomocí Buffer-Overflow-Exploits převzít kontrolu nad prohlížečem a tím pádem i nad celým PC. Proto se nejdříve musíme informovat o softwaru naší oběti. Dobře že jsme našemu kolegovi nedávno ukazovali on-line album z dovolené. Tak snadno zjistíme jméno a číslo verze prohlížeče. S každým nainstalovaným patchem jsou naše možnosti útoku menší, proto musíme nejprve zjistit, jaký prohlížeč oběť používá. V lepším případě nám tyto informace pošle hned samotný prohlížeč, ty lze poté vyčíst v protokolu webového serveru. Ale také verze programu je důležitá, neboť většina Buffer-Overflows funguje pouze s určitými verzemi.

Máme štěstí, jelikož jsme našli univerzální 0-Day-Exploit pro Internet Explorer 6. V bezpečnostním žargonu se tak označuje skulina, která je aktuální a doposud „nepatchovaná“. Hackeři z FrSIRT na webové stránce „Proof of Concept“ přesně demonstrovali, jak lze takovou slabinu využít, což nám vše usnadňuje. Použijeme již existující script a vložíme do něj takzvaná zadní vrátka – „Backdoor“. Díky tomu později do systému propašujeme další nástroje. Tyto „Backdoory“ se dokonce nacházejí na internetu, takže náš útok můžeme provést velmi lehce – pomocí Copy & Paste.

Nyní se ještě musíme postarat o to, aby náš kolega připravenou webovou stránku otevřel. Proto mu pošleme odkaz na tuto stránku s upozorněním, že jsou na ní fotografie z poslední podnikové oslavy. Jednoduchý trik, který funguje skoro vždy. V našem případě šlo všechno jako po másle. Poté, co naše oběť klikla na odkaz, otevřel se Internet Explorer a okamžitě opět spadl. Avšak ne bez toho, aniž by nainstaloval malý dárek – náš Backdoor.



Killer-Tool: Pomocí kliknutí můžeme v trojském koni nazývaném „Beast“ určovat, který ochranný software chceme ukončit.



Snadné vyzvídání: Program Cain & Abel lokalizuje všechny počítače v síti a umožní vám podle libosti nahrát VoIP hovory.

POZOR NA HACKERY A JEJICH NÁSTROJE

Ten, kdo ví, jak hacker pracuje, se nyní může i bránit. Ukážeme vám, jak používat síťové nástroje a zabezpečit tak síťové připojení.

Nmap:

Pomocí tohoto skeneru portů naleznete veškeré veřejné porty a IP adresy v síti, a tím pádem i možné slabiny. Tip: K prozkoumání všech počítačů a portů ve své síti zadejte následující příkazový řádek: `nmap -v -sS -O 192.168.*.*`. Otevřené porty, jež se vám poté zobrazí, byste měli zavřít.

SwitchSniffer:

Pokud jsou v síti instalovány switche, obdržíte pouze ty pakety, jež jsou určeny pro vás, ne však pakety ostatních počítačů. Tento nástroj slouží k přesměrování neznámých paketů. Tip: Abyste se proti takovým nástrojům, jako jsou SwitchSniffery, ochránili, použijte následující příkazový řádek: `arp -s 192.168.0.1 00-aa-00-62-c6-09`. Pomocí tohoto příkazu pevně určíte, která MAC adresa patří ke které IP adrese; v tomto případě je to adresa routeru, jelikož ten je jako připojení k internetu nejoblíbenějším cílem přesměrování.

Ethereal:

SwitchSniffer sice přesměrovává data, neumí je ale zobrazit. To však tento nástroj umožňuje. Tip: Aby vaše data nepřipadla do nesprávných rukou, měli byste vždy, pokud je to jen možné, používat zakódovaná spojení jako HTTPS a SSH.

Netcat:

Tento nástroj nabízí nejjednodušší způsob, jak vytvořit nezajištěné připojení k příkazovému řádku nebo jak zkopírovat data přes síť – aby došlo například k simulaci serveru. Tip: Pomocí jedné řádky se z nástroje stane opravdový webový server. Vytvořte vlastní index.html a server spusťte s následujícím příkazem: `netcat -l -p 80 < index.html`. Do adresního řádku vepište http://127.0.0.1/ pro vstup na tuto adresu. V okně serveru pak lze vyčíst jednoduché dotazy prohlížeče a informace o něm.

Obrana: Používejte alternativní prohlížeče jako Firefox nebo Operu. U nich sice experti na bezpečnost také našli závažné bezpečnostní „díry“, ty však nejsou využívány zdaleka tak často. Většina hackerů se totiž zaměřuje na Internet Explorer – protože je velmi rozšířený.

Důležité je také neotvírat každý odkaz v každém e-mailu. Především u e-mailů od neznámých odesilatelů musíte dávat největší pozor.

2 PROLOMENÍ FIREWALLU

Pravidlo číslo dvě špionážní příručky: Změnit & ukrýt. Například trojského koně lze velmi snadno ukrýt na zdánlivě neškodný CD. Výhoda hackera: Uživatel o takovém nebezpečí nic netuší. Stěží někoho napadne, že by reklamní CD s poutavým obsahem mohl obsahovat i trojského koně.

Útok: Namísto vytváření Backdooru a poté trojského koně využijeme tentokrát kapacitu tohoto datového nosiče a celého trojského koně na CD „zabalíme“. Pro naše účely použijeme již poněkud starší „Back Orifice 2000“. Výhodou open-source trojského koně je, že ho lze pomocí pár úprav přizpůsobit. Novější kód a jiný kompilační program – a běžné skenery virů trojského koně nenajdou.

Aby se trojský kůň po vložení CD také nainstaloval, použijeme již existující demo CD a pomocí volně dostupného nástroje „NSIS“ vytvoříme setup. Rozdílem je, že tentokrát se již nainstaluje balíček s naším trojským koněm. Jako třešničku na dortu jsme k této návnadě přidali ještě funkci „autostart“, neboť tak instalace naběhne automaticky, jakmile uživatel vloží CD do mechaniky.

Nyní už jen stačí, aby si uživatel daný demo CD nainstaloval, a trojský kůň se

```
//
// Harmless Calc.exe
//
shellcode = unescape("%u5053%u5053%u9090%uC929%uE983%uD9DB%
"%u5BF4%u7381%uA913%u4A67%u83CC%uFCEB%uF4E2%u8F55" +
"%uCC0C%u67A9%u89C1%uEC95%uC936%u66D1%u47A5%u7FE6" +
"%u93C1%u6689%u2FA1%u2E87%uF8C1%u6622%uFDA4%uFE69" +
"%u48E6%u1369%u0D4D%u6A63%u0E4B%u9342%u9871%u638D" +
"%u2F3F%u3822%uCD6E%u0142%uC0C1%uECE2%uD015%u8CA8" +
"%uD0C1%u6622%u45A1%u43F5%u0F4E%uA798%u472E%u57E9" +
"%u0CCF%u68D1%u8CC1%uECA5%uD03A%uEC04%uC422%u6C40" +
"%uCC4A%uECA9%uF80A%u1BAC%uCC4A%uECA9%uF022%u56F6" +
"%uACBC%u8CFF%uA447%uBFD7%uBFA8%uFFC1%u46B4%u30A7" +
"%u2BB5%u8941%u33B5%u0456%uA02B%u49CA%uB42F%u67CC" +
"%uCC4A%uD0FF")
```

Nebezpečné změti písmen: Na tomto místě webové stránky se nachází kód škodlivý pro kapesní počítače s Windows. Nasadíme zde „Backdoor“.

může spustit. V našem případě zaznamenal veškeré úhozy/stisknuté klávesy oběti a předal je nám – je zajímavé, co všechno naši kolegové na počítačích dělají.

Obrana: Dokonalá obrana proti takovýmto útokům neexistuje. Ale stejně jako u e-mailů i zde platí pravidlo: Programy, které neznáte, neinstalujte. To je však velmi obtížně proveditelné v praxi. Nejlepším řešením je samo-

ROOTKITS: NEVIDITELNÉ NEBEZPEČÍ

»JAK HACKEŘI OBCHÁZEJÍ VÁŠ ANTIVIROVÝ SOFTWARE

Rootkits se skryjí tak hluboko v systému, že běžné bezpečnostní nástroje nemají šanci je objevit. Tyto vyvinuté „trojské koně“ jsou něco jako sada nástrojů, které zaznamenávají hesla, umožňují přístup hackerům, zaznamenají veškeré stisky kláves nebo „slídí“ po informacích v síti – hlavně nenápadně.

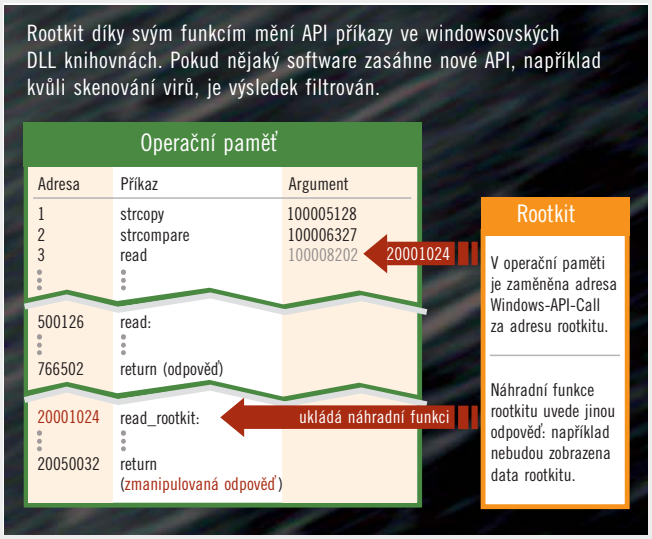
Pokud člověk věří specialistům, jako je F-Secure, očekává se od těchto technologií velký potenciál, který bude v budoucnu použit k posílení „maskování“ virů a červů. Už nyní existují červi, kteří využívají Sony-rootkit. Důvodem je to, že virové skenery nemohou rootkits vystopovat: oproti běžným nežádoucím programům, které pracují na uživatelově ploše, se rootkity schovají hluboko do Windows-API (Application program Interface). Přes API spouštějí aplikace operačního systému – ovlivňují tedy přístupy na harddisk a do registrů a také základní funkce virových skenerů a firewallů. Rootkit nyní zachytí jakoukoli výzvu a rozhodne, která data smí bezpečnostní aplikace vidět. V případě, že se antivirový program pokouší zjistit název rootkitu, vyfiltruje rootkit veškeré výpisy odpovídající požadovanému dotazu operačního systému. Trojský kůň tedy zůstane nadále neviditelný.

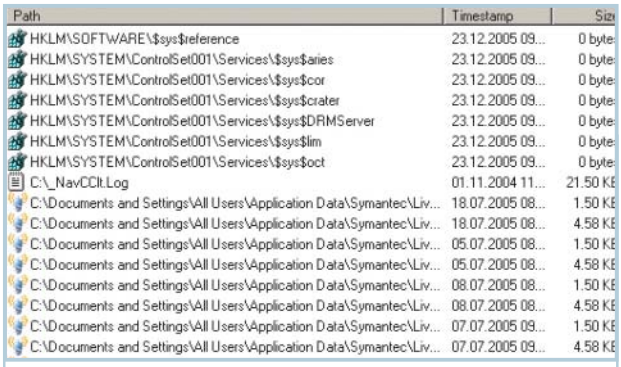
Jak rootkits objevit: Většina známých rootkitů pro Windows se naštěstí ještě neumí dokonale schovat. Pokud je tedy trojský kůň „Slanret“ koncipován jako ovladač systému, lze ho odhalit v nouzovém modu. Často také způsobuje zhroucení systému. Jiným „příznakem“ rootkitů je výrazně se snižující volné místo na vašem harddisku, nevysvětlitelný pokles výkonu CPU a neznámá internetová spojení. Profesionálové mimo jiné používají nástroje jako „RootkitRevealer“ pro zjištění, která IP adresa byla přesměrována. Nebo porovnají data na harddisku s dříve uloženou zálohou.

Jak se rootkitů zbavit: Nejlepším řešením je to nejradikálnější – zformátování a opětovná instalace vás zbaví veškerých hackerských nástrojů. Následně byste měli změnit všechna hesla.

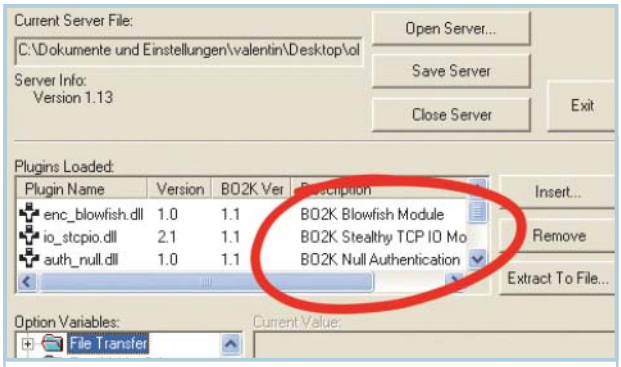
Speciální skenery jako například RootkitRevealer (*www.sysinternals.com*) a BlackLight (*www.f-secure.com*) jsou komplikované a pomáhají pouze profesionálům při vyhledávání a mazání rootkitů. Bohužel žádný jednoduchý program sloužící k odstranění početných variant „neupravených/divokých“ rootkitů neexistuje – na rozdíl od programu odstraňujícího rootkit v audio-ochraně proti kopírování Sony. Avšak jednu slabinu mají rootkity s běžnými nežádoucími programy společnou: na PC chráněný pomocí patchů, firewallů a skenerů virů se v případě, že uživatel nebude otevírat podezřelé přílohy a zřekne se stahování pochybných dat od neznámých autorů, nedostanou.

Informace: *www.rootkit.com*





Neviditelný plášť: Rootkit XPC od společnosti Sony BMG v systému ukryje vše, co začíná „sys“, včetně zápisů v registrech.



Mocný nástroj: Díky mnoha plug-inům patří Back Orifice 2000 stále ještě k nejoblíbenějším trojským koním.

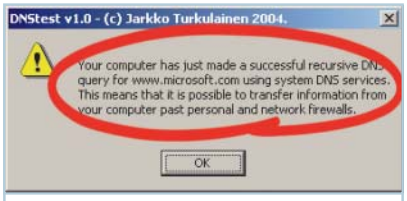
statný počítač, na kterém trojský kůň nemůže způsobit žádné škody. Tento počítač byste samozřejmě neměli propojovat se svým běžným systémem.

3 BUĎTE NEVIDITELNÍ

Třetí pravidlo zní: Pokud nejste vidět, nemůžete být ani odhaleni. Převedeno do oblasti PC špionáže to znamená: Sem s rootkitem. Takto se jednoduchý Backdoor stane skvělým trojským koněm, neboť jakmile je již program v systému, je velmi těžké ho objevit – natož odstranit.

Nejznámější rootkit pro Windows se jmenuje „FU Rootkit“. Ukrývá škodlivé programy do taskmanageru uživatele. Takto nelze trojského koně zastavit. Moderní rootkity, jako například „Beast“, však ukrývají ještě více: například zápisy v registrech, TCP/IP připojení a data umístěná na harddisku. Bez speciálního softwaru již takového profesionálního trojského koně neobjevíte, nemluvě o jeho odstranění. Důvodem je to, že rootkity ovládají funkce Windows a manipulují s výsledky, na něž jsou odkázány skenery virů.

Útok: Rozšiřujeme náš již tak velmi upravený „Back Orifice 2000“ o rozvoj, kterým prošel „FU rootkit“. To jde právě tak snadno jako integrace plug-inu ve Photoshopu. Jediné, co musíme udělat, je instalace a definování plug-inu rootkitu, jehož data uživatel nesmí vidět. Pro naše testovací účely tedy trojského koně stejně jako ostatní data schováme, abychom je mohli později uložit – například datový protokol Keyloggeru.



Pohled do tunelu: Pomocí DNS testu si můžete ověřit, jak moc (ne)bezpečný je váš firewall. Budete se opravdu divit!

Obrana: Proti tomuto druhu „stealth“ techniky se nedá bránit takřka vůbec. Jakmile je již trojský kůň v systému nainstalován, lze ho odstranit pouze pomocí speciálních nástrojů, jako je RootkitRevealer od společnosti Sysinternals. K tomu, abyste trojského koně vůbec odhalili, musíte svůj systém velmi dobře znát. Speciální programy jako například DaemonTools (které pouze vytvářejí virtuální mechaniky) používají tuto techniku neviditelného propojení se systémem.

4 ODPOSLECH TELEFONÁTŮ

Vše slyšet, ale sám nemluvit, to je pravidlo číslo čtyři. Odposlouchávat telefonní hovory už není privilegiem pouze tajné služby. Jestliže před pár lety hackery přitahovaly slabiny v ISDN zařízeních, nyní to jsou odposlechy VoIP telefonátů na internetu.

Útok: Pro demonstrační účely jsme z internetu stáhli hackerský nástroj „Cain & Abel“. Ten ovládá nejen triky jako prolomení hesel, ale umožňuje zaznamenat navštívené internetové stránky a především také nahrát VoIP rozhovory jako data wav. Předpokladem pro tento typ útoku je to, že hacker určí místo v síti, kam proudí veškerá data. To může být například připojení v místní (wireless) síti nebo také trojský kůň na počítači jedné z obětí. Nyní spustíme takzvané Man-in-the-middle útoky a napojíme se na datový tok našeho kolegy. Poté dáme našemu trojskému koni příkaz, aby data posílal nejprve nám. Ta přesměrujeme na jiného uživatele – ale teprve poté, co uspokojíme svou zvědavost. Náš milý kolega nic z toho nezpozoroval.

Obrana: Nejjednodušší opatření jsou nasnadě: Svou lokální síť zajistěte proti cizím typům sítě pomocí filtrů MAC adres a stejně tak svůj skener virů zajistěte proti trojským koňům. Již existují řešení k zakódování VoIP rozhovorů, jako například nástroj Zfone od vývojáře PGP Phila Zimmermana. Problémem je, že většina providerů tuto verzi nepodporuje, čímž uživatel poněkud ztrácí komfort.

5 PAŠOVÁNÍ DAT

Poslední a nejdůležitější pravidlo zní: Nenechte se při špionáži přistihnout. Instalace trojského koně na počítač je pouze polovina práce, neboť bez zpětné vazby k vám domů je vám k ničemu. Protože neznáme infrastrukturu sítě naší oběti, musíme se připravit na všemožné firewally, obzvláště na desktop-firewally, které případně blokují každý aktivní program, a na IDS (Intrusion Detection System), který analyzuje obsah každého paketu. To znamená, že nestačí jen odeslat data z počítače. Informace

ZAJÍMAVÉ ODKAZY

www.rootkit.com
nejznámější stránka s mnoha technickými podrobnostmi týkajícími se tohoto tématu

www.bo2k.com
webová stránka open-source trojských koní; v anglickém jazyce

www.securityfocus.com
stránka s mnoha odbornými články zabývajícími se bezpečností a novinkami v této oblasti

musí být také dostatečně zamaskovány, aby akce nebyla zmařena. Za tímto účelem hackeři vymýšlejí stále nové a nové triky. K trojskému koni „Back Orifice 2000“ neexistují žádné volně dostupné plug-iny, které by se k tomuto účelu hodily. Jedině plug-in „STCP“ zakóduje data tak, že není poznat žádný vzor. To je ale signál, že se eventuálně jedná o komunikační data trojského koně. Přece však existují metody, jak mohou hackeři posílat tato komunikační data i přes firewall.

Útok: Nejoblíbenějším prostředkem je takzvané tunelování přes jiný, zdánlivě neškodný protokol, jako je HTTP, SMTP nebo DNS. My jsme se rozhodli pro DNS tunel, abychom se mohli nepozorovaně dostat přes všechny bezpečnostní kontroly v síti. To znamená, že naše informace sbalíme do nenápadných paketů se jménem domény. Ty přes 90 % firewallů neblokuje, neboť protokol DNS je nutný pro bezchybnou komunikaci s internetem. Kromě toho informace mírně zakódujeme a pošleme co možná nejméně paketů, aby IDS nic z toho nezachytil. Nadměrný přenos paketů se jménem domény by byl totiž podezřelý a dobrým IDS by to mohlo být nápadné. Nyní zbývá už jen desktop-firewall. Ten obejdeme pomocí metody zvané Injection-Attack. To znamená, že najdeme program, který firewall zaručeně neblokuje – například standardní prohlížeč. Zda je to Internet Explorer, nebo Firefox, se dozvíme z Windows registrů, jež můžeme snadno číst díky trojskému koni. Nyní musíme počkat, až naše nic netušící oběť tento program spustí. Tím dojde k jeho uložení do operační paměti. Povedlo se! Náš trojský kůň se připojí k vhodnému programu a používá ho ke svým účelům. Jsme zvědavi, a proto si necháme poslat wordové dokumenty našeho kolegy, samozřejmě aniž by on nebo jeho firewall něco zpozorovali.

Obrana: Zde je zřejmé, že mezi hackery a bezpečnostními firmami probíhá hra na kočku a myš. Firewally, skenery virů a IDS rozpoznají a blokují čím dál tím více útoků. Ty jsou zato stále rafinovanější. Čím více informací útočník o svém cíli má, tím nepravděpodobnější je, že by byl odhalen. Pro každý ochranný mechanismus existuje zpravidla nějaký trik, jak ho obejít. Pro administrátory je tedy velmi důležité zajistit, aby počítače i ochranné programy byly co nejaktuálnější. ■ ■ ■

ROOTKITS: NEVIDITELNÉ NEBEZPEČÍ

»JAK HACKEŘI OBCHÁZEJÍ VÁŠ ANTIVIROVÝ SOFTWARE

Toho, kdo si již někdy zakoupil hudební CD od Sony BMG, tiskárnu od Xeroxu nebo hru od společnosti Blizard Entertainment, by určitě nenapadlo, že na něj někdo použil trik hackerů. Avšak to, co si zde velké koncerny dovolují, spadá z právního hlediska v lepším případě do takzvané šedé zóny.

Audio CD, který „volá domů“

Rána byla odražena zpět. Kvůli ochraně hudby proti kopírování si japonský koncern Sony BMG nechal naprogramovat speciální ochranu. Pokud chcete na svém počítači poslouchat hudbu, musíte si nainstalovat přehrávač, který se nachází na CD. Uživateli je však zatajeno, že společně s přehrávačem se také nainstaluje rootkit, který schovává ochranná data před zvědavými pohledy. Náhodný nález programátora společnosti Sysinternals Marka Russinoviche vše zmařil. Jelikož tato ochrana proti kopírování s tajemným jménem XPC přivádí operační systém do nestabilního stavu a kromě toho navazuje připojení na internet, musela společnost Sony kvůli velkým protestům stáhnout dané CD disky z trhu. Uživatelé ostatních operačních systémů mezitím mohli bez problémů ukládat kopie – na nich totiž nejde tento rootkit nainstalovat.

Aktivní okno „slídí“

Aby mohli být účastníci on-line hry „World of Warcraft“ chráněni před cheatery (podvodníky), přistoupila společnost Blizard Entertainment také k určitému triku, který se společenství hráčů vůbec nelíbí. Profesionální cheateři, kteří vydělávají prodejem virtuálních předmětů na eBay, používají takzvané bots-tools, které zcela automaticky ovládají herní postavu a činí tak lidský faktor zcela nadbytečným. Proti tomu se postavili tvůrci her, kteří začali třídit titulní řádky každého aktivního programu a tyto informace zprostředkovávat na herním serveru. Fatální však je, že tyto informace jsou zprostředkovány i v momentu, kdy máte otevřené například okno on-line bankovnictví.

Skryté označení identifikující tiskárnu

Důvěrné nebo anonymní dokumenty v žádném případě netiskněte na tiskárně Color-Docu-Printer od společnosti Xerox. Podle zjištění amerického hnutí za občanská práva EFF (Electronic Frontier Foundation) je totiž na každý list papíru vytištěn neviditelný kód. Obsahuje sériové číslo a jiné identifikační údaje (datum a čas). Díky tomu lze určit vlastníka i bez vytištěného jména. Tento pouze několik milimetrů veliký kód lze objevit pouze jako malé žluté tečky – a to jen v případě, že víte, kde máte hledat. A poté musí být tento kód desetkrát zvětšen pod mikroskopem, aby byl čitelný.

Kdo z toho má užitek, není jasné. Některé odvážné spekulace sahají od tajné služby až k oddělení podpory zákazníků společnosti Xerox. Poté, co EFF rozluštila převážnou část kódovaných informací, vydal koncern tiskové vyjádření, ve kterém tuto metodu obhajuje jako prostředek proti falšování dokumentů.