Jak zdemaskować nadawcę listu

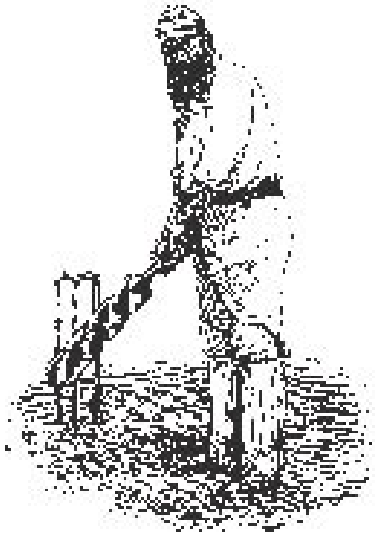
Tomasz Nidecki

Artykuł opublikowany w numerze 5/2004 magazynu *hakin9*. Zapraszamy do lektury całego magazynu.

Magazyn *hakin9*, Software-Wydawnictwo, ul. Piaskowa 3, 01-067 Warszawa, *pl@hakin9.org*

Jak zdemaskować nadawcę listu

Tomasz Nidecki



Wielu użytkowników poczty elektronicznej jest przekonanych, że zapewnia ona pełną anonimowość. Zakładając darmowe konto pocztowe można przecież podać fałszywe dane, a adresat wiadomości ma niewielkie szanse na domyślenie się, kim jest na przykład misio@chatkapuchatka.com. Poczucie anonimowości jest jednak złudne – wprawne oko może wyłuskać z nagłówków otrzymanej wiadomości sporo informacji o nadawcy, a następnie wykorzystać je przeciw jemu.

Załóżmy, że otrzymaliśmy list z adresu *misio@chatkapuchatka.com*. Jego nadawca grozi nam, że jeśli nie oddamy mu całego zgromadzonego zapasu miodu, naśle na nas Tygryska, który zabryka nas na śmierć. Oczywiście adres nadawcy może być bardzo łatwo sfałszowany (patrz Artykuł *Jak wysyłany jest spam*, *Hakin9* 2/2004), a Puchatek jest naszym dobrym znajomym i nie sądzimy, by wysyłał nam takie groźby. Spróbujmy więc zdemaskować prawdziwego autora gróźb, a następnie zgłosić jego przewinienie, by wyciągnięte zostały wobec niego stosowne konsekwencje.

Analizę nagłówków poczty elektronicznej rozpocznijmy od podzielenia ich na istotne i nieistotne. Od razu możemy pominąć te, w których podany jest adres nadawcy: `From` i `Return-Path`, bowiem SMTP umożliwia wstawienie w to miejsce dowolnego adresu (patrz Artykuł *Jak wysyłany jest spam*, *Hakin9* 2/2004).

Równie mało istotne z punktu widzenia analizy będą takie nagłówki, jak `Subject`, `Date`, `To`, `Delivered-To` i inne, odpowiedzialne na przykład za kodowanie znaków. Zwróćmy jednak uwagę na nagłówki niestandardowe, rozpoczynające się od `X-` – niektóre z nich mogą okazać się, wbrew pozorom, użyteczne.

Podział zawęził nasze poszukiwania praktycznie do dwóch grup. Pierwszą są nagłówki `Received`, które będą stanowiły podstawę naszych poszukiwań. Drugą są wszelkie nagłówki zaczynające się od `X`, oczywiście jeżeli występują w wiadomości i jeśli dane wyłuskane z nagłówków `Received` okażą się niewystarczające (patrz Ramka *Informacje w nagłówkach X*).

Z artykułu nauczysz się...

- jak zareagować w przypadku otrzymania pocztą elektroniczną np. gróźb – jak wychwycić informacje o prawdziwym nadawcy z nagłówków poczty, jak dowiedzieć się nieco więcej o nim na podstawie wychwyconych informacji oraz gdzie i w jaki sposób zgłosić przewinienie.

Powinieneś wiedzieć...

- znać podstawy funkcjonowania poczty elektronicznej,
- wiedzieć, jak odczytać pełne nagłówki listu w swoim programie pocztowym.

Podstawy

Listing 1. *Pogróżki od Misia*

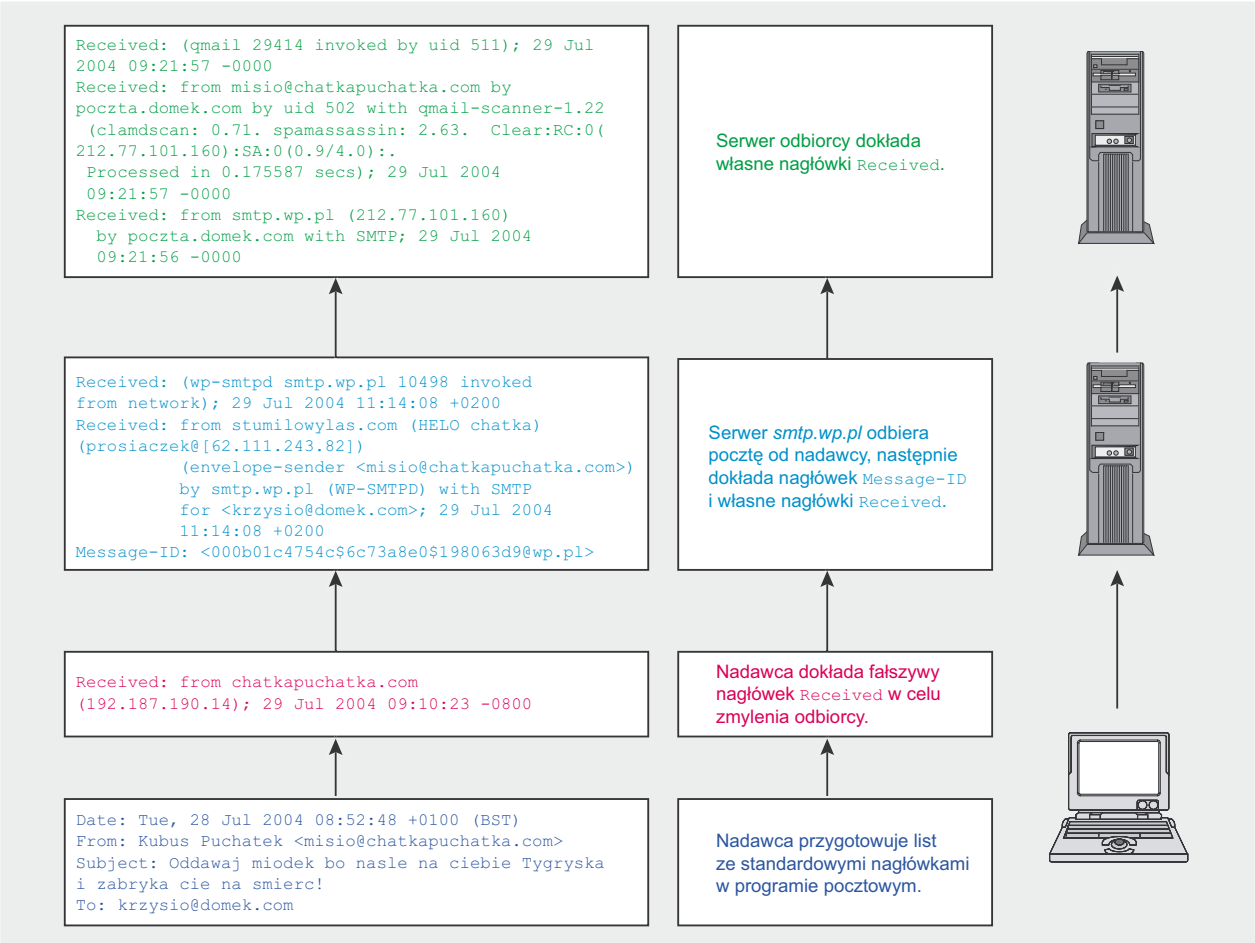
```
Return-Path: <misio@chatkapuchatka.com>
Delivered-To: krzysio@domek.com
Received: (qmail 29414 invoked by uid 511); 29 Jul 2004 09:21:57 -0000
Received: from misio@chatkapuchatka.com by poczta.domek.com
 by uid 502 with qmail-scanner-1.22
 (clamdscan: 0.71. spamassassin: 2.63.
 Clear:RC:0(212.77.101.160):SA:0(0.9/4.0):.
 Processed in 0.175587 secs); 29 Jul 2004 09:21:57 -0000
Received: from smtp.wp.pl (212.77.101.160)
  by poczta.domek.com with SMTP; 29 Jul 2004 09:21:56 -0000
Received: (wp-smtpd smtp.wp.pl 10498 invoked from network);
          29 Jul 2004 11:14:08 +0200
Received: from stumilowylas.com (HELO chatka) (prosiaczek@[62.111.243.82])
          (envelope-sender <misio@chatkapuchatka.com>)
          by smtp.wp.pl (WP-SMTPD) with SMTP
          for <krzysio@domek.com>; 29 Jul 2004 11:14:08 +0200
Message-ID: <000b01c4754c$6c73a8e0$198063d9@wp.pl>
Received: from chatkapuchatka.com (192.187.190.14); 29 Jul 2004 09:10:23 -0800
Date: Tue, 28 Jul 2004 08:52:48 +0100 (BST)
From: Kubus Puchatek <misio@chatkapuchatka.com>
Subject: Oddawaj miodek bo nasle na ciebie Tygryska i zabryka cie na smierc!
To: krzysio@domek.com
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="0-183171874-1090572768=:27263"
Content-Transfer-Encoding: 8bit
(...)
```

Nagłówki Received

Nagłówki `Received` są dodawane automatycznie przez każdy serwer pocztowy, przez który przechodzi wiadomość. Ich zadaniem jest dokładne zobrazowanie drogi, jaką podążała wiadomość.

Każdy nowy nagłówek `Received` dokładany jest nad istniejącymi. Tak więc, aby prześledzić trasę wiadomości, należy je odczytywać z dołu do góry. Pierwszy (górny) nagłówek `Received` będzie więc pochodził od naszego serwera, zaś ostatni (dolny) – od serwera nadawcy. Przynajmniej teoretycznie, bowiem serwery nie usuwają żadnych nagłówków – nic więc nie stoi na przeszkodzie, by nadawca dodał własne, mające na celu zmylenie odbiorcy. Proces dodawania nagłówków `Received` przedstawiamy na Rysunku 1.

Na Listingu 1 przedstawiono nagłówki listu z pogróżkami, które wydają się pochodzić od Kubusia Pu-



Rysunek 1. *Proces dokładania nagłówków do listu*

chatka. Przeanalizujmy je dokładnie, by przekonać się, czy jest on faktycznym nadawcą tego listu.

Analiza nagłówków Received

Ostatnim nagłówkiem `Received` jest:

```
Received:
  from chatkapuchatka.com
  (192.187.190.14);
  29 Jul 2004 09:10:23 -0800
```

Wszystko wskazuje na to, że nadawca listu skorzystał z komputera o adresie IP 192.187.190.14. Adres symboliczny (*chatkapuchatka.com*) możemy pominąć – mógłby zostać sfałszowany, dlatego lepiej oprzeć się na adresie w formie liczbowej.

Zanim jednak dowiemy się czegoś więcej o adresie IP 192.187.190.14 i wyślemy Kłapouchego na odsiecz do chatki Kubusia Puchatka, poświęćmy jednak chwilę na analizę dalszych nagłówków. Oto drugi od dołu nagłówek `Received`:

```
Received:
  from stumilowylas.com
  (HELO chatka)
  (prosiaczek@[62.111.243.82])
  (envelope-sender
  <misio@chatkapuchatka.com>)
  by smtp.wp.pl (WP-SMTPD) with SMTP
  for <krzysio@domek.com>;
  29 Jul 2004 11:14:08 +0200
```

Serwery pocztowe mają w zwyczaju przekazywać list jak najkrótszą drogą. Wydaje się więc podejrzane, że *chatkapuchatka.com*, zamiast wysłać list bezpośrednio do *smtp.wp.pl*, przekazał go wcześniej do *stumilowylas.com*.

Obejrzyjmy ponownie nagłówki `Received`. Zauważymy, że ostatni z nich znajduje się za nagłówkiem `Message-ID`, a nie przed nim, jak pozostałe. Nagłówek `Message-ID` jest jednak dodawany albo przez program pocztowy nadawcy albo przez serwer, który odebrał wiadomość od nadawcy (jeśli list nie miał jeszcze tego nagłówka). Nie jest więc możliwe, by był on umieszczony powyżej istniejącego nagłówka `Received`, który jest dodawany przez serwer po wcześniejszym nadaniu `MessageID`.

Na podstawie powyższych faktów (niewytłumaczalnej kolejności przekazywania listu i dziwnej lokalizacji nagłówka) można się domyślić, że ostatni nagłówek `Received` jest sfałszowany – dodany przez samego autora listu w celu zmylenia odbiorcy. Możemy więc go pominąć i skoncentrować się na drugim od dołu.

W drugim od dołu nagłówku widzimy dwie części: `from` i `by`, czyli odpowiednio *otrzymane od* i *otrzymane przez*. Interesuje nas oczywiście część *otrzymane od*, w której widzimy:

- `from stumilowylas.com` – adres symboliczny, który możemy pominąć w dalszej analizie – lepiej korzystać z adresu w formie liczbowej,

Informacje w nagłówkach X

Użyteczne informacje możemy czasem także znaleźć w nagłówkach zaczynających się od `X-`. Dzieje się tak szczególnie w przypadku, jeśli nadawca do wysłania wiadomości skorzystał ze strony internetowej, a nie programu pocztowego i protokołu SMTP. Oprogramowanie umożliwiające użytkownikom kont pocztowych dostęp przez WWW zazwyczaj automatycznie dodaje nagłówki informujące o adresie IP, z którego nawiązano połączenie ze stroną. Często informacje te są zawarte w samych nagłówkach `Recived` (na przykład `Received: from ... by ... via HTTP`); jeśli jednak nie, znajdziemy je właśnie w nagłówkach `X-...`.

Niestety, nie ma żadnego standardu obowiązującego nazewnictwo tych nagłówków. Dlatego też pozostaje nam tylko ich dokładna analiza i szukanie nazwy sugerującej, że może zawierać adres IP nadawcy (przykłady: `X-External-IP`, `X-IP`).

Regionalne rejestry internetowe

Adresami IP przydzielanymi dostawcom usług internetowych zarządza ogólnoświatowa organizacja IANA (*Internet Assigned Numbers Authority*). Rozdziela ona zakresy IP do wykorzystania na cztery regionalne organizacje, działające w określonych rejonach świata. Z kolei organizacje te, zwane regionalnymi rejestrami internetowymi (*Regional Internet Registry*, RIR), przyznają zakresy IP dostawcom usług internetowych. Tak więc, jeśli dostawca usług internetowych potrzebuje zakresu IP dla swoich klientów, zwraca się do odpowiedniego (w zależności od położenia geograficznego dostawcy) rejestru z prośbą o przyznanie nowych adresów.

Rejestry dysponują też bazami danych zawierającymi informacje na temat właścicieli. Dane te z kolei są uzupełniane przez samych dostawców. Tak więc na pewno w rejestrze można znaleźć informacje na temat samego dostawcy odpowiedzialnego za dany zakres IP, a czasem także wprowadzone przez dostawcę informacje na temat klienta. Dzięki temu możliwe jest łatwe zlokalizowanie osoby odpowiedzialnej za dane IP.

Cztery obecnie funkcjonujące regionalne rejestry to:

- ARIN (*http://www.arin.net*) – *American Registry for Internet Numbers*, działająca na terenie USA, Kanady i południowej Afryki,
- APNIC (*http://www.apnic.net*) – *Asia Pacific Network Information Centre*, działająca na terenie Azji południowo-wschodniej, Australii i Oceanii,
- LACNIC (*http://www.lacnic.net*) – *Latin America and Caribbean IP Address Regional Registry,* działająca na terenie Ameryki Łacińskiej (Meksyk, Ameryka Środkowa, Ameryka Południowa),
- RIPE NCC (*http://www.ripe.net*) – *Réseaux IP Européens Network Coordination Centre*, działająca na terenie Europy, Bliskiego Wschodu, północnej Afryki i północno-zachodniej Azji.

W niedługiej przyszłości zacznie działać AfricNIC (*http://www.afrinic.net/*), który przejmie od pozostałych rejestrów odpowiedzialność za adresy IP w Afryce. Kraje podlegające poszczególnym rejestrom można znaleźć w informacjach zawartych na stronach rejestrów.

- `(HELO chatka)` – słowo kluczowe `HELO` wskazuje na to, że ciąg występujący po nim został podany podczas sesji SMTP (przy wysyłaniu poczty) jako parametr instrukcji `HELO` – to z kolei sugeruje, że komputer nadawcy nazywa się *chatka* (programy pocztowe jako parametr `HELO` najczęściej podają nazwę komputera, np. z NetBiosu),
- `(prosiaczek@[62.111.243.82])` – ten fragment nagłówka zawiera dwie bardzo istotne informacje; po pierwsze – adres IP, z którego dotarła wiadomość, po drugie – ciąg występujący przed znakiem `@` to nazwa użytkownika podana podczas autoryzacji SMTP. Niestety, ten element jest dostępny w praktyce tylko wtedy, gdy serwerem, który odebrał pocztę od nadawcy był *qmail* z łatką SMTP AUTH. Co prawda w *Eximie* także istnieje możliwość samodzielnej definicji nagłówków, ale w domyślnych nie ma nazwy autoryzowanego użytkownika.

Analiza nagłówków naprowadziła nas już na trop winowajcy. Wiemy, że list został wysłany z komputera o adresie IP 62.111.243.82 i że prawdziwy login użytkownika na serwerze *wp.pl* to... *prosiaczek*. Mamy więc podejrzanego o podszywanie się pod Kubusia Puchatka i wysyłanie pogróżek. Zobaczmy, czego więcej możemy dowiedzieć się o jego adresie IP.

Co mówi IP

Aby dowiedzieć się nieco więcej o IP uzyskanym podczas analizy nagłówków, możemy zastosować jedno z podstawowych narzędzi dostępnych w systemie Linux, lub też, jeśli nie dysponujemy maszyną linuksową, skorzystać z mechanizmów dostępnych na stronach WWW. W obu przypadkach będziemy pobierać informacje z bazy danych regionalnego rejestru internetowego (patrz Ramka *Regionalne rejestry internetowe*).

Uzyskanie informacji z rejestru polega na wykonaniu dwóch kroków:

Listing 2. *Zapytanie whois.arin.net o adres 62.111.243.82*

```
[whois.arin.net]
OrgName:    RIPE Network Coordination Centre
OrgID:      RIPE
(...)
ReferralServer: whois://whois.ripe.net:43
(...)
```

Listing 3. *Zapytanie whois.ripe.net o adres 62.111.243.82*

```
[whois.ripe.net]
(...)
remarks:      All abuse reports orginated from CDP network: abuse@cdp.pl
(...)
person:       ADAM GODLEWSKI
address:      SOFTWARE - WYDAWNICTWO SP. Z O.O.
address:      LEWARTOWSKIEGO JOZEFA 6
address:      WARSZAWA
address:      POLAND
phone:        +48 (22) 860 18 81
fax-no:       +48 (22) 860 17 71
(...)
person:       Aleksander Cesarz
address:      CROWLEY DATA POLAND Sp. z o.o.
address:      ul. Stawki 2
address:      00-193 Warszawa
address:      POLAND
phone:        +48 22 8606960
fax-no:       +48 22 6351400
e-mail:       acesarz@cdp.pl
(...)
person:       Przemyslaw Mujta
(...)
person:       Grzegorz Swiderek
(...)
```

- ustaleniu, który z czterech rejestrów jest odpowiedzialny za dany adres IP,
- sformułowania zapytania do rejestru.

Połączmy te kroki, zadając zapytanie dowolnej z czterech baz, za pomocą narzędzia *whois*. Adres bazy whois otrzymujemy zamieniając człon `www` w adresie strony rejestru na `whois`. Opcja `-h` w programie *whois* umożliwia określenie serwera whois, z którego chcemy pobrać informacje.

```
$ whois -h whois.arin.net 62.111.243.82
```

W zamian otrzymamy informację, że adres IP należy do zakresu, którym administruje RIPE NCC (patrz Listing 2). Możemy więc zadać to samo zapytanie, tym razem RIPE NCC:

```
$ whois -h whois.ripe.net 62.111.243.82
```

Skrócony rezultat przedstawiono na Listingu 3.

Jeśli nie mamy dostępu do maszyny linuksowej, możemy uzyskać te same dane za pomocą oficjalnych witryn internetowych rejestrów (każda z nich oferuje możliwość zadania pytania przez formularz WWW).

Najbardziej interesującymi elementami otrzymanych danych są fragmenty zaczynające się od nagłówka `person` – są to osoby odpowiedzialne za dany adres IP. Oczywiście są to administratorzy łacza, a nie jego użytkownicy – nie możemy więc wnioskować, że za podszywanie się pod Kubusia Puchatka odpowiedzialna jest jedna z wymienionych osób. Dzięki uzyskanym danym możemy jednak upewnić się, że nadawca wiadomości zdecydowanie nie był Kubusiem Puchatkiem (oczywiście zakładając, że wiemy, iż Kubuś Puchatek nie pracuje w Wydawnictwie Software ani

w Crowley Data Poland) oraz przesłać w stosowne miejsce prośbę o zdemaskowanie i wyciągnięcie konsekwencji wobec osoby faktycznie odpowiedzialnej za groźby.

Zgłaszanie przewinienia

Wiemy już wystarczająco dużo na temat nadawcy wiadomości, by móc zgłosić jego przewinienie i oczekiwać, że zostaną wyciągnięte odpowiednie konsekwencje. W pierwszej kolejności powinniśmy zgłosić nadużycie osobom odpowiedzialnym za adres IP, z którego wysłano list. Kontakt do tych osób znaleźliśmy za pomocą *whois*.

Nie należy jednak wysyłać raportu pod wszystkie znalezione adresy – najpierw należy spróbować wyszukać adres jednostki odpowiedzialnej u danego dostawcy za nadużycia. Jest to w znakomitej większości przypadków (a przynajmniej powinien być) adres *abuse*. Dopiero gdy w otrzymanych danych nie znajdziemy takiego adresu, skorzystajmy z innych adresów.

W naszym przypadku w otrzymanych danych wyraźnie widzimy rekord:

```
remarks: All abuse reports
  orginated from CDP network:
  abuse@cdp.pl
```

Tak więc raport powinniśmy wysłać pod adres *abuse@cdp.pl*.

Dodatkowo – jak pamiętamy – zauważyliśmy w nagłówkach, że nadawca wiadomości skorzystał z uwierzytelnienia SMTP AUTH na serwerze *wp.pl* – zalogował się na konto *prosiaczek*. Możemy więc złożyć raport także do *wp.pl*. Raport wyślijmy na adres *abuse@wp.pl*, jako że istnieje formalny obowiązek istnienia tego adresu dla każdej domeny, w której istnieje serwer pocztowy (patrz Ramka *RFC a adres abuse*).

Jak sformułować raport

Aby zwiększyć szanse na to, że administrator potraktuje poważnie nasz raport, warto przestrzegać kilku zasad podczas jego przygotowywania:

- absolutnie niezbędne jest przesłanie wszystkich nagłówków, a najlepiej całej otrzymanej wiadomości (np. jako załącznik MIME) – bez nich nasz raport nie będzie wiarygodny,
- warto na początku raportu wyjaśnić, z jakiego powodu został przesłany pod dany adres (na przykład informując, że adres został zidentyfikowany na podstawie wpisu w bazie whois i IP nadawcy z nagłówka `Received`) – zwiększy to naszą wiarygodność, wzkazując na to, że adres przesłania raportu nie był przypadkowy,
- lepiej przesłać raport pod mniejszą liczbę adresów, niż pod adresy źle wybrane; w przypadku wysyłania pod wiele adresów jednocześnie, lepiej wysłać list oddzielnie pod każdy z nich (nie stosować ani CC, ani BCC) – zbyt duża liczba odbiorców wskazuje na to, że nie wiemy do kogo zgłosić przewinienie,
- warto określić na początku raportu wagę przewinienia – np. w przypadku otrzymanych mailem gróźb można powołać się na fakt, iż jest to przestępstwo z art. 190§1 Kodeksu karnego – może to spowodować, że nasz raport zostanie potraktowany jako priorytetowy.

Tekst przykładowego raportu przedstawiamy na Listingu 4.

Niestety, trzeba liczyć się z tym, że nasz raport może pozostać bez odpowiedzi. Większość firm przykłada małą wagę do przesyłanych im raportów o nadużyciach. Oczywiście, jeśli raport e-mailowy pozostanie bez odpowiedzi, możemy skontaktować się z dostawcą telefonicznie – na podstawie numerów pozostawionych w bazie whois. Praktyka wykazuje, że kontakt telefoniczny jest zazwyczaj skuteczniejszy. Miejmy jednak nadzieję, że z czasem kontakty e-mailowe będą traktowane co najmniej równie poważnie, jak telefoniczne – szczególnie przez firmy, które utrzymują się ze świadczenia usług internetowych. ■

Listing 4. *Przykładowy raport*

```
From: Krzysio <krzysio@domek.com>
To: abuse@cdp.pl
Subject: Raport - grozba karalna od Panstwa klienta

Szanowni Państwo,
dnia 29 lipca 2004 roku otrzymałem list zawierający groźbę karalną
(przestępstwo z art. 190§1 Kodeksu karnego). Przesyłam ten list do
Państwa, ponieważ na podstawie analizy nagłówków Received określiłem,
iż list został wysłany z łącza, za które Państwo są odpowiedzialni,
z adresu IP 62.111.243.82. Państwa adres pobrałem z bazy whois.ripe.net.
Proszę o zbadanie sprawy i odpowiedź. Jako dowód, przesyłam nagłówki
i otrzymany list (ostatni nagłówek Received jest sfałszowany).
```

RFC a adres abuse

RFC2142 z maja 1997 roku jest pierwszym dokumentem, w którym formalnie określono obowiązek utrzymania adresu *abuse* w domenie, jeśli funkcjonuje w niej poczta elektroniczna. Wcześniej było to uznawane za dobry zwyczaj, ale nie było takich wymagań formalnych.

Niestety, nie każdy administrator serwera pocztowego wie o istnieniu tego wymogu. Dlatego też możemy natrafić na serwer, który nie przyjmie naszej poczty wysłanej na adres *abuse*. Istnieje jednak drugi, starszy i o wiele częściej przestrzegany wymóg dotyczący innego adresu: *postmaster* – tak więc, jeśli nasz raport nie zostanie dostarczony pod adres *abuse*, możemy przekazać go pod adres *postmaster*, jednocześnie informując administratora o obowiązku utrzymania adresu *abuse*.

Jeśli jednak administrator zignoruje naszą prośbę, lub też list nie dojdzie nawet na adres *postmaster*, możemy zgłosić ten fakt w serwisie *http://www.rfc-ignorant.org*, który przechowuje listę firm i instytucji ignorujących standardy obowiązujące w Internecie, w tym także listę serwerów pozbawionych adresów *abuse* lub *postmaster*.