

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTELNIA

FRAGMENTY KSIĄŻEK ONLINE

Spam. Profilaktyka i obrona

Autor: Bartosz Danowski, Łukasz Kozicki

ISBN: 83-7361-316-1

Format: B5, stron: 184



Jan K. z Warszawy nie przeczytał jej i tydzień później jego skrzynkę odbiorczą zapełniły reklamy środków na porost włosów. Anna W. z Wrocławia odłożyła tę książkę na półkę, a kilka dni później jej adres e-mailowy został znaleziony wśród subskrybentów listy dyskusyjnej pl.rec.lancuszki.szczescia i przekazany do gdyńskiej firmy Internet Zakupy, która natychmiast wysłała do niej ponad 30 MB materiałów reklamowych opisujących najnowsze urządzenia kuchenne. Kazimierz C. natomiast poświęcił kilka godzin na lekturę tej książeczki i od tej pory nikt nie nęka go spamem.

Co Kazimierz C. znalazł w tej książce? Przede wszystkim informacje dotyczące tego, czym jest spam, skąd się bierze, jak uchronić swoje dane publikowane w sieci przed wyszukaniem przez programy zbierające adresy e-mailowe, jak zainstalować filtry antyspamowe i jak bronić się przed spamem różnego rodzaju. Poza tym dowiedział się również, że pojęcie SPAM pochodzi ze skeczu znanej angielskiej grupy komików i że istnieją regulacje prawne pozwalające na ściganie autorów spamu. W kolejnych rozdziałach książki „Spam. Profilaktyka i ochrona” czytelnik znalazł następujące informacje:

- Historia i rodzaje spamu
- Przepisy prawne dotyczące walki ze spamem w Polsce i Unii Europejskiej
- Ochrona adresu e-mailowego
- Mechanizmy antyspamowe w programach pocztowych i na serwerach
- Sposoby obrony przed różnymi typami spamu
- Korzystanie z systemu mailingowego bez oskarżeń o spamowanie
- Przegląd oprogramowania antyspamowego dla Windows i Linuksa



Spis treści

Wstęp	9
Rozdział 1. Wprowadzenie do tematyki spamu	11
Zarys historyczny spamu.....	11
Co jest spamem	15
Co nie jest spamem.....	18
„SPAM” i „spam” to nie to samo	21
Kto zarabia na spamie	22
Polska a spam.....	24
Konsekwencje istnienia spamu.....	25
Rozdział 2. Obszary funkcjonowania i popularne typy spamu	27
Obszary funkcjonowania spamu.....	27
Poczta elektroniczna.....	27
Grupy dyskusyjne.....	29
Strony WWW.....	29
Komunikatory internetowe.....	30
Spam wysyłany za pomocą windows-messengera	31
Telefony, faksy, SMS-y i MMS-y.....	32
Ulotki reklamowe w skrzynkach pocztowych.....	33
Popularne typy spamu e-mailowego.....	35
E-maile reklamowe	35
Oszustwa i wyłudzenia.....	39
Łańcuszki i żarty biurowe	43
Spyware, zombie i e-pluskwy	44
Rozdział 3. Spam a regulacje prawne w naszym kraju	47
Ustawa zasadnicza — konstytucja.....	48
Ustawa o świadczeniu usług drogą elektroniczną	48
Ustawa o ochronie danych osobowych.....	52
Ustawa o zwalczaniu nieuczciwej konkurencji	54
Ustawa o ochronie konkurencji i konsumentów	55
Ustawa o ochronie praw konsumentów	55
Prawo działalności gospodarczej.....	56
Prawo antyspamowe w Unii Europejskiej	56

Rozdział 4. Analiza nagłówków pocztowych.....	57
Analiza nagłówka SMTP.....	57
Szukanie osób odpowiedzialnych za konkretne adresy IP.....	60
Rozdział 5. Profilaktyka — ochrona adresu e-mailowego.....	63
Bardzo osobisty adres e-mailowy.....	64
Ochrona adresów e-mail w usenecie	65
Odsпамiacze	67
Ochrona adresów na stronie WWW	70
Kodowanie	70
Użycie grafiki.....	72
Użycie JavaScriptu.....	72
Flash, formularze, CGI.....	76
Aliasy pocztowe.....	77
Rozdział 6. Obrona, czyli jak skutecznie bronić się przed spamem.....	79
Bierna ochrona konta e-mailowego.....	79
Proste filtrowanie	79
Analiza statystyczna.....	80
Czarne i białe listy nadawców.....	82
RBL.....	83
Szare listy.....	86
Systemy typu pytanie-odpowiedź	87
Systemy rozproszone	88
Obrona po stronie serwera.....	90
Obrona za pomocą mechanizmów zaimplementowanych w systemie obsługi konta e-mail poprzez WWW.....	90
Procmail	93
Obrona po stronie klienta	96
Obrona za pomocą klienta pocztowego — Outlook Express (proste filtrowanie).....	96
Obrona za pomocą klienta pocztowego — Mozilla (metoda Bayesa).....	99
Obrona za pomocą zewnętrznych programów	103
Obrona poprzez oddziaływanie na spamera	128
Pisz skargi	128
Tłumacz spamerowi, że spam jest zły	129
Nie wypisuj się z list mailingowych, z których dostajesz spam	130
Nie korzystaj z „list Robinsona”	131
Rozdział 7. Atak — wyprzedź uderzenie spamera.....	133
Pułapki antyspamowe.....	133
Podsuwanie fałszywych adresów	137
Filtry samoatakujące.....	139
Rozdział 8. Przykłady obrony przed różnymi typami spamu	141
Dlaczego może jednak nie blokować reklam.....	141
Blokowanie popupów oraz natrętnych reklam	144
Usuwanie oprogramowania szpiegującego.....	150
Blokowanie usługi Messenger.....	152
Przykład pisma z prośbą o zaprzestanie nadawania reklam.....	161
Rozdział 9. Rady dla stawiających pierwsze kroki w e-biznesie.....	163
Listy opt-in i opt-out	164
Po pierwsze — witryna internetowa.....	165
Uruchamiasz listę opt-in.....	166
Przykład gotowego systemu mailingowego.....	169

Dodatek A	173
Netykieta i standardy obowiązujące w sieci	173
Akty prawne związane ze spamem obowiązujące w Polsce	173
Akty prawne związane ze spamem obowiązujące w Unii Europejskiej (po polsku)	174
Prawo w internecie	174
Metody walki ze spamem	175
Oprogramowanie do walki ze spamem	175
Unix, Linux	175
MS Windows	175
Najpopularniejsze czarne listy (RBL)	175
Sprawdzanie wielu list RBL jednocześnie i inne narzędzia	176
Strony poświęcone tematyce spamu	176
Podsumowanie	177
Skorowidz	179

Rozdział 4.

Analiza nagłówków pocztowych

Informacje zawarte w tym rozdziale są szalenie istotne dla prawidłowej identyfikacji nadawcy spamu oraz jego blokowania. Dlatego koniecznie dokładnie zapoznaj się z przykładami i komentarzami zamieszczonymi na następnych stronach.

Analiza nagłówka SMTP

Poczta elektroniczna działa w oparciu o tysiące, a nawet setki tysięcy serwerów rozproszonych na całym świecie. Każdy z serwerów może działać pod kontrolą innego systemu operacyjnego — takich jak Unix, Linux, Sun Solaris czy MS Windows. Z tego powodu musiano wprowadzić pewne standardy kierujące przepływem poczty w sieci. Jednym z takich standardów jest dołączany do każdej wiadomości nagłówek SMTP, na podstawie którego można dokonać identyfikacji drogi, jaką przeszła poczta, ustalić, kto jest jej nadawcą oraz kilku innych elementów. Każda wiadomość e-mailowa składa się zatem z dwóch części: częściowo niewidocznego zazwyczaj nagłówka oraz widocznej treści. Większość programów pocztowych pokazuje niektóre elementy nagłówka — takie jak adres nadawcy, datę wysłania wiadomości i jej temat. Nagłówek zawiera jednak znacznie więcej przydatnych informacji.

Aby sprawdzić nagłówek poczty, musisz skorzystać z odpowiedniej opcji w Twoim programie pocztowym. Ze względu na dużą ilość dostępnych programów do obsługi poczty elektronicznej nie będziemy opisywać, w jaki sposób w danej aplikacji dostać się do jej kodu. Musisz sobie sam poradzić¹. Nie jest to trudne.

Nagłówek SMTP poza możliwością sprawdzenia drogi, jaką przeszedł list, pozwala jeszcze na określenie kilku ciekawych elementów. Mamy tutaj na myśli użyty do wysyłki program pocztowy, jego wersję, priorytet wiadomości czy też identyfikację

¹ Jeśli znasz język angielski, kompletne instrukcje na temat sposobu przeglądania nagłówków większości popularnych programów pocztowych znajdziesz na stronie <http://news.spamcop.net/cgi-bin/fom?file=19>.

oprogramowania antywirusowego, jakie zostało użyte do sprawdzenia wiadomości pod kątem obecności wirusów.

Pozwoliliśmy sobie zamieścić listing przykładowego nagłówka, gdyż na konkretnym przykładzie omówimy jego najważniejsze części.

```
Return-Path: <bartek@poczta.onet.pl>
Received: from cdrinfo.pl ([unix socket])
  by cdrinfo (Cyrus v2.1.15) with LMTP; Thu, 22 Apr 2004 22:56:38 +0200
X-Sieve: CMU Sieve 2.2
Received: from smtp6.poczta.onet.pl (smtp6.poczta.onet.pl [213.180.130.36])
  by cdrinfo.pl (8.12.10/8.12.10) with ESMTMP id i3MKuWgh019784
  for <naczelny@cdrinfo.pl>; Thu, 22 Apr 2004 22:56:38 +0200
Received: from ait28.neoplus.adsl.tpnet.pl ([83.29.73.28]:55799 "HELO Micha")
  by ps6.test.onet.pl with SMTP id <S2115060AbUDVUwb>;
  Thu, 22 Apr 2004 22:52:31 +0200
From: = bartek@poczta.onet.pl
To: <naczelny@cdrinfo.pl>
Subject: Zgłoszenie awarii
Date: Sat, 24 Apr 2004 11:31:22 +0200
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1409
X-Virus-Scanned: by amavisd-new
```

Jeden wpis nagłówka może być zapisany w jednej lub kilku liniach. Jeżeli jeden wpis zajmuje kilka linii, każda — poza pierwszą — linia tego wpisu zaczyna się od jednego lub więcej znaków spacji lub TAB (na powyższym listingu widoczne jako „wcięcie”). Na podstawie wpisów zaczynających się od słowa *Received* możesz powiedzieć nieco więcej na temat drogi, jaką przeszedł przykładowy list. Możesz listę nagłówków *Received* analizować od pierwszego (najniższego) do ostatniego (najwyższego, dopisanego przez ostatni — czyli nasz — serwer pocztowy). Analiza nagłówków od dołu jest najbardziej uzasadniona w przypadku wiadomości, które nie są spamem — bowiem w tym wypadku zapewne wszystkie nagłówki są prawdziwe, tj. nie są celowo sfałszowane przez nadawcę. Jednak w wypadku spamu do nagłówków należy stosować zasadę ograniczonego zaufania: wierzyć można na pewno nagłówkom dopisanym przez ostatni, czyli Twój serwer pocztowy. Zaufanie do pozostałych nagłówków zależeć powinno od wyniku ich analizy.

W powyższym przykładzie analiza zacznie się od góry i będzie posuwać się w dół, czyli od nagłówków dopisanych do wiadomości przez Twój serwer pocztowy, poprzez nagłówki dopisane przez hosty pośredniczące, aż do nagłówka wpisanego przez komputer, z którego wiadomość pochodzi.

Zgodnie z tą zasadą, ostatni wpis *Received* zawiera informacje na temat Twojego serwera, który odebrał pocztę.

```
Received: from cdrinfo.pl ([unix socket])
  by cdrinfo (Cyrus v2.1.15) with LMTP; Thu, 22 Apr 2004 22:56:38 +0200.
```

Następny wpis zaczynających się od słowa *Received* zawiera informacje o tym, z jakiego serwera skorzystał nadawca poczty.

```
Received: from smtp6.poczta.onet.pl (smtp6.poczta.onet.pl [213.180.130.36])
  by cdrinfo.pl (8.12.10/8.12.10) with ESMTMP id i3MKuWgh019784
  for <naczelny@cdrinfo.pl>; Thu, 22 Apr 2004 22:56:38 +0200
```

W powyższym przykładzie poczta została wysłana poprzez serwer *smtp6.poczta.onet.pl* — ten zapis to tak zwany adres kanoniczny hosta². Ponieważ jeden serwer może mieć kilka nazw kanonicznych, dla Ciebie szczególnie ważny jest adres IP umieszczony nieco dalej, w nawiasach []. Tu należy się jednak uwaga, że niektóre programy do przesyłania poczty na serwerach nie zapisują adresu IP w nawiasach kwadratowych, tylko w okrągłych. Na podstawie nazwy i adresu IP możesz określić, kto jest właścicielem serwera. Tak się składa, że analizowana poczta trafiła do Ciebie poprzez serwer należący do *http://onet.pl*.

A oto ostatni omawiany nagłówek:

```
Received: from ait28.neoplus.adsl.tpnet.pl ([83.29.73.28]:55799 "HELO Micha")
  by ps6.test.onet.pl with SMTP id <S2115060AbUDVUwb>;
  Thu, 22 Apr 2004 22:52:31 +0200
```

Wynika z niego, że list został wysłany z komputera podłączonego do sieci za pomocą Neostrady. Świadczy o tym wpis *ait28.neoplus.adsl.tpnet.pl*. Oczywiście nazwa rejestrowana w odwrotnym DNS może odbiegać od faktycznego nadawcy, dlatego również w tym przypadku znacznie ważniejszy jest adres IP zapisany w nawiasie []. W powyższym przykładzie droga e-maila rozpoczęła się od adresu *83.29.73.28*, który należy do klasy adresów używanych przez TP S.A., nierzadko blokowanych na całym świecie. Oczywiście na podstawie samego adresu nie stwierdzisz, kto jest jego właścicielem, dlatego warto skorzystać z usługi *whois*. Więcej na temat identyfikacji nadawcy spamu na podstawie informacji zwartych w nagłówkach znajdziesz w jednym z następujących podrozdziałów.

Musisz pamiętać, że nagłówek SMTP może być sfałszowany i dlatego jedyną istotną i wiarygodną informacją są adresy IP, które, jak wspomnieliśmy, są zazwyczaj umieszczane w nawiasach kwadratowych lub okrągłych, najczęściej tuż za nazwą kanoniczną hosta. Czasem w jednym nagłówku można zobaczyć 2 adresy IP tuż obok siebie — jeden zapisany bez nawiasu, drugi w nawiasach. W takim wypadku adres został z całą pewnością sfałszowany. Jeśli zaś obok adresu IP znajduje się słowo *unknown*, to najprawdopodobniej znaczy, że wiadomość została przesłana przez serwer typu Open-Proxy, choć niektóre serwery OP podają również swoje nazwy kanoniczne, zatem „normalnie” wyglądający wpis (nazwa kanoniczna + adres IP) również może pochodzić od serwera proxy. Aby się tego dowiedzieć, możesz zweryfikować „reputację” danego adresu IP, na przykład za pomocą serwisu OpenRBL *http://openrbl.org/*. Jeśli po wpisaniu adresu do formularza otrzymasz odpowiedzi „proxy”, „open proxy”, „trojan” lub „zombie” — to znaczy że ten e-mail został przesłany poprzez serwer specjalnie przygotowany do wysyłki spamu i wszystkie nagłówki *Received* poniżej ostatnio omawianego zostały sfałszowane, na tym więc możesz przerwać analizę. Ostatnio na listach takich komputerów szczególnie często można znaleźć maszyny korzystające ze stałego szerokopasmowego dostępu do internetu, w tym na przykład komputery polskich użytkowników neostrady. Na komputerach tych często działają bez wiedzy ich właściciela programy zainstalowane podstępnie przez spamerów, celem masowej wysyłki spamu bez wiedzy właściciela łącza, w sposób uniemożliwiający wykrycie sprawcy. Na szczęście jednak wielu providerów po wykryciu takiego przypadku natychmiast odcina mu połączenie internetowe — dlatego warto składać skargi do operatorów internetowych — o tym, jak się do nich dowiedzieć, gdzie je składać nieco niżej.

² Host — serwer internetowy lub komputer klientki podłączony do internetu.

Jeśli zaś nagłówek nie zawiera w ogóle adresu IP, nie znaczy to, że jest on fałszywy (choć często tak może być), ale na pewno jest bezwartościowy dla celów analizy — mógł być bowiem dopisany w trakcie przesyłania e-maila z jednego programu do drugiego, działającego na tym samym serwerze. Jeśli zaś najwyższe nagłówki zawierają wpisy podobne do (*localhost [127.0.0.1]*) — również możesz je zignorować — zostały one dopisane na Twoim serwerze pocztowym, na przykład przez program antywirusowy lub filtr antyspamowy.

Na koniec tej części drobna uwaga: w przypadku spamu wysłanego do grup dyskusyjnych najbardziej będą Cię interesowały nagłówki *X-trace* (w których powinien znajdować się adres IP źródła wiadomości) oraz nagłówki *NNTP-Posting-Host* — zawierający adres komputera, poprzez który wiadomość została wysłana do systemu *news*.

Szukanie osób odpowiedzialnych za konkretne adresy IP

Jeżeli wejdiesz w posiadanie adresu IP, to bez większych problemów może on posłużyć jako punkt zaczepienia pozwalający na znalezienie osoby odpowiedzialnej za jego administrację. W tym celu musisz posłużyć się usługą *whois*. Zanim jednak zamienisz adres IP na konkrety, musisz wiedzieć, że internetowy świat został podzielony na trzy części i każda z nich ma przypisaną sobie organizację przydzielającą i zarządzającą adresami. Poniżej prezentujemy tabelę z odpowiednimi danymi.

Tabela 4.1. Dane organizacji zajmujących się przydziałem adresów IP na świecie

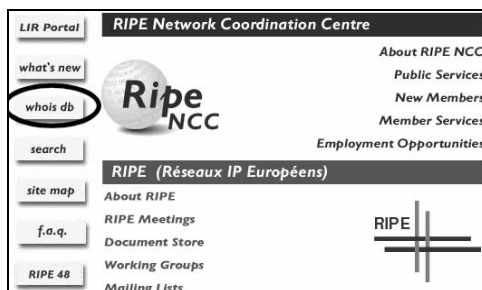
Region	Instytucja	Strona WWW
Europa i Afryka	RIPE	www.ripe.net
Ameryka	ARIN	www.arin.net
Azja, Pacyfik	APNIC	www.apnic.net

Niestety, zwykły laik nie będzie mógł na podstawie samego adresu powiedzieć, z której części świata on pochodzi. Dlatego w skrajnych przypadkach trzeba będzie zbadać wszystkie trzy organizacje, aby uzyskać potrzebne informacje.

W ramach testu przyjrzyj się, do kogo należy IP 83.29.73.28. Wejdź na stronę <http://www.ripe.net> i odszukaj odwołania do *whois* — rysunek 4.1.

Rysunek 4.1.

Widok witryny
<http://www.ripe.net>



Po kliknięciu przycisku *whois db* na ekranie monitora zobaczysz prosty formularz, w którym należy wpisać badany adres IP — rysunek 4.2 — a następnie kliknąć przycisk *Search*.

Rysunek 4.2.
Sprawdzanie adresu IP
— etap pierwszy

```

% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% see http://www.ripe.net/ripenncc/pub-services/db/copyright.html

inetnum:      83.29.0.0 - 83.29.127.255
netname:      NEOSTRADA-ADSL
descr:        Neostrada Plus
descr:        Krakow
country:      PL
remarks:      ! - ! - ! - ! - ! - !
remarks:      Contact to ABUSE TP S.A. :
remarks:      abuse@tpnet.pl
remarks:      ! - ! - ! - ! - ! - !
admin-c:      TPHT
  
```

Po chwili pod formularzem powinny pojawić się wyniki.

Z pierwszej części odpowiedzi wynika, że adres jest używany przez krakowski oddział Telekomunikacji Polskiej, który w swoim posiadaniu ma adresy z przedziału od *83.29.0.0* do *83.29.127.255*.

```

inetnum:      83.29.0.0 - 83.29.127.255
netname:      NEOSTRADA-ADSL
descr:        Neostrada Plus
descr:        Krakow
country:      PL
remarks:      ! - ! - ! - ! - ! - !
remarks:      Contact to ABUSE TP S.A. :
remarks:      abuse@tpnet.pl
remarks:      ! - ! - ! - ! - ! - !
admin-c:      TPHT
tech-c:       HT2189-RIPE
status:       ASSIGNED PA
mnt-by:       TPNET
changed:      hostmaster@tpnet.pl 20031211
source:       RIPE
  
```

Analiza dalszych części wyników szukania pozwala znaleźć dokładniejsze dane.

```

role:         TP S.A. Hostmaster
address:      TP S.A. "POLPAK"
address:      ul. Nowogrodzka 47A
address:      00-695 Warszawa
address:      Poland
  
```

```

phone:          +48 22 6252383
fax-no:         +48 22 6225182
e-mail:         hostmaster@tpnet.pl
trouble:        Network problems: hostmaster@tpnet.pl
trouble:        Abuse and spam notification: abuse@telekomunikacja.pl
trouble:        DNS problems: dns@tpnet.pl
trouble:        Routing problems: registry@tpnet.pl
admin-c:        TK569-RIPE
tech-c:         TK569-RIPE
tech-c:         JS1838-RIPE
nic-hdl:        TPHT
remarks:        ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - !
remarks:        Please send spam and abuse notification only to
abuse@telekomunikacja.pl
remarks:        ! - ! - ! - ! - ! - ! - ! - ! - ! - ! - !
mnt-by:         TPNET
changed:        hostmaster@tpnet.pl 20030122
changed:        hostmaster@tpnet.pl 20030904
source:         RIPE

```

Kolejne wyniki sprawdzenia adresu IP zawierają dane kontaktowe z instytucją zarządzającą danymi adresami. Pamiętaj jednak, że w przypadku dużych operatorów telekomunikacyjnych nie dzwoni się do nich ze skargami. Do tego służą specjalne adresy e-mail podane w wynikach sprawdzania danego adresu. W tym konkretnym przypadku można skorzystać z adresu *abuse@telekomunikacja.pl* oraz *abuse@tpnet.pl*.



Każdy dostawca usług internetowych powinien udostępnić specjalne adresy kontaktowe, na które można zgłaszać różne problemy — w tym te dotyczące spamu.

Jeżeli dla badanego adresu IP nie otrzymałeś odpowiedzi, oznacza to, że pochodzi on z innej strefy i musisz skorzystać z pozostałych *whois*.

Aby złożyć skargę, otrzymany e-mail wyślij *jako załącznik* (to ważne) pod znalezione adresy *abuse@*. Na wstępie warto dodać kilka słów wyjaśniających okoliczności otrzymania tego spamu.