Žádnou reklamu prosím...

Toto krátké oznámení možná ochrání vaši poštovní schránku, e-mailovou schránku však spammeři zahltí v každém případě. Chip vám ukáže, jak tyto otravné maily zablokovat – pomocí **CHYTRÝCH SPAMOVÝCH FILTRŮ.**

MARKUS HERMANNSDORFER

Filtrování: Většina freemailů nebo poskytovatelů nabízí kvalitní antispamovou ochranu schránek, u některých z nich je navíc možné ji ještě vylepšit.

Na narozeniny, na které se nikdo netěšil: spam letos oslavil své třicáté narozeniny. 3. května 1978 Garry Thuerk poprvé odeslal 400 reklamních mailů přes internet (Arpanet), který byl v té době ještě v plenkách. Čísla roku 2008 ale vypráví jiný příběh: podle firmy Sophos **(www.sophos.com)** je ze 100 miliard mailů, které jsou v každém okamžiku v „oběhu“, až 92% spamu. Množství však není jediným problémem. Ukazuje se, že odesilateli spamu často bývají nebezpeční zločinci. Ochranu proti nim si můžete zajistit pomocí celé řady opatření a chytrých spamových filtrů, které jsme pro vás připravili na našem DVD. Pomocí nich můžete webové mafii zavřít dveře před nosem – a také zablokovat spam, který je posílán přes upravené webové stránky a botnety.

Bez stresu: Používejte výhody providera

Všichni známí mailoví provideři (od Yahoo až po Seznam) nabízí filtry, pomocí nichž je spam vytříděn už na jejich serverech. Pokud vám tato ochrana z jakéhokoliv důvodu nevyhovuje, lze ji obvykle vypnout nebo přizpůsobit svým potřebám. Například na serveru mail.centrum.cz najdete toto nastavení takto: po přihlášení k poště klikněte v horní liště na odkaz »Nastavení schránky«, poté na sekci »Uspořádání zpráv« a nakonec v dolní části na »Zabezpečení proti spamu«. Zde si můžete ručně nastavit blokování vybraných adres, nebo naopak zadat adresy, ze kterých by se zprávy nikdy neměly dostat do spamového koše. Je zde také možné zcela vypnout antispamový filtr, to lze ale doporučit jen v krajním případě – filtr je nastaven dobře a jeho nahrazení by vás stálo příliš mnoho času a energie...

Filtrováno: Povolení pouze pro přátele

Zasilatelé spamu nejen často mění své adresy, ale dokáží také proniknout skrz některá ochranná opatření poskytovatelů, například pomocí vložení speciálních znaků nebo použitím neobvyklých formátů mailu. Spamihilator většinu zmiňovaných útoků eliminuje a jeho schopnosti lze i rozšířit pomocí plug-inů. Tento nástroj je ale praktický pouze u mailových klientů, jako je Outlook nebo Thunderbird, a to proto, že Spamihilator se mezi providerem a klientem chová jako proxy server. Kontroluje všechny maily s podezřelým obsahem a s „hříšníky“ naloží podle vašich požadavků. Tímto způsobem můžete zabránit spamu (který prošel filtry poskytovatele) v útoku na váš diskový prostor.

NASTAVENÍ Dříve než spustíte instalaci Spamihilatoru, ukončete spuštěného mailového klienta. Při instalaci (pro zajištění komplexní ochrany) zvolte »Complete instalation« – tato volba nainstaluje Spamihilator i celou řadu doplňkových filtrů. Poté nástroj sám identifikuje používaného e-mailového klienta a používaný protokol. Spamihilator už nějakou dobu také podporuje moderní

NA DVD

Nástroje proti spamu

Ad-aware 2007 ► nástroj proti malwaru
Adblock Plus ► rozšíření do Firefoxu na blokování reklamy
Cloudmark Desktop ► nástroj na boj s nevyžádanou poštou
defNULLSpam ► filtr pro poštovního klienta
G-Lock Spam Combat ► nástroj na blokování spamu
IE7pro ► vylepšené surfování s Internet Explorerem
K9-Filter ► antispamový filtr pro Outlook
POPFile ► univerzální antispamový filtr pro elektronickou poštu
SpamAssassin ► profesionální antispamový nástroj
SpamAware ► nástroj na filtrování spamu v Outlooku
SPAMfighter ► antispamový software, chránící i před phishingovými maily
Spamihilator ► nejrozšířenější nástroj proti spamu
SpamPal ► nástroj na odfiltrování spamu z vaší pošty
Spam Terrier ► antispamový nástroj od firmy Agnitum
SpyBot S&D ► oblíbený nástroj proti malwaru
SuperSpamKiller Pro ► nástroj na blokování spamu
Thunderbird ► alternativní poštovní klient
WPoison ► skript pro ochranu před harvestery e-mailových adres

► **NA DVD:** Všechny nástroje najdete na DVD pod indexem **BEZ SPAMU**.

protokol IMAP. Ihned po instalaci jsou filtry nástrojem nakonfigurovány, nemusíte tedy dělat žádné změny v jejich nastavení. To platí i pro efektivní DCC filtr (Distributed Checksum Clearinghouse). Ten funguje takto: pokud obdržíte mail, Spamihilator pošle jeho kontrolní součet na DCC server. Zde se zjišťuje, zda (nebo kolikrát) byl už mail s tímto kontrolním součtem poslán. Pokud je frekvence posílání mailu příliš velká, DCC server ho klasifikuje jako spam a to také nahlásí Spamihlatoru.

TŘÍDĚNÍ Souběžně s DCC filtrem nabízí Spamihilator také všechna populární „bezpečnostní opatření“, od slovního filtru až po „black and white list“. Spusťte si svého poštovního klienta, poté klikněte pravým tlačítkem na symbol Spamihilatoru a zvolte »Training area«. V novém okně uvidíte všechny přijaté maily. Mail od známé osoby můžete otevřít pomocí příkazu »View Message«. Pokud se navzdory vašemu očekávání jedná o reklamní mail, můžete ho označit jako spam. Po opakovaném označení spamu už Spamihilator typ „nevyžádaný obsah“ pozná a vícekrát ho do vašeho mailboxu nepustí.

Přes 90 % e-mailů je spam

Chcete vědět, jak se adresa vašich známých či přátel ocitla ve špatných rukou? Možností je několik. Jednou z nich je do systému propašovaný škůdce, který načte seznam adres mailového klienta. Mnohem častěji ale stačí, aby dotyčný zveřejnil svou adresu na internetu – na své webové stránce, v diskusním fóru nebo v podobě registrace u pochybné služby.

Pokud e-mailové adresy vašich přátel ještě v rukou internetové mafie neskončily, další obrana Spamihilatoru se skrývá pod položkou „whitelist“. V nabídce »Settings« klikněte ve složce „Senders“ na položku »Friends« a zde zadejte adresy všech svých přátel. Obvykle to lze udělat jednoduše pomocí „drag & drop“.

VYLEPŠENÍ SPECIÁLNÍCH FITRŮ Bezpečnostní opatření, o kterých jsme se až doposud zmínili, vám pomohou pouze u standardních formátů spamu. Abyste zablokovali maily ve speciálních formátech, se zvláštními znaky nebo s netradičními přílohami, budete potřebovat speciální rozšíření. V nabídce »Settings« klikněte na »Plugins | Advanced Plugins«. Zde najděte „Alphabet Soup Filter“, který dokáže vytřídit maily obsahující speciální znaky. „Foreign Language Filter“ a „Mystic Signs“ vám pomohou proti spamu s textem v cyrilici a čínštině. V některých případech budete při instalaci přesměrováni na stránku výrobce, kde si budete muset stáhnout nejnovější verzi filtru.

Efektivněji: Správné nastavení mailového klienta

Dalším krokem v ochraně před spamem je správné nastavení mailového klienta. Chip vám ukáže ty správné volby pro Outlook a Thunderbird.

OUTLOOK Pro udržení čistoty v mailovém klientu od Microsoftu zvolte »Actions | Junk E-Mail | Junk E-Mail Options«. V kartě „Options" nastavte »High«. Také můžete nastavit, aby se spam okamžitě mazal. Tím sice zabráníte zaplavení složky „Junk E-Mail" spamem, riskujete však i ztrátu špatně „vytříděného dopisu". I v Outlooku lze použít tzv. whitelist – zde jeho funkci plní volba »Safe Senders«, která může obsahovat kontakty na vaše přátele z adresáře.

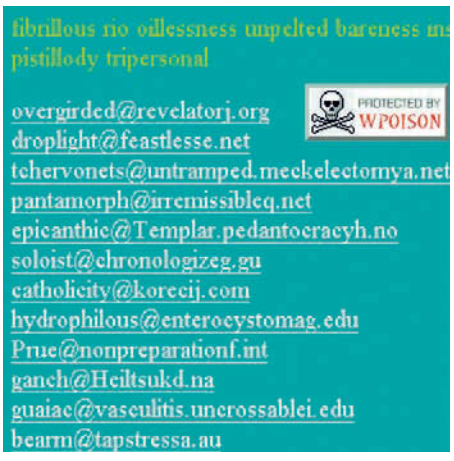
THUNDERBIRD Nástroj Mozilly si udržuje informace o všech mailech, které považujete za spam. Je pouze nutné klienta informovat, jak s tímto komerčním odpadem naložit. To provedete následujícím způsobem: kliknutím na »Nástroje | Možnosti« otevřete stejnojmenné okno. Zde v sekci »Soukromí« v kartě „Nevyžádaná pošta" zvolte možnost, která vám vyhovuje.

Chytře: Ochrana pro pokročilé uživatele

Díky výše uvedeným opatřením je vaše PC téměř stoprocentně chráněno proti většině hrozeb – alespoň do té doby, než spammeři vymyslí nový druh útoku. Aby váš mailbox zůstal bez reklamy i v budoucnu, potřebujete pro svůj e-mail dobré maskovací prostředky. To znamená zabránit automatickým sběračům adres, aby ulovily váš e-mail na internetu (na vaší homepage, v diskusích nebo v chatech).

POUŽÍVÁNÍ JEDNOÚČELOVÝCH ADRES Problémem je to, že na celé řadě internetových stránek potřebujete pro vložení příspěvku nebo stažení souboru platnou e-mailovou adresu. Na většině „slušných" serverů se zneužití svého mailu nemusíte bát, ale na pochybnějších stránkách je vložení „pravé" e-mailové adresy zbytečným rizikem.

Řešení: Využijte bezplatné služby „Spamgourmet" **(www.spamgourmet.com)**. Tam dostanete k dispozici falešné konto, na které vám může přijít až dvacet mailů (pro registrační účely bohatě stačí limit pět zpráv). E-mail s potvrzením registrace u libovolné služby tak bez problémů dorazí, vlna spamu však skončí v bezedné jámě falešného konta.



Protiúder: Skript v Perlu s názvem WPoison znepříjemní sběračům adres jejich práci...

OCHRANA WEBOVÉ STRÁNKY Většina tvůrců webových stránek by chtěla být v kontaktu s uživateli (ať už kvůli zpětné vazbě, nebo kvůli další propagaci svých stránek).

Jenže to je ta pravá voda na mlýn pro spammery – internet neustále křižuje velké množství automatických sběračů adres, které „prohlížejí" weby a pátrají zde po e-mailových adresách. Existuje celá řada způsobů, jak tento problém vyřešit, my vám doporučíme dva (podle našeho názoru) nejlepší.

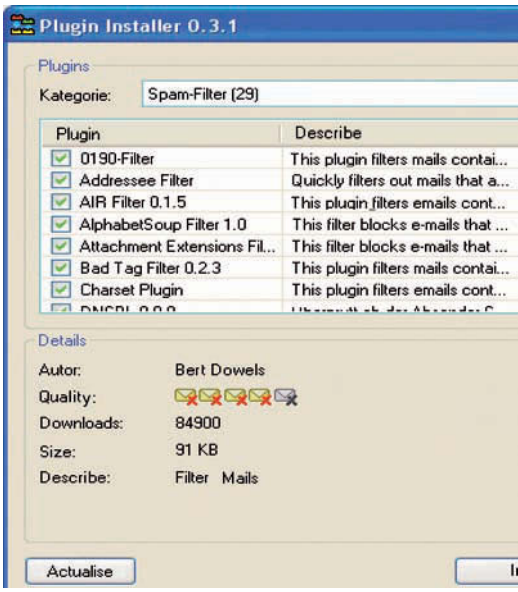
První možností je vložit svůj e-mail na stránku v obrázku. Problémem ovšem je, že i když obrázek nepojmenujete email.gif, není pro internetové čmuchaly velkým problémem z něj adresu zjistit. Je lepší obrázek s adresou vhodně rozdělit na dvě části a ty pak uložit pod různými jmény. Tím automatické sběrače zmatete a vaše adresa zůstane v bezpečí.

Pokud preferujete vložení e-mailu ve formě HTML, můžete sběrače zmást směsicí nesmyslných HTML příkazů. Místo klasického „Kontakt: mail@adresa.cz" vložte do kódu své stránky následující příkazy:

```
<P>Kontakt: <FONT color=#000000> mail</
FONT>@<FONT color=#000000> ad</FONT>
<FONT color=#000000>resa.cz</FONT></P>
```

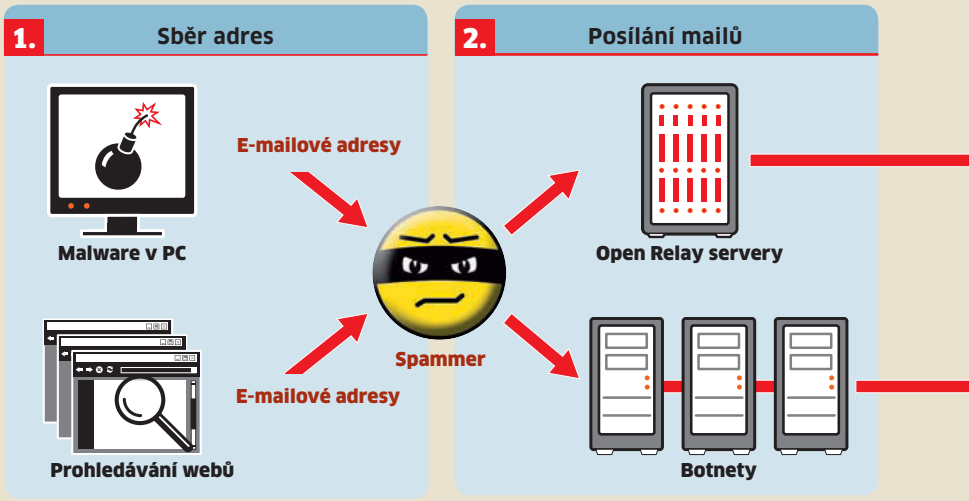
Finta je jednoduchá – ačkoliv je font implicitně černý, jeho barva je nastavena na černou a poté je toto nastavení zrušeno. Navíc je adresa rozdělena na dvě části, což opět zhoršuje identifikaci. To by mělo zmást sběrače adres natolik, že nebudou schopny vaši adresu připojit do svých úlovků. Poslední, už známou fintou je vynechání znaku @ a jeho nahrazení výrazem (z) nebo (na). Sběrače adres na základě tohoto znaku už dlouhou dobu dokáží identifikovat poštovní adresu a dokáží si ji převést do správného formátu. Pokud si to chcete vyzkoušet, použijte „textový browser" Lynx **(http://lynx.ics.org)** takto

```
lynx -dump <url> | grep @
```



Jak se spam dostává do vašeho PC

Nejprve spameří shromáždí velké množství emailových adres. Poté zneužijí cizí počítače k rozeslání spamu.



1. SBĚR ADRES
Spammeři dokáží pomocí speciálních nástrojů zjišťovat z webů e-mailové adresy. Ještě horší je metoda, kdy propašují do počítače trojského koně, který získá adresy ze seznamu kontaktů nebo přímo z lokálně uložené pošty.

2. ROZESÍLÁNÍ SPAMU
V dřívějších dobách byl spam rozesílán především přes Open Relay servery. V současné době jsou největšími katapulty spamu především botnety, což jsou armády počítačů zotročených zákeřným malwarem. Protože ale každý takovýto počítač odešle pouze pár mailů, filtrování pomocí blacklistu je neúčinné…

INFO

ASIRRA: Jak využít kočky a psy proti spamu

Ve vývojové laboratoři Microsoftu byla vyvinuta nová zázračná zbraň proti spamu: projekt MSR.

Platné mailové adresy jsou pro spammery neocenitelné. Pomocí harvesterů pročesávají webové stránky, diskusní fóra nebo logy instant messengerů, aby se takovýchto adres zmocnili. I to je důvod, proč na přístupu k většině podobných služeb najdete tzv. CAPTCHA.

PROLOMENÁ OBRANA

Pokud chce uživatel získat přístup k určité webové službě, musí do políčka vložit obsah z CAPTCHA, což je obvykle kombinace písmen a číslic. Problémem je ale fakt, že i tento na první pohled dobrý systém už byl „prolomen“, a to pomocí nástroje PWNtcha. adresa: **http://libcaca.zoy.org/wiki/PWNtcha**

PŘINÁŠÍ ASIRRA BEZPEČÍ?

Jako náhradu za systém CAPTCHA vyvíjí Microsoft projekt MSR ASIRRA. Model procesu je podobný: ASIRRA (Animal Species Image Recognition for Restricting Access) zobrazuje obrázky psů a koček. Při registraci musíte identifikovat obrázky a potvrdit ty samé pomocí „adopt me“. Volba a umístění obrázků jsou náhodné. Překonání tohoto systému pomocí mechanického vyhodnocování spambotů by bylo příliš obtížné a nákladné. Zároveň si s ASIRRA užije trochu zábavy i běžný uživatel…
Pokud si chcete nástroj otestovat sami, navštivte stránky **http://research.microsoft.com/asirra.**

Nelítostně: Eliminace spammerů

Jakkoliv jsou výše uvedená opatření dobrá, boj se spammery připomíná hru na kočku a myš. I když se vám podaří zablokovat spamovou vlnu, odesilatelé si stejně časem najdou způsob, jak nevyžádanou reklamu do vašeho mailboxu procpat.

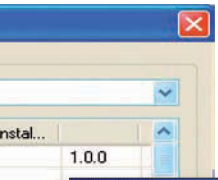
ZÁVĚR Pokud se chcete zbavit spamu, nelze jednou nainstalovat jeden program a spoléhat se na něj – musíte být stále ve střehu a vaše nástroje musí stále držet krok s protivníkem.

KLADENÍ TOXICKÉ NÁVNADY Jestliže spravujete vlastní webové stránky, můžete se zbavit jednoho z hlavních nástrojů spammerské mafie – toho, který prohledává stránky a hledá adresy (tzv. harvesteru). Na našem DVD najdete perl-cgi skript „wpoison.pl“ a soubor words.zip ve složce Wpoison. Ten druhý musíte rozbalit na webovém serveru ve složce, která obsahuje ostatní skripty. Proces integrace skriptu záleží na poskytovateli služeb (hostingu) a webovém editoru, který používáte. Na adrese **www.webweavers.de/material/cgi.rtf** najdete instrukce, jak skript propojit se zdrojovým textem. Autoři skriptu „wpoison.pl“ nabízejí svůj „produkt“ zdarma. Na oplátku žádají jen začlenění jejich loga do vaší stránky. Ty samé instrukce najdete i na webu **www.monkeys.com/wpoison**.

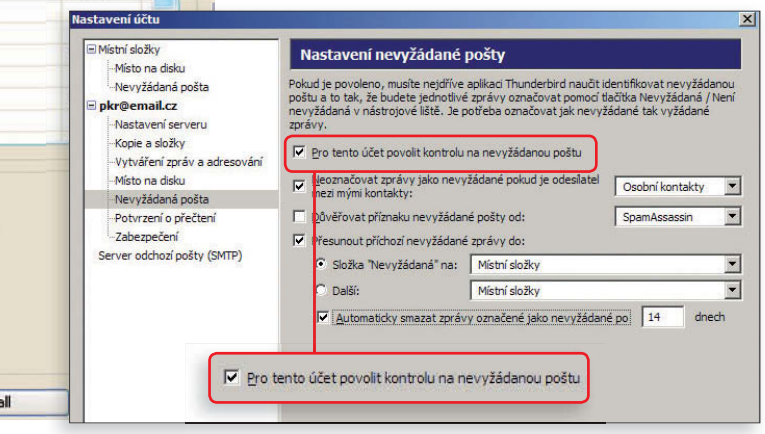
Pokud vás i navzdory integraci skriptu navštíví „sběrač adres“, nebude se mu u vás moc líbit. Stane se totiž následující: když harvester přečte kód vaší stránky, skript vytvoří nahodilé e-mailové adresy a odkazy na další stránky. Pokud tyto linky harvester sleduje, skript neustále generuje další a další linky. Sběrač adres je tak vržen do „bezedné jámy“ plné nesmyslných e-mailů, které neustále odesílá svému autorovi…

BITVA NEKONČÍ Je logické, že se spammeři snaží na tento trik reagovat – většinou tak, že skripty nespouští ze svých počítačů, ale na špinavou práci používají botnety. I tak je však díky skriptu boj s nimi snadnější, protože nemalý tok dat zpravidla neunikne pozornosti providera, který má možnost proti PC z botnetu zasáhnout. Webová stránka **www.spamcop.net** vyhodnocuje zaslané spamy a zjišťuje „odpovědného“ poskytovatele. Po registraci přes „Register Now“ obdržíte potvrzující mail a poté se již můžete k serveru přihlásit. Pak už stačí jen na server poslat spam – pokud je odeslán z amerických serverů, SpamCop je dokáže zablokovat.

AUTOR@CHIP.CZ



Speciální filtry: Pomocí filtrů lze ve Spamihilatoru filtrovat i neobvyklé formáty pošty.



Thunderbird: Další nastavení akcí proti spamu najdete i v nabídce Nastavení účtu.

Obrana: Proti spamu už pomáhají bojovat i kočky a psi…