

Estonia vs. Russia

The DDOS War

Birmingham InfraGard
June 2007 Meeting

InfraGard Sharing

- This presentation may be shared freely.
- Please leave this slide in place to acknowledge that the research of Gary Warner, who wrote this presentation for the Birmingham InfraGard June 2007 meeting.
- <http://www.birmingham-infragard.org/>
- (First of three DDOS presentations)

Nashi Hackers

Konstantin Goloskov, a Nashi activist, told the Rosbalt news agency on May 2 that he personally took part in cyber-attacks on Estonian websites. But he denied that Moscow state offices were used. The hacking, he said, was done from the breakaway Moldovan region of Transdniester.

A Bit of History

- Estonia was occupied by the Soviets in June of 1940 and officially annexed as the Estonian SSR in August of 1940.
- Nazi Germany occupied Estonia from 1941 to 1944.
- The Red Army reconquered Estonia in the autumn of 1944.
- In 1949, 20,000 families were deported to labor camps in Siberia. Afterwards the remainder quickly converted to Collective Farming.

A Bit of History

- The “Forest Brothers” led an ongoing guerilla war against the Soviet occupation through the early 1950s.
- Many Estonians remember Russia for:
 - Forced enlistments during WWII (70% died)
 - Forced deportations to Siberia
 - Forced collective farming

In Contrast . . .



- The Bronze Soldier
- AKA “The Monument to the Liberators of Tallinn”
- honors the Red Army soldiers who “freed” Tallinn from Fascism (or Hitler’s Nazis)
- The ashes of many of the fallen Red Army soldiers are buried there.



After years of protests . .

- Each year Estonian nationalists protest the presence of The Bronze Soldier.
- On April 27, 2007, the stone portion of the structure was relocated from the center of the city to an outlying cemetery.
- The unveiling of the relocated soldier was scheduled for May 9, which is celebrated by the Russian's as "Victory Day".



Tallin Riots

- On April 28, the rioting began as ethnic Russians, who saw the statue as a symbol of their right to be in Estonia, gathered to resist the removal of the statue.
- The BBC reports 1 man was killed, 153 injured, and 800 arrested. Police fired tear gas and rubber bullets while protesters trashed shops.
- 25% of Estonia's 1.3 million residents are ethnically Russian or speak Russian.
- <http://news.bbc.co.uk/2/hi/europe/6602171.stm>

Kovalyov to Estonia: RESIGN!

- On April 30, a delegation from Russia's State Duma, the lower house of parliament, visited Tallinn to investigate the events around the removal of the Bronze Soldier memorial. The delegation was headed by Nikolai Kovalyov, the former director of the Federal Security Service (FSB) and currently the head of the Duma Veterans Affairs Committee. While in Tallinn, Kovalyov called for the immediate resignation of the Estonian government.

The DDOS

- With only 1.3 Million citizens, Estonian government websites don't normally see a lot of traffic. Estonian Defense Ministry spokesman, Madis Mikko, says "sites that normally received 1,000 visitors per day were now receiving 2,000 visitors per second?"

Estonia Online?

- 2/3rds of Estonians have broadband Internet service.
- 80% of Estonians filed their taxes online
- The majority of Estonians use online bill payments.
- <http://online.wsj.com/article/SB117944513189906904.html>

How to respond?

- "There is a discussion over how cyber aggression should fit into current law and whether a conventional attack would be suitable retaliation"

(Johannes Ullrich, chief technology officer at the SANS Institute) quoted in the Wall Street Journal

Estonia blames Russia

Estonian Prime Minister Andrus Ansip has directly accused Russia of being responsible, pointing the blame at the Russian government.

The BBC report (May 17) called Estonia “an Internet Pioneer”, and mentioned that the attacks including government computers, banks, and newspapers.

Putin on Estonia

- The May 25th Moscow Times explains Putin's thoughts on Estonia
 - Estonians betrayed his father's NKVD sabotage unit to the Germans. (24 of the 28 were captured, his father escaped, being carried across a frozen river, badly injured, under German fire)
 - The Soviets explained in 1989 to the Estonians that the Molotov-Ribbentrop pact of 1939 did not reflect current Soviet policy. "Do you think we must do this every year?" he asked an Estonian reporter, mocking her Russian accent.
 - The article makes it clear that Putin sees the removal of the statue as an insult to his father and other Russians who fought the Nazis in Estonia.

Youth organizations familiar with CyberWar tactics

- pro-Kremlin groups, such as Nashi, Young Russia, and Mestniye, and ultranationalist youth organizations, like The Other Russia and Movement Against Illegal Immigration have all had their websites attacked in the past few months.
- Alexander Kalugin, a spokesman for Young Russia, said his group was DDOSed for six hours in March, saying the attack was by Estonians angered at their protests.
- His group burned Estonian banners and trampled an effigy of the Estonian president, which led to the cyber retaliation.

High Ranking Russian IPs

- A NATO computer expert was sent to Estonia to assist with the DDOS response.
- A list of attacking IP addresses was provided by the Estonian Foreign Ministry to the Moscow Times.
- One attacking netblock had been registered by Mikhail Polyakov, who identified himself as an adviser to the president, and who used the presidential administration address (4 Staraya Ploschchad) in the WHOIS information.

High Ranking Russian IPs

- Yury Mashevsky (with Moscow based Kaspersky Lab) and Paul Sop (with London based Prolexic Technologies) both were quoted as saying how rare it is to actually identify the criminals behind a DDOS.
- Political analyst Stanislav Belkovsky suggested the attacks were being run from a secret department in Putin's administration by **Vladislav Surkov**, Putin's deputy administrator.

Nashi in Newsweek

“Putin’s Powerful Youth Guard”

- Some 15,000 volunteers donned red jackets, with Putin's communicators emblazoned on the back, and spread out across Moscow distributing brochures and 10,000 specially made SIM cards for mobile phones. The cards allowed users to send text messages to the Kremlin—to be answered promptly by Nashi volunteers. Recipients were also instructed to use the cards to report any signs of an incipient Orange revolution. In that event, the cards would instantly relay text-message instructions on what to do and where to rally. **"We explained to Muscovites that we should all be prepared for the pro-Western revolution, funded by America,"** says Nashi activist Tatyana Matiash, 22. "People must know what to do to save their motherland in case their radio and TV stop working."
- Lesson: NASHI admits to being involved in the DDOS Against Estonia, and their leadership anticipates an Orange Revolution, funded by America . . . Hmmm....

<http://www.msnbc.msn.com/id/18753946/site/newsweek/page/0/>

Interesting notes from Estonia

- “BCP38” is considered a “Best Practice” by many Estonian ISPs – this helped mitigate the attack.

Best Current Practice May 2000

Network Ingress Filtering:

Defeating Denial of Service Attacks which employ IP Source Address Spoofing

<http://www.faqs.org/rfcs/bcp/bcp38.html>

From Interview with Gadi Evron*

- *The botnet traffic was distributed globally, with some of the botnets being bought. However, many of the attacks were not by a botnet, but rather by a mass of home users using commands such as ping to manually attack Estonian sites. As they coined in Estonia, this was a riot, and not just in the streets. Many different Russian-speaking forums and blogs (the Russian blogosphere?) encouraged people to attack Estonia using crude commands or simple tools. Others used more advanced techniques.*

* <http://fistfulofeuros.net/afoe/the-european-union/russian-hide-and-see-with-routers>

DDOS Facts

- April 27th - 1st hit: Foreign Minister Urmas Paet's Free Market Liberal Reform Party homepage
- June 6th – Biggest Economic impact – SEB Eesti Uhispank (Bank) in Estonia under heavy DDOS

DDOS Facts (from Arbor)

- 128 unique DDOS Attacks:
- May 3 – 21 attacks
- May 4 – 17 attacks
- May 8 – 31 attacks
- May 9 – 58 attacks

DDOS Facts (from Arbor)

- Attack durations:
- 17 less than 1 minute
- 78 1 minute to 1 hour
- 16 1 hour to 5 hours
- 8 5 hours to 9 hours
- 7 10 hours or more

DDOS Facts

- Bandwidth
- 42 – less than 10 Mbps
- 52 – 10Mbps to 30 Mbps
- 22 – 30 Mbps to 70 Mbps
- 12 – 70 Mbps to 95 Mbps

DDOS Facts

- Destination blocks

- 35 195.80.105.107 pol.ee
- 7 195.80.106.72 riigikogu.ee
- 36 195.80.109.158 riik.ee, peaminister.ee,
valitsus.ee
- 2 196.80.124.53 m53.envir.ee
- 2 213.184.49.171 sm.ee
- 6 213.184.49.194 agri.ee
- 4 213.184.50.6
- 35 213.184.50.69 fin.ee
- 1 62.65.192.24

How did they recover?

OS, Web Server and Hosting History for www.valitsus.ee

<http://www.valitsus.ee> was running Apache on Linux when last queried at 5-Jun-2007 05:30:55 GMT - [refresh now](#) [Site Report](#)
Try out the [Netcraft Toolbar](#)

[FAQ](#)

OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache	23-May-2007	195.80.102.44	Department of Data Communications
unknown	Apache	16-May-2007	195.80.109.158	Department of Data Communications
Linux	Apache	11-May-2007	195.80.109.158	Department of Data Communications
Linux	Apache	9-May-2007	84.53.139.18	Akamai Technologies
Linux	AkamaiGHost	8-May-2007	84.53.139.18	Akamai Technologies
unknown	Apache/2.0.58 (Unix) DAV/2	2-May-2007	195.80.102.43	Department of Data Communications
unknown	Apache/2.0.58 (Unix) DAV/2	1-May-2007	195.80.102.43	Department of Data Communications
Linux	Apache/1.3.33 (Debian GNU/Linux) PHP/4.3.10-20 mod_ssl/2.8.22 OpenSSL/0.9.7e	29-Apr-2007	195.80.102.46	Department of Data Communications
Linux	Apache/1.3.33 (Debian GNU/Linux) PHP/4.3.10-16 mod_ssl/2.8.22 OpenSSL/0.9.7e	27-Aug-2006	213.184.51.43	Department of Data Communications, Estonian Informatics Center
Linux	Apache	7-Apr-2003	195.80.107.77	Department of Data Communications

9-May-2007	84.53.139.18	Akamai Technologies
8-May-2007	84.53.139.18	Akamai Technologies
2-May-2007	195.80.102.43	Department of Data Communications
1-May-2007	195.80.102.43	Department of Data Communications

First arrest

- An unnamed 19-year-old university student, an Estonian citizen, was arrested for arranging and realizing virtual attacks against the government, after being found posting advice on how to carry out DDOS attacks.

Lesson One: Digital Warfare is here

- Lesson 1: Large scale digital warfare is being researched and practiced. The Netherlands attacks had several thousand victim companies who shared only one thing – a common nation of origin

Lesson Two:

The Causes can be Trivial

- A government (this time Estonia, who is next) was shut down for more than two weeks because one war memorial was relocated.
- What grievance will bring the wrath of hackers against your company or your nation?

Lesson Three: The Enemy of my Enemy is my friend

- The Prophet cartoons united hackers in the entire Arab speaking world.
- The Bronze Soldier has united hackers in the entire Russian speaking world.
- How many people in the world hate America?

Lesson Four: Nothing can withstand 2 Gbps

- There are 13 year old hackers who command 1Gbps worth of DDOS.
- What sort of DDOS bandwidth do you think a foreign state could put together?
- Recommended Reading:
- “Beyond Estonia-Russia: The Rise of China’s 5th Dimension Cyber Army”
- http://www.intentblog.com/archives/2007/05/cyber_warfare_b.html