Spammer v pasti

Chip začal bojovat proti **OTRAVNÝM SPAMŮM** pomocí tzv. honeypotu – a díky němu dopadl spammera při činu.

DOMINIK HOFERER

„Čeká vás velké překvapení! Jakmile totiž spolknete jednu z těchto tablet, začnou se dít divy i s vašimi žhavými sousedkami!“

Tak nějak vypadá typický spam „na viagru“, který každý z nás už alespoň jednou dostal do své schránky. Většina uživatelů dostává podobných „nabídek“ denně desítky – jde o poměrně velký problém, který vyžaduje řešení. Mnoho uživatelů už ale rezignovalo – na tento způsob „otravování“ si již dávno zvykli.

Výzva pro náš tým: Nastražíme past

Chipu je však poraženecký přístup cizí. Místo aby se vzdal, rozhodl se přijít spamu na kloub: najít původce spamu, kteří jsou odpovědní za 98 procent e-mailového provozu po celém světě. Abychom zjistili, kdo zasílá zprávy a zda opravdu existuje někdo, kdo si na základě spamu viagru nebo dokonce akcie koupí, bylo nutné chytit odesilatele při činu a potrestat ho. Proto jsme na spammery nalíčili past, tzv. honeypot.

Nezabere to mnoho času. Na webové stránky sportovního klubu (v našem případě třeba www.FC-Novak.cz), jsme vložili kód. Jakmile někdo stránku otevře, tento speciální kód nepřetržitě generuje nové e-mailové adresy. Všechny vygenerované e-mailové adresy míří do jedné „sdružené“ schránky bez spamového filtru. Spammeři, kteří používají harvester (nástroj, jenž systematicky prohledává síť a pátrá po adresách), by se do takové léčky měli chytit.

Profesionální spammeři: Většina mailů přichází od stejného odesilatele

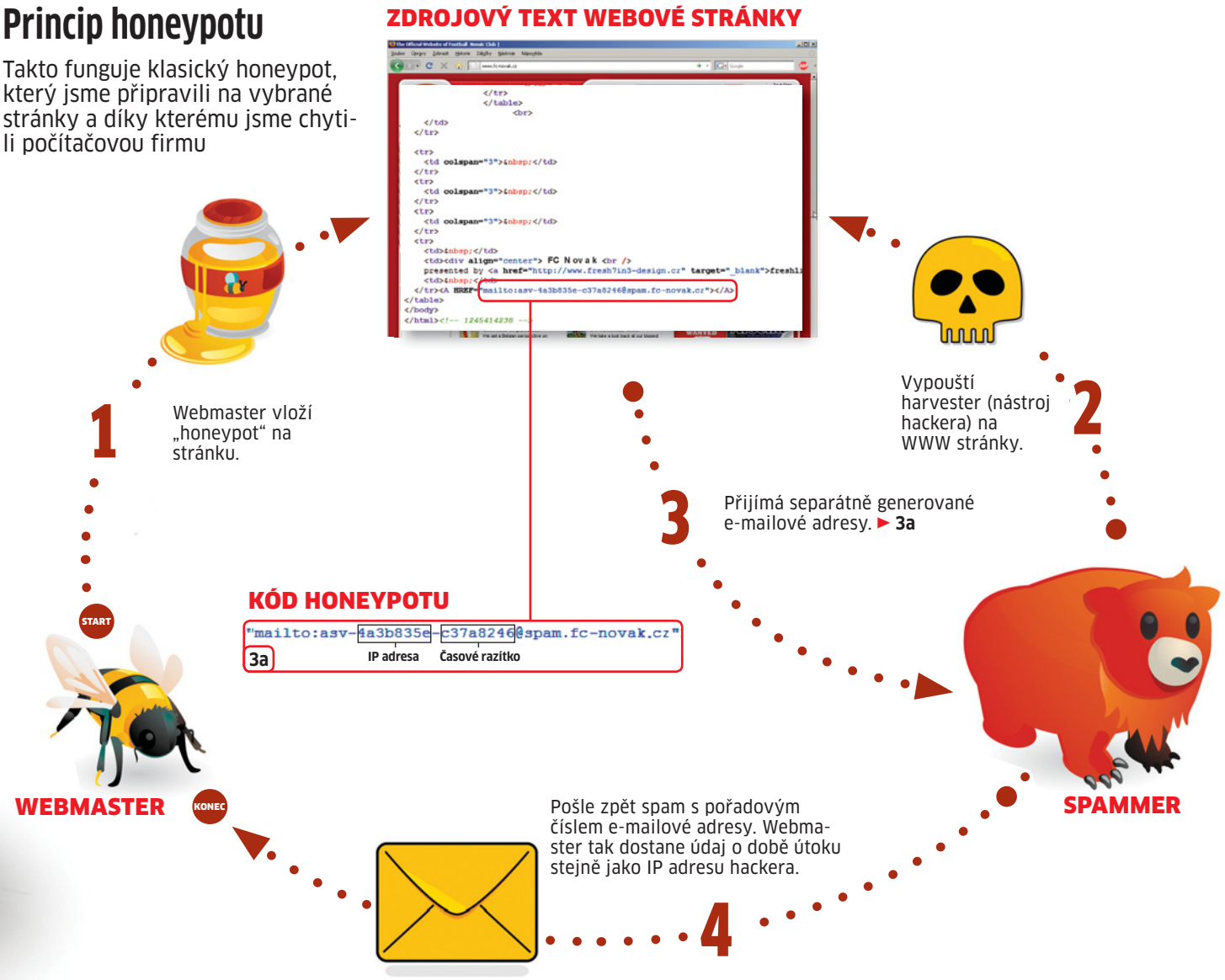
Výsledek: Naši schránku zaplavilo 20 000 spamových mailů. Kromě reklamy na viagru, které přicházely v různých formách, jsme obdrželi reklamy na stažení softwaru za úžasné ceny a klasický „nigerijský scam“. Pod tímto pojmem se skrývají maily, ve kterých jsou příjemci lákáni na sliby spousty peněz, pokud pomohou africkému obchodníkovi či bohatým vdovám převést miliony liber na evropské konto. Přistoupíte-li na takový obchod, jste přirozeně lapeni.

Náš průzkum jsme začali hledáním pachatele, který za těmito maily stojí. To ale není jednoduché, protože většina zasilatelů používá maskovanou identitu. Pokud bychom vzali za vděk globálními statistikami, závěr by byl jednoduchý: většina spamu pochází z gangu rusko-amerického spammera Leo Kuvayeva. Adresář na Spamhaus.org, což je mezinárodní projekt pro kontrolu spamu, uvádí Kuvayeva jako jednu z hlavních osob odpovědných za generování spamu. Statistiky uvádějí, že je spolu se zbývajícími devíti členy „top desítky“ zodpovědný za 80 procent světového spamu. Všechny pokusy zastavit ho skončily neúspěchem: v roce 2002 byl americkým soudem zažalován za škodu v hodnotě 37 milionů amerických dolarů. On však v pravý

ILUSTRACE: ISTOCKPHOTO

Princip honeypotu

Takto funguje klasický honeypot, který jsme připravili na vybrané stránky a díky kterému jsme chytili počítačovou firmu



čas odešel do Ruska a odtud ve své činnosti pokračuje – bez jakékoliv reakce ze strany ruských úřadů. Zde tedy mohlo naše pátrání neslavně skončit s konstatováním, že je pachatel nepostižitelný a boj proti němu je možné vést jen pomocí klasických antispamových nástrojů a triků. Po několika dnech se však na nás usmálo štěstí.

Na scénu vstoupil spammer ze severu Čech, který nejen nezatajoval odesilatele mailu, ale dokonce částečně odhalil jeho identitu – a to pro nás byla výzva.

Jednoho rána jsme dostali do schránky mail: „Zaregistrujte se prosím na našem portálu, objevte přátele a vytvořte si vlastní síť!“ Podpis v mailu odkazoval na odesilatele z České republiky, nechyběl ani klasický „osobní úvod“ s pozdravem: „Drahý příteli FC Novak“.

Na první pohled klasický dopis, který můžete po vymazání prvního řádku s oslovením komukoliv přeposlat. Jde tedy o omyl? Pokud se pořádně podíváte na adresu příjemce, je hned jasné, že do naší pasti spadl spammer. Adresa je asv-4582-fa9-3e4bf443@spam.fc-novak.cz.

Humpolácká adresa, kterou žádný funkcionář sportovního klubu určitě nepoužívá – ta byla vygenerována naším „honeypotem“ na webových stránkách. Navíc běžní návštěvníci tuto mailovou adresu nemohou vidět; všimnete si jí pouze tehdy, pokud se podíváte na zdrojový kód webové stránky a pátráte po symbolu @.

Tato e-mailová adresa je navíc výjimečná, protože to, co vypadá jako libovolný řetězec znaků, je individuálně vygenerované jméno, které o spammerovi odhaluje dvě věci: čas, kdy webovou stránku navštívil, a jím užívanou IP adresu. Avšak ani to není spolehlivý způsob, jak dokázat, kdo je zasilatel. Můžeme ho však nalákat do pasti a přinutit, aby nám vyzradil svůj zdroj dat. Konfrontovali jsme tedy autora nevyžádaného letáku, který ihned odpověděl:

„Drahý p. N. (...) upřímně se vám omlouváme, pokud máte pocit, že vás náš dopis obtěžoval. Samozřejmě vaši adresu ihned odstraníme z naší databáze.“

S touto odpovědí jsme však nebyli spokojeni a položili jsme několik otázek. Přece jenom jsme chtěli vědět, jak přesně se portál dostal k našim datům. Odesilatel v dalším dopise připustil, že použil harvester, který web systematicky prohledává, shromažďuje e-mailové adresy a zasílá je spammerovi. Dopis také odkryl důvod, proč zasilatel použil tento způsob získávání e-mailů:

„V případě nedostatečných finančních zdrojů, je poměrně častá tendence použít cesty, která není úplně optimální, ale v daném případě jediná možná. A právě z tohoto důvodu se snažíme najít naše kontakty co možná nejselektivněji, abychom se nestali součástí obrovského spamo-

vého gangu. Místo toho předkládáme nabídku pouze těm, kteří se o ni mohou zajímat."

Toto prohlášení objasňuje, proč je spam tak populární: e-maily jsou zdarma bez ohledu na to, zda jich pošlete tisíc, nebo milion. Jediným zádrhelem je tak přístup k zákaznickým datům. „Zvědavé společnosti" však mají k dispozici celou řadu různých zdrojů.

Naše čtenáře určitě nepřekvapí skutečnost, že existuje prosperující obchod se seznamy plnými e-mailových adres s různými úrovněmi „kvality". Jde o e-maily čerstvě nasbírané z internetu, částečně potvrzené nebo zcela schválené. Obchodníci se seznamy mají jednoduché prostředky ke zjištění, zda se e-mailová adresa stále používá, nebo zda leží nevyužitá: zašlou spam s HTML kódem. Pokud je zpráva otevřena, počítač automaticky ze serveru, který patří spammerovi, stáhne obrázky či jiné prvky. Tímto způsobem lze potvrdit, že adresa je funkční – a lze ji zařadit do seznamu „vysoké kvality". Tyto seznamy ale stojí peníze, zatímco harvester lze na internetu sehnat zdarma...

Dostupná reklama: Adresy získané pomocí harvesteru

Připravili jsme test, sehnali generátor e-mailů a vyvěsili ho na www.chip.cz. Během několika minut jsme vygenerovali téměř 100 adres různých lidí, kteří teoreticky mají nejspíše zájem o témata související s počítači. Data, která mohou být zajímavá pro podvodné IT obchodníky. Ve druhém kole testu jsme nasadili náš honeypot a harvester jsme aktivovali na stránce s nastraženými adresami. Během několika sekund jsme měli „v kapse" všechny adresy. Přesně tímto způsobem se náš spammer zmocnil dat – s jednou výjimkou: místo aby použil freeware nebo zakoupený software, napsal svůj vlastní nástroj a zaslal ho na číhanou po adresách. Skript zjistil několik set adres, na které byl zaslán spammerův leták a ze kterých dostal kladnou odezvu. Odesilatelé obdrželi pouze pár stížností a zbývající příjemci se změnili na věrné stoupence.

Nicméně harvester byl pro portál experimentem a zodpovědné osoby podle jejich tvrzení už nikdy nástroj nepoužijí. Uvedeným důvodem bylo, že ústní doporučení bylo elegantnějším způsobem, jak navázat kontakt s novými „zákazníky".

Závěr je ale jasný: Tato komunita a podobné „experimenty" jsou zodpovědné jen za nepatrnou část spamových mailů. Profesionálové, kteří pravidelně zaplavují síť spamem, pracují mnohem agresivněji: během jediného víkendu zasáhla internet vlna 4 500 mailů. Pro spamový útok podobného rozsahu jsou harvester a jeho zdroje nepoužitelné; pro podobné „útoky" se používají botnety, sítě počítačů, které jsou infikovány trojskými koni. Tyto sítě existují v různých velikostech, od tisíců infikovaných počítačů (příkladem může být síť známá jako „Zambie") až po miliony „zotročených" počítačů. Podle Marshal8e6 TRACElabs, bezpečnostního institutu se sídlem v USA, zasílají infikované počítače (v rámci nejefektivnějšího botnetu Rustock) až 25 tisíc spamových mailů za hodinu.

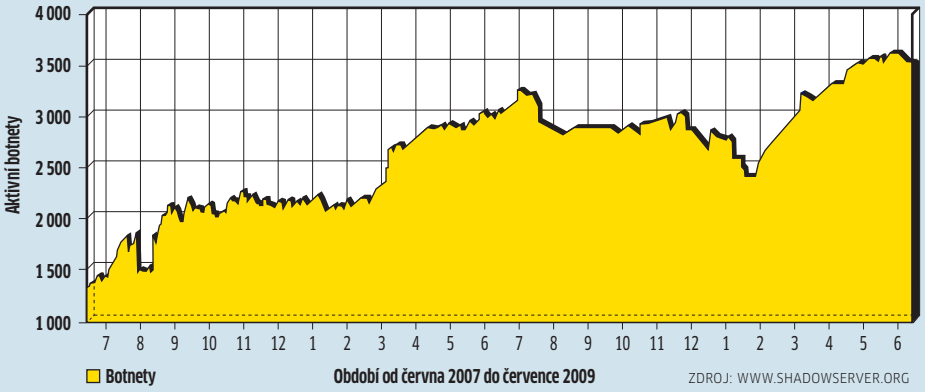
Na základě znalostí o schopnostech jednotlivých botnetů lze odhadnout objem spamu rozeslaného do celého světa. Podle jednoho z největších evropských webhosterů jsou celkové údaje děsivé: „V běžných dnech obdržíme za 24 hodin celkově asi 350 milionů mailů; o Vánocích dosáhne objem e-mailů asi 1 miliardy, přičemž 98 procent komunikace tvoří spam." Je tedy pochopitelné, že většina providerů a webhosterů investuje spoustu peněz do ochrany proti spamu. Odhaduje se, že průměrně utratí větší firma v této oblasti přibližně 350 000 eur ročně. To je hodně, avšak v případě zanedbání ochrany by později mohly být náklady na boj se spamem mnohem vyšší.

Kontrola spamu: Pomůže vám jen chytrá technologie

Pro většinu IT firem je jediným efektivním řešením v boji proti tomuto proudu mailů špičková antispamová technologie; jakékoliv pokusy o soudní řízení totiž ve-

POČET BOTNETŮ V LETECH 2007–2009

Počítačoví specialisté ze Shadowserver Foundation už delší dobu sledují rychlý nárůst počtu botnetů.



ZDROJ: WWW.SHADOWSERVER.ORG

Hon na spammery: Jak to funguje

Dokonce i vy můžete na svém prostoru na webu nastražit na harvestery past. Pomocí několika triků vám ukážeme, jak na to...

Aby se spammeři zmocnili e-mailových adres, používají harvestery, které slídí na internetu po datech. Ukážeme vám, jak můžete nastavit „honeypot", pomocí něhož se můžete i vy vydat na lov „harvesterů". Potřebujete k tomu „PHP kompatibilní" prostor na webu, všezachytávající e-mailovou adresu snipet kódu, který najdete v textovém souboru na DVD (kód Spam). Autorem myšlenky honeypotu je Daniel Rehbein; chcete-li se dozvědět více informací, můžete navštívit jeho webové stránky (**http://spamfang.rehbein.net**).

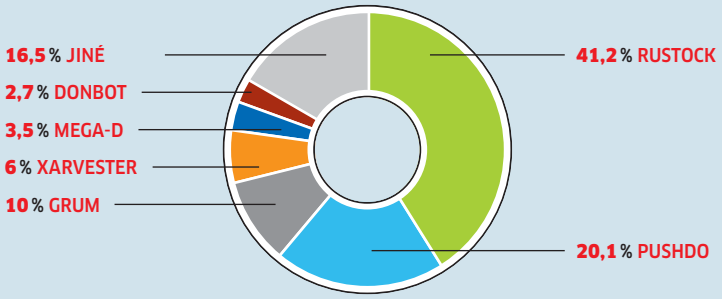
FUNGUJE TO TAKTO...

Nejdříve si nastavte „zachytávací" e-mailovou adresu a zadejte, aby všechny e-maily vygenerované honeypotem byly zaslány do této schránky. V ideálním případě byste si kvůli tomu měli vytvořit doménu třetího řádu (je zbytečné používat již existující adresy).

Nyní si do „šablony" své WWW stránky zkopírujte zdrojový kód z textového souboru

NEJVĚTŠÍ SÍTĚ SPAMBOTŮ

Statistiky serveru Marshal8e6 k 5. červnu 2009 ukazují, že největším botnetem je Rustock – má „na svědomí“ největší počet napadených počítačů…

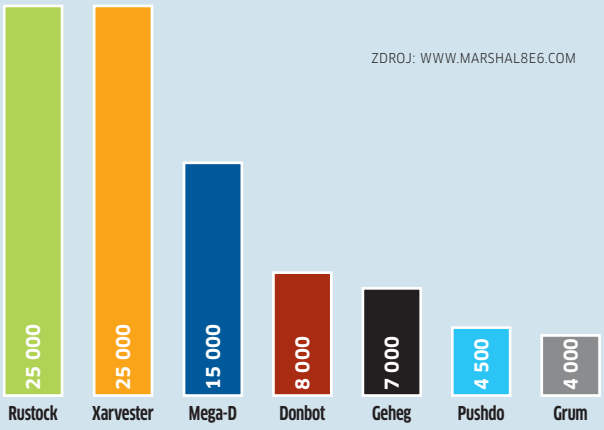


ZDROJ: WWW.MARSHAL8E6.COM

SPAM ODESLANÝ ZA HODINU „NAKAŽENÝMI“ POČÍTAČI

Počítače ovládané botnety Rustock a Xarvester rozesílají každou hodinu 25 tisíc spamových e-mailů.

ZDROJ: WWW.MARSHAL8E6.COM



dou do slepé uličky. Ačkoli je v celé EU rozesílání nežádoucích spamových mailů nelegální, ve většině případů nemohou být spammeři chyceni (natož souzeni), protože se skrývají v zemích, které proti kyberzločincům nic nepodnikají. Obvykle také skrývají svou identitu a k rozesílání spamu zneužívají napadené počítače nic netušících uživatelů.

I z tohoto důvodu jsme proti výše uvedené společnosti nepodnikli žádné další právní kroky, ale pouze jsme ji pokárali. Nicméně – stále máme jednoduché (ale nereálné) řešení problému spamových mailů: nikdo by nikdy neměl na spam odpovídat. Nebudou-li existovat zákazníci ochotní na tento druh „obchodní nabídky“ reagovat, elektronická pošta jako inzertní médium skončí. Proč je ale toto řešení nereálné? Protože se stále najdou lidé, kteří na podvodnou reklamu ve své schránce skočí. Potvrzuje to průzkum provedený na podzim roku 2008. Tým výzkumníků z USA se dokázal zmocnit botnetu pro výzkumné účely a pomocí něj zasílal spamové maily. Konkrétně šlo o Botnet Storm – síť, která ovládala miliony počítačových „Zombie“. Tým z ní použil pouze 80 tisíc počítačů, aby spustil pseudokampaň na software proti spamu a rozeslal přibližně 350 milionů mailů. Výsledek: 28 objednávek během 26 dnů. Je však pravděpodobné, že pokud by se něco podobného stalo v Evropě, zájem by projevila pouze hrstka lidí a ti zbývající by byli těmito otravnými maily pobouřeni.

Boj proti spamu je těžkým úkolem a globálním problémem, ve kterém inzertní kampaň výše uvedené komunity vypadá jako nevinná internetová legrácka. Profesionální spammeři jsou internetoví zloději, kteří se nedají snadno chytit. Za vším navíc pravděpodobně stojí opravdové kriminální živly, žijící v zemích, kde neexistuje řádný soudní systém. Odtud mohou bez obav ovládat své botnety.

Taková „zotročená“ aktivní počítačová síť pomáhá hackerům vydělat spoustu peněz. Ti pak mohou nejenom prodávat výpočetní výkon pro spamming, ale i přímo internetové mafii pro mnohem děsivější aktivity. Klasikou jsou například DDos útoky (Distributed Denial of Service) na webové stránky, které selhávají kvůli přetížení, nebo získávání čísel kreditních karet a PIN/TAN seznamů. Jedním z nejznámějších příkladů ohrožení sítě je červ Conficker. Už nějakou dobu se šíří po síti a po médiích a na milionech počítačů způsobuje pohromu.

Spammeři jsou internetoví kapsáři

Skutečnost, že se škůdci tak rychle šíří a dokáží infikovat spoustu počítačů, je především chybou uživatelů. Mnoho z nich to totiž zločincům neuvěřitelně usnadňuje – únos počítače a jeho integrace do botnetu je často hračkou. Počítače s nelegálními (a nezáplatovanými) Windows, počítače, jejichž antivirový software není aktualizován, počítače, jejichž uživatelé automaticky klikají na všechno, co vidí, jsou snadnými terči i pro hackerské začátečníky. Proto vás určitě nepřekvapí odhad německých bezpečnostních expertů: každý pátý počítač v Evropě je prý součástí sítě botů a mimo jiné zasílá spam…

Botnety: Největší hrozba pro internetovou bezpečnost

Zakročit proti hrozbám typu Conficker není jednoduché. Obecně se ví, že poskytovatelé internetových služeb dokážou vystopovat, který počítač byl „ukořistěn“ a je řízen hackery jako zombie. Teoreticky také mohou uživateli počítače poslat mail informující ho o situaci. Zákon o ochraně dat však tuto informaci nepovoluje uchovávat ani ji dále šířit. V každém případě ale mohou soukromí uživatelé proti spamu a botnetům něco dělat: udržovat počítač čistý a neobjednávat si viagru přes mail.

AUTOR@CHIP.CZ

z DVD. Část „example.com“ nahraďte svou doménou. Nyní si otevřete svou stránku nebo blog a otestujte a zkontrolujte zdrojový kód.

Pokud pomocí klávesové zkratky [CTRL]+[F] hledáte znak @, najdete vygenerovanou e-mailovou adresu. Jestliže byl kód vložen správně, měla by být tato adresa viditelná jen ve zdrojovém kódu a neviditelná při klasickém surfování. Nyní nakonfigurujte e-mailový program tak, aby zaznamenával odesilatelovu adresu, jinak po čase rychle ztratíte přehled, až vás zasáhne první vlna spamu. Díky e-mailové adrese, kterou může spammer nalézt pouze ve zdrojovém kódu webové stránky, můžete spammera konfrontovat prohlášením, že používal harvester, protože běžný uživatel tuto adresu nenajde.