Bezplatné surfování v cizí síti

Internet na letišti, v kavárně nebo na koupališti je příjemný, ale drahý. Díky našemu návodu a programům z Chip DVD budete i zde moci **SURFOVAT ZCELA ZADARMO**. Zabezpečení totiž není v těchto případech tak silné, abyste je nepřekonali.

VRATISLAV KLEGA

Chat, ICQ, e-maily, zprávy, surfování – nic z toho nefunguje, jestliže nemáte připojení k internetu. Podle nejnovějších informací Českého statistického úřadu má připojení k internetu 42 % domácností, 33 % domácností je připojeno k vysokorychlostnímu internetu. Není se čemu divit, vždyť nejlevnější připojení lze často pořídit od 200 Kč měsíčně. Co ale dělat, vydáte-li se mimo dosah svého access pointu? Zde se cena dramaticky zvyšuje. Ani připojení přes mobilní síť není žádnou výhrou. 3G internet je dostupný jen na vybraných místech a rychlost je oproti připojení přes Wi-Fi řádově nižší.

O mnoho lepší není ani situace na veřejných místech, jako jsou třeba letiště. Připojení je předražené, a navíc se často prodává po celých hodinách. Přečtení jednoho e-mailu se tak může pořádně prodražit. Proto vám ukážeme, jak se připojit k hotspotu a nezaplatit ani haléř. A jak je to s právní problematikou takového jednání? Podrobnosti najdete v boxu na straně 45. Na závěr vám pak ještě poradíme, jak byste si měli zabezpečit svoji vlastní Wi-Fi síť, aby se do ní nikdo nedostal.

DNS trik: Neprůchodný firewall

Hotspot je vlastně takovou informační dálnicí. Abyste mohli po dálnici jezdit, je třeba zaplatit mýto. Jenže obyčejná cesta, která vede hned vedle dálnice, je zcela zadarmo. A právě této cesty využijeme. Nebudeme připojeni k běžnému proxy serveru poskytovatele internetu, ale využijeme DNS (Domain Name System) serveru. DNS server slouží standardně k tomu, aby převáděl názvy serverů na IP adresy. Pokud do svého internetového prohlížeče zadáte **www.chip.cz**, DNS server prozradí, že se jedná o server s IP adresou 217.31.59.53, ke kterému se pak prohlížeč připojuje. Servery jsou totiž na internetu identifikovatelné právě podle IP adres a uživatel by si nikdy nezapamatoval desítky čísel svých oblíbených serverů. DNS servery vlastně fungují jako telefonní seznam – vy zadáte jméno a DNS najde správné číslo.

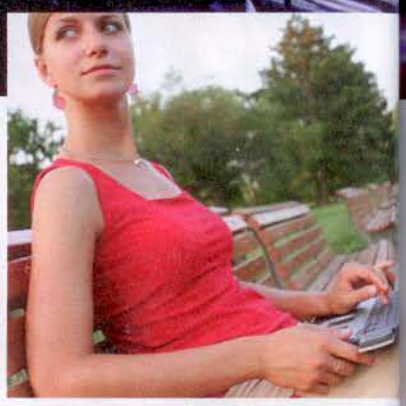
DNS server je naší první cestou k bezplatnému surfování. Provozovatel hotspotu totiž může zakázat přístup do domén, ale ne k DNS serverům. Pokud by zakázal přístup k DNS serveru, nemohla by se zobrazit ani úvodní obrazovka, která vás nabádá k zaplacení internetu a přihlášení se ke službě.

Toho můžeme využít. Svoje pakety přidružíme k DNS paketům a oklikou je pošleme, kam budeme chtít. Tak se dostaneme na běžné webové stránky. Příchozí pakety se pak navíc správně pošlou na náš počítač.

Jednoduchý princip, který ale vyžaduje pečlivou přípravu: aby DNS server převáděl jména na IP adresy, musíme vytvořit obejížďku. Je třeba vytvořit speciální server, který provede DNS převod. Tím vytvoříme kódované spojení, přes které je možné posílat data.

Příprava serveru: Datový převáděč

Pro přípravu vlastního DNS serveru neboli převáděče budete potřebovat počítač při-



Vlastní přenos: Pomocí nástroje PuTTY bude obsah webu zabalený v DNS paketech, které vám hotspot rád předá.

NAJDETE NA CHIP DVD

Prolomení Wi-Fi

OzymanDNS ► server pro DNS

PuTTY ► telnet klient

Backtrack ► linuxová distribuce pro hackery

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **PROLOMENÍ WI-FI**.

pojený k internetu. Tento počítač musí mít vlastní doménové jméno, aby jej bylo možné po zadání dotazu vyhledat v DNS databázi.

DYNDNS POMŮŽE: Aby bylo možné váš vlastní DNS server v internetu najít, je třeba, aby měl veřejnou statickou IP adresu. Jen tak budete mít jistotu, že se ke svému serveru budete moci kdykoliv dostat. Používáte-li k připojení k internetu ADSL od O2, dostanete sice veřejnou adresu, ale ne statickou. Adresa se tedy kdykoliv může změnit. Pokud byste chtěli statickou adresu, je třeba za ni připlatit.

Řešením je služba DynDNS (**www.dyndns.com**). Je-li vaše IP adresa přidělována dynamicky, DynDNS problém vyřeší. Otevřete si uvedenou webovou stránku a klikněte na »Create Account«. Zaregistrujte si službu – bude po vás vyžadován jen login a e-mail. Pro dokončení registrace je třeba otevřít e-mail, který přijde vzápětí po registraci, a dále kliknout na uvedený odkaz. Poté se ke službě znovu přihlaste. V části »My Services« klikněte na »Add Host Services«. Do řádku »Hostname« zadejte libovolné jméno své subdomény a vpravo si pak vyberte doménu. Do řádku »IP Address« zadejte současnou IP adresu svého připojení, případně můžete využít funkci pro automatickou detekci. Tu můžete použít v případě, že jste právě na internetovém připojení, na kterém bude v provozu také váš DNS server. Kliknutím na »Create Host« je dynamický DNS záznam vytvořen.

Většina domácích routerů již dnes podporuje službu DynDNS. Stačí se připojit k webovému rozhraní routeru. Pod položkou Advanced zde nejčastěji bývá Dynamic DNS nebo přímo DynDNS. Do rozhraní pak stačí vyplnit své uživatelské jméno a heslo, které jste zadávali při registraci, a doménu, kterou jste registrovali, v našem případě to bylo »chipdns«.

POUŽITÍ DOMÉNOVÉHO JMÉNA: Aby mohl DNS server na straně poskytovatele hotspotu přistupovat k vašemu převáděcímu DNS serveru, potřebujete mít doménové jméno, které bude přesměrováno na váš server. Máte dvě možnosti: Buď máte zakoupenu vlastní doménu, a pak si sami můžete upravit DNS záznam na odpovídající hodnotu (IP adresu). Ve většině případů stačí poslat vašemu správci e-mail s novými údaji, a tím je vše zařízeno.

Pokud doménu nevlastníte, je zde služba **www.dnstunnel.de**. Na uvedené stránce je vysvětleno, co musíte udělat. Celá stránka je bohužel v angličtině, proto přinášíme stručný popis. Poté, co máte vytvořen DynDNS záznam nebo máte pevnou IP adresu, pošle-

INFO

Zbavte se spolusurfařů

Náš trik se zneužitím DNS funguje jen u hotspotů, za které chce pronajímatel zaplatit. U domácích access pointů a routerů je třeba na několika frontách provést opatření, aby se k nim nikdo nepřipojil.

ZABEZPEČENÍ ROUTERU

Když vybalíte router z krabice a připojíte kabely, většinou už funguje. I notebook se sám připojí k otevřené Wi-Fi a vše se zdá v pořádku. Většina uživatelů se proto ani nesnaží nic měnit a nechá Wi-Fi tak, jak je. To je ovšem ten nejhorší případ – Wi-Fi síť je nezabezpečená, kdokoliv se k ní může přihlásit a změnit nastavení routeru. Je proto třeba provést potřebná zabezpečení.
Jak zabezpečení provést, to si ukážeme na routeru AirLive WN-300R. Spusťte internetový prohlížeč a zadejte adresu http://192.168.1.254. Výchozí adresu svého routeru najdete v návodu, někdy bývá adresa napsaná na spodní části routeru. Router bude požadovat uživatelské jméno a heslo. Jméno zadejte »admin«, heslo »airlive«.
V menu poté zvolte »Password«. Router bude vyžadovat napsání starého hesla (airlive) a dvakrát budete muset zadat nové heslo. Doporučujeme zvolit délku aspoň osm znaků.

SKRYTÁ SÍŤ

V části »Wireless« nastavte parametry sítě. Pod položkou »Mode« zadejte název sítě. Zrušte také zatržení u položky »Broadcast SSID«. Díky tomu nebude síť standardním způsobem viditelná, což řadu čmuchalů odradí. Pokračujte kliknutím na »Configure SSID1«.

SILNÉ HESLO

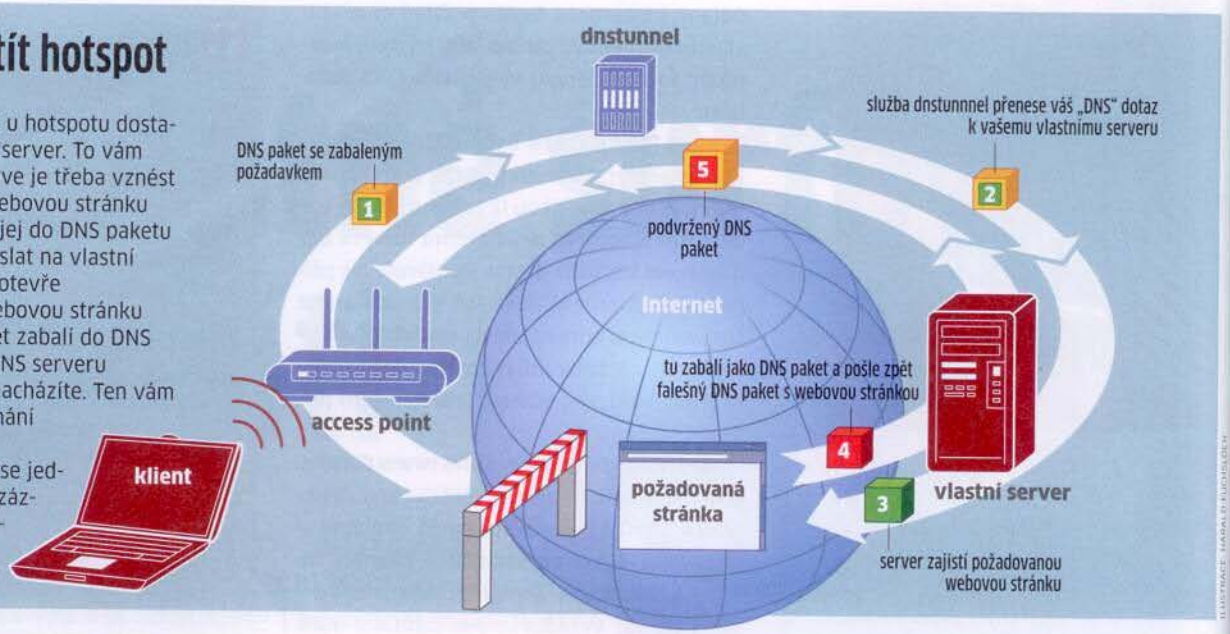
V části Security System vyberte »WPA2-PSK«. To je jediné šifrování, které lze považovat za dostatečně bezpečné. Do řádku PSK pak napište své heslo. Chcete-li mít jistotu neprůstřelnosti, zvolte heslo aspoň o délce 15 znaků. Kliknutím na »Save« změny uložíte.

JEN PRO VYVOLENÉ

Šifrování pomůže také k tomu, aby nikdo nerozkódoval vaši internetovou komunikaci. Pro dokonalou bezpečnost nastavte, aby se k síti nepřipojil nikdo cizí. Klikněte na »MAC Filter«. Dále zvolte »Trusted Wireless stations only«. Router nyní zobrazí seznam Wi-Fi klientů, kteří jsou nebo byli připojeni k routeru. Ta zařízení, kterým chcete dovolit přístup k Wi-Fi, označte a kliknutím na »<<« je přesuňte do důvěryhodné zóny. Budete-li chtít přidat nové zařízení, stačí vyplnit jeho jméno a MAC adresu. Ta je většinou zapsaná na zařízení; jedná-li se o počítač s Windows, zjistíte ji příkazem »ipconfig -all« v příkazovém řádku.
Máte-li síť skrytou, použito šifrování WPA2 a aktivován filtr MAC adres, do vaší Wi-Fi sítě se nedostane ani profesionální hacker.

Jak přelstít hotspot

Bez zaplacení se u hotspotu dostanete jen na DNS server. To vám však stačí. Nejprve je třeba vznést požadavek na webovou stránku (zelená), zabalit jej do DNS paketu (žlutý) a poté poslat na vlastní DNS server. Ten otevře požadovanou webovou stránku (červená), tu opět zabalí do DNS paketu a pošle DNS serveru v místě, kde se nacházíte. Ten vám pak data bez váhání předá, protože předpokládá, že se jedná o běžné DNS záznamy, a ne o placený web.



ILUSTRACE: HARALD FLÖRKEN

te e-mail na adresu **request@dnstunnel.de**. Do e-mailu uveďte své jméno, IP adresu, případně DynDNS záznam a také jméno subdomény, kterou chcete používat – jakmile bude vaše žádost vyřízena, získáte záznam v podobě jméno.dnstunnel.de.

Nyní je ještě třeba doplnit CNAME záznam služby DynDNS. Ten je určen k přesměrování na subdoménu. Pokud je referenční záznam například »chipdns.chip.cz«, bude záznam ze služby DynDNS vypadat třeba jako »chipdns.gotdns.com«. Odpovídající CNAME záznam pak vypadá takto: Do »Alias Name« zadejte název subdomény, v našem případě »chipdns«. Jako »Host Name« zadejte jméno včetně adresy svého DynDNS serveru, v našem případě »chipdns.gotdns.com«. Do položky »TTL« se zadává, jak dlouho má mít server uloženo připojení – standardně se zadává jedna hodina.

DNS PŘEVÁDĚČ: Nyní dojde k přípravě samotného serveru. Současné verze serverů jsou dostupné jen pro operační systém Linux. Bude tedy třeba spustit Linux. Ani jej nemusíte instalovat, zcela postačí vhodná live verze, kterou stačí nabootovat. Pro spuštění tak bude stačit starý počítač, případně si vystačíte i s virtuálním počítačem pod Windows. My jsme použili Slax, který je základem záchranného Chip DVD 5/09, stejně tak ale můžete použít jakýkoliv jiný Linux. Upozornění: Ve Slaxu se místo příkazu sudo používá sulogin.

Ke spuštění serveru použijeme aplikaci OzymanDNS, kterou naprogramoval v Perlu DNS guru Dan Kaminsky. Nástroj se skládá z pěti souborů – dva slouží pro upload/download za využití DNS. Hezké, ale pro nás nezajímavé. Skript nomde.pl je pak samotný server. Používá port UDP 53, který je privilegovaný, proto je třeba skript spustit jako root. Také se ujistěte, že port 53 je dostupný zvenku – aby jej neblokoval firewall. Poté spusťte server tímto příkazem:

```
sudo ./nomde.pl -i 0.0.0.0 vaše doména
```

Místo „vaše doména" zadejte doménu, kterou jste registrovali jako CNAME-DNS záznam.

Server je hotový, teď je třeba přichystat klienta.

Klient: Vše ve Windows

I klient funguje standardně jen pod Linuxem, už se však objevily první verze, které klienta zprovozní i pod Windows. Vlastní spojení mezi klientem a vaším DNS serverem je chráněno a šifrováno pomocí SSH. Takto se vytvoří DNS tunel až k vašemu serveru.

Pro tunelování použijeme program PuTTY, který protokol SSH podporuje. Spusťte PuTTY – najdete jej na Chip DVD. Zvolte »Connection | Proxy« a »Proxy Type« nastavte na »Local«. Jako »Proxy hostname« zadejte »proxy« a port »80«. Poté aktivujte volbu »Consider proxying local host connections« a do »Telnet command« zadejte:

```
droute.exe -r 1.1.1.1 vaše doména
```

V menu »SSH« ještě zatrhněte položku »Enable compression«. To zrychlí komunikaci. Dále v menu »Session« jako »Host Name« zadejte libovolný název. Bez jména by PuTTY nefungovalo. Port ponechejte na hodnotě »22«. Kliknutím na tlačítko »Open« provedete připojení.

Nyní je vše nastaveno. Abyste se však mohli třeba z Internet Exploreru připojit do sítě, je ještě třeba provést úpravu v konfiguraci připojení. Spusťte Internet Explorer, zvolte »Nástroje | Možnosti Internetu | Připojení«, klikněte na »Nastavení místní sítě« a zatrhněte položku »Použít pro síť LAN server proxy«. Pokračujte kliknutím na »Upřesnit« a do řádku »Socks« zadejte »localhost« a port »5000«. Po kliknutí na »OK« můžete nyní surfovat ve všech placených hotspot sítích zcela zdarma.

Vloupejte se k sousedovi: Prolomení WEP

Hotspoty využívají poskytovatelé připojení k internetu. Co když se ale chcete podívat třeba do Wi-Fi sítě svého souseda? Pokud nečte Chip a neprovedl preventivní opatření před možným zneužitím, můžete se pomocí našeho postupu do jeho sítě dostat.

BACKTRACK: Abychom mohli síť rozlousknout, budeme potřebovat profesionální výzbroj, kterou používají hackeři po celém světě. Na Chip DVD najdete image bootovacího Linuxu Backtrack. Tím, čím je pro kuchaře vařečka, je pro hackera Backtrack. Je třeba, aby měl Linux plný přístup k hardwaru, proto nemá smysl jej pouštět ve virtuálním počítači. Pomocí vhodného vypalovacího programu vypalte image na CD a nabootujte z něj počítač. Zhruba po třech minutách vás přivítá grafické rozhraní systému.

Tip: Na webové stránce **http://backtrack.offensive-security.com/index.php/HCL:Wireless** je seznam podporovaných Wi-Fi karet. U některých je také poznámka, jak pomocí několika jednoduchých příkazů upravit ovladače, aby návod fungoval.

WI-FI OVLADAČE: Vedle tlačítka »K«, které je na stejném místě jako tlačítko »Start« ve Windows a které má i stejnou funkci, najde-

PRÁVO

Je to vlastně legální?

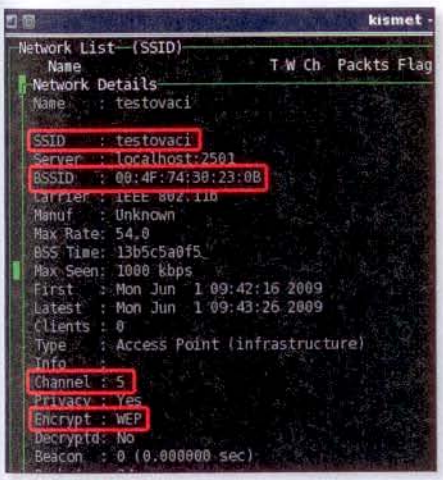
Je třeba se na letišti schovávat do temného koutku a neustále se dívat, nepřijde-li policejní kontrola? Nebo se není čeho bát?

PRÁVNÍ PROBLEMATIKU JEDNÁNÍ NÁM OBJASNIL ADVOKÁT.

Povolí-li provozovatel připojení omezený přístup na svůj hotspot, nedává tím sám o sobě najevo možnost jeho volného užívání. Pokud je dostupná jen některá neklíčová služba, využití takové služby k jinému účelu (např. služby tunelování HTTP pomocí DNS) v naprostě většině případů také není provozovatelem povoleno. Uživatel tak bude nejspíše porušovat obchodní podmínky provozovatele a způsobovat mu zejména neoprávněným vytížením přenosové kapacity škodu a dále ušlý zisk. Stejné je to s neoprávněným přístupem k cizí šifrované Wi-Fi síti. Navíc neoprávněné připojení k takové síti bude od příštího roku trestné.

Chip dodává: Ušlý zisk je v takovém případě v řádu desetikorun. Je tedy nepravděpodobné, že se v kavárně objeví zásahová skupina mužů v černém. Zkrátka: Kde není žalobce, tam není soudce.

Každopádně ale platí, že vás Chip nenabádá k tomu, abyste se takto prolomili do sítě, u které nemáte od jejího provozovatele svolení. Veškerou popsanou činnost **PROVÁDÍTE NA SVÉ VLASTNÍ RIZIKO.**



Informace o síti: Nástroj Kismet poskytne podrobné informace o síti, do které se chcete dostat.

te ikonu s černou obrazovkou – spuštění terminálu. Klikněte na ni, otevře se černé okno. Zadejte příkaz

```
iwconfig
```

a potvrďte klávesou [Enter]. Program vypíše, které síťové karty jsou v počítači dostupné.

Distribuce Backtrack obsahuje ovladače pro množství Wi-Fi karet, takže je vysoká pravděpodobnost, že najde i tu vaši. Na našem počítači našel Backtrack dvě karty: eth0 a eth1. U eth0 je poznámka »no wireless extensions«, u eth1 je správně popsaná konfigurace. Víme tedy, že eth1 je správná karta, se kterou budeme laborovat. Pokud je u vašeho počítače Wi-Fi eth0, ve všech příkazech zadávejte eth0.

Dále zadejte příkaz

```
macchanger -s eth1
```

Tím se vypíše MAC adresa vaší síťové karty. Tu si poznamenejte, budete ji potřebovat.

OKOLNÍ SÍTĚ: Nyní je čas podívat se, jaké sítě jsou v okolí. Zvolte »K | Backtrack | Radio Network Analysis | 80211 | Analyser | Kismet«. Během několika sekund se spustí aplikace, která zobrazí dostupné Wi-Fi sítě. Na klávesnici stiskněte [s] a znovu [s]. Tím se sítě seřadí podle názvu. Šipkami si vyberte síť, do které se chcete nabourat, a stiskněte klávesu [Enter]. Zobrazí se podrobnosti o síti, tak jak vidíte na obrázku. Najděte řádek »Encrypt« a podívejte se, zda je v něm uvedeno »WEP«. Jedná se o typ šifrování. WEP lze relativně jednoduše prolomit, na rozdíl od WPA, kde je postup složitější. Pokud je nastaveno šifrování WEP a síť nemá omezený přístup podle MAC adres, máte téměř vyhráno. Ze zobrazeného okna si ještě poznamenejte hodnoty »SSID« (název Wi-Fi sítě), »BSSID« (MAC adresa přístupového bodu) a »Channel« (číslo kanálu). Stisknutím [q] a [Q] (velikost písmen hraje roli) aplikaci Kismet ukončíte.

SBĚR DAT: Aby bylo možné heslo najít, je třeba nejprve začít sbírat data, která sviští vzduchem. Z nich se pak heslo rozkóduje. Spusťte Terminál a zadejte dva následující příkazy

```
cd Desktop
```

```
airodump-ng eth1 -w mojedata
--channel 5 --ivs
```

Za příkazem »channel« se zadává číslo (v našem případě 5), podle čísla kanálu sítě, do které se snažíte dostat. Toto číslo jste si zapsali v minulém kroku. Po potvrzení se spustí ukládání – nemusíte mu věnovat pozornost, do okna se vrátíme až na konci tohoto návodu.

PŘÍSTUP NA AP: Teď je třeba začít „oťukávat" access point. K tomu poslouží utilita aireplay. Spusťte nové okno terminálu a zajdete následující příkaz:

```
aireplay-ng -1 0 -e testovaci -a
00:4F:74:30:23:0B -h 00:11:22:33:44:55 eth1
```

Tím přesně definujete, co je terčem vašeho útoku. Hodnota –1 říká, jaká je forma útoku, 0 je pak prodleva mezi útoky. Hodnotu »testovaci« zaměňte za SSID sítě, do které se chcete dostat, MAC adresu za parametrem –a zaměňte za MAC adresu AP. Oboje jste si zapsali v okně s příkazem kismet. MAC adresa za parametrem –h je MAC adresa vaší síťové karty. Také ji tedy změňte, je to první hodnota, kterou jste si poznamenali. Příkaz ještě nepotvrzujte a spusťte další okno terminálu.

INJEKCE PAKETŮ: Nyní začneme na access point posílat pakety a zjišťovat, co nám odpoví. Zadejte tedy příkaz

```
aireplay-ng -3 -b 00:4F:74:30:23:0B -h
00:11:22:33:44:55 eth1
```

První MAC adresa je opět vzdálený AP, druhá je opět vaše síťová karta.

Příkaz potvrďte, vraťte se do předchozího okna terminálu a příkaz také potvrďte. Nejlepší bude, když si okna dáte vedle sebe, abyste je mohli sledovat.

V prvním okně se budou posílat žádosti o autentizaci, ve druhém uvidíte, jak se injektují pakety. Zde je důležité sledovat hodnotu ARP, která se postupně zvyšuje. Čím větší je provoz na síti, tím rychleji hodnota roste. Aby bylo možné heslo určit, je třeba, aby ARP mělo aspoň hodnotu 1000. Někdy to trvá pět minut, jindy to může být hodina. Pokud se stane, že v prvním okně příkaz skončí, spusťte jej znovu. Již jej nemusíte celý opisovat, stačí na klávesnici stisknout šipku nahoru a potvrdit. Jakmile dosáhne ARP hodnoty 6000, můžete obě terminálová okna zavřít. Vraťte se do terminálového okna, které jste otevřeli v bodě „sběr dat".

NALEZENÍ HESLA: Sběr dat ukončete klávesovou zkratkou [Ctrl]+[c]. Mezitím na ploše systému uvidíte nové soubory, které ukládaly informace potřebné k rozluštění hesla. Zadejte příkaz

```
aircrack-ng -s mojedata-01.ivs
```

Soubor mojedata-01.ivs vidíte na ploše systému. Pokud je název souboru odlišný, přizpůsobte jej. Po potvrzení se zobrazí tabulka s informacemi, co je v souboru uloženo. V prvním sloupci je číselný identifikátor sítí. Vyberte tu, do které jste se vlámali. Nyní dojde k hledání hesla – to může několik minut trvat. Nakonec vás přivítá hláška »KEY FOUND«.

VRATISLAV.KLEGA@CHIP.CZ

KASPERSKY LAB

Kaspersky Mobile Security 8.0

Společnost PCS, oficiální distributor Kaspersky Lab pro ČR a SR, oznámila vydání Kaspersky Mobile Security 8.0. Toto řešení je navrženo pro ochranu mobilních telefonů (smartphonů) před všemi typy softwarových a síťových hrozeb stejně jako před rizikem úniku citlivých dat v případě krádeže nebo ztráty přístroje. Nový produkt ocení zejména lidé, kteří mají ve smartphonech uložena citlivá data.

„Nová verze řešení Kaspersky Mobile Security obsahuje množství nových funkcí, které jsou mezi dalšími řešeními na trhu zcela unikátní. Jedná se například o SMS Find, rodičovskou kontrolu či rozšířené možnosti blokování SIM karty," říká Bohdan Vrabec, Kaspersky Distribution Manager. Služba SMS Find dokáže v případě zařízení s navigací GPS odhalit přesnou pozici ztraceného telefonu. Služba funguje tak, že uživatel pošle na ztracené zařízení SMS zprávu s předem určeným heslem a jako odpověď obdrží odkaz do systému Google Maps s přesnými souřadnicemi polohy. Modul proti krádežím v řešení Kaspersky Mobile Security 8.0 umožňuje vlastníkovi ztraceného nebo odcizeného smartphonu vzdáleně zablokovat přístup k zařízení nebo zcela vymazat jeho paměť pouze tím, že pošle na číslo telefonu SMS zprávu obsahující kódové slovo. Pro případ, že je ze ztraceného nebo ukradeného telefonu vyjmuta SIM karta, je v řešení Kaspersky Mobile Security 8.0 obsažen modul SIM Watch, který skrytě odešle zprávu, oznamující vlastníkovi telefonu nové telefonní číslo přístroje. Tato funkce zajišťuje, že vlastník bude moci bez ohledu na okolnosti smazat svá data nebo telefon zablokovat. Policie může nové číslo použít také k tomu, aby ukradené zařízení vysledovala a vrátila právoplatnému majiteli.

Další bezpečnostní funkce

Pro uložení citlivých nebo důvěrných informací do mobilního telefonu umožňuje řešení Kaspersky Mobile Security 8.0 přidat další úroveň zabezpečení. Ve smartphonu je vytvořena zabezpečená složka, jejíž obsah je neustále zašifrován a je přístupný pouze po zadání uživatelem definovaného hesla. Po zadání hesla složka kvůli zvýšení komfortu práce zůstává přístupná, dokud systém nedetekuje určitou dobu bez uživatelovy aktivity; pak složku opět uzamkne. Novinkou v řešení Kaspersky Mobile Security 8.0 je rodičovská kontrola. Tato komponenta umožňuje rodičům omezit na mobilním telefonu dítěte zasílání nebo přijímání určitých zpráv (například na čísla se speciální tarifikací, na čísla se službami pro dospělé apod.). Pomocí funkce SMS Find mohou rodiče v případě, že telefon podporuje GPS, své děti také najít.

Řešení Kaspersky Mobile Security 8.0 obsahuje rovněž vylepšený antispamový modul, antivirový skener a firewall. Aplikace je kompatibilní s operačními systémy Symbian 9.1, 9.2 a 9.3 a Windows Mobile 5.0, 6.0 a 6.1.

INFO: www.kaspersky.com

TIPY KASPERSKY LAB

Nárůst útoků na Facebooku

15. května zasáhl web Facebooku další phishingový útok. David Emm, člen týmu Global Research and Analysis Team společnosti Kaspersky Lab, popisuje současnou situaci takto: „Fenomenální úspěch Facebooku, Twitteru a dalších oblíbených serverů sociálních sítí vyvolal samozřejmě zájem počítačových zločinců. Tato skutečnost není nijak překvapivá a neobjevují se žádné známky toho, že by se situace měla zlepšit. Phishingové podvody jsou založeny na tom, že útočníci obětem předhodí návnadu, předstírají něco, co se na první pohled může zdát legitimní. Nechcete-li spadnout do této pasti, je klíčové používat určité obranné prostředky a zachovávat ostražitost."

Škodlivý kód distribuovaný pomocí serverů sociálních sítí je podle odhadu z hlediska počtu úspěšných infekcí 10krát účinnější než malware šířený e-mailem. Uživatelé internetu s daleko větší pravděpodobností kliknou na odkaz, který dostali od důvěryhodného „přítele" (kontakt v sociální síti), než na odkaz v náhodném spamovém e-mailu. Společnost Kaspersky Lab v poslední době zaznamenala masivní nárůst phishingových útoků na přihlašovací stránku Facebooku. Počítačoví zločinci používali interní systém Facebooku pro zasílání zpráv k rozesílání krátkých textů, které po kliknutí na odkaz přivedou uživatele na stránku záměrně navrženou tak, aby vypadala jako přihlašovací stránka Facebooku.

Společnost Kaspersky Lab nabídla praktický návod a informace určené pro minimalizaci rizika, že se uživatel stane obětí phishingových podvodů a dalších útoků počítačových podvodníků. Your Guide To Stopping Cybercrime (Průvodce pro zastavení počítačové kriminality) je zdarma k dispozici na webu www.kaspersky.com/downloads/pdf/stopcybercrime_guide.pdf.

Hlavní tipy společnosti Kaspersky Lab pro ochranu proti phishingovým útokům:

- U serverů, jako je Facebook, si přihlašovací stránku uložte do oblíbených položek (záložek) webového prohlížeče nebo zadávejte URL přímo do adresního řádku prohlížeče.
- Neklikejte na odkazy v e-mailových zprávách.
- Důvěrná data zadávejte pouze na bezpečných webových serverech.
- Kontrolujte si pravidelně svůj bankovní účet a ihned kontaktujte banku v případě čehokoliv podezřelého.
- Sledujte, zda určitá zpráva nenese znaky phishingového e-mailu. Mezi takové znaky patří například to, že není adresována přímo vám, že nejste jediným příjemcem, že zpráva obsahuje pravopisné, gramatické nebo syntaktické chyby nebo jinak nesprávně používá jazyk.
- Nepřihlašujte se zbytečně s oprávněními správce.
- Zálohujte svá data.

Daň za popularitu: Facebook se stává stále častějším cílem útoků. Velká komunita uživatelů láká i internetovou mafii...

David Emm své varování zakončuje následujícími slovy: „Velký počet zpráv o probíhajících podvodech, jejichž příkladem je poslední útok proti Facebooku, zvyšuje povědomí o rizicích počítačové kriminality. Je ale důležité si ujasnit, že se nejedná o izolovaný incident. Každý den zaznamenáváme více než 17 000 nových internetových hrozeb."

Komentář redakce: *Uživatelé sociálních sítí jsou lákavým cílem nejen proto, že mezi nimi panuje „větší důvěra", ale z toho důvodu, že zde lze narazit na velké procento méně zkušených uživatelů. Popularita sítí tohoto typu vzrostla natolik, že v nich najdete i naprosté začátečníky, kteří mají s hrozbami z internetu jen malé, nebo dokonce žádné zkušenosti.*

Dobrá zpráva na závěr: Uživatelé českých „alternativ" mohou být prozatím klidní – díky naší „velikosti" jsou jako cíle phishingových útoků pro internetové zločince nezajímavé.

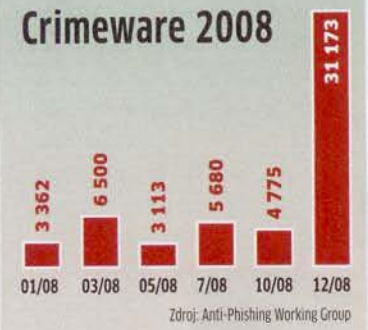
INFO: www.kaspersky.com

DATA A FAKTA

Barometr nebezpečí
v květnu:

Poté, co lovci virů dostali pod kontrolu červa Conficker, nastalo trochu klidu. Spammeři a „phisheři" však nikdy nespí, a proto buďte i nadále opatrní.

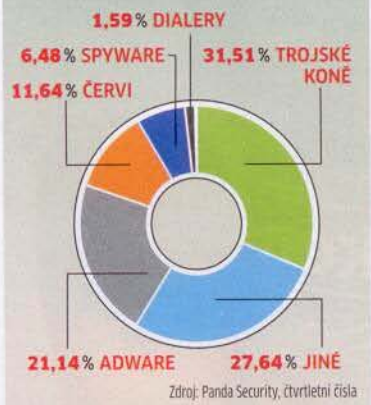
Crimeware 2008



Zdroj: Anti-Phishing Working Group

Počet podvržených stránek (phishing) stoupl v roce 2008 celosvětově o 927 %, na 31 173.

Spyware boom



Zdroj: Panda Security, čtvrtletní čísla

Trend: Četnost infekcí spywarovými nástroji vzrostla z 2,93 na 6,48 %.

Číslo měsíce

0,06

eura stojí platná kreditní karta s odpovídajícím kontrolním číslem na ilegálních hackerských webových stránkách.

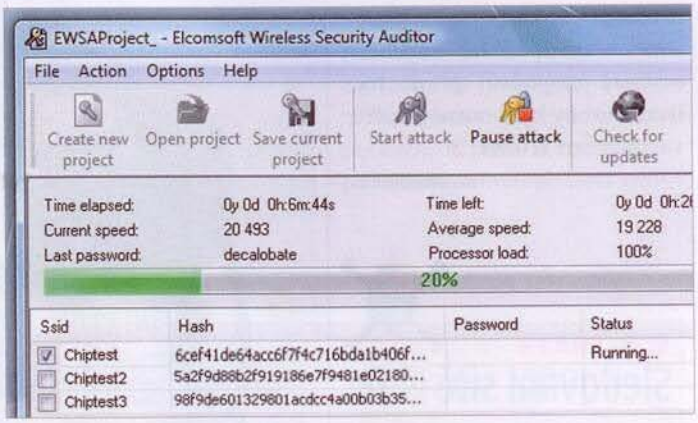
Průlom do Wi-Fi silou grafiky

Ruský nástroj prorazí **BĚHEM NĚKOLIKA MINUT** bezpečná hesla pro WLAN. Využívá k tomu výpočetní výkon grafického čipu.

FABIAN VON KEUDELL

Sítě WLAN chráněné standardem WPA a WPA2 až dosud platily za bezpečné. Nyní však program Wireless Security Auditor od ElcomSoftu dokáže jejich hesla prolomit. A stačí mu na to pár minut – má-li ovšem k dispozici výkonnou grafickou kartu.

Oba typy šifrování používají k výměně dat TKIP (Temporal Key Integrity Protocol). Vlastní šifrování zajišťuje u WPA algoritmus RC4, u WPA2 postup AES. Slabým místem je v obou případech autentifikace. Dříve než si dva WLAN moduly mohou mezi sebou vyměnit data, musí si navzájem důvěřovat. Za tím účelem každá ze stran vypočítá z hesla WLAN, názvu sítě (SSID) a délky SSID klíč PMK (Pairwise Master Key). S ním pak oba partneři vypočítají další klíč, tzv. PTK (Pairwise Transient Key). Na základě PTK, MAC adres obou přístrojů a náhodných čísel vygenerují komponenty příslušným šifrovacím postupem RC4 nebo AES konečné zašifrování.



Heslový thriller: Nástroj Wireless Security Auditor od ElcomSoftu se do sítě WLAN dokáže vloupat v několika minutách.

Poněvadž přístroje přenášejí náhodná čísla a MAC adresy v nezašifrovaném tvaru, každý, kdo zná PMK, se může dostat do sítě.

Právě toho nyní využívají programy jako Wireless Security Auditor, které se pokoušejí zjistit PMK obyčejnou hrubou silou. Pro útočníka mají tu výhodu, že nemusí být v blízkosti napadené WLAN. Nástroj u každého hesla zjišťuje, zda se z něj dá vypočítat odpovídající PTK. Programy tohoto typu však předpokládají enormní výpočetní výkon.

Rychlý proces: Slovník a grafická karta prolomí skoro všechno

Nástroj od ElcomSoftu sází vedle obvyklé výpočetní síly CPU na nesmírný výkonnostní potenciál, který dřímá v grafických kartách. Program pro sebe může nechat pracovat až osm GPU s libovolným počtem jader; v praxi by to mohly být čtyři karty se zdvojenou GPU, které jsou propojeny prostřednictvím SLI. Pokud přitom útočník použije zvláště výkonné modely, třeba nVidia GeForce GTX295, dokáže Wireless Security Auditor vyzkoušet 250 milionů hesel za sekundu – na jednu kartu je program dvacetkrát rychlejší než běžná aplikace, pro kterou pracuje například Intel Core 2 Duo E4500. S rychlým hledáním jednoduchých hesel pomáhají slovníky v různých jazycích. Program snadno pozná i zmodifikované pojmy, například „freak mutations" (písmena nahrazená zvláštními znaky) a „order mutation" (kombinace zapsané pozpátku). Ale ten, kdo používá tzv. silná hesla alespoň o dvaceti znacích, je i nadále v bezpečí.

INFO: www.icann.org

ESET ON-LINE

Nová verze bezplatného skeneru

ESET oficiálně spustil novou verzi bezplatného nástroje na zjištění stavu bezpečnosti počítače. ESET Online Scanner je možné najít na adrese **www.eset.cz/eset-online-skener**. Oproti předchozí verzi má nový on-line skener rozšířené možnosti svého nastavení, vyhledává rootkity a je kompatibilní s více webovými prohlížeči.

ESET Online Scanner se od své předcházející verze, která je k dispozici od léta 2007, výrazně změnil. Podle Michala Vidomana, produktového manažera společnosti ESET, prošla nová verze nástroje ESET Online Scanner několikaměsíčním náročným testováním ve fázích beta a release candidate, aby bylo zabezpečeno bezproblémové používání. „ESET Online Scanner je vynikající první pomoc v případě, když uživatel nemá jistotu v otázce bezpečnosti svého počítače," dodává Michal Vidoman.

Nový ESET Online Scanner dokáže nalezené infiltrace nejen odhalit, ale i odstranit. Všechny objevené infiltrace jsou přesouvány do karantény, kde už nepředstavují další nebezpečí. Soubory je možné z karantény obnovit nebo vymazat.

Mezi další nové funkce ESET Online Scanneru patří implementovaná technologie Anti-Stealth pro odhalování a odstraňování rootkitů, podpora 64bitových platforem nebo nastavení proxy pro pokročilé uživatele.

Komentář redakce: *Verze RC se zúčastnila i našeho testu on-line bezpečnostních nástrojů (viz Chip 05/09), kde potvrdila své kvality a opět se umístila mezi nejlepšími. Potěšila nás uživatelská přívětivost nástroje a především jeho rychlost – ve srovnání s konkurencí byl až o polovinu rychlejší. Jedinými dvěma drobnostmi, které jsme nástroji vytkli, byla absence pozastavení testu (nástroj je možné jen ukončit) a chybějící export výsledků.*

INFO: www.eset.cz

Anonymně na

Vyzkoušejte naše tipy a **OCHRAŇTE SI SVÉ SOUKROMÍ** nejen před slidivými pohledy – a to jak na internetu, tak i na domácím počítač. Na Chip DVD navíc najdete všechny důležité nástroje...

DOMINIK HOFERER

Pravděpodobně nejste ani tajný agent, ani na internetu nejednáte s islámskými teroristy. Nejspíš také na svém počítači nemáte „citlivé" informace, kvůli kterým potřebujete šifrovat svá data pomocí nejdůmyslnějších metod šifrování.

Přesto lze na vašem počítači narazit na dokumenty, které je možné označit za osobní a u kterých by únik „na internet" přinejmenším „nebyl žádoucí"...

Mohou to být výpisy z on-line bankovnictví, informace o daních nebo detaily z rodinného rozpočtu.

Jen málokterý uživatel by také ocenil, kdyby mohl kdokoliv zjistit podrobnosti o jeho toulkách internetem nebo dotazy, které zadá v Googlu. Proto vám ukážeme, jak surfovat na webu, aniž byste za sebou nechávali stopy, a také jak s co nejmenším úsilím na počítači ukládat soubory takovým způsobem, aby pro ostatní uživatele zůstaly nepřístupné. Jako obvykle pak všechny zmiňované nástroje, nutné k „vymazání stop", najdete na našem DVD.

Bez výčitek svědomí: Surfujte s Firefoxem

Přestože se schopnosti Internet Exploreru s každou verzí rapidně zlepšují, stále ještě platí, že Firefox vás dokáže ochránit před útoky z webu lépe než konkurence od Microsoftu. Ale pozor, i Firefox za sebou zanechává stopy – pouze nabízí jednodušší a rozsáhlejší možnosti jejich eliminace.

Při běžném surfování mohou váš pohyb po internetu sledovat nejen správci navštívených stránek. Obvykle je sledován i váš pohyb po internetových obchodech – a to i v případě, že si žádné zboží nekoupíte. My vám poradíme několik triků, které o vás prozradí jen to nejnutnější.

NASTAVENÍ: Nejprve musíte v prohlížeči udělat několik málo změn. V nabídce »Nástroje | Nastavení | Soukromí« přejděte do sekce „Důvěrná data" a zde klikněte na tlačítko »Nastavení«. Označte všechny položky, potvrďte kliknutím na »OK« a na závěr nezapomeňte aktivovat zatržítko u položky „Při ukončení aplikace Firefox vymazat důvěrná data". Díky tomuto nastavení zmizí většina stop po surfování spolu s ukončením prohlížeče.

Abychom však odstranili skutečně všechny stopy, musíme se podívat ještě hlouběji do konfiguračních dialogů. Kam tedy zajít, aby nebyly prozrazeny navštívené stránky a aby cíle vašich toulek internetem zůstávaly maskované?

Do adresního řádku prohlížeče zadejte příkaz

```
About:config
```

Pro zjednodušení hledání potřebné položky ještě do řádku „Filtr" zadejte slovo „send". Objeví se několik položek, nás ale zajímá pouze jediná: „network.http.send RefererHeader". Dvojitým kliknutím ji otevřete a nastavte její hodnotu na „0". Tím zabráníte správcům webu vysledovat, odkud jste se na jejich stránky dostali, tedy ani vyhledávací řetězec, který jste zadali do Googlu. Toto nastavení vám také pomůže s celou řadou „problémů", které někteří správci webů připravují „cizím" návštěvníkům (například při prohlížení obrázků).

ROZŠÍŘENÍ: Rozšíření Firefoxu CustomizeGoogle jde ještě o krok dál. Tento šikovný doplněk aktivně brání, aby si vyhledávače vytvářely váš přesný profil. Po instalaci ale musíte doplněk nejprve nakonfigurovat v nabídce »Nástroje | Nastavení CustomizeGoogle«.

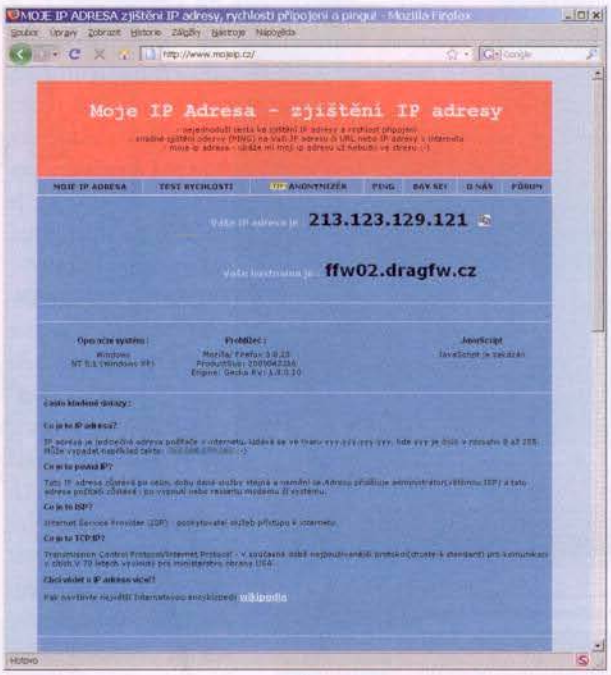
Zde můžete například odstranit sledování myši, zbavit se otravných reklam nebo vypnout nápovědu Googlu. Další dvě volby důležité pro ochranu dat najdete v sekci »Soukromí«. Zde lze skrýt před Googlem svou identitu, stejně jako zakázat zasílání cookies serveru Google Analytics.

APLIKACE: Ještě mocnějším nástrojem z hlediska anonymního surfování je TOR. Zjednodušeně řečeno jde o „proxy", maskující vaše stopy na síti a tím i vaši identitu. Používáte-li jej při surfování, ani správci webových stránek nebudou nikdy schopni vystopovat vaši opravdovou IP adresu, protože „od Toru" dostanete novou.

Nejkomplexnějším způsobem maskování je zahalení se do neviditelného pláště pomocí kombinace programů Tor, Privoxy a Vidalia. To jsou nejdůležitější nástroje pro váš pobyt na internetu „beze stop" – pokud je zkombinujete s Firefoxem, získáte snadný přístup k anonymnímu surfování. Balíček programů navíc k Firefoxu přidává tlačítko Tor, jehož pomocí lze jednoduše zapnout či vypnout proxy přímo z lišty prohlížeče. Při příštím spuštění už v pravém dolním rohu uvidíte, zda je Tor aktivován, nebo ne. Stav můžete změnit pomocí kliknutí pravým tlačítkem na ikonu Toru, čímž si rychle zajistíte anonymitu během surfování. Pokud chcete mít stoprocentní jistotu, navštivte například web **www.mojeip.cz**, kde se dozvíte svou současnou „identitu" (například IP adresu a další informace o používaném softwaru). A protože proxy tuto informaci v nepravidelných intervalech „upravuje", je téměř nemožné vystopovat vaše aktivity na síti. Cena za anonymitu však není zrovna malá: rychlost při surfování na webu je podstatně nižší. Podrobný návod na anonymní surfování najdete na našem webu na adrese **www.chip.cz**.

Další alternativou je nástroj CyberGhost. Přestože Tor zakryje vaše stopy lépe, aplikace CyberGhost nabídne jinou, pro celou řadu uživatelů důležitější výhodu: můžete surfovat podstatně rychleji.

Po nainstalování a spuštění programu si vytvořte na webu firmy (**www.cyberghostvpn.com**) zdarma účet a přihlaste se. V rámci bezplatného anonymního provozu máte k dispozici 10 GB dat na měsíc, což je pro běžné surfování více než dostatečné. Drobnou nevýhodou je ještě automatické odpojení po šesti hodinách provozu a negarantovaná rychlost. Ti, kteří potřebují více, si mohou objednat prémiové konto za přibližně 10 eur měsíčně (s datovým tokem 40 GB, minimální garantovanou rychlostí 2 000 Kb/s a 2GB online šifrovaným úložištěm). Avšak CyberGhost neumí jen „anonymní surfování" – dokáže skrýt i váš „poštovní provoz".



Jste skryti: Na tomto webu si můžete ověřit, zda je vaše IP adresa skutečně změněna...

Neprůstřelná pošta: Komunikujte s Thunderbirdem

Existuje někdo, kdo má rád cizí lidi čmuchající v jeho soukromé poště? Většina běžných uživatelů se musí

NAJDETE NA CHIP DVD

Zabezpečení soukromí

CustomizeGoogle ► upravuje rozhraní a výsledky Googlu
CyberGhost ► maskuje vaši IP adresu
Enigmail ► zabezpečuje vaši elektronickou poštu
Gpg4win ► chrání soubory a složky heslem
GnuPG ► šifruje a podepisuje emaily
Mozilla Thunderbird ► alternativní poštovní klient
Prism ► nabízí pokročilou konfiguraci cookies
TrackMeNot ► nástroj na mazání stop
TrueCrypt Portable ► šifruje přenosné disky
Stegano32 ► skrývá dokumenty do multimediálních souborů
Steganos Shredder ► trvale odstraňuje data

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

u mailů spoléhat na fakt, že poskytovatelé freemailových kont osobní maily obvykle nekontrolují. Existuje ale jiné riziko: vzhledem k tomu, že většina komunikace po internetu probíhá nešifrovaně, stačí, aby někdo „vyzkoušel" zachytávání paketů na lokální síti příjemce nebo odesílatele, a cestu k obsahu vašich dopisů má volnou...

S Mozillou Thunderbird a novým rozhraním se můžete přestat tohoto rizika bát. Použijte nástroj GnuPG, který s Thunderbirdem bezproblémově spolupracuje. Stačí jen zařídit šifrování vašich mailů tak, aby zprávy mohl číst jen příjemce, a naopak abyste vám určené dopisy rozšifrovali jen vy. Kódování je asynchronní a funguje následovně: Pomocí GnuPG vytvořte sadu dvou klíčů; jeden bude osobní a ten druhý veřejný. Předejte veřejný klíč všem, od koho čekáte důležité e-maily. Zároveň si musíte dávat dobrý pozor na osobní klíč – nikdy byste ho neměli zveřejnit. To proto, že kódované maily odesilatelů můžete dekódovat pouze pomocí tohoto klíče. Podrobnější teoretické informace o této technologii najdete v minulém Chipu.

V praxi to funguje takto:

Na svůj počítač si nainstalujte GnuPG a k Thunderbirdu si přidejte doplněk Enigmail. V menu hlavního klienta klikněte na »OpenPGP | Key management«. V okně, které se objeví, přejděte na nabídku » Generate | New key pair« a zvolte ID (identifikaci e-mailového konta v Thunderbirdu).

Poté zadejte tzv. passphrase, což je (zjednodušeně řečeno) heslo, pomocí kterého se bude komunikace šifrovat (ideálně by se mělo skládat jak z čísel, tak z písmen). Toto „heslo" si dobře zapamatujte, protože ho budete potřebovat k dekódování mailů. Profesionálové mohou ještě definovat sílu klíče v sekci „Advanced" nebo zvolit speciální algoritmus. Nyní můžete vygenerovat samotné klíče (příkaz »Generate key pair«), což si ale vyžádá několik minut. Poté je váš poštovní klient připraven posílat utajené zprávy.

GnuPG vám nabízí dvě verze „lepší pošty". První jen vylepšuje identifikaci: můžete zprávy podepsat digitálně. Díky tomu se může příjemce přesvědčit, zda byla zpráva opravdu zaslána vámi. Není to zbytečná práce, protože existuje celá řada metod, jak poslat mail vaším jménem (tuto technologii velmi často používají spammeři). Tomuto riziku se můžete vyhnout podepsáním svých e-mailů (v programu příkaz »OpenPGP | Sign message«). Jestliže příjemce vlastní váš veřejný klíč, Thunderbird potvrdí správného odesilatele a označí ho zeleným proužkem v horní části mailu. Pozor: Tento postup zprávu jen podepíše, ne zašifruje!

Druhá, bezpečnější a zároveň „nijak náročná" varianta je zakódování odchozí pošty. Opravdu to není nic složitého – vyzkoušejte si to: Nejprve klikněte na »Compose«, poté klikněte na »OpenPGP | Encode message« a pošlete si mail. Zpráva by měla za nějakou dobu dorazit do vaší schránky. Zároveň by měl Thunderbird zeleným pruhem upozornit, že jde o „bezpečný e-mail". GnuPG toho ale umí mnohem více – pomůže vám nejenom při kódování vašich mailů, ale i při šifrování lokálních souborů. Podrobnější informace najdete v programu v sekci „Secret".

Tajný: Šifrování pomocí open-source

Ať už jde o telefonní účet, nebo o bankovní výpis stažený z portálu banky, papír postupně mizí z našeho běžného života, v současné době jsou důležité dokumenty stále častěji zasílány ve formátu PDF. Často pak leží nechráněné v počítači a kdokoliv, kdo má k vašemu počítači přístup, si je může prohlédnout. Jak se tomu bránit?

OCHRANA DOKUMENTŮ: Chraňte jednotlivé soubory jednoduše hesly pomocí softwaru GnuPG, který jsme již popsali v sekci o šifrování pošty. Libovolný soubor lze jednoduše zašifrovat pomocí aplikace Gpg4win přes kontextové menu Windows. Po instalaci programu stačí na soubor kliknout pravým tlačítkem. Nejprve je ale nutné nástroj v nabídce »GPGee | Configure« nakonfigurovat. Zde musíte například určit cestu k programu („Path of the program") - zadat cestu k souboru „gpg.exe" (ten se většinou nachází ve složce „C:\Program Files\GNU)". Poté je software připraven k použití. Nyní lze pomocí jednoduchého kliknutí pravým tlačítkem šifrovat vybraný soubor či celou složku.

ALTERNATIVNÍ METODA: Zvolte příkaz »GPGee | Encrypt (symmetrical)«. Jakmile vložíte již zmiňovanou „passphrase", nástroj vaše data zašifruje.

ŠIFROVÁNÍ DISKŮ: Komplexnějším nástrojem vhodným pro šifrování většího objemu dat je TrueCrypt Portable, který najdete na našem DVD. Ten dokáže chránit i přenosná paměťová média. Nyní vám ukážeme, jak lze pomocí tohoto nástroje šifrovat USB.

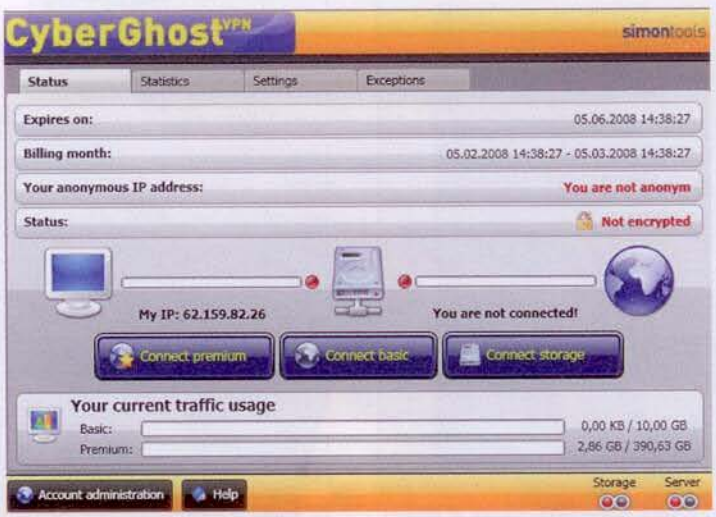
Rozbalte si program na svém počítači a jeho kompletní složku zkopírujte na USB. Poté program TrueCrypt spusťte a klikněte na »Create volume«. Nyní zvolte možnost umístěnou v horní části nabídky a vytvořte virtuální, zakódovaný disk. V dalším okně vyberte variantu „standardn TrueCrypt volume" a klikněte na »Next« a poté na »File«. Poté zvolte svůj USB, upřesněte název „kontejneru", do kterého si přejete ukládat důvěrné informace v kódované formě, a volbu potvrďte pomocí »Save«. Dále určete velikost kontejneru a zadejte „passphrase".

Nakonec vše potvrďte pomocí příkazu »Format«, který kontejner připraví k použití. Pokud si nepřejete vytvořit další „skrýše", klikněte na »End«. Váš USB nyní obsahuje šifrovaný datový kontejner, k jehož obsahu se bez programu TrueCrypt a vaší „passphrase" nikdo nedostane...

Abyste mohli kontejner otevřít a soubor použít, otevřete tento soubor v programu TrueCrypt v nabídce »File | Integrate« a zadejte „heslo". Poté se v okně „Tento počítač" objeví virtuální disk s vašimi daty. Pozor: Jakmile jednou uložíte všechny soubory do kontejneru, zavřete je tak, že zvolený „virtuální disk" označíte a zvolíte příkaz »Disconnect«. Nyní jsou vaše data chráněná, i pokud svůj USB disk ztratíte.

PERMANENTNÍ SMAZÁNÍ: Hrozí-li nebezpečí, že se USB disk dostane do nepovolaných rukou, doporučujeme alternativní opatření. „Nálezce" totiž může poměrně snadno na disku obnovit i soubory, které jste vymazali. Tomu se nyní můžete bránit například pomocí programu Steganos Shredder, který dokáže data z příslušného média odstranit natrvalo...

AUTOR@CHIP.CZ



Neviditelný plášť: Tento nástroj vám nabídne nejen skrytí adresy...

Znepokojuje vás rostoucí množství spamu ve vaší e-mailové schránce? Představíme vám pomocníky, kteří umí **DOTĚRNÉ SPAMY** odpálkovat.

RADEK KUBEŠ

Pomocníci v nerovném boji

Podíl spamu na celosvětové e-mailové komunikaci se v současné době pohybuje mezi 70 a 80 procenty. Kromě spamu s nabídkami zboží (nejčastěji se jedná o léky, repliky značkových produktů, software, akcie atd.) vám prostřednictvím hromadně rozesílané, nevyžádané pošty hrozí také útoky virů a pokusy o odcizení vašich osobních údajů (phishing). Přestože existují zákony postihující odesílatele nevyžádané elektronické pošty, jsou na stále agresivnější spammery krátké. Jejich útokům je tedy třeba čelit jinými prostředky. Filtry nevyžádané pošty nasazují na své servery provozovatelé freemailů, nechybějí samozřejmě na firemních poštovních serverech a je možné jimi vybavit i váš počítač a používaného e-mailového klienta. Přestože e-mailoví klienti bývají často vybaveni vlastním filtrem nevyžádané pošty, vždy můžete udělat něco navíc – v tomto případě instalací specializovaného nástroje na odhalování spamu. Představíme si nejlepší filtry nevyžádané pošty pro běžně používané e-mailové klienty, které očistí vaši schránku od spamu zcela zdarma.

MailWasher: Kontrola před převzetím

Princip fungování antispamového programu MailWasher je velmi jednoduchý, a právě proto může tento program spolupracovat téměř s jakýmkoliv e-mailovým klientem a poštovním serverem. MailWasher zkontroluje poštu ještě před jejím stažením do počítače a pomůže vám s identifikací spamu. Teprve po vyčištění schránky na poštovním serveru si do svého e-mailového klienta stáhnete nové zprávy a nebudete si zanášet počítač spamem.

MailWasher startuje po instalaci průvodcem, který buď identifikuje e-mailové účty v Outlooku či jiném e-mailovém klientovi, nebo vám umožní nastavit parametry účtů ručně. Podstatou nastavení je, aby se MailWasher dostal k vaší poště ještě dříve, než si ji stáhne e-mailový klient. Podporován je POP3 i IMAP pro přístup k poště, stačí jen zadat adresu poštovního serveru (zjistíte v nastavení svého účtu na freemai-

NA DVD

Nevyžádaná pošta

MailWasher Free ► antispam

SPAMfighter ► antispam

Spamihilator CZ ► antispam

Spam Terrier ► antispam

Plná verze:
PC Internet Security 2009 ► ochrana počítače

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

lech typu Seznam, Gmail atp.) a přihlašovací jméno (nejčastěji e-mailová adresa a přístupové heslo). Po výběru nebo ručním nastavení účtu si ještě zvolíte instalovaného e-mailového klienta (z běžně používaných je podporován Outlook, Outlook Express a Windows Live Mail), se kterým bude MailWasher spolupracovat. Tím základní nastavení končí.

Další použití programu je velmi snadné, MailWasher jej navíc demonstruje pomocí krátké animace, přehrávané při spuštění programu. Tlačítkem »Check Mail« zkontrolujete novou poštu na serveru. MailWasher roztřídí poštu na spam, na bezpečné zprávy a na e-maily, u kterých nemůže jednoznačně rozhodnout. Kliknutím na ikon-

KNOW-HOW

Techniky boje se spamem

Filtry nevyžádané pošty pracují se dvěma základními technologiemi, založenými na způsobu přenosu spamu po síti a nebo jeho obsahu. Filtrování spamu podle způsobu přenosu je založeno na existenci tzv. blacklistů, greylistů a whitelistů. Blacklisty jsou seznamy e-mailových adres (nejčastěji falešných) a především IP adres, ze kterých bylo zaznamenáno rozesílání nevyžádané pošty. Zprávy ze serverů zařazených na některý z blacklistů jsou antispamovými filtry automaticky odmítány, případně je výskyt odesílatele na blacklistu používán jako jeden z indikátorů při posuzování zprávy spamovým filtrem. Protikladem blacklistů jsou tzv. whitelisty, což jsou pro změnu seznamy bezpečných adres, ze kterých bude pošta bez problému přijímána. V rámci uživatelských nastavení antispamových filtrů si můžete blacklisty i whitelisty doplňovat sami. Pokročilejší alternativou blacklistů jsou tzv. greylisty, které rozhodují na základě stejných vstupních informací (adresa odesílatele), ale přidávají ještě faktor času, konkrétně v podobě dočasného odmítnutí doručení podezřelé zprávy. Spammeři využívající roboty pro rychlé odesílání zpráv na obrovské množství adres se nedoručitelností zpráv zpravidla vůbec nezabývají a ani nezkoušejí nedoručené zprávy opakovaně odeslat. Na svůj útok totiž mají málo času, než je jejich adresa zařazena na některý z blacklistů. Seriózní poštovní servery se oproti tomu pokoušejí zprávu doručit opakovaně a jsou filtry po určité době (řádově desítky minut) odblokovány.

Samostatnou vědeckou disciplínu by mohly tvořit způsoby filtrování nevyžádané pošty podle obsahu. Posouzení obsahu zprávy je totiž velmi individuální záležitostí každého příjemce a nelze jej snadno zobecnit. Filtry založené na pravidlech vyhledávají typické znaky nevyžádané pošty. Může přitom jít o konkrétní slova a slovní spojení (např. viagra atd.), ale i o běžnému uživateli skryté vlastnosti, jako je chybně označený typ zprávy, nekorektní hlavička atd. Filtr přidělí každému indikátoru spamu bodové hodnocení a podle celkového výsledku a nastavené hranice citlivosti je zpráva předána dále, nebo naopak zablokována. Úskalím této metody je především nutnost neustálé aktualizace pravidel filtru v reakci na stále se měnící techniky spammerů. Z tohoto důvodu byly také vyvinuty tzv. bayesovské filtry (podle matematika Bayese), založené na učení se. Inteligentnímu filtru se v režimu učení předkládají zprávy označené jako spam a nespam a filtr si do vlastní databáze ukládá informace charakteristické pro oba druhy elektronické pošty. Filtr pak funguje na základě statistiky a pravděpodobnosti, že zpráva s určitými vlastnostmi je nebo není spam. Bayesovské filtry mohou učit samotní uživatelé ve svých e-mailových klientech (např. Mozilla Thunderbird), nebo mohou fungovat zcela automaticky na poštovních serverech a studovat všechny přicházející e-maily.

INFO

Proč se rozesílá spam?

Jistě vás napadne logická otázka, jaký cíl vlastně rozesílatelé spamu sledují, jaký užitek ze zahlcování schránek nevyžádanými zprávami mají. K pochopení smyslu rozesílání spamu s nabídkami na zakoupení léků, softwaru a jakéhokoliv dalšího zboží je třeba si uvědomit, že rozeslání e-mailu na miliony adres téměř nic nestojí. I při zcela zanedbatelné úspěšnosti lze říci, že každá kladná odpověď a pořízení nabízeného zboží jsou pro spammera ziskem. Přesto lze s úspěchem pochybovat o úspěšnosti tohoto obchodního modelu. U nás je známý případ hotelu U Lípy, propagujícího své služby prostřednictvím nevyžádané pošty. Provozovatel hotelu dostal nejdříve od Úřadu na ochranu osobních údajů pokutu ve výši čtvrt milionu korun za rozesílání spamu, a nyní je dokonce v insolvenčním řízení. Ani obrovské množství rozeslaného spamu asi nepřilákalo hotelu nové hosty.

Jinou kategorií jsou spamy slibující úžasné výhry, převody majetku a jiný prospěch za sdělení důležitých osobních údajů (číslo bankovního účtu, kreditní karty atd.). Zde se již točí zajímavé peníze za prodej údajů získaných od důvěřivých příjemců spamu a z vykradených bankovních účtů. Dalším „posláním" nevyžádané pošty je také šíření virů a dalšího škodlivého softwaru, který pak například sleduje aktivitu uživatele a vynáší z počítače citlivá data. V každém případě, neutuchající aktivita spammerů pohání celé odvětví věnující se vývoji technik pro filtrování nevyžádané pošty.

ky označující spam či bezpečnou poštu můžete klasifikaci změnit, MailWasher si přitom vaše rozhodnutí zapamatuje. Kliknutím na tlačítko »Process Mail« spustíte vyčištění pošty a pomocí tlačítka »Mail Program« spustíte svého e-mailového klienta, do kterého si poštu stáhnete a kde s ní můžete dále pracovat. Došlou poštu umí MailWasher samozřejmě kontrolovat i automaticky, podle zadaných intervalů a pravidel. Potřebná nastavení najdete pod tlačítkem »Settings«.

MailWasher používá několik způsobů identifikace a filtrování nevyžádané pošty. Jmenujme především použití blacklistů a whitelistů, filtrování na základě adresy příjemce, použité znakové sady textu, analýzu obsahu nebo učící se filtr, rozhodující na základě klasifikace e-mailů uživatelem. Možnosti nastavení filtrování pošty najdete v okně »Settings« pod nabídkou »Spam Tools«.

Vedle bezplatně použitelné verze Free existuje také placený MailWasher Pro, který umožňuje pracovat s více uživatelskými účty, zobrazuje náhled textu zprávy před jejím stažením z poštovního serveru a neobsahuje reklamní banner. Pro jeden e-mailový účet je ovšem plně použitelná i bezplatná verze.

SPAMfighter: Neohrožený bojovník

Již během instalace se vás bude SPAMfighter ptát na adresu a heslo k e-mailovému účtu, který chcete očistit od nevyžádané pošty. Následně je třeba vypnout všechny e-mailové klienty v počítači a dokončit instalaci. SPAMfighter přitom integruje své funkce přímo do e-mailového klienta – například Outlooku nebo Thunderbirdu. Po instalaci najdete jeho ovládací prvky v hlavním panelu nástrojů e-mailového klienta. Program komunikuje česky a je velmi snadné jej nastavit a používat. O osudu doručených zpráv rozhodujete pomocí tlačítek »Blokovat« a »Odblokovat«, přímo v prostředí Outlooku nebo jiného e-mailového klienta.

S filtrováním pošty vám pomůže především systém blacklistů a whitelistů a nastavitelná úroveň důkladnosti kontroly příchozích e-mailů. SPAMfighter se zároveň učí z vašich rozhodnutí a sdílí informace pro blokování nevyžádané pošty se všemi dalšími uživateli programu. Funkce SPAMfighteru se neomezují na jeden e-mailový účet, záleží jen na nastavení vašeho e-mailového klienta.

Bezplatná verze funguje v plném modu po dobu 30 dní, poté jsou některé funkce omezeny. Do blacklistu nebo whitelistu můžete například přidat jen 100 adres, přijdete o funkci filtrování pošty podle použitého jazyka zprávy, nemůžete odstranit informační patičku o používání SPAMfighteru z odesílaných e-mailů a musíte se také smířit se zobrazováním reklamy na placenou verzi programu. Bezplatnou verzi SPAMfighteru můžete používat pouze k soukromým účelům. Po zaplacení registrace komerční verze SPAMfighter Pro můžete dále bez omezení využívat všechny funkce antispamového programu – na domácím počítači i v práci.

Spam Terrier: Roztrhá spam na kusy

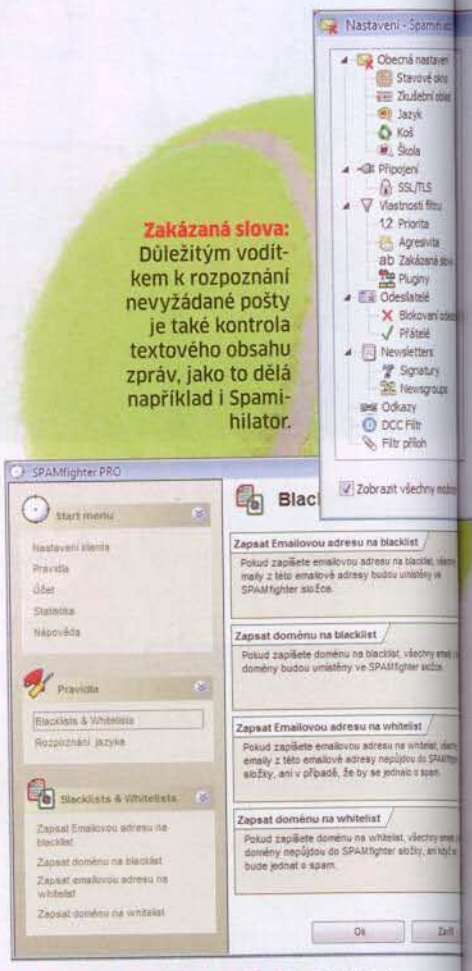
Také funkce antispamového filtru Spam Terrier se integrují přímo do poštovního klienta. Během instalace programu je třeba provést bezplatnou registraci a získat licenční klíč. Když dojdete v instalačním průvodci do okna »Free Registration«, ponechte označenou volbu »Get free license now« a do dvou volných řádků zadejte své jméno a e-mailovou adresu. Jakmile kliknete na tlačítko

Bojovník se spamem: SPAMfighter se integruje do prostředí Outlooku a podle nastavených pravidel identifikuje nevyžádanou poštu.

»Další«, bude vám v e-mailu odeslán potřebný registrační klíč, který použijete hned v následujícím okně průvodce. Pak už stačí jen dokončit instalaci a spustit e-mailového klienta. Podporován je Outlook v různých verzích, Windows Mail nebo The Bat!.

Po spuštění e-mailového klienta se na hlavním panelu funkcí objeví nové ovládací prvky – tlačítka »Mark as Spam« a »Mark as Not Spam« pro označení spamu a toho, co spamem není. Kromě automatické identifi-

Zakázaná slova: Důležitým vodítkem k rozpoznání nevyžádané pošty je také kontrola textového obsahu zpráv, jako to dělá například i Spamihilator.



SPAMfighter Blacklisty a whitelisty: Základním prostředkem pro boj s nevyžádanou poštou jsou seznamy povolených a zakázaných odesílatelů zpráv.

kace nevyžádané pošty je klíčovou funkcí programu schopnost naučit se rozpoznávat spam podle vašich preferencí. Průvodce učením spustíte kliknutím na nabídku »Train« v menu »Agnitum Spam Terrier«. V prvním kroku si můžete zvolit, zda budete rozšiřovat stávající znalostní bázi antispamového filtru, nebo zda si začnete tvořit úplně novou. Doporučujeme vám ponechat první volbu a prohlubovat znalosti programu. Dále si vyberte složku, ve které jsou uloženy nevyžádané zprávy, na kterých se má Spam Terrier učit. V Outlooku jde zpravidla o složku »Nevyžádaná pošta«. Následně označte jednu nebo více složek s poštou, kterou nepovažujete za spam. Spam Terrier prozkoumá zprávy ve vybraných složkách a zapamatuje si vlastnosti pošty podle vaší klasifikace na spam a „nespam". Proces učení je samozřejmě vhodné průběžně opakovat a rozšiřovat tak znalosti programu Spam Terrier pro rozpoznávání nevyžádané pošty.

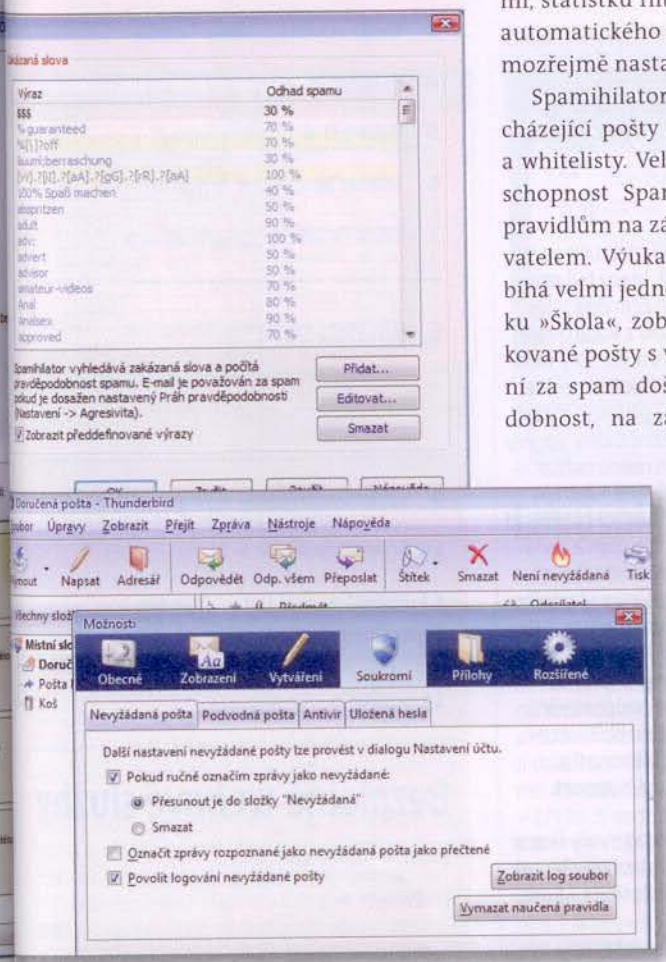
Spamihilator: Prohlídka na hranicích

Antispamový program Spamihilator sice také spolupracuje s e-mailovými klienty, ale přímo se do nich neintegruje. Výhodou takového přístupu je široká podpora různých e-mailových klientů. Spamihilator pracuje na pozadí operačního systému a o své činnosti dá vědět, pokaždé když e-mailový klient začne stahovat zprávy z poštovního serveru. Spamihilator během stahování zprávy zkontroluje a zablokuje spam.

Instalaci a použití Spamihilatoru zvládne i běžný uživatel. Během instalačního průvodce není třeba měnit žádná nastavení, stačí pouze vybrat používaného e-mailového klienta a označit e-mailové účty, jejichž zprávy bude Spamihilator kontrolovat. Spamihilator podporuje protokoly POP3 a IMAP, prostřednictvím kterých se stahuje pošta do vašeho počítače. Češtinu doinstalujete pomocí jazykového balíčku a uživatelské rozhraní se automaticky přepne při spuštění. Ikona aplikace se usídlí v oznamovací oblasti hlavního panelu Windows (vedle hodin). Po kliknutí pravým tlačítkem myši můžete vybrat zobrazení koše se zablokovanými zprávami, statistku filtrování pošty, funkci učení automatického rozpoznávání spamu a samozřejmě nastavení Spamihilatoru.

Spamihilator používá pro kontrolu přicházející pošty bayesovský filtr, blacklisty a whitelisty. Velmi důležitá je samozřejmě schopnost Spamihilatoru učit se dalším pravidlům na základě klasifikace pošty uživatelem. Výuka rozpoznávání spamu probíhá velmi jednoduše. Pokud zvolíte nabídku »Škola«, zobrazí se vám seznam zablokované pošty s vysvětlením, proč k označení za spam došlo (»Důvod«), a pravděpodobnost, na základě které Spamihilator rozhodl (»Probability«). Pomocí tlačítek »Spam« a »Ne-spam« můžete sami určit klasifikaci zprávy a pak kliknutím na tlačítko »Uč se!« ovlivnit budoucí chování filtru. Další nastavení Spamihilatoru nabízejí například určení priority použitých filtrů (filtr newsletterů, příloh, obrázků, odkazů, zakázaných slov atd.), úrovně ochrany (označeno jako »Agresivita«) a samozřejmě i seznamů blokovaných a povolených odesílatelů zpráv. Možností nastavení je opravdu mnoho, což dává uživatelům značné možnosti při experimentování s optimálním nastavením Spamihilatoru, tak aby propouštěl skutečně jen korektní zprávy a neblokoval jinou než nevyžádanou poštu. Popisky možností nastavení nejsou přeloženy do češtiny ve všech případech, nicméně pro bezproblémovou orientaci v nastavení antispamu bez problému vystačí i méně zkušeným uživatelům.

Velkou výhodou Spamihilatoru je podpora plug-inů, pomocí kterých můžete rozšířit funkce programu při odhalování stále nových druhů nevyžádané nebo nebezpečné pošty.



Bez další instalace: Open-source poštovní klient Thunderbird nabízí kromě kompletní nabídky funkcí pro příjem, odesílání, třídění a další zpracování pošty i inteligentní antispamový filtr.

Spam tvoří až 80 % e-mailů

Thunderbird: Antispam v základní výbavě

Zatímco Outlook zůstává i v době záplavy nevyžádané pošty nadmíru konzervativní a filtrování spamu se příliš nevěnuje, open-source e-mailový klient Thunderbird obsahuje bayesovský filtr nevyžádané pošty. Thunderbird automaticky posuzuje příchozí poštu a označuje nevyžádané zprávy. Pomocí tlačítka »Nevyžádané« můžete sami ovlivňovat klasifikaci zpráv a doplňovat tak znalosti Thunderbirdu pro filtrování další pošty. Další volby nastavení najdete pod nabídkou »Možnosti« v menu »Nástroje«, na záložce »Soukromí«. Vestavěná antispamová kontrola nicméně vůbec nebrání použití dalších filtrů nevyžádané pošty, které jsme představili.

Nejlepší filtr?: Pro každého něco

Bezplatně použitelné antispamové filtry z našeho přehledu nabízejí ideální příležitost k experimentování s nastavením kontroly nevyžádané pošty. Antispamovou aplikaci volte především podle počtu e-mailových účtů, jejichž zprávy potřebujete kontrolovat, používaného e-mailového klienta nebo třeba i dostupnosti české verze uživatelského rozhraní programu. Současné použití více filtrů nevyžádané pošty vám ovšem nedoporučujeme. Omezili byste tím především schopnost automatického prohlubování znalostí antispamu na rozpoznávání nevyžádané pošty podle klasifikace obsahu zpráv uživatelem.

RADEK.KUBES@CHIP.CZ

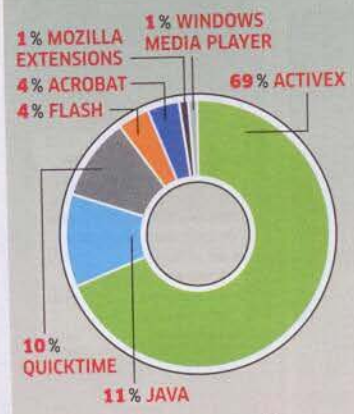
DATA A FAKTA

Barometr nebezpečí
v srpnu

Malwaru je méně

Nebezpečí trvá: I přes pokles je výskyt malwaru děsivě vysoký.

Útoky na browsery



Nebezpečí z webu: Hackeři nejraději využívají mezer v plug-inech Microsoftu.

Číslo měsíce

500

eur stojí přístupová data k „hacknutému" on-line účtu s vkladem přes 10 000 eur.

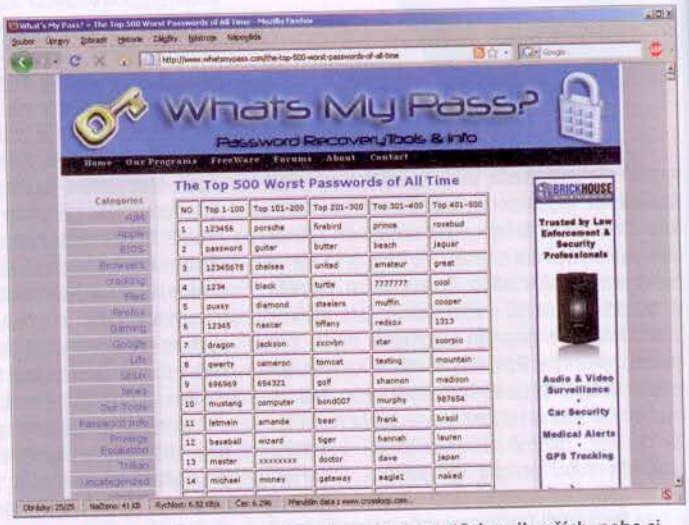
Nejhorší hesla všech dob

Chrání vás kvalitní firewall, máte nejnovější updaty operačního systému, používáte výborný antivir, a přesto byl váš počítač úspěšně napaden hackerem? Problém může být ve **ŠPATNĚ ZVOLENÉM HESLE**.

PETR KRATOCHVÍL

Útoky hackerů se vždy snaží zamířit na nejslabší článek řetězu – pokud má váš počítač kvalitní softwarovou výbavu, mohou se hackeři pokusit zaútočit na vaše přístupová hesla. Ačkoliv mezi nejčastější varování v článcích o počítačové bezpečnosti patří „zásada bezpečného hesla" (varující před používáním jednoduchých hesel), jen málokdo se jí drží. To pravidelně potvrzují průzkumy bezpečnostních firem i vlastní zkušenosti uživatelů.

První hesla, vytvářená ve snaze o maximální zabezpečení nového počítače, bývají komplikovaná a opravdu bezpečná. Po čase ale ostražitost klesá a s ní se snižuje i komplikovanost hesel. To je nebezpečné riskování. Metod, jak uhodnout vaše heslo, je celá řada a většinu uživatelů určitě napadne „slovníková metoda". Při ní hacker zkouší kombinace a variace slov ze slovníku daného jazyka – v ohrožení jsou tedy hesla typu „reflektor" nebo „laparoskopie". V praxi ale mají hackeři situaci ještě snadnější.



Tabule hanby: Najdete i vy své heslo v seznamu těch nejhorších, nebo si svých dat a soukromí vážíte více?

500 nejhloupějších hesel

Při vytváření knihy o heslech zjišťoval její autor Mark Burnett (na vzorku více než milionu uživatelů), jaká hesla uživatelé používají. Výsledky jeho výzkumu překonaly i ty nejhorší předpoklady: neuvěřitelné množství lidí používá stále se opakující primitivní hesla, která dokáže uhodnout i cvičená opice. K demonstraci lidské hlouposti sestavil Mark Burnett seznam 500 nejhloupějších hesel, která používá více než desetina uživatelů! Pojďme se podívat na některá z nich:

- 123456 – klasika, „náročnější" uživatelé pokračují až k devítce, líní končí na čtyřce či pětce;
- password – „heslo" jako heslo má být trik k ošálení hackerů, opak je bohužel pravda;
- 666666 – s alternativami v podobě sedmi sedmiček, pěti pětek, kreativitě se meze nekladou;
- zxcvbn – heslo „qwerty" se uživatelům nezdá bezpečné, tak to zkouší v dolní části klávesnice;
- qazwsx – pokročilejší kreace předchozí metody, ovšem se stejnou bezpečnostní úrovní;
- ncc1701 – oblíbené heslo „nerdů", skrývající označení kosmické lodi ze seriálu Star Trek;
- porsche – s alternativou v podobě značky vašeho vysněného vozu (ano, v seznamu je i ferrari).

S těmito znalostmi tedy může být práce hackerů snadná a efektivní – zkuste si sami odhadnout, kolik počítačů tvoří zmiňovanou desetinu se snadno „odhalitelnými" hesly. A jak jsou na tom vaše účty? Najdete i vy své heslo v seznamu 500 nejhloupějších hesel na adrese **www.whatsmypass.com/the-top-500-worst-passwords-of-all-time?**

LINUXOVÉ WEBSERVERY ÚTOČÍ

Nové triky malwaru

Ruský nezávislý bezpečnostní výzkumník a analytik Denis Sinegubko objevil skupinu infikovaných linuxových serverů, na kterých běží speciální druh botnetů. Ty poté rozesílají malware nic netušícím uživatelům surfujícím po webu. Takto postižené stroje sice na první pohled fungují zcela normálně a pracují na standardním TCP portu (80), vzápětí však využijí pro „tajný provoz" port 8080.

Sinegubko ve své zprávě uvádí, že už dva poskytovatelé dynamického hostingu, DynDNS.com a No-IP.com, jejichž služby útočníci využívali, stihli na danou situaci zareagovat, a to aktivním vypínáním domén, které jsou k těmto útokům zneužívány. Dále však dodává, že to určitě není naposledy, co se s tímto fenoménem setkáváme , když každou hodinu přibývají dvě nové IP adresy...

Detailnější informace o dané problematice najdete na stránkách serveru The Register **(www.theregister.co.uk/2009/09/12/linux_zombies_push_malware/)**. Tento nález také poukazuje na neustálý vývoj „záškodného" softwaru, jehož oběťmi se už mohou snadno stát i velikáni jako Twitter, nebo dokonce Google Groups.

INFO: zprávy.actinet.cz

VÝZKUM AVG

Zranitelnější uživatelé sociálních sítí

Společnost AVG Technologies uvolnila ve spolupráci s CMO výsledky ankety „Jak přinést bezpečnost na sociální sítě" (Bringing Social Security to the On-line Community). Z výzkumu vyplynulo, že uživatelé sociálních sítí mají sice obavy o bezpečnost při komunikaci, málokdo však podniká alespoň základní kroky k ochraně před on-line hrozbami. Jen necelá třetina respondentů se jim aktivně brání, téměř polovina se obává krádeží identity v on-line komunitách a také rostoucího množství phishingu, spamu i virových útoků.

Anketa na internetu shromážděla ve druhém čtvrtletí 2009 odpovědi náhodného vzorku více než 250 uživatelů. I přes masivní používání nejrůznějších sociálních sítí doma nebo v práci (86 %) nedodržuje většina uživatelů pravidelně ani následující základní bezpečnostní pravidla:

- změny hesel (64 procent zřídka nebo vůbec);
- úpravu nastavení soukromí (57 procent zřídka nebo vůbec);
- informování administrátora sociální sítě (90 procent zřídka nebo vůbec).

Respondenti zmiňovaného výzkumu definovali několik obvyklých praktik, které provádí navzdory zřejmým bezpečnostním rizikům při zapojení do sociálních sítí (tyto praktiky mohou nechráněné uživatele poškodit):

- 21 procent respondentů přijme nabídku na kontakt od členů sítě, které osobně nezná;
- 51 procent nechá známé či spolubydlící navštěvovat sociální sítě na svém osobním počítači;
- 64 procent respondentů kliká na odkazy od dalších členů sítě;
- 26 procent dotázaných sdílí prostřednictvím sociálních sítí soubory.

Výsledkem šíření odkazů, souborů a nevyžádaných kontaktů je, že se uživatelé sociálních sítí velmi často setkávají s nejrůznějšími hrozbami a narušením soukromí:

- téměř 20 procent již zažilo krádež identity;
- 47 procent se stalo obětí nákazy nějakým typem škodlivého kódu;
- 55 procent dotazovaných se setkalo s phishingovým útokem.

Ředitelka komunikace a vztahů s investory AVG Technologies Siobhan MacDermottová doufá, že se AVG podaří tento trend zvrátit na známých sítích, jako je Facebook nebo Twitter. „Naše kampaň Data Snatchers je virálním prostředkem, který by měl přimět uživatele přemýšlet o své osobní bezpečnosti. Poskytne jim také jednoduché nástroje, pomocí nichž mohou pro svou bezpečnost něco udělat, a zvláště pokud se pohybují v místech, kde se cítí zranitelní."

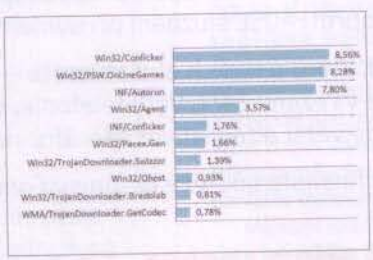
AVG Technologies také doporučuje šest jednoduchých kroků, které uživatelům pomohou zajistit bezpečí:

1. Nepotvrzujte pop-up okna či výzvy ke stažení softwaru, dokud váš počítač není vyzbrojen webovým štítem, jakým je například AVG LinkScanner **(http://free.avg.cz/linkscanner)**. Pomocí něj si zkontrolujte každou stránku ještě předtím, než na ni vstoupíte.
2. V sociální síti nikdy neuvádějte, neposílejte ani nepřikládejte žádná soukromá osobní data (například rodné číslo, údaje k bankovnímu účtu či zdravotní záznamy). Sociální sítě nevyžadují informace podobného typu k tomu, abyste se mohli stát jejich členem.
3. Měňte své heslo pravidelně, alespoň jednou za měsíc. Neměňte ho, když jste k tomu vyzváni. Mohlo by jít o trik třetí strany, která z vás chce heslo vylákat.
4. Nenechávejte své přátele, spolužáky, kolegy atd., aby navštěvovali sociální sítě z vašeho počítače, a ani vy je nenavštěvujte z cizího. Další osoby by svým neopatrným chováním mohly zanést do vašeho počítače infekci, případně by vaše přihlašovací údaje mohly být ohroženy prostřednictvím cookies, uložených na váš počítač.
5. Nikdy nevyužívejte automatického uložení vašich hesel a pravidelně mažte historii, alespoň jednou za týden.
6. Nikdy nepřijímejte nabídky na přátelství nebo o něj nežádejte osoby, které sami neznáte.

STATISTIKA FIRMY ESET

Počítačové hrozby: Conficker mírně na ústupu, roste podíl trojských koní

V celé východní Evropě Conficker konečně oslabuje. S podílem 8,56 % byl sice i v srpnu globálně nejrozšířenějším typem malwaru ze všech světově detekovaných hrozeb, ve srovnání s červencovými statistikami však zaznamenal pokles o více než dvě procenta. Silnější globální pozici naopak získala směs hrozeb sestávající převážně z trojanů útočících na hráče on-line her – Win32/PSW.OnLinegames (8,28 %). Nejrůznější trojské koně, které ke svému spuštění využívají funkci souboru autorun.inf, jsou stále rovněž v první trojici celosvětových hrozeb – v srpnu byla infiltrace INF/Autorun zaznamenána na 7,80 % počítačů. Varianty malwaru z rodiny Agent, schopné vykrádat informace z počítače, pak byly na čtvrtém místě, s výrazným odstupem za první trojicí a celkovým podílem 3,57 %. První pětku uzavírá INF/Conficker, který stejně jako INF/Autorun využívá autorun.inf v operačních systémech Windows k šíření infiltrace – konkrétně červa Conficker. Desítku celosvětově nejrozšířenějších počítačových hrozeb podle ESET ThreatSense.Net doplnily v srpnu škodlivé kódy Win32/TrojanDownloader.Swizzor (1,39 %) a Win32/TrojanDownloader.Bredolab (0,89 %). Cílem obou uvedených infiltrací je především stáhnout další malware a nainstalovat jej do infikovaného počítače.



Evropa a zbytek světa

Stejně jako v červenci i v srpnu byl Win32/TrojanDownloader. Bredolab top hrozbou v Česku (7,06 %) i na Slovensku (5,25 %). V červenci ovládal lokální statistiky hrozeb s podílem 6,48 %. Tento malware se sám umisťuje do běžících procesů v počítači a snaží se vypnout bezpečnostní programy (uživatel o něm nemusí vůbec vědět). Je schopen se sám kopírovat do systémových souborů a spouštět se při každém zapnutí počítače. Zároveň komunikuje se vzdáleným serverem prostřednictvím HTTP. Pokud je tedy tento trojský kůň v systému, jeho hlavní úlohou je stahovat do infikovaného počítače další škodlivé kódy. Varianty červa Conficker jsou nejrozšířenější především na Ukrajině a v Rusku, ale i na jihu Afriky a ve Velké Británii.

Polsko je typické dominancí trojanů útočících na on-line hry Win32/PSW.OnLineGames. Ty mají stále vysoký podíl (13,59 %) mezi všemi hrozbami. I ve Francii (10,07 %), Turecku (13,7 %) a Spojených arabských emirátech (7,61 %) jsou uživatelé nejčastěji ohroženi trojskými koňmi souvisejícími s on-line hrami. Win32/Agent je nejrozšířenější počítačovou hrozbou v Dánsku (3,78 %) a Švédsku (3,49 %), přičemž v severských zemích je proti jiným evropským zemím zvláště vysoký podíl specifického červa Koobface, útočícího na uživatele sociálních sítí typu Facebook či MySpace. Koobface je v Dánsku s podílem 2,59 % dokonce v první trojce, na Islandu je s 1,94 % v první pětce a první desítku okupuje i v Norsku a Švédsku.

2009: Rok supervirů

Conficker patří minulosti – pro útoky na váš počítač nyní hackeři připravují nové, mnohem nebezpečnější zbraně. Prozradíme vám, co mají v záloze, a poradíme, **JAK SE PROTI TOMU BRÁNIT**.

CLAUDIO MILLER, PETR KRATOCHVÍL

Nový malware funguje jako víceúčelové zbraně.

Na počátku tohoto roku vystrašil celou řadu uživatelů vir Conficker. Tato hrozba, šířící se prostřednictvím staré mezery ve Windows (Microsoft nabízí záplatu už téměř rok) jako lesní požár, napadla miliony uživatelů po celém světě. Již během řádění Confickeru se po internetu začal nenápadně šířit nový vir – Gumblar. Ten je podle bezpečnostních expertů mnohem nebezpečnější než Conflicker: od března do června dokázal napadnout více než sto tisíc britských webů, včetně známých „lifestyle" portálů (například **www.variety.com**).

Gumblar je extrémně nebezpečnou ukázkou nové zbraně počítačových zločinců. Trend je zřejmý: malware útočí tak, aby nepoškodil nebo nesmazal data uživatelů, a zároveň pátrá po citlivých a zpeněžitelných informacích. V hledáčku má čísla kreditních karet, přístupové údaje na weby a osobní informace. Zároveň hackeři neustále vylepšují techniky šíření virů a jejich ukrývání v počítači. Nový malware (jako například Gumblar) a jeho metody útoku naznačují ještě jeden trend: ještě nikdy nebylo surfování po internetu tak nebezpečné jako letos. My jsme pro vás na DVD připravili nástroje, které toto riziko sníží a které vám v případě napadení pomohou s obranou.

Gumblar: Dynamický kód viru

Tím, co dělá vir jménem Gumblar tak nebezpečným, je rafinovaný způsob budování svého „hnízda" na napadených stránkách: nikdy nepoužívá stejný kód znovu a mění „scénář" u každého napadeného webu. Tento dynamicky generovaný kód ztěžuje internetovým firmám detekci jednotlivých útoků.

Když uživatel navštíví napadený web, Gumblar zaútočí na prohlížeč a pomocí mezery ve flash/pdf plug-inu se pokusí proniknout do počítače. V případě úspěchu zaznamená historii surfování uživatele a na disku pátrá po přihlašovacích údajích a heslech. V Internet Exploreru navíc manipuluje s výsledky vyhledávání pomocí Googlu. Pokud uživatel klikne na některý z těchto „vyhledaných" odkazů, je přesměrován na jeden z dalších napadených webů s další dávkou malwaru. Jako „bonus" pak Gumblar vytváří zadní vrátka, prostřednictvím kterých mohou hackeři počítač připojit do sítě botů a zneužívat například k rozesílání spamu.

Obrana před Gumblarem není prozatím nijak extrémně obtížná – jeho útoku dokáže zabránit většina kvalitních bezpečnostních balíků. Podstatně nepříjemnější je jeho odstranění z infikovaného počítače. V době vzniku tohoto článku byla známa pouze jediná, radikální metoda – naformátování disku a reinstalace Windows.

Plug-iny v browserech: Brány do počítače

Rozšíření a plug-iny se dnes využívají na většině webů – přehrávají filmy a hudbu, nabízejí animace, zobrazují dokumenty, a dokonce i spouští aplikace. Jejich deaktivace je tak pro většinu uživatelů téměř nemožná. Zdá se tedy, že jedinou cestou je mít všechny tyto „doplňky" v nejnovějších verzích...

K podobné situaci již v minulosti došlo – před několika lety byly nejčastějším cílem hackerů ActiveX komponenty, které podporoval tehdy jednoznačně dominantní Internet Explorer. V operačních systémech před Windows Vista nabízí ActiveX rozsáhlá přístupová práva k systému, a tak hackerům usnadňuje čtení dat, nebo dokonce samotné ovládnutí systému. Kvůli vylepšenému řízení uživatelských práv ve Vistě a rostoucí popularitě alternativních prohlížečů (například Firefoxu a Google Chrome) si hackeři začali všímat i těchto aplikací. Po určité době však kyberzločinci zjistili, že nejsnáze zneužitelnou slabinou budou doplňky rozšiřující schopnosti prohlížečů. Právě proto dnes malware do počítačů proniká pomocí komponent pro Javu, QuickTime, PDF rozšíření a Flash plug-inů.

FTP server: Nové metody šíření

Aby hackeři zajistili co nejlepší šíření malwaru mezi uživatele, obvykle používají jako „základny" známé a často navštěvované weby. Tyto weby ale mívají poměrně kvalitní ochranu, která rychle zasáhne a ukončí šíření malwaru. Tvůrci Gumblaru našli jinou cestu, jak škůdce rychle rozšířit mezi maximální počet uživatelů. Pokud je vir umístěn na počítači obsahujícím přístupová data na FTP server, infikuje škůdce všechny webové stránky připojující se k serveru. V hledáčku škůdců jsou především stránky nabízející velké objemy dat – například stránky výzkumných ústavů nebo „stahovacích" portálů, které často na FTP serverech ukládají data.

Triky s FTP však používají i jiní hackeři. V červnu tohoto roku hackeři infikovali pomocí ukradených přístupových údajů k FTP serverům více než 40 tisíc stránek. Pokud uživatel otevře jednu z těchto stránek a spustí se škodlivý „javascript", je uživatel automaticky přesměrován na falešné stránky Google Analytics. Tam už proběhne známý proces: prostřednictví mezer v prohlížeči a jeho doplňcích je do počítače nahrán příslušný malware...

NA DVD

AVG 8.5 CHIP EDITION

Plná verze

Na Chip DVD najdete i plnou verze bezpečnostního balíku od AVG, která nabízí komplexní zabezpečení počítače před škodlivým softwarem a útoky z internetu. Více informací o programu a zabezpečení počítače najdete na Chip DVD.

INFO

Pět nejaktivnějších virových hrozeb

1. STUH

Trojský kůň z rodiny Stuh nahrává stisky klávesnice a pátrá po heslech. Zároveň vypíná systém automatického nahrávání oprav (Windows Update), čímž připravuje cestu pro pozdější útoky.

2. FRAUDLOAD

Tento typ virů je také označován jako falešné antiviry (Rogue AV). Pomocí bezpečnostních mezer proniknou tyto viry do počítače, začnou uživatele zahlcovat hlášeními o nalezených virech a snaží se ho donutit ke koupi „bezpečnostního produktu", během které zneužijí informace o použité kreditní kartě.

3. MONDER

Také Monder patří do rodiny „falešných antivirů". Navíc ale „upravuje" bezpečnostní nastavení operačního systému a do počítače nahrává další malware.

4. AUTORUN

Tato virová hrozba se vždy šíří stejným způsobem: škůdce při vložení/připojení externích datových nosičů zneužije funkci autostart a spustí exe soubor s malwarem.

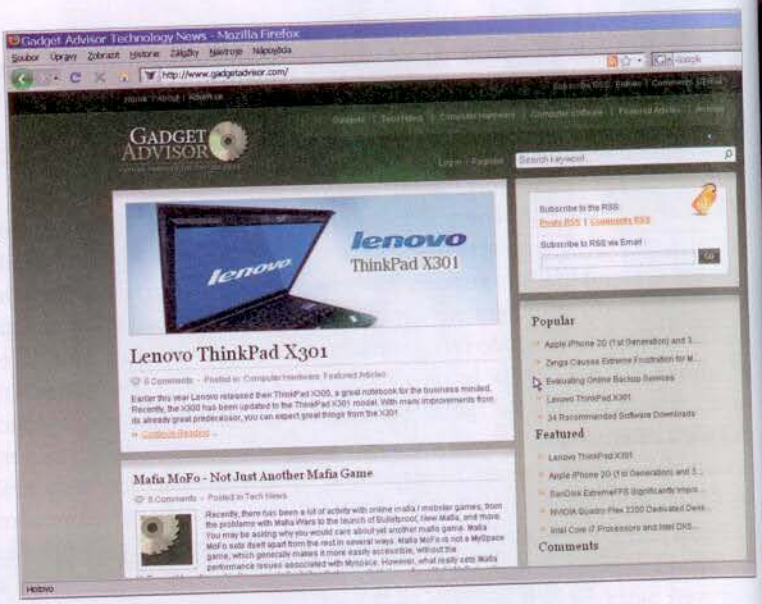
5. BUZUS

Škůdce jménem Buzus patří mezi klasický spyware. Prohledává napadený počítač a pátrá po číslech kreditních karet a přístupových datech k bankovním účtům. Nepohrdne ani přístupovými údaji k e-mailovým kontům a FTP serverům.

ZDROJ: G DATA

V minulosti platilo pravidlo, že pokud nesurfujete po pornografických a nebezpečných stránkách, útoků virů se bát nemusíte. Dnes ale moderní malware nestaví svá „hnízda" jen na pochybných stránkách. Odhaduje se, že v současnosti se 85 procent malwaru šíří přes populární a na první pohled bezpečné weby. Typickou ukázkou je napadení známého amerického „tech-

nologického" webu „Gadget Advisor", který se ve spárech internetové mafie ocitl letos v květnu. Tato taktika přináší hackerům celou řadu výhod: těmto populárním webům uživatelé obvykle důvěřují a stahují z nich cokoliv bez větších obav. U webu Gadget Advisor byla použita zranitelnost při zpracování PDF **(www.f-secure.com/vulnerabilities/SA29773)** a pomocí škodlivého kódu v „iframe" se do počítače dostal malware (Trojan-Downloader.Win32.Agent.brxr), který nakazil obrovské množství počítačů...



V utajení: Malware na vás může zaútočit i ze zdánlivě bezpečného webu. Útokům hackerů neodolal ani populární portál Gadget Advisor.

BlackHat-SEO: Zneužití Googlu

K přilákání co největšího počtu uživatelů však počítačoví zločinci používají i další triky. Pomocí analytických nástrojů Googlu najdou nejvíce vyhledávané pojmy a vytvoří weby, které budou přesně odpovídat těmto pojmům. Ty také dokáží prosadit do čela vyhledaných výsledků. Tato forma optimalizace pro vyhledávače (Search optimization – SEO) je také označována jako Blackhat SEO a funguje následujícím způsobem: hackeři zvolí nejpopulárnější pojmy, jako například „YouTube" nebo „TV on-line", případně aktuální témata (zřícení letadla AirFrance, herní veletrh E3). Na takové téma pak vytvoří speciálně upravené stránky, které umístí na servery freewebhostingových firem. Tyto stránky ale nejsou zavirované – pouze obsahují skript, který vás přesměruje na jiné weby, které se pokusí na počítač oběti nainstalovat malware. Pokud nemáte kvalitní softwarovou ochranu, během chvíle se váš počítač hemží malwarem...

Sociální sítě: Cíl hackerů

Kromě odkazů „vyhledaných" Googlem existuje celá řada jiných metod využívaných hackery k lákání uživatelů na nakažené weby. Oblíbeným trikem je šíření odkazů ve velkých sociálních sítích – například ve Facebooku, který má přibližně 200 milionů registrovaných uživatelů. Hackeři používají specializované nástroje, kterými automaticky zakládají uživatelské profily. Tyto nástroje také dokáží detekovat a překonat ochrany typu „captcha". Falešné profily jsou poté použity k odesílání zpráv ostatním uživatelům. Tyto zprávy obsahují odkazy na weby, ze kterých uživatelé mohou „získat" malware, aniž by na cokoliv klikli. Stejný trik používají hackeři pro microblogovací službu Twitter.

I zde jsou pro šíření odkazů na infikované stránky vytvářeny falešné profily. S cílem odlišit se od běžných zpráv (Tweets) zde ale hackeři využívají aktuální nejpopulárnější výrazy (Hashtags).

Vzhledem k limitu 140 znaků na jednu zprávu musí hackeři často zkracovat a „šifrovat" dlouhé odkazy pomocí služeb, jako je například TinyURL – tak skrývají odkazy na zavirované weby. Ukázkou této zákeřné metody v praxi byla série útoků z konce května letošního roku, kdy Twitter zavalila lavina zpráv s odkazy na weby s videem. Po jejich navštívení byli uživatelé vyzváni k nainstalování „videokodeku" pro korektní zobrazení filmů. Místo kodeku se ale na disk uživatele stáhl PrivacyCenter, známý falešný antivirový nástroj (označovaný jako Rouge AV). Po nainstalování začal program předstírat kontrolu systému a varovat před „nalezenými" viry.

Po neúspěšném „pokusu" o odstranění virů přesměroval nástroj PrivacyCenter vyděšeného uživatele na WWW stránku, kde si mohl zakoupit „plnou verzi" bezpečnostního nástroje, která si s viry určitě poradí. Co se dělo s účtem, ke kterému neznalý uživatel při nákupu fiktivního bezpečnostního nástroje prozradil informace o kreditní kartě, si jistě dokáže čtenář Chipu představit...

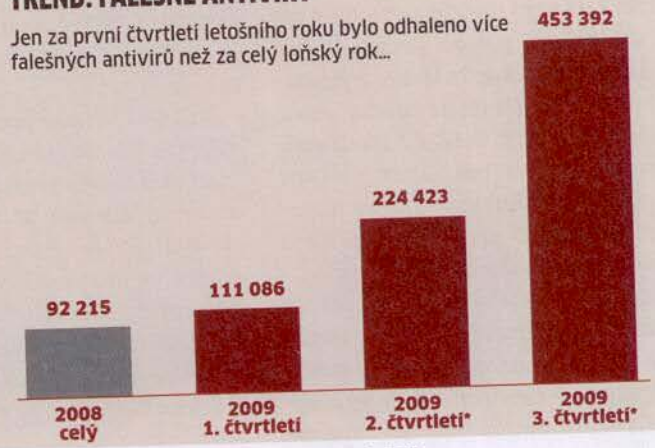
Uživatelé Facebooku se také mohli setkat s několika nepříjemnými viry v neuvěřitelném počtu variací. Například červ Boface, který se objevil na počátku roku 2008, zaútočil na uživatele hned v 56 různých variantách. Zajímavé je, že tento škůdce je nebezpečný pouze pro uživatele Facebooku – na počítači se stává aktivním teprve poté, co se

POČET NOVĚ DETEKOVANÉHO MALWARU

Od té doby, co se viry dokáží samy modifikovat, počet jejich variant rapidně stoupá.

TREND: FALEŠNÉ ANTIVIRY

Jen za první čtvrtletí letošního roku bylo odhaleno více falešných antivirů než za celý loňský rok...



Hnízdo virů: Hackeři stále častěji využívají pro distribuci svých „nástrojů" také služby pro úschovu souborů.

přihlásíte ke svému účtu na této komunitní síti. Pak začne všem kontaktům uživatele rozesílat krátké e-maily obsahující odkaz na „zajímavé videostránky". Tyto stránky také obsahují vir Boface a jako bonus přidávají „falešný antivir". Ten je na napadený počítač nainstalován a okamžitě začne bombardovat uživatele falešnými virovými varováními. Opět je cílem získat údaje o kreditní kartě, a to poté, co se uživatel rozhodne zakoupit „plnou verzi" bezpečnostního nástroje. Odhaduje se, že škůdce s označením Boface napadl již téměř dva miliony uživatelů, a jejich počet se neustále zvyšuje.

PDF: Vnímavý Office formát

Za největší hrozbu současnosti považují experti falešné antivirové programy, které mají za cíl zjistit informace o vašem kontu a číslech kreditních karet, případně „zkontrolovat" váš počítač na přítomnost citlivých dat. Odhaduje se, že počet „falešných AV programů" za čtvrtletí se ještě v tomto roce zdvojnásobí (viz graf dole). Dalším nepříjemným trendem je nárůst útoků za použití zmanipulovaných PDF souborů. Až doposud byly považovány za nejoblíbenější cíl hackerů formáty kancelářských programů od Microsoftu. V současnosti je však překvapivě polovina všech napadených dokumentů ve formátu PDF.

V tomto trendu hrají roli tři důležité faktory. Především hackeři často identifikovali bezpečnostní mezery v programech Adobe (například Acrobat a Reader), které jim umožňovaly převzít kontrolu nad systémem a infiltrovat do počítače další malware. Pro ilustraci stačí uvést odkaz na statistiku serveru Secunia pro produkty Adobe Acrobat 8.x a 9.x – se 40 a 22 zranitelnostmi **(http://secunia.com/advisories/product/12256/)**.

Druhým faktorem je skutečnost, že dokumenty ve formátu PDF mohou být zmanipulovány relativně snadno, např. implementací zákeřného JavaScriptu.

Posledním faktorem je podceňování tohoto problému uživateli – mnoho uživatelů nemá o těchto hrozbách ani tušení, a tudíž si ani bezpečnostní aktualizace těchto programů nestahují.

Základním krokem k bezpečnějšímu surfování tedy může být i pravidelná aktualizace produktů pro zobrazení souborů PDF a zakázání JavaScriptu. Například v Adobe Readeru/Acrobatu toho dosáhnete pomocí odstranění zatržítka v nabídce »Úpravy | Předvolby | Všeobecné | JavaScript«.

Sdílení souborů: Obvyklý zdroj virů

Infikované PDF soubory se šíří dvěma cestami: přes webové stránky, které přímo nahrají PDF do okna prohlížeče, případně přes přílohy e-mailů. Protože PDF je jedním z obvyklých formátů pro dokumenty na webu a má (stále ještě) dobrou pověst, nevěří těmto souborům pouze zlomek uživatelů, a jen málokdo tedy očekává v přílohách ve formátu PDF zákeřný malware.

Jiné formáty souborů, které slouží jako nositelé virů, preferují cestu šíření pomocí služeb sdílení souborů a služeb pro „úschovu" souborů (typickým příkladem je služba Rapidshare). Podle Symantecu byly v roce 2008 rozšířeny pomocí „sdílení souborů" přibližně dvě třetiny virem infikovaných EXE souborů. Již zmiňované „úschovny" jako RapidShare nebo MediaFire jsou také stále častěji cílem útoků kyberzločinců. Stále oblíbenější taktikou je rozšíření odkazů na stažení souborů pomocí diskusních fór a sociálních sítí. Do karet hackerům hraje i fakt, že většina podobných serverů není na „černém seznamu" nebezpečných stránek, a nezanedbatelnou výhodou je i naprostá anonymita...

Všechny tyto nové metody mají jedno společné – jsou mnohem efektivnější než šíření nebezpečných linků přes spamové e-maily. Ve chvíli, kdy tempo růstu spamu a phishingových mailů v elektronických schránkách klesá, měli by se uživatelé připravit na nové taktiky kyberzločinců. Jejich útoky totiž budou stále efektivnější a nebezpečnější... AUTOR@CHIP.CZ

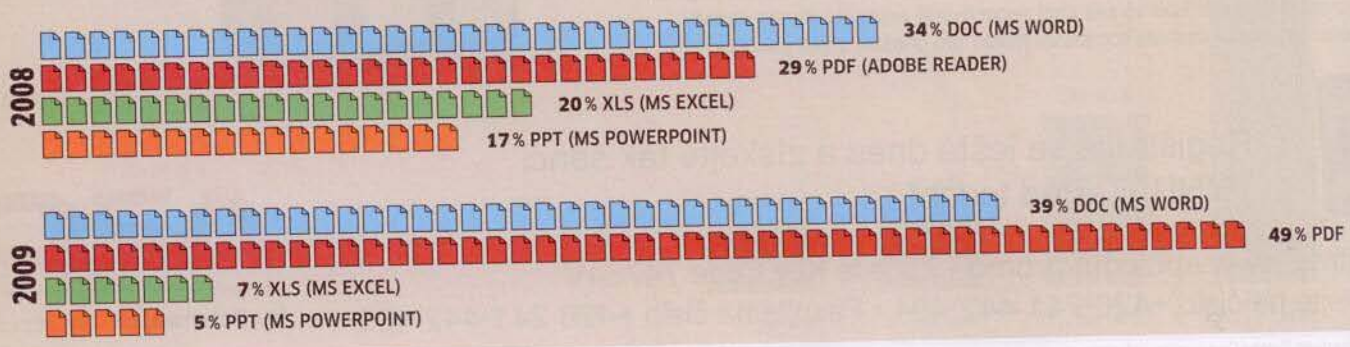
INFO

Útoky pomocí USB disků

Zpátky ke kořenům – to je nejnovější heslo hackerů při šíření malwaru. V dobách před masovým rozvojem internetu byly hlavním médiem pro šíření virů diskety. V současnosti se tato taktika znovu začíná využívat, a to na základě obrovského nárůstu popularity přenosných datových médií – USB flash disků nebo datových karet (např. SD). Tímto způsobem se vir šíří od počítače k počítači. Ochrana je však relativně snadná: kvalitní antivirový nástroj, nebo alespoň deaktivace funkce autostart...

ÚTOKY NA KANCELÁŘSKÉ DOKUMENTY

V roce 2008 se hackeři zaměřili na formáty Microsoftu a šířili viry pomocí typů souborů z kancelářského balíku MS Office. Letos trend ukazuje větší počet upravených PDF souborů...



ZDROJ: F-SECURE

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**.

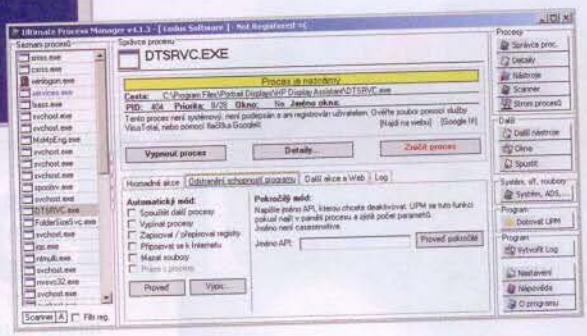
Ultimate Process Manager

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.

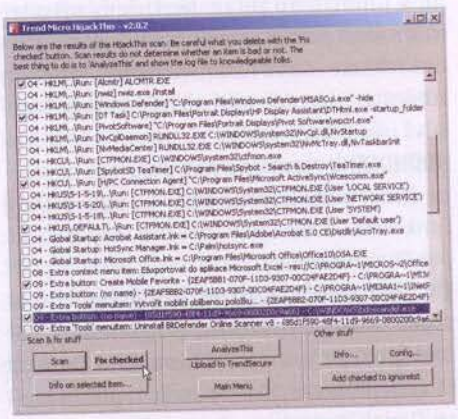
ukázková videa. Poradí vám, jak odrovnat i ty nejnebezpečnější škůdce.

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 jednoduššího 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 JISTÍ?

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...