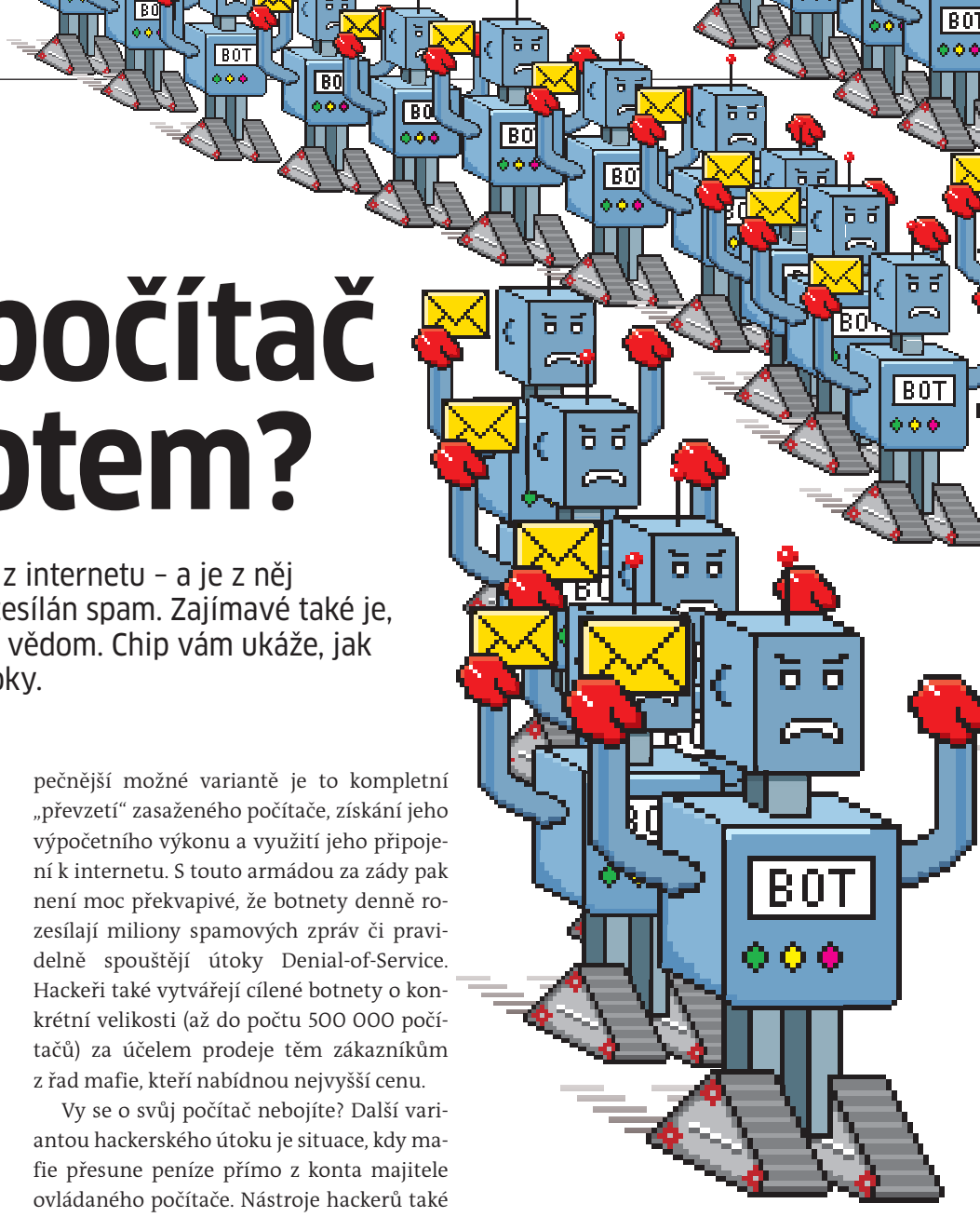


Je váš počítač spambotem?

Každý čtvrtý počítač je ovládán z internetu – a je z něj v zastoupení **WEBOVÉ MAFIE** rozesílán spam. Zajímavé také je, že si uživatel nemusí být ničeho vědom. Chip vám ukáže, jak můžete své PC ochránit před útoky.

FABIAN VON KEUDELL

Podobá se to poněkud nepříjemnému sci-fi filmu: vnější síly přebírají kontrolu nad počítačem a změní ho na svůj poslušný nástroj. Počítač se tak stane dálkově ovládaným robotem, sloužícím internetové mafii. Podle statistických údajů bezpečnostní firmy Symantec nejde pouze o několik počítačů. Denně je po celém světě „infikováno“ a přeměněno na roboty mafie přibližně 50 000 počítačů. Víte, že váš domácí počítač může být nakažen už při pouhé návštěvě zmanipulované webové stránky?

Podle internetového průkopníka Vintona Cerfa je v současnosti již každý čtvrtý počítač součástí sítě botů. To znamená, že součástí internetové armády mafie je nyní už přibližně 150 milionů počítačů na celém světě. A důsledky pro uživatele? V nejbezpečnější možné variantě je to kompletní „převzetí“ zasaženého počítače, získání jeho výpočetního výkonu a využití jeho připojení k internetu. S touto armádou za zády pak není moc překvapivé, že botnety denně rozesílají miliony spamových zpráv či pravidelně spouštějí útoky Denial-of-Service. Hackeři také vytvářejí cílené botnety o konkrétní velikosti (až do počtu 500 000 počítačů) za účelem prodeje těm zákazníkům z řad mafie, kteří nabídnou nejvyšší cenu.

Vy se o svůj počítač nebojíte? Další variantou hackerského útoku je situace, kdy mafie přesune peníze přímo z konta majitele ovládaného počítače. Nástroje hackerů také obvykle umožňují přímý přístup k tajným datům uživatele PC. Dokáží zaznamenat libovolnou „akci“ a svým zločineckým pánům tak například zasílat přístupové údaje k účtům. „Většina obětí si dokonce ani není vědoma toho, že byl jejich počítač napaden a že byla jejich osobní data ukradena,“ říká James Finch, ředitel počítačové divize FBI. „Útočník získává kontrolu nad počítačem, ale počítač funguje stále tak, jak fungoval původně.“ V roce 2008 američtí vědci pokusně infiltrovali síť „Storm“, která zasáhla asi 200 000 počítačů. Zjistili, že za tento rok pouze „přes spam“ rozeslaný z této sítě vydělala mafie asi dva miliony amerických dolarů. Je načase s tím něco udělat! I váš počítač se totiž může stát otrokem v armádě robotů mafie...

Základní ochrana: Plná verze bezpečnostního balíčku a aktualizace

Zapomeňte na svůj freewarový virový skener! Abyste svůj počítač ochránili před boty, potřebujete plnou verzi bezpečnostního nástroje. Nemusíte si ho však kupovat – na našem DVD jsme pro vás připravili speciální verzi bezpečnostního balíčku AVG, který ochrání váš počítač i před internetovou mafií.

Pokud na AVG Internet Security přecházíte z jiného (například freewarového) virového skeneru či bezpečnostního balíčku, doporučujeme nejdříve odinstalovat starý program a teprve poté začít s novou instalací. Na Chip DVD zvolte »Instalace AVG Security Chip Edition 8.5« a v průvodci klikněte na »Další«. Můžete použít všechna ostatní standardní nastavení (volba Standardní instalace). Od té chvíle už vás bude ikona AVG Internet Security v systémové liště Windows upozorňovat, že nástroj chrání váš počítač. Po dvojitém kliknutí na ikonu se také otevře hlavní okno programu.

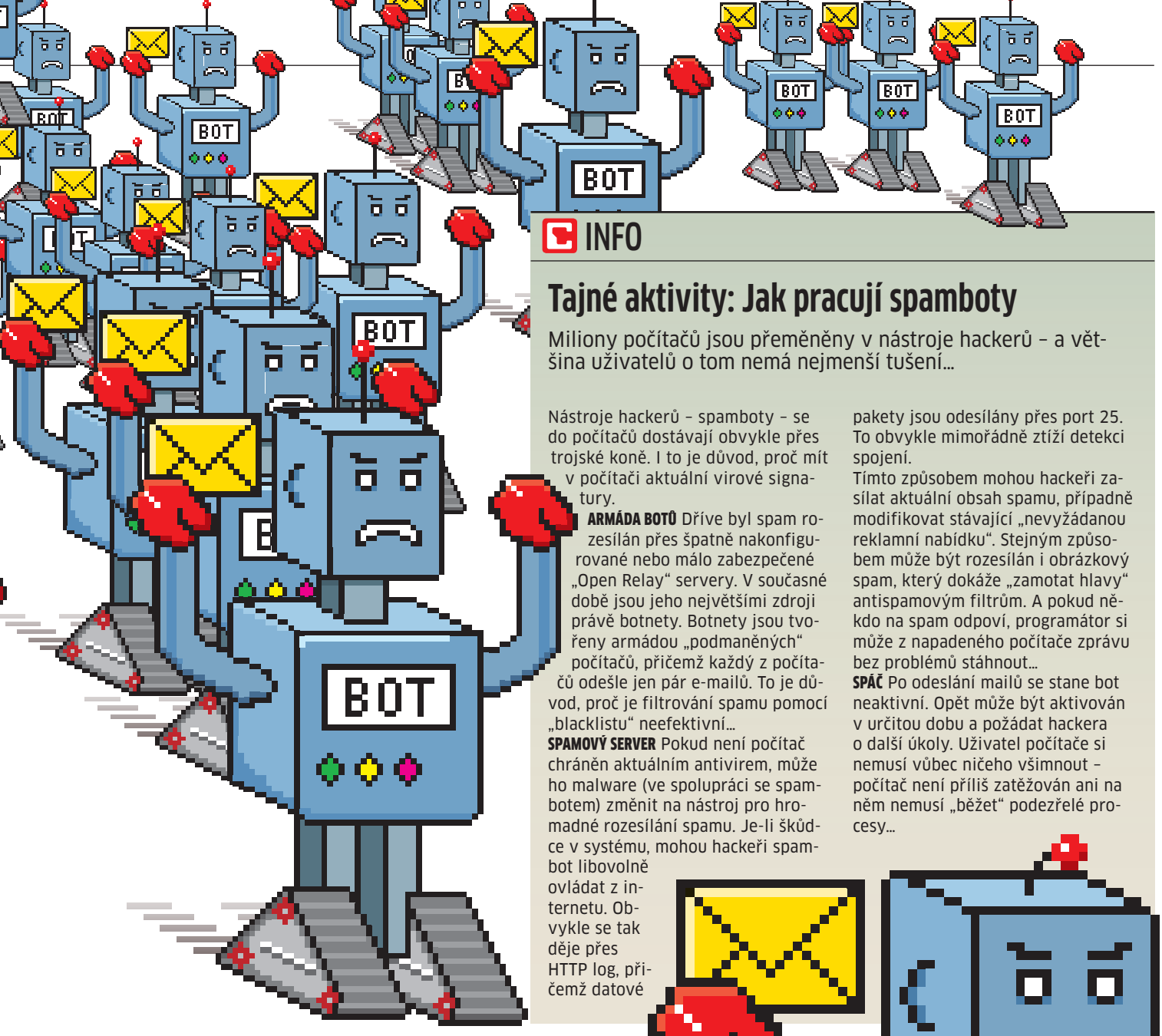
V levé části okna poté klikněte na tlačítko »Aktualizovat«, které odstartuje aktualizační proces. Nastavení pravidelné kontroly „updatu“ programu najdete v nabídce »Komponenty | Manažer aktualizací«. Zde můžete nastavit, kdy nebo v jakých intervaILUSTRACE: HARALD FUCHSLOCH

NA CHIP DVD

Nejlepší bezpečnostní nástroje

F-Secure Internet Security 2009 ► bezpečnostní balík
a-squared Anti-malware 4.0.0.79 ► nástroj proti malwaru
Spamihilator 0.9.9.44 ► antispamový pomocník
NoScript 1.9.2.6 ► rozšíření Firefoxu
Spybot Search & Destroy ► ochrana pro Windows
Snort 2.8 ► nástroj na síťovou analýzu
Gmer 1.0.15 ► antirootkit
HijackThis 2.0.2 ► detekční utilita

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



INFO

Tajné aktivity: Jak pracují spamboty

Miliony počítačů jsou přeměněny v nástroje hackerů – a většina uživatelů o tom nemá nejmenší tušení…

Nástroje hackerů – spamboty – se do počítačů dostávají obvykle přes trojské koně. I to je důvod, proč mít v počítači aktuální virové signatury.

ARMÁDA BOTŮ Dříve byl spam rozesílán přes špatně nakonfigurované nebo málo zabezpečené „Open Relay" servery. V současné době jsou jeho největšími zdroji právě botnety. Botnety jsou tvořeny armádou „podmaněných" počítačů, přičemž každý z počítačů odešle jen pár e-mailů. To je důvod, proč je filtrování spamu pomocí „blacklistu" neefektivní…

SPAMOVÝ SERVER Pokud není počítač chráněn aktuálním antivirem, může ho malware (ve spolupráci se spambotem) změnit na nástroj pro hromadné rozesílání spamu. Je-li škůdce v systému, mohou hackeři spambot libovolně ovládat z internetu. Obvykle se tak děje přes HTTP log, přičemž datové pakety jsou odesílány přes port 25. To obvykle mimořádně ztíží detekci spojení.

Tímto způsobem mohou hackeři zasílat aktuální obsah spamu, případně modifikovat stávající „nevyžádanou reklamní nabídku". Stejným způsobem může být rozesílán i obrázkový spam, který dokáže „zamotat hlavy" antispamovým filtrům. A pokud někdo na spam odpoví, programátor si může z napadeného počítače zprávu bez problémů stáhnout…

SPÁČ Po odeslání mailů se stane bot neaktivní. Opět může být aktivován v určitou dobu a požádat hackera o další úkoly. Uživatel počítače si nemusí vůbec ničeho všimnout – počítač není příliš zatěžován ani na něm nemusí „běžet" podezřelé procesy…

lech bude probíhat kontrola aktualizací. Podle vytížení počítače zde doporučujeme nastavit volbu „Pravidelně" a interval v rozmezí 4–6 hodin. Po kompletní aktualizaci ještě proveďte test celého počítače.

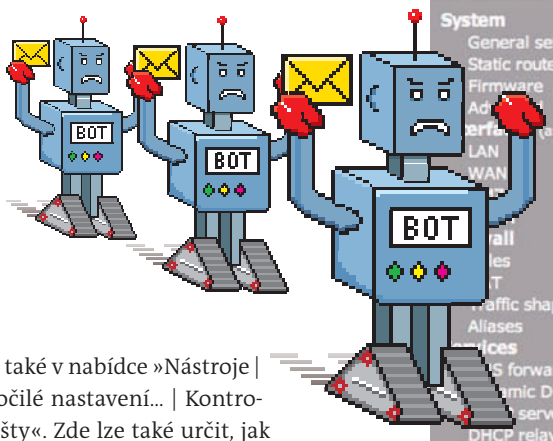
Pokud váš počítač není na instalaci komplexního bezpečnostního balíku připraven (například používáte-li více různých bezpečnostních nástrojů), rozhodně instalaci neriskujte – mohlo by dojít ke konfliktům driveru a zhroucení celého systému. Lepší variantou je použití on-line virového skeneru (například **http://support.f-secure.com/enu/home/ols.shtml** nebo **www.eset.cz/eos/eset-online-scanner**), který zkontroluje váš počítač zcela zdarma „přímo z internetu" (test on-line skenerů najdete v minulém Chipu).

Pro efektivní ochranu počítače by také měla být Windows vždy aktualizovaná – což platí i pro antivirový systém a ostatní nainstalované programy. Nejprve byste ale měli zabezpečit systém: v XP stiskněte klávesu [Windows]+[Pause], přejděte na záložku »Automatické aktualizace« a zde zvolte možnost »Automaticky (doporučeno)«.

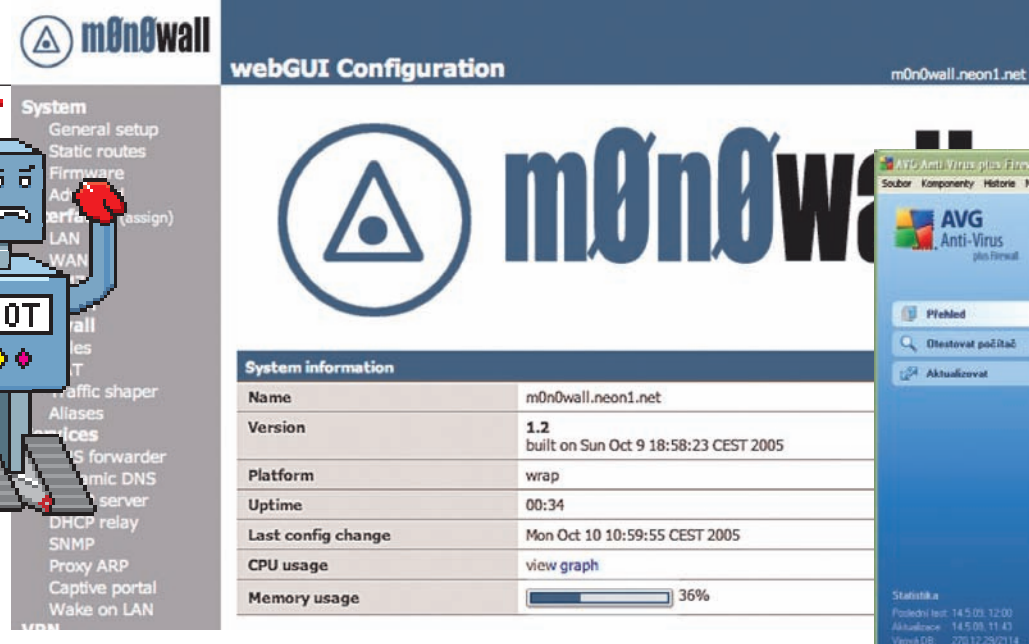
Kontrola e-mailu: Virové skenery odhalí skryté problémy

Programy se skrývajícími se boty (nebo přímo malware) se mohou do vašeho počítače dostat různými způsoby – mezi poměrně časté cesty patří i ta přes mail.

Z tohoto důvodu si v našem bezpečnostním balíčku zcela určitě aktivujte integrovaný „e-mailový skener". To provedete následujícím způsobem: V hlavní nabídce klikněte na »Komponenty | Kontrola pošty« a přidejte zatržítka u položek „Test příchozích zpráv" a „Test odchozích zpráv". Posledně jmenovaná volba vám napoví, zda váš systém nerozesílá e-maily nakažené viry (což může napomoci v odhalení skrytých botů). Další možnosti nastavení kontroly pošty na-



jdete také v nabídce »Nástroje | Pokročilé nastavení... | Kontrola pošty«. Zde lze také určit, jak se bude nakládat s nalezenými podezřelými přílohami. Jestliže v odchozí poště skener objeví vir, měli byste počítat s tím, že váš počítač je infikován. K odstranění škůdce opět použijte obranný mechanismus bezpečnostního balíčku. Pokud to pomocí AVG nefunguje, zkuste využít další bezpečnostní nástroje z našeho DVD.



Profesionální ochrana: Firewall M0n0wall dokáže ochránit i celou síť. Profesionální ochrana: Firewall m0n0wall dokáže ochránit i celou síť.

Před hackery v bezpečí: Dobrou ochranu před riziky z internetu nabízí i AVG Security Chip Edition 8.5.

Firewall: Alternativní použití

Dalším důležitým nástrojem je firewall. Někteří uživatelé v diskusních fórech čas od času argumentují, že desktopový firewall je zbytečný.

Fakt sice je, že bude-li odborník chtít, obvykle dokáže PC firewall přechytračit, ale softwarový firewall není jen pouhým ochranným opatřením před masovými útoky. Můžete ho také nakonfigurovat takovým způsobem, že dokáže snadno odhalit každý spamový bot. Musíte mu pouze sdělit, aby vás informoval o každém e-mailu, který váš počítač posílá. Jestliže sami žádný e-mail neposíláte, pak je jakékoliv odeslání pošty neklamným znamením, že je váš počítač zneužíván – obvykle tak, že rozesílá spamové maily pro internetovou mafii.

Router: Druhý firewall pro dokonalou ochranu

Pokud jste k internetu připojeni pomocí routeru, rozhodně doporučujeme využívat v něm integrovaný firewall. SPI firewally (Stateful Packet Inspection) současných modelů se totiž od desktopových firewallů zásadně liší. Na rozdíl od nich nehlídají „streamy“ aplikací, ale řídí cestu každého datového paketu. Například je-li na počítači připojeném k internetu vytvořeno připojení na WWW stránku (přes http), může cílový server (díky SPI firewallu) reagovat pouze na „http data pakety“.

Pokouší-li se útočník o „vstup“ do počítače, firewall přístup zablokuje, protože PC o žádná data nežádal. To je dodatečná ochrana například před spamboty.

Ukážeme vám, jak můžete tento firewall aktivovat například u oblíbeného routeru Netgear WNDR3300. V případě routerů jiných výrobců bude postup podobný...

Nejprve v prohlížeči zadejte adresu routeru, což je ve většině případů „192.168.1.1“, a vložte své přístupové údaje. V kartě „WAN configuration“ odstraňte zatržítko u položky „Deactivate SPI Firewall“. Následně nastavení potvrďte kliknutím na »Apply«. U některých routerů je už tento firewall standardně aktivován.

Pokud chcete, aby váš počítač byl skutečně v bezpečí, můžete si vytvořit téměř „neprůstřelný“ firewall z počítače, který bude zabezpečovat interní síť nezávisle na počtu a stavu počítačů skrytých za ním. K tomu účelu vám postačí starší počítač, Linux a dobrý „open-source“ firewall (často se pou-

INFO

Ochrana před lovci adres

Pro své sítě botů potřebují spammeři aktuální e-mailové adresy. Prozradíme vám, jak je získávají a jak se jejich metodám bránit.

Funkční e-mailové adresy mají pro spammery cenu zlata. Jak je získávají? Základní metodou je využití e-mailových „adresářů“ nalezených v napadených počítačích. Také ale prohledávají WWW stránky, chaty a záznamy instant messengerů pomocí nástrojů označovaných jako „adress harvesters“. A právě proto chrání celá řada správců webu pomocí technologie „CAPTCHA“.

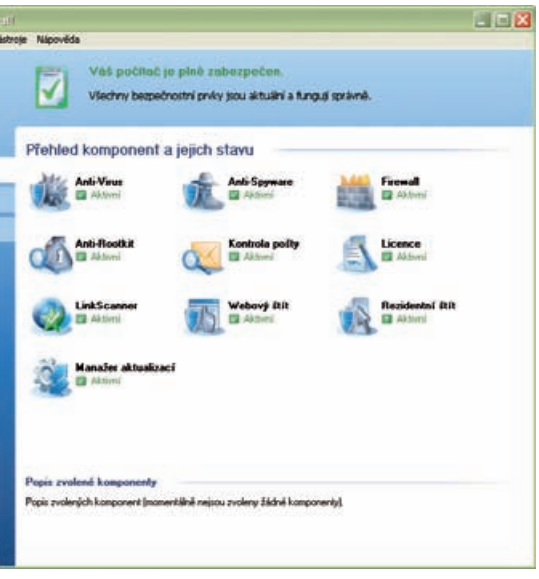
CO PŘEČTOU JEN LIDÉ

Jak „CAPTCHA“ funguje? Jestliže se chce uživatel přihlásit do diskusního fóra nebo mít přístup ke zprávám ostatních uživatelů, musí zadat kombinaci čísel a písmen, která se na stránce zobrazí v „upravené“ podobě. Problémem ovšem je, že hackeři si poměrně rychle našli způsob, jak tuto ochranu obejít – nástroje, které dokáží „CAPTCHA“ přečíst. Tyto nástroje obvykle fungují v jednom z pěti případů, což je ale pro potřeby „hledačů adres“ zcela dostatečné.

S KOČKAMI PROTI SPAMU

Jako náhradu za překonanou ochranu v podobě „CAPTCHA“ vyvinuli v laboratořích MSR (Microsoft Resarch) projekt ASIRRA (Animal Species Image Recognition for Restricting Access). Jeho podstata se od překonaného systému „CAPTCHA“ příliš neliší. ASIRRA zobrazuje obrázky koček a psů, přičemž vy musíte rozpoznat kočky a vše potvrdit pomocí „Adopt me“. Výběr a pozice obrázků jsou náhodné, což ztěžuje práci nástrojům hackerů. Překonání tohoto „ochranného systému“ sice možné je, ale jde o velmi náročnou a nákladnou záležitost.

Zákaz vstupu: Správci webů se snaží bránit vstupu hackerských botů pomocí technologie „CAPTCHA“.



žívá například MOnOwall, **www.m0n0.ch/wall**). Toto řešení má ale jednu podstatnou nevýhodu – vyžaduje dobrou znalost (mimo jiné) i TCP/IP.

Spamový filtr: Detekce a eliminace škůdců v pravý čas

Abyste jednou provždy zabránili internetové mafii v přístupu k vašemu počítači, měli byste se také co nejdříve zbavit škůdců v e-mailové schránce. Používáte-li služby freemailu (např. email.cz), jste proti spamu chráněni už poskytovatelem služeb – zde je výhodou i skutečnost, že tento filtr nechrání jen váš účet, ale i účty ostatních uživatelů, což zvyšuje úspěšnost filtrace a také omezuje šíření virů. My však přesto doporučujeme použít ještě jeden filtr, který zaručí stoprocentní ochranu.

Každý čtvrtý počítač je skrytým spambotem

Ochranu proti spamu nabízí i mnoho bezplatných poštovních klientů, obvykle je ale nutné tuto ochranu dodatečně aktivovat. My doporučujeme známý spamový filtr „Spamihilator“, jehož výhodou je fungování v transparentním režimu. Spolupracuje se všemi e-mailovými klienty, protože se v jednotlivých mailových klientech nepoužívá jako plug-in, ale pracuje jako již zmiňovaná transparentní proxy. To ale není jediná výhoda Spamihilatoru. Dalším plusem je fakt, že nástroj nepoužívá jen jeden filtr, ale maily „posílá“ přes řadu „testovacích stanic“, které mohou být neustále aktualizované a také přizpůsobené konkrétním potřebám. Bojíte se po přečtení předchozích řádek složité konfigurace? Zbytečně. Samotná konfigurace je otázkou několika kliknutí. Navíc – zdaleka nejefektivnější filtr je již implicitně nainstalován a připraven k okamžitému použití. Tento filtr se skrývá pod zkratkou DCC (Distributed Checksum Clearinghouse). Funguje velmi dobře, protože je založen na „komunitním principu“: každé PC, které si aktivovalo tento plug-in, zašle z každého e-mailu kontrolní součet na jeden z DCC serverů. Tam server jednoduše vypočítá frekvenci kontrolních součtů. Pokud počítadlo překročí kritickou hladinu, DCC klasifikuje mail jako spam.

Jestliže DCC filtr neuspěje, vypomohou ostatní: například Bayesovský filtr, který kontroluje obsah dopisu na výskyt určitých termínů (sex, viagra atd.), přičemž samozřejmostí je schopnost učit se. Pokud je váš e-mailový účet zasypáván spamem a selhává i posledně jmenovaný filtr, navštivte stránky **www.spamihilator.com/plugins**. Zde naleznete další užitečné plug-iny a rozšíření typu „Empty Mail“, které automaticky vymaže e-maily bez obsahu. Také plug-in „Attachment Extensions Filter by ve vaší sbírce rozhodně neměl chybět. Pomocí tohoto užitečného nástroje můžete filtrovat e-maily s určitými potenciálně nebezpečnými přílohami.

Tento filtr využívá skutečnosti, že u celé řady typů příloh lze odhadnout úroveň nebezpečí. Například soubory s příponou PIF jsou obvykle hrozbou. Důvodem je to, že tento formát souboru (který se dnes už nepoužívá) může mít příkazy, jejichž pomocí dáte zelenou virům a trojským koním. A to je přesně to, na co čekají zasilatelé phishingových mailů a spamu. Do kategorie „nebezpečné“ lze zahrnout i soubory EXE, COM a BAT.

Doporučujeme: Stanovte si přísná bezpečnostní pravidla a rizikové maily vůbec nepřijímejte.

I to může být důležitým kamenem ve zdi, která vás chrání před napadením a proměnou vašeho počítače na robota internetové mafie.

AUTOR@CHIP.CZ