Analýza podvodného webu (rogue website)

Vložil/a RubberDuck [1], 1 Únor, 2012 - 12:17

- Spam [2]
- Unsorted [3]

V e-mailových schránkách se každému z nás dnes a denně hromadí velký počet zpráv. Některé dokáží spam-filtry odhalit jako spamy, některé zůstanou neodhaleny. Na jeden takový neodhalený spam jsem se podíval trochu blíže.

V e-mailové schránce, kterou používám pro účely registrace, jsem nalezl e-mail od nějaké slečny:

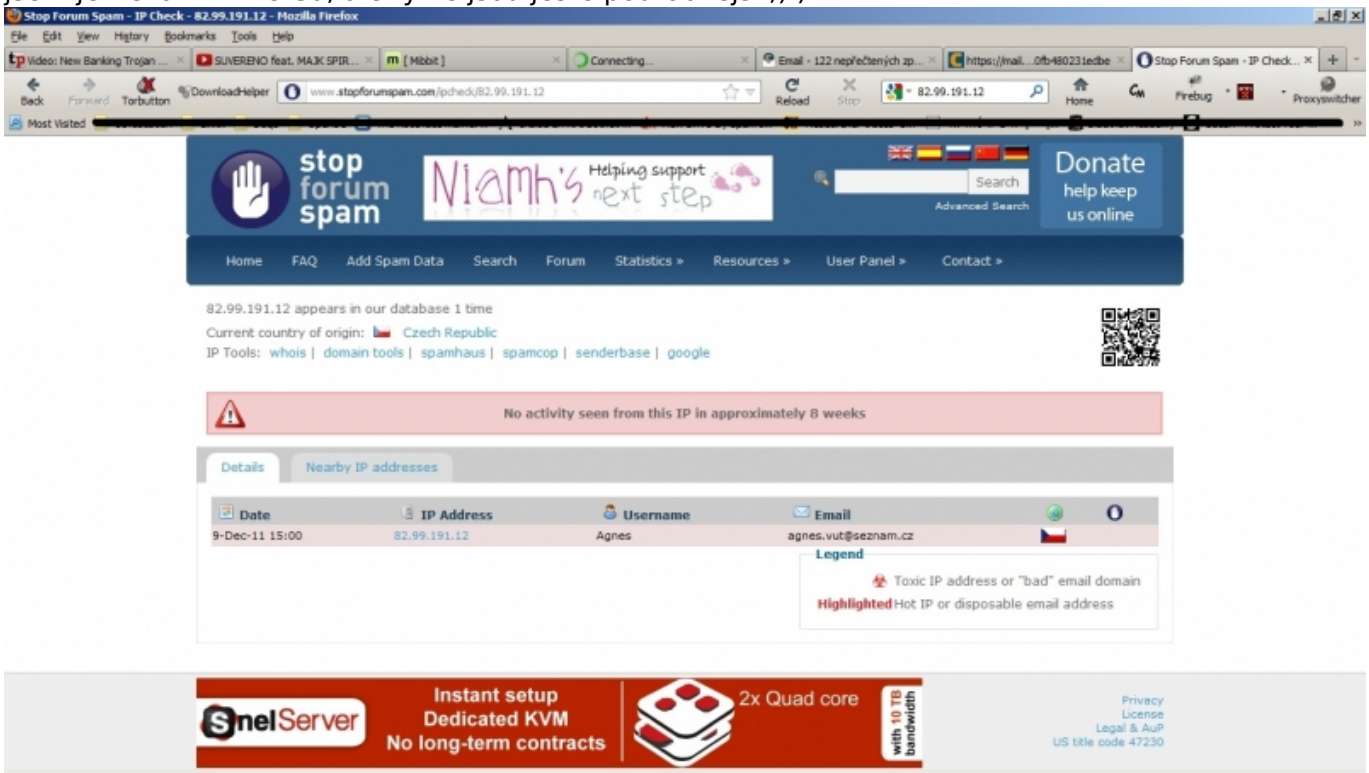
Čau Jak se ti daří?
Chtěla bych ti říct něco o sobě. Jmenuji se Mira. Pravě jsem prohlížela seznamovací webové stránky a nalezla jsem tvůj profil.
Rozhodla jsem se ti napsat e-mailovou zprávu. Myslím si, že v budoucnu bychom mohly být kamarádi, pokud nemáš nic proti tomu. Doopravdy to potřebuju.
Já nejsem vdaná. Nemám děti a nemám blízkého přítele.
Narodila jsem se 5. února 1989. Je mi 23.
Mám ráda poslouchat hudbu všech směrů a stylů a také ráda vařím. Zajímáš se o něco?
Máš rád poslouchat hudbu?
napiš mně na hxxp://lavina.baleset.info/
Opravdu doufám, že můžeme být kamarády a, že se můžeme dozvědět hodně zajímavého jeden o druhém.
Děkuji ti, že jsi přečetl můj dopis!.
Tvá Mira.

Už od prvopočátku se mi na něm zdálo něco podezřelého. Gramatika ukazuje tak na šestou třídu základní školy nebo na někoho, kdo není rodilý Čech. Pro jistotu jsem se podíval ještě na zdrojový kód e-mailové zprávy:

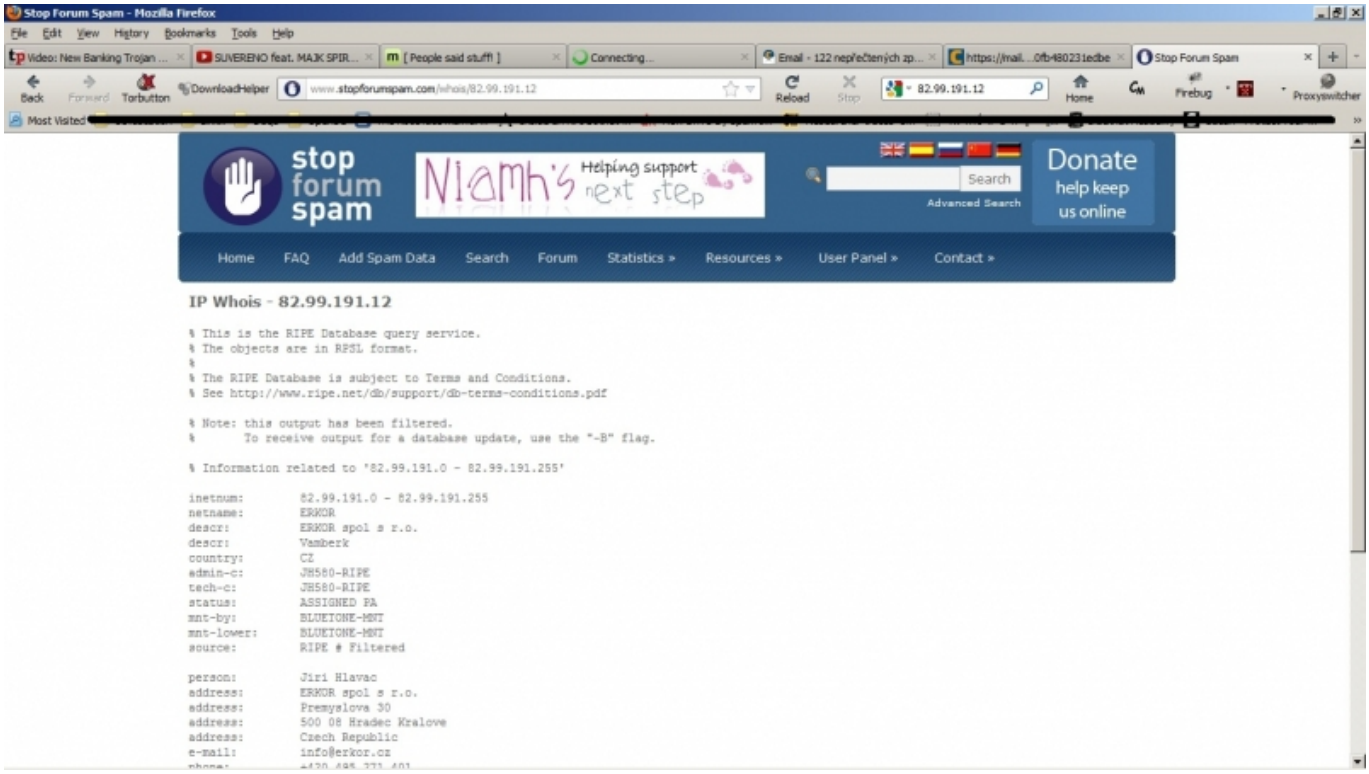
```
Received: from ironport1.centrum.cz (unknown [10.32.3.101])
        by gmmr3.centrum.cz (Postfix) with ESMTP id E68021400F8E5
        for <[CENSORED]@centrum.cz>; Mon, 30 Jan 2012 03:45:35 +0100 (CET)
Received: from mxl2.seznam.cz ([77.75.76.44])
  by mx.centrum.cz with ESMTP; 30 Jan 2012 03:45:35 +0100
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=beta; d=seznam.cz;
        h=Disposition-Notification-To:To:Date:From:Received:Subject:Content-Transfer-
Encoding:Content-Type:Mime-Version:Message-Id:X-Country:X-Abuse:X-Seznam-User:X-Virus
-Info:X-Seznam-SPF:X-Seznam-DomainKeys;
        b=n1cEAADxZtTizXD2npdoa6FiqyCPUaR4PMcLX0cx6F0M1FajzXSBbJTETFJfTq90s
        E7sn+GSghNU+ZgaIk9DJV4NaN8ERLJ338fLDhPw6ch0WEPIYgAdqHanf9dg3uBy6NAM
        0fSpzuZKdeHXrxrfkRjp95t9/KdP/4kQlJ0AITs=
Disposition-Notification-To: johriczoa@seznam.cz
To: [CENSORED]@centrum.cz
Date: Mon, 30 Jan 2012 03:45:15 +0100 (CET)
From: johriczoa@seznam.cz
Received: from  ( [82.99.191.12])       by email.seznam.cz (Email.Seznam.cz) with
HTTP  for johriczoa@seznam.cz;        Mon, 30 Jan 2012 3:45:15 +0100 (CET)
Subject:
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain;       charset="iso-8859-2"
Mime-Version: 1.0
Message-Id: <1967.912.2116-14509-882906973-1327891515@seznam.cz>
```

```
X-Country: CZ
X-Abuse: abuse@seznam.cz
X-Seznam-User: johriczoa@seznam.cz
X-Virus-Info:clean
X-Seznam-SPF:neutral
X-Seznam-DomainKeys:neutral

=C8au Jak se ti da=F8=ED?
Cht=ECla bych ti =F8=EDct n=ECco o sob=EC. Jmenuji se Mira. Prav=EC jse=
m prohl=ED=BEela seznamovac=ED webov=E9 str=E1nky a nalezla jsem tv=F9j=
 profil.
Rozhodla jsem se ti napsat e-mailovou zpr=E1vu. Mysl=EDm si, =BEe v bud=
oucnu bychom mohly b=FDt kamar=E1di, pokud nem=E1=B9 nic proti tomu. Do=
opravdy to pot=F8ebuju.
J=E1 nejsem vdan=E1. Nem=E1m d=ECti a nem=E1m bl=EDzk=E9ho p=F8=EDtele.=

Narodila jsem se 5. =FAnora 1989. Je mi 23.
M=E1m r=E1da poslouchat hudbu v=B9ech sm=ECr=F9 a styl=F9 a tak=E9 r=E1=
da va=F8=EDm. Zaj=EDm=E1=B9 se o n=ECco?
M=E1=B9 r=E1d poslouchat hudbu?
napi=B9 mn=EC na <a href="http://lavina.baleset.info/<br />
Opravdu" title="http://lavina.baleset.info/<br />
Opravdu">http://lavina.baleset.info/<br />
Opravdu</a> douf=E1m, =BEe m=F9=BEeme b=FDt kamar=E1dy a, =BEe se m=F9=BEem=
e dozv=ECd=ECt hodn=EC zaj=EDmav=E9ho jeden o druh=E9m.
 D=ECkuji ti, =BEe jsi p=F8e=E8etl m=F9j dopis!.
Tv=E1 Mira.
```

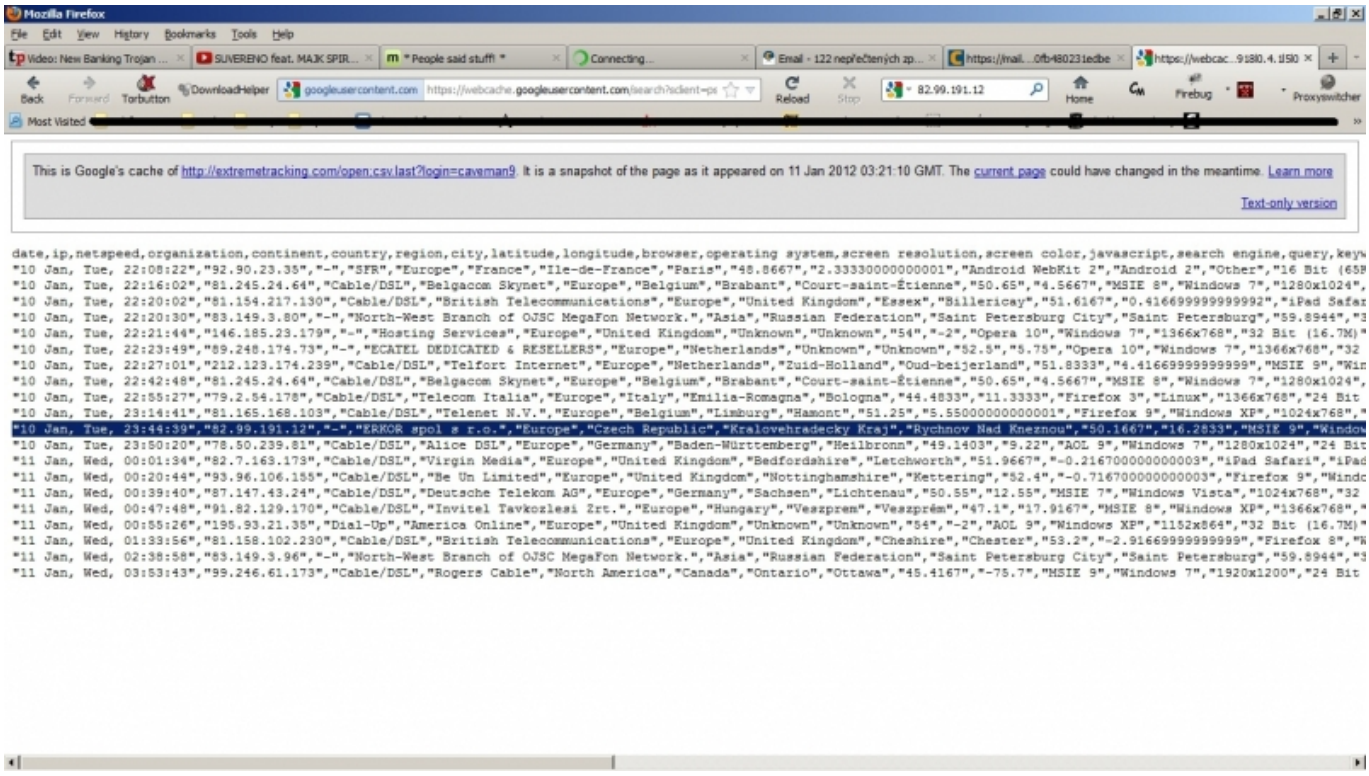
Stále nic nenasvědčovalo tomu, že se jedná o podvodný e-mail. Začal jsem tedy přemýšlet, kde jsem se mohl registrovat, protože seznamky vážně nepoužívám :D Zkusil jsem tedy zadat e-mail johriczoa@seznam.cz [4] do googlu. Ten mi však nic nevrátil. Zkusil jsem do googlu zadat ještě IP adresu 82.99.191.12 a dostal jsem dva zajímavé výsledky. Jeden udával, že byla IP adresa v blacklistech jako zdroj spamu, druhý pak poskytoval přesné informace o této IP adrese (jasně, mohl jsem je získat z WHOISu, ale tyhle jsou ještě podrobnější ;))



StopSpam

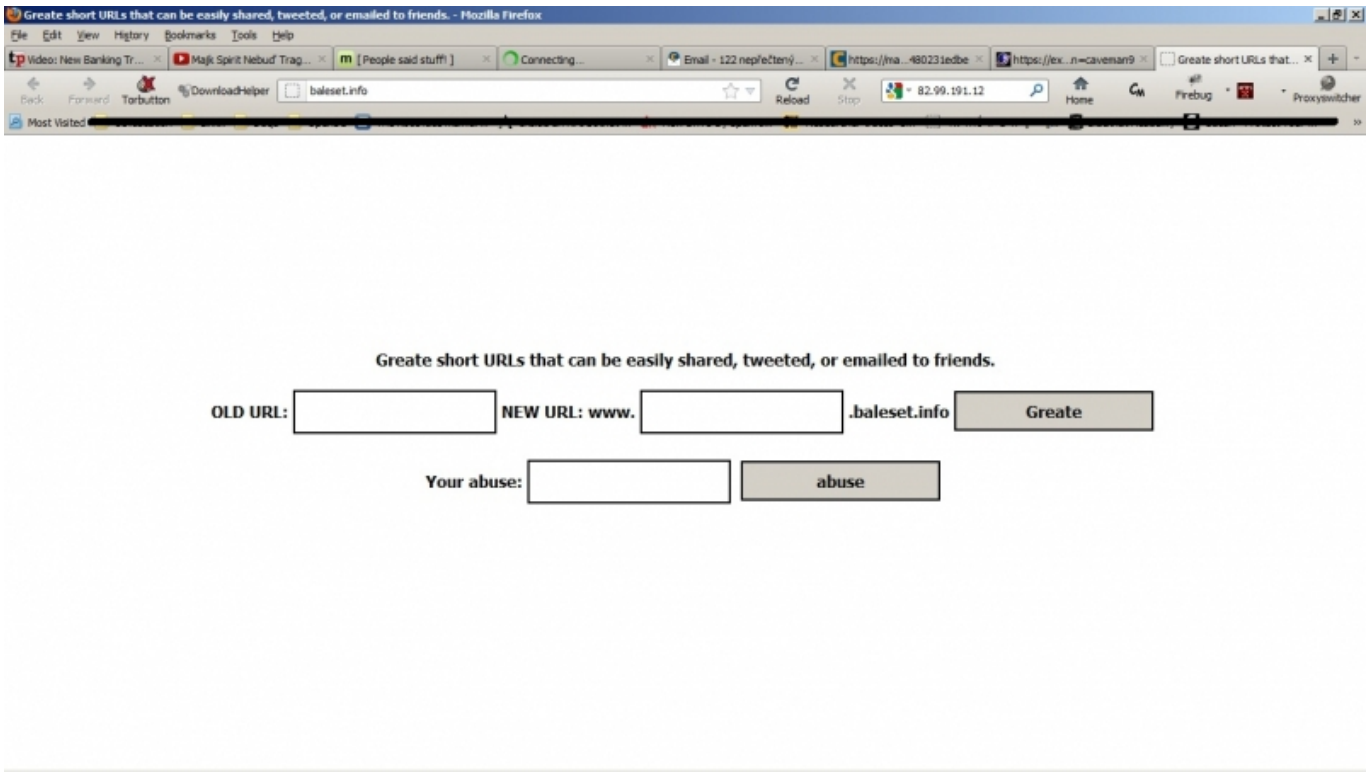


ExtremeTracker



Výstup z ExtremeTrackeru

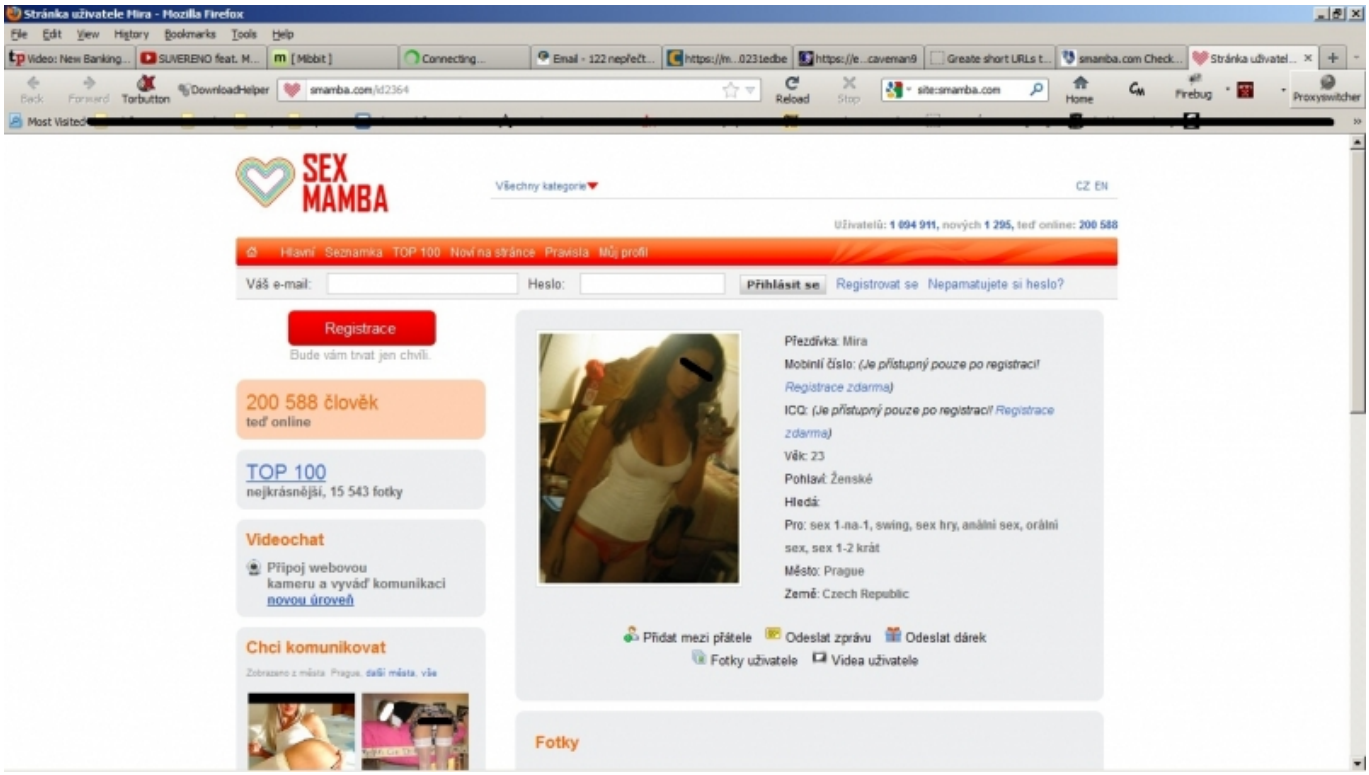
URL adresa v e-mailu taky nepůsobila moc přesvědčivě. Opět jsem použil google a tentokrát zadal doménu baleset.info, abych zjistil, že se jedná o další populární "zkracovací" službu hostovanou v Rusku.



URL Shorter baleset

Protože jsem si nevěřil a nechtěl si zbytečně infikovat stroj nějakým malwarem, rychle jsem si vytvořil v PHP skript, který mi stáhl danou stránku a uložil ji do textového souboru. V něm jsem našel odkaz vedoucí sem:

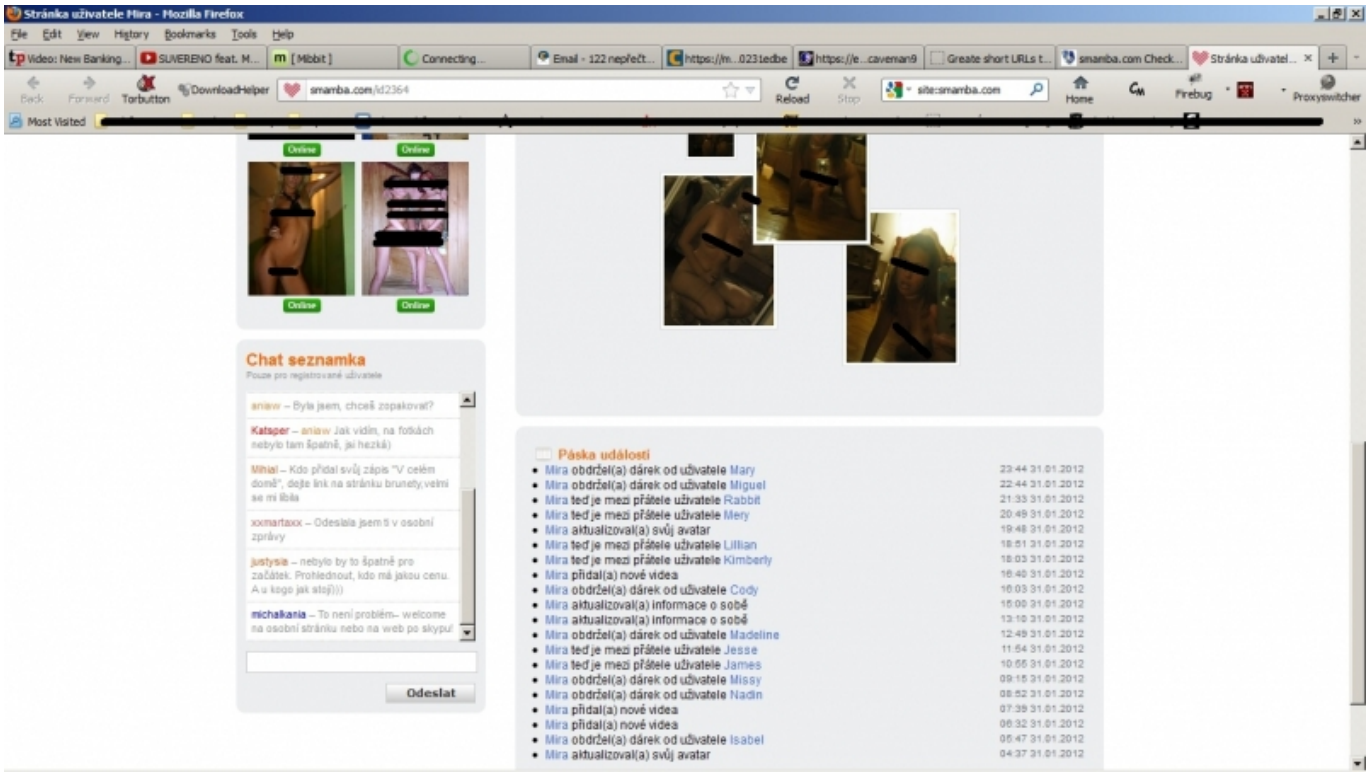
hxxp://smamba.com/id2364



Portál sex-mamba.com v plné kráse

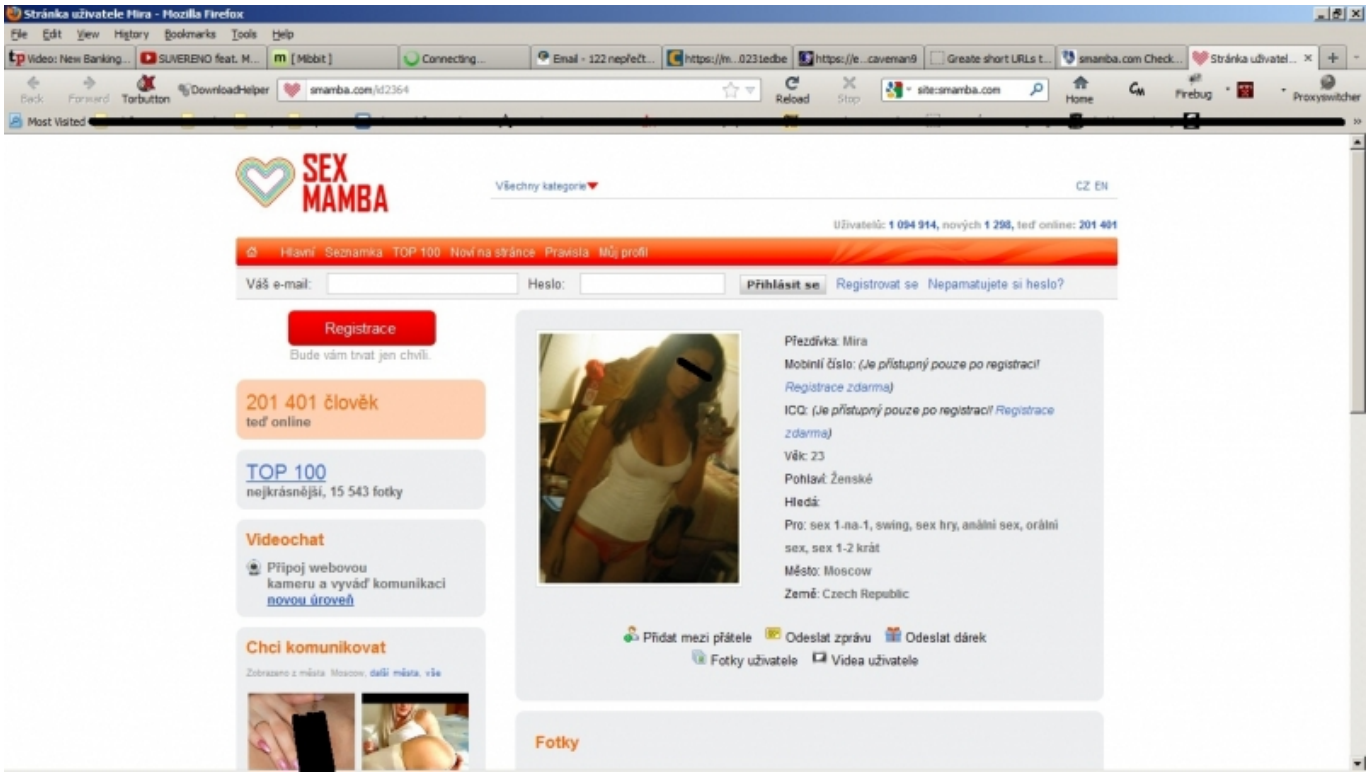
Na první pohled se jedná o legitimní stránku a nic nenasvědčuje, že by mělo jít o podvod. Dokonce i google mlčí a vrací pouze odkazy na jednotlivé profily. Služba www.safersite.de [5] taktéž stránku považuje za víceméně důvěryhodnou. Pořád mi ale něco nehrálo. Pokud se podíváme do levé části

na chat zjistíme, že je překládán pomocí překladače. V chatu se objevují i česká jména jako Kamil nebo Lucie, ale že by taky neuměli pořádně česky? Navíc vložené posty se po nějaké době začínají opakovat. Dalším vtipnou věcí je skutečnost, že v sekci "Páska událostí" se provádí jedna akce každou hodinu. To ta holka nespí?



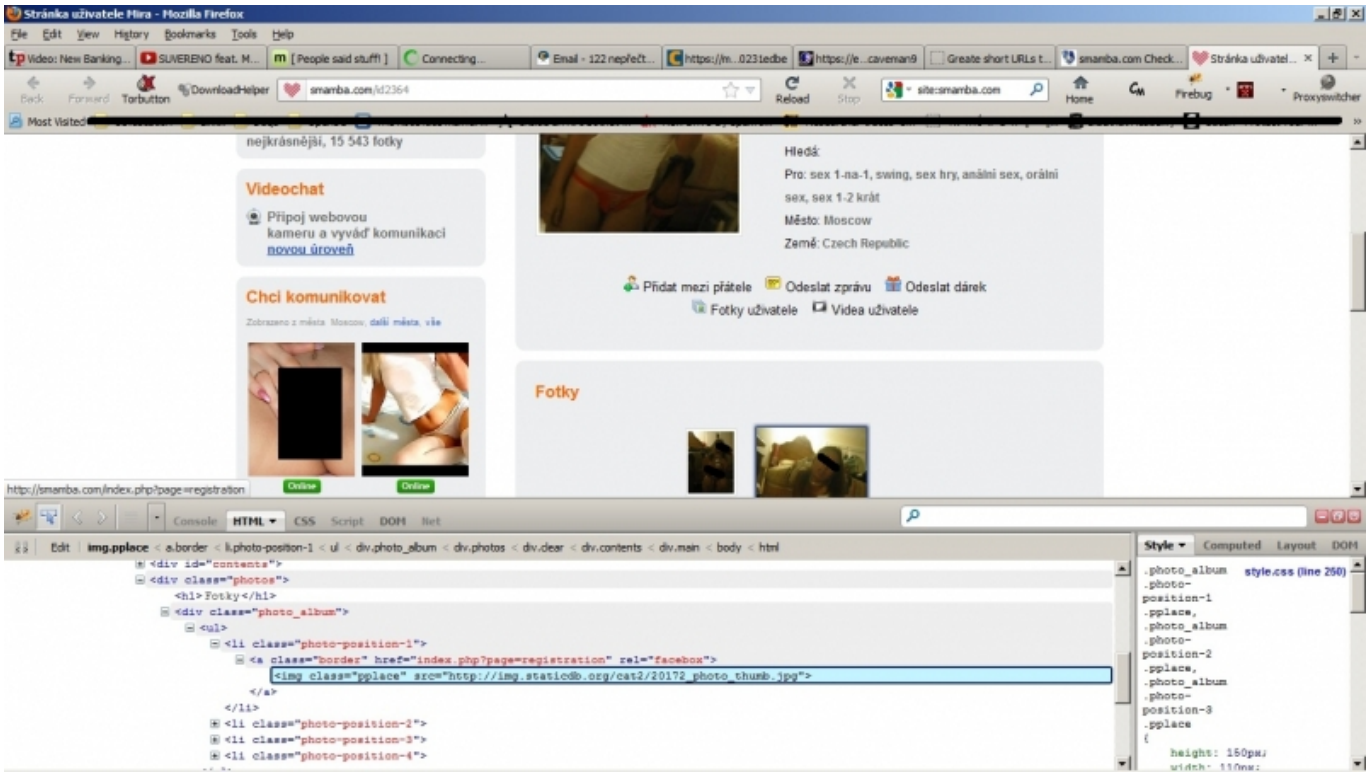
Podezřelý chat a podezřelá Páska událostí

Zkusil jsem tedy pátrat dále. Co ukrývají cookies? Informace o lokaci (stát, město) a další údaje. Změnil jsem lokaci na town_name=Moscow a obnovil jsem stránku. Nevěřil jsem vlastním očím. Slečna rázem nebyla z Prahy, ale z Moskvy, stejně jako čtyři další (nutno podotknout, že oproti dřívějšku úplně stejné!!) kontakty vlevo.

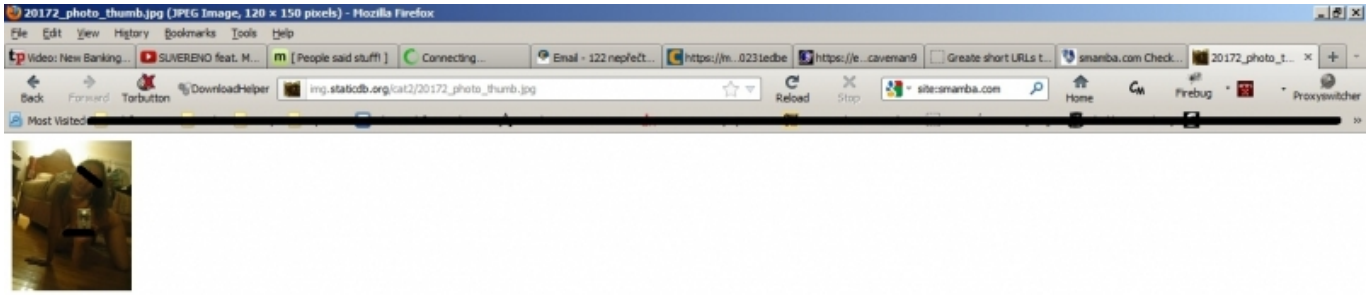


Moskva už je v České republice, stejně jako se bleskově 'přestěhovala Mira'

Dobře. Tak se tomu koukneme na zoubek ještě víc. Co například čtyři vybrané fotky? Po kliknutí na jednu z nich se mi objevil registrační formulář. Jenže já se registrovat nechci :) Zvolil jsem tedy jinou cestu. Použil jsem FireBug [6] (plugin do FireFoxu určený jako pomůcka při vývoji webových aplikací) a nechal si zobrazit zdroj fotografie (ano, dalo se to vyčíst ze zdrojového kódu stránky, ale proč si práci neulehčit? :)). Dostal jsem adresu http://img.staticdb.org/cat2/20172_photo_thumb.jpg [7].



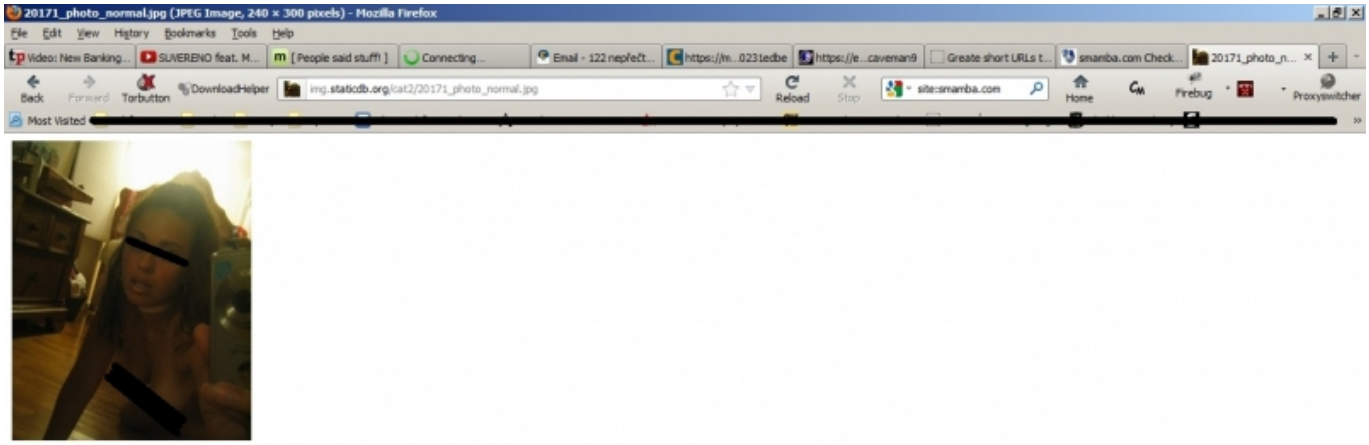
Cesta k fotce na serveru ...



... a zmenšenina fotky (xxx_photo_thumb.jpg)

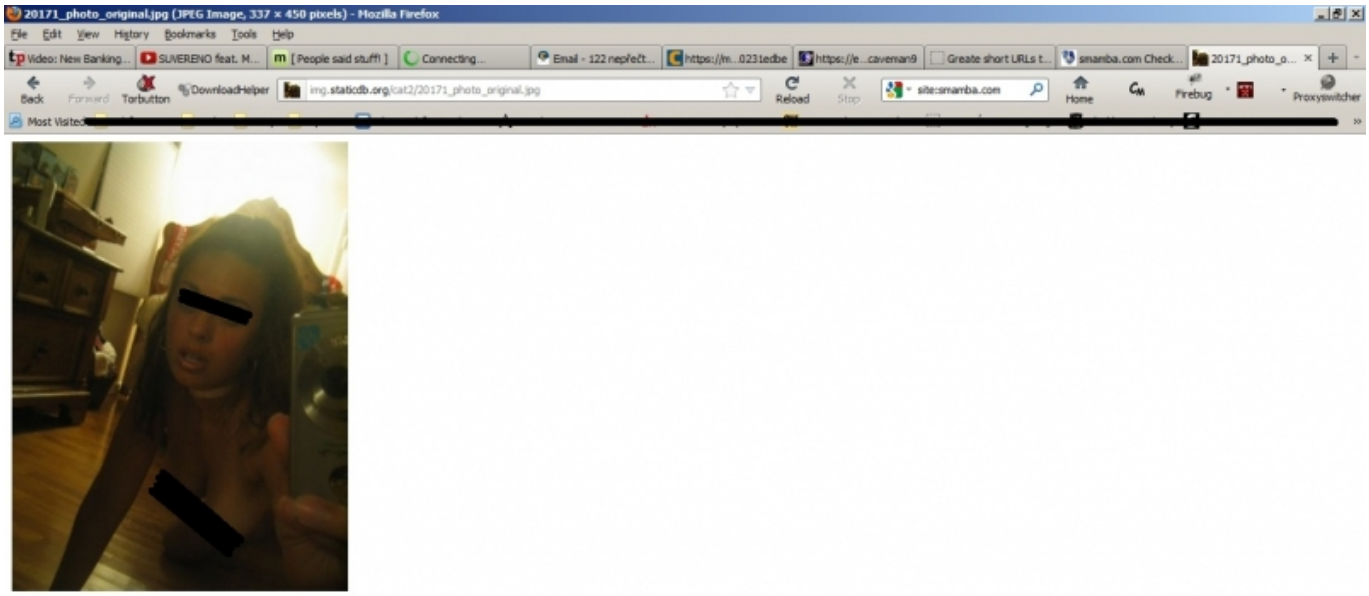
Změnou číselné hodnoty jména obrázku jsem si zajistil možnost procházet další fotky, ale pochybuji, že je sem někdo nahrál takhle maličké. Co třeba zkusit získat původní velikost fotek? Zaměnil jsem v

URL slovo **thumb** v názvu fotky slovem **normal**.



Fotka v normální velikosti (xxx_photo_normal.jpg)

Ovšem stále se mi zdála fotka nějak malá. Co zkusit místo slova normal použít slovo **original**?



Fotka v originální velikosti (xxx_photo_original.jpg)

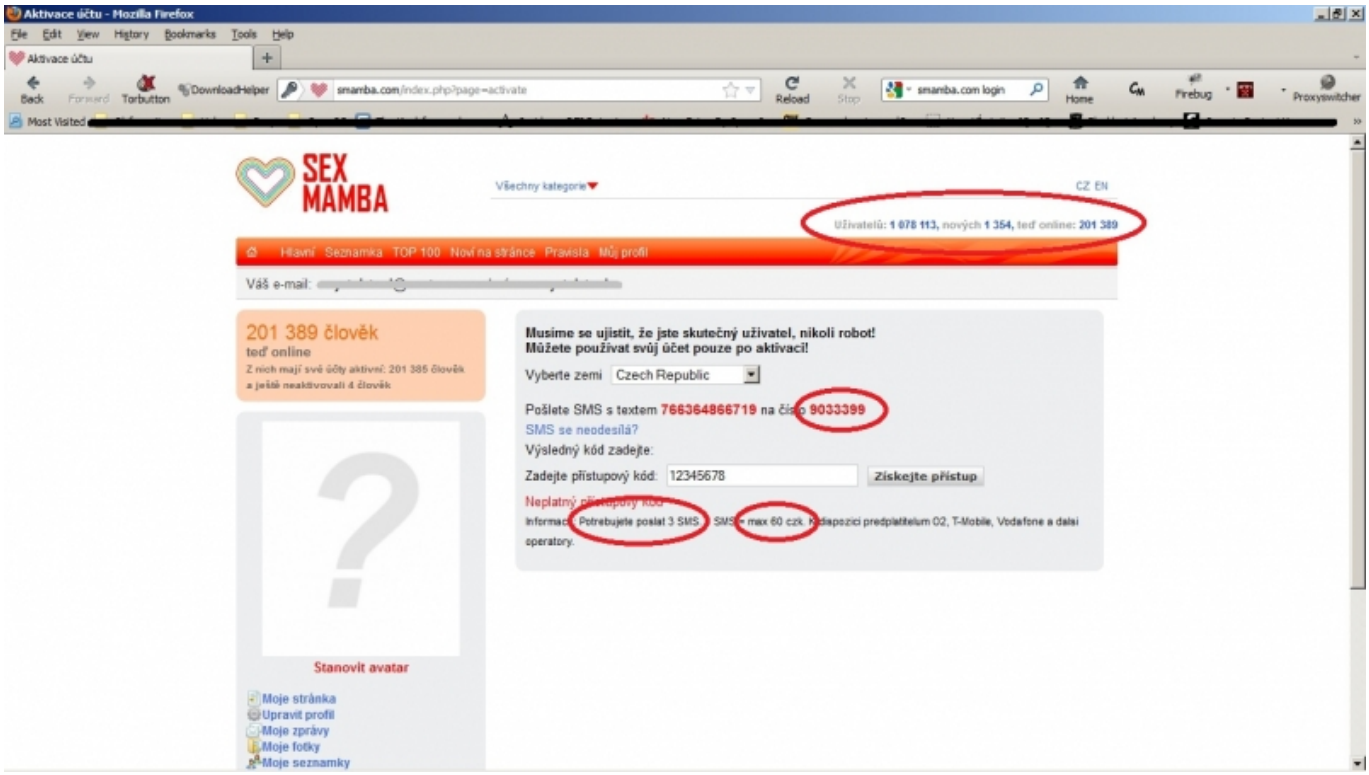
To už je znatelně lepší :) Prošel jsem pár adres směrem vzhůru a pár adres směrem dolů. Zjistil jsem, že adrey od hodnoty 20500 jsou patrně prázdné. Pro jistotu jsem si ale napsal jednoduchý PHP skript, jehož cílem bylo projít adresy od názvu fotky 1_photo_original.jpg do 20600_photo_original.jpg a uložit je do adresáře. Světe div se, nebylo jich ani 588. Pak jsem si povšiml skutečnosti, že avatary používají označení <id_profilu>_avatar_normal.jpg. Tato skutečnost se stala dobrým vodítkem pro

zjištění reálného počtu "profilů". Když k tomu přidáme fakt, že "profily" začínají na adrese 2194 a končí 2402, a za předpokladu, že pouze minimální počet "profilů" bude vynechaný, zjistíme pomocí jednoduchého PHP skriptu, že je počet "profilů" 178.

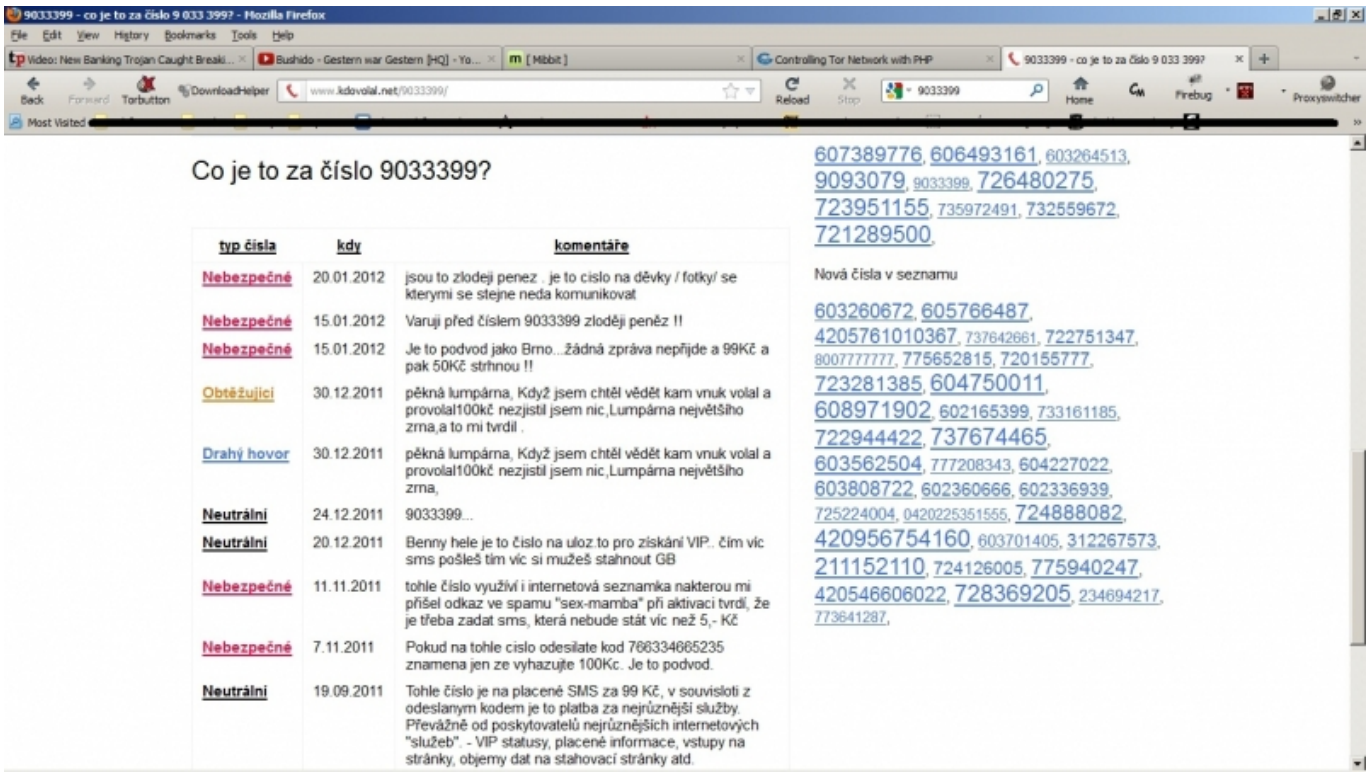
To má do zmiňovaného milionu registrovaných uživatelů, celkem daleko. Nehlědě na to, že je údajně v každý okamžik online 200 tisíc lidí a na to, že z mužských "profilů" má více než jednu fotku zhruba 5 mužů a žádný není v rouše Adamově. Celkem divné vzhledem k tomu, že se jedná o erotickou seznamku (sociální síť), kde se ženské vůbec nestydí, ale muži ano.

Téměř všichni "registrovaní uživatelé" používají pro úpravu fotek známý grafický editor ACDSee. Když jsem fotky zběžně procházel a zkoušel dohledat na internetu, zjistil jsem, že se některé nachází na různých porno portálech. Další nálezy v porno galeriích mi potvrdil i Bystroushaak (díky za spolupráci :)).

Pokud se i přes všechny předešlé informace budete chtít zaregistrovat, budete vyzváni k zaslání tří SMS zpráv, z nichž jedna by neměla přijít na více než 60 korun, ač číslo končí dvojčíslím 99, což znamená, že **cena jedné SMS je 99 korun**. Uvedené číslo 90333399 jsem tedy ještě otestoval v googlu a zjistil, že má úvaha o podovodné stránce je více než pravděpodobná.



Zaplať nebo nic neuvidíš!!



Pokud zaplatíš, tuplem nic neuvidíš!! (ani slečny, ani peníze)

Z mé soukromé analýzy jsem udělal následující závěr

- E-mail pochází patrně z Ruska nebo rusky mluvící země (podle skladby vět). Protože mail přišel z české IP adresy, naučili se zřejmě útočníci cílit na konkrétní státy jejich vlastním jazykem a dokonce zvyšují důvěryhodnost tím, že posílají e-mail z české e-mailové schránky.
- Za předpokladu, že používají útočníci k rozesílání spamu bránu seznamu, znamená to, že dokáží lámat CAPTCHA, kterou seznam používá.
- URL Shorter má za úkol snížit pravděpodobnost odhalení, pokud by se doména dostala na blacklist a snížit podezřívavost samotných obětí.
- Samotný portál má za úkol vylákat z lidí hlavně peníze ve formě vysoce placených SMS a pak osobní informace tváříce se (hlavně e-mailovou adresu, která bude dále používána pro cílený spam, a heslo, které se dokonce ukládá do cookies v podobě čistého textu), že se jedná o skutečnou erotickou seznamku (sociální síť).

Dodatek

Večer, když jsem psal tuto jednoduchou analýzu, bylo údajně registrovaných něco málo přes milión "uživatelů" a každou vteřinu přibývalo průměrně 8 nových "uživatelů". Každou vteřinu se připojilo nebo odpojilo více než 30 tisíc "uživatelů", přičemž 200 tisíc jich bylo neustále online. Téměř každý uživatel je podle "Pásky událostí" online 24 hodin denně a aktualizuje svůj profil minimálně 1x za hodinu. Ráno, když jsem ze zvědavosti kontroloval tyto stavy jsem došel k následujícím hodnotám:

- Registrováno necelých 950 tisíc "uživatelů"
- každou vteřinu je online skoro 201 tisíc uživatelů
- a opět je každý z "uživatelů" online 24 hodin denně

URL článku:
https://security-portal.cz/blog/anal%C3%BDza-podvodn%C3%A9ho-webu-rogue-website

Odkazy:
[1] https://security-portal.cz/users/rubberduck

[2] https://security-portal.cz/category/tagy/spam
[3] https://security-portal.cz/category/tagy/unsorted
[4] mailto:johriczoa@seznam.cz
[5] http://www.safersite.de
[6] https://addons.mozilla.org/en-US/firefox/addon/firebug/
[7] http://img.staticdb.org/cat2/20172_photo_thumb.jpg