Politically Motivated Denial of Service Attacks

Jose NAZARIO
Arbor Networks, United States

Abstract. Cyberwarfare has been waged for well over a decade, utilizing methods such as website defacement, data leakage, and distributed denial of service attacks (DDoS). This paper focuses on the latter, attacks that are easily carried out and designed to overwhelm a victim's network with wasted traffic. The goal of a DDoS attack is to make the use of the network impossible for internal or external users. Through a brief examination of the history of these attacks, we find they previously were designed to inflict punitive damage on the victim but have since grown into sophisticated censorship tools. Our approach measure such attacks by looking at Internet backbone traffic, botnet activities, BGP routing changes, and community chatter about such attacks to provide a robust picture of politically targeted DDoS attacks. Our analysis indicates that most of the attackers are non-state actors but are able to fluidly utilize a growing botnet population to launch massive denial of service attacks. This finding has broad ramifications for the future of these attacks.

Keywords. DDoS, botnets, Estonia, Georgia, China, Russia

Introduction

Internet attacks take on many forms, including system compromises and information theft, as well as denial of service attacks designed to disrupt services. Motivations for cyber-attacks include frustration, fun, and extortion, especially against gambling and pornography sites. Anger and frustrations appears to be the major motivation in attacks against gaming sites and forums, where player-on-player attacks happen quite frequently. Politically targeted attacks are extremely rare in the sphere of daily attacks. The types of attacks launched depend on the attackers' skills and motivations.

A distributed denial of service (DDoS) attack is nothing more than a coordinated effort that instructs PCs to send a victim a flood of traffic designed to overwhelm their servers or consume their bandwidth [[1]]. Regardless of the attacker's underlying motivations, the attacks are designed to disrupt the normal flow of the site for internal or external users. The PCs used in the attacks can be the bots in a botnet or a zombie army, or it can be tools willingly installed on peoples' computers. A simple form of a DDoS attack is when individuals work together and to continuously reload a website in a browser such as Internet Explorer. In each case, the purpose is to aggregate the PCs' bandwidth together to overwhelm an adversary who is usually superior in their bandwidth resources, and to do so from a large enough number of locations to make source-based filtering unmanageable.

DDoS attacks are among the most visible and disruptive of cyber-attacks. When coupled to political motivations, they can be seen as an extension of politics in the 21st century, to borrow a phrase from von Clausewitz. Currently, researchers infer a political motivation for various attacks based on internal information, such as the nature of the victim and the attack commands seen. Investigators may also use external sources to validate this finding by looking at news reports and website conversations discussing diplomatic grievances and their redress through online attacks. In this context, cyber-attacks are sometimes referred to as "fifth generation warfare".

Arbor Networks' Peakflow products are used by many Internet service providers to detect and defend against DDoS attacks [[2]]. Independently run Peakflow deployments collect data on such attacks and provide a distillation of the events to the Arbor Networks ATLAS portal. Attack data is gathered in three different ways to provide a nearly complete picture.

The first data source is direct traffic measurement using Arbor Peakflow deployments around the world using data collected as part of the ATLAS project. Customers can share attack information with each other through the Fingerprint Sharing Alliance. Some of this data is made available in ATLAS and can be analyzed by network or country affected or launching the attack. Peakflow counts attacks based on the traffic types (e.g. TCP SYN, ICMP echo request) and destination networks for a time period using dynamically learned baselines or static thresholds. Therefore, Peakflow may register multiple concurrent attacks if they target the same destination but use different traffic, such as a simultaneous TCP SYN flood and ping flood.

The second way attacks are measured is to look at commands sent to botnets to launch attacks. Malicious software analysis can be used to discover botnets and infiltrate them by communicating with the botnet's command and control (C&C) server by mimicking legitimate bot clients, enabling a record of the botnet's activities for later analysis. This data is valuable to understand the attack's root origins for disruption but also for post-event analysis to understand the nature of the attackers. Most of the attacks tracked are against inconsequential targets, but sometimes they target victims such as financial firms, major e-commerce sites, or government assets.

The third form of continuous measurements is to look at border gateway protocol (BGP) routing data used to provide Internet backbone routing. Sometimes the paths may change during an attack as a direct result of the attack, such as BGP session drops during congestion, or through attempts to mitigate the attack. Changes to the BGP routes for a victim can indicate an attack.

This paper focuses on the confluence of DDoS attacks with political targets and political or ideological motivations. DDoS attacks are crippling because they are designed to make the networks they target unusable, either to inflict damage to the victim or, in the case of many recent events, to silence their opponents by making their resources inaccessible. This paper does not analyze information on attacks such as website defacements or compromises through malicious software that may be a part of these attacks.

1. Major Events in Political DDoS Attacks

DDoS attacks became widely popular in the late 1990s following the development of toolkits such as Tribe Flood Network and Trinoo [[1]]. These methods were quickly adapted for political targets. Major attacks from the past 10 years can be used to highlight changes and illustrate how sweeping this problem can be.

Very early events in this field include attacks on NATO computers in the former Yugoslavia during the campaigns in the late 1990's, and also the attacks from Chinese hackers on US military sites following the bombing of the Chinese embassy by a US plane in the former Yugoslavia during that NATO mission [[3]]. This list of attacks shows how many different regions are affected and how many different motivations exist for these attacks. It also shows how these attacks have evolved over time. This section also shows that such attacks didn't start with Estonia in May 2007 and didn't end with Georgia in the summer of 2008.

1.1. Hainan Spy Plane Incident

In April 2001, a US Navy spy plane was on a reconnaissance mission off the southern coast of China when multiple Chinese fighter planes intercepted it, and one of the planes clipped the US Navy plane, causing damage to both planes. The pilot of that Chinese fighter plane was lost after his plane broke up in mid air, and due to the damage it sustained during the accident, the US Navy plane had to make an emergency landing in Chinese territory on Hainan Island. The crew was held for several days before diplomatic efforts released them.

During this time, tensions between the US and China ran high. Among the events that occurred were multiple attacks, including DDoS attacks and probes on US military Internet sites. The Chinese hacking group "Honker Union" is believed to have been behind the attacks [[4]].

The attackers in this situation appeared to see these attacks as acts of patriotism. The public outrage was undeniable and bubbled over to Internet forums. Multiple groups and parties appeared to take part in these actions.

1.2. Estonia, 2007

Beginning in late April 2007, the European nation of Estonia was hit by a series of coordinated denial of service attacks. Ethnic Russians make up a significant percentage of Estonia's population, and by many accounts Estonians and the ethnic Russians co-existed peacefully [[5]]. As is commonly found throughout Russia and much of the former Soviet Union, Estonia has a statue of a Soviet soldier commemorating the end of World War II.

The statue has been a sore point in Estonian politics for many years and was moved in April 2007, leading to civil unrest within Estonia and complaints by the government in Russia [[14]]. Coinciding with the street protests, online DDoS attacks began to target Estonian government and private sector sites, including banking institutions and news sites.

The attacks seen in Estonia built up over the course of a few weeks and peaked on Victory Day, May 9. On this day, Peakflow systems around the world measured attacks lasting 10 hours each with a peak bandwidth utilization of 95 Mbps. This data comes from multiple Peakflow sensor sources that are aggregated into ATLAS via ISPs that provide transit for Estonian ISPs [[6]].

The attackers used multiple attack methods. They used Russian language forums and blogs to spread tools such as ping flood scripts and to coordinate their efforts, and they also recruited botnets into the effort. For example, they worked hard to take their collective tools, botnets, and activities and fire them at the same time (e.g. 11pm in Moscow).

The attacks in Estonia hit many parts of the infrastructure, including the websites for the prime minister, parliament, various ministries, and even government name and mail servers. News reports contained information about slowdowns with some banks and financial transactions. All of this is consistent with a nation that makes heavy use of the Internet for daily life suffering from systemic flooding.

Most of the attacks measured in ATLAS died out after Victory Day, although reports from first-hand accounts within Estonia indicate that they continued for several weeks.

1.3. China and CNN

In April 2008, the CNN news personality Jim Cafferty commented on air about the Chinese preparations for the Olympics in Beijing, China. Many Chinese found these remarks offensive, and this sentiment quickly brewed into anti-CNN hacking events.

A number of hacking groups activated and worked to coordinate their activities. The attacks included website defacements and many probes to try and disrupt the CNN.com website. Peakflow and ATLAS also monitored the flows for the site as well as for botnet attack activity [[7]].

During the investigations, a number of Windows tools developed to target CNN specifically were discovered, in addition to a few botnets that were targeting CNN more generally. The first tool was dubbed “Supper DDoS” is a simple flooder usable by an average computer user, with only an input for the victim’s address together with “Attack” and “Stop” buttons. This tool was distributed on Chinese language forums by an unknown number of authors.

Researchers also discovered a botnet apparently operated by “Ice Kernel”, using a bot dubbed “KernelBot”. KernelBot is a flexible DDoS attack system, supporting common attack types, as well as full control of the victim’s PC. Commands for this botnet targeting CNN’s website appeared during this event. Another tool released in late April 2008 to target CNN was a specialized version of the NetBot Attacker tool, a general purpose DDoS tool that is usually deployed on a victim’s PC using standard malware infection methods. This particular version of NetBot Attacker is hard coded to target CNN.com and provides the user with some basic control over their PC. This kit includes the flooding portion of the bot and the attacker’s UI for control, something not normally seen. Typically, the bots run without any UI for the victim.

1.4. Georgia and Russia

In July 2008, the website for Georgian President Mikheil Saakashvili was hit with a DDoS attack. In this case the botnet was based on a codebase that is only seen in Russian-language botnets. The command and control server for this botnet was located in a regional ISP, PaeTech, and had been under surveillance by ATLAS and other researchers for some time. This was the only attack launched by this botnet and lasted from July 18-20, 2008 [[9]].

These attacks were corroborated together with ShadowServer, a volunteer botnet monitoring team. We attempted to reach the site during the attack and found that the Georgian President's website was unable to load from a number of North American vantage points, consistent with a major attack [[10]]. When asked by the press, spokespeople for Saakashvili's office said that no such attacks had occurred, however.

A message was included in the attacks that read "win love in Russia", consistent with the ongoing tensions in the region. A few days before the DDoS attacks began in July 2008, the ITAR-TASS news agency from Moscow ran a story with the translated headline "Withdrawal of Georgian troops only way out of Abkhazia conflict - Medvedev". At the time, Russian president Dimitry Medvedev had been in power for a few months. There had been ongoing, minor skirmishes between Georgia and Russia over two regions within Georgia. South Ossetia and Abkhazia, two semi-autonomous areas have historically stronger ties to Moscow than does the rest of Georgia. These two regions had been seeking more independence and closer ties to Russia than Tbilisi would allow. The diplomatic flames going back and forth were substantial and included reports of gunfire between Georgian and Russian forces. After the shutdown of the PaeTech C&C server, the July 2008 attacks stopped [[9]].

A few weeks later, in early August, a large-scale shooting war between Georgia and Russia broke out with Russian tanks entering Georgian territory. Almost immediately, very substantial DDoS attacks began to flood into Georgia and were caused by multiple botnets and ping flood scripts. Targets included the Georgian president's site, various ministries, news agencies, and others [[6]]. Furthermore, ATLAS monitors recorded some attack commands into Russia at the same time, suggesting that someone - either Georgian or possibly a Georgian sympathizer - tried to counter attack.

Arbor Peakflow and ATLAS live traffic monitors on the Internet showed that the peak size of the attack was substantially larger than the attacks in Estonia the year before. The peak bandwidth recorded during the attacks was over 800 Mbps, and the attack were much more intense [[9]].

Key Georgian properties were quickly relocated to various countries with better defense capabilities. The president's website, for example, was moved to Atlanta Georgia and Tulip Networks. Other sites were moved to Estonia, which had experience and tools after the previous year's attacks [[11]].

This was the first time in nearly 10 years that a military conflict and a cyber conflict coincided, the most recent being attacks between Israel and Palestinian militias. These attacks on Georgian websites, especially after what happened in Estonia, have raised concerns around the world by governments concerned about an apparently growing trend of politically motivated attacks on government networks. This is discussed later in this paper.

1.4.1. Investigating Active Routing Attacks

One unique aspect of the attacks is that Georgia gets nearly all of its Internet access from two main countries: Russia and Turkey, with some additional connectivity from Europe. Analysis by Bill Woodcock at Packet Clearing House shows that nearly all of the major connectivity routes go through Turkey or 0Russia. This provides a high bandwidth connection for Russian bots, if they are located in Russia, to flood Georgia. Turk Telecom, the main upstream for Georgia in Turkey, is also a major source of bots.

Russian ISPs were accused during the fighting of filtering or blocking Georgian sites, which would have been possible for some routes but not all. In our analysis, we have found no data that suggests that Russian ISPs performed such filtering [[12]].

Routeviews monitors did see some unexplained BGP announcements via Turk Telecom but we attribute those to fighting the DDoS traffic or drops due to congestion, rather than active attempts to disrupt normal Georgian traffic.

Our measurements indicate that approximately 100 BGP updates per day occurred for Georgian prefixes immediately before the onset of ground fighting with Russia. After ground fighting began, less than 10 BGP updates per day were seen. The August cyber attacks began within 24 hours of Russian tanks rolling into Georgia, making the data hard to decipher conclusively. Any BGP disruptions could be due to fighting on the ground, DDoS attacks (and congestion leading to drops), or active disruptions by upstream peers.

1.5. Democratic Voice of Burma

Starting in the summer of 2008, DDoS attacks were launched against the Burmese dissident site the Democratic Voice of Burma (DVB) and its sister sites. Many of the attacks were website defacements and the attackers got in through a poorly configured and poorly secured site. ATLAS monitors recorded some packet flooding to the sites, as well [[14]].

Most of the attacks were apparent attempts to censor the sites and to thwart planned 8-8-2008 protests around the world. 20 years before on August 8, 1988, a significant protest occurred in Burma against the ruling Junta centered on the 8-8-88 date. The number 8 is very significant in Chinese and Burmese society, providing the protests on 8-8 are a powerful rallying point. The Burmese government is believed to be behind the attacks, although no such evidence has been provided.

1.6. Russian Elections, 2007

In the lead up to the Russian elections in late 2007, the website for the dissident politician and well-known chess Grand Master Gary Kasparov and his political party were both hit with substantial DDoS attacks. Kasparov has been a very vocal counterpoint to the powers in Moscow, specifically former Russian president Putin's administration, for many years. During the attacks, Kasparov's site was inaccessible, and so was his political party's [[13]].

The attack command activity traced back to botnets possibly run by Russian or pro-Russian hackers. The botnets have been used in the past to strike political targets among other targets.

1.7. Radio Free Europe/Radio Liberty

In April 2008, Radio Free Europe and Radio Liberty (RFE/RL) websites were hit with DDoS attacks [[15]]. It is thought that the attacks were in retribution for the reporting that RFE/RL made to cover the anniversary of the Chernobyl disaster.

The attacks started on April 26 and first targeted the website of RFE/RL's Belarus Service and quickly spread to other RFE/RL sites. Within a few hours, eight different RFE/RL websites serving Belarus, Kosovo, Azerbaijan, Tatar-Bashkir, Radio Farda, South Slavic, Russian, and Tajik-language listeners were all affected by such attacks.

The botnet behind the attacks was a Russian-language botnet that had been active in other politically motivated attacks in the recent past.

1.8. Ukraine Anti-NATO Protests

In March 2008, various Ukrainian newspaper sites were hit with DDoS attacks due to internal political tensions. The C&Cs behind the attacks were located in the Ukraine [[13]], although it is possible that outsiders or parties operating within the Ukraine used these botnets.

Also in 2008, the website for '5.ua', a news website for Ukraine, came under attack with the message "NATO go home" in the HTTP request as part of the flood. These attacks coincided with street protests against NATO expansion into the Ukraine. ATLAS monitoring tracked the C&C behind the attacks in this case to the hosts 'my-loads.info' and 'ultra-shop.biz', a BlackEnergy botnet controlled located (at the time) in China that uses multiple names for the same IP address [[14]].

1.9. Kazakhstan Government Criticism, MSK Forums

In early 2009, the forums for the Russian website MSK came under denial of service attacks. It is believed that these attacks were in retribution for the MSK site posting a PDF copy of a newspaper that was censored through the Kasakh government by pro-Moscow forces. The newspaper published an article written by the Kasakh president that was critical of the Russian government. When no other newspaper would carry the article, MSK offered to host it online and came under attack shortly thereafter [[16]].

The MSK site forums, in response to the DDoS attacks on site in conjunction with the Kazakhstan newspaper, hosted a poll on who people thought were responsible for the DDoS attacks. The poll, dated March 2, 2009, asked, "Who do you think organized DDoS-attack on forum.msk?" The results speak very significantly at the amount of distrust in the region:

Kremlin (185)

FSB (121)
Pro-Kremlin youth organizations (68)
MIA (4)
Administration of the Moscow region (3)
Administration Himok (11)
Communist Party (14)
Simple network hooligans (21)
Anti-power (23)
Neo Trotsky Fighters (22)
Other (15)

At this time it is still unclear what group launched the attacks, although ATLAS data indicates the attacks were lead by the botnets hosted on the sites 'candy-country.com', '22x2x2x22.com', and 'sexiland.ru'. All three of these are identified BlackEnergy-based botnet controllers.

1.10. Russian Opposition Websites

In late December 2008, a related attack struck the newspaper sites 'grani.ru', 'ikd.ru,' (which publishes news about demonstrations going on around Russia) and 'nazbol.ru' (the website of the banned National Bolshevik Party) [[17]]. All of these attacks are consistent with the basic premise that the opposition is routinely censored by DDoS. Data gathered by Arbor Networks indicates that some of the same botnets behind the MSK attacks (above) participated in these attacks.

1.11. Israel-Gaza/Hamas

During the Israeli-Hamas fighting in Gaza in January of 2009, multiple cyber attacks were launched both from Israeli hackers and Palestinian (and pro-Palestinian) attackers. The bulk of the attacks were website defacements, although we did see some DDoS attacks [[18]]. This is not the first time such cross-border cyber-attacks have occurred. In fact, the long-standing Israeli-Palestinian conflicts are the source of many such attacks and the cause for many website defacements on both sides of the conflict.

One of the tools distributed during these attacks was the "Patriot DDoS tool" from the website "Help Israel Win". The tool was loaded onto a number of websites and domains and was routinely shut down by various groups. It had also undergone a number of iterations to fix bugs and evade any antivirus detection. This is another example of the voluntary cyber attacks sometimes observed in the wild during diplomatic conflicts and shooting wars.

1.12. Kyrgyzstan, January 2009 – False Positive?

In mid-January 2009, reports started appearing that the small former Soviet Bloc nation of Kyrgyzstan was under a cyber attack. The data so far consists mainly of a few NetFlow logs and some web server logs of a few sites in Kyrgyzstan, but very little else. The main site reporting this attack, in a blog posting by Secure Works researcher Don Jackson, blamed the Russian government for the attacks [[19]]. This was followed up on the IntelFusion blog with some analysis and speculation as to the causes behind any such attacks [[20]].

In a posting on January 30, the author at IntelFusion made a case that the Kyrgyzstan government itself launched the attacks [[21]], basing this on some speculations that are consistent with the events in the region. While many researchers' attention in the United States was drawn to the threats at the time to close the Manas airbase (vital to NATO and US efforts in Afghanistan), events within Kyrgyzstan reveal another story. Instead, IntelFusion's analysis suggests that it was an effort to silence critics, since the Kyrgyzstan government is already very pro-Moscow and will happily comply with any offers that Moscow wields. Indeed, Moscow did openly offer Kyrgyzstan money if they closed the Manas air base.

ATLAS data was unable to discover independent data to suggest attacks came through the usual routes such as botnets and coordination via forums [[22]]. ATLAS data also did not show any Internet backbone flow data that suggests that the attacks crossed the normal channels.

1.13. Kommersant, 2008

On March 14, 2008, The Kommersant newspaper had complained to police and prosecutors about a massive hacker attack on its web site, which it suspected was orchestrated by the pro-Kremlin youth group Nashi. Nashi is one of several youth groups in Russia that has been involved in street protests and highly organized activities. They are also suspected in several online attacks including the ones against Kommersant. At the time, the Kommersant paper had published articles critical of Nashi and the government and came under fire, possibly in retaliation for this reporting. ATLAS data tracked several botnet C&C servers issuing commands to their BlackEnergy-based botnets to launch attacks against the Kommersant servers [[23]]. During the attacks, the Kommersant website was moved to the UK for improved hosting, although the attacks continued after the relocation.

1.14. Kazakh opposition websites allegedly under DDoS attacks

In February 2009, a Kazakh newspaper website came under attack for publishing material critical of the government in Astana [[24]]. The newspaper's site, 'zonakz.net', had published articles and recordings of several government officials purportedly committing crimes and acts of corruption. The site was first shut down in Kazakhstan and then moved overseas where it came under a DDoS attack.

In a report titled "The Contradictory State of Kazakhstan" that appeared on the site EurAsia.net, reporter Bruce Pannier wrote about the attacks [[25]]:

> Critics claim there is ample evidence of increased scrutiny of media outlets -- whether traditional or Internet-based.

> The owner and editor in chief of the independent weekly "Almaty-Info" is currently on trial for divulging state secrets in a November 2008 article, and is also being sued for defaming a businessman.
>
> Also this week, the head of the zonakz.net website complained that Kazakh law enforcement agencies were blocking access to the website, which is known for having carried material critical of, and at times potentially damaging to, the government.
>
> After a shutdown of zonakz.netℸs domestic servers that followed its posting of purported recordings and transcripts of senior Kazakh officialsℸ phone conversations, the site was registered abroad only to find access blocked by a new distributor-denial-of-service program known as DDOS-attack.

Additionally, various political parties have described DDoS attacks against news outlets in Kazakhstan as a means of silencing political opponents [[26]].

1.15. Iranian Elections, 2009

Beginning in mid-June, 2009, Arbor Networks began to see signs of Internet attack activity following the disputed presidential elections in Iran [[32]]. Street protests were organized using online forums and especially the Twitter service, and DDoS attacks against Iranian media and government sites began almost immediately. Most of the attacks used simple “page reboot” scripts, which are websites that construct a repeatedly reloading web page for an attacker that can be used by just browsing to the website. To maximize their effect, attackers coordinated the timing of their efforts using Twitter. However, attackers just as quickly suggested the attacks stop due to bandwidth consumption issues in light of the country’s Internet traffic filtering. It is unclear if the attacks had any significant impact on the target sites’ availability.

1.16. Coordinated South Korean-US Attacks, July 2009

Beginning on July 4 2009, a series of DDoS attacks began to strike first South Korean and then both South Korean and US government and commercial websites [[33]]. Sites targeted included the Korean Assembly, the US and South Korean presidents’ websites, the US State Department, the public websites for the US stock exchanges NYSE and NASDAQ, and popular sites in South Korea such as ‘naver.com’. Investigations revealed a botnet that was apparently built using a variant of the MyDoom worm from early 2004 together with rudimentary DDoS attacks such as HTTP request floods, UDP and ICMP floods. The attacks continued from July 4 until July 10, when the infected PCs were programmed to encrypt files and render themselves unbootable.

The targets, the US and South Korea, together with the timing between a North Korean missile test launch on July 4 and the 15th anniversary of North Korea’s Kim Il Sung’s death on July 8 lead some to suggest that North Korea was behind the attacks. To date, we have not seen any evidence of this. The real motivations for these attacks remains a mystery, but it is widely considered a political attack.

2. Attackers' Motivations

In many of the above cases, classic right-wing sentiments are apparently behind the attacks. In most cases, we appear to see attackers using DDoS attacks to express support of an official government position, either against external or internal foes. This is analogous to street protests organized by a political party to stifle opposition through a show of force. Increasingly, we are seeing DDoS attacks used to silence opposition sites, such as in the Kommersant attacks, the attacks on MSK, and the recent attacks in Kazakhstan. A notable exception is the Iranian attacks in June 2009, where anti-Iranian government protesters apparently organized a series of DDoS attacks to protest the election results. The July 2009 attacks on government sites in South Korea and the US may have been a protest, but it is unclear at this time.

In many of these situations, the attacker is able to employ classic guerilla warfare tactics to grow their size and power through the use of propaganda that appeals to an ethnic or national base. In these conflicts the attackers first answer the rally call at the beginning of diplomatic or military hostilities to begin their attacks. They then extend this force by providing easy to use tools through an extensive network of social forums and media including blogs, bulletin boards, and specialized information sites (often dubbed "inform" sites by the Russian hacker underground). Materials posted and re-posted here encourage new recruits to seek retribution against their enemies and join the fight. What starts as a small, core group is can grow into a massive force. Propaganda effects can be so strong, and long lasting, that Estonia still watches for renewed attacks every year on Victory Day. They have seen some attacks but nothing that rises to the level of the 2007 attacks.

By using cheaply and widely available technology, the enemy can leverage IP protocols, botnets, and applications as a force multiplier. That is to say that by using such tools attackers have a reach and power significantly beyond their normal capacity. The techniques to launch these attacks are commonly discussed; fortunately any advance in the sophistication of these techniques is much slower. However the attackers are able to codify their methods into easy to use tools that can be shared freely. There is an increasing emphasis on the ease of use for these tools by outsiders or non-technical parties. An example is the appearance of websites that use dynamic HTML methods to launch HTTP floods simply by loading a specific website. These tools were popular in the recent DDoS attacks on the Iranian government following a disputed national election, commonly using the website 'pagereboot.com'.

3. Attackers' Aims and Goals

Historically, these DDoS attacks have been aimed to cause the victim some punitive damage or register their dissent with the victim's actions. These are the apparent motivations in the attacks from Chinese hackers in retaliation for the embassy bombing in the late 1990s, and the 2007 Estonia attacks, the 2008 Georgia attacks, and the 2009 attacks on Iranian websites. We have seen changes with recent attack activity. Lately, the apparent goal of the attacks is to censor the opposition, either a dissident populace within the country, or dissidents outside the country, or an adversary elsewhere in the world. These are the kinds of attacks we see in the Russian elections of 2007 and subsequent attacks.

The Internet has become a major communication tool for news media, governments, political parties, the opposition and dissidents. Striking at their voice, their printing press, and their Internet channels makes perfect sense. This is apparently the main motivation of the attacks against the Democratic Voice of Burma, where a coordinated series of website hacks and defacements, as well as some DDoS attacks, were used to disrupt global protests against the ruling military in Myanmar.

The cheap and easy availability of the tools and weapons - botnet armies, hacker groups, and the like - have caused governments around the world to eye this approach as a means of silencing enemies. Even when there is no direct tie to the government, such actions can benefit the ruling party's aims. However, in every case we have been unable to conclusively say that the government has been behind the attacks. If governments use such tactics and tools in modern information warfare, then these attacks, by using independently operated botnets, make an excellent attack tool with plausible deniability for the attack director.

4. Attribution

Many have accused government actors or sponsored actors of carrying out these sorts of DDoS attacks. It is important to note that we cannot attribute any of these attacks to a specific group or agency with our data. We simply do not have the evidence to confirm it. All analysis of the data we have suggests non-state actors, however. This comes from observing the attack through three major means: direct data observations, community discussions encouraging and organizing the attacks, and analyzing the botnets and tools used to conduct the attacks.

In a LiveJournal account that we spotted we read representative during the denial of service attacks on Estonia in 2007 [[27]]. The post contains a simple DOS batch script that lists Estonian servers and IP addresses to be ping flooded and enters an infinite loop. The messages around the posting, and in similar forum postings, describe the Estonians as "fascists", "amateurs", and saying that they must be attacked.

Based on flow data from one of the attacks during the Estonian incident, we mapped where the traffic origins to geographic coordinates. The result quite clearly shows how widely distributed the attacks were sourced, namely from all over the world. In this case this particular attack was from a botnet. We do not think that this attack used source spoofing as all of the IP addresses in question mapped back to allocated netblocks and not unallocated IP address space, as is commonly seen when the attacks used spoofed or forged source IP addresses.

Some of the attacks were from far more discrete sources and likely came from the ping flood scripts that were in circulation. These were run by far fewer people and therefore had a smaller base of hosts to come from. We identified these attacks by their traffic type, ICMP echo request, and by the networks the traffic sources aggregated to, network allocations in Europe and Russia.

During the investigations into who launched the attacks, a 20-year-old Estonian student was charged and fined for his part in the attacks [[28]]. His fine was very small, only about $1650. Based on our data showing botnets, ping flood scripts, and the attackers' discussion, we conclude that it is unlikely that Dmitri Galushkevich is the only person responsible for the attacks, however.

Attribution continues to a significant challenge in this problem space when retaliatory measures are considered. In the July 2009 attacks on South Korean and US websites, the South Korean intelligence services stated through the press that they suspected North Korean hackers were behind the attacks. This was picked up and used as a call for retaliation on North Korea by a US lawmaker a few days later. Clearly, these kinds of attacks can spiral into significant diplomatic incidents if great care is not taken.

4.1. Role of Russian Youth Groups

An examination of recent attacks shows that in many cases there are political skirmishes with Russia at the core of the attacks. In these scenarios, one commonly fingered segment of the Russian hard-line community is political youth groups. These organizations are partially state-sponsored and used to hold pro-Kremlin rallies, but have also been accused in various physical attacks over the years. As noted earlier in this paper, they have been accused of the Kommersant attacks, among others. The Russian youth group Nashi claimed responsibility for the Estonian attacks of May 2007 in a news report from mid-2007 [[29]].

Claims about who was behind the Estonia attacks in 2007 were renewed during a 2009 videoconference between Moscow and Washington, and was described in a news report [[30]]. The participants talked about the methods and technologies of information warfare in the 21st century, based on examples of the "Inform Campaign" model that accompanied the military and economic conflicts in recent years (the five-day war in Georgia in August 2008, Israeli military operation in Gaza in early 2009, the gas delivery conflict between Ukraine and Russia, etc.). "Inform campaigns" are routinely used to coordinate such attacks and are widely thought to be government assisted if not outright sponsored.

> Sergei Markov, a State Duma Deputy from the pro-Kremlin Unified Russia, claimed in a March 3, 2009, discussion that his assistant was responsible for the attacks. Said Marvov, "They did not know what to do next. There were feasts, to whom they could not reach. They call to me and say: Sergey, what to do now? Here, we have disabled Estonian sites. I do not know what to do! I say: So what? Let's let this information that is learned." Markov reportedly said ominously, "and, incidentally, such things will happen more and more." Nashi, the Russian youth group, renewed their claim of a role in the attacks as well.
>
> "In this way, the boys expressed their protest against the policy of the state of fascism carried out by the leadership of the Republic of Estonia", - quoted Commissioner movement Webplanet.ru.

4.2. Hainan Island incident

The Chinese hacker group "Honker Union" took credit for the 2001 hacking incidents in relation to the Hainan Island incident, including the DDoS attacks and the probes on US government computers. This claim is widely believed to be accurate [[4]]. Honker Union is now merged with another Chinese hacking group. Such groups appear to operate openly in China and can sometimes organize such political attacks.

4.3. Botnets behind Georgia-Russia Cyber War

Many of the botnets we listed above, and more, actively participated in attacks against Georgian websites. We recorded well known as well as new BlackEnergy-based botnets striking Georgian targets, most launching generic flood attacks. We identified only a few botnets launching attacks into Russia.

One of the sites set up to coordinate cyber-attacks on Georgia as well as to share ongoing information about the war was the site 'OSInform.RU'. The website contained imagery of death and skulls, and also claims of genocide, material seen consistently in sites set up by Russian hackers detailing attacks on Georgian sites. Multiple blogs begin sharing a simple ping flood scripts targeted Georgian sites, a very similar scripts to the ones seen in Estonia.

A "Stop Georgia" site was set up to coordinate cyber attacks on Georgian web properties. Self appointed representatives of the Russian hacker underground claimed to be behind the site, and it was hosted in multiple locations (via mirroring). The translated comments on the site were:

> *Our response to aggression by Georgia*
>
> *We - the representatives of Russian hacker underground 0 will not tolerate provocation by the Georgian in all its manifestations. We want to live in a free world and exist free from aggression and lies space. We do not need the guidance from the authorities or others, but act according to their convictions based on patriotism, conscience and belief in the virtue of justice. You can call us criminals and cyber-terrorists, continuing with war and killing people. But we will fight and unacceptable aggression against Russia in cyberspace.*
>
> *We demand the cessation of attacks on information and government resources on RUNET, as well as appeal to all media and journalists with a request to cover events objectively. Until the situation has changed, we will impede the dissemination of false information by the Georgian government and information resources. We did not launch an information war, we are not responsible for its consequences.*
>
> *We call for the assistance of all who care about the lies of Georgian political sites, everyone who is able to inhibit the spread of false information.*
>
> *StopGeorgia.ru*
>
> *P.S. There is one formal mirror project - www.stopgeorgia.info. All other resources have nothing to do with the movement StopGeorgia.ru.*

The "Stop Georgia" site also contains a list of sites belonging to Georgia government agencies or Georgian properties abroad. The exhaustive list provides victim IP addresses for targeting and shows their status.

Russian attackers had significant coordination to their activities that was quickly set up, many within a day of the ground offensive beginning. We are not clear on the timelines of the buildup of border tensions or any propaganda campaigns by Russia against Georgia, although a significant lead up to the shooting war could have allowed attackers to establish their operations in time for the ground hostilities.

5. Official Responses Since Estonia

The spring 2007 events in Estonia have served as a clear wake up call to governments around the world about the power of cyber attacks and the damage they can inflict. The events in the summer of 2008 against Georgia were a forceful reminder of the attacks and added great urgency to this analysis. Many governments are reviewing their own vulnerability to DDoS attacks or more common infiltrations. A small handful of nations are investigating active cyber attack programs of their own.

5.1. Defensive Responsibilities

Especially since May 2007, but even more after the 2008 Georgia attacks, governments and groups around the world are worried about being a victim of a cyber attack. NATO, the EU, and other groups have been investigating their role in responding and their responsibilities and obligations. To date neither the EU nor NATO has articulated clear strategies for countering such attacks on member states.

The IMPACT alliance (http://www.impact-alliance.org/) has been founded in Malaysia to combat cyber terrorism and has been working to become a UN of cyber security, in part with the help of the ITU.

5.2. Role of Attribution in Response

Attribution is a key aspect for any large-scale response including retribution attacks or seeking redress via the international community, such as in the UN or via diplomatic channels. These kinds of attacks give a nation-state clear plausible deniability if they are actively sponsored, and an even bolder claim if these are simply run out of the civilian populace but tolerated or even tacitly controlled.

Some have claimed that the use of subtle language cues is commonly employed by the Chinese to direct such attacks. Phrases that seem innocent can have a sweeping impact on how the populace responds, either in street protests or in online attacks. If this is the case then we should expect that these kinds of attacks would continue and become a tool for managing opposition or foes in the 21st century. Their impact - bandwidth, durations, victims - is likely to grow and their frequency, scale, and the number of origins is likely to grow as well, as we have seen in the past several years.

6. Recommendations

Recent history has shown that packet flooding attacks are increasingly a favorite weapon of politically motivated attackers regardless of their geographic region. These attacks threaten communication mechanisms, the integrity of elections, and the freedom of an independent press, the activities of dissident groups and politicians, and may, in the future, grow in sophistication and disrupt normal daily life. In this time we have seen investigations and defense measures spawned from independent parties, the commercial sector, and the government sector through mostly ad-hoc means. While this has been marginally effective so far, this has quickly become an untenable situation.

A number of recommendations follow based on the author's experience in a number of the conflicts described above.

6.1. Broad Defensive Contributions Must be Possible

If we are to successfully defend national infrastructure against the sorts of attacks that affected Estonia and Georgia then we must be open to all forms of assistance. In both cases the public were firmly on the side of the victim (Estonia, Georgia), a sentiment that must be harnessed more effectively in the future. This must be turned into *Schwerpunkt* - a unity of purpose and goals - which will make us effective in our mission of defending the Internet.

Commercial tools from various vendors, including the author's employer, exist to detect and filter DDoS attack traffic and have been deployed to help thwart some of the attacks reviewed above. The technology in these tools is commonly available and the only barrier to their deployment is budget. However, as a total solution to the political DDoS problem this is insufficient from a cost or management perspective. We must think about how to utilize new methods to defend critical and civilian infrastructure as well as government infrastructure.

The enemy, attackers, uses public sentiment on his side to grow an organic legion of supporters to aid in their cause. Their aim is more amorphous than the defenders' role but the principle applies: by utilizing propaganda campaigns and nationalist and ethnic sentiment, he grows his army of volunteers. This is exactly analogous to the enemy in guerilla warfare.

Defenders do not use organic support for their mission of stopping these attacks, however. Outside support has been used to some extend in the recent past, with Tulip Networks in Atlanta, Georgia, in the United States providing bandwidth and connectivity for some of the Georgian infrastructure under attack. This was made possible through a direct, personal friendship that enabled this help. This kind of assistance is rare and no formal agreements are in place, leaving victims at risk.

For the victims, successes in defending an online presence usually come when a group or an individual acts on his or her own with the best interests in mind. Many more individuals or groups who could help are usually blocked from providing assistance. More outsiders are willing to help in these cases through meaningful ways, and we must enable them to provide aid if we are to defend these networks and this infrastructure. One challenge that will have to be addressed is to discover which offers are credible or worthy.

However, a network of professionals to defend against these sorts of attacks exists in the commercial Internet service provide realm.

Governments must be open to assistance from the private, commercial sector for dedicated DDoS-resilient hosting for public facing Internet properties. At this time the targets of these attacks mainly consist of information-only sites, but in the future will surely include key infrastructure equipment such as VoIP exchange points, DNS servers, and email systems which, if targeted, could impact the ability of a government to communicate internally. Governments and other likely political targets such as newspapers must identify how they can migrate their infrastructure to a third-party's systems to ensure continuity.

Furthermore, governments and targets must be trained and willing to accept a rapid deployment of commercial tools to defend against these kinds of attacks. All members of the government's information technology staff should be able to receive an offer of help and determine its credibility, and route that offer to the appropriate internal party for follow up. We have seen this work in limited cases in the past but too often we find that government victims in these attacks do not know how to accept an offer of assistance in a timely fashion.

6.2. Improved Efficiency in the Decision Making Process

A review of the OODA loop, or the Boyd cycle, provides ample areas to review and seek improvement in our current posture [[31]]. The cycle is built of four core steps that provide feedback to each other: observe, orient, device, act. The faster and more accurately one side can complete the loop - and begin the cycle again - the bigger an advantage he has.

Our observation points are currently piecemeal and hampered by competing business interests. This is nothing new, but it means we have a poor foundation on which to base our decisions. Because we lack a complete overview of Internet activity about the origins of attacks and how we may stop them, we often waste valuable time defending against attacks when we could stop them at their root. Information collection, sharing, and recall are woefully ignored and falling behind.

As a community of defenders we are usually able to orient at the broader goal - defend a specific country's assets (e.g. Estonia), identify the attackers behind it - but our more specific tactics to achieve that goal are unfocused and lacking. We fail to communicate what we need, what we find, and what the next steps are.

Our decision making process is often mired in consensus building and dogged by second-guessing. We are ineffective in many cases because we fail to make decisions for fear of making the wrong one. Committees with the wrong stakeholders and people who have no value to the process hijack and derail the process.

Finally, our actions are bound by laws and jurisdictions but also by seeking the permission of too many parties. In short, we move too slowly, too blindly, and too ineffectively, if we move at all. We are not consistently effective.

Moving forward, governments and coordination centers must be given the authority to act without requiring a consensus of all parties but rather act quickly in the best interests of the group. This should be treated as an authority akin to a military command authority and should coordinate public-sector, private-sector, and military efforts at combating attacks.

Careful balance must be taken to work with carriers, for example, to avoid disruptions to the infrastructure, a key facet to ensuring the carriers will accept outside leadership in such events.

7. Conclusions

DDoS attacks provide a simple, easily available mechanism to disrupt the Internet presence of a group or a small nation. Previously, they have been confined to retaliatory attacks seeking punitive damage to the victim, but in recent years the role of the Internet in publishing newspapers or organizing dissident efforts has grown. The growing importance of the Internet to potential victims has not escaped cyberwar practitioners. DDoS attacks will continue as a tool of censorship as long as the Internet remains a communications medium.

Cyber-warfare takes on different forms in different areas of the world. Political targets and motivations in DDoS attacks are most popular in Russia and the region, less so in China, Asia and the Middle East. China favors more surgical, infiltration events for serious cyber warfare. We have seen an explosion of DDoS tools from Chinese hackers, although most of their targets are commercial sites located in China, but many are in Korea or Japan. These sites are the targets of bullying or extortion attacks that do not yet rise to the level of political warfare. Burma benefits from website defacements and destruction. Israel and Palestine often use website defacements to challenge each other. At this time we expect to see DDoS attacks continue to be a political weapon in the Russian power sphere, particularly for former Soviet bloc nations.

These attacks will continue to provide the nation-state benefits from their actions as well as plausible deniability should they actively engage in such actions. Because of this we expect their frequency to grow in the Russian region, together with their sophistication as victims begin to develop improved defenses. Furthermore we anticipate that other nations may begin using DDoS attacks as a simple, blunt force political weapon to silence critics or opponents.

Much of the theory of cyber-warfare remains to be written, but may borrow from other warfare theories. Specifically theories on guerilla and asymmetric warfare need to be reviewed to understand the enemy's tools and tactics, as well as to understand responses. While governments and private industry control the communication's fabric, they have yet been unable to muster a unified, consistent defense. Instead, defenses have largely been ad-hoc and at the mercy of generous outsiders. Responses must be cohesive if not unified in order to be consistent, an approach that would be well informed with an understanding of defense tactics learned from studying theories of cyber-warfare.

References

[1] Mirkovic, J. and Reiher, P., A taxonomy of DDoS attack and DDoS defense mechanisms, in *ACM SIGCOMM Computer Communication Review,* 2004.

[2] Arbor Networks Website, http://www.arbornetworks.com/en/products.html.

[3] ACTIVISM, HACKTIVISM, AND CYBERTERRORISM: THE INTERNET AS A TOOL FOR INFLUENCING, Denning, D.E., in *Networks and netwars: The future of terror, crime, and militancy*, 2001.

[4] Cyber Protests: The Threat to the U.S. Information Infrastructure, National Infrastructure Protection Center, 2001. Available online at http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.pdf.

[5] US State Department Website. Available online at http://www.state.gov/r/pa/ei/bgn/5377.htm.

[6] Estonian DDoS Attacks - A summary to date, by Jose Nazario, on Security To The Core weblog, May 17, 2007. Available online at http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

[7] CNN Attack Summary, by Jose Nazario, on Security To The Core weblog, April 21, 2008. Avaiable online at http://asert.arbornetworks.com/2008/04/cnn-attack-summary/.

[8] Cyber Attacks Against Georgia: Legal Lessons Identified, by Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, 2008.

[9] Georgia On My Mind – Political DDoS, by Jose Nazario, on Security To The Core weblog, July 20, 2008. Available online at http://asert.arbornetworks.com/2008/07/georgia-on-my-mind-political-ddos/.

[10] The Website for the President of Georgia Under Attack - Politically Motivated? by Steven Adair, in Shadowserver Foundation Calendar, July 20, 2008. Available online at http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720.

[11] Estonia hosts Georgian Web sites to halt hackers, on FoxNews.com, August 26, 2008. Available online at http://www.foxnews.com/wires/2008Aug26/0,4670,EstoniaGeorgiaHaltingHackers,00.html.

[12] An In-Depth Look at the Georgia-Russia Cyber Conflict of 2008, Jose Nazario and Andre M. DiMino, at the Botnet Task Force meeting, October 2008.

[13] Political DDoS? Ukraine, Kasparov, by Jose Nazario, on Security To The Core weblog, December 13, 2007. Available online at http://asert.arbornetworks.com/2007/12/political-ddos-ukraine-kasparov/.

[14] Political DDoS: Estonia and Beyond, Jose Nazario, in a presentation give at Usenix Security, 2008. Available online at http://www.usenix.org/events/sec08/tech/slides/nazario-slides.pdf.

[15] Radio Free Europe DDoS, by Jose Nazario, on Security To The Core weblog, April 29, 2008. Available online at http://asert.arbornetworks.com/2008/04/radio-free-europe-ddos/.

[16] MSK Forum, February 28, 2009, available online at http://forum.msk.ru/notice/.

[17] Russian Opposition Websites Shut Down By Attacks, December 25, 2008, on The Other Russia. Available online at http://www.theotherrussia.org/2008/12/25/russian-opposition-websites-shut-down-by-attacks/.

[18] The Effects of War: Gaza and Israel, by Jose Nazario, on Security To The Core weblog, January 5, 2009. Available online at http://asert.arbornetworks.com/2009/01/the-effects-of-war-gaza-and-israel/.

[19] Kyrgyzstan Under DDoS Attack From Russia, by Don Jackson, on SecureWorks Research Blog, January 28, 2009. Available online at http://www.secureworks.com/research/blog/in-dex.php/2009/01/28/kyrgyzstan-under-ddos-attack-from-russia/.

[20] The Kyrgyzstan DDoS Attacks of January, 2009: Assessment and Analysis, Jeff Carr, jart Armin and Greg Walton, on IntelFusion blog. Available online at http://intelfusion.net/wordpress/?p=516.

[21] Why I believe that the Kyrgyzstan Government hired Russian hackers to launch a DDOS attack against itself, by Jeff Carr, on IntelFusion blog. Available online at http://intelfusion.net/wordpress/?p=520.

[22] Kyrgyzstan DDoS Attacks, by Jose Nazario, on Security To The Core weblog, February 2, 2009. Available online at http://asert.arbornetworks.com/2009/02/kyrgyzstan-ddos-attacks/.

[23] Russian DDoS Attacks: Kommersant, by Jose Nazario, on Security To The Core weblog, March 19, 2008. Available online at http://asert.arbornetworks.com/2008/03/russian-ddos-attacks-kommersant/.

[24] Quick Notes on Cyber Warfare News, by Jose Nazario, on Security To The Core weblog, February 19, 2009. Available online at http://asert.arbornetworks.com/2009/02/quick-notes-on-cyber-warfare-news/.

[25] THE CONTRADICTORY STATE OF KAZAKHSTAN, by Bruce Pannier, in EURASIA INSIGHT, March 6, 2009. Available online at http://www.eurasianet.org/departments/insightb/articles/pp030609d.shtml.

[26] Kazakhstan: Five political parties report about the information terrorists to the public prosecution office, February 25, 2009, on the website Ferghana.ru. Avalable online at http://enews.ferghana.ru/news.php?id=1024.

[27] "Load quickly on chuhonofilam", in a posting on a LiveJournal blog by w8kl8dlaka. Available online at http://w8lk8dlaka.livejournal.com/52383.html.

[28] Student fined for attack against Estonian Web site, Jeremy Kirk, InfoWorld, January 24, 2008.

[29] Nashi, Russia's new militant nationalist movement, Rediff India Abroad, May 21, 2007. Available online at http://www.rediff.com/news/2007/may/21nashi.htm.

[30] Behind the Estonia Cyberattacks, Radio Free Europe/Radio Liberty, March 6, 2009.

[31] Osinga, Frans. Science, Strategy and War: The Strategic Theory of John Boyd. Abingdon, UK: Routledge, 2007.

[32] Iran DDoS Activity: Chatter, Tools and Traffic Rates, by Jose Nazario, on the Security to the Core weblog, June 19, 2009. Available online at http://asert.arbornetworks.com/2009/06/iran-ddos-activity-chatter-tools-and-traffic-rates/.

[33] Korean/U.S. DDoS Attacks – Perplexing, Disruptive, and Destructive, by Steven Adair, on the Shadow Server Foundation Calendar blog on July 10, 2009. Available online at http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090710.