The Shadowserver Foundation

AS40989

RBN AS RBusiness Network

Clarifying the "guesswork" of Criminal Activity

The Russian Business Network

On or about November 6th, 2007 21:00 UTC [1] the primary group of networks run by a organization commonly referred to as *The Russian Business Network* [RBN] disappeared from the Internet. This is not the first time RBN's network has gone dark, but it is certainly the longest and probably the last. Due to a recent media blitz of sorts, pressure seems to have been exerted in the right places to surrender all hope for the network. In light of what would appear to be the abandonment of the ASN so vigorously reported on in the past few months, we have decided to clear the air of any possible questions regarding the legitimacy of complaints against the network. This report does not concentrate on any other malicious RBN activity other than the malware associated with AS40989.

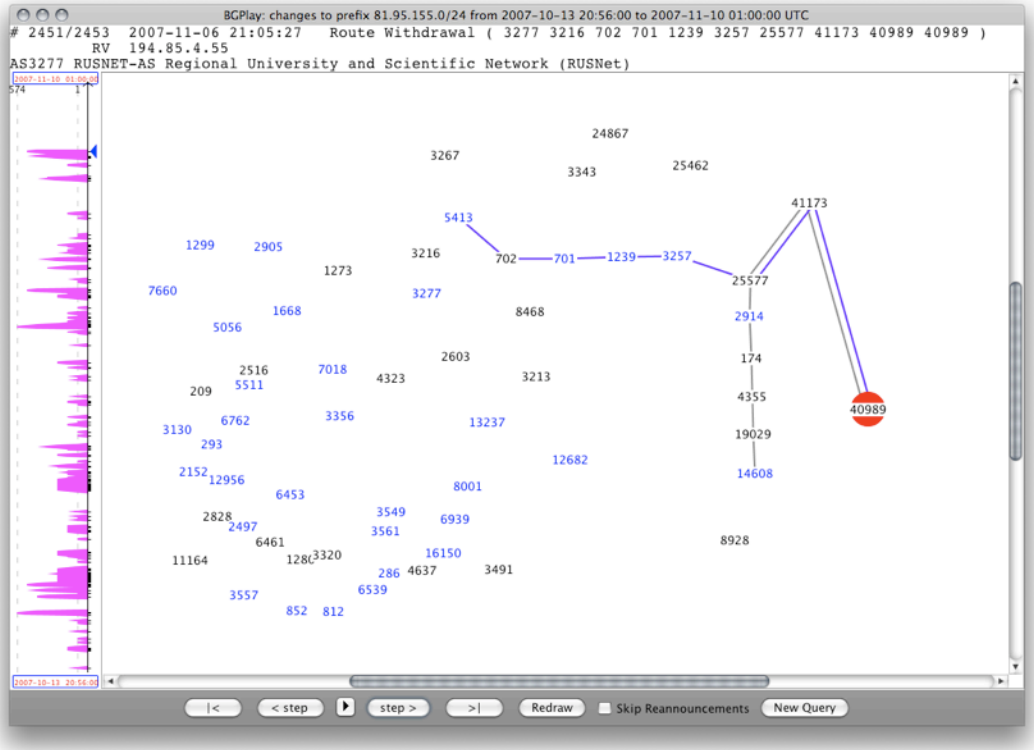


Figure 1.
Was it an experiment in attempting to bring a "brick and mortar" philosophy to the malware business or was it a virtual middle finger from Russia with love?

"We can't understand on which basis these organizations have such an opinion about our company," Jaret of the Russian Business Network told Wired in an e-mail interview. "We can say that this is subjective opinion based on these organizations' guesswork." [1]

-'Jaret' an RBN Spokesman

[1] Wired Magazine "Russian Hosting Firm Denies Criminal Ties, It May Sue Blacklister" Ryan Singel
http://www.wired.com/politics/security/news/2007/10/russian_network

Malicious Binary Activity Directed to and Commanded by AS40989

A Multitude of Samples

In our overall collection of sandnet run malware, AS40989 ranked #10 out of 1447 (November 2007) in having the highest number of unique pieces of malware communicating via HTTP with specific ASNs. As HTTP was the primary mode of communication with malware communicating with AS40989 we concentrated our statistical analysis on HTTP borne malware.

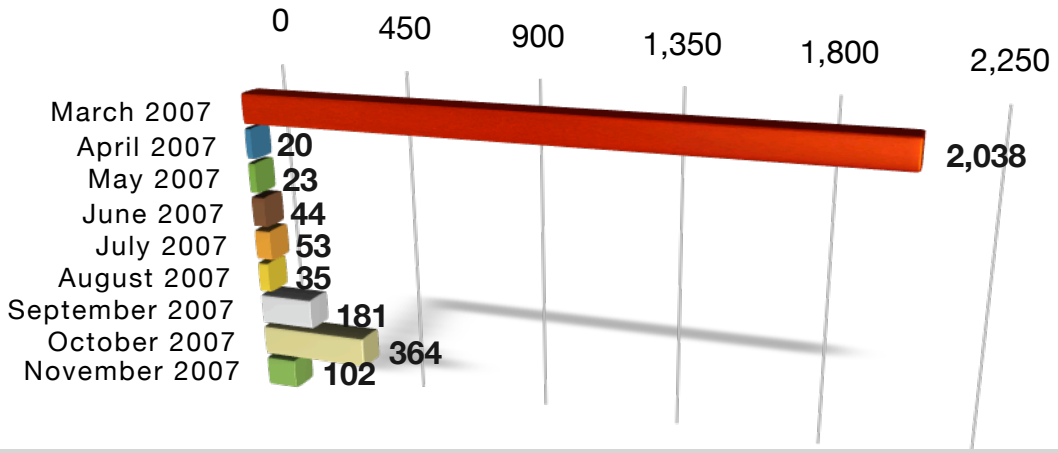


Figure 2.
Chart based on sandnet analysis of 2,859 pieces of malware which initiated HTTP connections to AS40989. Malware strains included but were not limited to: Gozi, Goldun, Hupigon, Nurech, Nuklus, Pinch, Sinowal, Tibs, Xorpix, various dialers, downloaders, worms, adware, page hijackers, and proxies.

RBN malware hosts have generally been run in a very professional manner. By "professional" it is meant that rarely are malware back-ends misconfigured or open to inspection and, rarely do they generate errors or move from host to host. While malware back-end infrastructures associated with other groups will move from provider to provider on a regular basis -- RBN hosts would service the same strains of malware from the same hosts for many months.

Significant Longevity

In Figure 3 we present an almost four month progression of a password stealing trojan communicating with the same back-end infrastructure and host. In that four month time period the back-end host the command and control URLs never changed, and no other strain was monitored communicating back to the host. It is believed the strain of malware in question was only publicly enumerated by Trend Micro[2] associating to RBN.

[2] Trend Micro - http://www.trendmicro.com/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY%5FSMALL%2EACF

Date	Host	Strain	MD5 Hash
2007-03-18 22:52:12	81.95.151.43	PWStealer	e618265920f99c3486573d38504a89d1
2007-03-19 00:05:47	81.95.151.43	PWStealer	cd5af5eaa55d7230fce91dc6229db358
2007-03-19 02:48:00	81.95.151.43	PWStealer	00c9c3c17baa83a24483a598dc016734
2007-03-19 13:15:49	81.95.151.43	PWStealer	acad21873331cf509f0d74fd2df0675c
2007-03-19 22:20:57	81.95.151.43	PWStealer	97860af5cfff0976c7a9d6ca2f8ae8b5
2007-03-19 23:47:20	81.95.151.43	PWStealer	f50c4761ee6f507081b8e89f418586c2
2007-03-22 22:01:15	81.95.151.43	PWStealer	4c2395a58f8e7c4b9f46f933fbb215eb
2007-03-23 11:05:26	81.95.151.43	PWStealer	6535d7901bf4cb1ca7d8dc7ca20a1520
2007-03-28 12:49:56	81.95.151.43	PWStealer	2fbcf521e4bc80d1f7f16a2e855f24a0
2007-03-28 14:54:32	81.95.151.43	PWStealer	0ed8bedb656fb0efbb0b8595afe4586b
2007-05-30 00:31:14	81.95.151.43	PWStealer	dfeefbc2ad8071a5b211fd3f68352a00
2007-05-30 06:28:35	81.95.151.43	PWStealer	74d0c935cff89ada398c7ee27b66a940
2007-06-01 06:43:41	81.95.151.43	PWStealer	325e705cbafa45fbf49b4ca16a08303b
2007-06-27 18:11:34	81.95.151.43	PWStealer	2705b6df862c3e9ce333d3da3b9437d2
2007-06-28 06:11:01	81.95.151.43	PWStealer	50007ff034f32951bf044f59a68d4add

Figure 3.
The malware stole credentials in Microsoft Protected Storage as well as open a SOCKS 5 proxy.

The Trend Micro analysis also notes a partially disclosed IP address of the back-end host their malware was taking commands from and reporting to. Their report indicates the first sample of this strain appearing to them in October 2006.

TREND MICRO ENUMERATED SAMPLE
Unknown MD5 Hash - http://81.95.{BLOCKED}.107/cgi-bin/pstore.cgi - October, 2006
SHADOWSERVER ENUMERATED SAMPLE
9bda4b33349b024e077f88601d3bbb68 - http://81.95.147.107/cgi-bin/pstore.cgi - July, 2007

In addition to the strain in Figure 3 we have 27 samples utilizing what would appear to be the same server as reported by Trend Micro. Our last sample which generated an active server response, was tested July 3rd, 2007. This equates, roughly, to a nine month period this strain of password stealing malware run from a single host in AS40989 address space. Both of the aforementioned strains also open a SOCKS 5 proxy on the infected hosts. Of course we now all know this malware by the name Gozi.

The AS40989 & Tibs Relationship

Tibs - The Longer Lived Storm

It is rarely reported in Storm news but, the Storm trojan so often making headlines the past few months had a parent. And it just so happens that this Storm precursor had a long and beneficial relationship with the RBN. Storm's precursor is known as Tibs (also related to or alternatively known as NuWar and Zhelatin).

Generally malware tagged as Tibs act as an agent taking command and control from an HTTP server and downloading additional malicious software. The malware which Tibs downloads typically consist of a spam engine (Zhelatin), but it is also known to install affiliate adware from "Matcash", SOCKS 5 servers, and additional remote control agents and keyloggers.

To call attention to these relationships we use a piece of Tibs malware run through our sandnet in March, 2007.

MD5 Hash	Host	FQDN	ASN
b57f0445acea54fd09750e0840bad3c8	69.50.175.181	download.bravesentry.com	INTERCAGE - 27595
b57f0445acea54fd09750e0840bad3c8	81.95.148.38	stattrader.biz	RBusiness Network - 40989
b57f0445acea54fd09750e0840bad3c8	81.95.148.38	stattrader.biz	RBusiness Network - 40989
b57f0445acea54fd09750e0840bad3c8	81.95.148.38	stattrader.biz	RBusiness Network - 40989
b57f0445acea54fd09750e0840bad3c8	81.95.148.38	stattrader.biz	RBusiness Network - 40989
b57f0445acea54fd09750e0840bad3c8	81.95.148.38	stattrader.biz	RBusiness Network - 40989
b57f0445acea54fd09750e0840bad3c8	81.95.148.38	stattrader.biz	RBusiness Network - 40989
b57f0445acea54fd09750e0840bad3c8	81.95.148.38	stattrader.biz	RBusiness Network - 40989
b57f0445acea54fd09750e0840bad3c8	81.95.148.38	stattrader.biz	RBusiness Network - 40989
b57f0445acea54fd09750e0840bad3c8	85.255.114.164	85.255.114.164	INTERCAGE - 27595

Figure 4.
Trojan.Tibs.Gen!Pac.80 Drive-by drop from RBN Host: http://stattrader.biz/

The files downloaded from the RBN host are, as described by their AV classifications and sandnet output, all components of Tibs. The Intercage downloads are the Bravesentry Rogueware[3] and a dialer.

Further enumeration of a Tibs and RBN relationship can be seen in the *fa4ecd2cef35bc3ba13fe2a353eca30a* sample wherein the RBN host 81.95.146.245 was utilized for command and control.

At least 10 RBN hosts were tracked hosting Tibs components.

The AS40989 Range of Malicious Code & Hosts

Cross section sampling of malicious RBN code

While RBN may profess innocence regarding the malicious nature of software hosted on its infrastructure as well as the malware built to communicate with the RBN infrastructure it is quite clear that their business model was almost wholly based on the distribution of software to spam and steal personal information. Figure 5 clearly illustrates the vast breadth of malware associated with RBN hosts. While this table does not completely represent of all tracked hosts and malware strains from AS40989, it does give a an accurate indication to the range of malware and their back-ends running out of RBN address space.

[3] Bravesentry Rogueware - http://research.sunbelt-software.com/threatdisplay.aspx?name=bravesentry&threatid=44152

Malware Classifications Across a Selection of RBN Hosts

Host	Strain	Host	Strain
81.95.144.59	Downloader	81.95.144.146	Nurech
81.95.144.75	Sinowal	81.95.144.172	Cimuz
81.95.144.77	Banker	81.95.144.221	Tibs

Host	Strain	Host	Strain
81.95.146.112	Tibs	81.95.146.147	Downloader.Agent
81.95.146.132	SpyForms	81.95.146.148	SelfStarterInternetTrojan
81.95.146.133	SpyForms	81.95.146.236	Backdoor.Delf

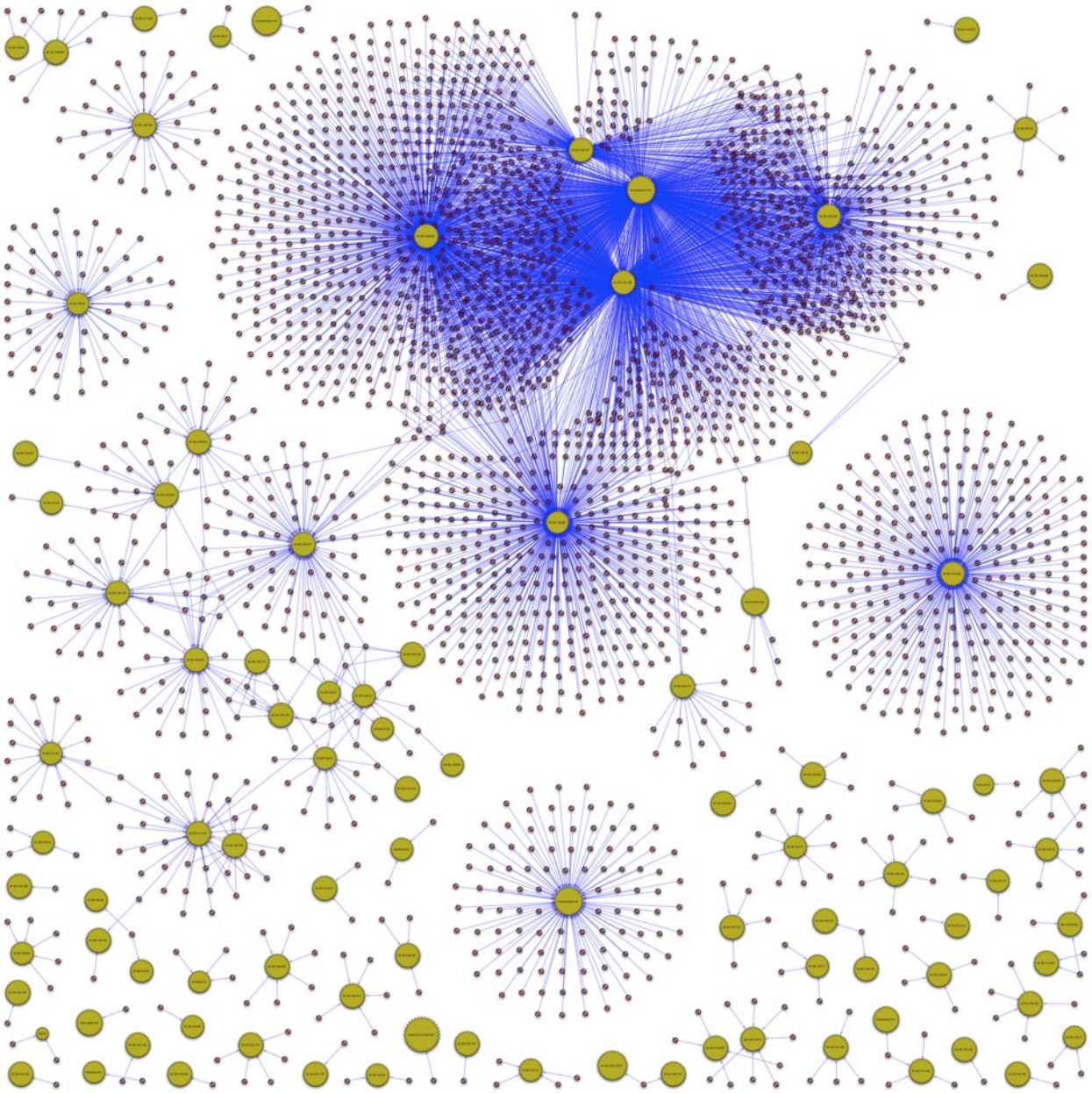
Host	Strain	Host	Strain
81.95.148.10	CL.Agent	81.95.148.155	Banker
81.95.148.14	Downloader.Agent	81.95.148.187	Hupigon
81.95.148.38	Tibs	81.95.148.244	Banker

Host	Strain	Host	Strain
81.95.149.165	Zeus	81.95.149.235	SpamTool.Win32.Delf
81.95.149.166	Sinowal	81.95.149.237	Downloader.Agent
81.95.149.34	Daemonize	81.95.149.250	Nurech

Host	Strain	Host	Strain
81.95.150.42	Pinch	81.95.150.82	Zeus
81.95.150.50	Nurech	81.95.150.52	Downloader-lcg
81.95.150.74	Zeus	81.95.151.43	PWStealer

Figure 4.
Chart spans six /24 networks. Multiple information thieves, remote control, and spam tools.

Visualizing Relationships between Malware and Hosts in AS40989



AS40989 (RBN) - "A Year of Malware in Review"

Figure 5.
Plotted representation of 94 RBN hosts, 2662 pieces of selected malware, and their relationships. Larger (7 MB) version is available at http://public.box.net/ssimages.
Legend: Gold Starburst is Host/IP, Red Icon is Unique Malware, Blue Arrow is HTTP Traffic

Notes and Comments

AS40989 Notes and Comments

RBN, and more specifically, AS40989 was a known rogue network well before we began purposefully keeping statistics on the network. Any takedown notifications sent by Shadowserver to the network before and after we kept these published statistics were never acted upon by anyone associated with RBN. While there was serious consideration within Shadowserver for publicly "outing" RBN we received enough push-back from other researchers to indefinitely hold any public comment on the network.

On reflection it is disconcerting that it seems to have taken the visibility from the Washington Post[4] and Wired articles to bring the necessary pressure to bear on this network to affect its disappearance. While public movement against the network took considerably longer than it should have in our opinion, it is worth noting that around late August the temperament of researchers toward publicly outing known rogue networks seemed to significantly warm. And, from a distance, this tactic seems to have been overall very effective.

Broken Windows, Zero Tolerance and Quality of Internet Life

Historically, with a few notable exceptions, we have had little reason to expect modern computer criminals to continually utilize a singular network space as their primary hub of distribution and communication with malware. Additionally, the breakup of AS40989 has shown that there is little reason to believe that occasional network takedowns alone will truly curb their ability to distribute their malicious wares. Yet, as has been debated in other areas of rampant crime, it is certainly arguable that creating a consistently inhospitable atmosphere for criminal activity can curb the crime. So while it is laudable that AS40989 was held to task regarding its safehousing for criminal activity it certainly isn't enough.

Anyone who has seen numerous caches of gigabytes of keylog data over time cannot realistically continue to write off these criminal exploits as minor annoyances. These are real crimes, affecting real people and the air of "tolerance for research" is increasingly becoming too polluted for many to bear.

To this end we would like to bring back to debate the practice of publicly publishing known rogue networks, ASPs and ISPs in a format that is accessible to most any interested parties. This is not suggested lightly, nor without due consideration of the issues in past debates. It is however being suggested again given the following beliefs:

- the initial audience of this paper knew about RBN and its practices long before any effective action was taken to remove the general threat it posed
- networks utilized for criminal activities with unresponsive or non-existent abuse departments which are not prosecuted or brought to light of the public eye are disproportionately responsible more malware propagation than larger responsibly run networks
- breeding an atmosphere of intolerance toward networks which harbor criminal activities can be achieved with minimal to no impact to ongoing criminal investigations

---

[4] Washington Post - Security Fix "Mapping the Russian Business Network" Brian Krebs http://blog.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html

Acknowledgements

Thanks To:

Everyone in Shadowserver and members of the [II] mailing list.

This document was compiled in November of 2007, shelved in December 2007 and finalized and released in January 2008.