Russian Invasion of Georgia

Russian Cyberwar on Georgia

10 November, 2008

Regular updates can be found on the Georgia Update website:

www.georgiaupdate.gov.ge

1. INTRODUCTION

The Russian invasion of Georgia was preceded by an intensive build up of cyberattacks attempting to disrupt, deface and bring down critical Georgian governmental and civilian online infrastructure. These attacks became a massive assault on the eve of the invasion which resulted in the blocking, re-routing of traffic and control being seized of various sections of Georgian cyberspace. The attack marks a new phase in the history of warfare, being the first case in which a land invasion was co-ordinated with an orchestrated online cyber-offensive. This offers crucial lessons for strategists and planners whilst providing vital information about how the Russian Federation is developing its offensive capacities on the internet.

The campaign has been reported in the media, with wide coverage suggesting the campaign was a spontaneous outburst of popular feeling in Russia lead by independent hackers. However, as this report suggests, the offensive was too large, coordinated, and sophisticated to be the work of independent hackers; the evidence leads by-and-large to the Russian Business Network (RBN) in St. Petersburg, Russia. Whilst only a criminal investigation can directly prove the involvement of the Kremlin, both experts and commentators have accused Moscow of sponsoring the attacks as their magnitude requires the involvement of the kind of resources only a state-sponsor can provide.

2. BACKGROUND ON CYBERWARFARE

Cyberattacks are becoming an increasingly established and virulent form of warfare in the early Twenty-First Century. High technology and online skills are now available for rent to a variety of customers, including private individuals and terrorist organizations, and can potentially destabilize a country's whole economy and crucial security infrastructure. Cyberwarfare has found its primary state-sponsor in the Russian Federation, which is widely suspected of having played a leading role in the first large scale cyberattack on a NATO member state last year.

In the spring of 2007 government computers in Estonia came under sustained attack from cyberterrorists following the decision taken by Estonian officials to move a statue placed commemorating a Red Army soldier that died fighting the Nazis, to the military cemetery in the capital Tallinn. The event roused emotions and led to large scale protests by the Russian minority. It was then that the Estonian Government's online networks came under massive assault using

Distributed Denial-Of-Service (DDoS) assaults on its infrastructure. The attacks, which flooded computers and servers, blocking legitimate users were described as `crippling' by experts, owing to Estonia's high dependence on information technology. Commentators have pointed out that the assault had very serious consequences for Estonia`s banks and airports. Consequences similar in effect to a full scale missile strike. This provided vital lessons for Estonia and NATO and has led to the development of a cutting edge cyberwarfare institute in Tallinn.

3. RUSSIA'S ONLINE WAR ON GEORGIA: FIRST STRIKE

In August 2008, cyberwar associated with the Russian Federation struck once more, this time against Georgia. The DDoS attacks began in the weeks running up to the outbreak of the Russian invasion and continued after the Kremlin announced that it had ceased hostilities on 12 August. Georgian claims have been confirmed by Tom Burling, an executive of Tulip Systems, a U.S. Internet firm, which took over hosting of the web sites for Georgia's government agencies during the conflict. In a recent interview Burling said its experts had worked frantically to curtail the damage from the hackers, remarking that "They have been attacking Georgia from a cyber standpoint since July." Some of the Western sources confirm this claim.

On 20 July the Shadowserver Foundation published news about the serious attack against the website of the President of Georgia: "For over 24 hours the website of President Mikhail Saakashvili of Georgia (**www.president.gov.ge**) has been rendered unavailable due to a multi-pronged distributed denial of service (DDoS) attack."

Computerworld, 21 July: "The Web site for the president of Georgia was knocked offline by a distributed denial-of-service (DDOS) attack over the weekend, yet another in a series of cyberattacks against countries experiencing political friction with Russia."

New York Times, 12 August: "Weeks before bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace."

The Russian invasion of Georgia was preceded by a cyber attack on Georgia's Internet facilities. A large number of Georgia's Internet servers were seized and placed under external control from late Thursday, 7 August, whereas Russia's invasion of Georgia officially commenced on Friday, 8 August. Also, much of Georgia's traffic and access was taken under unauthorized external control at the same time that this first large scale attack occurred.

The defacement of President Mikheil Saakashvili web site **president.gov.ge** with the screen-shot provided below which operated as a moving slideshow was part of the initial phase of the attack. What

followed were large numbers of DDoS against the site designed to prevent the Georgian government from getting its message across to the general population and international media during this critical time.

Dancho Danchev is an independent security consultant and cyber threats analyst, with extensive experience in open source intelligence gathering, malware and E-crime incident response. As an expert in the field, he views the defacement attacks as clearly being Kremlin linked and not undertaken by independent or un-coordinated attackers.

- "What am I trying to imply? It smells like a three letter intelligence agency's propaganda arm has managed to somehow supply the creative for the defacement of Georgia President's official web site, thereby forgetting a simple rule of engagement in such a conflict - risk forwarding the responsibility of the attack to each and every Russian or Russian supporter that ever attacked Georgian sites using publicly obtainable DDoS attack tools in a coordinated fashion."

An example of Russian efforts to shut the mouse of Georgian media is the story of the Georgian news agency GHN. The first attack against the agency's website occurred in August 2008. Another wave of cyber attacks started on 8 September. As a result, the GHN news agency website had been paralyzed for 2 weeks. Another Georgian media website that came under consistent cyber attacks after the end of the armed conflict is www.apsny.ge – website of the Georgia-Online news agency. It is interesting to note that Russian efforts to prevent Georgian

Internet media resources from disseminating information continued even after the war.

4. CYBER BLOCKADE

The Russian assault on Georgian cyberspace was intensely co-ordinated and directed out of St. Petersburg, inside the territory of the Russian Federation. The primary orchestrator was the Russian Business Network (RBN) which conducted the cyber-blockade so that all Georgian Internet traffic was going through Russia, denying Georgia its internet independence. Computers in Georgia showed that an assault was clearly taking place, which is presented here as evidence of Russian sponsored cyber-terrorism:

- Two trace routes for the web site **mfa.gov.ge**, that of the Georgian Ministry of Foreign Affairs, were showing:

  (a) From US - Ge = Blocked via TTnet Turkey

  (b) From Ukraine - Ge = available & slow; not accessible, cached (forged page) now only via redirect through **Bryansk.ru**

- Other Georgia government websites such as **mod.gov.ge**, the website of the Georgian Ministry of Defense and the web site **president.gov.ge**, the web site of the Georgian Presidency showed

  (c) From US - Ge = **Blocked** via TTnet Turkey

  (d) From Ukraine - Ge = **Blocked** via TTnet Turkey

By examining Internet routes before and after the beginning of the war, it is clear that they were altered either legally or illegally, blocking traffic in and out of Georgia. Some of those routers are known to be under control of the Russian Business Network (RBN). This can be demonstrated via a comparison of route configuration before and after the war.

5. SITES PROVIDING DDOS ATTACK TOOLS

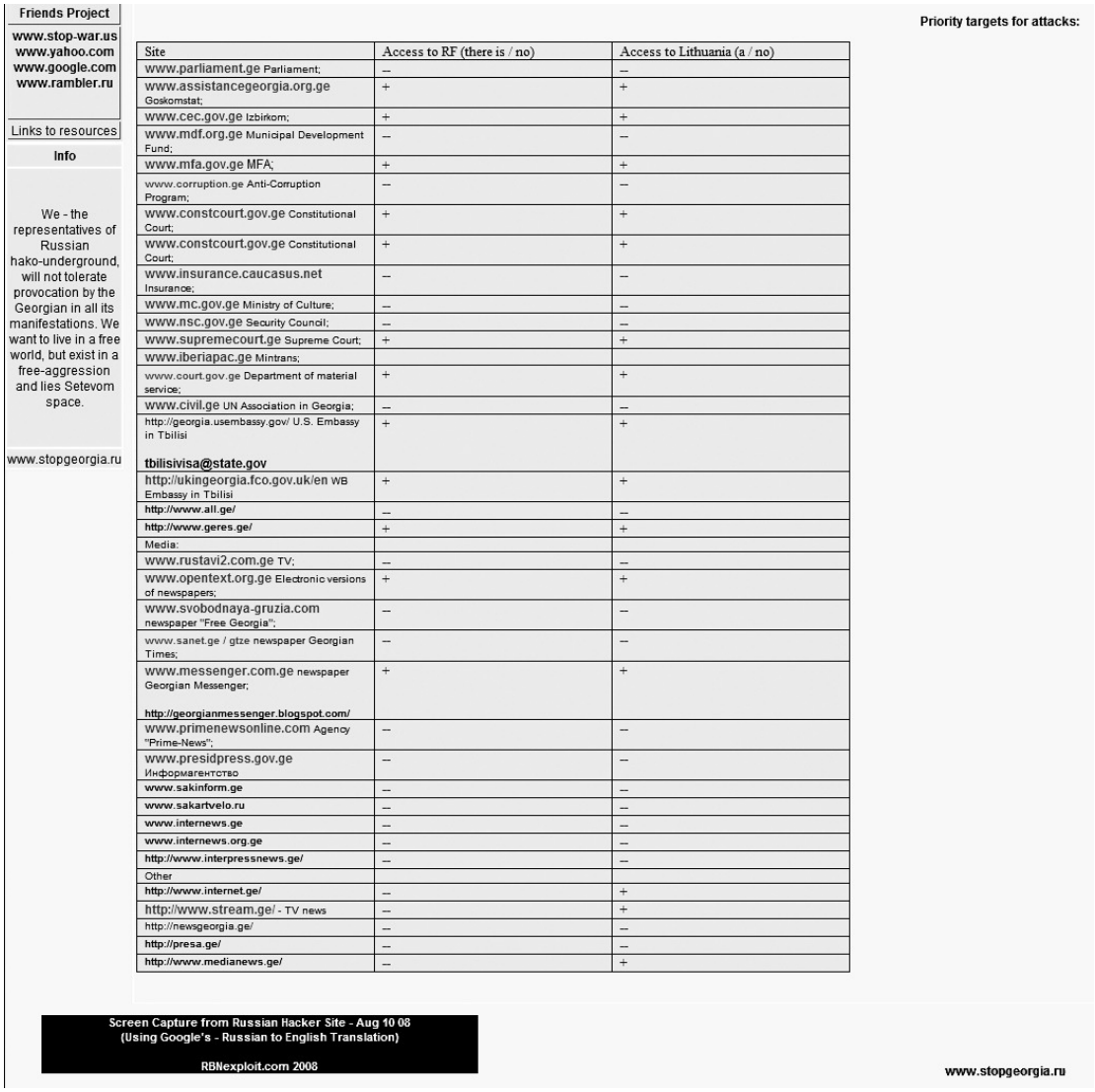
Here we can provide clear evidence of co-ordination and a full list of targets the cyber-terrorists had selected taken from the Russian hosted web site **stopgeorgia.ru** (which also appears as **stopgeorgia.info** a redirected page). This site provided the necessary attack tools for the cyber assault against Georgia for hackers. As we can see the screen-shot shows that mostly **.ge** web sites are listed for priority attacks. However - also targeted for assault is the US embassy in Tbilisi. This web site, as seen before, is an open site to attract future FSB cyber warriors. The following evidence below shows how these sites can be traced back to the Russian Business Network (RBN) in ST. Petersburg and other cybercriminal locations.

- The information site **Stopgeorgia.ru** which provided information and tools for independent hackers to attack Georgian sites was hosted by AS36351 Softlayer of Plano Texas. This is a well known location that is associated with Atrivo and Intercage malware hosting connectivity, which is highly disruptive to online service.
- The information site **Stopgeorgia.info** was hosted by AS28753 NETDIRECT in Frankfurt, Germany as well as in AS12578 APOLLO LATTELEKOM APOLLO in Latvia.

The link back to the Russian Business Network (RBN) was provided by the clues left in the registration, which reads as:

- Sponsoring Registrar: EstDomains, Inc. Registrant: Domain Manager, Protect Details, Inc, Street1: 29 Kompozitorov St., Saint Petersburg, RU, Phone:+7.8129342271

In summary, 36 important web sites were identified as targets for hackers, including the US and UK Embassies in Tbilisi, Georgian Parliament, Georgian Supreme Court, Ministry of Foreign Affairs, various news agencies and other media resources, the Central Election Commission, and many others.



Friends Project

www.stop-war.us
www.yahoo.com
www.google.com
www.rambler.ru

Links to resources

Info

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, but exist in a free-aggression and lies Setevom space.

www.stopgeorgia.ru

Priority targets for attacks:

Site	Access to RF (there is / no)	Access to Lithuania (a / no)
www.parliament.ge Parliament;	–	–
www.assistancegeorgia.org.ge Goskomstat;	+	+
www.cec.gov.ge Izbirkom;	+	+
www.mdf.org.ge Municipal Development Fund;	–	–
www.mfa.gov.ge MFA;	+	+
www.corruption.ge Anti-Corruption Program;	–	–
www.constcourt.gov.ge Constitutional Court;	+	+
www.constcourt.gov.ge Constitutional Court;	+	+
www.insurance.caucasus.net Insurance;	–	–
www.mc.gov.ge Ministry of Culture;	–	–
www.nsc.gov.ge Security Council;	–	–
www.supremecourt.ge Supreme Court;	+	+
www.iberiapac.ge Mintrans;		
www.court.gov.ge Department of material service;	+	+
www.civil.ge UN Association in Georgia;	–	–
http://georgia.usembassy.gov/ U.S. Embassy in Tbilisi tbilisivisa@state.gov	+	+
http://ukingeorgia.fco.gov.uk/en WB Embassy in Tbilisi	+	+
http://www.all.ge/	–	–
http://www.geres.ge/	+	+
Media:		
www.rustavi2.com.ge TV;	–	–
www.opentext.org.ge Electronic versions of newspapers;	+	+
www.svobodnaya-gruzia.com newspaper "Free Georgia";	–	–
www.sanet.ge / gtze newspaper Georgian Times;	–	–
www.messenger.com.ge newspaper Georgian Messenger; http://georgianmessenger.blogspot.com/	+	+
www.primenewsonline.com Agency "Prime-News";	–	–
www.presidpress.gov.ge Информагентство	–	–
www.sakinform.ge	–	–
www.sakartvelo.ru	–	–
www.internews.ge	–	–
www.internews.org.ge	–	–
http://www.interpressnews.ge/	–	–
Other		
http://www.internet.ge/	–	+
http://www.stream.ge/ - TV news	–	+
http://newsgeorgia.ge/	–	–
http://presa.ge/	–	–
http://www.medianews.ge/	–	+

Screen Capture from Russian Hacker Site - Aug 10 08
(Using Google's - Russian to English Translation)

RBNexploit.com 2008

www.stopgeorgia.ru

Due to efforts of many IT specialists in Internet hosting routing companies, normal traffic was mostly resumed after the initial strikes. Most critical websites were hosted outside of Georgia.

6. PART OF THE INFORMATION WAR

To help to make a final judgment regarding the cyberwar against Georgia these two declarations from Russian officials can help us to evaluate how Moscow thinks in regard to online warfare. The Russian State Duma deputy and member of the Security Committee Deputy Nikolai Kuryanovich stated in 2006 within a formal Russian parliamentary letter of appreciation to hackers who had taken down several Israeli web sites:

- "In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a

small force of hackers is stronger than the multi-thousand force of the current armed forces."

Should we interpret this declaration as a statement of intent, or merely a prediction? A few days ago, the Editor of the Russian Online journal **cybersecurity.ru**, made a similar statement that provides insight into the Russian war aims:

- "Cyber-attacks are part of the information war, making your enemy shut up is a potent weapon of modern warfare."

Clear examples that such thinking is being applied as guiding principles of Russian strategy as part of the intense information-war taking place can be drawn from the second wave of attacks that showed up from Russian Business Network (RBN) server range. This time the weapon was a new campaign purporting to come from the BBC that mocked Georgia's President and spread as a new virus.

The malware from various locations caused the virus to be delivered from a single site, (IP address: 79.135.167.49).
The name of the malware is "name.avi.exe", and as of September 2008, only FOUR out of 36 anti-virus products could detect it. The Russian Business Network (RBN) had created a highly virulent strain designed to act as a propaganda weapon against Georgia.

7. RUSSIAN BUSINESS NETWORK

The individual, with direct responsibility for carrying out the cyber "first strike" on Georgia, is a RBN operative named Alexandr A. Boykov of Saint Petersburg, Russia. Also involved in the attack was a programmer and spammer from Saint Petersburg named Andrey Smirnov. These men are leaders of RBN sections and are not "script-kiddies" or "hacktivists," as some have maintained of the cyber attacks on Georgia – but senior operatives in positions of responsibility with vast background knowledge.

Intelligence can suggest further information about these individual cyber-terrorists. According to Spamhaus SBL64881, Mr. Boykov operates a hosting service in Class C Network 79.135.167.0/24. It should be noted that the pre-invasion attacks emanated from 79.135.167.22, clearly showing professional planning and not merely `hacktivism.' Due to the degree of professionalism and the required massive costs to run such operations, a state-sponsor is suspected. Further information gathered also links the RBN to known disruptive websites.

- The IP addresses of the range**, 79.135.160.0/19** are assigned to Sistemnet Telecom to provide services to companies who are classified as engaging in illicit activities such as credit card fraud, malware and so on.

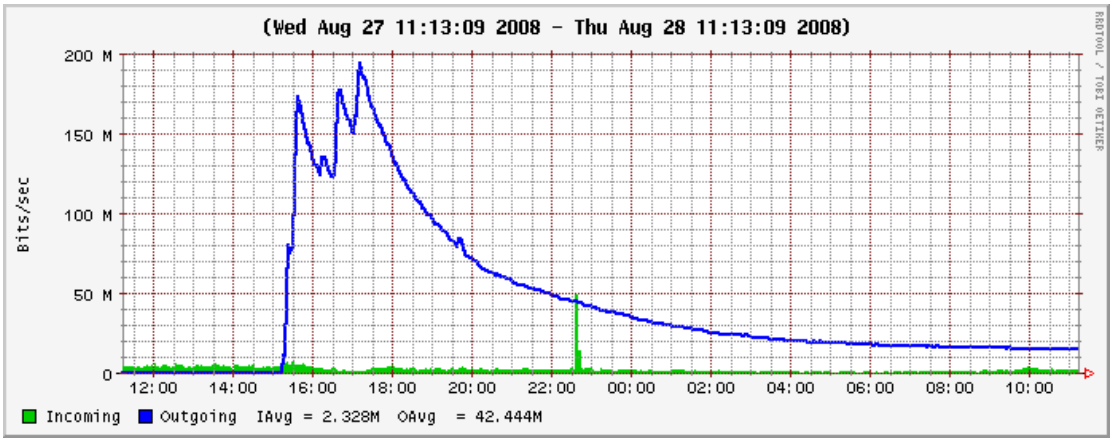
- **79.135.160.0/19** Sistemnet Telecom and **AS9121** TTNet (Turkey) are associated with AbdAllah_Internet which is linked with cybercrime hosting such as **thecanadianmeds.com.** These are known Russian Business Network routes.

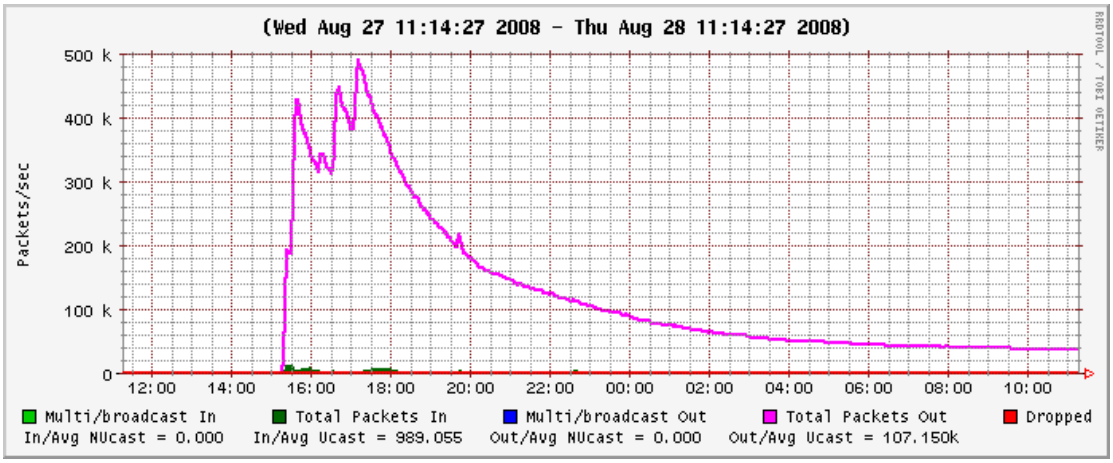
8. THE 27 AUGUST ATTACK

The last large cyberattack took place on 27 August. After that, there have been no serious attacks on Georgian cyberspace. By that is meant that minor attacks are still continuing but these are indistinguishable from regular traffic and can certainly be attributed to regular civilians.

On 27 August, at approximately 16:18 (GMT +3) a DDoS attack against the Georgian websites was launched. The main target was the Georgian Ministry of Foreign Affairs.

The attacks peaked at approx 0,5 million network packets per second, and up to 200–250 Mbits per second in bandwidth (see attached graphs). The graphs represent a 5-minute average: actual peaks were higher.





The attacks mainly consisted of HTTP queries to the **http://mfa.gov.ge** website. These were requests for the main page script with randomly generated parameters. These requests were generated to overload the web server in a way where every single request would need significant CPU time.

The initial wave of the attack disrupted services for some Georgian websites. The services became slow and unresponsive. This was due to the load on the servers by these requests.

As you see from the graphs above the attacks started to wind down after most of the attackers were successfully blocked. The latest attack may have been initiated as a response to the media coverage on the Russian cyber attacks.

CONCLUSION

The information presented in here catalogues and explains the historic first major use of cyberattacks as a weapon of war during the Russian aggression against Georgia. Considering that this is the second Russian-sponsored cyber-attack in just over a year, as well as the alarming fact that the US Embassy in Tbilisi was listed for assault by cyberterrorists, NATO member states as well as NATO aspirant countries need to be on full alert for future Russian aggression against critical online infrastructure.

APPENDIX: Articles About Cyberwar on Georgia

Contents

SHADOWSERVER

20 July 2008; Updated on 10 August 2008

The Website for the President of Georgia Under Attack - Politically Motivated?

For over 24 hours the website of President Mikhail Saakashvili of Georgia (**www.president.gov.ge**) has been rendered unavailable due to a multi-

pronged distributed denial of service (DDoS) attack. The site began coming under attack very early Saturday morning (Georgian time). Shadowserver has observed at least one web-based command and control (C&C) server taking aim at the website hitting it with a variety of simultaneous attacks. The C&C server has instructed its bots to attack the website with TCP, ICMP, and HTTP floods.

Commands seen so far are:

flood http www.president.gov.ge/
flood tcp www.president.gov.ge
flood icmp www.president.gov.ge

The server (62.168.168.9) which houses the website has been largely offline since the attack started. Passive DNS records show the system houses several other websites which are mostly unrelated to the Georgian government. However, the server does also host the Social Assistance and Employment State Agency website (www.saesa.gov.ge). This website along with the others on the host have been rendered inaccessible.

Is the attack political or perhaps nationalistic in nature? Your guess is as good as ours but it doesn't take much to come to this possible conclusion. Recent DDoS attacks against various other neighbors of Russia to include Estonia have been quite popular in the last few years. We do not have any solid proof that the people behind this C&C server are Russian. However, the HTTP-based botnet C&C server is a MachBot controller, which is a tool that is frequently used by Russian bot herders. On top of that the domain involved with this C&C server has seemingly bogus registration information but does tie back to Russia.

Who else have these guys been attacking with this MachBot C&C server? The answer is no one. This server recently came online in the past few weeks and has not issued any other attacks that we have observed until recently. All attacks we have observed have been directed right at www.president.gov.ge.

The C&C server involved in these attacks is on the IP address **207.10.234.244**, which is subsequently located in the United States. Beaconing traffic from your network to this host may indicate that you have infected machines on your network and are most likely participating in this DDoS attack. We would recommend blocking and/or monitoring for traffic to this address.

Update (7/20/2008: 1:36 PM EST): It appears the host site for 207.10.234.244 has taken action against this system and appears to now be blocking access to it. However, the server being targeted by the C&C is still unreachable.

Update (8/10/2008: 10:34 AM EDT): With the recent events in Georgia, we are now seeing new attacks against .ge sites. www.parliament.ge & president.gov.ge are currently being hit with http floods. In this case, the C&C server involved is at IP address 79.135.167.22 which is located in Turkey. We are also observing this C&C as directing attacks against www.skandaly.ru.

Traffic from your network to this IP or domain name of googlecomaolcomyahoocomaboutcom.net may indicate compromise and participation in these attacks.

COMPUTERWORLD

21 July 2008

By Jeremy Kirk

Georgia president's Web site falls under DDOS attack

Botnet took down site for one day

The Web site for the president of Georgia was knocked offline by a distributed denial-of-service (DDOS) attack over the weekend, yet another in a series of cyberattacks against countries experiencing political friction with Russia.

Georgia's presidential Web site was down for about a day, starting early Saturday until Sunday, according to the Shadowserver Foundation, which tracks malicious Internet activity.

Network experts said the attack was executed by a botnet, or a network of computers that can be commanded to overwhelm a Web site with too much traffic.

The command-and-control server for the attack is based in the U.S., Shadowserver said. The botnet appears to be based on the "MachBot" code, which communicates to other compromised PCs over HTTP, the same protocol used for transmitting Web pages.

The tool used to control this kind of botnet "is frequently used by Russian bot herders," according to Shadowserver. "On top of that, the domain involved with this (command-and-control) server has seemingly bogus registration information but does tie back to Russia."

One of the commands contained in the traffic directed at the Web site contained the phrase "win+love+in+Rusia," wrote Jose Nazario, a senior security engineer at Arbor Networks, on a company blog.

On Sunday, it appeared that the host for the command-and-control server had been taken offline, Shadowserver said.

The motivation for the attacks is not entirely clear. But Georgia is just one of several former Soviet satellites, including Estonia and Lithuania, that are seeking to downplay their historical legacy with Russia.

Georgia has angered Russia by pushing for entry to NATO, a pro-Western security alliance. It has also tangled with Russia over the handling of South Ossetia and Abkhazia, two rebellious regions pushing for independence.

In Lithuania, 300 Web sites were defaced around July 1 following a new law prohibiting the public display of symbols dating from the Soviet era and the playing of the Soviet national anthem. The hacking was blamed on an unpatched vulnerability in a Web server at a hosting company.

Estonian Web sites were pounded by a massive DDOS attack in April and May 2007. The attacks are believed to have been connected to a decision to move a monument honoring Soviet World War II soldiers to a less prominent place, which ignited protests from ethnic Russians.

COMPUTERWORLD

11 August 2008

By Gregg Keizer

Cyberattacks knock out Georgia's Internet presence

Large-scale attacks, traffic rerouting traced to Russian hacker hosting network

August 11, 2008 (Computerworld) Hackers, perhaps affiliated with a well-known Russian criminal network, have attacked and hijacked Web sites belonging to Georgia, the former Soviet republic now in the fourth day of war with Russia, a security researcher claimed on Sunday.

Some Georgian government and commercial sites are unavailable, while others may have been hijacked, said Jart Armin, a researcher who tracks the notorious Russian Business Network (RBN), a malware and criminal hosting network.

"Many of Georgia's Internet servers were under external control from late Thursday," Armin said early Saturday in an entry on his Web site. According to his research, the government's sites dedicated to the Ministry of Foreign Affairs, the Ministry of Defense, and the country's president, Mikhail Saakashvili, have been blocked completely, or traffic to and from those sites' servers have been redirected to servers actually located in Russia and Turkey.

As of midnight Eastern time on Sunday, Georgia's presidential and defense ministry sites were unavailable from the U.S. Although the foreign ministry's site remained online, the most recent news item was dated Aug. 8, the day Georgian and Russian forces first clashed.

Armin warned that Georgian sites that appeared online may actually be bogus. "Use caution with any Web sites that appear of a Georgia official source but are without any recent news (such as those dated Saturday, Aug. 9, or Sunday, Aug. 10), as these may be fraudulent," he said in another entry posted midafternoon on Sunday.

Statements from Georgia's foreign ministry have appeared in a blog hosted on Google, perhaps in an attempt to circumvent attacks.

Researchers at the Shadowserver Foundation, which tracks malicious Internet activity, confirmed some of Armin's claims. "We are now seeing new attacks against .ge sites (*Editor's note: .ge is the top-level domain for Georgia.*) ... *www.parliament.ge* and *president.gov.ge* are currently being hit with HTTP floods," the researchers said in a Sunday update to a July post.

On Saturday, Armin reported that key sections of Georgia's Internet traffic had been rerouted through servers based in Russia and Turkey, where the traffic was either blocked or diverted. The Russian and Turkish servers Armin identified, he said, "are well known to be under the control of RBN and influenced by the Russian government."

RBN, which pulled up stakes last year and shifted network operations to China in an attempt to avoid scrutiny, has been fingered for a wide range of criminal activities, including a massive subversion of Web sites last March.

Later on Saturday, Armin added that network administrators in Germany had been able to temporarily reroute some Georgian Internet traffic directly to servers run by Deutsche Telekom AG. Within hours, however, the traffic had been again diverted to Russian servers, this time to ones based in Moscow.

The attacks are reminiscent of other coordinated campaigns against Estonian government Web sites in April and May 2007 and against about 300 Lithuanian sites on July 1. Like Georgia, both countries are former republics in the Soviet Union.

Three weeks ago, a distributed denial-of-service attack knocked Georgia's presidential site offline for about a day.

Late Sunday, Russian ground forces were reported advancing toward Gori, an important transportation hub in central Georgia.

SOFT SECURITY

11 August 2008

This day highlights

Coordinated Russia vs Georgia cyber attack in progress (extract)

In the wake of Russian-Georgian conflict, a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia's Internet infrastructure, whose tactics have already managed to compromise several government web sites and is continuing to launch DDoS attacks against numerous other Georgian government sites…

THE TELEGRAPH

August 11 2008

By Jon Swaine

Georgia: Russia 'conducting cyber war'

Several Georgian state computer servers have been under external control since shortly before Russia's armed intervention into the state commenced on Friday, leaving its online presence in disarray.

While the official website of Mikheil Saakashvili, the Georgian President, has become available again, the central government site, as well as the homepages for the Ministry of Foreign Affairs and Ministry of Defence, remained down. Some commercial websites have also been hijacked.

The Georgian Government said that the disruption was caused by attacks carried out by Russia as part of the ongoing conflict between the two states over the Georgian province of South Ossetia.

In a statement released via a replacement website built on Google's blog-hosting service, the Georgian Ministry of Foreign Affairs said: "A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Ministry of Foreign Affairs."

Barack Obama, the Democratic US Presidential candidate, has demanded Moscow halt the internet attacks as well as observing a ceasefire on the ground.

Last April the computer systems of the Estonian Government came under attack in a coordinated three-week assault widely credited to state-sponsored Russian hackers. The wave of attacks came after a row erupted over the removal of the Bronze Soldier Soviet war memorial in Tallinn, the Estonian capital. The websites of government departments, political parties, banks and newspapers were all targeted.

Analysts have immediately accused the Russian Business Network (RBN), a network of criminal hackers with close links to the Russian mafia and government, of the Georgian attacks.

Jart Armin, a researcher who runs a website tracking the activity of the RBN, has released data claiming to show that visits to Georgian sites had been re-routed through servers in Russia and Turkey, where the traffic was blocked. Armin said the servers "are well known to be under the control of RBN and influenced by the Russian Government."

Mr Armin said that administrators in Germany had intervened at the weekend, temporarily making the Georgian sites available by re-routing their traffic through German servers run by Deutsche Telekom. Within hours, however, control over the traffic had been wrested back, this time to servers based in Moscow.

As in the barrage against Estonian websites last year, the Georgian sites are being bombarded by a distributed denial-of-service (DDoS) attack, in which

hackers direct their computers to simultaneously flood a site with thousands of visits in order to overload it and bring it offline.

The Shadowserver Foundation, which tracks serious hacking, confirmed: "We are now seeing new attacks against .ge sites - www.parliament.ge and president.gov.ge are currently being hit with http floods."

Mr Armin warned that official Georgian sites that did appear online may have been hijacked and be displaying bogus content. He said in a post on his site: "Use caution with any web sites that appear of a Georgia official source but are without any recent news ... as these may be fraudulent."

The Baltic Business News website reported that Estonia has offered to send a specialist online security team to Georgia

However a spokesman from Estonia's Development Centre of State Information Systems said Georgia had not made a formal request. "This will be decided by the government," he said

NEW YORK TIMES

12 August 2008

By John Markoff

Before the Gunfire, Cyberattacks

Weeks before bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace.

Jose Nazario of Arbor Networks in Lexington noticed a stream of data directed at Georgian government sites containing the message: "win+love+in+Rusia."

Other Internet experts in the United States said the attacks against Georgia's Internet infrastructure began as early as July 20, with coordinated barrages of millions of requests — known as distributed denial of service, or D.D.O.S., attacks — that overloaded and effectively shut down Georgian servers.

Researchers at Shadowserver, a volunteer group that tracks malicious network activity, reported that the Web site of the Georgian president, Mikheil Saakashvili, had been rendered inoperable for 24 hours by multiple D.D.O.S. attacks. They said the command and control server that directed the attack was based in the United States and had come online several weeks before it began the assault.

As it turns out, the July attack may have been a dress rehearsal for an all-out cyberwar once the shooting started between Georgia and Russia. According to Internet technical experts, it was the first time a known cyberattack had coincided with a shooting war.

But it will likely not be the last, said Bill Woodcock, the research director of the Packet Clearing House, a nonprofit organization that tracks Internet traffic. He said cyberattacks are so inexpensive and easy to mount, with few fingerprints, they will almost certainly remain a feature of modern warfare.

"It costs about 4 cents per machine," Mr. Woodcock said. "You could fund an entire cyberwarfare campaign for the cost of replacing a tank tread, so you would be foolish not to."

Exactly who was behind the cyberattack is not known. The Georgian government blamed Russia for the attacks, but the Russian government said it was not involved. In the end, Georgia, with a population of just 4.6 million and a relative latecomer to the Internet, saw little effect beyond inaccessibility to many of its government Web sites, which limited the government's ability to spread its message online and to connect with sympathizers around the world during the fighting with Russia.

It ranks 74th out of 234 nations in terms of Internet addresses, behind Nigeria, Bangladesh, Bolivia and El Salvador, according to Renesys, a Manchester, N.H., firm that provides performance data on the state of Internet. Cyberattacks have far less impact on such a country than they might on a more Internet-dependent nation, like Israel, Estonia or the United States, where vital services like transportation, power and banking are tied to the Internet.

In Georgia, media, communications and transportation companies were also attacked, according to security researchers. Shadowserver saw the attack against Georgia spread to computers throughout the government after Russian troops entered the Georgian province of South Ossetia. The National Bank of Georgia's Web site was defaced at one point. Images of 20th-century dictators as well as an image of Georgia's president, Mr. Saakashvili, were placed on the site. "Could this somehow be indirect Russian action? Yes, but considering Russia is past playing nice and uses real bombs, they could have attacked more strategic targets or eliminated the infrastructure kinetically," said Gadi Evron, an Israeli network security expert. "The nature of what's going on isn't clear," he said.

The phrase "a wilderness of mirrors" usually describes the murky world surrounding opposing intelligence agencies. It also neatly summarizes the array of conflicting facts and accusations encompassing the cyberwar now taking place in tandem with the Russian fighting in Georgia.

In addition to D.D.O.S. attacks that crippled Georgia's limited Internet infrastructure, researchers said there was evidence of redirection of Internet traffic through Russian telecommunications firms beginning last weekend. The attacks continued on Tuesday, controlled by software programs that were

located in hosting centers controlled by a Russian telecommunications firms. A Russian-language Web site, stopgeorgia.ru, also continued to operate and offer software for download used for D.D.O.S. attacks.

Over the weekend a number of American computer security researchers tracking malicious programs known as botnets, which were blasting streams of useless data at Georgian computers, said they saw clear evidence of a shadowy St. Petersburg-based criminal gang known as the Russian Business Network, or R.B.N.

"The attackers are using the same tools and the same attack commands that have been used by the R.B.N. and in some cases the attacks are being launched from computers they are known to control," said Don Jackson, director of threat intelligence for SecureWorks, a computer security firm based in Atlanta.

He noted that in the run-up to the start of the war over the weekend, computer researchers had watched as botnets were "staged" in preparation for the attack, and then activated shortly before Russian air strikes began on Saturday.

The evidence on R.B.N. and whether it is controlled by, or coordinating with the Russian government remains unclear. The group has been linked to online criminal activities including child pornography, malware, identity theft, phishing and spam. Other computer researchers said that R.B.N.'s role is ambiguous at best. "We are simply seeing the attacks coming from known hosting services," said Paul Ferguson, an advanced threat researcher at Trend Micro, an Internet security company based in Cupertino, Calif. A Russian government spokesman said that it was possible that individuals in Russia or elsewhere had taken it upon themselves to start the attacks.

"I cannot exclude this possibility," Yevgeniy Khorishko, a spokesman for the Russian Embassy in Washington, said. "There are people who don't agree with something and they try to express themselves. You have people like this in your country."

"Jumping to conclusions is premature," said Mr. Evron, who founded the Israeli Computer Emergency Response Team.

AFP

13 August 2008

By Glenn Chapman

Georgia targeted in cyber attack

Georgian government websites have been under intense cyber attack on top of the Russian military strikes launched against the country late last week, a US Internet firm said Tuesday.

Tulip Systems Inc said they took over hosting of the websites for Georgia's presidency and a major television network on Saturday, a day after Russian forces poured into Georgia in response to Tbilisi's attacks on a Moscow-backed rebel province.

Tulip executive Tom Burling said the distributed-denial-of-service (DDoS) attacks began in the weeks running up to the outbreak of the Russia-Georgia conflict and continued Tuesday after the Kremlin announced it had ceased hostilities in the former Soviet state.

"They have been attacking Georgia from a cyber standpoint since July," Burling told AFP. "They are still doing it now."

"Our poor technician here has gotten three hours sleep in the past four days," he said.

Burling suggested that Russia was behind the attacks, which are similar to a cyber offensive waged against Estonia last year that coincided with a diplomatic spat between the Baltic state and Moscow.

DDoS attacks consist of overloading websites with so many online requests that systems crash.

Burling said Georgian government websites were being slammed with hundreds of millions of simultaneous requests for documents when Tulip gave them refuge, Burling said.

"The cyber attack was taking down every Georgian government website," he said.

On Tuesday, the Georgian sites hosted on Tulip were still reportedly getting hit with 68,000 requests at a time.

Russia has denied involvement in cyber assaults on Georgia and experts say it is difficult to determine exactly who is behind such attacks.

"The Georgian government's websites have obviously been under attack," said Gadi Evron, an Israeli computer security specialist that investigated the cyber assault on Estonia.

"It is simply too early and we lack enough information to reach any conclusion as to the motive and identity of the attackers," he said.

Evron said that such cyber warfare has become commonplace in the past decade.

"These types of attack are only natural and happen immediately following any conflict or political tension," Evron told AFP in an email.

DDoS attacks are simple, economical and hard to trace.

The assaults are typically done by using networks of computers that have been turned into "zombies" or "bots" with malicious software planted by hackers without the owners of machines being aware.

"Botnets" can grow to thousands or millions of machines and be commanded to simultaneously make requests at targeted websites.

Andre DiMino, director of Shadowserver, a nonprofit Internet security watchdog with team members around the world, warned against jumping to the conclusion that Russia's government is the culprit in the Georgia cyber attacks.

"This actually looks more like grass roots hacktivist types -- people that jumped on the bandwagon," DiMino said, using Internet jargon referring to political activists that resort to online evil-doing.

Tulip's Burling said the trend of such cyber maliciousness was a cause for concern.

"It's like the Olympics. We are supposed to be above politics in the Internet community."

Georgian forces attacked the Moscow-backed rebel province of South Ossetia to regain control of the region which broke away from Tbilisi in the early 1990s.

Russian troops and tanks poured into Georgia on Friday after the Georgian offensive.

INTERNATIONAL DATA GROUP

13 August 2008

By Jeremy Kirk

Estonia, Poland help Georgia fight cyber attacks

In an intriguing cyber alliance, two Estonian computer experts are scheduled to arrive in Georgia by evening to keep the country's networks running amid an intense military confrontation with Russia.

And Poland has lent space on its president's Web page for Georgia to post updates on its ongoing conflict with Russia, which launched a military campaign on Friday to eject Georgian troops from South Ossetia and Abkhazia, two renegade areas with strong ties to Russia.

The cooperation between the former Iron Curtain allies is aimed at blunting pro-Russian computer hackers, who have been blamed over the last few years for cyber attacks against Estonia, Lithuania and Georgia in incidents linked to political friction between those nations and Russia.

Two of the four experts that staff Estonia's Computer Emergency Response Team (CERT) were waiting Tuesday morning in Yerevan, the capital of Armenia, seeking permission to drive into Georgia, said Katrin Pärgmäe, communication manager for the Estonian Informatics Center. The two officials are also bringing humanitarian aid, she said.

Estonia is also now hosting Georgia's Ministry of Foreign Affairs Web site, which has been under sustained attack over the last few days.

"Let's just say we moved it," Pärgmäe said. "I know that there are interested parties who read media so it's not good to say exactly where the hosting is."

The Web site for Georgia's president, Mikheil Saakashvili, remained up on Tuesday morning. That site was knocked offline around mid-July after a DDOS attack from a botnet, network experts said.

The botnet was based on the "MachBot" code, which communicates to other compromised PCs over the HTTP (Hypertext Transfer Protocol), the same protocol used for transmitting Web pages. MachBot code has been known to be used by Russian bot herders, according to the Shadowserver Foundation, which tracks malicious Internet activity.

Shadowserver said Monday that hackers had at one point defaced the Web site for Georgia's parliament. "The attackers have inserted a large image made up of several smaller side-by-side images of pictures of both the Georgian President and Adolf Hitler," the group wrote.

Georgia is now also hosting some sites in the U.S., a logical move to better defend the sites against attacks, Pärgmäe said. Shadowserver wrote that the presidential site appeared to have been moved to an IP (Internet protocol) address belonging to Tulip Systems, an ISP in Atlanta, Georgia.

The country is also looking to other ways to keep information flowing. A Georgian news site was also up, but the site warned it was under "permanent DDOS attack" That Web site has set up a group in Google's Groups service, where subscribers can get the news stories it regularly posts.

Georgia's banking sites also suffered attacks that caused them to shut down their online systems, said David Tabatadze, a security officer with the Georgia Research and Educational Networking Association and Georgia's CERT. Some of those systems are still down, he said.

Tabatadze said that the majority of Georgia's Internet traffic is routed through Turkey, with some of it going through Russia. Although some news reports indicated Georgia's Internet traffic may have been shifted through Russia, Tabatadze said that's not the case.

"We have checked the traffic route on Ripe.net...and we did not see any traffic re-routing via Russia," Tabatadze said.

It appears that large groups of hackers are working together to take down the Web sites, but the attacks have been so intense that it will take a while to analyze, Tabatadze said.

Other CERTs around the world have been helping to provide information on the attacks, Tabatadze said.

The last few days have been a nerve-racking time for Georgians, said Tabatadze, who said he heard explosions on Sunday when Russian planes bombed air-traffic control stations near Tbilisi, Georgia's capital.

"You can't even imagine the situation," Tabatadze said. "This is a terrible end for Georgia."

On Tuesday morning, Russia announced it would stop military operations in South Ossetia and Abkhazia, saying the safety of its peacekeepers in the region had been secured.

THE TELEGRAPH

13 August 2008

By John Swaine

Russia continues cyber war on Georgia

Their assault, which began before the commencement of the five-day Russian military offensive, has again crashed the official website of the central government and has been widened to include a US company which stepped in to rescue the website of Mikheil Saakashvili, the Georgian President.

Tom Burling, from Tulip Systems, which began hosting the President's site on its servers in Atlanta after it was brought down by the hackers, said his company had become the latest target of a flood of bogus traffic sent from Russia to crash the sites. He said the malicious visits were outnumbering legitimate ones 5000 to 1.

Mr Burling, who has reported the attacks to the FBI, said his company was working around the clock to combat the hackers. "Our people aren't getting any sleep," he said.

The President's website is currently accessible, as are the sites of the Ministry of Foreign Affairs and Ministry of Defence, which were also brought down in the initial wave of attacks. At one stage, photographs comparing Mr Saaskashvili with Adolf Hitler were posted on the Foreign Ministry's site. The website of the National Bank of Georgia has also been compromised.

The Russian hackers are launching waves of distributed denial-of-service (DDoS) attacks on the websites. This means their computers, and the computers of unsuspecting people whose home systems they have hacked and enlisted for their "botnet", or swarm of zombie computers, are directed to simultaneously flood a chosen site with thousands of visits in order to overload it and bring it offline.

Last April the computer systems of the Estonian Government came under attack in a co-ordinated three-week assault that was widely credited to state-sponsored Russian hackers.

The Georgian Government said that the present disruption was being caused by attacks carried out by Russia as part of the conflict between the two states, which was triggered last week over Georgia's attempt to reassert authority over its northern rebel province of South Ossetia.

In a statement, the Georgian Ministry of Foreign Affairs said: "A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Ministry of Foreign Affairs."

Analysts immediately laid the blame for the attacks on Georgian sites with the Russian Business Network (RBN), a gang of criminal hackers which has close links to the Russian mafia and government.

Jart Armin, a researcher who tracks RBN activity, said visitors to the Georgian sites had been re-routed through servers in Russia and Turkey, which were "well known to be under the control of RBN and influenced by the Russian Government."

Greg Day, a security analyst at McAfee, said increasingly hacking will be a matter of national security.

"We can expect to see cyber attacks being increasingly used as a weapon. The benefits of using such methods are that no one is directly physically hurt or killed and it is much harder to pinpoint the source and who is involved," he told Sky News.

The hackers have also been targeting the website of Garry Kasparov, the Russian opposition figure and former chess champion.

WASHINGTON POST

27 August 2008

By Kim Hart

A New Breed Of Hackers Tracks Online Acts of War

'Hacktivists' Update Their Mission

TORONTO -- Here in the Citizen Lab at the University of Toronto, a new breed of hackers is conducting digital espionage.

They are among a growing number of investigators who monitor how traffic is routed through countries, where Web sites are blocked and why it's all happening. Now they are turning their scrutiny to a new weapon of international warfare: cyber attacks.

Tracking wars isn't what many of the researchers, who call themselves "hacktivists," set out to do. Many began intending to help residents in countries that censor online content. But as the Internet has evolved, so has their mission.

Ronald J. Deibert, director of the Citizen Lab, calls the organization a "global civil society counterintelligence agency" and refers to the lab as the "NSA of operations."

Their efforts have ramped up in the past year as researchers gather evidence that Internet assaults are playing a larger role in military strategy and political struggles. Even before Georgia and Russia entered a ground war earlier this month, Citizen Lab's researchers noticed sporadic attacks aimed at several Georgian Web sites. Such attacks are especially threatening to countries that increasingly link critical activities such as banking and transportation to the Internet.

Once the fighting began, massive raids on Georgia's Internet infrastructure were deployed using techniques similar to those used by Russian criminal organizations. Then, attacks seemed to come from individuals who found online instructions for launching their own assaults, shutting down much of Georgia's communication system.

Two weeks later, researchers are still trying to trace the origins of the attacks. "These attacks in effect had the same effect that a military attack would have," said Rafal Rohozinski, who co-founded the Information Warfare Monitor, which tracks cyber attacks, with Citizen Lab in 2003. "That suddenly means that in cyberspace anyone can build an A-bomb."

The cyber attacks that disabled many Georgian and Russian Web sites earlier this month marked the first time such an assault coincided with physical fighting. And the digital battlefield will likely become a permanent front in modern warfare, Deibert said.

Seven years ago, Deibert opened the Citizen Lab using grant money from the Ford Foundation. Soon after, he and Rohozinski helped begin the OpenNet Initiative, a collaboration with Harvard's Law School, Cambridge and Oxford universities that tracks patterns of Internet censorship in countries that use filters, such as China. The project received an additional $3 million from the MacArthur Foundation. Deibert and Rohozinski also launched the Information Warfare Monitor to investigate how the Internet is used by state military and political operations. And Citizen Lab researchers have created a software tool called Psiphon that helps users bypass Internet filters.

The combined projects have about 100 researchers in more than 70 countries mapping Web traffic and testing access to thousands of sites.

A number of companies specialize in cyber security, and several nonprofit organizations have formed cyber-surveillance projects to keep international vigil over the Web. Shadowserver.org, for example, is a group of 10 volunteer researchers who post their findings about cyber attacks online.

The small Toronto office of Citizen Lab, tucked in a basement of the university's Munk Centre for International Studies, serves as the technological backbone for the operations. World maps and newspaper clips cover the walls. Researchers move between multiple computer screens, studying lists of codes with results from field tests in Uzbekistan, Cambodia, Iran and Venezuela, to name a few.

"We rely on local experts to help us find out why a particular site is being blocked," Deibert said. It could be a problem with the Internet service provider, a temporary connection glitch or a downed server. "But what's more effective is blasting a site into oblivion when it is strategically important. It's becoming a real arms race."

He's referring to "denial of service" attacks, in which hundreds of computers in a network, or "botnets," simultaneously bombard a Web site with millions of requests, overwhelming and crashing the server. In Georgia, such attacks were strong enough to knock key sources of news and information offline for days.

Georgian Internet service providers also limited access to Russian news media outlets, cutting off the only remaining updates about the war. On the night of Aug. 12 -- the height of the fighting -- "there was panic in Tbilisi brought about by a vacuum of information," Rohozinski said.

Shadowserver saw the first denial of service attack against Georgia's presidential Web site July 20. When the fighting began, Andre M. Di Mino, Shadowserver's founder, counted at least six botnets launching attacks, but it was "difficult to tell if it was a grass-roots effort or one commissioned by the government."

The organization detects between 30 and 50 denial of service attacks every day around the world, and Di Mino said they have become more sophisticated over the past two years.

"It really went from almost a kiddie type of thing to where it's an organized enterprise," he said. But he's hesitant to label this month's attacks as a form of cyberwar, although he expects networks to play an expanded role in political clashes.

Jose Nazario, a security researcher with Arbor Networks, said cyber attacks used to target a computer's operating system. But he's seen a "tremendous rise" in attacks on Web browsers, allowing attackers access to much more personal information, such as which sites a person visits frequently. An attacker then could learn which servers to target in order to disrupt communication.

It's unclear who is behind the attacks, however. In some cases, the locations of botnet controllers can be traced, but it's impossible to know whether an attacker is working on the behalf of another organization or government. "It's going to take a year to figure this out," Nazario said.

The data trail often goes cold when it crosses borders because there is little legal framework for such investigations. And many countries, along with the United Nations and other international bodies, are still weighing whether a cyber attack is an act of war.

"If a state brings down the Internet intentionally, another state could very well consider that a hostile act," said Jonathan Zittrain, co-founder of Harvard's Berkman Center for Internet Society, and a principal investigator for the OpenNet Initiative.

There are also strategic reasons not to disrupt networks in order to monitor the enemy's conversations or to spread misinformation.

"That's an amazing intelligence opportunity," he said.

Using the Internet to control information can be more important than disrupting the networks when it comes to military strategy, Rohozinski said. In Georgia, for example, the lack of access to both Georgian and Russian sources of information kept citizens in the dark while the fighting continued.

"Sometimes the objective is not to knock out the infrastructure but to undermine the will of the people you're fighting against," he said. "It's about the nuts and bolts, but it's also about how perceptions can be shaped through what's available and what's not."

NEWSWEEK

1 September 2008

By Trevis Wentworth

You've Got Malice

Russian nationalists waged a cyber war against Georgia. Fighting back is virtually impossible.

On July 20, weeks before Russia stunned Georgia with a rapid invasion, the cyber attack was already under way. While Moscow baited Georgia with troop movements on the borders of the breakaway provinces of Abkhazia and South Ossetia, the "zombie" computers were already on the attack. Russian viruses had seized hundreds of thousands of computers around the world, directing them to barrage Georgian Web sites, including the pages of the president, the parliament, the foreign ministry, news agencies and banks, which shut down their servers at the first sign of attack to pre-empt identity theft. At one point the parliament's Web site was replaced by images comparing Georgian president Mikheil Saakashvili to Adolf Hitler. This was not

the first Russian cyber assault—that came against Estonia, in April of 2007—but it was the first time an Internet attack paralleled one on land.

The labyrinthine ways of the Web and the complicated interfaces between the Russian government's clandestine services and organized crime make it impossible, at this point, to say with certainty who was responsible, or how far up the chain of command it went. The Russian military certainly had the means to attack Georgia's Internet infrastructure, says Jonathan Zittrain, cofounder of Harvard's Berkman Center for Internet and Society. Moreover, the attacks were too successful to have materialized independent of one another. Bill Woodcock, the research director at Packet Clearing House, a California-based nonprofit group that tracks Internet security trends, says the attacks bear the markings of a "trained and centrally coordinated cadre of professionals."

But who? Jart Armin, who has tracked Russian cybercrime, points to the possibility that a role was played by the notorious Russian Business Network, a cybermafia that specializes in identity theft, child pornography, extortion and other dark and lucrative Internet crimes. The RBN's political agenda is vague or nonexistent, but it often contracts out its services, and Armin says there is increasing evidence that it is connected to, or at least tolerated by, the Kremlin.

Indeed the timing is such that it's hard to discount some sort of Kremlin coordination, even if it's impossible to prove, and Woodcock argues that such cyber assaults have become a tool of Russian political leadership. As the attacks' political intentions became more specific, he notes, the operations have grown more complex. In addition to targeting Georgian government and media Web sites, Russian hackers brought down the Russian newspaper Skandaly.ru, apparently for expressing some pro-Georgian sentiment. "This was the first time that they ever attacked an internal and an external target as part of the same attack," he says.

Fighting back is tough. When Russian hackers made a name for themselves last year by bringing down the Web site of the Estonian parliament along with the sites of banks, ministries and newspapers, Estonian Foreign Minister Urmas Paet immediately accused the Kremlin of backing the attacks. But he was unable to produce evidence supporting his claims. Putin eventually named a suspect, or scapegoat, within his government. As Russian hackers waged a similar assault on Georgian sites over the past few weeks, Estonia—one of Europe's most wired countries—offered its better-defended servers to host many Georgian government Web sites. Lithuania and Poland have stepped up as well, prompting some excited bloggers to suggest that this is a digital Sarajevo, akin to the events of August 1914, the start of the first Internet world war. Certainly that's exaggerated, but the mutual defense going on in cyberspace shows that these nations take the Russian threat to their online infrastructure seriously.

Still, the nature of the Internet is such that it is almost impossible to respond quickly enough. The government doesn't maintain its own botnets—large networks of zombified computers standing ready to attack—but can rent one

from a crime network, like the Russian Business Network. Then, through state-controlled media, the government can inspire waves of nationalists to amplify the destructive force. "Everybody with a laptop has the responsibility to attack the enemy—and you find out who the enemy is by looking at what the government is saying," Woodcock says.

While no one can say who wrote the malware that was used to cause Georgian servers to crash, it certainly proliferated on Russian Web sites in a user-friendly form. Gary Warner, a cybercrime expert at the University of Alabama at Birmingham, says he found "copies of the attack script" posted in the reader comments section at the bottom of virtually every story in the Russian media that covered the Georgian conflict, complete with instructions on how the script could be used to attack a specific list of Web sites. The efficiency is enough to make Russia's tanks and planes and ships, however deadly, appear downright anachronistic.

AFP

4 September 2008

Experts call for united global action against cyber attacks

The world has to unite against the growing menace of cyber terrorism, IT experts said Thursday, evoking a recent "cyber war" against Georgia as the latest example of the threat.

"The world has finally woken up and understood that cyber security needs a global approach and is a very serious matter," Estonian politician Mart Laar told a cyber security forum in the Estonian capital Tallinn.

Estonia had to deal with attacks on government websites blamed on Russian hackers in the spring of 2007.

Official Georgian websites suffered a similar cyber offensive last month in the wake of Russia's military offensive on Georgian soil. Estonia was among several states that stepped in to host hacked Georgian websites.

"The cyber war against Georgia in August demonstrated how it has become part of the real war on the ground and we must act," Laar added.

According to Laar, cyber attacks against the Georgian websites came a day ahead of Russia's August 8 military action in the country, a move roundly condemned in the West.

Robert Kramer, vice-president of public policy for CompTIA, the Computing Technology Industry Association uniting the world's top IT firms, underscored that global cyber security starts at home with the average Internet user.

"The weakest link in cyber space is the human being behind the computer with not enough awareness and skills on IT security matters," Kramer told the forum.

Heli Tiirmaa-Klaar, an IT expert with Estonia's defence ministry, repeated the warning.

"People everywhere need to understand that your unprotected computer at home can be used as a tool in cyber-war," she said.

Tim Boerner, an IT security expert with the US Secret Service, said experts noted increased attacks on Georgian web sites weeks before the first bombs fell on Georgia.

"Over one million computers worldwide were used during the cyber attacks against Estonia in spring 2007," he added.

An ex-Soviet republic that broke free from Moscow in 1991, the tiny Baltic Sea state of Estonia joined the European Union and NATO in 2004.

It has become a leader in global IT development and has focused heavily on cyber security since suffering the wave of cyber attacks in early 2007.

WASHINGTON POST (blog)

16 October 2008

By Brian Krebs

Russian Hacker Forums Fueled Georgia Cyber Attacks

An exhaustive inquiry into August's cyber attacks on the former Soviet bloc nation of Georgia finds no smoking gun in the hands of the Russian government. But experts say evidence suggests that Russian officials did little to discourage the online assault, which was coordinated through a Russian online forum that appeared to have been prepped with target lists and details about Georgian Web site vulnerabilities well before the two countries engaged in a brief but deadly ground, sea and air war.

The findings come from an open source investigation launched byProject Grey Goose, a volunteer effort by more than 100 security experts from tech giants like Microsoft and Oracle, as well as former members of the Defense Intelligence Agency, Lexis-Nexis, theDepartment of Homeland Security and defense contractor SAIC, among others.

The group began its inquiry shortly after the cyber war disabled a large number of Georgia government Web sites. Starting with the Russian hacker forum Xaker.ru (hacker.ru), investigators found a posting encouraging would-be cyber militia members to enlist at a private, password-protected online forum called StopGeorgia.ru. Grey Goose principal investigator Jeff Carr said the administrators of the hacker forum were keenly aware that American cyber sleuths were poking around: Within hours after discovering the link to the StopGeorgia site, Xaker.ru administrators deleted the link and banned all access from U.S.-based Internet addresses.

At StopGeorgia.ru, project members unearthed a top-down hierarchy of expert hackers who doled out target lists of Georgian government Web sites to relative novices, complete with instructions on how to exploit vulnerabilities in the sites in order to render them inaccessible. Following a July defacement of the Georgian president's Web site that was blamed on Russian hackers, the Georgian government blocked Russian Internet users from visiting government Web sites.

But Carr said StopGeorgia administrators also equipped recruits with directions on evading those digital roadblocks, by routing their attacks through Internet addresses in other Eastern European nations. The level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government and or military, Carr said.

"The fact that the StopGeorgia.ru site was up and running within hours of the ground assault -- with full target lists already vetted and with a large member population -- was evidence that this effort did not just spring up out of nowhere," said Carr, speaking at a forum in Tysons Corner, Va., sponsored by Palantir Technologies, an In-Q-Tel funded company in Palo Alto, Calif., whose data analysis software helped Grey Goose investigators track the origins and foot soldiers involved in the cyber attack. "If they were planning ahead of the invasion, how did they know the invasion was going to occur? The only way they could have known that is if they were told."

Initially, security experts assumed that the sites were felled via "distributed denial of service" (DDoS) attacks, a well-known method of assault that uses hundreds or thousands of compromised personal computers to flood a targeted site with so much junk traffic that it can no longer accommodate legitimate visitors. But investigators soon learned that attackers were instructed in the ways of a far more simple but equally effective attack strategy capable of throttling a targeted Web site using a single computer.

Security researcher and Grey Goose investigator Billy Rios said attackers disabled the sites using a built-in feature of MySQL, a software suite widely used by Web sites to manage back-end databases. The "benchmark" feature in MySQL allows site administrators to test the efficiency of database queries, but last year hackers posted online instructions for exploiting the benchmark feature to inject millions of junk queries into a targeted database, such that the Web servers behind the site become so tied up with bogus instructions that they effectively cease to function.

"Not only can a small number of users bring down the back end databases, it indicates that there was some form of planning, reconnaissance, and some technical sophistication by some of the members," Rios said. "It also indicates that all the information from the attacked systems was most likely already compromised and pilfered before the injection point was posted."

While Grey Goose members could find no direct link between Russian government officials and the StopGeorgia.ru forum administrators, they claim it is unreasonable to conclude that no such connection exists.

"The historical record shows clear support by members of the Russian government and implied consent in its refusal to intervene or stop the hacker attacks," the report states, naming at least three Russian politicians and military officials who have previously endorsed coordinated cyber attacks against other nations as a show of nationalistic pride.

Oleg Gordievsky, a former colonel in the Russian KGB who defected to the British intelligence wing MI6 in 1985, spoke in 1998 at an international conference on crime and discussed how Russian hackers convicted of cyber crime are sometimes offered an alternative to prison -- working for the FSB" (the federal security service of the Russian Federation and a successor to the KGB).

According to a cyber warfare analysis by researchers at Dartmouth College, Moscow has a track record of offensive hacking into Chechen Web sites. The researchers provide this account of incidents in 2002, when Russian hackers used cyber warfare in to supplement the ongoing military conflict with Chechnya.

"In 2002, Chechen rebels claimed that two of their Web sites, kavkaz.org and chechenpress.com, crashed under hack attacks by the Russian FSB security service. The website crashes were reportedly timed to occur concurrently or shortly after Russian Special Forces troops stormed the Moscow Theater in which the rebels had taken hostages. "On October 26 ... our Web Site kavkaz.org was attacked by a group of hackers," said a spokesman for the Chechen rebel site run by Movladi Udugov. Following the attack on the site, which is based in the United States, Udugov said that he was "amazed Russia's special services can operate so freely on U.S. territory." The attacks on one site, chechenpress.com, fell under the category of brute-force denial of service (DoS) attacks, while on the other site, kavkaz.org, the attacks appeared much more sophisticated.

According to Chechen sources, the Web site was hijacked by hackers from the FSB. The FSB hackers reportedly accomplished this by changing the domain registration of the site and then eliminating the data for the site from the hosting server. Upon learning of these attacks, the rebels moved the information on the sites to kavkazcenter.com. However, that site was attacked just a week later, also apparently the work of FSB hackers.

In July, Russian hackers were blamed for a similar assault on Lithuanian government Web sites. In Security Fix's account of that attack, I posted a copy of a congratulatory letter sent to nationalist Russian hackers by Nikolai Kuryanovich, a former member of the Russian Duma. The missive is dated March 2006, and addresses the hacker group Slavic Union after the group had just completed a series of successful attacks against Israeli Web sites.

"In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers," Kuryanovich wrote. "This means that a small force of

hackers is stronger than the multi-thousand force of the current armed forces."

The Grey Goose report concludes that the journeyman-apprentice relationship observed in the StopGeorgia forum will continue to be the training model used by nationalistic Russian hackers, and that those hackers are actively engaged in finding more efficient ways to disable networks.

In the meantime, Carr said, the Russian government will continue to deny any involvement in any nation-level cyber attacks.

"The Russian government has adopted this hands-off and satisfying position of deniability while enjoying the rewards achieved by the Russian hacker community," Carr said.