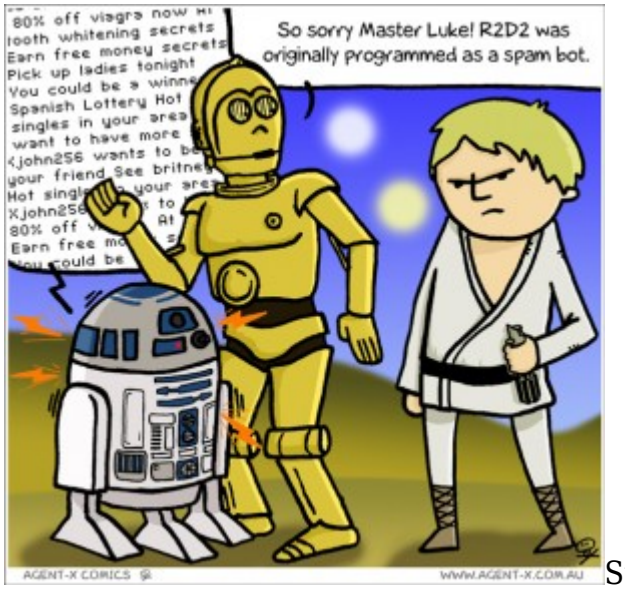
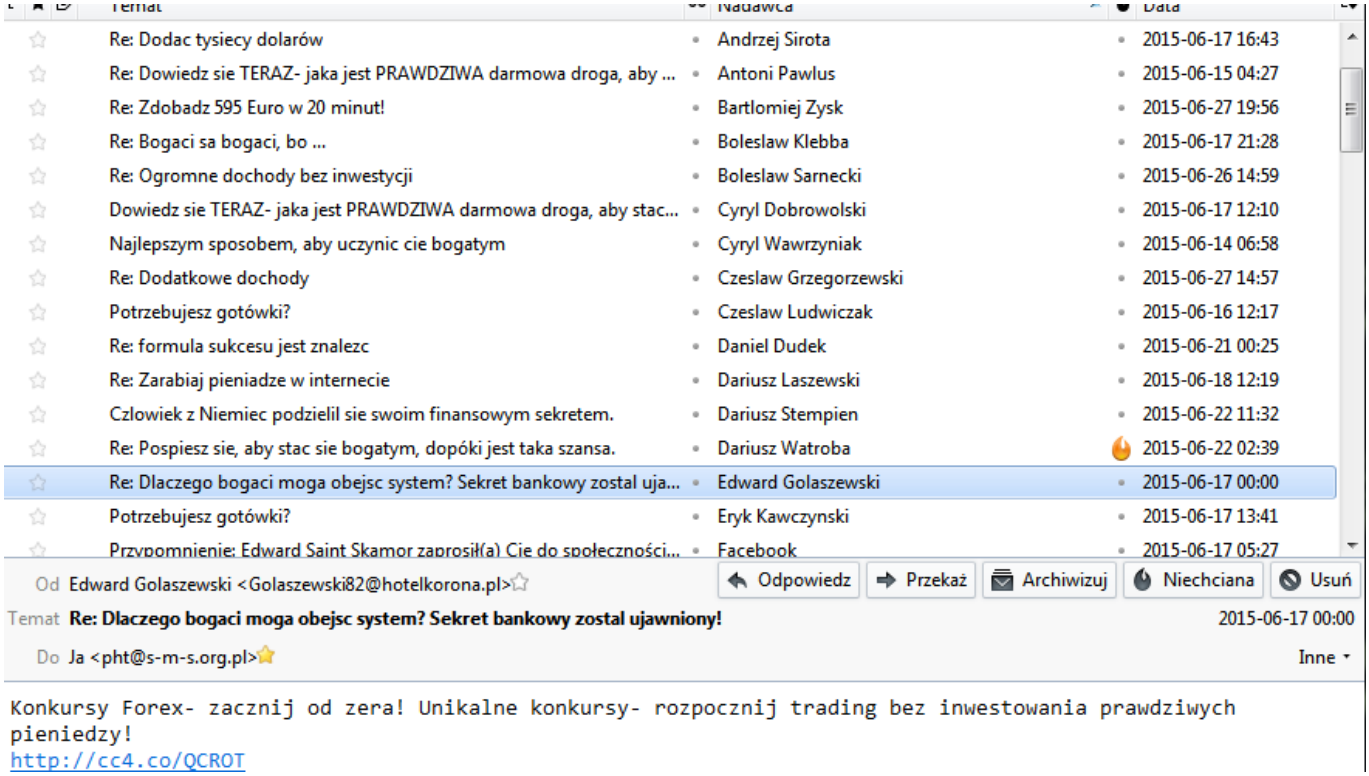
A więc stało się! Spam dotarł i do mnie.



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.

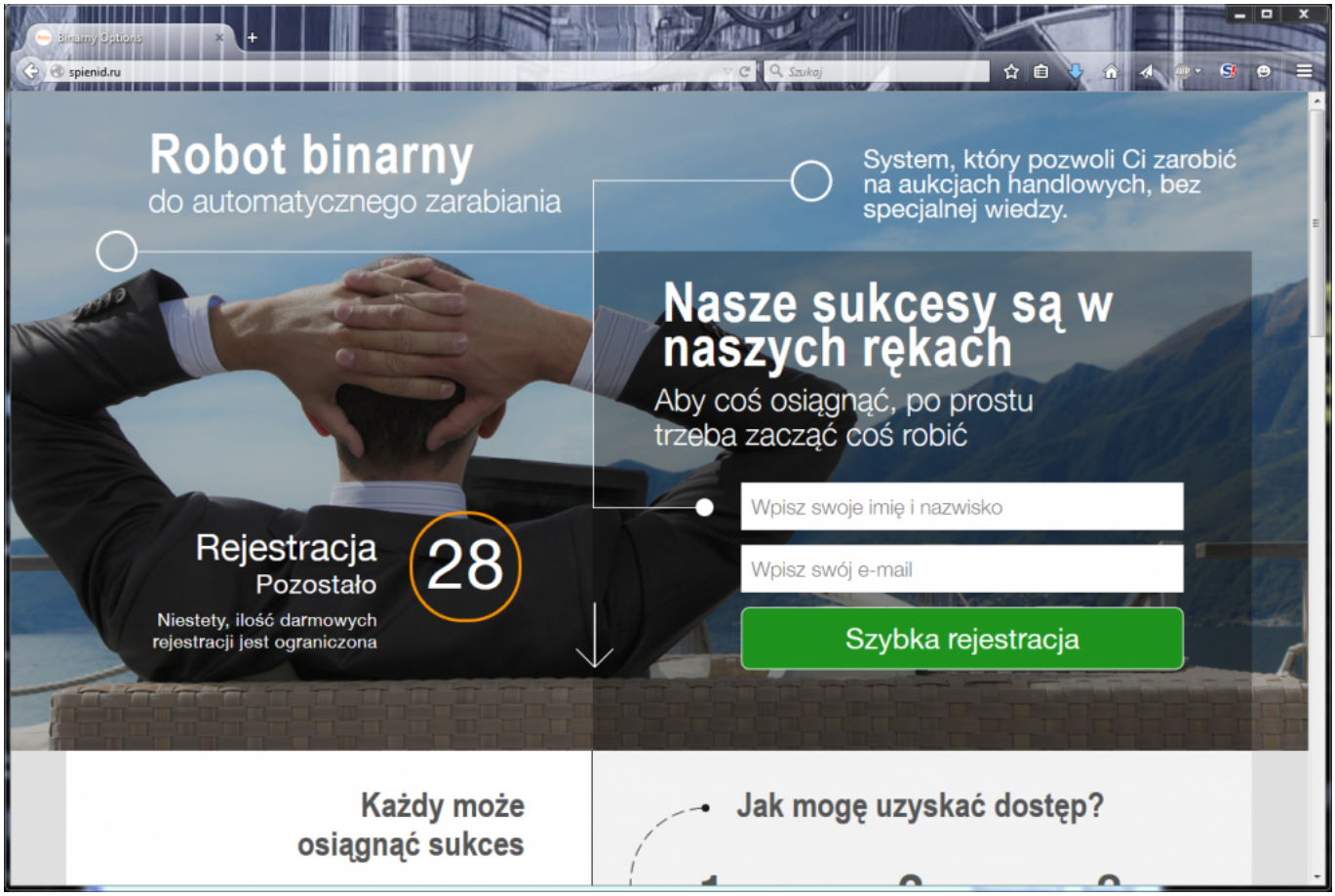
Jak już pisałem, przeniosłem swój hosting do firmy az.pl. Zrobiłem to z kilku powodów między innymi była to większa ilość baz danych i przestrzeni. Ku mojemu zdziwieniu zacząłem otrzymywać maile w ilościach masowych o zabawnej treści:

A więc stało się! Spam dotarł i do mnie.

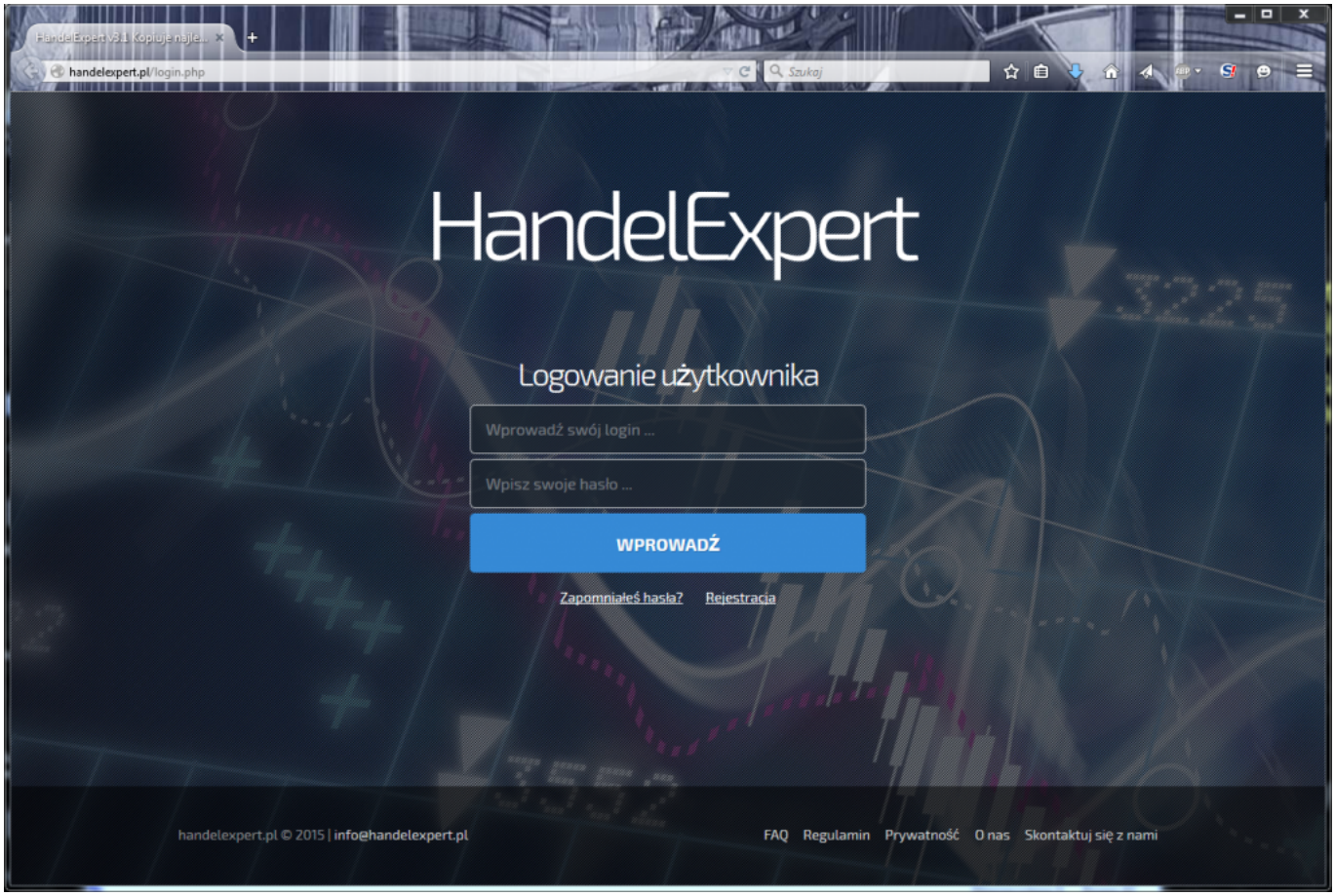


Linki które zawierają owe wiadomości kierują do ciekawej strony:

A więc stało się! Spam dotarł i do mnie.

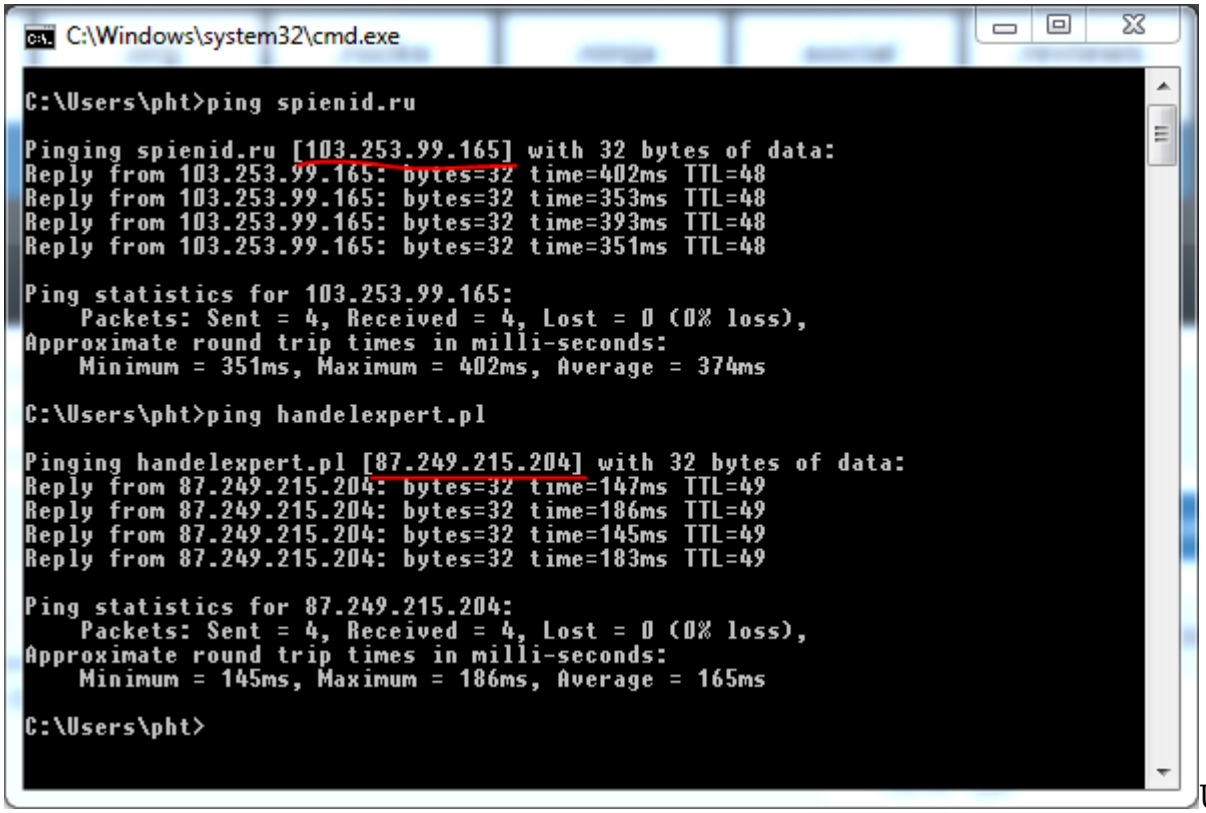


Każdy odsyłacz na tej stronie prowadzi do polsko brzmiącej strony handelexpert.pl.



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.

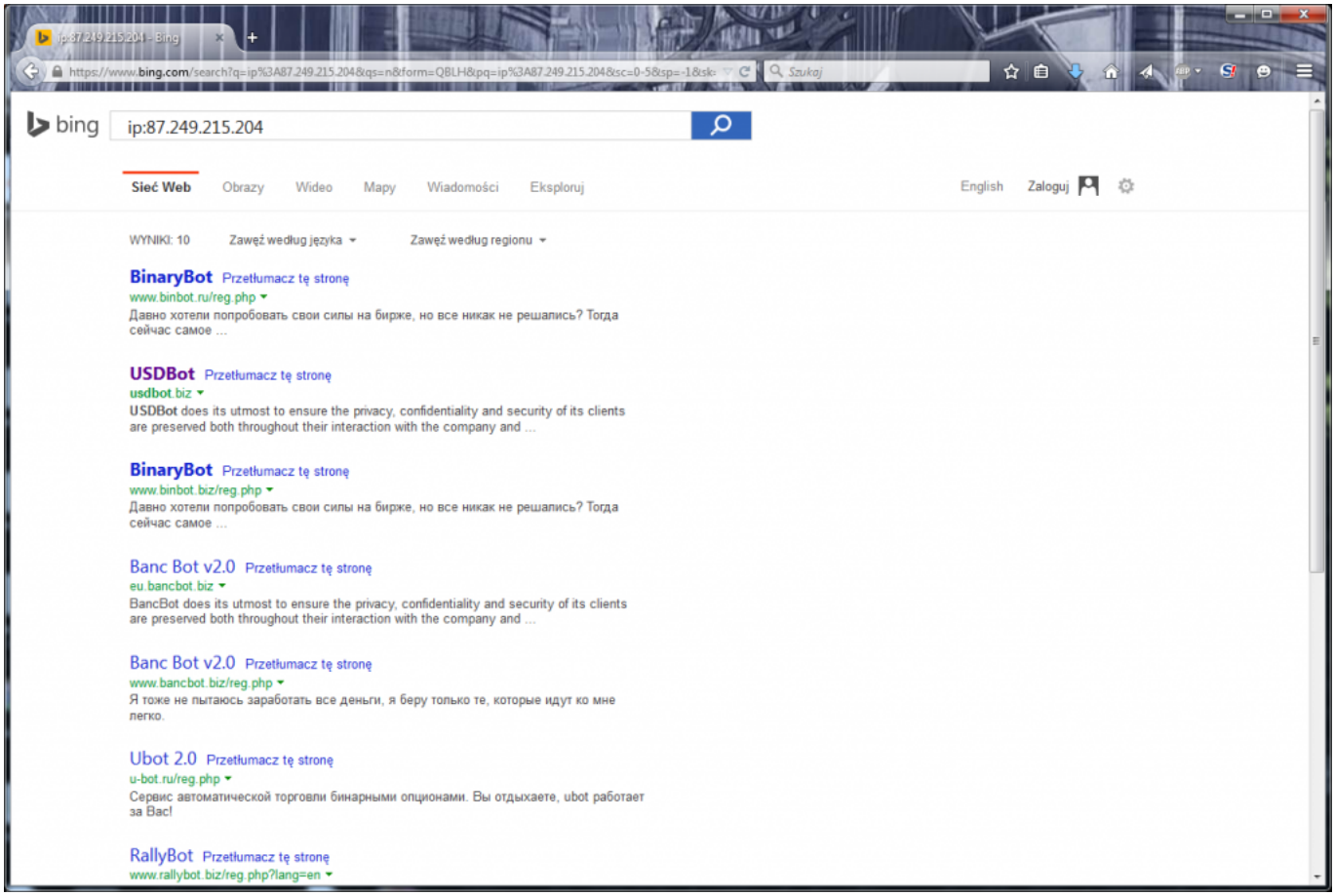
A więc stało się! Spam dotarł i do mnie.

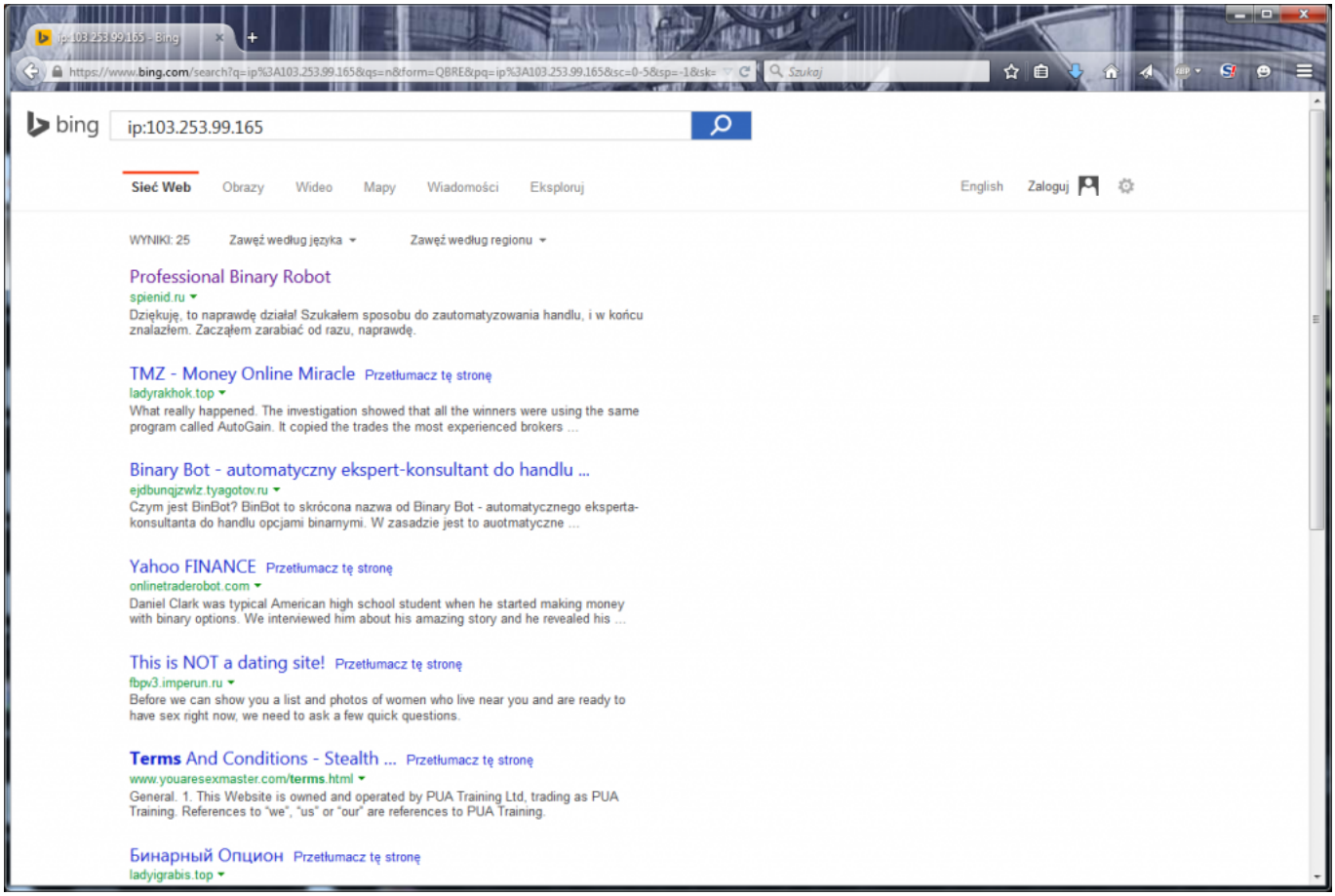


Użyłem klasycznego zagrania – „ip:<adres ip>” w wyszukiwarce bing by sprawdzić jakie jeszcze strony znajdują się na tych serwerach.

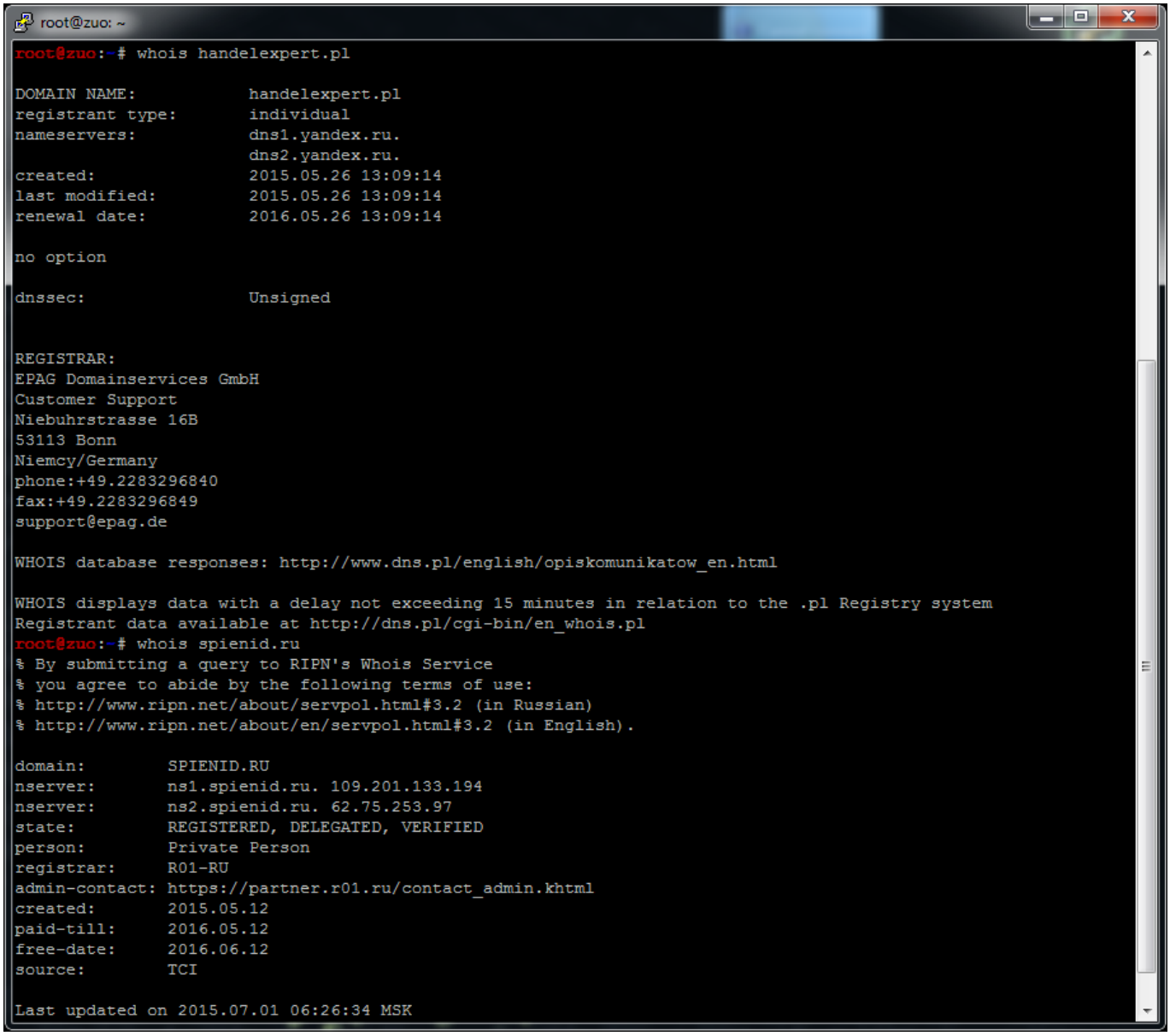
NO SYSTEM IS SAFE

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 pieniądza, a więc kochani Rosjanie dają nam szanse zarobić ale i okazje by wydać. Ale! Czas przyjrzeć się wpisom w WhoIs.



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.

A więc stało się! Spam dotarł i do mnie.

Postanowiłem przeczytać regulamin HandelExpert, aby znaleźć dodatkowe smaczki.

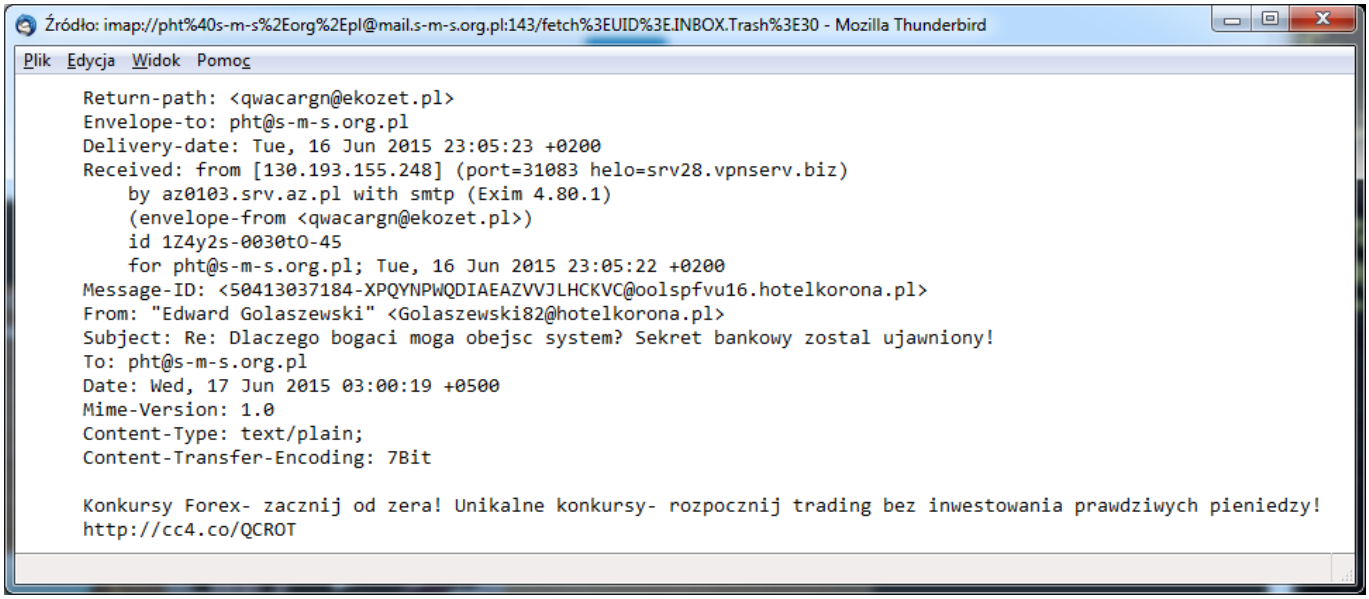
WYBÓR PRAWA I JURYSDYKCJI

> 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.

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 handelexpert.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.

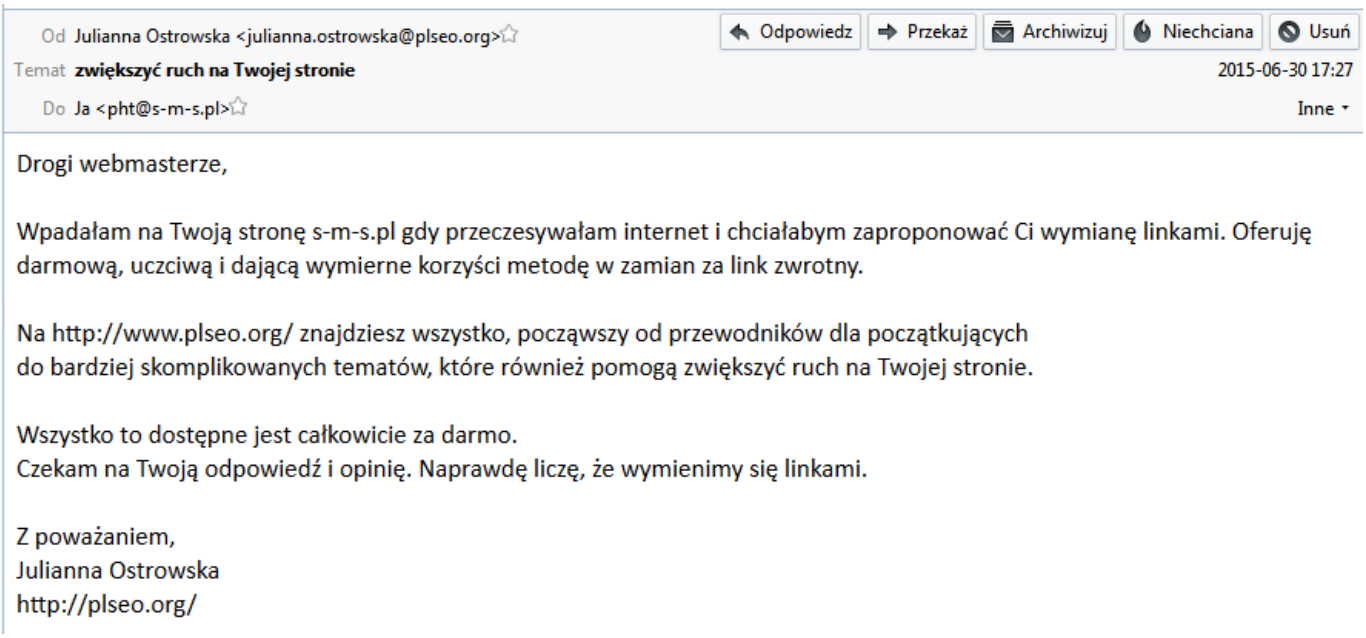


Jak się dokładnie przyjrzeć od razu widać kilka ciekawych rzeczy. Między innymi to iż mail zwrotny poszedł by do „qwacargn@ekozet.pl”, natomiast oficjalne „from” jest „Golaszewski92@hotelkorona.pl”. Mój serwer pocztowy dostał tą wiadomość od hosta o adresie IP 130.193.155.248 – czyli gdzieś z Kurdystanu!

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>
Odpowiedz | Przekaż | Archiwizuj | Niechciana | Usuń
Temat **zwiększyć ruch na Twojej stronie**
2015-06-30 17:27
Do Ja <pht@s-m-s.pl>
Inne

Drogi webmasterze,

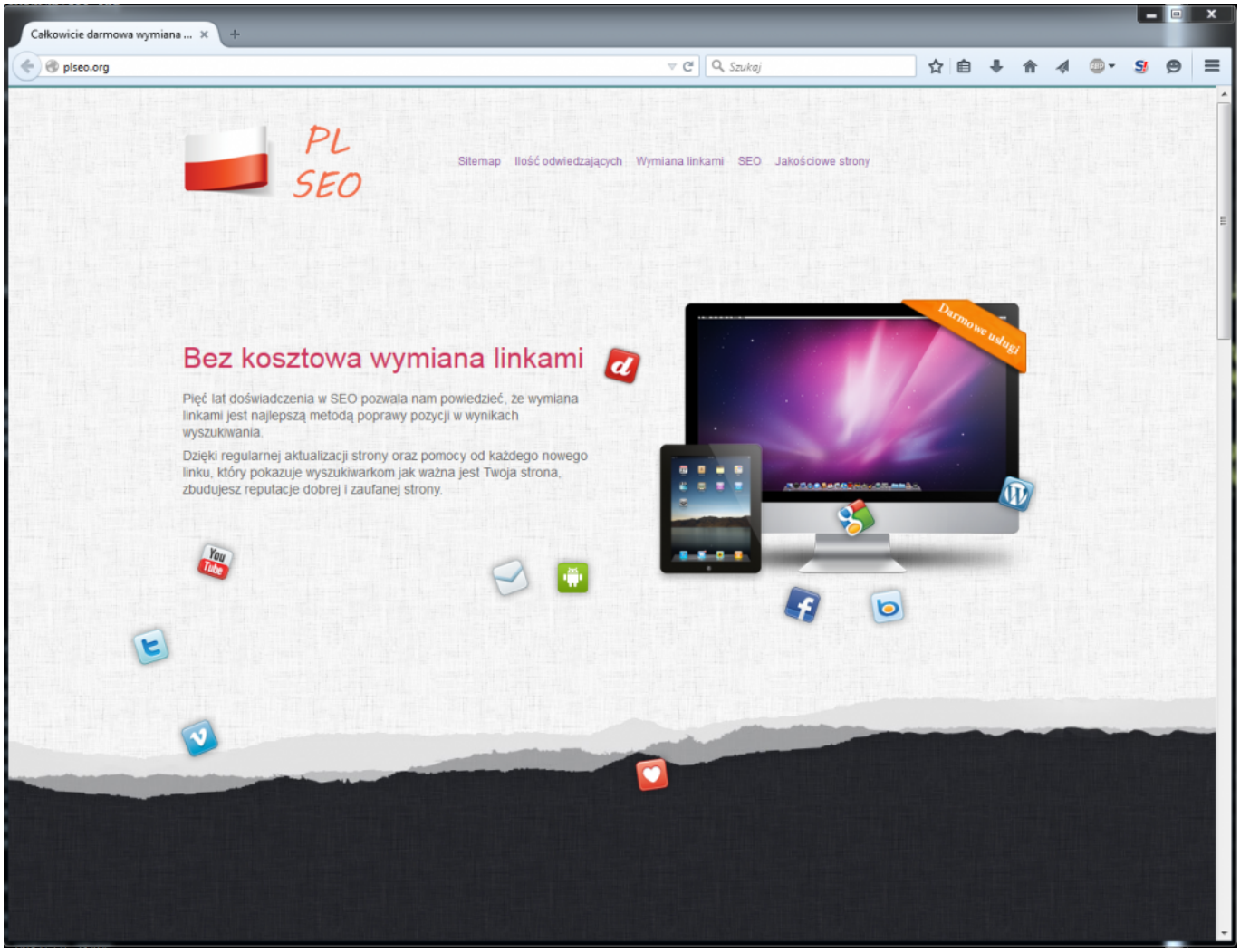
Wpadałam na Twoją stronę s-m-s.pl gdy przeczesywałam internet i chciałabym zaproponować Ci wymianę linkami. Oferuję darmową, uczciwą i dającą wymierne korzyści metodę w zamian za link zwrotny.

Na http://www.plseo.org/ znajdziesz wszystko, począwszy 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. Zacznijmy od podstaw – whois.

NO SYSTEM IS SAFE

A więc stało się! Spam dotarł i do mnie.

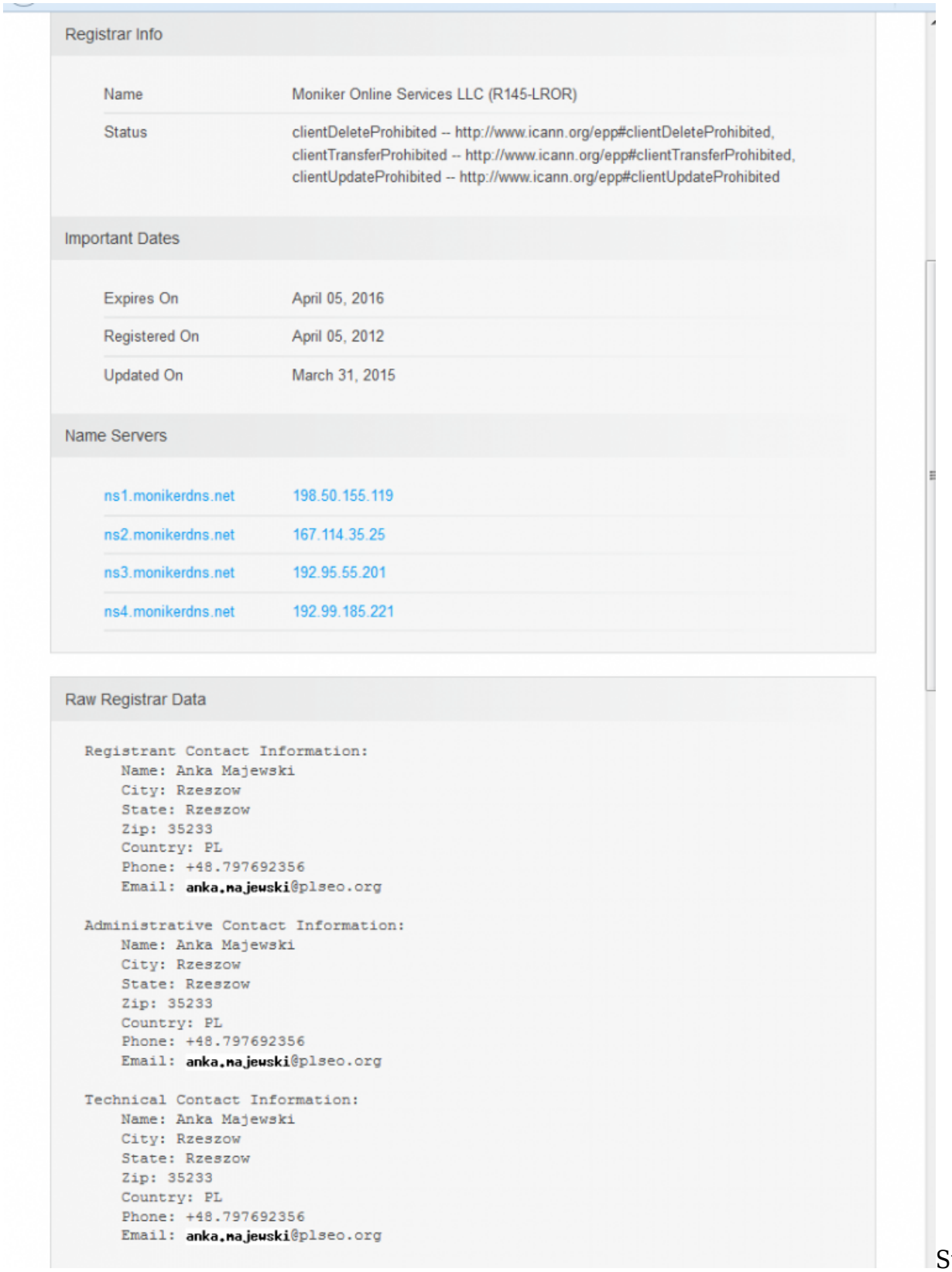
NO SYSTEM IS SAFE

A więc stało się! Spam dotarł i do mnie.

NO SYSTEM IS SAFE

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.majewski@plseo.org

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

Technical Contact Information:
    Name: Anka Majewski
    City: Rzeszow
    State: Rzeszow
    Zip: 35233
    Country: PL
    Phone: +48.797692356
    Email: anka.majewski@plseo.org
```

Strona

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 Linkedln 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.