Project Grey Goose Phase II Report:

The evolving state of cyber warfare

March 20, 2009

greylogic

About Project Grey Goose

Project Grey Goose is an Open Source Intelligence (OSINT) initiative launched on August 22, 2008 whose original remit was to examine how the Russian cyber war was conducted against Georgian Web sites and if the Russian government was involved or if it was entirely a grass roots movement by patriotic Russian hackers.

Starting in 2009, Project Grey Goose has evolved into a formal business entity – GreyLogic; a consultancy and information services provider to governments.

This report features GreyLogic's information and analysis services for Computer Network Exploitation and Cyber Intelligence. Western government agencies for Intelligence, Law Enforcement, and Defense are invited to contact GreyLogic for more information on our services.

Executive Summary

Introduction

There has been a marked increase in cyber attacks by State and Non-State hackers since the Russia Georgia War of 2008.

In addition to the cyber clashes resulting from Israel's Operation Cast Lead and the Web site defacement of India's Eastern Railway, the British government has reported thousands of cyber attacks occurring each day on its critical infrastructure.[1]

The French Embassies in Britain, the U.S., China, and Canada came under Chinese cyber attacks in December 2008.[2]

The government of Zimbabwe has been waging a cyber war against its opposition party for the past five years.[3]

As this report is being written, a 60 day U.S. cyber security review on how the U.S. government may best proceed to protect its cyberspace from a wide variety of attacks against U.S. financial infrastructure and national security threats on a daily basis.[4]

This report aims to answer the following questions by examining three different cyber events impacting almost a dozen nations:

> How effective is Social Network Analysis in Computer Network Exploitation?
>
> How critical is the ability to access black (classified) data in a cyber intelligence effort?
>
> Is there evidence that points to Russian government involvement in the Georgia cyber attacks of July and August 2008?

---

1 http://www.timesonline.co.uk/tol/news/uk/crime/article4592677.ece
2 http://intelfusion.net/wordpress/?cat=413
3 http://concernedafricascholars.org/the-glass-fortress/
4 http://news.cnet.com/8301-13578_3-10159975-38.html

Our Key Findings

Eastern Railway Web Site

On December 24, 2008, a group that self identified as the Whackerz Pakistan defaced the Indian Eastern Railway Web site with a variety of financial threats against Indian citizens. Our findings indicate that:

- At least three of the six members of Whackerz Pakistan are well-educated professionals, and at least two are employed in the technology industry.
- Their members' religious affiliation (Muslim) is at least as important as their Geopolitical allegiances (Pakistan).
- At least one Whackerz member represents an Insider Threat for his employer, a global wireless communications company based in North America.

Operation Cast Lead

Israel began a military assault on Hamas's infrastructure in Gaza on December 27, 2008, called "Operation Cast Lead." A cyber backlash by Arabic hackers targeted thousands of Israeli government and civilian Web sites. Our findings indicate that:

- Unlike other instances of cyber conflicts (Chechnya, Estonia, Lithuania, Georgia, India), this conflict involved both State (Israel and possibly Iran) and Non-State hackers.
- Most of the Non-State Arabic hackers involved do not have the technical skill to carry out sophisticated network attacks, opting instead for small to mid-scale denial of service attacks and mass website defacements.
- We have not observed any zero day vulnerabilities exploited in these attacks. Instead, most attackers focused on old Web site vulnerabilities that had not been patched.
- This is the first instance of a voluntary botnet ("Help Israel Win") used in a Cyber conflict where individuals voluntarily passed control of their own computers to the botnet host server.

The Russia Georgia Cyber War

This section follows up our Phase I investigation of the cyber component of the Russia/Georgia war of August 2008 by looking at question of attribution in two distinct parts:

a) What can we tell by examining the network supporting the StopGerogia.ru forum

b) Is there a link between the Kremlin and those involved in the cyber attacks against Georgian Web sites

Our findings indicate that:

- Russian military policy acknowledges the strategic value achieved by utilizing methods of cyber attacks which can appear to be acts of cyber crime or terrorism.
- The StopGeorgia.ru forum was part of a bulletproofed network that relied on shell companies and false WHOIS data to (a) prevent its closure through Terms of Service violations, and (b) to mask the involvement of the Russian FSB/GRU. By mimicking the structure of the Russian Business Network, a cyber criminal enterprise, it creates plausible deniability that it is a Kremlin-funded Information Operation (IO).

- Nashi members have been involved in Cyber attacks against internal and external opponents of the Kremlin, up to and including the Estonia Cyber war. Since the Nashi receives some of its funding from the Kremlin, receives direction on focus areas from government officials, and has the favor of highly placed politicians, Nashi involvement is equivalent to Kremlin involvement.

Summary of Findings

Having examined three disparate cyber events in different regions of the world at a much deeper level than has heretofore been performed, we present the following conclusions:

Non-State hackers rely on publicizing their exploits to build their online reputations. Thanks to this need for recognition among their peers, data mining foreign language forums and social media sites can produce meaningful results. It is not, however, sufficient in and of itself and should be combined with server-level data, as well as an examination of geopolitical events occurring around the time of the cyber attacks.

Furthermore, when State interests are involved, a review of the Nation State's military doctrine related to Information Warfare is also important.

If all of this information is available, then there is little need for accessing classified (black) data. In fact, the incorporation of black data can be counterproductive as it precludes the sharing of information between non-cleared international researchers which often adds speed and veracity to an otherwise challenging pursuit.

The identification and prosecution of Non-State hackers who engage in these attacks can be an effective deterrent as shown by the Eastern Railway investigation.

Although some of the members of Whackerz Pakistan were in the position to make good on their threats of causing financial harm to Indian citizens, nothing further has been done by this group. We believe that's at least partly due to the sharing of GreyLogic's investigative results with the FBI, RCMP, and CBI shortly after the initial incident occurred.

In the case of possible Russian government involvement with the cyber attacks on Georgian government websites in July and August, 2008, the available evidence supports a strong likelihood of GRU/FSB planning and direction at a high level while relying on Nashi intermediaries and the phenomenon of crowdsourcing to obfuscate their involvement and implement their strategy.

1

India

The Eastern Railway Web Site Defacement

Action

On December 24, 2008, the Whackerz Pakistan Cr3w defaced India's Eastern Railway Website with the following announcement[1]:

"Cyber war has been declared on Indian cyberspace by Whackerz-Pakistan"

When clicked, a new window opened saying that "Mianwalian of Whackerz" has hacked the site in response to an Indian violation of Pakistani airspace; that Whackerz-Pakistan would continue to attack more Indian military and government Web sites as well as Indian financial institutions where they will destroy the records of their Indian customers.

Actors

Hacker Crew	Whackerz Pakistan
Members	PakBrain, MianWalian, Fady911x, Saudia_Hacker, Ch33ta, and Iced_rose
Also Known As	Jubni team
Country affiliation	Pakistan
Religious affiliation	Muslim
Attack history	8/2005: as Jubni, attacked India Institute of Technology Web sites at Mumbai, Guwahati, Kharagpur, and Chennai campuses. 12/2008: as Whackerz, attacked Eastern Railway Web site.
Methods	Defacements

1 http://www.financialexpress.com/news/Pak-hacker-attacks-E-Rlys-site-threatens-cyber-war-on-India/402609/

This crew has been operating for at least 3 years, probably longer. This article[1] refers to them as the Jubni team who attacked four India Institute of Technology Web sites in 2005.

In the month of August, the websites of four IITs - Mumbai, Guwahati, Kharagpur and Chennai - were hacked and defaced by a group of Pakistani hackers who call themselves the Jubni team. The hackers claimed that some of the members of the group are Majeed, Jubni, Zohaib, Pak Brain, Mian Walian and Ch33ta. The ire of the group was directed towards India, USA and Israel.

While the name of the group and some of its members have changed, the theme of being anti-India, USA, and Israel remains consistent.

[HAKR profiles for Whackerz members have been redacted from the public report]

Analysis

Whackerz-Pakistan is motivated by both nationalistic and religious allegiances, unlike their Russian or Chinese counterparts who are purely nationalistic. At least one of the members is Egyptian and two live in Canada so their geographical identity may be less important than their religious affiliation.

Their stated preferred targets are India, Israel, and the United States, so besides their involvement in the Pak-India cyber conflict they may also be involved in the Israel-Palestine cyber attacks.

At least half of its current membership are educated professionals in their 20s or older so this is a mature crew with financial resources and professional contacts in the international technology community. The employment by one of its members at a well-known global wireless communications company means that they are potentially both an external and internal threat.

1 http://archives.neohapsis.com/archives/isn/2005-q4/0323.html

2

Israel

Operation Cast Lead / Gaza Cyberwar

Action

Israel began a military assault on Hamas's infrastructure in Gaza on December 27, 2008, called "Operation Cast Lead." After almost a month into the operation, Palestinian officials declared the death toll had topped 1,000, and media reports carried images of massive property destruction and civilian casualties[1].

The exact number of Israeli or other websites that have been disrupted by hackers is unknown, but the number is well into the thousands. According to one estimate, the number reached 10,000 by the first week of January alone.

While media coverage focuses on the most high profile hacks or defacements, this current cyber campaign is a "war of a thousand cuts," with the cumulative impact on thousands of small businesses, vanity websites, and individual websites likely outweighing the impact of more publicized, larger exploits.

However, successfully compromising higher profile websites not only brings more public attention, it compels businesses all over Israel to preventatively tighten security, costing money. For that reason the financial impact of infiltrating a few larger corporate websites may be as important as disrupting thousands of smaller sites.

---

1 Overall death tolls, as well as the proportion of dead who are civilians rather than militants, is currently disputed by the Israel Defense Forces (IDF), but they admit to at least 900 people killed as of January 22, 2009. Lazaroff, Tovah and Yaakov Katz. "Israel Disputes Gaza Death Toll," Jerusalem Post, January 22, 2009. http://www.jpost.com/servlet/Satellite?cid=1232292939271&pagename=JPost%2FJPArticle%2FShowFull

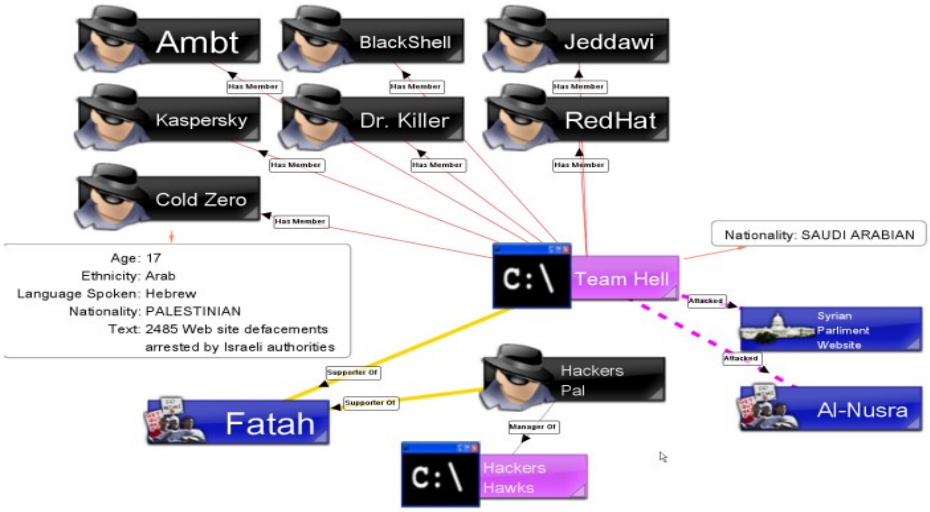
Actors

Cold Zero: Cold Zero is a member of Team Hell. Unlike the majority of Team Hell members who are Egyptian, Cold Zero is Palestinian and is proficient in Hebrew. The Arabic Mirror credits him with 2485 Web site defacements, of which 779 occurred during Operation Cast Lead. His website is www.hackteach.net.

According to a French language news source Zataz News, January 3, 2009, Cold Zero was arrested by Israeli authorities. The news source identified him as a 17 year old Israeli Arab. It reported that he appeared on January 6 before the Federal Court of Haifa, where the Israeli Justice Department alleged that he attacked commercial and political sites, mentioning the Likud Party website hack as well as an attack on the website of the Tel Aviv Maccabis basketball team.

According to the same source, he worked with accomplices in Turkey, Lebanon, Saudi Arabia, and elsewhere. He was caught in a "honey pot" set up by authorities. Authorities also uncovered his identity from a database stolen from Turkish hackers.

Team Hell:



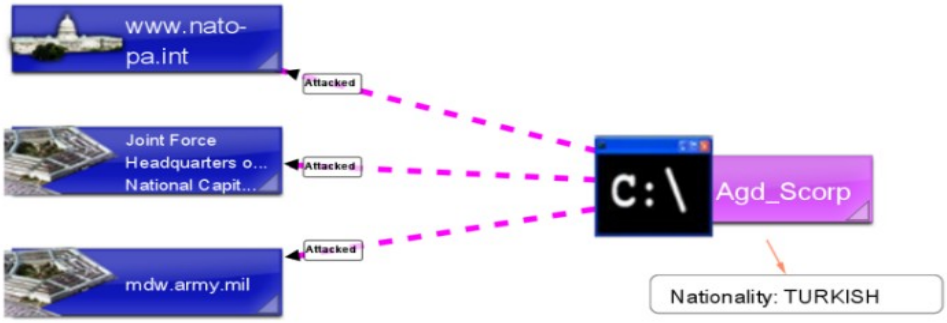
Team Hell self-identifies as a Saudi-based hackers group, usually consisting of Kaspersky, Jeddawi, Dr. Killer, BlackShell, RedHat, Ambt, and Cold Zero.

Team Hell's politically oriented-hacks include more than just Israeli sites. In April 2007, Team Hell hacked Al-Nusra, a Palestinian-focused Jihadist website. They left a message indicating they associated al-Nusra with religious deviancy.

On websites they have defaced, Cold Zero and Team Hell have expressed support for the secular, nationalist Fatah party. This would explain why Team Hell would hack Al-Nusra, a Salafist-Jihadist website, even though it is also anti-Israel. The group has also defaced the website of the Syrian parliament[2].

2 http://www.zone-h.org/component/option,com_mirrorwrp/Itemid,160/id,5573205/

Agd_Scorp/Peace Crew:



Agd_Scorp/Peace Crew are Turkish hackers who defaced NATO and US military Web sites in response to Operation Cast Lead. On three subdomains of mdw.army.mil, belonging to the US Army Military District of Washington, and on the NATO parliament site www.nato-pa.int, the group posted a message reading "Stop attacks u israel and usa! You cursed nations! One day muslims will clean the world from you."[3] The group also used a SQL Injection attack to deface the Web site of the Joint Force Headquarters of the National Capital Region.[4]

Jurm Team: Jurm Team is a Moroccan group that has partnered with both Agd_Scorp and Team Evil in defacements. They have recently defaced the Israeli portals for major companies or products, including Kia, Sprite, Fanta, and Daihatsu. Their members call themselves: Jurm, Sql_Master, CyberTerrorist, Dr. Noursoft, Dr. Win, J3ibi9a, Scriptpx //Fatna and Bant Hmida.

C-H Team: C-H Team consists of two hackers or hacker teams: Cmos_Clr and hard_hackerz. C H Team targets Dutch and Israeli websites, leaving threatening messages in Hebrew on the latter. [5] The two are Algerian. Besides defacing sites, Cmos_Clr claims to have used a variant of the Bifrost Trojan horse in order to break into Israeli computers, infiltrating 18 individual machines.[6]

Hackers Pal: Hackers Pal is the administrator of the Hackers Hawks website, and has claimed 285 defacements of Israeli websites. He is a supporter of the secular Fatah party.

Gaza Hacker Team: Gaza Hacker Team runs the website of the same name. They were responsible for defacing the Kadima party website on February 13. The team consists of six members: Lito, Le0n, Claw, Virus, Zero code, and Zero Killer.

---

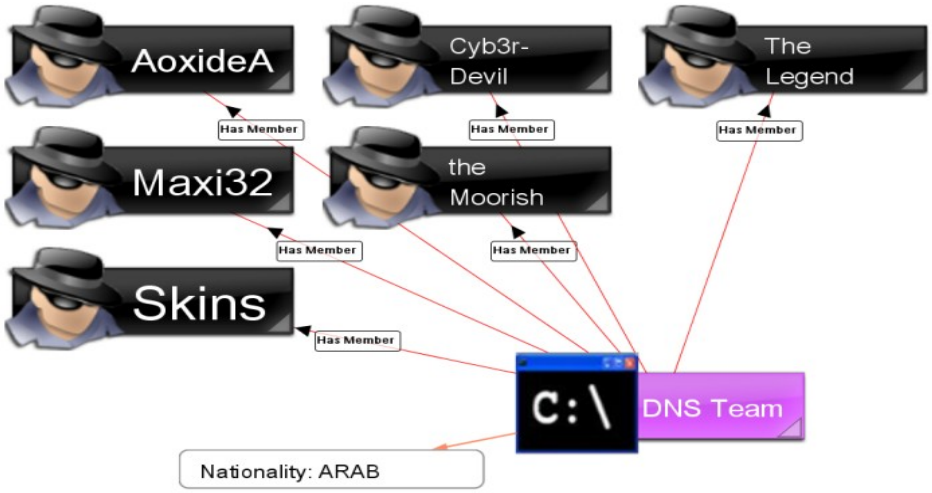
3 McMillan, Robert. "Hackers Deface NATO, US Army Web Sites," Computer World, January 9, 2009. http://www.zone-h.org/content/view/15003/30/

4 Ibid

5A mirror of one of C-H Team's defacements can be seen here: http://www.arabic-m.com/index.php?page=mirror&id=23550

6http://www.hackteach.org/cc/showthread.php?t=137613&page=2.

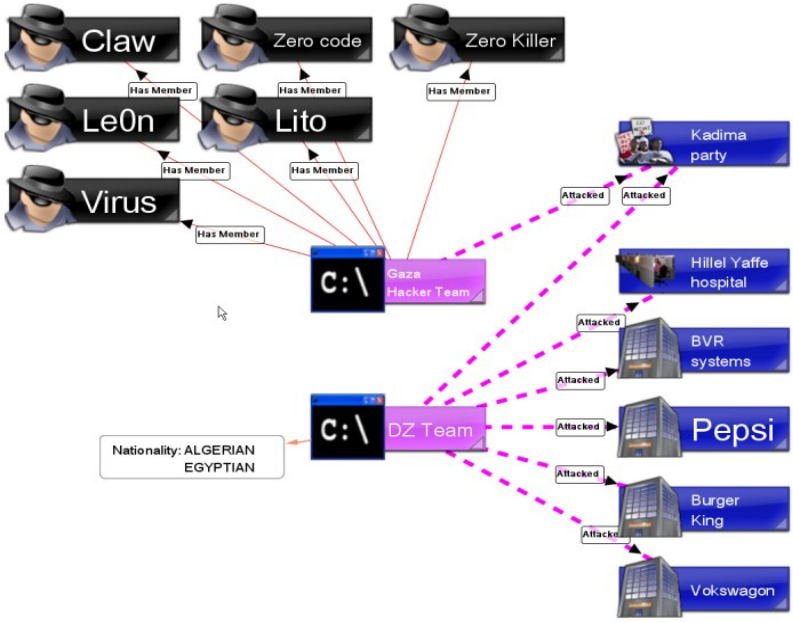
DNS Team:



DNS team is an active Arab hackers team focused primarily on apolitical hacking, however they occasionally exhibit politically motivated attacks such as targeting Web sites in Denmark and the Netherlands during the Fall of 2008 in retaliation for the cartoon controversy. They've also participated in recent anti-Israel hacks.

DNS team maintains a hacking and security forum at http://www.v4-team.com/cc/.

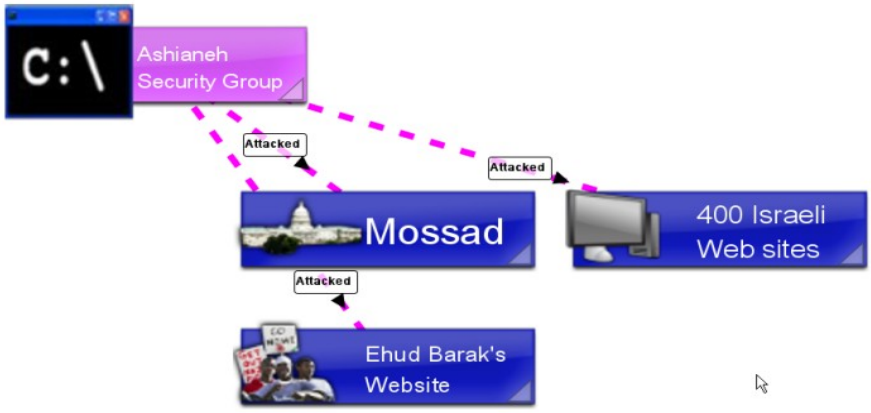
DZ Team:



DZ Team consists of Algerian and Egyptian hackers who use the aliases AoxideA, Maxi32, Skins, The Legend, Cyb3r-Devil, and the Moorish. They have defaced several Israeli Web sites including Vokswagon, Burger King, and Pepsi's Israeli portals, the Web site of israeli defense contractor BVR systems, the Kadima party Web site, and the Hillel Yaffe hospital Web site. Videos of the groups' successful defacements were posted to YouTube.[7]

7 http://www.youtube.com/watch?v=OuRhHjYb8SQ

Ashianeh Security Group:



The Iranian Fars News Agency reported that the Ashianeh Security Group hacked 400 Israeli Web sites, including those of the Mossad and Israeli Defense Minister Ehud Barak.[8]

Since this group doesn't participate in online hacker forums, it may be State-supported (Iran).

Nimr al-Iraq: Nimr al-Iraq is credited with updating the al-Durrah Distributed Denial of Service (DDoS) tool for use during Operation Cast Lead. He has also provided links to a Remote Administration Tool (RAT) program called hackattack[9], which enables a hacker to gain remote control over another person's computer.

According to his profile on soqor.net, Nimr al-Iraq is a 22 year old Iraqi named Mohammed Sattar al-Shamari and is listed as a former moderator on the site.

Analysis

Analysis of discussions on Arabic hacker forums and general pro-Jihad forums indicate that anti-Israeli hackers would like to carry out serious cyber attacks against Israeli targets, however, they do not have a demonstrated capability to carry out such attacks. Instead, their actions have been limited to small to mid-scale denial of service attacks and mass website defacements.

They may also have attempted to compromise individual computers via Trojans, particularly the Bifroze Trojan, a variant of which was developed by members of the 3asfh hacker forum.

They also discuss the desire to use viruses against Israeli computers, although the kind of viruses under discussion are relatively old and many computers would already have been updated with protections against them.

DDoS Attacks

Muslim hackers are using both indigenously developed and borrowed DDOS tools, and making them available for download on hacker forums. One tool, named after Mohammed al-Durra, a Palestinian child allegedly shot and killed by Israeli soldiers in 2000, was first developed in 2006. An updated version has been provided by Nimr al-Iraq for use in the current conflict.

With the al-Durra program, a user voluntarily downloads the program and then

---

8 Fars News Agency, January 7, 2009 and January 10, 2009. Via World News Connection.

9 http://www.soqor.net/forums/hackattack-play-10000000000000000Percent-t9646.html

checks to see what the target websites are on Arabic hacker forums. He then plugs in the target and the program will repeatedly send requests to it. When a sufficient number of people utilize the al-Durra program against a site, they can overwhelm it and bring it down. Other DDOS tools developed by hackers outside this community, such as hack tek, are also being used.

Such tools do not require sophisticated technical skills or training, which make them useful in a political dispute such as the Gaza crisis, when there is a very large community globally willing to assist in cyber attacks against Israel, but not necessarily skilled enough for more sophisticated attacks.

Web Site Defacements

The hackers download vulnerability scanners from hacker forums to find websites with exploitable vulnerabilities. On the Arabic language forums, they have discussed using a few different methods, including SQL injection, xss, and other web server software vulnerabilities.

In most cases, they are reusing previously released exploit code to attack known vulnerabilities picked up by vulnerability scanners. This is somewhat more difficult than the denial of service attacks, but is still not considered sophisticated on the larger spectrum of hacking activities. The vulnerabilities being exploited by these hackers have already been identified and patches and updates have been released to fix them. The only websites that are still vulnerable are those whose administrators have been lax in updating their software and downloading patches. There is no evidence that this community is locating “zero day” vulnerabilities at this time – those that have not yet been discovered.

Viruses and Trojans

Hacker forums reveal a desire to use viruses against Israeli targets but no evidence of success thus far. A couple of hackers have boasted of successfully using Trojans and RAT (Remote Administrations Tools) to gain wide access to individual Israeli computers. This could give them the ability to capture passwords and other important data, facilitating financial crime and harassment. However, there is not yet much evidence that they have been successful with these tools.

Israeli Retaliation

Israel and its supporters have also participated in this cyber conflict in a couple of ways. The Israeli government is behind an effort to recruit supporters who speak languages other than Hebrew – mostly new immigrants – to flood blogs with pro-Israel opinions.

The Israel Defense Forces has hacked a television station belonging to Hamas. Supporters of Israel have also been hacking pro-Palestinian Facebook groups, using fake login pages and phishing emails to collect the login details of group members.

According to the administrators of one of the anti-Israeli hacker websites, Gaza Hacker Team, pro-Israel activists are also pressuring hosting companies to cut off service to hacker websites. After the Gaza Hacker Team defaced the Kadima party website, they reported that their US hosting company denied them service after being subjected to “Jewish” pressure.

Voluntary Botnet: Perhaps the most creative tactic employed by Israel’s supporters is the development of a voluntary botnet. Developed by a group of Israeli hacktivists known as “Help Israel Win,” the distributed denial of service tool, called “Patriot,” is designed to attack anti-Israel websites.

Once installed and executed, Patriot opens a connection to a server hosted by

Defenderhosting.com. It runs in the background of a PC and does not have a configurable user interface that allows the user to control which sites to attack. Rather, the server at defenderhosting.com likely updates the client with the IP addresses to target.

“Help Israel Win” describe themselves as “a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering…”

Their stated goal is to create “a project that unites the computer capabilities of many people around the world. Our goal is to use this power in order to disrupt our enemy’s efforts to destroy the state of Israel.”

The Help Israel Win website is registered to Ron Shalit of Haifa, Israel.

3

Russia

Attribution and Bulletproof Networks

This section follows up our Phase I investigation of the cyber component of the Russia/Georgia war of August 2008 by looking at question of attribution in two distinct parts:

c) What can we tell by examining the network supporting the StopGerogia.ru forum

d) Is there a link between the Kremlin and those involved in the cyber attacks against Georgian Web sites

Creating a bulletproof network

A bulletproof network allows its customers a great degree of latitude in conducting operations that would otherwise constitute terms of service (TOS) violations.

StopGeorgia.ru

StopGeorgia.ru was a password-protected forum built with phpBB software and launched within 24 hours after the commencement of Russia's ground, sea, and air assault on the nation of Georgia on August 8, 2008. While cyber attacks occurred against Georgian government Web sites as early as July 21, 2008, this particular forum was not active until the day after the invasion. It provided hackers of all levels with vetted target lists, links to malware to be used to attack Georgian government Web sites, and expert advice for novice hackers (of which there were many).

A WHOIS search on the StopGeorgia.ru domain revealed the following information:

Domain	STOPGEORGIA.RU
Type	CORPORATE
Nserver	ns1.gost.in
Nserver	ns2.gost.in
State	Registered, Delegated
Person	Private Person

Phone	+7 908 3400066
E-mail	anac109@mail.ru
Registrar	NAUNET-REG-RIPN

NAUNET.RU

NAUNET is a Russian registrar that is blacklisted by the Spamhaus Project for providing cybercrime/spam/phish domains (Spamhaus SBL advisory #SBL67369 01 Dec 2008).

The domain name StopGeorgia.ru was acquired at Naunet.ru. Part of the complaint against Naunet on file at Spamhaus is that it has knowingly accepted false information in violation of RPIN rules.

In the Whois info for StopGeorgia.ru, the phone number of 7 908 3400066 and e-mail address anac1099mail.ru are both listed in the registrar information for a variety of Web sites selling things like fake passports, adult porn, and ATM skimmers.

While the domain information for StopGeorgia.ru doesn't list a person's name, opting instead for the ubiquitous “private person”, other domains with the same telephone number and e-mail address have been registered under the name Andrej V Uglovatyi.

Andrej V Uglovatyi, however, is most likely a fictitious person. A search on Yandex.com returns only two unique hits for the name. Considering the amount of data being collected online for individuals today, as well as the fact that Andrej V. Uglovatyi is purportedly conducting a number of businesses online, receiving so few hits can only be due to this name being a pseudonym used in shady domain registrations such as this one at www.dokim.ru (Creation of passports aned driver licenses for Russia and EU countries)l.

SteadyHost.ru

Performing a WHOIS on the IP address is an important step in the money trail process. Someone need to purchase time on a server to host the PHP forum. The Stopgeorgia.ru IP address is 75.126.142.110 which resolves to a small Russian company called SteadyHost (www.steadyhost.ru).

The domain registration for Steadyhost.ru provides the following information:

Domain	STEADYHOST.RU
Type	CORPORATE
Nserver	ns1.steadyhoster.com
Nserver	ns2.steadyhoster.com
State	Registered, Delegated
Person	Sergey A Deduhin
Phone	+7 905 4754005
E-mail	****@steadyhost.ru
Registrar	RUCENTER-REG-RIPN
Created	09/30/06

Paid till	09/30/09
Source	TC-RIPN

Sergey A. Deduhin, the person who registered the domain name Steadyhost.ru, doesn't seem to have any more of an Internet footprint than Andrej V Uglovatyj of StopGeorgia.ru.

According to contact information at SteadyHost's Web site, it has its offices in an apartment building at 88 Khoroshevskoe Shosse, Moskva (Moscow). A search on Yandex reveals another tenant at that same address – Uniastrom Bank, which is a private bank catering to individuals and small to medium-sized companies throughout the Russian Federation.

Neighboring Uniastrom Bank, at 86 Khoroshevskoe Shosse, is a Ministry of Defense Research Institute called the **Center for Research of Military Strength of Foreign Countries**. And just down the block, at 76 Khoroshevskoe Shosse is **GRU** headquarters, also known as The Aquarium.

Based upon the proximity of the GRU to the apartment building, it's reasonable to assume that some GRU personnel live there. It does provide convenient access on a number of levels, not the least of which is the ability to provide cover accommodations (i.e., someone to provide minimum business support activities for SteadyHost.

Figure 7.5: Google Earth view of GRU headquarters

The GRU is the Main Intelligence Directorate of the Russian Armed Forces. its primary business is deploying several thousand spies in foreign countries for political and military information gathering.

According to the Federation of American Scientists (FAS) Web site, the GRU may be thought of as the Russian equivalent of the U.S. Defense Intelligence Agency (DIA). It is involved in the collection of Human Intelligence (HUMINT) via foreign agents, Signals Intelligence (SIGINT) via various electronic mediums, and Image Intelligence (IMINT) via satellite imagery.

In 1996, in an interview with Pravda, the leader of the GRU at that time, General

Fedor Ladygin, included technical espionage among the missions of his organization (Komsomolskaya Pravda, 05 November 1996). This includes the hacking of computer networks to gain access to sensitive data.

The current leader, General Valentin Korabelnikov, added Open Source Intelligence (OSINT) to the GRU's mission according to an interview with CDI Russia Weekly on July 17, 2003.

Innovation IT Solutions Corp

Most legitimate registrars will confirm at least some of the registration information provided by a customer as part of the process of registering a domain name. Those that don't have become favorites of spammers and cyber criminals.

If you look deeper at the information provided on the StopGeorgia.ru IP address, you'll see that it is part of an IP block leased to Innovation IT Solutions Corp in England by SoftLayer Technologies in Dallas.

Innovation IT Solutions Corp has a Web site URL: http://init-sol.com/ but no Web site. Instead visitors see a place holder page providing basic contact information:

According to WHOIS data, the Init-sol.com domain name was registered by an employee of Innovation IT Solutions Corp named Andrey Nesterenko. Mr. Nesterenko purchased the domain name through another company – Mirhosting.com.

If you examine the WHOIS records below, you'll see that Mr. Nesterenko is apparently employed by both companies, and that both companies share the same business address: 95 Wilton Road, Suite 3, London. A Google search for that address brings up a variety of businesses including a porn site (Cheeky-Touch), a teen site (Teencharts.com), Goldstein Equitas Inc., and Global Securities Consulting; in other words, 95 Wilton Road, Suite 3, London, is a mail drop.

Domain name	INIT-SOL.COM
Registrant	Innovation IT Solutions Corp Andrey Nesterenko 95 Wilton Road, Suite 3 London London,SW1V 1BZ GB Tel. +44.8458692184 Fax. +44.8450205104
Creation date	10/10/04
Expiration date	10/10/09
Domain servers	ns5.dnska.com ns6.dnska.com
Administrative contact	Innovation IT Solutions Corp
Status	Active

Innovation IT Solutions Corp is not a registered business in the UK or anywhere else and doesn't seem to exist outside of its London mail drop address.

Mirhosting.com

MirHosting provides some substantive information on its Web site regarding its services, albeit in the Russian language. According to Dun and Bradstreet, its principal and sole stockholder, Andrey Nesterenko, is a Russian national living in the Netherlands, yet its business address is a mail drop in London; the same one used by Innovation IT Solutions Corp.

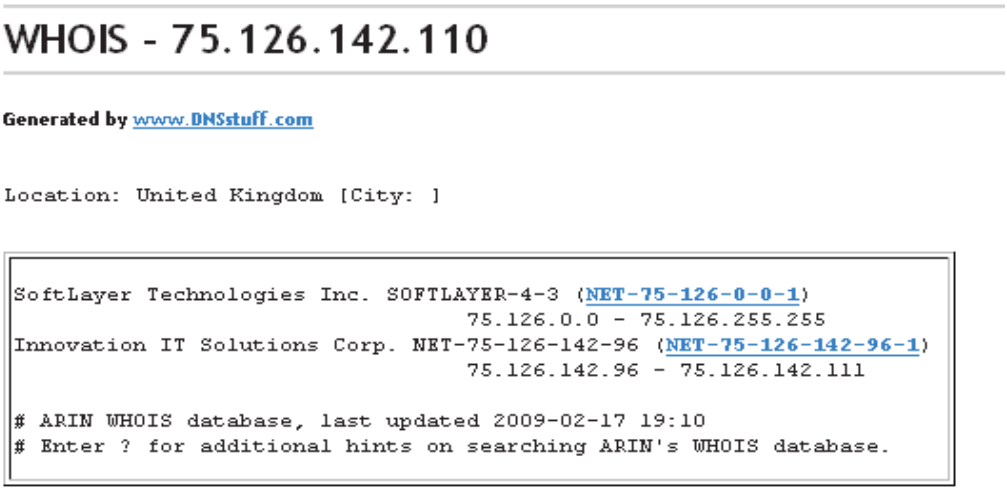
Domain name	MIRHOSTING.COM
Registrant	Innovation IT Solutions Corp Andrey Nesterenko 95 Wilton Road, Suite 3 London London,SW1V 1BZ GB Tel. +44.8458692184 Fax. +44.8450205104
Creation date	10/10/04
Expiration date	10/10/09
Domain servers	ns2.dnska.com ns1.dnska.com
Administrative contact	Innovation IT Solutions Corp
Status	Active

MirHosting provides some substantive information on its Web site regarding its services, albeit in the Russian language. According to Dun and Bradstreet, its principal and sole stockholder is a Russian national living in the Netherlands, yet its business address is a mail drop in London; the same one used by Innovation IT Solutions Corp.

SoftLayer Technologies

The IP address for the StopGeorgia.ru forum (75,126.142.110) can be traced backwards from SteadyHost to Innovation IT Solutions Corp to SoftLayer Technologies, a U.S. Company based in Dallas, TX with server locations in Seattle, WA and Washington D.C.

Figure 7.7: WHOIS data for 75.126.142.110



WHOIS - 75.126.142.110

Generated by www.DNSstuff.com

Location: United Kingdom [City:]

```
SoftLayer Technologies Inc. SOFTLAYER-4-3 (NET-75-126-0-0-1)
                                  75.126.0.0 - 75.126.255.255
Innovation IT Solutions Corp. NET-75-126-142-96 (NET-75-126-142-96-1)
                                  75.126.142.96 - 75.126.142.111

# ARIN WHOIS database, last updated 2009-02-17 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

SoftLayer Technologies and The Planet (also in Dallas, TX) share the unique distinction of being on StopBadware.org's Top 10 worst badware network blocks. To add some perspective to this, StopBadware.org's May 2008 report reveals China to be the world leader hosting 52% of all badware sites, while the U.S. hosts 21%. None of the other countries involved, including Russia, individually host more than 4%.

The Kremlin and the Russian Internet (RUNET)

One of the most difficult questions that the Project Grey Goose team faced in investigating the cyber war between Russian and Georgia was if there was evidence that the Russian government was involved. Our key finding in October, 2008 was:

We assess with high confidence that the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions.

While forum members are quite open about their targets and methods, we were unable in this round of collection/analysis to find any references to state organizations guiding or directing attacks. There are several possible explanations as to why this is the case.

- There was no external involvement or direction from State organizations
- Our collection efforts were not far-reaching or deep enough to identify these connections
- Involvement by State organizations was done in an entirely non-attributable way

The situation has since changed. In February, 2009, the Russian media reported a story that has provided new evidence pointing to how the Russian government sponsors and pays leaders of Russian youth organizations to engage in Information Operations up to and including hacking to silence or suppress opposition groups.

The Nashi

Figure 3.9: The Nashi Logo

Nashi (http://nashi.su) is short for *Molodezhnoye demokraticheskoye antifashistskoye dvizhenye* "*Nashi*" (translation, "Youth Democratic Anti-Fascist Movement "Ours!"). It was formed in 2005 to either counter the possibility of another youth revolt like the 2004 Orange Revolution in Ukraine or to counter a growing interest in Nazism in Russia. Funding for the group purportedly comes from Russian business owners however there has been widespread speculation that it receives government funding as well. That speculation has been strengthened in recent days by the Anna Bukovskaya story related below.

One of the most important supporters of Nashi is Vladislav Surkov, the First Deputy Chief of the Presidential Staff and, more importantly, a man who has the ear of Russian Prime Minister Vladmir Putin.

Surkov intends to use Nashi to enforce the Kremlin's will regarding Russian Internet (RUNET) communications; i.e., "Ensure the domination of pro-Kremlin views on the Internet" (The New Times Online in Russian 16 Feb 09). That's easier said then done, particularly since that effort was tried and abandoned about 10 years ago by RUNET co-founder Anton Nosek.

Surkov has a new plan which involves the enlistment of Russian youth organizations including Nashi and United Russia. He has organized a March 2009 conference with about 20 key people in the Russian blogging community as well as leaders of the aforementioned youth organizations to discuss an information strategy for the Internet:

"To every strategy there should be a response, or better still, two responses simultaneously."

Anna Bukovskaya is a Nashi member and St. Petersburg activist who was paid by the Kremlin to spy on opposition political youth movements.

In March, 2008, Nashi hackers were accused of orchestrating a series of Distributed Denial of Service (DdoS) attacks against the Russian newspaper Kommersant. A Nashi spokesperson denied that the group was involved.

In October, 2007, another Russian youth movement known as The Eurasian Movement of the Youth (ESM) launched a DDoS Web attack against the President of Ukraine's Web site, shutting it down for three days, and both Nashi and the ESM participated in protests against the Estonian embassy in Moscow in May, 2007.

Membership in Nashi has served the political aspirations of its leaders well. "Vasily Yakemenko, the group's founder, is now the head of the government's youth committee. Sergei Belokonev, the head of the "Nashi elections" division, accepted a post in Russia's Parliament." [10]

Sergei Markov, Estonia, and the Nashi

10 http://www.theotherrussia.org/2008/01/30/kremlin-slims-down-nashi-youth-movement/

On March 3, 2009, Sergei Markov, a State Duma Deputy and member of the Unified Russia party, participated in a panel discussion with Russian and U.S. experts including James Lewis of the Center for Strategic and International Studies, about Information Warfare in the 21st century. During that discussion, Markov stunned everyone present by announcing that it was his assistant who started the Estonia cyber attacks in 2007. The following quote comes from Radio Free Europe which broke the story on March 6, 2009 at its Web site:

"*Markov, a political analyst who has long been one of Vladimir Putin's glibbest defenders, went on to explain that this assistant happened to be in "one of the unrecognized republics" during the dispute with Estonia and had decided on his own that "something bad had to be done to these fascists." So he went ahead and launched a cyberwar.*

"Turns out it was purely a reaction from civil society," Markov reportedly said, adding ominously, "and, incidentally, such things will happen more and more."

This is most likely Konstantin Goloskov[11], a Commissar in Nashi, who acknowledged his involvement and those of his associates in the Estonia Cyber attacks.

Markov, a supporter of the Nashi youth movement, attended its second annual Innovation Forum on July 21, 2008; one day after the President of Georgia's web site came under a Distributed Denial of Service (DDoS) attack and 19 days before Russia's invasion of Georgia.

Russian Military Policy for Information Warfare

In a speech before the National Forum of Information Security "InfoForum-10" in Moscow on February 2008, Russian Deputy Chief of the General Staff Aleksandr Burutin spoke on the topic "Wars of the Future will be Information Wars"[12] wherein he discussed how the rise of technological development brings with it military applications:

"The uniqueness of information weapons lies in the fact that while developing their national information infrastructure, states create a material base for using information technologies for military purposes. The higher the scientific and technical potential, the wider the set of potential targets: telecommunication and communication systems, space vehicles, automated troop and weapons control systems, financial, bank and commercial activity, power supply systems and so on."

"For this purpose specialized subdivisions are being created in the armed forces and special services, conceptual documents regulating questions of preparation and conducting information operations are being developed, and appropriate training is being conducted."

Another piece of Russia's cyber strategy is spelled out in a multi-authored article in Moscow Military Thought[13] which addresses the strategic tactic of disguising acts of information warfare as criminal activities:

"In our view, isolating cyberterrorism and cybercrime from the general context of

---

11 http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?nclick_check=1

12 Speech by Aleksandr Burutin, Info-Forum 10, February, 2008

13Moscow Military Thought (English), "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect" 31 Mar 07

international information security is, in a sense, artificial and unsupported by any real objective necessity. This is because the effect of a "cybernetic" weapon does not depend on the motivation of a source of destructive impact, whereas it is primarily motivation that distinguishes acts of cyberterrorism, cybercrime, and military cyberattacks. The rest of their attributes may be absolutely similar. The practical part of the problem is that the target of a cyberattack, while in the process of repelling it, will not be informed about the motives guiding its source, and, accordingly, will be unable to qualify what is going on as a criminal, terrorist or military-political act. ***The more so that sources of cyberattacks can be easily given a legend as criminal or terrorist actions*** *(emphasis added)."*

Who Controls the Data Flow

Even with a bulletproofed network, it's important to remember that while the Kremlin provides open and global Internet access to its citizens, it also collects and controls all of the data originating within its borders.

A recent interview with the Editor-in-Chief of the Russian news Web site BFM.ru, Anton Nosik, was published in the Russian online newspaper The New Times. In it, Nosik spoke of SORM-2 (System of Operation Research Measures) which copies every byte of Internet traffic coming from Russian households and businesses and sends it to the Federal Security Service (FSB) via a Redundant Array of Inexpensive Disks (RAID).

Nosik also pointed out that the Kremlin either owns the pipes (Rostelekom, Transtelekom, and Elektrotelekom) or controls the licenses of every communications channel in Russia.

Credits and Acknowledgments

Project Grey Goose

Principal Investigator

Jeff Carr

Researchers

Billy Rios, Derek Plansky, Greg Walton, Matt Devost, Ned Moran, Rebecca Givner-Forbes, Shannon Silverstein

Reviewers

Derek Plansky, Kristan Wheaton

Acknowledgments

This project could not have occurred without the help of the highly talented and passionate Palantir Technologies crew and their CEO Dr. Alexander Karp. In addition, I'd like to thank the few researchers and reviewers who have opted to keep their participation confidential.