



A więc stało się! Spam dotarł i do mnie.



Spam w sieci nie jest czymś nowym. Codziennie na moje skrzynki mailowe @o2.pl, @wp.pl, oraz @gmail.com przychodzi kilkanaście wiadomości od Banków, specjalistów od powiększania męskości lub zawierające inne cudowne okazje i oferty. Jednakże to, co dzieje się od około miesiąca jest ciekawe i zastanawiające.

Jak już pisałem, przeniósłem swój hosting do firmy az.pl. Zrobiłem to z kilku powodów między innymi była to większa ilość baz danych i przestrzeni. Ku mojemu zdziwieniu zacząłem otrzymywać maile w ilościach masowych o zabawnej treści:



A więc stało się! Spam dotarł i do mnie.

	Temat	Indywidual	Data
☆	Re: Dodac tysiecy dolarów	• Andrzej Sirota	• 2015-06-17 16:43
☆	Re: Dowiedz sie TERAZ- jaka jest PRAWDZIWA darmowa droga, aby ...	• Antoni Pawlus	• 2015-06-15 04:27
☆	Re: Zdobadz 595 Euro w 20 minut!	• Bartłomiej Zysk	• 2015-06-27 19:56
☆	Re: Bogaci sa bogaci, bo ...	• Boleslaw Klebba	• 2015-06-17 21:28
☆	Re: Ogromne dochody bez inwestycji	• Boleslaw Sarnecki	• 2015-06-26 14:59
☆	Dowiedz sie TERAZ- jaka jest PRAWDZIWA darmowa droga, aby stac...	• Cyryl Dobrowolski	• 2015-06-17 12:10
☆	Najlepszym sposobem, aby uczynic cie bogatym	• Cyryl Wawrzyniak	• 2015-06-14 06:58
☆	Re: Dodatkowe dochody	• Czeslaw Grzegorzewski	• 2015-06-27 14:57
☆	Potrzebujesz gotówki?	• Czeslaw Ludwiczak	• 2015-06-16 12:17
☆	Re: formula sukcesu jest znalezc	• Daniel Dudek	• 2015-06-21 00:25
☆	Re: Zarabijaj pieniadze w internecie	• Dariusz Laszewski	• 2015-06-18 12:19
☆	Czlowiek z Niemiec podzielim sie swoim finansowym sekretem.	• Dariusz Stempien	• 2015-06-22 11:32
☆	Re: Pospiesz sie, aby stac sie bogatym, dopóki jest taka szansa.	• Dariusz Watroba	• 2015-06-22 02:39
☆	Re: Dlaczego bogaci moga obejsc system? Sekret bankowy zostal uja...	• Edward Golaszewski	• 2015-06-17 00:00
☆	Potrzebujesz gotówki?	• Eryk Kawczynski	• 2015-06-17 13:41
☆	Przypomnienie: Edward Saint Skamor zaprosil(a) Cie do społeczności...	• Facebook	• 2015-06-17 05:27

Od Edward Golaszewski <Golaszewski82@hotelkorona.pl>☆

Temat **Re: Dlaczego bogaci moga obejsc system? Sekret bankowy zostal ujawniony!** 2015-06-17 00:00

Do Ja <pht@s-m-s.org.pl>☆

Konkursy Forex- zacznij od zera! Unikalne konkursy- rozpocznij trading bez inwestowania prawdziwych pieniedzy!
<http://cc4.co/QCROT>

Linki które zawierają owe wiadomości kierują do ciekawej strony:



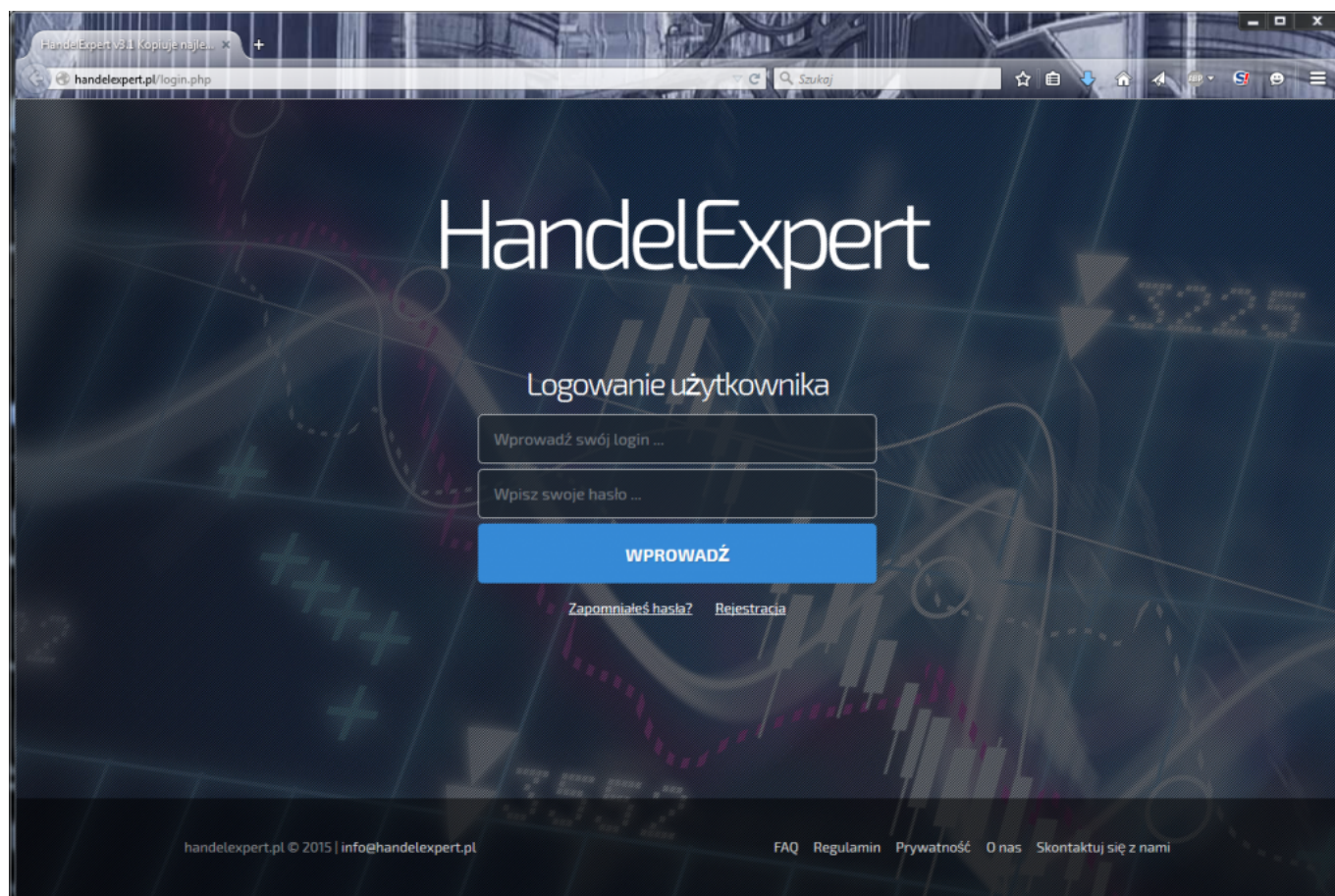
A więc stało się! Spam dotarł i do mnie.

The screenshot shows a web browser window with the URL 'spienid.ru'. The page features a background image of a person in a suit with their hands behind their head, looking out over a landscape. The main heading is 'Robot binarny do automatycznego zarabiania'. To the right, it says 'System, który pozwoli Ci zarobić na aukcjach handlowych, bez specjalnej wiedzy.' Below this is a large section titled 'Nasze sukcesy są w naszych rękach' with the subtext 'Aby coś osiągnąć, po prostu trzeba zacząć coś robić'. A registration form is present with fields for 'Wpisz swoje imię i nazwisko' and 'Wpisz swój e-mail', and a green button labeled 'Szybka rejestracja'. On the left, there is a section titled 'Rejestracja Pozostało' with a large orange circle containing the number '28' and the text 'Niestety, ilość darmowych rejestracji jest ograniczona'. At the bottom, there are two columns: 'Każdy może osiągnąć sukces' and 'Jak mogę uzyskać dostęp?'.

Każdy odsyłacz na tej stronie prowadzi do polsko brzmiącej strony handlexpert.pl.



A więc stało się! Spam dotarł i do mnie.



Postanowiłem co nieco poczytać na temat samego HandelExpert jak i spienid.ru. Pierwszą czynnością jaką zrobiłem to sprawdzenie jakie adresy IP odpowiadają przy pingowaniu tych domen.

```
C:\Windows\system32\cmd.exe

C:\Users\pht>ping spienid.ru

Pinging spienid.ru [103.253.99.165] with 32 bytes of data:
Reply from 103.253.99.165: bytes=32 time=402ms TTL=48
Reply from 103.253.99.165: bytes=32 time=353ms TTL=48
Reply from 103.253.99.165: bytes=32 time=393ms TTL=48
Reply from 103.253.99.165: bytes=32 time=351ms TTL=48

Ping statistics for 103.253.99.165:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 351ms, Maximum = 402ms, Average = 374ms

C:\Users\pht>ping handelexpert.pl

Pinging handelexpert.pl [87.249.215.204] with 32 bytes of data:
Reply from 87.249.215.204: bytes=32 time=147ms TTL=49
Reply from 87.249.215.204: bytes=32 time=186ms TTL=49
Reply from 87.249.215.204: bytes=32 time=145ms TTL=49
Reply from 87.249.215.204: bytes=32 time=183ms TTL=49

Ping statistics for 87.249.215.204:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 145ms, Maximum = 186ms, Average = 165ms

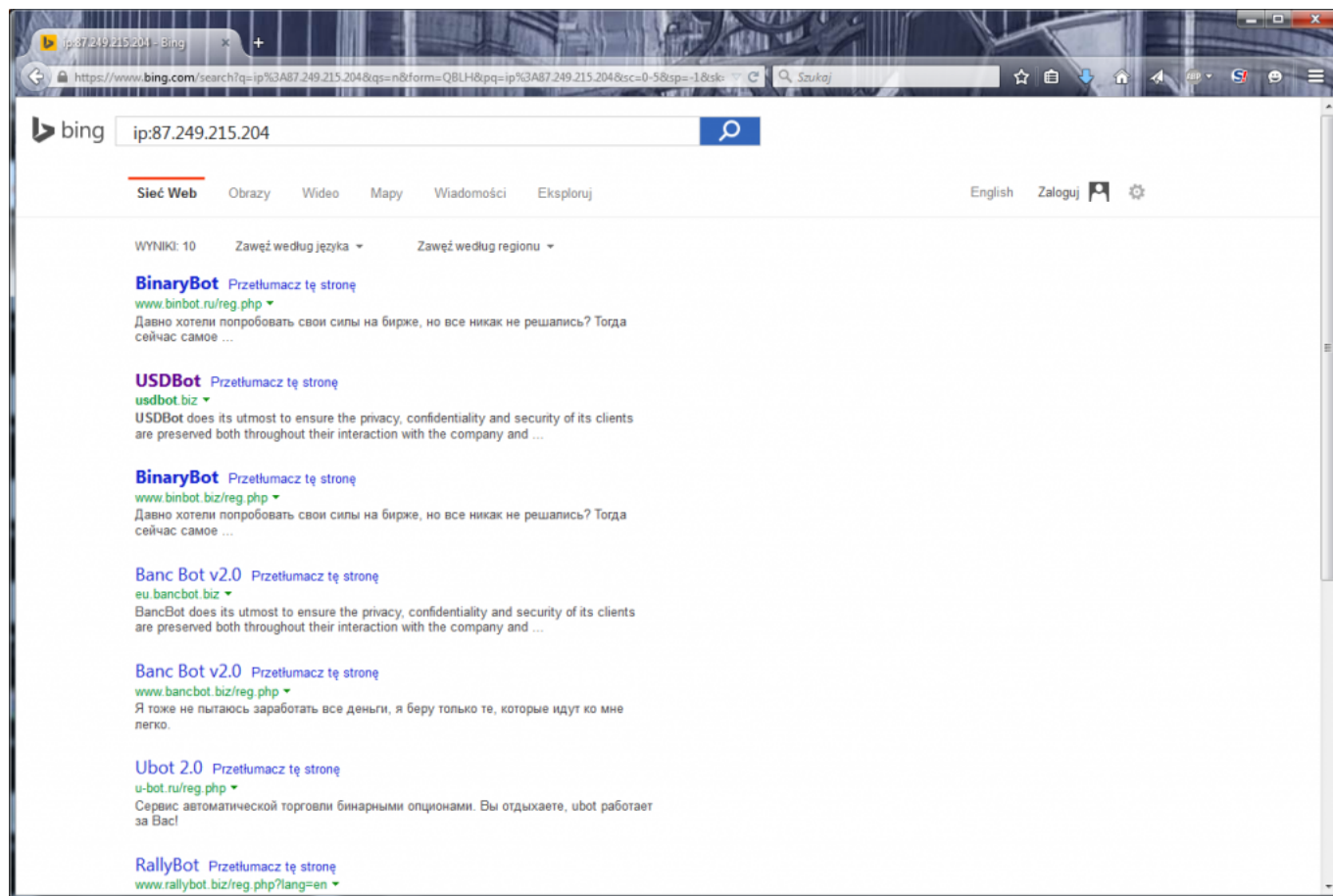
C:\Users\pht>
```

Użyłem

klasycznego zagrania - „ip:<adres ip>” w wyszukiwarce bing by sprawdzić jakie jeszcze strony znajdują się na tych serwerach.

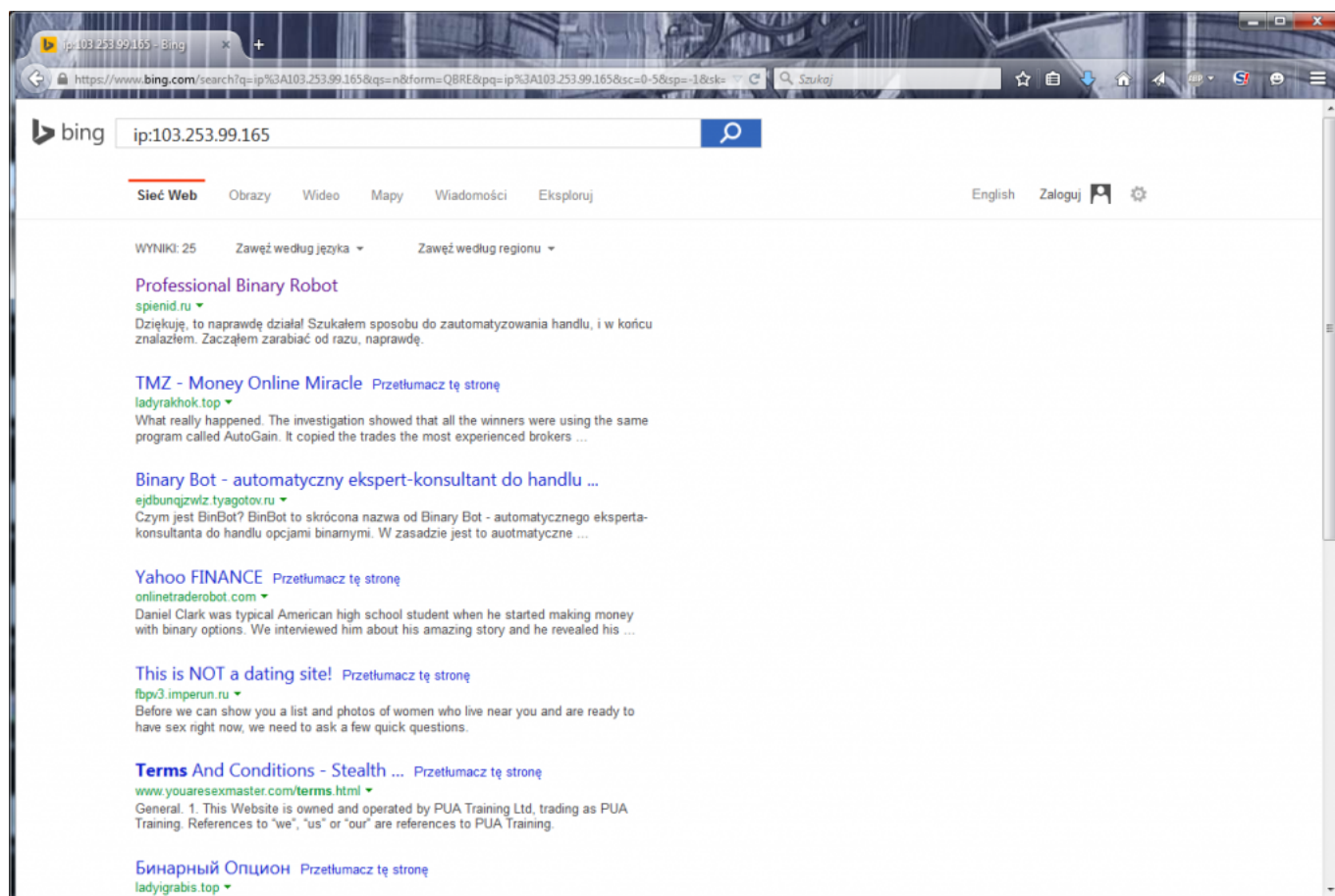


A więc stało się! Spam dotarł i do mnie.





A więc stało się! Spam dotarł i do mnie.



Oczywiście wyniki niebyły zbyt zadziwiające. No, prócz strony *fbpv3.imperun.ru*. Szczerze mówiąc nie spodziewałem się strony porno wśród botów „finansowych”. Jak widać nasi przyjaciele z wschodu pragną zaspokajać wszystkie potrzeby internauty. Wiadomo, aby umawiać się na randki, trzeba mieć pieniędzy, a więc kochani Rosjanie dają nam szansę zarobić ale i okazje by wydać. Ale! Czas przyjrzeć się wpisom w WhoIs.



A więc stało się! Spam dotarł i do mnie.

```
root@zuo: ~  
root@zuo:~# whois handelexpert.pl  
  
DOMAIN NAME:          handelexpert.pl  
registrant type:      individual  
nameservers:          dns1.yandex.ru.  
                     dns2.yandex.ru.  
created:              2015.05.26 13:09:14  
last modified:        2015.05.26 13:09:14  
renewal date:         2016.05.26 13:09:14  
  
no option  
  
dnssec:               Unsigned  
  
REGISTRAR:  
EPAG Domainservices GmbH  
Customer Support  
Niebuhrstrasse 16B  
53113 Bonn  
Niemcy/Germany  
phone:+49.2283296840  
fax:+49.2283296849  
support@epag.de  
  
WHOIS database responses: http://www.dns.pl/english/opiskomunikatow\_en.html  
  
WHOIS displays data with a delay not exceeding 15 minutes in relation to the .pl Registry system  
Registrant data available at http://dns.pl/cgi-bin/en\_whois.pl  
root@zuo:~# whois spienid.ru  
% By submitting a query to RIPN's Whois Service  
% you agree to abide by the following terms of use:  
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)  
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).  
  
domain:              SPIENID.RU  
nserver:             ns1.spienid.ru. 109.201.133.194  
nserver:             ns2.spienid.ru. 62.75.253.97  
state:               REGISTERED, DELEGATED, VERIFIED  
person:              Private Person  
registrar:           R01-RU  
admin-contact:      https://partner.r01.ru/contact\_admin.khtml  
created:             2015.05.12  
paid-till:           2016.05.12  
free-date:           2016.06.12  
source:              TCI  
  
Last updated on 2015.07.01 06:26:34 MSK
```

Jak narazie wszystko się potwierdza. Domena handelexpert.pl oraz spienid.ru podpięta do rosyjskich serwerów DNS. Ciekawostka jest fakt, iż „polska” domena handelexpert.pl, która odnosi się do dns*.yandex.ru jest zarejestrowana u niemieckiego rejestratora domen. Można by zażartować, że historia lubi się powtarzać.



KAROL HOLUB FOT. LASKI DIFFLSION 28 WRZEŚNIA 1939: PODPISANIE PAKTU NIEMIECKO-ROSYJSKIEGO. PODPISUJE WACŁESŁAW MOŁOTOW, ZA NIM DO LEWEJ JOACHIM VON RIBBENTROP.

Postanowił

em przeczytać regulamin HandelExpert, aby znaleźć dodatkowe smaczki.

WYBÓR PRAWA I JURYSDYKCJI

Wszelkie spory, kontrowersje lub różnice, które mogą powstać między stronami w odniesieniu do lub w związku z niniejszą Umową zostaje nieodwołalnie poddane wyłącznej jurysdykcji sądów w **Łotwie** z wyłączeniem wszelkich innych sądów i bez prawa do roszczeń w wyniku kolizji z prawem w innych krajach.

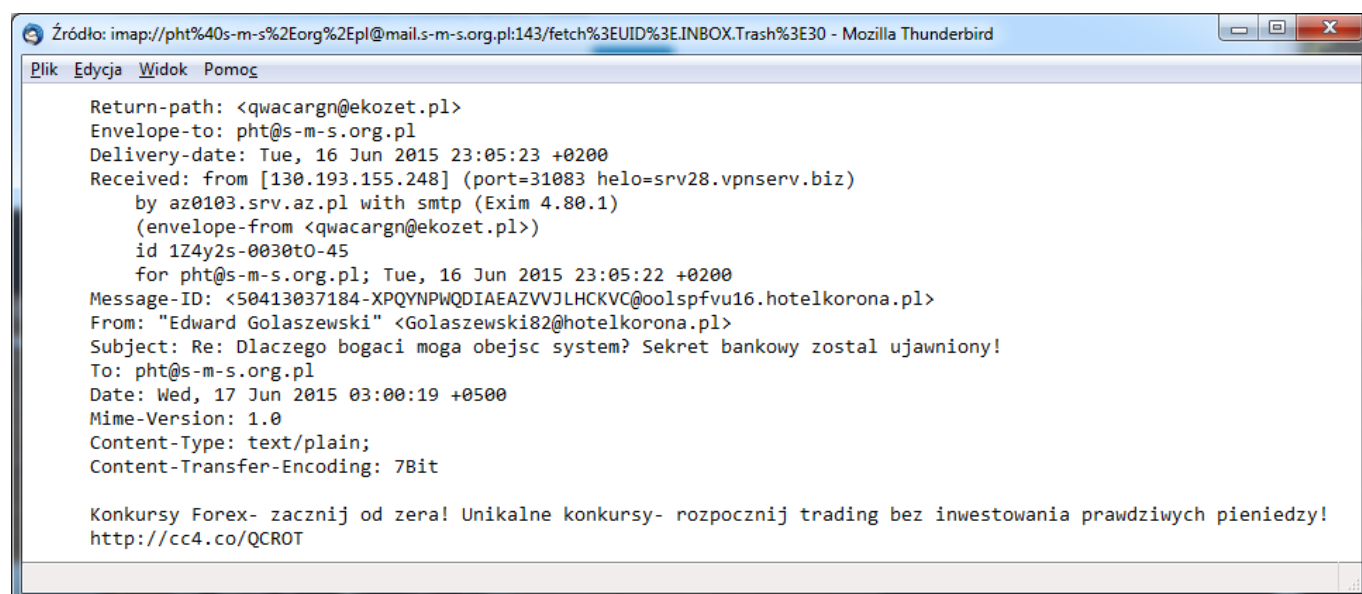
No! To teraz się robi ciekawie. Skoro właściciel strony powołuje się na sądy na Łotwie, można przypuszczać, iż tam znajduje się jego siedziba i tam prowadzi działalność gospodarczą. W internecie jest sporo stron, naruszających zasady moralne (showup.tv) lub polskie prawo (wszelakie strony z substancjami zakazanymi np kolekcjoner.nl). Podsumujmy więc dotychczasowy schemat działania.



A więc stało się! Spam dotarł i do mnie.

1. Osoba powołująca się na sądy na Łotwie tworzy bota do automatyzacji operacji na Utrader.com.
2. Rejestruje domenę .pl u niemieckiego rejestratora domen.
3. Deleguje domenę handlexpert.pl na rosyjskie serwery DNS: dns*.yandex.ru
4. Wysyła spam maile na adresy (nie wiadomo jak pozyskane) o różnej treści (do mnie dotarła polska treść powtarzająca się co x maili)

Dobra, przejdźmy do samych maili. tak wygląda pełen raw maila.



```
Źródło: imap://pht%40s-m-s%2Eorg%2Epl@mail.s-m-s.org.pl:143/fetch%3EUID%3EINBOX.Trash%3E30 - Mozilla Thunderbird
Plik Edycja Widok Pomoc
Return-path: <qwacargn@ekozet.pl>
Envelope-to: pht@s-m-s.org.pl
Delivery-date: Tue, 16 Jun 2015 23:05:23 +0200
Received: from [130.193.155.248] (port=31083 helo=srv28.vpnserv.biz)
  by az0103.srv.az.pl with smtp (Exim 4.80.1)
  (envelope-from <qwacargn@ekozet.pl>)
  id 1Z4y2s-0030t0-45
  for pht@s-m-s.org.pl; Tue, 16 Jun 2015 23:05:22 +0200
Message-ID: <50413037184-XPQYNPWQDIAEAZVVJLHCKVC@oolspfvu16.hotelkorona.pl>
From: "Edward Golaszewski" <Golaszewski82@hotelkorona.pl>
Subject: Re: Dlaczego bogaci mogą obejść system? Sekret bankowy został ujawniony!
To: pht@s-m-s.org.pl
Date: Wed, 17 Jun 2015 03:00:19 +0500
Mime-Version: 1.0
Content-Type: text/plain;
Content-Transfer-Encoding: 7Bit

Konkursy Forex- zacznij od zera! Unikalne konkursy- rozpocznij trading bez inwestowania prawdziwych pieniędzy!
http://cc4.co/QCROT
```

Jak się dokładnie przyjrzeć od razu widać kilka ciekawych rzeczy. Między innymi to iż mail zwrotny poszedł by do „qwacargn@ekozet.pl”, natomiast oficjalne „from” jest „Golaszewski82@hotelkorona.pl”. Mój serwer pocztowy dostał tą wiadomość od hosta o adresie IP 130.193.155.248 – czyli gdzieś z Kurdystanu!

Ale! No cóż wiele pisać. Ktoś pomyślał i trochę się nagłowił żeby przygotować tą akcje.

Ciekawszą akcją spamową za to jest akcja spamowa z darmową wymianą linków. Parę dni temu dostałem takiego o to maila:



A więc stało się! Spam dotarł i do mnie.

Od Julianna Ostrowska <julianna.ostrowska@plseo.org>☆
Temat: **zwiększyć ruch na Twojej stronie**
Do Ja <pht@s-m-s.pl>☆

Odpowiedz Przekaz Archiwizuj Niechciana Usun

2015-06-30 17:27

Inne ▾

Drogi webmasterze,

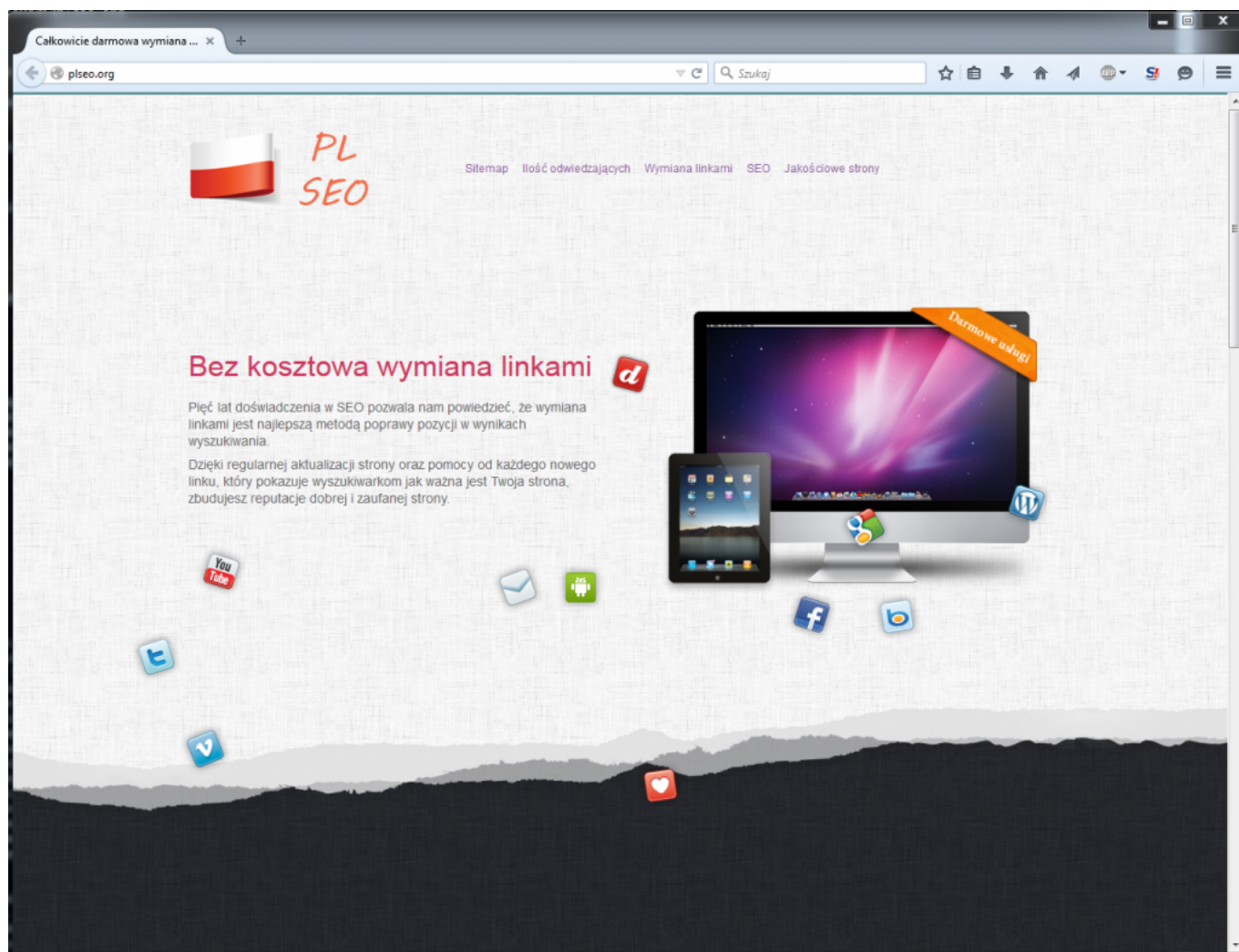
Wpadałam na Twoją stronę s-m-s.pl gdy przeczesałam internet i chciałabym zaproponować Ci wymianę linkami. Oferuję darmową, uczciwą i dającą wymierne korzyści metodę w zamian za link zwrotny.

Na <http://www.plseo.org/> znajdziesz wszystko, poczynwszy od przewodników dla początkujących do bardziej skomplikowanych tematów, które również pomogą zwiększyć ruch na Twojej stronie.

Wszystko to dostępne jest całkowicie za darmo.
Czekam na Twoją odpowiedź i opinię. Naprawdę liczę, że wymienimy się linkami.

Z poważaniem,
Julianna Ostrowska
<http://plseo.org/>

A więc, od początku. Strona plseo.org:



Wygląda całkiem polsko - nic bardziej mylnego. Zaczniemy od podstaw - whois.



A więc stało się! Spam dotarł i do mnie.



A więc stało się! Spam dotarł i do mnie.



A więc stało się! Spam dotarł i do mnie.



A więc stało się! Spam dotarł i do mnie.

Registrar Info

Name	Moniker Online Services LLC (R145-LROR)
Status	clientDeleteProhibited -- http://www.icann.org/epp#clientDeleteProhibited , clientTransferProhibited -- http://www.icann.org/epp#clientTransferProhibited , clientUpdateProhibited -- http://www.icann.org/epp#clientUpdateProhibited

Important Dates

Expires On	April 05, 2016
Registered On	April 05, 2012
Updated On	March 31, 2015

Name Servers

ns1.monikerdns.net	198.50.155.119
ns2.monikerdns.net	167.114.35.25
ns3.monikerdns.net	192.95.55.201
ns4.monikerdns.net	192.99.185.221

Raw Registrar Data

Registrant Contact Information:

Name: Anka Majewski
City: Rzeszow
State: Rzeszow
Zip: 35233
Country: PL
Phone: +48.797692356
Email: anka.najewski@plseo.org

Administrative Contact Information:

Name: Anka Majewski
City: Rzeszow
State: Rzeszow
Zip: 35233
Country: PL
Phone: +48.797692356
Email: anka.najewski@plseo.org

Technical Contact Information:

Name: Anka Majewski
City: Rzeszow
State: Rzeszow
Zip: 35233
Country: PL
Phone: +48.797692356
Email: anka.najewski@plseo.org



A więc stało się! Spam dotarł i do mnie.

jest zarejestrowana w stanach na polskie dane. Oczywiście, pogooglowałem trochę na temat strony plseo.org i nie tylko ja uznałem ich za spam. Cóż...

Ciekawostką jest, że „Anka Majewski”, a dokładnie konto powiązane z plseo.org na LinkedIn ma na profilowym zdjęcie rosyjskiej aktorki.

Kolejną ciekawostką jest fakt, że pod adresem ip na którym stoi plseo.org stoi całkowicie inna i niepowiązana strona. Czyżby ktoś miał dodatkowego admina o którym nie wie?

Morał z tego wszystkiego jest prosty. Spam będzie nas zalewać zawsze. Spam dostajemy do naszych skrzynek pocztowych na klatce, na ulicach wręczają nam ulotki. Spam on-line jest tylko kolejnym etapem zalewania nas niechcianą informacją handlową. Jedyne co możemy zrobić, to dostosowywać nasze filtry anty-spamowe i bronić się przed spamem.