Počítače těch druhých

Windows vás „odposlouchávají“. **TAJNÉ PROTOKOLY** o vás prozradí vše. Lze tomu však zabránit: pomocí našeho know-how a nástrojů z Chip DVD zabezpečíte svůj PC před špiony – a zahájíte ofenzivu.

MARKUS HERMANNSDORFER, VRATISLAV KLEGA

Nic není tajemstvím. Windows vědí, co a kdy jste dělali – a prozradí to každému, kdo o to projeví zájem. Pokud už má špion otevřená dvířka do vašeho počítače, stačí mu, aby Windows položil správný dotaz, a ta na vás prozradí vše, co špion potřebuje vědět. Uživatelské jméno přitom patří k těm nevinným informacím. Horší situace nastává v případě přístupu k vašemu bankovnímu kontu, v případě e-mailového hesla, nebo dokonce administrátorského hesla k počítači. Potom už špion může zcela ovládnout váš počítač. Abyste tomuto scénáři zabránili, zkuste se na chvíli vžít právě do role takového špiona. Teprve až budete vědět, jak hackeři a trojské koně pracují, budete se moci efektivně bránit.

UPOZORNĚNÍ: Následující programy jsou hackerské, proto je nikdy neinstalujte na cizí počítače, dopustili byste se trestného činu. Vše raději zkoušejte na svém počítači, ideálně pak na nějakém virtuálním stroji (viz článek na straně 104).

Snímače: Jména a hesla

Pokud chce špion infiltrovat cizí PC, musí nejprve zjistit přihlašovací jméno a heslo uživatele počítače. Aby ho zjistil, je třeba si otevřít zadní vrátka do Windows.

Zjištění uživatelského jména

Nástroje: cmd.exe, PsTools

Pár příkazů v příkazovém řádku stačí špionovi k tomu, aby se dostal ke skrytému administrátorskému kontu vašeho počítače. Jakmile se špion může přihlásit k vašemu počítači, nic už mu nezabrání v tom, aby získal všechna uživatelská jména.

Vžijte se na chvíli do role agenta. Otevřete si příkazový řádek a zadejte příkaz podle vzoru

```
ping www.jmenopocitace.cz
```

Tím získáte IP adresu daného počítače. Pomocí příkazu ping se rovněž dozvíte, zda je počítač on-line, a tedy dostupný. Pokud vám počítač odpoví, můžete se hned pokusit o přístup k administrátorskému kontu. Do příkazového řádku proto zadejte

```
net use \\IP-adresa\ipc$ /user:administrator
```

Místo IP-adresy samozřejmě zadejte IP adresu zkoušeného počítače ve tvaru x.x.x.x. Pokud se vám podaří se připojit, máte vyhráno.

Dalším nástrojem, který vám pomůže, je PsTools. Pochází přímo od Microsoftu, konkrétně od Sysinternals. Celý balík PsTools najdete na Chip DVD, ze všech jeho nástrojů však budete potřebovat jen soubory »psexec« a »psloggedon«. Oba tyto soubory zkopírujte do složky »windows\system32«. Nakonec otevřete příkazový řádek a na jeden řádek zadejte následující příkaz

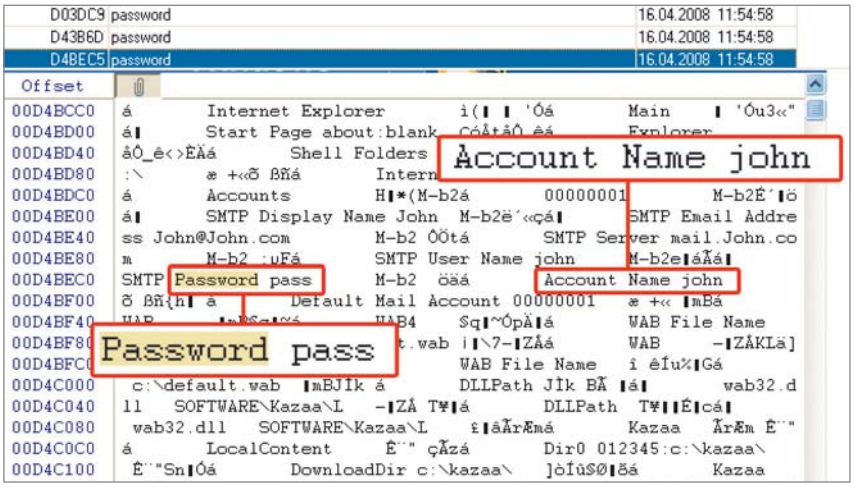
```
psexec \\IP-adresa -u administrator
psloggedon \\IP-adresa
```

Pokud se vám podaří připojit se ke vzdálenému počítači, uvidíte jména všech uživatelů systému, kteří jsou k počítači připojeni.

NAJDETE NA CHIP DVD

AxCrypt ► šifrování souborů
Exif Reader ► načítá EXIF z fotografií
Free PDF XP ► tvorba PDF
PageSpy ► zkoumá cookies
Process Explorer ► informace o procesech
PsTools ► soubor systémových nástrojů
ThumbsDbExtractor ► zkoumá thumbs.db
Vispa ► tweakování Visty
WinHex ► pokročilý editor textů
Wireshark ► odposlech LAN
xpy ► tweakování XP

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



Špatná ochrana: V odkládacím souboru Windows je možné najít jména k účtům, a dokonce i nijak nezašifrovaná hesla.

JAK SE CHRÁNIT: To, co jsme vám právě ukázali, se nazývá »Null session attack«. Tento způsob útoku používá porty 137, 138, 139 a 445. Prvním krokem je nainstalovat si Service Pack 2. Firewall, který je součástí SP2, je dostatečně odolný proti Null session attacku, takže se nikdo nebude moci k vašemu počítači přes internet přihlásit.

Je-li počítač připojen do lokální sítě, můžete zmíněné porty zakázat přímo ve firewallu. Spusťte editor registru a přejděte ke klíči »HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters«. Zde vytvořte nové DWORD klíče s názvem »AutoShareServer« a »AutoShareWks«. U obou klíčů nastavte hodnotu »0« a restartujte počítač. Po tomto nastavení si hacker při Null session attacku vyláme zuby.

Windows prozradí i hesla

Nástroj: WinHex

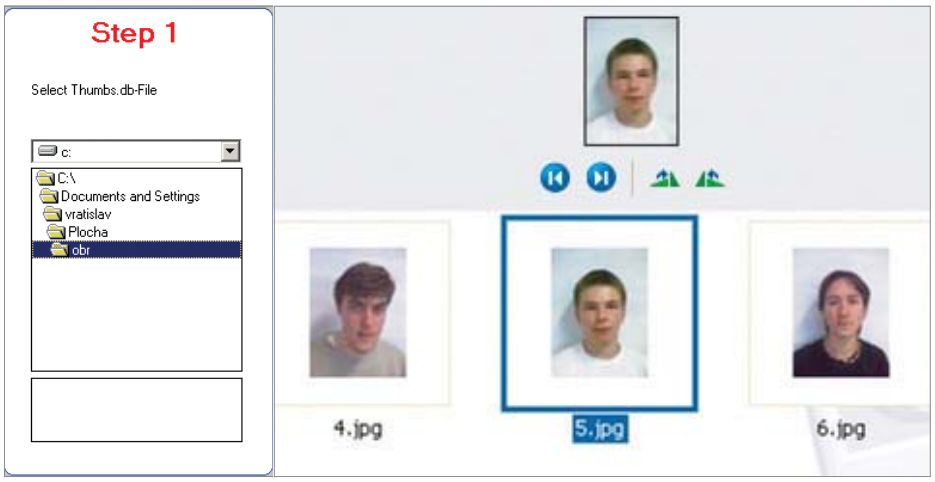
Uživatelské jméno je samozřejmě jen půl úspěchu. Když se špion úspěšně dostane do systému, musí ještě zjistit příslušná hesla.

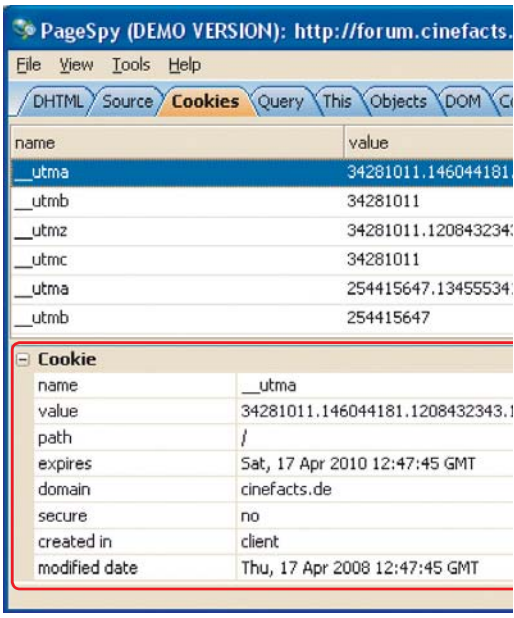
Nejjednodušší cestou je vyhledávací funkce ve Windows. Stačí najít soubory »*.pwd«, »*.ped«, »*.psr«, »*.psx« a »*.db«. Do těchto typů souborů si nejznámější programy pro ochranu hesel ukládají všechna hesla. Nejzajímavější jsou potom soubory s názvy »key« a »secmod«. Pokud tyto soubory otevřete prohlížečem WinHex, který najdete na Chip DVD, můžete si hesla snadno vyhledat. To však funguje jen tehdy, nejsou-li hesla zašifrovaná. V opačném případě neexistuje k rozlousknutí hesla žádná rychlá cesta.

WinHex toho umí ještě mnohem více. Jeho pomocí můžete například otevřít odkládací místo Windows (pagefile.sys). Pokud však budete chtít přistupovat k pagefile.sys, budete muset nabootovat do Visty nebo do jiného operačního systému. Jen tak budete moci soubor otevřít, ze stejné relace Windows to není možné.

Jakmile se vám podaří v nástroji WinHex otevřít zmíněný soubor, zvolte v menu »Search | Find text«. Do vyhledávacího řádku poté zadávejte slova jako »Password«, »admin« nebo nalezená uživatelská jména. Sami budete překvapeni, kolik hesel Windows prozradí. Budete moci najít hesla pro přístup k webovým fórům i pro otevření zamčených PDF dokumentů.

JAK SE CHRÁNIT: Používáte-li programy pro správu hesel, vždy si hesla zašifrujte.





Rekonstrukce fotografií: Na Googlu stačí najít „Thumbs.db" a poté použít »ThumbsDbExtractor«. Získat náhledy fotografií je pak záležitostí tří kliknutí.

Všechny programy pro správu hesel nějaký způsob šifrování používají. Potom budou vaše hesla jako v trezoru. Nepoužívejte funkce pro pamatování hesel, které nabízí internetové prohlížeče. Ty mají totiž velmi slabé zabezpečení a pro hackera nebude žádný problém hesla ukrást. Rovněž si dejte pozor na programy, které za vás vyplňují webové formuláře – konkrétně AI RoboForm a Password Safe. Hackeři dokázali najít v těchto programech slabiny a dokážou hesla extrahovat.

Zařídit lze i ochranu souboru pagefile.sys. To je možné provést v registru systému. Spusťte proto editor registru a přejděte ke klíči »HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\Memory Management«. Nalezněte záznam »ClearPageFileAtShutdown« a změňte hodnotu z 0 na »1«. Při vypnutí Windows se veškeré citlivé údaje z pagefil.sys vymažou a ani WinHex z nich nebude schopen nic vyčíst.

Vyslídit: Fotografie, maily, dokumenty

Nejen Windows jsou upovídaná – i samotné soubory prozradí na svého majitele úplně vše.

Rekonstrukce fotografií

Nástroje: ThumbsDbExtractor, Exif Reader

Na poslední party se vám podařilo pořídit několik fotografií, které by nikdy nikdo neměl vidět. Někdo ale ukradl z vašeho počítače soubor »thumbs.db« a podařilo se mu zrekonstruovat kompromitující obrázky. Jak se to dělá, to se dočtete v následujícím scénáři.

Nejprve jsme si obstarali soubor »thumbs.db« z cizího počítače. Nejsnazší cesta: do Googlu jsme zadali

```
filetype:db thumbs
```

Google našel asi 26 000 webových stránek, z nichž většina nabízí ke stažení i tento soubor. Náhodně vybíráme nějaké francouzské webové fórum a stahujeme z něj soubor »thumbs.db«. Soubor otvíráme v programu ThumbsDbExtractor. Zobrazí se obličeje tří mladíků, pravděpodobně se jedná o studenty. Jak jsme vyčetli z URL, jeden z chlapců by se měl jmenovat Alex.

Jdeme ještě dále a obrázek otevíráme v programu Exif-Reader. Kluci ale byli chytří a vyfotili se jen pomocí webové kamery, která mnoho dodatečných údajů neuchovává. Proto jsme se jen dozvěděli, který den byla fotografie pořízena a jakým modelem digitálního fotoaparátu – v tomto případě webové kamery.

JAK SE CHRÁNIT: Proti Googlu se můžete bránit jedině internetovou abstinencí. Druhou možností je, že vyhledáte na svém disku všechny soubory s názvem »thumbs.db« a odstraníte je. Navíc ještě musíte zabránit tomu, aby je Windows vytvořila znovu. Otevřete »Tento počítač«, zvolte »Nástroje | Možnosti složky | Zobrazení« a zaškrtněte položku »Neukládat miniatury do mezipaměti«. Abyste měli dokonalou jistotu, neměli byste používat aplikaci Windows »Prohlížeč obrázků a faxů«. Zkrátka bezpečnost má svoji cenu.

Co na nás prozradí e-mail

Nástroje: Outlook, Outlook Express

Dobře si rozmyslete, jestli e-mail pošlete. Elektronická pošta na vás totiž prozradí více, než by se vám mohlo líbit. Pro získání informací navíc ani nepotřebujete speciální nástroj. Zcela postačí i běžný e-mailový klient.

Za celým trikem jsou hlavičky e-mailů. V Outlooku stačí pro jejich čtení kliknout pravým tlačítkem myši na e-mail a zvolit »Možnosti«. Kolik informací se zobrazí, to záleží na mnoha faktorech. Tak například se můžete dozvědět, jakou verzi e-mailového klienta odesílatel používá. My se zaměříme na běžné faktory, které slouží třeba k identifikaci nebo vysledování uživatele.

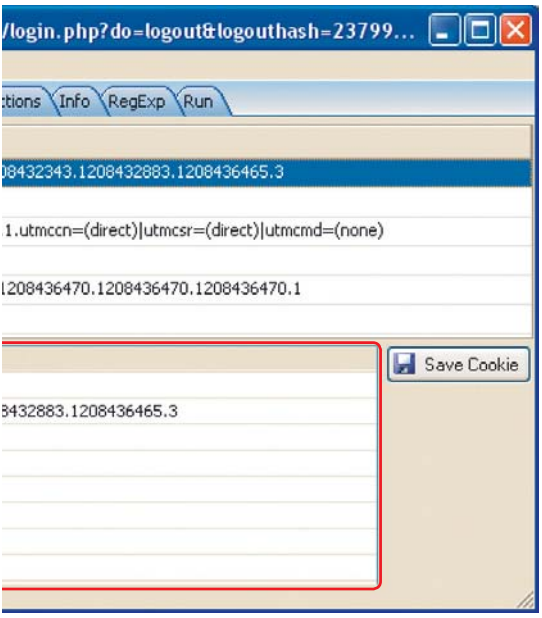
Po otevření možností zprávy se podívejte do části »Internetová záhlaví«. Zde se totiž vyskytují všechny informace o příchozím e-mailu.

První položkou je »Received«. Zde je identifikován odchozí mailový server včetně všech detailů, jako je třeba IP adresa. Tento záznam je velmi těžké zfalšovat. Přestože e-mail vypadá jako z vaší banky, pokud pochází se serveru s doménou .RU, rozhodně není odesílatelem ten, kdo se za něj vydává.

Příklad: Přišel nám e-mail, který vypadal jako z České spořitelny. Když jsme však chtěli zjistit skutečného odesílatele, přišli jsme na to, že mail pochází z počítače PPPoE-88-147-167-190.volsk.san.ru ([88.147.167.190]). Proto jsme otevřeli webovou stránku **http://samspade.org** a zadali jsme IP adresu 88.147.167.190. Výsledek nás nijak nepřekvapil – providerem odesílatele byl „Volgatelecom" se sídlem v Rusku.

Stejný postup je samozřejmě možné aplikovat u jakéhokoliv jiného odesílatele – zjistíte si, ze kterého poštovního serveru zpráva

Jména ani hesla nejsou žádným tajemstvím



pochází, a přes výše uvedenou webovou stránku si o dotyčném zjistíte všechny dostupné informace. Tak zjistíte nejen poskytovatele, ale třeba i fyzické umístění serveru a kontakt na providera.

JAK SE CHRÁNIT: Chcete-li poslat e-mail tak, aby vás nikdo nevypátral, je nutné použít službu pro anonymní posílání e-mailů, kterou lze najít například na adrese **www.anonymousspeech.com**. Pro poslání e-mailu je ale třeba se tak jako tak zaregistrovat, proto lze teoreticky konstatovat, že stoprocentně anonymní e-mail není možné poslat.

Další informace, které jsou uvedeny v internetovém záhlaví, nejsou již nijak zvlášť nebezpečné. Adresát se jen dozví, jakou máte verzi poštovního klienta, komu byl e-mail určen a další méně důležité informace.

MS Office špicluje

Nástroj: Notepad

Ideálním prostředkem pro špionáž jsou dokumenty z balíku Microsoft Office. Obsahují totiž řadu informací, mezi nimi třeba uživatelské jméno, cestu k souboru a další výrobní tajemství – kdo dokument vytvořil, jak dlouho jej editoval, kdo jej změnil či uložil. Samozřejmě nemůže chybět ani informace o použitém editoru. Pro získání těchto informací navíc agent nepotřebuje žádný speciální nástroj – stačí kliknout na dokument pravým tlačítkem myši, zvolit »Vlastnosti | Souhrn | Upřesnit...«. Zobrazí se všechny podrobnosti, které jen Windows umí prozradit. Jelikož je ve firmách standardem, že autor, který je napsaný právě v těchto informacích, má stejné jméno, jako je jeho login, chybí k prozrazení už jen heslo.

Otevřete-li wordovský dokument v poznámkovém bloku, ve změti znaků se můžete dozvědět ještě mnohem více informací – místo uložení i změny provedené v dokumentu.

Zrádné: Cookies si pamatují řadu informací, a dokonce i hesla. Hacker je přitom může pomocí javaskriptu velmi snadno ukrást.

Pokud vám to stále ještě nestačí, otevřete dokument v prohlížeči WinHex. My jsme byli velmi překvapeni, co jsme našli. Jednalo se třeba o odkaz na internetovou stránku. Tento odkaz však nebyl součástí dokumentu, jak by se dalo očekávat, dostal se dovnitř zcela jinak. Může za to Firefox, který byl spuštěný společně s Wordem. Jakmile začal Word ukládat na pozadí, uložil nejen samotný dokument, ale zapsal do něj i obsah schránky ve Windows – což byla v našem případě právě internetová adresa, kterou jsme zkopírovali ve Firefoxu. Pokud byste v době ukládání měli ve schránce třeba heslo, Word by jej bez okolků uložil. A to se může přihodit velmi snadno – třeba když vyplňujete hesla na stránce pomocí specializovaného nástroje, jako je například AI RoboForm. Word tak teoreticky může uložit úplně všechno, co máte ve schránce ve Windows.

JAK SE CHRÁNIT: Chcete-li odstranit veškeré informace, které Office 2002/2003 automaticky vkládá do dokumentů, navštivte stránku Microsoftu a stáhněte si nástroj RHDTool. Ten jednoduše odstraní veškeré soukromé údaje, které nechcete zveřejnit. Pokud používáte jinou verzi Office, je situace složitější. Nejjednodušeji se ubráníte tak, že dokumenty převedete do formátu PDF, který si nic z výše uvedeného nebude pamatovat. Není-li to z jakéhokoliv důvodu možné, pak doporučujeme, abyste své dokumenty z Office poskytovali jen těm osobám, kterým bezmezně důvěřujete.

Cookies: Možná krádež

Nástroj: PageSpy

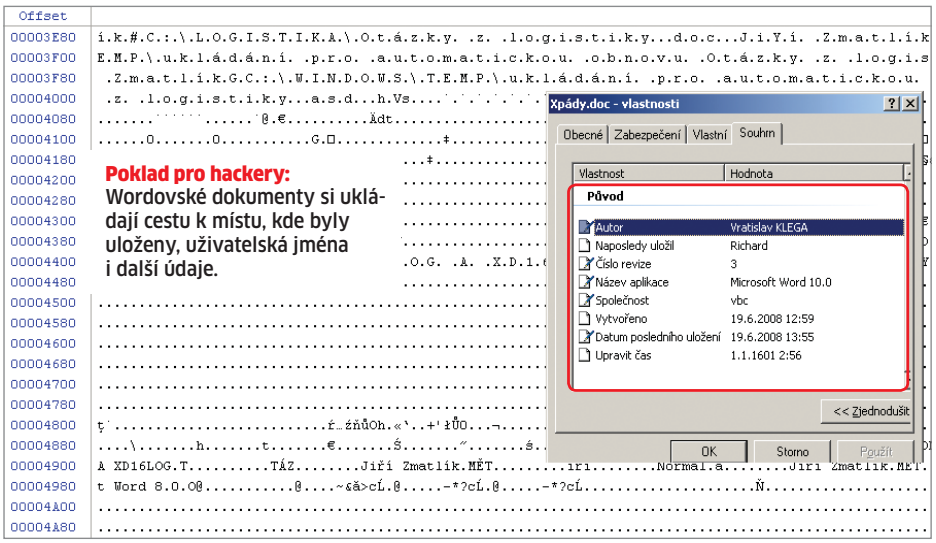
Jak nebezpečné jsou vlastně cookies? V Chipu vám neustále radíme, abyste cookies pravidelně mazali a vůbec byli v souvislosti s nimi velmi opatrní. Jsou taková opatření skutečně nutná, nebo si myslíte, že přeháníme? Odpověď získáte, proměníte-li se opět v agenta a možnosti cookies si sami vyzkoušíte.

Abyste možnosti cookies podrobně prozkoumali, musíte si nejprve nějaké vytvořit. Skutečně zlý špion připraví škodlivý javaskript, který nahraje na webový server, a tím jednoduše získá přístup ke cookies. Pokud návštěvník zavítá na takto infikovaný server, skript si stáhne jeho cookies. V odborném žargonu se tomu říká „Cross-Site-Scripting-Attack".

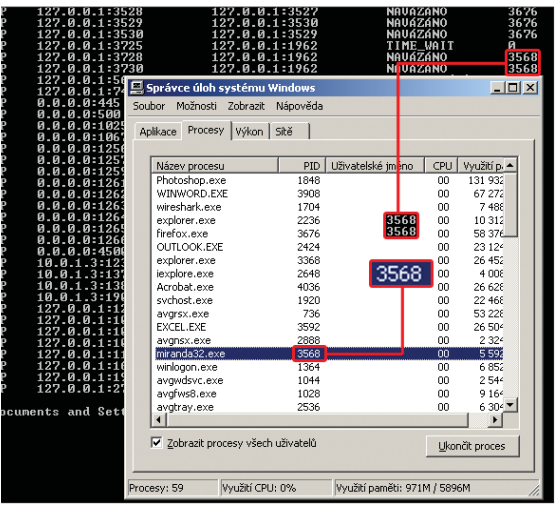
Protože chceme ještě stále zůstat na legální cestě, použijeme program PageSpy, který najdete na Chip DVD. Tento nástroj spolupracuje jen s Internet Explorerem od Microsoftu. Nástroj si nainstalujte a otevřete některou stránku v Internet Exploreru. Doporučujeme zvolit takové webové fórum, do kterého se vkládá uživatelské jméno a heslo. A jak data z cookies vyčíst?

Pokud to fórum umožňuje, zatrhněte volbu „Přihlásit automaticky". To uživateli usnadní přihlašování. Pokud do 14 dnů navštíví stejné fórum, nebude se muset přihlašovat, ale webové fórum ho samo automaticky rozpozná.

Na takové stránce klikněte pravým tlačítkem myši a zvolte položku »PageSpy«, která po nainstalování přibude v kontextovém menu. Tím se spustí špionážní nástroj. Okno PageSpy změňte na »Cookies«. Zde uvidíte všechny záznamy, které o vás webová stránka uchovává.



Poklad pro hackery: Wordovské dokumenty si ukládají cestu k místu, kde byly uloženy, uživatelská jména i další údaje.



Hledání špionů: V tabulce si zjistíte, které porty jsou otevřené, a pak jen dohledáte proces, který je ovládá.

Když nyní kliknete na první ze zobrazených cookies, uvidíte v okně za »Value« uživatelské jméno a heslo. Pokud tomu tak skutečně je, doporučujeme takové fórum raději nenavštěvovat. Vidíte-li jen nesrozumitelná čísla, jedná se o tzv. MD5 hash. I takto chráněné heslo je ovšem možné dostat zpět, třeba pomocí nástroje RainbowCrack. Tento postup je však časově i výpočtově velmi náročný. Jako ochrana soukromého hesla pro vstup na nějaké webové fórum to proto bude stačit.

Co v každém případě zloděj cookies získá, to je adresa navštěvovaných stránek (domain), údaje o tom, ve kterých dnech a hodinách jste stránku navštívili (modified date), zda jsou cookies zabezpečené (secure) a jak dlouho budou ještě platné (expires).

JAK SE CHRÁNIT: Každé fórum, které navštěvujete, si prověřte, především hodnotu »value«, zda jsou hesla zašifrována. Pokud tomu tak není, bude snad lepší vzdát se členství v tomto fóru.

Proti Cross-Site-Scripting útoku se snadno ubráníte tak, že ve svém webovém prohlížeči zakážete spouštění javaskriptů. V Internet Exploreru to provedete tak, že zvolíte »Nástroje | Možnosti internetu | Zabezpečení | Vlastní úroveň | Skriptování appletů v jazyce Java | Zakázat«.

Vyzvědač: Procesy Windows

Pozor! Špion nikdy nespí. Vypadá to, že se nic neděje, ale opak je pravda. Z vašeho počítače unikají informace ven. Ale jak? A kudy? Sken portů odhalil podivné procesy a otevřené kanály.

Windows – odposlouchávání

Nástroj: Process Explorer

Zahrajme si nyní pro změnu hru „lepší špion“ – koneckonců jde o zajištění vlastního počítače. Pomocí Správce úloh systému Windows, který je standardní součástí instalace, zjistíme, které procesy přenášejí informace na internet.

Nejprve si proskenujeme porty, které jsou v počítači otevřené a na kterých probíhá komunikace na pozadí. Otevřete si proto příkazový řádek a zadejte příkaz

```
netstat -ano
```

Zobrazí se přehled všech právě probíhajících připojení. Ve sloupci »Stav« vidíte, v jaké fázi se port zrovna nachází. Pokud je stav »Naslouchání«, znamená to, že port je otevřen. Přes tento port může být počítač odposlouchávání.

Máte-li některé porty otevřené, je docela velká šance, že se nějaký špion dostane do počítače.

Podívejte se do sloupce »Cizí adresa«. Pokud zde naleznete hodnotu »0.0.0.0:0«, nejsou v tuto chvíli tímto portem přenášena žádná data. Špion spí. Zajímavé to začne být v okamžiku, kdy v tomto sloupci objevíte nějakou cizí IP adresu. Pak je ten správný čas podívat se do sloupce »PID« k příslušnému přenosu. PID je jednoznačné identifikační číslo procesu, který je zodpovědný za přenos dat. Zapamatujte si PID číslo procesu, který přenáší data.

Stisknutím kláves [Ctrl]+[Shift]+[Esc] spusťte Správce úloh systému Windows. V menu zvolte »Zobrazit | Vybrat sloupce« a zaškrtněte položku »PID (Identifikátor procesu)«. Nyní stačí porovnat PID z tabulky s PID ze Správce úloh. Na našem počítači byla navázána dvě spojení s procesem 2476. Ve Správci úloh jsme našli, že název procesu je »miranda32.exe«, a že se tedy jedná o instant messenger. Horší je situace, když narazíte na společný proces, jakým je třeba svchost.exe. V tomto případě je lepší sáhnout po specializovaném nástroji, jako je například Process Explorer od Sysinternals, který naleznete na Chip DVD. Stačí na tento nástroj dvojitě kliknout – Process Explorer vám ukáže veškeré podrobnosti, včetně navázaných spojení, přístupů ke knihovnám a dalších informací. Pomocí tohoto nástroje pak špiony snadno odhalíte i smažete.

JAK SE CHRÁNIT: Obrana je v tomto případě velmi jednoduchá. Stačí se v tabulce podívat, který port je otevřený, případně navázaný, a ve svém firewallu tento port zablokovat.

VRATISLAV.KLEGA@CHIP.CZ

INFO

Velký odposlech vašeho PC

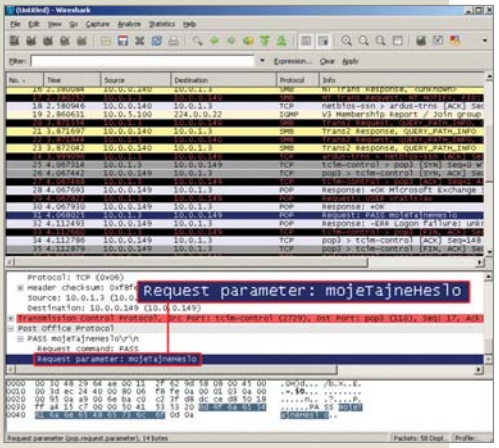
Trojské koně kradou hesla i konta. Chip vám na simulaci ukáže jak.

ODPOSLECH SÍŤOVÉ KARTY

Nainstalujte Wireshark, poté zvolte »Capture | Interfaces« a klikněte na tlačítko »Start« u té síťové karty, prostřednictvím které jste připojeni k internetu. Hned se začnou zobrazovat veškeré informace, které proudí přes síťovou kartu. Pro zastavení zvolte »Capture | Stop«. V okně zůstanou uloženy všechny přenesené informace na síťové kartě. Pokud jste v síti připojeni na hub, je na každé síťové kartě stejný obsah – soused tak může vidět veškerý váš přenášený obsah.

ZÍSKÁNÍ HESLA

Wireshark je uživatelsky velmi vstřícný – z hromady čísel byste totiž jen těžko něco vyčetli. Proto vše organizuje do paketů, a pokud rozpozná známý protokol, do detailu jej rozepíše. Protokolů zná celou řadu, proto není divu, že zobrazí třeba postup při přihlašování k e-mailu – nevynechá ani přihlašovací jméno a heslo. Vše je hezky napsáno v okně tak, jak vidíte na obrázku. Pokud v obrovském množství dat budete chtít najít přihlašovací údaje, využijte vyhledávání. Stiskněte [Ctrl]+[F] a vyhledávejte slova typická pro přihlašování – »login«, »pass«, »user« apod.



Prozradí: Wireshark zobrazí veškerou komunikaci na síťové kartě, včetně všech hesel.