Jak spammeři „sklízejí“ e-mailové adresy?
Uri Raz

Existuje mnoho způsobů, jak spammeři získávají e-mailové adresy. Ty, které znám, používají následující postupy:

1. **Z pošty s vaší e-mailovou adresou, kontrolovanou pomocí Usenet.**

Spammeři pravidelně, pomocí vytvořených programů, určených pro získávání e-mailových adres, kontrolují Usenet (http://www.earchiv.cz/a95/a511k140.php3, pozn. překl.). Některým programům se stačí podívat na články, které obsahují záhlaví s e-mailovou adresu (obvykle umístěnou za From:, Reply-To:, atd.), zatímco jiné programy kontrolují těla článků, počínaje programy, které prověřují podpisy, a konče např. programy, které prověřují kompletní obsah na znaky "@" a pokoušejí se provádět "demunging munging“ e-mailové adresy.

[„Munging" - někdy též nesprávně nazývaný „blokování spammu" - je změna e-mailové adresy na formu, kterou lidé mohou snadno pochopit, ale u počítačů je nepoužitelná. Např. e-mailová adresa <foo@example.com.no-spam> je „munging“ verze adresy <foo@example.com>. Člověk snadno určí správnou adresu, ale software určený ke zpracování e-mailových adres bude číst adresu nesprávnou, pozn. překl.].

Tam spammeři vždy mají příležitost k „demunging“ e-mailových adres, v rozmezí od „demunging“ jednotlivých adres za účelem spammu, až k automatickým metodám, které se snažily o „demunging“ e-mailových adres, které byly pomocí jistých způsobů změněny („munging“), např. odstraněním řetězce jako "nospam, no-spam" z e-mailových adres.

Jako lidé, kteří spamm často hlásí, vím, že frekvence spammu v mé poštovní schránce po období, ve kterém se zakládal Usenet, prudce klesla, stejně jako objem evidence spammerských shánění se po „čerstvých" a "živých" adresách, ale přesto se tato technika stále zdá být primárním zdrojem e-mailových adres pro spammery.

2. **Ze seznamu e-mailů.**

Spammeři se pravidelně pokouší kontrolovat seznamy účastníků e-mailových konferencí [některé mailové servery seznamy na vyžádání vydají], a vědí, že e-mailové adresy nejsou „munging“ a že jen málokterá z adres je neplatná.

Jsou-li poštovní servery nakonfigurovány takovou žádost odmítnout, pomůže jiný trik. Spammeři mohou na adresu konference poslat e-mail s hlavičkou

Return Receipt-To: <e-mail address> nebo **X-Confirm-Reading-To: <e-mail address>**.

Tyto hlavičky mohou způsobit, že někteří poštovní agenti a čtecí programy pošlou e-mail zpět na <e-mail address> a sdělí, že e-mail byl doručen/přečten na dané e-mailové adrese a tím to spammerovi prozradí.

Jiná technika používaná spammery je požádat server e-mailové konference o přenos seznamu všech zúčastněných na e-mailové konferenci (možnost, kterou provádějí některé servery s mail-seznamy pro pohodlí oprávněných uživatelů), a pak na seznam těchto e-mailových adres poslat spamm, takže server následně tvrdě pracuje při přeposílání kopie každému ze seznamu.
[Mám špatnou zkušenost se spammery, kteří tento trik používají. Někteří spammeři ho použili na seznam serveru společnosti, pro kterou pracuji, a který pokrývá většinu zaměstnanců, včetně

zaměstnanců, kteří pracovali na měsíční smlouvy a jejichž e-mailové adresy bylo obtížné získat jinými způsoby.]

3. **Z webových stránek.**

Spammeři mají programy, které pomocí „pavouka“ webových stránek hledají e-mailové adresy, např. e-mailové adresy obsažené v **mailto: HTML tags** [na ty můžete kliknout a získat otevřené okno pošty].

Někteří spammeři se zaměřují i na poštu založenou na webových stránkách. Zjistil jsem, že moji webovou stránku objevil v Yahoo nějaký spammer, který sesbíral e-mailové adresy z každé nové stránky, která se v Yahoo objevila a poslal mi spamm týkající se této webové stránky.

Široce používaný způsob boje s touto technikou je tzv. "jedovatý" CGI skript. Skript vytvoří stránku s několika falešnými e-mailovými adresami a linkem (odkazem) sama na sebe. Software spammera stránku navštíví, začne “sklízet“ falešné e-mailové adresy a naváže na odkaz, čímž uzavře nekonečnou smyčku „znečišťující“ jeho vlastní seznamy se staženými falešnými e-mailovými adresami.

Pro více informací o „jedovatém“ skriptu, viz http://www.monkeys.com/wpoison/.

4. **Z různých webových stránek a papírových formulářů.**

Některé weby lze požádat o různé detaily cestou formulářů, např. žádat o návštěvní knihy nebo formuláře registrace. Spammeři z nich mohou získat e-mailové adresy. Buď proto, že formulář bude k dispozici i na www nebo proto, že stránky prodávají/poskytují seznam ostatních e-mailů.

Některé společnosti prodávající/poskytující seznamy e-mailů je mají na papírových formulářích. Např. organizátoři shromáždění mají seznamy e-mailových adres účastníků, a prodávají je, když již nejsou potřeba.

Někteří spammeři vlastně zadávají e-mailové adresy z tištěných materiálů, např. z profesionálních adresářů a sborníků (zápisů z konferencí).

Doménová jména na registračních formulářích jsou oblíbená stejně - adresy jsou velmi často správné a aktualizované, a lidé čekající důležité zprávy e-maily čtou.

5. **Prostřednictvím démona Ident.**

Mnoho počítačů se systémem UNIX spouští démona (program, který běží na pozadí a je iniciovaný správcem systému), jehož cílem je umožnit ostatním počítačům identifikovat lidi, kteří se k nim připojují.

Když uživatel takového počítače surfuje a připojí se k webové stránce nebo zpravodajskému serveru, stránka nebo server se může připojit na takový počítač zpětně a dotázat se prostřednictvím démona na e-mailovou adresu uživatele.

Někteří chatující klienti se na počítačích chovají stejným způsobem a prostřednictvím IRC (Internet Relay Chat – komunikace po internetu v reálném čase) mohou získat e-mailovou adresu, která bude poskytnuta jako odpověď na nevyžádanou poštu.

6. **Z webového prohlížeče.**

Některé weby používají různé triky k získání e-mailové adresy z webového prohlížeče uživatele, někdy bez toho, že by si toho „surfující“ vůbec všiml. Tyto metody zahrnují :

1. Při vytváření čtené stránky prohlížeč načte jeden z obrázků na stránce přes anonymní FTP připojení k těmto stránkám.
Některé prohlížeče „ví“, že e-mailovou adresu má uživatel nakonfigurovánu do prohlížeče jako heslo k anonymnímu FTP účtu. „Surfař“ si není vědom této techniky a ani si nevšimne, že jeho e-mailová adresa unikla.

2. Použití JavaScript-u tak, že prohlížeč pošle e-mail na zvolenou e-mailovou adresu ze seznamu adres nakonfigurovaných v prohlížeči.
Některé prohlížeče umožňují odeslat e-mail, který bude odeslán tehdy, když ukazatel myši prochází přes nějaké části stránky. Není-li prohlížeč správně nastaven, nebude poskytnuto varování.

3. Použití HTTP_FROM hlavičky prohlížeče při odesílání na server.
Některé prohlížeče projdou hlavičku vašich e-mailových adres na každém webovém serveru, který navštívíte. Chcete-li zkontrolovat, zda váš prohlížeč prostě „dává“ vaši e-mailovou adresu, všem „na cestě“, navštivte http://www.cs.rochester.edu/u/ferguson/BrowserCheck.cgi/.

Stojí za to poznamenat, že když někdo čte e-maily pomocí prohlížečů (nebo poštovního klienta, který rozumí HTML), měl by si čtenář být vědom aktivního obsahu (Java applety, JavaScript, VB, atd.) stejně, jako webové nákazy.

E-mail obsahující HTML může obsahovat skript, který při načítání (předmět může být přímo zvýrazněn) automaticky odešle e-mail na všechny e-mailové adresy. Dobrým příkladem tohoto případu je virus Melissa. Takový skript mohl spammer poslat nejen čtenáři e-mailu, ale na všechny adresy jeho čtenářského adresáře.
http://www.cert.org/advisories/CA-99-04-Melissa-Macro-Virus.html.
O webové nákaze FAQ Richard M. Smith si můžete přečíst na
http://www.tiac.net/users/smiths/privacy/wbfaq.htm.

7. **Od IRC a chatovacích místností.**

Někteří klienti IRC dají uživatelskou e-mailovou adresu každému, kdo se o ni zajímá. Mnoho spammeři sbírá e-mailové adresy z IRC, protože vědí, že to jsou "živé" adresy a pak spamm na tyto e-mailové adresy posílají.

Tato metoda se používá vedle nepříjemných IRC botů, kteří vysílají zprávy do IRC a chatovacích místností interaktivně, aniž by se snažily poznat, kdo participuje na prvním místě.

Jedná se o další významný zdroj e-mailových adres pro spammery, zejména pokud jde o jednu z prvních veřejných činností nováčka se připojit, proto pro spammery je „sklízení čerstvých" adres lidí, kteří mohou mít velmi malé zkušenosti s bojem proti spammu, snadné.

AOL chatovací místnosti jsou nejoblíbenější z nich. Podle zpráv je to nástroj, který lze získat přímo na obrazovce jmen účastníků AOL v místnosti chatu. Nástroj se údajně specializuje na AOL ze dvou hlavních důvodů – na AOL obrazovce je seznam jmen aktivních účastněných uživatelů k dispozici a AOL uživatelé jsou považováni za primární cíle spammerů vzhledem k pověsti AOL jako ISP volby nováčků.

8. **Od démonů.**

Někteří démoni jsou nastaveni velmi přátelsky – dotykové dotazy požádají „john@hostitel“ o vytvoření seznamu informací, a to včetně přihlašovacích jmen pro všechny lidi jménem John, na tomto počítači. Dotaz na @host vytvoří seznam všech aktuálně přihlášených uživatelů.
Spammeři používají tuto informaci pro získání rozsáhlého seznamu uživatelů od hostitelů a aktivních účtů. Ty, kteří jsou "živí" a budou číst jejich poštu, brzy budou opravdu atraktivními spamm cíli.

9. **Z AOL profilů.**

Spammeři sklizeň AOL jména ze seznamů uživatelských profilů , protože jim umožňuje " zaměřit " své e-mailové konference . Také AOL má jméno bytí volba ISP z nováčků , kteří nemusí vědět, jak rozpoznat podvody, nebo vědět, jak zacházet spammu.

10. **Z bodů doménových kontaktů.**

Každá doména má jedno až tři kontaktní místa - administrační, technické a fakturační. Kontaktní místo obsahuje e-mailovou adresu kontaktní osoby.
Protože kontaktní místa jsou volně k dispozici, např. pomocí "whois" příkazu spammeři „sbírají“ e-mailové adresy z kontaktních míst seznamů domén (seznam domény je obvykle zpřístupněn veřejnosti podle registru domén) . To je velmi lákavá metoda spammerů, protože tyto e-mailové adresy jsou velmi často platné a e-maily na ně poslané jsou čteny a pravidelně kontrolovány.

11. **Pomocí hádání (tušení) a čištění.**

Někteří spammeři e-mailové adresy „hádají“ a odesílají seznam zkušebních zpráv (nebo skutečný spamm), který takové adresy obsahuje. Pak čekají buď na chybová hlášení vráceného e-mailu, což znamená, že e-mailová adresa je správná/nesprávná nebo na potvrzení. Potvrzení může být vyžádané vložením nestandardního, ale běžně používaného záhlaví zpráv se žádostí, aby dodávající systém nebo poštovní klient zaslal potvrzení o doručení nebo přečtení. „Žádné novinky nechceme“ jsou pro spammery dobrou zprávou.

Konkrétně se jedná o hlavičky:
Return-Receipt-To: <email-address>, která způsobuje potvrzení o doručení, které má být zasláno a
X-Confirm-Reading-To: <email-address>, která zasílají potvrzení o přečtení.

Jiný způsob potvrzení platné e-mailové adresy posílá HTML v těle e-mailu (které vysílá webová stránka v obsahu e-mailu), a to vkládáním do HTML obrazu. E-mailoví klienti, kteří dekódují HTML - např. Outlook a Eudora to dělají v podokně náhledu, kde se pokusí o „okouzlující“ obraz - i někteří spammeři, dají příjemci e-mailovou adresu do obrazu URL a zkontrolují, zda webový server e-mailové adresy příjemců, kteří spamm viděli, loguje.

Takže toto je dobrá rada pro nastavení poštovního klienta. V žádném případě „NE“ náhledu multimediálních e-mailů, které ochrání příjemce z obou náhodou potvrzených e-mailových adres před spammery a viry.

„Hádání“ může být provedeno na základě skutečnosti, že e-mailové adresy jsou založeny na jménech osob, obvykle běžně používanými způsoby, jako je „first.last@domain“ nebo „uvedením počátečního písmene jednoho z jmen, za nímž/před nímž je druhé@domain“).
Některé e-mailové adresy jsou standardní – „postmaster“ je např. zmocněn RFC dokumenty pro internetovou poštu. Další běžné e-mailové adresy jsou „postmaster, hostmaster, root“ [na hostitelích UNIX] apod.

12. **Z bílých a žlutých stránek.**

Existují různé weby, které slouží jako bílé stránky, někdy pojmenované lidmi vyhledávajícími webové stránky. Žluté stránky mají nyní e-mailový adresář na webu.

Tyto bílé/žluté stránky obsahují adresy z různých zdrojů, např. z Usenet, ale někde tam bude uvedena vaše e-mailová adresa zapsána přímo na vás. Např. Hotmail přidávat e- mailové adresy do Bigfoot standardně, takže nové adresy k dispozici veřejnosti.

Spammeři prochází tyto adresáře za účelem získání e-mailových adres. Většina adresářů zakazuje „sklízení“ e-mailových adres spammery, přesto ale tyto databáze obsahují obrovské seznamy e-mailových adres + jména, takže jsou pro spammery lákavým cílem.

13. **Tím, že mají přístup ke stejnému počítači.**

Pokud spammer má přístup k počítači, může obvykle získat seznam platných uživatelských jmen (a tedy e-mailové adresy) z tohoto počítače.

Na unixových počítačích je soubor uživatelů (/etc/passwd) je běžně čitelný, a seznam aktuálně přihlašovaných uživatelů je možné přečíst prostřednictvím příkazu "who".

14. **Získáním e-mailových adres předchozích majitelů.**

E-mailová adresa může být ve vlastnictví toho, kdo se tohoto PC zbavil. Může se to stát pomocí vytáčeného spojení k ISP pod uživatelským jménem. Někdo má údaje pro ISP, má jeho/její e-mailovou adresu „sklizenou“ spammery a zrušil účet. Když se někdo podepíše u stejného ISP stejným uživatelským jménem, spammeři už o tom ví.

Podobné věci se běžně stávají AOL obrazovek se jmény. Někdo používá přezdívku, unaví ho, uvolní ji. Později někdo jiný klidně může mít stejnou přezdívku.

15. **Používáním sociálního inženýrství.**

Tato metoda znamená, že spammer použije hoax s úmyslem přesvědčit podváděného, aby mu poskytl platné e- mailové adresy.

16. **Dobrým příkladem je řetězový dopis RichardDouche´s "Free CD´s".**

V dopise slibuje zdarma CD každé osobě, které bude dopis předán, pokud bude odkaz na ni duplikován Richardovi (CC'ed Richard). Richard tvrdil, že je spojován s Amazonem a Music Boulevard (Music Blvd), tedy společnostmi, které zmocnil k této nabídce. Avšak neposkytoval žádné odkazy na webové stránky a používal volnou e-mailovou adresu. Všechno co Richard chtěl, bylo, aby mu lidé poslali platné e-mailové adresy s cílem vytvořit seznam adres pro spamm nebo prodej.

17. **Ze seznamů adres a e-mailů na počítačích jiných lidí.**

Některé viry a červi se šíří prostřednictvím e-mailu se na všechny e-mailové adresy, které najdete v e-mailovém adresáři. Někteří lidé přeposílají vtipy a další materiály e-mailem svým přátelům a uvádějí e-mailové adresy svých přátel v polích „To:“ nebo „Cc:“ spíš, než v poli „Bcc:“ (skryté kopie), některé viry a červi skenují poštovní pole e-mailových adres, které jsou nejsou v adresáři v naději, že se trefí do schématu „přátelé přátel“, „přátelé přátel přátel“ atd.

Pokud to ještě neučinili, je to jen otázka času, než takový malware odešle nejen spamm kopie sebe sama, ale také extrahované seznamy e-mailových adres tvůrci.
Neviditelné e-mailové adresy nemohou být „sklízeny“, takže dobrá rada je, aby se e-mailové adresy příjemců vtipů vkládaly jako „skryté“, a předávané adresy vložené předchozím odesílatelem je nutné odstraňovat z těla e-mailové zprávy.

18. **Pomocí nákupů seznamů od jiných stran.**

Ten zahrnuje dva typy obchodů . První se sestává z nákupu seznamu e-mailových adres (často na disku CD-ROM), které byly „sklizeny“ prostřednictvím jiných metod , např. někdo „sklízel“ e-mailových adresy na Usenet a prodává seznam buď společnosti, která chce inzerovat prostřednictvím

e-mailů (někdy lidem mimo seznam, kteří se rozhodli pro reklamu e-mailem) nebo dalším, kteří dále seznamy přeprodávají.

Druhý typ se týká podniku , který získal e-mailové adresy legitimně (např. časopis, který se ptá účastníků na jejich e-maily proto, aby zůstávali v kontaktu přes internet) a prodává seznamu pro zvýšení svého příjmu. To se týká i prodeje e-mailových adres společností, které získaly prostřednictvím jiných možností, např. od zájemců, kteří se právě e-mailem dotazovali společnosti na cokoliv v rámci jakéhokoliv kontextu.

Třetí typ je tvořen technickým personálem, prodávajícím e-mailové adresy spammerům. O tom byla novinová zpráva o zaměstnanci, který prodal e-mailové adresy společnosti AOL spammerovi.

19. **Hackováním stránek.**

Slyšel jsem zvěsti, že na stránky, které poskytují bezplatné e-mailové adresy se pro získání seznamu e-mailových adres naboural hacker s cílem získat seznam kreditních karet.

Pokud byla vaše adresa „sklizena“ a jste zahlcován nevyžádanou poštou, mohou vám níže uvedené následující stránky pomoci:

1. Stránka MindSpring vysvětluje, jak se dostat do hlavičky e-mailu
http://help.mindspring.com/features/emailheaders/extended.htm.

2. Stránky FAQ ohledně spammu, udržované Ken Hollis
http://digital.net/~Gandalf/spamfaq.html.
http://www.cs.ruu.nl/wais/html/na-dir/net-abuse-faq/spam-faq.html.

3. Report spamm stránka - vynikající zdroj
http://www.ao.net/waytosuccess/.

4. Čtení hlavičky pošty.
http://www.stopspam.org/email/headers/headers.html.

5. Stránka Julian Haight´s spamm Cop
http://spamcop.net/.

6. FAQ Chris Hibbert ohledně nevyžádané pošty
http://www.fortnet.org/WidowNet/faqs/junkmail.htm.

7. „Rýče“ spammu, lovec spammu
http://samspade.org.

8. Penn´s stránky spammu
http://home.att.net/~penn/spam.htm.

9. FAQ WD Baseley´s – „munging“ adres
http://members.aol.com/emailfaq/mungfaq.html.

10. Boj proti spamu na internetových stránkách
http://spam.abuse.net/.

11. Recycling Center spammu
http://www.spamrecycle.com/.

12. Busters stránky odpadu
http://www.junkbusters.com/.

13. Stánky nevyžádané pošty
http://www.junkemail.org/.

14. BCP 30: Anti- spammová doporučení pro SMTP MTAs
http://www.faqs.org/rfcs/bcp/bcp30.html.

15. FYI 28: Pokyny Netiquette
http://www.faqs.org/rfcs/fyi/fyi28.html.

16. FYI 35: DO NOT SPEW (nezvracet)
Sada pokynů pro hromadnou nevyžádanou korespondenci a komentáře
http://www.faqs.org/rfcs/fyi/fyi35.html.

Několik míst na webu vám pomůže při sledování spammu:

1. Seznam Pete Bowden´s bran trasovacích cest
http://www.missing.com/traceroute.html.

Chcete-li najít brány trasovacích cest v každé zemi, hledejte zde
http://www.traceroute.org/.

2. . Allwhois.com brána pro dotaz na libovolnou doménu na celém světě
http://www.allwhois.com/.

3. Seznam „whois“ (dotazovacích) serverů. Shromáždil Matt Power
ftp://sipb.mit.edu/pub/whois/whois-servers.list.

4. Alldomains.com stránky - odkazy na síťové karty po celém světě.
http://www.alldomains.com/.

Podobnou stránku lze nalézt na
http://www.forumnett.no/domreg.html.

5. Koalice proti Usolicited komerčních e-mailů.
http://www.cauce.org/.

Evropská CAUCE.
http://www.euro.cauce.org/en/index.html.

Koalice proti nevyžádaným e-mailům, Austrálie.
http://www.caube.org.au/.

Ruská Anti-Spamm organizace.
http://www.antispam.ru/.

6. No More Spam - ISP spamm - blokování zásahů narušujících podnikání
http://www.byte.com/columns/digitalbiz/1999/04/0405coombs.html.

7. Dobrá kniha o manipulaci spamu: Removing the Spam, Geoff Mulligan, publikováno u Addison Wesley, ISBN 0-201-37957-0.

Právní zdroje:

1. FTC Consumer Alert - FTC Names Its Dirty Dozen: 12 největších podvodů s vysokou pravděpodobností přicházejících prostřednictvím hromadných e-mailů
http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.htm.

2. Zpráva Federální obchodní komise Ad_Hoc pracovní skupiny pro nevyžádanou reklamní poštu.
http://www.cdt.org/paper/report-federal-trade-commission-ad-hoc-working-group-unsolicited-commercial-email?quicktabs_4=1.

3. Pyramidové hry, Ponzi schémata a související podvody
http://www.impulse.net~thebob/Pyramid.html.

4 . Případ AOL vs Cyberpromo
http://legal.web.aol.com/decisions/dljunk/cyber.html.
Devět nových soudních tiskových zpráv:
http://legal.web.aol.com/decisions/dljunk/ninepress.html.

5. Intel skóre v e-mail „obleku“, Jim Hu, CNET News.com.
http://www.news.com/News/Item/0,4,29574,00.html?st.ne.ni.lh.

6. Spamm stránky John Marshall Law School
http://www.jmls.edu/cyber/index/spam.html.

7. První dodatek otázky týkající se UBE, Paul L. Schmehl.
http://www.utdallas.edu/~Pauls/spam_law.html.

8. Anti-Spam zákony USA
http://www.the-dma.org/antispam/statespamlaws.shtml.

9. Zákonná ochrana dat v UK
http://www.dataprotection.gov.uk/.

10. Italské Anti-Spam zákony
http://www.parlamento.it/parlam/leggi/deleghe/99185dl.htm.

11. Rakouský zákon Telecm
http://www.parlament.gv.at/pd/pm/XX/I/texte/020/I02064_.html.
http://www.bmv.gv.at/tk/3telecom/recht/tkg/inhalt.htm.

12. Norský zákon o kontrole marketingu
http://www.forbrukerombudet.no/html/engelsk/themcact.htm.