Analiza nagłówków pocztowych

Paweł Krawczyk
kravietz@aba.krakow.p

21 kwietnia 2001

1 Wstęp

Poczta elektroniczna jest usługą, w której obsługę może być zaangażowane od kilku do kilkunastu serwerów, nieraz rozsiadnych po całym świecie. Teoretycznie każdy z nich może działać pod innym systemem operacyjnym i innym oprogramowaniem pocztowym. Ponieważ standardy poczty elektronicznej definiują tylko pewną część tego, co może znaleźć się dodanych do listu nagłówkach, dla niewprawnego oka mogą one być w dużej mierze nieczytelne. Równocześnie umiejętność ich prawidłowego rozpoznania stanowi klucz do określenia rzeczywistego nadawcy listu, serwera z którego skorzystał oraz serwerów, które pośredniczyły w jego przesyłaniu.

Artykuł ten prezentuje podstawowe informacje praktyczne, przydatne podczas analizy poczty elektronicznej, prowadzonej czy to przez użytkownika, który otrzymał spam, czy to administratora, który stara się wyśledzić pochodzenie spamu, obraźliwego listu lub pospolitego *mailbombingu*.

2 Kilka podstawowych zasad

- Nagłówki **From**, **To** i **Subject** nie mają tak naprawdę *żadnego* znaczenia dla poprawnego doręczenia listu.
- Kolejne serwery przesyłające list *prawie zawsze* pozostawiają w nim ślad w postaci nagłówka **Received**.
- Kolejne serwery *z reguły* pozostawiają w tym nagłówku informację, od kogo otrzymały list oraz do kogo był on przeznaczony.
- List *może* zawierać sfałszowane nagłówki **Received**, ponieważ nie mają one znaczenia dla trasy, którą będzie przesyłany list.
- Informacje zawarte w nagłówkach **Received** *prawie zawsze* pozwalają z całkowitą pewnością określić źródło listu[1].

[1] Wyjątkiem są listy wysłane przez anonimowe remailery.

3 Procedura

Typowa procedura rozpoczyna się oczywiście od otrzymania samego emaila. Osoba prowadząca analizę może być adresatem tego emaila. Może też być administratorem, który otrzymał od użytkownika prośbę o pomoc wraz z załączonym spamem lub kopią listu, którym zalano jego skrzynkę pocztową. W tym drugim wypadku do dobrej praktyki należy przyzwyczajenie użytkowników, by odnośne listy przysyłali zawsze z pełnymi nagłówkami, najlepiej jako załączniki MIME.

Dalsze kroki są następujące:

1. Analiza nagłówków otrzymanego maila.
2. Określenie rzeczywistego nadawcy.
3. Określenie serwerów pośredniczących.
4. Stwierdzenie, kto jest odpowiedzialny za dane sieci.

4 Analiza nagłówków pocztowych

4.1 Przykład pierwszy

```
Received: from PACIFICO.mail.telepac.pt (mail2.telepac.pt [194.65.3.54])
        by tau.ceti.com.pl (8.8.8/8.8.8/bspm1.13/prot) with ESMTP id EAA27017
        for <webmaster@ceti.com.pl>; Tue, 19 May 1998 04:37:47 +0200
Received: from mail.telepac.pt ([194.65.180.41])
          by PACIFICO.mail.telepac.pt (Intermail v3.1 117 241) with SMTP
          id <19980519033740.GDQ29969@mail.telepac.pt>;
          Tue, 19 May 1998 03:37:40 +0000
Date: Tue, 19 May 1998 03:39:19
From: versailles@mail.telepac.pt
Subject: Easy Links!
```

List ten przeszedł przez dwa serwery pocztowe, o czym świadczą dwa nagłówki *Received*, które czytamy od dołu do góry - nagłówek dolny został dodany najpierw.

Nasz system (`tau.ceti.com.pl`) otrzymał ten list z portugalskiego serwera `mail2.telepac.pt`. Informacja ta pochodzi z górnego nagłówkach i znajduje się w okrągłych nawiasach. Należy pamiętać, że jedyną pewną informacją jest tutaj adres IP umieszczony w nawiasach kwadratowych. Nazwa zarejestrowana w odwrotnym DNSie może nie mieć nic wspólnego z prawdziwym nadawcą listu, może jej też w ogóle nie być, tak jak to jest w przypadku kolejnego nagłówka.

Wynika z niego, że list został faktycznie wysłany z adresu IP `194.65.180.41`, o którym nie wiadomo nic więcej. Jednak podobieństwo adresów pozwala

przypuszczać, że w tym wypadku nadawcą listu po prostu klient lub użytkownik sieci portugaleskiej firmy telekomunikacyjnej *TelePac*.

Nazwa `mail.telepac.pt`, która pojawia się w dolnym nagłówku tak na prawdę nie ma najmniejszego znaczenia — jest to nazwa, którą ustawiono ręcznie lub automatycznie wygenerował ją program spammera, i którą program ten przedstawił się serwerowi pocztowemu (przy pomocy komendy *HELO*).

4.2 Przykład drugi

```
From Warning@yahoo.com  Fri May 22 12:02:46 1998
Return-Path: <Warning@yahoo.com>
Received: from VAX.KVCC.EDU (vax.kvcc.edu [198.108.138.10])
        by tau.ceti.com.pl (8.8.8/8.8.8/bspm1.13/prot)
        with SMTP id MAA24918 for <kravietz@ceti.com.pl>;
        Fri, 22 May 1998 12:02:45 +0200
Date: Fri, 22 May 1998 12:02:45 +0200
Received: from PC.svsu.edu ([199.174.167.21]) by VAX.KVCC.EDU
          with SMTP; Fri, 22 May 1998 0:36:10 -0400 (EDT)
From: Tom Christiansen <Warning@yahoo.com>
To: Stealth Mailer <ami-net@ryukyu.ne.jp>
Received: from SMTP.XServer     (Smail4.1.19.1 #20) [...]
Received: from mail.apache.net(really [164/187]) [...]
Received: from 32776.21445(really [80110/80111]) [...]
Received: from local.nethost.org(really [24553/24554])
```

Ten nagłówek jest doskonałym przykładem listu, wysłanego przez specjalizowane oprogramowanie spammerskie, w tym wypadku *Stealth Mailer*. Po przyjrzeniu się najniższym nagłówkom *Received* można zauważyć, że zawierają one dość bezsensowne dane, dodane właśnie przez to oprogramowanie, zapewne w celu zaciemnienienia nagłówków i utrudnienia analizy osobie niezbyt wprawnej (linijki były znacznie dłuższe, zostały pocięte dla przejrzystości).

Faktyczna droga listu zaczyna się od serwera o adresie `199.174.167.21`, o którym nie wiadomo nic więcej, poza tym że używa *Stealth Mailera*. Program ten, jak inne tego typu produkty, posiada zapewne długą listę otwartych serwerów SMTP z całego świata, stworzoną przez producenta. W tym wypadku program wybrał sobie serwer `vax.kvcc.edu` i przez niego przesłał swoją reklamę.

4.3 Uzyskane informacje

Na podstawie dwóch powyższych analiz uzyskaliśmy następujące informacje co do tych dwóch listów:

- Zostały one wysłane z adresów IP nie zarejestrowanych w DNSie, konkretnie `194.65.180.41` (spam „portugalski") oraz `199.174.167.21` (drugi spam).
- W każdym wypadku w przesyłaniu listu pośredniczyły dodatkowe serwery pocztowe. W pierwszym wypadku (`mail2.telepac.pt`) był to zapewne serwer firmy, z której usług korzysta spammer. W drugim zaś serwer `vax.kvcc.edu`, należący do jakiejś uczelni amerykańskiej, której nie stać było w tym wypadku na poprawne zabezpieczenie maszyny.

5 Reakcja na spam

5.1 Po co wysyłać skargi?

Wysyłanie spamu stoi z reguły w sprzeczności z regulaminami korzystania z usług firm ISP. Wysłanie do nich skargi w sprawie spamu wysłanego przez ich użytkownika przeważnie powoduje zamknięcie jego konta w razie stwierdzenia, że była ona uzasadniona. W przypadku spamu wysyłanego przez pracowników firm działa to rzadziej, jednak wysłanie skargi zawsze jest dla firmy znakiem, że zaczyna swoimi działaniami marketingowymi wchodzić na śliski grunt, które to działania mogą popsuć wizerunek firmy i ostatecznie zmniejszyć sprzedaż, zamiast ją poprawić.

Skargę należy także wysłać do administratora serwera, który został wykorzystany do przesłania spamu. W wielu przypadkach administratorzy takich serwerów nie są w ogóle świadomi, że przez ich maszyna oraz łącze przesłano nieraz kilka milionów reklam. Otrzymanie nawet kilku skarg często jest wystarczającym motywem do zadbania o bezpieczeństwo serwera.

Przykłady tekstu takiej skargi w języku polski i angielskim zostały podane na końcu tego artykułu. Do skargi należy zawsze załączyć sam spam, koniecznie z pełnymi nagłówkami — tak, by umożliwić osobie po drugiej stronie potwierdzenie naszych pretensji lub stwierdzenie, który z użytkowników jest odpowiedzialny za ten incydent. W tym celu najlepiej załączyć taki list jako załącznik MIME.

5.2 Jak znaleźć osoby odpowiedzialne?

Odnalezienie kontaktów do osób zarządzających lub odpowiedzialnych za serwery wykorzystane do przesłania tych dwóch reklam jest czasem dość trudne. Pierwsza rzecz, jaka się w tym wypadku narzuca to wykorzystanie ich nazw zarejestrowanych w DNS. A zatem, jeśli spam przeszedł przez serwer `mail2.telepac.net`, to możnaby spróbować wysłać skargę do admi-

nistratora pod adres `postmaster@mail2.telepac.net` [2]

Korzystanie z tej metody nie jest jednak godne polecenia poza przypadkami, kiedy domena należy do znanej firmy i jej autentyczność nie ulega raczej wątpliwości. Można wtedy wejść na jej stronę i znaleźć odpowiednie adresy kontaktowe.

W większości przypadków będziemy jednak mieli do czynienia z adresem IP jako jedyną pewną informacją co do pochodzenia spamu. Wtedy potrzebne adresy można uzyskać z usługi *Whois*.

5.3 Usługa *whois*

Usługa ta jest związa z systemem przydzielania adresów IP obowiązującym na całym świecie. Każdy blok jest przydzielany konkretnej organizacji, która udostępnia instytucji rejestrującej takie dane jak nazwa, adres oraz emaile i telefony kontaktowe osób odpowiedzialnych za sieć. Dane te są potem publicznie dostępne właśnie za pomocą *whois*, czyli interfejsu do bazy danych odpowiedniej instytucji rejestrującej.

Tych ostatnich może być wiele w każdym kraju, jednak są tylko trzy w skali całego świata. Są to odpowiednio:

Instutucja	**Region**	**WWW**	**Whois**
RIPE	Europa, Afryka	`www.ripe.net`	`whois.ripe.net`
ARIN	Ameryka	`www.arin.net`	`whois.apnic.net`
APNIC	Azja, Pacyfik	`www.apnic.net`	`whois.apnic.net`

Odpowiednie interfejsy do przeszukiwania baz można znaleźć na stronach odpowiednich instytucji. Poniżej podamy tylko przykład pozyskania informacji o adresie IP, z którego wysłano jeden z przeanalizowanych przez nas spamów. Do przeszukiwania bazy *whois* wykorzystaliśmy najpopularniejszego klienta dla systemów unixowych, który nazywa się po prostu *whois*.

```
$ whois -h whois.ripe.net 194.65.180.41 | head

% Rights restricted by copyright.

inetnum:      194.65.160.0 - 194.65.255.255
netname:      TELEPAC-POPS
descr:        Telepac - Comunicacoes Interactivas, SA
descr:        Point Of Presence Networks
country:      PT
admin-c:      TP3302-RIPE
```

[2] Przyjętym zwyczajem jest, że administrator danego serwera pocztowego jest osiągalny przez konto *postmaster* na tym serwerze. W przypadku dużych firm providerskich często działa także adres *abuse*, przeznaczony właśnie do obsługi takich incydentów.

```
admin-c:     PG259-RIPE
[...]
```

Baza zwraca informację, komu został przydzielony dany adres IP oraz kto jest administratorem tej części sieci. Informacja ta jest z reguły zupełnie wystarczając, jednym z podawanych sposobów kontaktowania się jest bowiem adres email.

5.4 Inne serwisy

Istnieją serwisy, ułatwiające czy wręcz załatwiające za użytkownika wysyłanie skarg w sprawie niechcianej poczty (swoją drogą, świadczy to o skali problemu). Wśród dwóch najpopularniejszych wymienić można **abuse.net** oraz **SpamCop**. Obie z nich wymagają darmowej rejestracji.

Pierwsza usługa pozwala na automatyczne wysłanie skargi do administratorów domeny, z której przyszedł dany list. Polega to po prostu na wysłaniu emaila pod adres *domena.com@abuse.net*, a serwer zajmie się już przesłaniem tej skargi pod adresy odpowiednie dla domeny *domena.com*. Działa to w szczególności dla „dużych" domen, których komórki do spraw nadużyć zarejestrowały swoje adresy w *abuse.net*. Dla pozostałych domen skarga jest przesyłana po prostu pod typowe adresy, takie jak *postmaster* czy *administrator@domena.com*.

Serwis **SpamCop** jest bardziej zaawansowany i potrzebne informacje uzyskuje m.in. z bazy *Whois*. Działanie użytkownika ogranicza się do wklejenia otrzymanego spamu w odpowiednim formularzu na WWW serwisu, który dalej automatycznie powiadamia administratora odpowiedniej domeny i oczekuje na wyjaśnienie incydentu.

Strona tego serwisu jest dostępna pod adresem http://www.spamcop.net/. Aby skorzystać z *abuse.net*, należy po prostu wysłać na jego adres pierwszą skargę. Serwis odpowie prośbą o potwierdzenie automatycznej rejestracji i następne skargi będzie obsługiwał bez pytania.

6 Przykłady

6.1 Przykład skargi po polsku

```
Otrzymalem spam (przesylke reklamowa) wyslana z waszej sieci. Nie
zapisywalem sie na zadna liste wysylkowa i nie podoba mi sie fakt ze na
moj adres sa wysylane reklamy, ktore mnie nie interesuja i zasmiecaja
moja skrzynke pocztowa. Prosze o uniemozliwienie swoim uzytkownikom
wysylania tego rodzaju reklam w przyszlosci.

Dostajesz ta skarge, poniewaz Twoj adres jest podany jako adres kontaktowy
dla sieci, z ktorej ten spam zostal wyslany, lub dla serwera pocztowego,
```

ktory go przeslal.

Kompletny list, ktory otrzymalem, wysylam w tym liscie w postaci zalacznika MIME aby pomoc Ci w okresleniu jego pochodzenia. Wiecej informacji na temat walki z naduzywaniem poczty elektronicznej znajdziesz na nastepujacych stronach:

http://spam.abuse.net/
http://www.mail-abuse.net/

6.2 Przykład skargi po angielsku

We have received a spam (unsolicited commercial email) from your network. We don't like this and we ask you to stop your users or customers from doing this in future.

The contact information was obtained from whois database. You probably got this complaint because you're listed as contact person for either the originating network, or for the SMTP server that relayed this spam.

The complete spam message is sent within this complaint as an MIME attachment, to help you identify origin of the spam. You can find more information on preventing abuse of email on the following sites:

http://spam.abuse.net/
http://www.mail-abuse.net/