

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 neodhalené. Na jeden takový neodhalený spam jsem se podíval trochu blíže.

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

Čau Jak se ti daří?

Chtěla bych ti říct něco o sobě. Jmenuji se Mira. Právě jsem prohlížela seznamovací webové stránky a našla 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 <http://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 mx12.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=noaws; 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
    0fSpzuZKdeHXrxfkRjp95t9/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>
```

Analýza podvodného webu (rogue website)

Publikováno na serveru Security-Portal.cz (<https://security-portal.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=ECl a 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/

Opravdu" title="http://lavina.baleset.info/

Opravdu">http://lavina.baleset.info/

Opravdu 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.

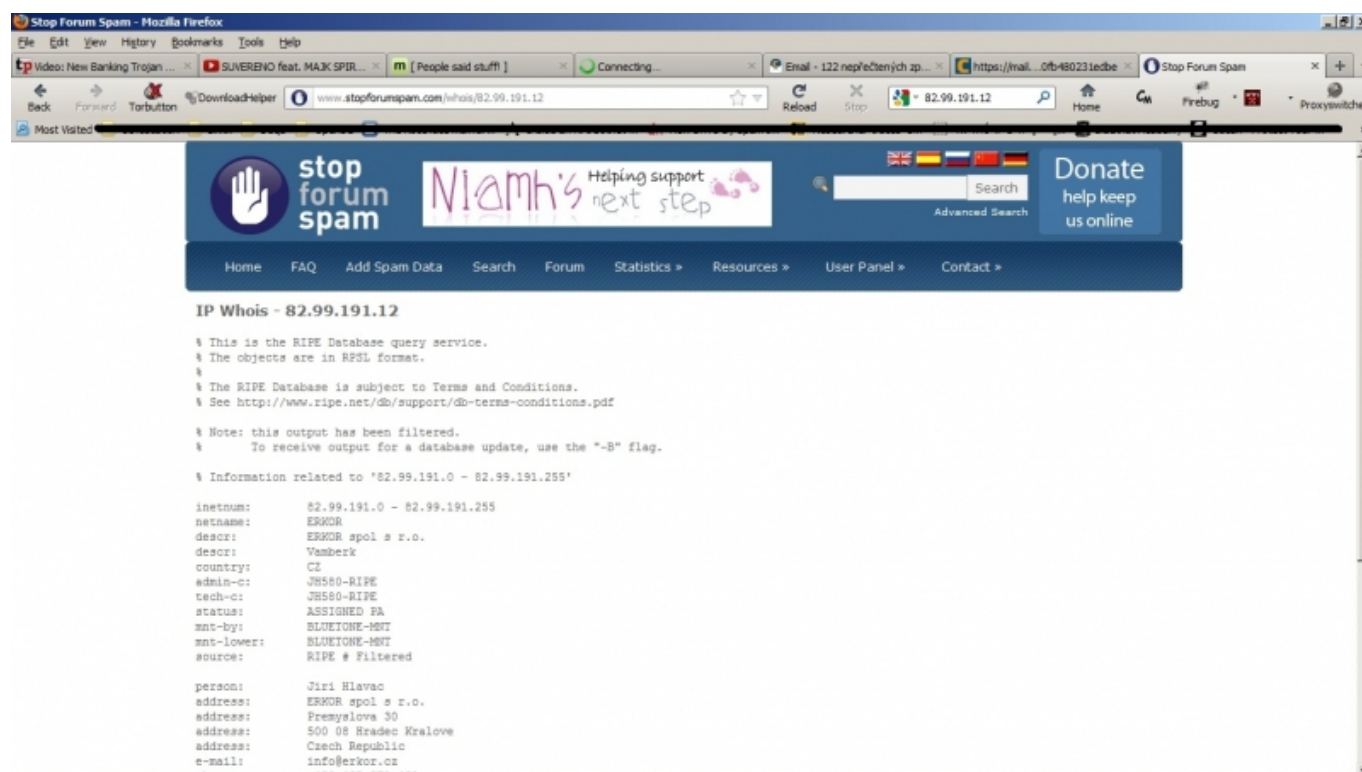
Stále nic nenasevřčovalo tomu, že se jedná o podvodný e-mail. Začal jsem tedy přemýšlet, kde jsem se mohl registrovat, protože seznamky vážně nepoužívám :D Zkusil jsem tedy zadat e-mail johriczoa@seznam.cz [4] do googlu. Ten mi však nic nevrátil. Zkusil jsem do googlu zadat ještě IP adresu 82.99.191.12 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 ;))

The screenshot shows the 'stop forum spam' website interface. At the top, there's a navigation bar with links like Home, FAQ, Add Spam Data, Search, Forum, Statistics, Resources, User Panel, and Contact. Below this, a search bar shows the IP address 82.99.191.12. The main content area displays information about this IP: it appears in the database 1 time, its current country of origin is the Czech Republic, and it's listed in various IP tools like whois, domain tools, spamhaus, spamcop, senderbase, and google. A warning box states: 'No activity seen from this IP in approximately 8 weeks'. Below this, a table titled 'Nearby IP addresses' shows a single entry for the IP 82.99.191.12, associated with the username 'Agnes' and email 'agnes.vut@seznam.cz'. A legend explains that a red flag icon indicates a 'Toxic IP address or "bad" email domain' and a red highlight indicates a 'Hot IP or disposable email address'. At the bottom of the page, there are banners for 'SnelServer' (Instant setup, Dedicated KVM, No long-term contracts) and '2x Quad core' servers, along with a privacy policy link.

StopSpam

Analýza podvodného webu (rogue website)

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)



Stop Forum Spam - Mozilla Firefox

File Edit View History Bookmarks Tools Help

tp Video: New Banking Trojan ... SUNERENO feat. MAJK SPIR ... m [People said stuff] Connecting ... Email - 122 nepřetčených zp ... https://inail...ofb48023iedbe ... Stop Forum Spam

Back Forward Torbutton Download-helper www.stopforumspam.com/whois/82.99.191.12 Reload Stop 82.99.191.12 Home Firebug Proxyswitcher

stop forum spam Helping support Niamh's next step

Home FAQ Add Spam Data Search Forum Statistics Resources User Panel Contact

IP Whois - 82.99.191.12

% This is the RIPE Database query service.
% The objects are in RPSL format.
% The RIPE Database is subject to Terms and Conditions.
% See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

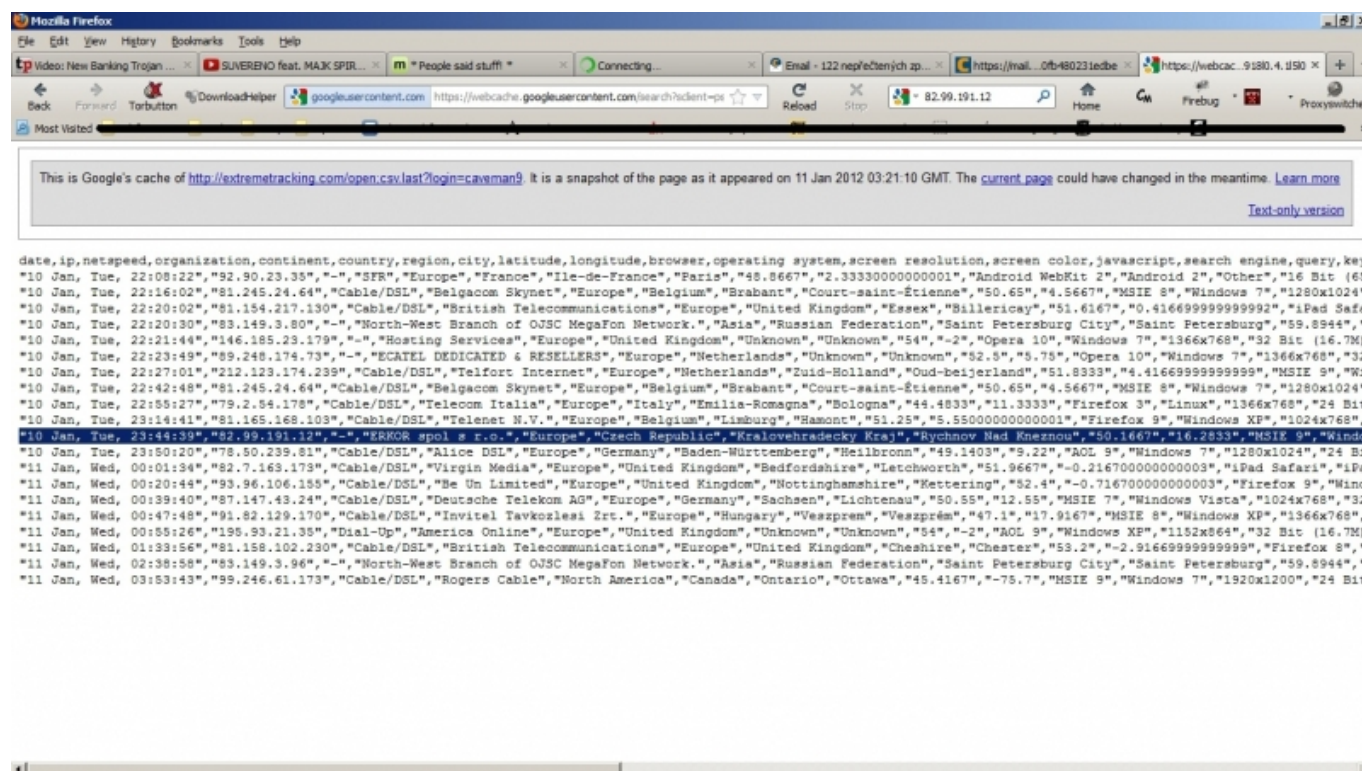
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '82.99.191.0 - 82.99.191.255'

inetnum: 82.99.191.0 - 82.99.191.255
netname: ERKOR
descr: ERKOR spol s r.o.
descr: Vamberk
country: CZ
admin-c: JHS80-RIPE
tech-c: JHS80-RIPE
status: ASSIGNED PA
mnt-by: BLUETONE-HVT
mnt-lower: BLUETONE-HVT
source: RIPE # Filtered

person: Jiri Hlavac
address: ERKOR spol s r.o.
address: Premyslova 30
address: 500 08 Hradec Kralove
address: Czech Republic
e-mail: info@erkor.cz
phone: +420 488 371 401

ExtremeTracker



Mozilla Firefox

File Edit View History Bookmarks Tools Help

tp Video: New Banking Trojan ... SUNERENO feat. MAJK SPIR ... m [People said stuff] Connecting ... Email - 122 nepřetčených zp ... https://inail...ofb48023iedbe ... https://webcac.9.1880.4.U50

Back Forward Torbutton Download-helper googleusercontent.com https://webcac.googleusercontent.com/search?ident=pe Reload Stop 82.99.191.12 Home Firebug Proxyswitcher

This is Google's cache of <http://extremetracking.com/open.cav?last?login=cavman9> It is a snapshot of the page as it appeared on 11 Jan 2012 03:21:10 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

[Text-only version](#)

date,ip,netspeed,organization,continent,country,region,city,latitude,longitude,browser,operating system,screen resolution,screen color,javascript,search engine,query,key

*10 Jan, Tue, 22:08:22", "82.90.23.35", "-", "SFR", "Europe", "France", "Ile-de-France", "Paris", "48.8667", "2.3333", "Android WebKit 2", "Android 2", "Other", "16 Bit (659

*10 Jan, Tue, 22:16:02", "81.245.24.64", "Cable/DSL", "Belgacom Skynet", "Europe", "Belgium", "Brabant", "Court-saint-Etienne", "50.65", "4.5667", "MSIE 8", "Windows 7", "1280x1024",

*10 Jan, Tue, 22:20:02", "81.154.217.130", "Cable/DSL", "British Telecommunications", "Europe", "United Kingdom", "Essex", "Billericay", "51.6167", "0.4166", "iPod Safari

*10 Jan, Tue, 22:20:30", "83.149.3.80", "-", "North-West Branch of OJSC MegaFon Network.", "Asia", "Russian Federation", "Saint Petersburg City", "Saint Petersburg", "59.8944", "3

*10 Jan, Tue, 22:21:44", "146.185.23.179", "-", "Hosting Services", "Europe", "United Kingdom", "Unknown", "Unknown", "54", "2", "Opera 10", "Windows 7", "1366x768", "32 Bit (16.7M)

*10 Jan, Tue, 22:23:49", "89.248.174.73", "-", "ECATEL DEDICATED & RESELLERS", "Europe", "Netherlands", "Unknown", "Unknown", "52.5", "5.75", "Opera 10", "Windows 7", "1366x768", "32

*10 Jan, Tue, 22:27:01", "212.123.174.239", "Cable/DSL", "Telfort Internet", "Europe", "Netherlands", "Zuid-Holland", "Oud-beijerland", "51.8333", "4.4166", "MSIE 9", "Win

*10 Jan, Tue, 22:42:48", "81.245.24.64", "Cable/DSL", "Belgacom Skynet", "Europe", "Belgium", "Brabant", "Court-saint-Etienne", "50.65", "4.5667", "MSIE 8", "Windows 7", "1280x1024",

*10 Jan, Tue, 22:55:27", "79.2.84.178", "Cable/DSL", "Telecom Italia", "Europe", "Italy", "Emilia-Romagna", "Bologna", "44.4833", "11.3333", "Firefox 3", "Linux", "1366x768", "24 Bit

*10 Jan, Tue, 23:14:41", "81.165.168.103", "Cable/DSL", "Telenet N.V.", "Europe", "Belgium", "Limburg", "Hamont", "51.25", "5.5500", "Firefox 9", "Windows XP", "1024x768", "

*10 Jan, Tue, 23:44:39", "82.99.191.12", "-", "ERKOR spol s r.o.", "Europe", "Czech Republic", "Kralovehradecky Kraj", "Rychnov Nad Kneznou", "50.1667", "16.2833", "MSIE 9", "Wind

*10 Jan, Tue, 23:50:120", "78.80.239.81", "Cable/DSL", "Alice DSL", "Europe", "Germany", "Baden-Württemberg", "Heilbronn", "49.1403", "9.22", "AOL 9", "Windows 7", "1280x1024", "24 Bit

*11 Jan, Wed, 00:01:34", "82.7.163.173", "Cable/DSL", "Virgin Media", "Europe", "United Kingdom", "Bedfordshire", "Letchworth", "51.9667", "0.2167", "iPod Safari", "iPod

*11 Jan, Wed, 00:20:44", "93.96.106.155", "Cable/DSL", "Be Un Limited", "Europe", "United Kingdom", "Nottinghamshire", "Kettering", "52.4", "0.7167", "Firefox 9", "Wind

*11 Jan, Wed, 00:39:40", "87.147.43.24", "Cable/DSL", "Deutsche Telekom AG", "Europe", "Germany", "Sachsen", "Lichtenau", "50.55", "12.55", "MSIE 7", "Windows Vista", "1024x768", "32

*11 Jan, Wed, 00:47:48", "91.82.129.170", "Cable/DSL", "Invitel Tavkozlesi Zrt.", "Europe", "Hungary", "Veszprem", "Veszprem", "47.1", "17.9167", "MSIE 8", "Windows XP", "1366x768", "

*11 Jan, Wed, 00:55:26", "195.93.21.35", "Dial-Up", "America Online", "Europe", "United Kingdom", "Unknown", "Unknown", "54", "2", "AOL 9", "Windows XP", "1152x864", "32 Bit (16.7M)

*11 Jan, Wed, 01:33:56", "81.158.102.230", "Cable/DSL", "British Telecommunications", "Europe", "United Kingdom", "Cheshire", "Chester", "53.2", "2.9166", "Firefox 8", "W

*11 Jan, Wed, 02:38:58", "83.149.3.96", "-", "North-West Branch of OJSC MegaFon Network.", "Asia", "Russian Federation", "Saint Petersburg City", "Saint Petersburg", "59.8944", "3

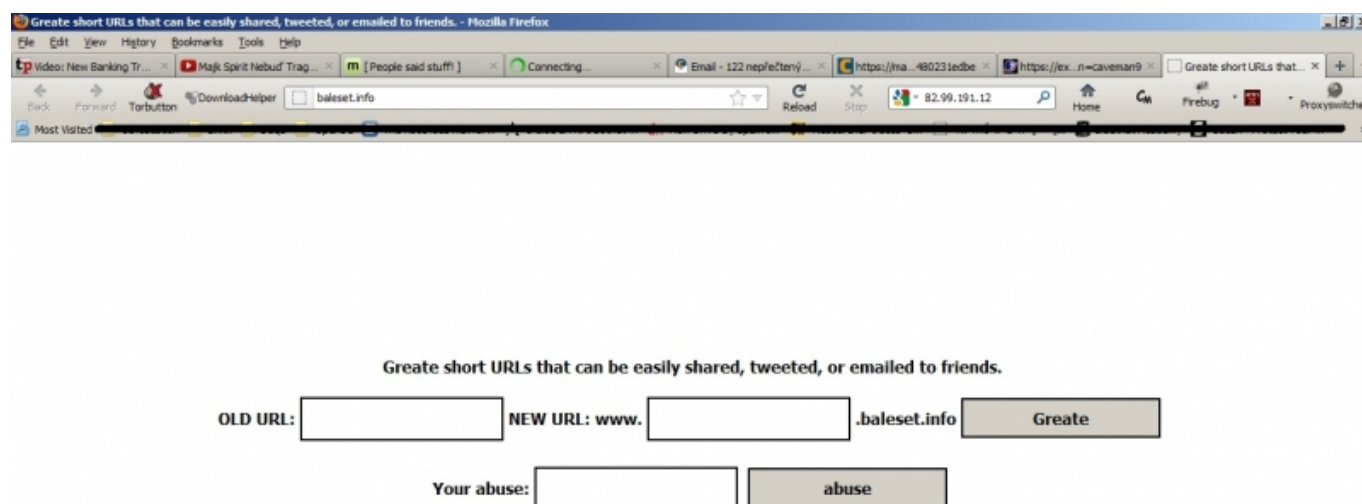
*11 Jan, Wed, 03:53:43", "99.246.61.173", "Cable/DSL", "Rogers Cable", "North America", "Canada", "Ontario", "Ottawa", "45.4167", "75.7", "MSIE 9", "Windows 7", "1920x1200", "24 Bit

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.

Analýza podvodného webu (rogue website)

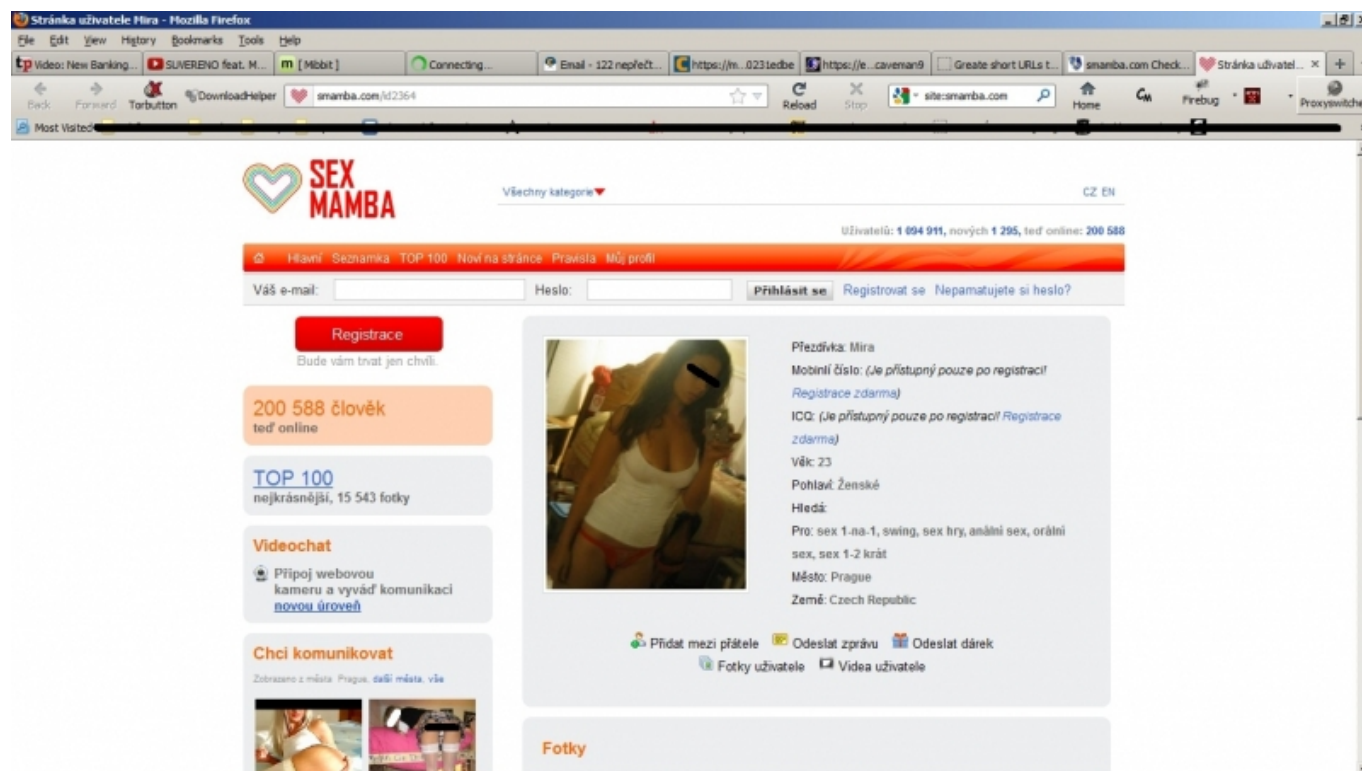
Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)



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

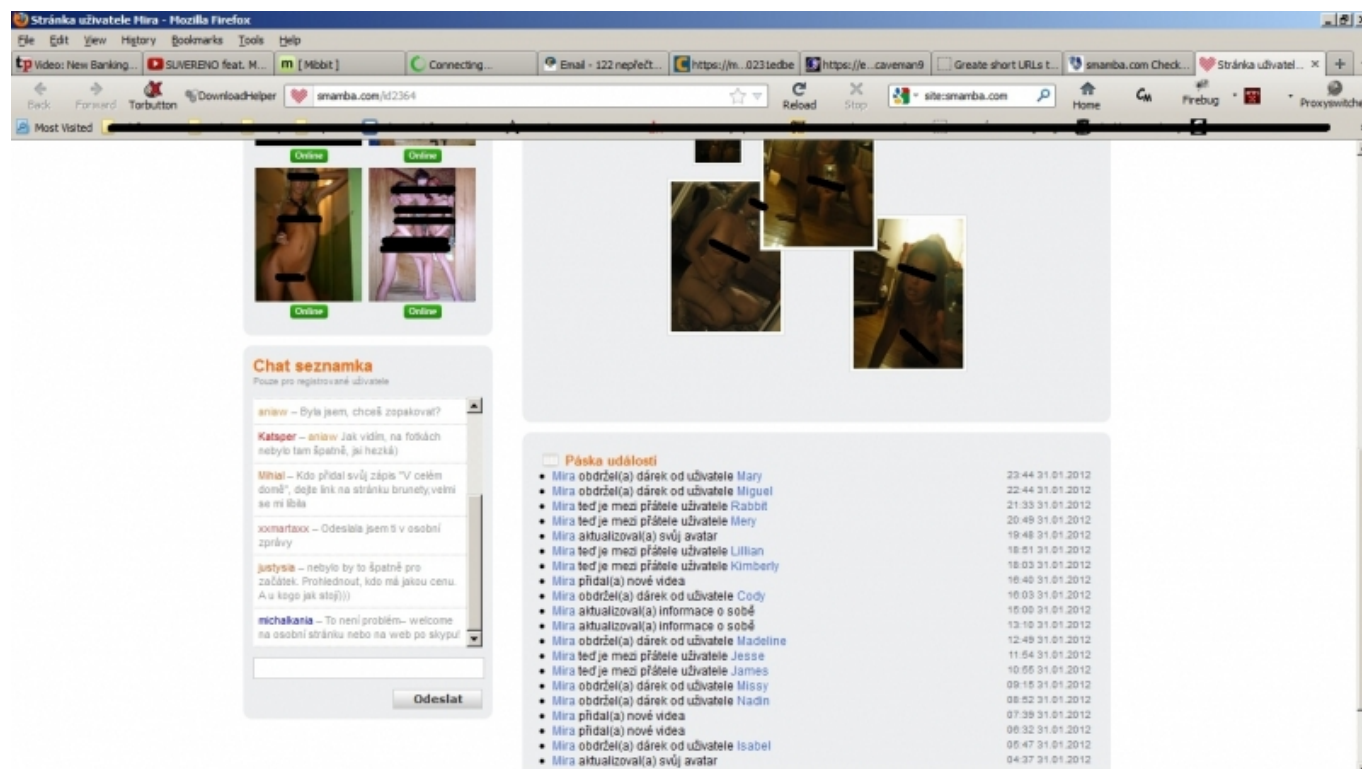
Na první pohled se jedná o legitimní stránku a nic nenasvědčuje, že by mělo jít o podvod. Dokonce i google mlčí a vrací pouze odkazy na jednotlivé profily. Služba www.safersite.de [5] taktéž stránku považuje za víceméně důvěryhodnou. Pořád mi ale něco nehrálo. Pokud se podíváme do levé části

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Analýza podvodného webu (rogue website)

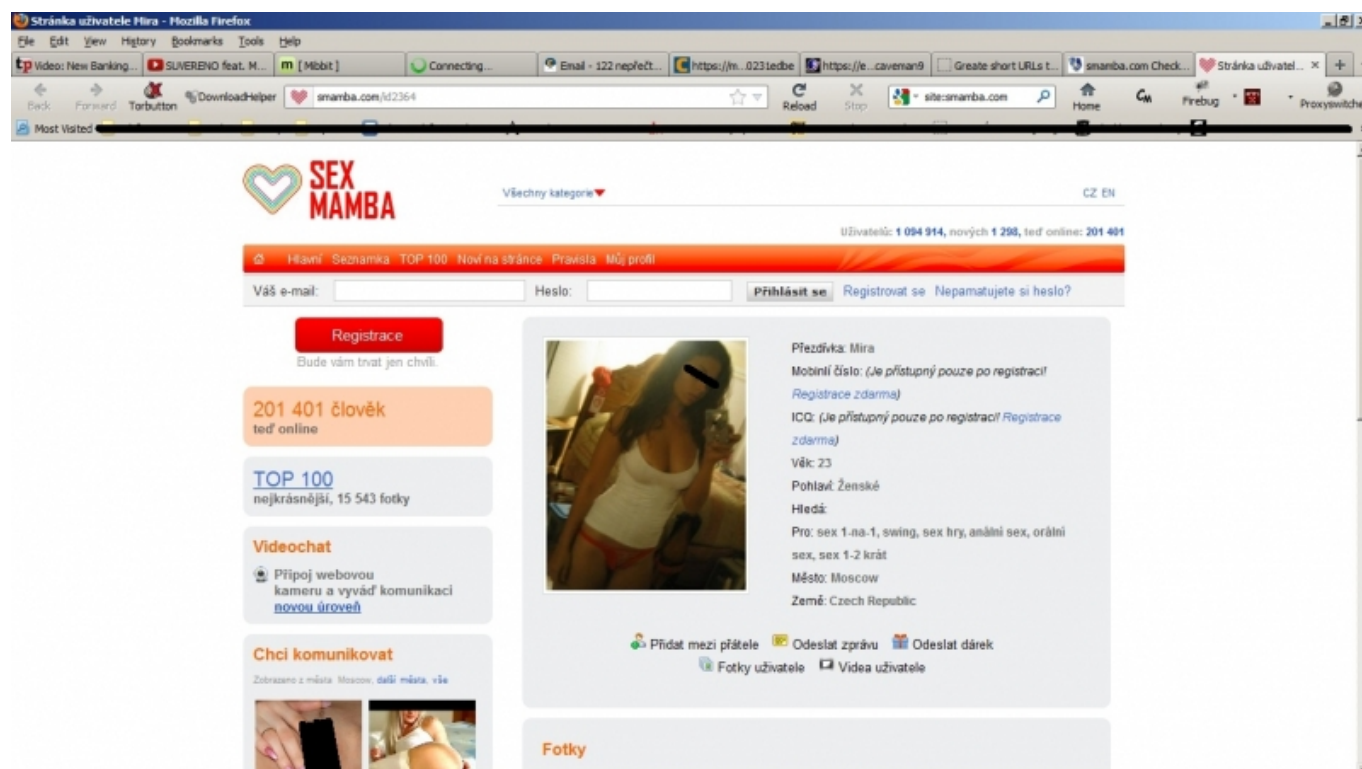
Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

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 vtípnou 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 dřívějšímu úplně stejné!!) kontakty vlevo.

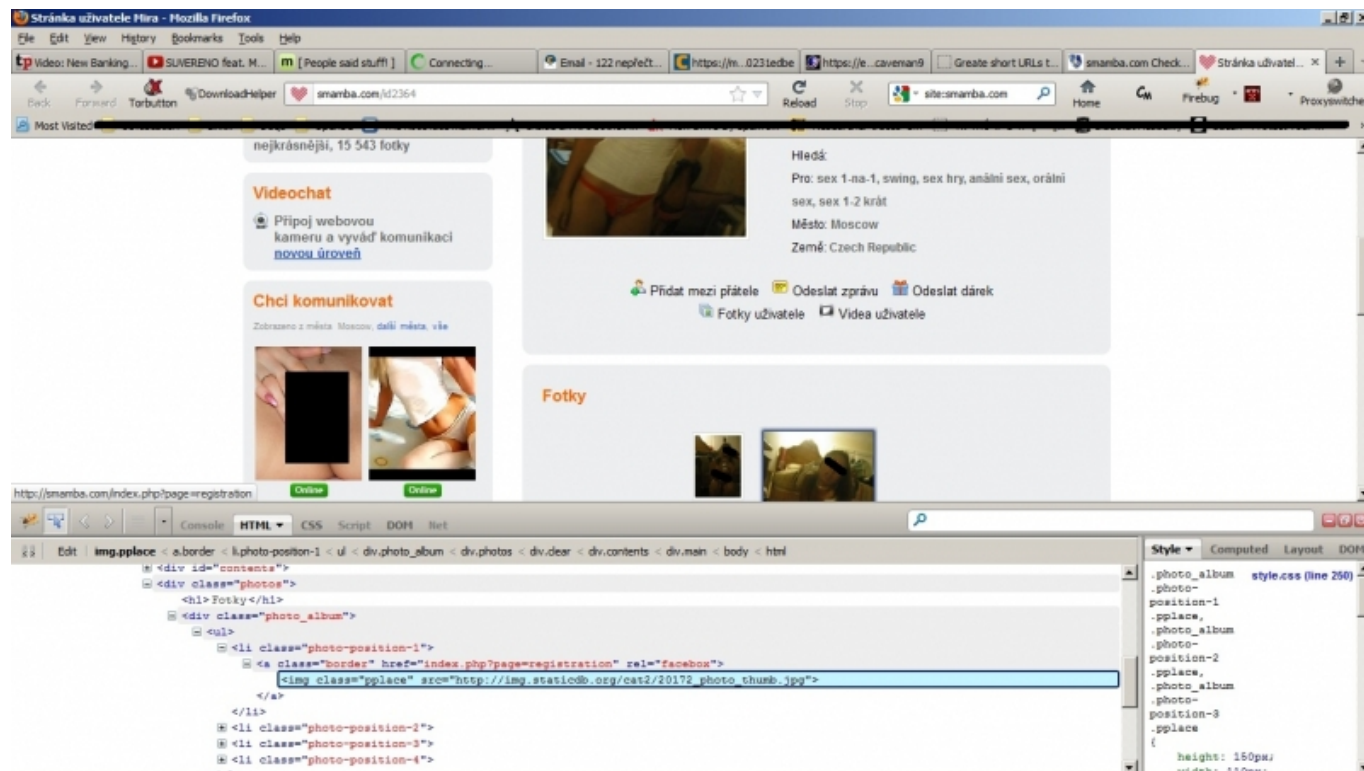


Moskva už je v České republice, stejně jako se bleskově 'přestěhovala Mira'

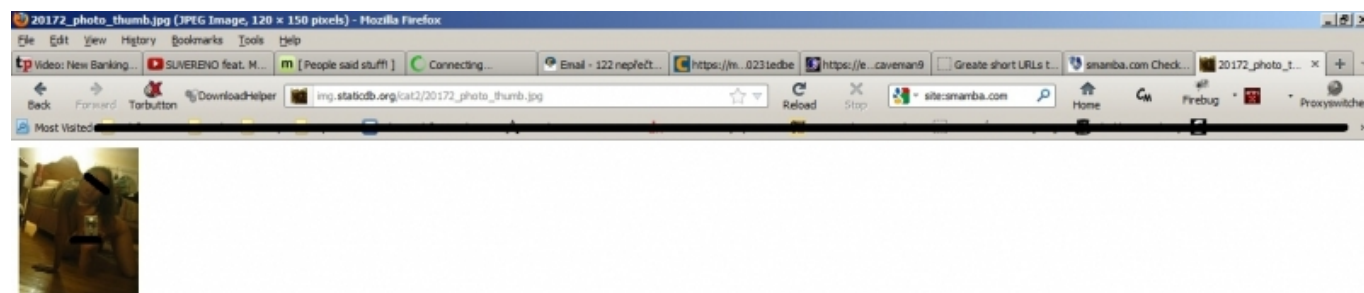
Analýza podvodného webu (rogue website)

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

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 ...



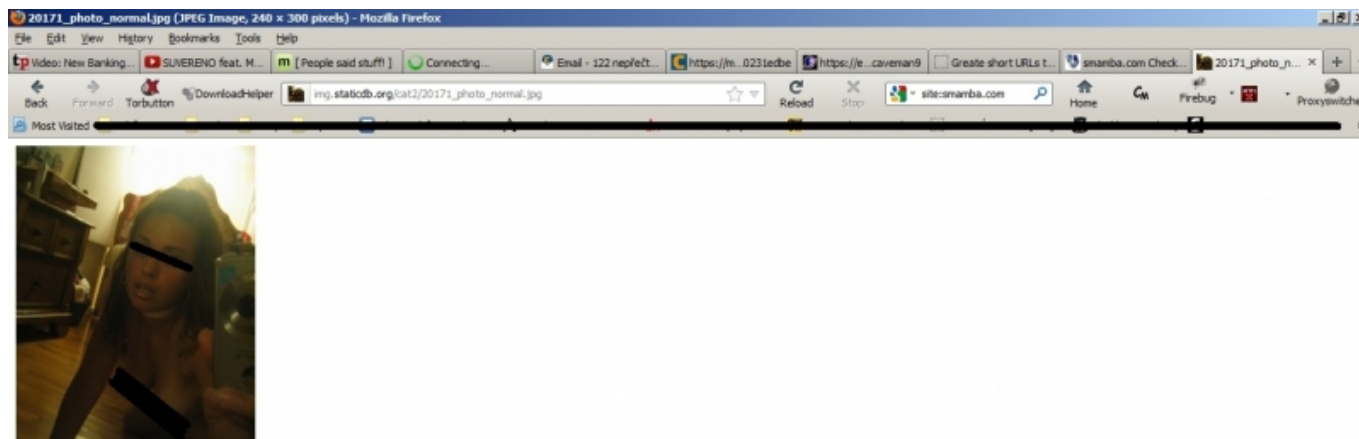
... a zmenšenina fotky (xxx_photo_thumb.jpg)

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 CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Analýza podvodného webu (rogue website)

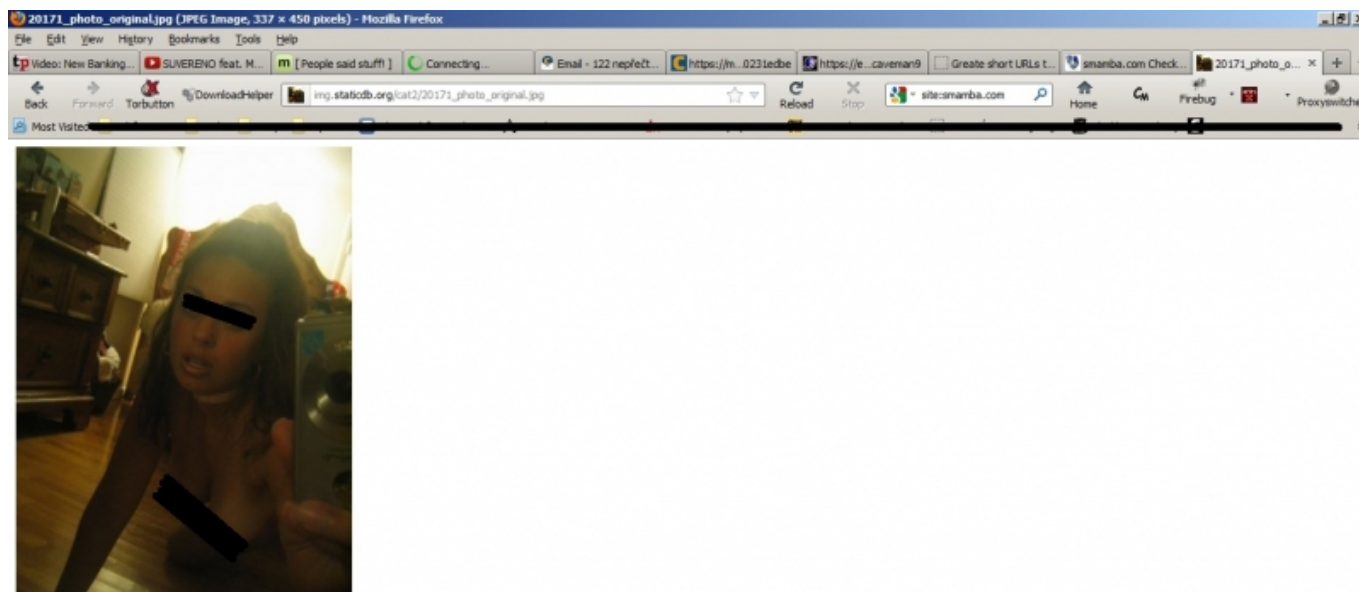
Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

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)

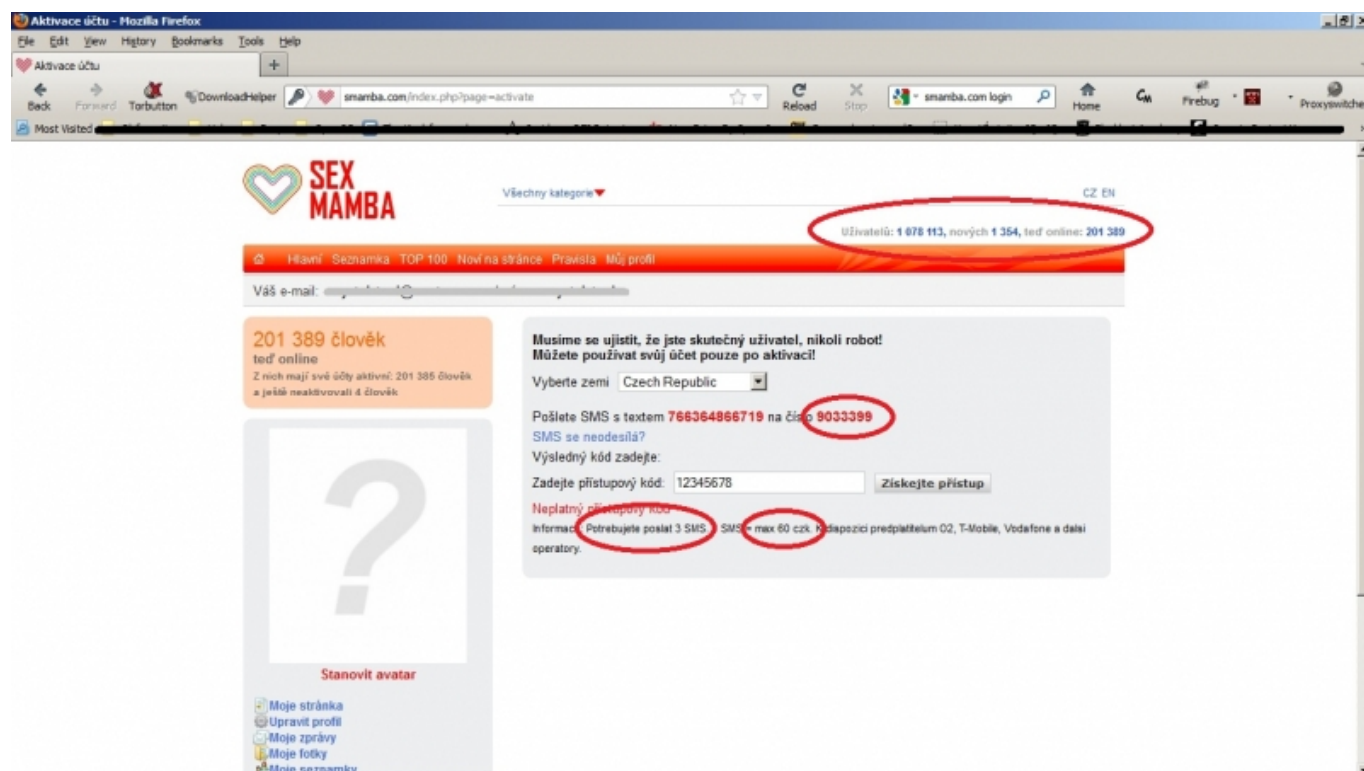
To už je znatelně lepší :) Prošel jsem pár adres směrem vzhůru a pár adres směrem dolů. Zjistil jsem, že adrey od hodnoty 20500 jsou patrně prázdné. Pro jistotu jsem si ale napsal jednoduchý PHP skript, jehož cílem bylo projít adresy od názvu fotky 1_photo_original.jpg do 20600_photo_original.jpg a uložit 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 CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

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. Nehledě 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 podvodné stránce je více než pravděpodobná.



Zaplať nebo nic neuvidíš!!

typ čísla	kdy	komentáře
Nebezpečné	20.01.2012	jsou to zloději peněz je to číslo na děvky / fotky/ se kterými se stejně nedá komunikovat
Nebezpečné	15.01.2012	Varuji před číslem 9033399 zloději peněz !!
Nebezpečné	15.01.2012	Je to podvod jako Brno... Žádná zpráva nepřijde a 99Kč a pak 50Kč strhnou !!
Obtěžující	30.12.2011	pěkná lumpárna, Když jsem chtěl vědět kam vnuk volal a provolal100kč nezjistil jsem nic, Lumpárna největšího zma, a to mi tvrdil.
Drahý hovor	30.12.2011	pěkná lumpárna, Když jsem chtěl vědět kam vnuk volal a provolal100kč nezjistil jsem nic, Lumpárna největšího zma,
Neutrální	24.12.2011	9033399...
Neutrální	20.12.2011	Benny hele je to číslo na ulož. to pro získání VIP.. čím víc sms pošleš tím víc si můžeš stáhnout GB
Nebezpečné	11.11.2011	tohle číslo využívá i internetová seznamka nakterou mi přišel odkaz ve spamu "sex-mamba" při aktivaci tvrdil, že je třeba zadat sms, která nebude stát víc než 5,- Kč
Nebezpečné	7.11.2011	Pokud na tohle číslo odesíláte kod 766334665235 znamená jen ze vyhazují 100Kč. Je to podvod.
Neutrální	19.09.2011	Tohle číslo je na placené SMS za 99 Kč, v souvislosti z odeslaným kódem je to platba za nejrůznější služby. Převážně od poskytovatelů nejrůznějších internetových "služeb". - VIP statusy, placené informace, vstupy na stránky, objemy dat na stahovací stránky atd.

Nová čísla v seznamu

607389776, 606493161, 603264513, 9093079, 9033399, 726480275, 723951155, 735972491, 732559672, 721289500.

603260672, 605766487, 4205761010367, 737642661, 722751347, 8007777777, 775652815, 720155777, 723281385, 604750011, 608971902, 602165399, 733161185, 722944422, 737674465, 603562504, 777208343, 604227022, 603808722, 602360666, 602336939, 725224004, 0420225351555, 724888082, 420956754160, 603701405, 312267573, 211152110, 724126005, 775940247, 420546606022, 728369205, 234694217, 773641287,

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

Z mé soukromé analýzy jsem udělal následující závěr

- E-mail pochází patrně z Ruska nebo ruský 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 milion "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>

Analýza podvodného webu (rogue website)

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

- [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