From: "Aaron Barr" <aaron@hbgary.com>
To: "Greg Hoglund" <greg@hbgary.com>
Sent: Friday, February 05, 2010 9:29 AM
Subject: Fwd: EndGames Report Images

Begin forwarded message:

From: Aaron Barr <aaron@hbgary.com>
Date: February 5, 2010 9:24:24 AM EST
To: Aaron Barr <aaron@hbgary.com>
Subject: EndGames Report Images

Computer Network Operations Profile

This section details the Russian Federation's Internet Profile, with a specific temporal focus on December, 2009. EGS passively detected over nine million unique events[1]. Additionally, EGS actively detected web-facing assets, some of which reveal vulnerabilities in key organizations within the Russian Federation.

Botnet Activity

Figure 1 shows the number of daily unique botnet infections for the month of December. On average, EGS collected 360,469 unique events every day. Even if the spike on 2009-12-27 were treated as an outlier, the average represents a 133% increase from the first day of data collection.

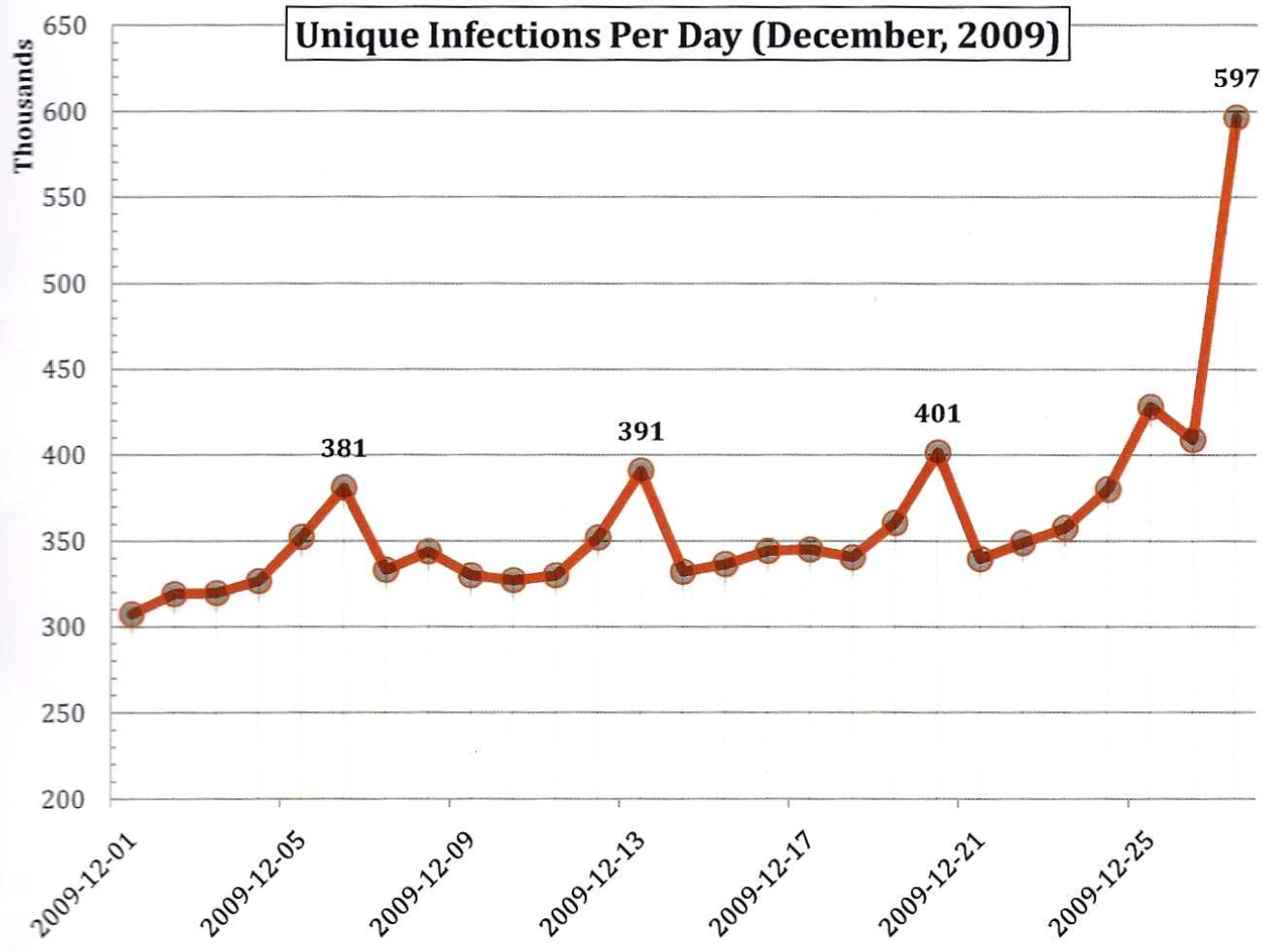

Figure 1: Number of unique infections per day between 2009-12-01 and 2009-12-27.

[1] Endgames' Cayman data repository has accumulated over 63,531,332 events, of which 9,732,651 are unique events, for Russia during the month of December, 2009.

Figure 2 - Visual representation of infected regions in Russia.

EGS creates visual models of infection for any given country. Figure 2 represents the geographical distribution of particular infections detected passively in December 2009 in Russia.

collects data and tracks a wide variety of botnets and general malicious C2 traffic. For example, Figure 3 shows the top three botnet infections discovered in Russia; however, EGS also tracks some much smaller individual botnets (e.g. Tiniresu, Bobax, HacDef-0, NP-NFC, RAT) that are also active in Russia.

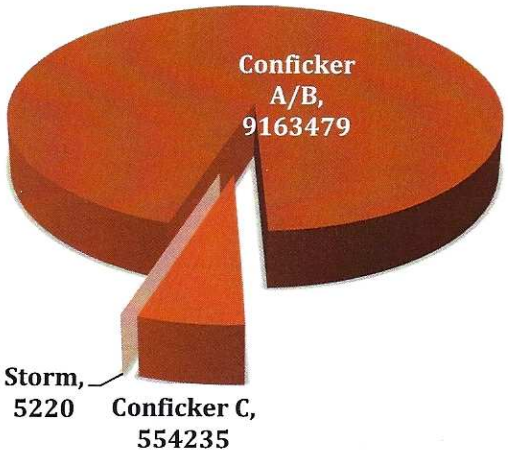

Figure 3 - Top Three Botnet Infections in Rus

Two particularly powerful capabilities EGS possesses involve detecting infections of particular registered organizations and autonomous system routes. Table 1 shows the Top 10 registered organizations carrying malicious traffic *en masse*. Broadly, the top infected organizations in any country are Internet service providers, which is the case in Russia. This points to individual users, not large government or company networks, showing the most botnet activity. However, Appendix A shows some infected organizations of interest, mostly governmental and infrastructure-related.

Table 1 - Top ten infected Organizations

Number of Infections	Name of Infected Organization
1,203,230	Investelektrosviaz Ltd.
579,653	OJSC North-West Telecom
544,441	Dynamic distribution IP's for broadband services
362,185	OJSC Sibirtelecom
331,460	Network for PPPoE clients terminations in
170,009	infrastructure in Msk
157,659	CJSC Company ER-Telecom
150,352	Oleg A. Yurlov
135,223	Network of Saratov branch of OJSC Volgatelecom
123,117	Comstar-Direct CJSC

Table 2 - Top ten identified infected autonomous system number prefixes.

Number of Infections	AS Number	AS Name
1,119,637	8402	CORBINA-AS Corbina Telecom
583,921	8997	ASN-SPBNIT OJSC North-West Telecom Autonomous System
345,530	25405	NMTS-AS OJSC VolgaTelecom Nizhny Novgorod
330,511	41440	SIBIRTELECOM-AS Sibirtelecom backbone AS
261,360	47395	SCARTEL-AS Scartel Ltd.
219,297	8359	COMSTAR COMSTAR-Direct global network
184,658	16345	BEE-AS JSC _VimpelCom_
167,180	15500	OJSC VolgaTelecom
162,595	12705	PFES OJSC _Uralsviazinform_
149,110	6828	USI Uralsviazinform

Table 3 - Browser distribution Ratio

% Used	Browser
99.70%	Mozilla/4.0
0.14%	Mozilla/5.0
0.02%	OPERA/9.6
0.02%	OPERA/9.4
0.02%	OPERA/9.8

User-Agent Analysis

EGS is able to make inferences and affirmations through the use of user-agent strings provided via data collection. User-Agent strings contain invaluable information about web components that particular user is using during their Internet usage. This information can lead to actionable intelligence for CNA efforts.

- Our collection of Russian data shows that the majority (approximately 94.5%) of the infected users are running a 32-bit version of Window XP; Table 4 shows the distribution.

Table 4 - Running operating system detection numbers.

Identified Version	Number of Detections	Approx. OS Version
Windows NT 5.1	9,199,530	Windows XP 32-bit
Windows NT 6.0	450,137	Windows Vista
Windows NT 5.0	37,075	Windows 2000
Windows NT 5.2	24,680	Windows XP 64-bit
Windows NT 6.1	226	Windows 7

- MRSPUTNIK 2 is an agent tracker add-on, generally found pre-configured with custom Browser installations. One such example is FunWebProducts, a customer web browser commonly used for ad-ware/spyware distribution[2].
    - Number of unique WebProduct browser installations: `51,115`
    - Number of unique MRSPUTNIK 2 add-on installations: `2,852,572`

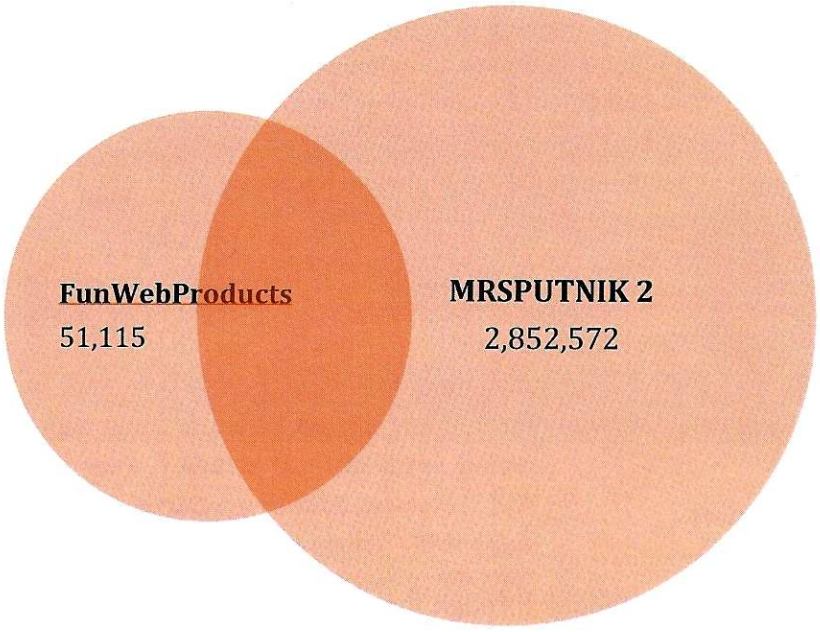

Figure 4 - Represents the overlap between the MRSPUTNIK add-on and the custom browser product, FunWebProducts

[2] Gibbs, Mark; Network World, "No Fun with FunWebProducts", 2003, 12, 10; http://www.networkworld.com/newsletters/web/2003/1208web2.html

Web-facing Assets

In mid-2009, EGS mapped Russian IP space using active reconnaissance techniques. The scope of the project involved crawling 26,449,591 unique locations. The data below summarizes the mapping results:

- HTTP servers: 601,676
- HTTPS servers: 267,531
- Total servers: 869,207
- Unique servers: 650,755
- SSL certs retrieved: 107,838
- Total seeds: 709,514

Web Servers

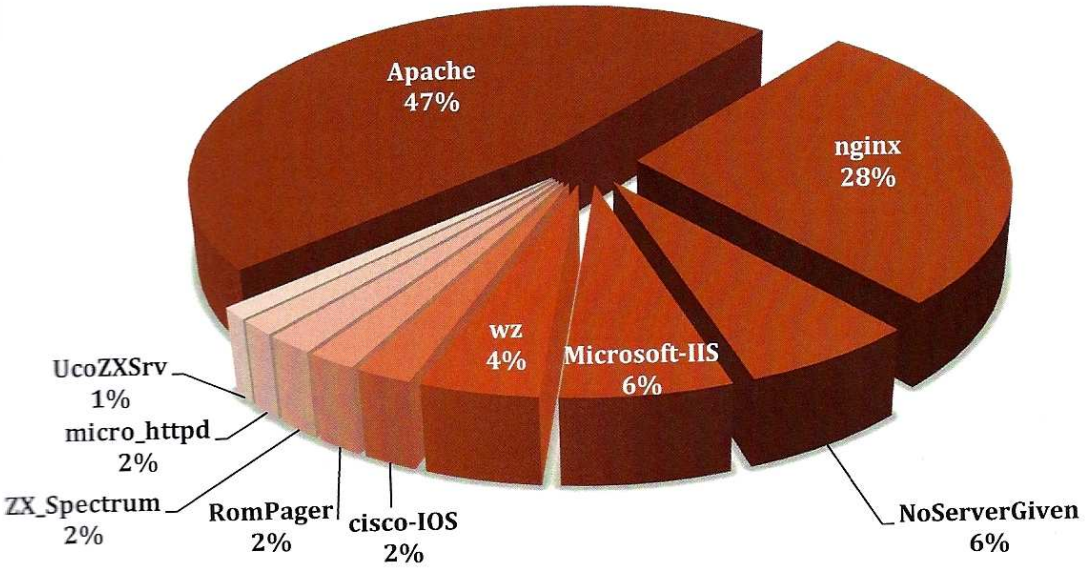

Figure 5 - Top ten web servers detected during mapping.[3]

Figure 5 shows the top ten web servers identified through the mapping project of Russia[4]; overall, there are over 800 uniquely identifiable base web servers. On some servers, it is possible to add modules, which add or modify a particular capability to suit the needs of its users. These modules

[3] *NoServerGiven* is an identification we apply in conditions that are nondeterministic. For example, this value will be applied when the server header value is missing (i.e. the server did not identify itself or it supplied the server header without a value).

[4] Some notable web servers that are not among the ten most numerous in Russia include Oracle Application Server 10g, lighttpd, and GoAhead-Webs.

are detectable, notably on Apache servers, and when these are included in the analysis, there are at least 22,605 uniquely identifiable web servers. Modules can be useful in linking seemingly disparate organizations; if more than one organization shares a particular combination of modules, it is conceivable that they might also share a parent organization, or at least an IT provider.

Table 5 details platform distribution.

Table 5 - Listing of identified platforms

# Identified	Server Platform
177580	(Unix)
110570	Unknown
58598	(FreeBSD)
24960	(Debian)
23383	(Fedora)
22751	(CentOS)
19448	(Win32)
18163	(Sinclair_BASIC)
8571	(Red Hat)
5785	(Ubuntu)
4620	(Linux/SUSE)

For further information, please reference Appendix C for a larger listing of discovered servers and Appendix D for a larger listing of discovered modules.

Another area of interest are the web application, devices, and assets EGS discovers during the mapping process. Figure 6 shows the top 10 identified web applications currently in use; other web applications of interest, not shown above, are MikroTik Router Admin, Webmin, phpMyAdmin, and Open WebMail. Overall, there were 93 unique applications discovered, disregarding specific version information for simplicity.

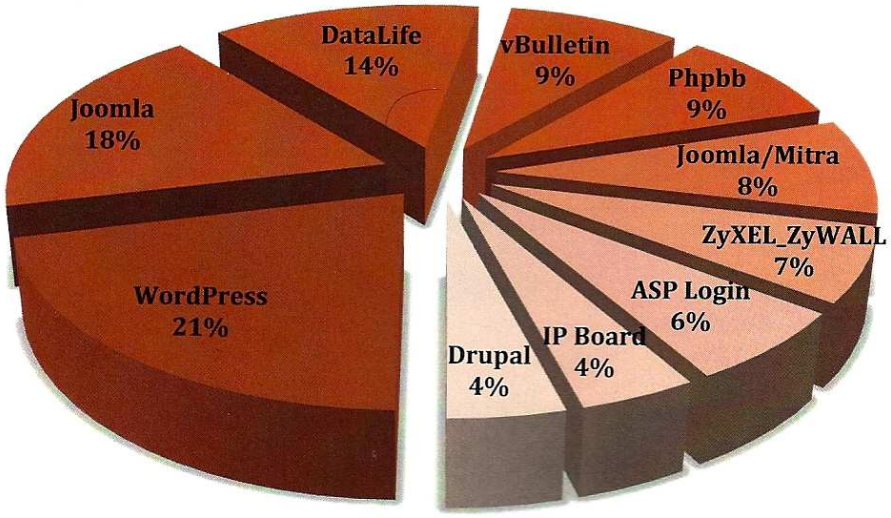

Figure 6 - Top 10 identified web applications

More detail of selected vulnerable assets discovered and selected organizations are shown in Appendix B.

Appendix A

The data shown below is not an inclusive list of the data discovered.

Infected Organizations Of Interest

IP	Organization	City	Infections
195.19.189.0/24	Administration of Perm region	Perm	4
83.146.74.0/24	Administration of Kurgan oblast	Kurgan	8
82.162.127.32/28 82.162.142.176/28 86.102.119.32/28	Administration of Vladivostok	Vladivostok	1
193.150.0.0/17 212.14.203.0/24 212.40.192.0/24 212.40.193.0/24 212.40.194.0/24	Central Dept. for Central Bank of Russian Fed.	Moscow	249
83.242.131.64/28 89.175.22.32/28 212.154.169.104/29	Embassy USA	Moscow	4
195.80.224.0/24	Ministry of Finance	Moscow	4
83.221.217.0/25 98.129.217.32/29 217.106.58.208/28 ... (too many to list) ... 217.107.209.0/24	Ministry of Taxation (various regions)	(various)	21
82.204.182.192/27 212.176.54.32/28 212.176.63.192/28	National Reserve Bank	Moscow	4
195.98.93.64/26	Novovoronezh Nuclear Power Plant	Novovoronezh	1
81.195.129.248/29	EL AL ISRAEL AIRLINES LTD (Izrailskie avalinii)	Moscow	1

Appendix B

The data shown below is not an inclusive list of the data discovered.

Web servers table

IP	Organization	City	Server
194.84.134.33/32 194.84.134.34/31 194.84.134.36/31	Sberbank	Irkutsk	RomPager/4.06
212.41.1.154/31 212.41.1.156/31	Achinsk Oil Refinery Plant	Achinsk	Apache/2.2.0 (Linux/SUSE) Apache/2.2.8 (Win32)
83.146.74.1/32 83.146.74.2/31 83.146.74.4/30 83.146.74.8/29 83.146.74.16/28 83.146.74.32/27 83.146.74.64/27 83.146.74.96/28 83.146.74.112/29 83.146.74.120/30 83.146.74.124/31	Administration of Kurgan Oblast	Kurgan	Apache/2.2.8 (Linux/SUSE) Apache-Coyote/1.1 Apache/2.2.4 (Linux/SUSE) Apache/2.2.4 (FreeBSD)[5] Microsoft-IIS/6.0 Apache/1.3.37 (Unix)[6] Apache/2.2.10 (Linux/SUSE) Apache/1.3.31 (Unix)[7] Apache/1.3.34 (Unix)[8]
195.19.189.0/24	Administration of Perm Region	Perm	Apache/2.2.3 (FreeBSD)[9] Apache/2.0.48 (Win32)[10] cisco-IOS Apache/2.2.4 (Win32)[11] Apache/2.2.4 Microsoft-IIS/7.0 Apache/1.3.33 (Win32)[12]
80.92.34.0/24	Aeroflot Moscow Sheremetevo Airport	Moscow	Lotus-Domino Apache/2.0.52 (Win32)[13] Apache/1.3.33 (Win32)[14] Cisco AWARE 2.0 IMB_HTTP_Server
212.120.164.129 89.20.101.201	Aeroflot Russian Air Lines Ltd	Moscow Perm	RomPager/4.07 UPnP/1.0 RomPager/4.51 UPnP/1.0
217.12.96.64/31 217.12.96.0/24	Alfa Bank	Moscow	Microsoft-IIS/6.0 IBM HTTP Server/6.0[15] Lotus-Domino Apache/2.0.59 (Linus/SUSE)

[5] Apache/2.2.4 (FreeBSD) mod_ssl/2.2.4 OpenSSL/0.9.7e-p1 DAV/2 PHP/4.4.7 with Suhosin-Patch
[6] Apache/1.3.37 (Unix) mod_ssl/2.8.28 OpenSSL/0.9.7e-p1
[7] Apache/1.3.31 (Unix) PHP/4.4.9
[8] Apache/1.3.34 (Unix) PHP/4.4.2
[9] Apache/2.2.3 (FreeBSD) DAV/2 PHP/5.2.6 mod_ssl/2.2.3 OpenSSL/0.9.7e-p1
[10] Apache/2.0.48 (Win32) PHP/4.3.4
[11] Apache/2.2.4 (Win32) PHP/5.2.3
[12] Apache/1.3.33 (Win32) PHP/4.3.11
[13] Apache/2.0.52 (Win32) mod_ssl/2.0.52 OpenSSL/0.9.7e PHP/5.0.2
[14] Apache/1.3.33 (Win32) mod_ssl/2.8.22 OpenSSL/0.9.7e PHP/4.3.4
[15] IBM_HTTP_Server/6.0 Apache/2.0.47 (Win32)