

SECURITY RESPONSE

The continued rise of DDoS attacks

Candid Wueest

Version 1.0 – October 21, 2014, 13:00 GMT

“ *Attackers can rent DDoS attack services for as little as \$5...* ”

CONTENTS

Overview	3
Evolution of DDoS attacks	6
Current DDoS Trends	6
DoS malware trends.....	10
Linux server malware	11
Dirtjumper	11
DDoS as a service trends	12
Targets.....	15
Motivation	16
Extortion and Profit	16
Diversion.....	16
Hacktivism.....	16
Disputes.....	17
Collateral damage	17
Examples of recent DDoS attacks	19
Attacks against gaming sites	19
Attack against bitcoin traders.....	20
Hacktivist attacks.....	20
Impacts of DDoS attacks	20
Mitigation	22
Be prepared	22
Best practices.....	22
Blacklist sources	23
Over-provisioning bandwidth	23
Insurance	23
Don't become the source	23
Stop spoofing	23
Conclusion.....	25
Appendix	27
Types of DDoS attacks	27
Resources.....	31

OVERVIEW

Distributed denial-of-service (DDoS) attacks, as the name implies, attempt to deny a service to legitimate users by overwhelming the target with activity. The most common method is a network traffic flood DDoS attack against Web servers, where distributed means that multiple sources attack the same target at the same time. These attacks are often conducted through botnets.

Such DDoS attacks have grown larger year over year. In 2013, the largest attack volume peaked at 300 Gbps. So far in 2014, we have already seen one attack with up to 400 Gbps in attack volume. In recent times, DDoS attacks have become shorter in duration, often lasting only a few hours or even just minutes. According to [Akamai](#), the average attack lasts 17 hours. These burst attacks can be devastating nonetheless, as most companies are affected by even a few hours of downtime and many business are not prepared. In addition to the reduced duration, the attacks are getting more sophisticated and varying the methods used, making them harder to mitigate.

In 2014, amplification and reflection attacks were still the most popular choice for the attacker. This method multiplies the attack traffic, making it easier for attackers to reach a high volume of above 100 Gbps even with a small botnet. From January to August 2014, DNS amplification attacks grew by 183 percent. The use of the network time protocol (NTP) amplification method has increased by a factor of 275 from January to July, but is now declining again. The use of compromised, high bandwidth servers with attack scripts has become a noticeable trend.

According to a survey by [Neustar](#), 60 percent of companies were impacted by a DDoS attack in 2013 and 87 percent were hit more than once. The most common affected sectors are the gaming, media, and software industries. The purpose of most attacks is to disrupt, not to destroy. In contrast to targeted attacks, DDoS attacks will not lead to data breaches, but on the other hand, they are a lot easier to conduct. Attackers can rent DDoS attack services for as little as \$5, letting them conduct a few minutes-worth of DDoS attacks against any chosen target.

Hackivist groups often use flooding attacks as a political protest and generate media attention. One example of a hackivist group is the al-Qassam Cyber Fighters, which attacked US financial institutions. DDoS attacks are also used by cybercriminals to extort money from online services, by gamers to settle disputes, or as diversions during targeted attacks. For the first half of 2014, most DDoS attack traffic originated in India, followed by the United States. One reason for this might be the large number of badly configured servers that can be misused for amplification attacks and the high number of bots.

DDoS attacks often cause collateral damage to companies close to the real target. Once the bandwidth fills up, any site hosted by the same provider may not be accessible through the Internet. As a result, these sites might face downtime even if they were not directly targeted.

DDoS attacks are not a new concept, but they have been proven to work and can be devastating for companies. There is no way to prevent a DDoS attack, but there are some ways to mitigate its impact to the business. The most important step is to be prepared and have an action plan ready.

EVOLUTION OF DDOS ATTACKS

“ Most attackers have moved to using HTTP-controlled command servers or have even started using peer-to-peer (P2P) networks... ”

Evolution of DDoS attacks

A few years ago, DDoS attacks were mostly conducted using large botnets to directly flood the target with traffic. Now, we often see the use of amplification attacks through open third-party services or botnets of hijacked servers, which have more bandwidth than compromised computers. But common botnets still play an important role in DDoS attacks. In the past, many DDoS bots were controlled through Internet Relay Chat (IRC) channels. In recent years, most attackers have moved to using HTTP-controlled command servers or have even started using peer-to-peer (P2P) networks to make their attack infrastructure more resilient against takedowns.

In order to make it harder for static signatures to be applied for filtering traffic, modern attack scripts randomize every possible part of their traffic. For example, in application layer attacks, HTTP requests' user agent string is varied and HTTP GET requests call on random Web pages. Newer versions of these attacks also allow the attacker to use specific bots in a certain region to perform the attacks. If the bots are in the same geolocation as the target, it makes it even harder to filter the malicious traffic early in the network chain, as one DDoS mitigation tactic for local businesses is to simply drop every connection from foreign countries.

Some attackers have started to [impersonate Google Bots](#) with their requests as they believe that the target will not filter these bots out. Of course, smart prevention systems are easily able to identify the fake bots by verifying the source IP address and the frequency of their visits. As a result, this is not a tactic to be worried about, but it highlights how attackers are experimenting with new ideas to bypass DDoS protection mechanisms. Sometimes, even the servers of DDoS [protection services are hijacked](#) for attacks.

Instead of attacking the targets directly, attackers have been increasingly targeting connected resources. The most obvious example is to attack the domain name system (DNS) server responsible for resolving the target's domain. If all name servers are not responding over a long time, then users will not be able to reach the company's website, as they don't know the site's IP address. A prime example of this was the attack [against the Chinese registry](#), which pulled many .cn websites offline for several hours. But some attackers have also started to attack the hardware along the path, such as proxies or gateway solutions in front of Web servers. Attackers are getting smarter at finding the weakest link and attacking this possibly unprotected resource instead. They can even breach the physical world as well. In August 2014, attackers [cut the fiber optic cables](#) of a network provider in Germany, pushing 160,000 users offline for multiple hours.

Another DDoS attack evolution seen in recent years is how mobile malware has started to include DDoS functionality as well. Of course, unless the mobile devices have 4G connectivity, the bandwidth resources are quite limited. But even if the devices don't have 4G, they can still be used to perform application-layer attacks as, for example, the [Dendroid](#) toolkit for Android malware demonstrates. In addition, there are standalone DoS tools available for smartphones, like [Android.Loicdos](#)—a mobile version of Low Orbit Ion Canon (LOIC)—and Slowloris. In these cases, the user manually installs and deliberately executes the stress test tools. Attackers also have gained an increased interest in the reverse attack, where the victim's phone is flooded with inbound telephone calls. This type of attack rose in popularity after a presentation on the technique at a recent security conference.

In general, we see that attackers are trying to leverage every angle to attack their target from multiple sides from various devices. The bandwidth at their disposal has grown over the years and is combined with customized application-level attacks against Web applications. DDoS attacks have long since moved from a single method used by frustrated "script kiddies" to an attack technique used by various professional groups.

Current DDoS Trends

The most obvious trend seen at the end of 2013 and in 2014 was the increased use of amplification attacks. Such attacks allow the adversary to increase their attack power by reflecting spoofed traffic onto third-party sites. Symantec's Global Intelligence Network (GIN) recorded an increase of 183 percent in DNS amplification attacks from January to August 2014. Meanwhile, generic Internet control message protocol (ICMP) flood attacks increased by 293 percent by the end of March, but dropped to 75 percent of the total amount of attacks observed in January by August 2014. It is not uncommon to see fluctuations of different DDoS methods being used over time, as there are many factors at work that influence this. Different attack groups have different

preferences for their DDoS campaigns, for example ICMP flood attacks were one of the main methods used by the Darkness/Optima botnet. Some methods, particularly amplification attacks, may no longer work that well. This could happen if the media extensively covers a high profile attack, which often results in more people patching and protecting their open servers. In addition, botnets that were used to perform previous attacks may get taken down or get upgraded to newer versions which provide new functionality. Last but not least, DDoS attack trends also depend on the monitored network space of the Internet.

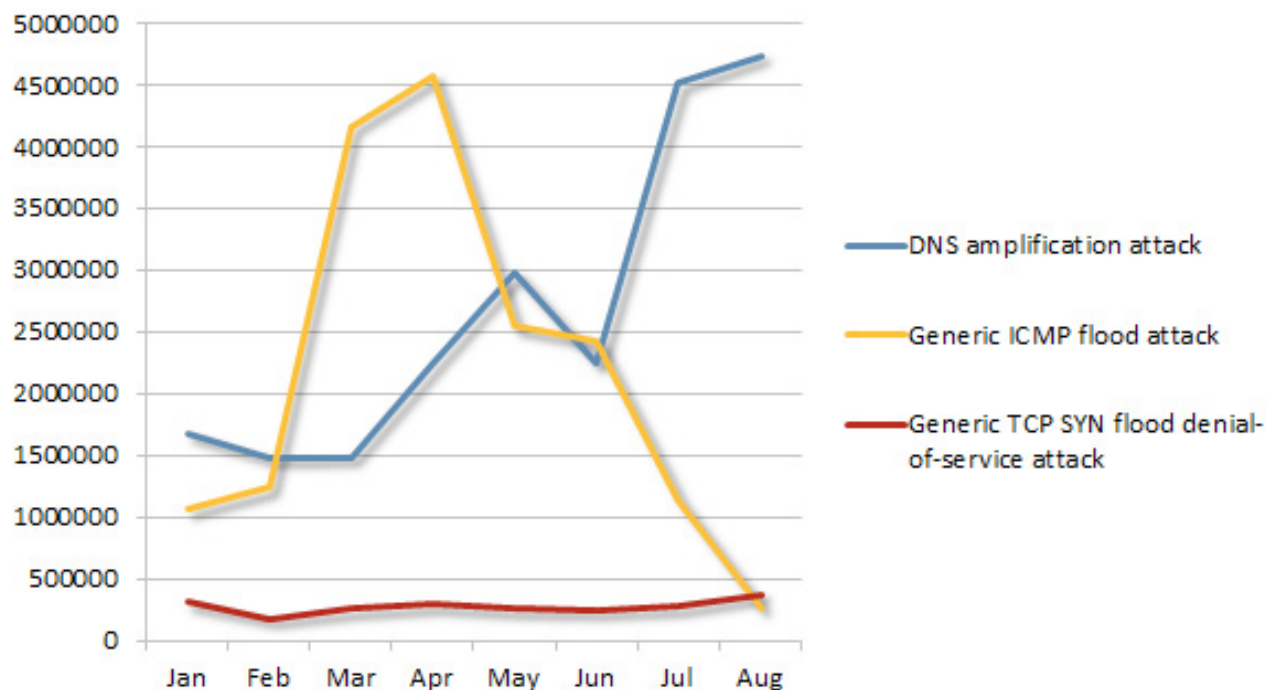


Figure 1. DDoS attack traffic seen by Symantec's Global Intelligence Network

At the beginning of 2014 the largest attacks used user datagram protocol (UDP) floods through NTP amplification attacks. NTP amplification attacks have increased by a factor of 275 from January till July, but have been declining since. This may be a result of multiple initiatives aimed at reducing the number of public amplifier servers and upgrading vulnerable instances. We have noticed a few simple network management protocol (SNMP) reflection attack attempts, which could be an indication that the attackers are trying to find a replacement for NTP amplification attacks.

Prolexic reports a 14 percent decrease of average attack bandwidth being used, dropping to 7.76 Gbps for the second quarter of 2014 [1]. However, Verisign noted a 216 percent increase in attack bandwidth, reaching an average of 12.4 Gbps in DDoS attack volume [2]. However, both sources agree that the level of attacks is high and that they are getting stronger. Sixty-five percent of the attacks were larger than one Gbps and 16 percent were larger than ten Gbps. This is a substantial amount of traffic and is sufficient to knock small and medium sized companies from the Internet.

Application-level attacks, which target specific applications and misuse their logic, were down to ten percent of DDoS attacks in the second quarter from 30 percent in the first quarter of 2014 [2]. This is a remarkable drop, but these types of attacks remain important, as they are difficult to filter and do not need large bandwidth to succeed. It might be that, due to the popularity of DNS and NTP amplification attacks, the focus was temporarily drawn from application-level attacks, since the attackers already succeed in their goal using these other types of attacks.

In addition, application-level attacks need some knowledge about the target application and often require some manual fine-tuning, which not all attackers can achieve. Therefore, these attacks are less commonly found in off-the-shelf malware.

Prolexic reported that 69 percent of application-level attacks targeted unencrypted HTTP GET requests in the second quarter [1]. But we have noticed an increase in the use of SSL traffic in these attacks. Along with the extra load that decrypting SSL traffic generates on the server, using SSL traffic can bypass some pre-filtering measures, as network devices will not be able to analyze the application-layer content without breaking up the encryption.

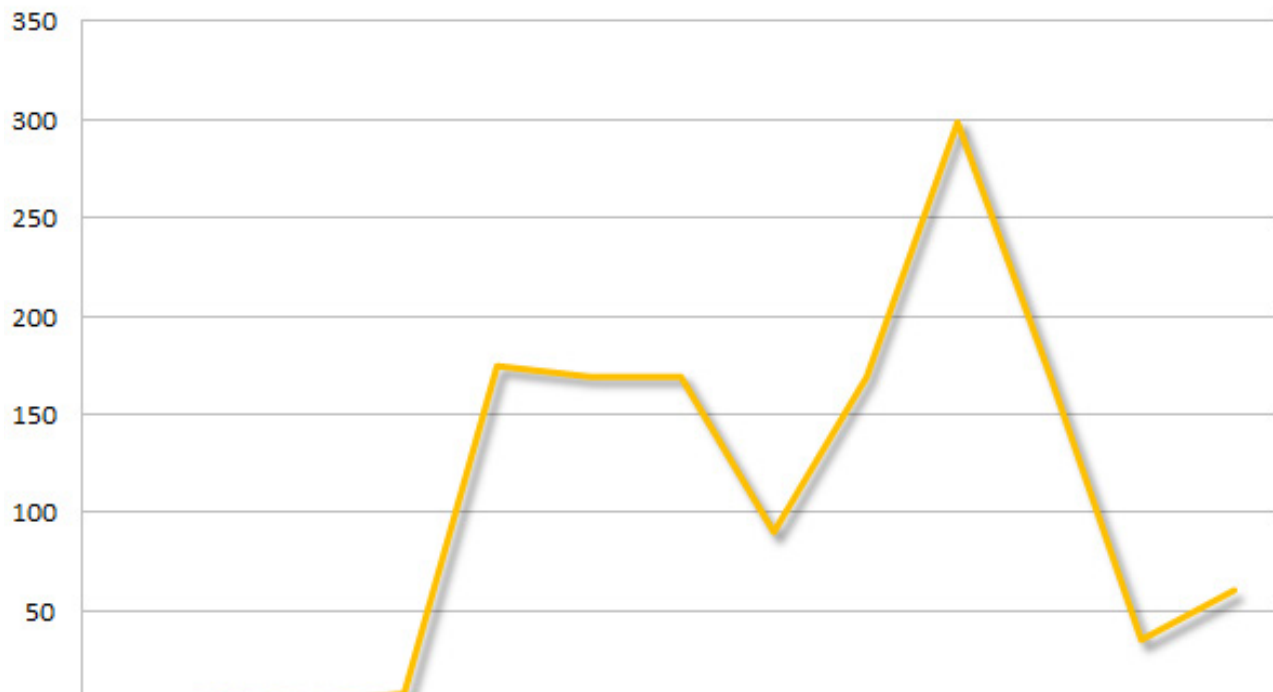



Figure 2. NTP amplification attacks seen by Symantec's Global Intelligence Network

Towards the end of 2013, we noticed an increase in servers being compromised and the high bandwidth being used in DDoS attacks. This trend is highlighted in the case of [Backdoor.Piltabe](#), which this paper will discuss. The trend was recently seen again when the ShellShock Bash vulnerability was exploited [within hours of the bug's discovery, allowing attackers to install DDoS](#) scripts on servers. Considering that there may potentially be a few hundred million vulnerable Web servers, this could end in a huge disaster if only a fraction of the servers gets added to a DDoS botnet. The Bash vulnerability can be exploited to download a malicious ELF file and run it on the server. The analyzed malware sample in this campaign is able to perform UDP and transmission control protocol (TCP) floods against chosen targets. This malware is detected by Symantec as [Backdoor.Trojan](#).

Another trend that we noticed is that DDoS attacks have become shorter in duration but larger in volume. Attackers have often been carrying out bursts of attacks with high peaks and changing the attack type over time. For some of the cases, we noticed short, initial probe attacks, which served to determine what kind of DDoS protection the target had implemented. The attacker then followed up later with larger attacks. In other attacks, small bursts were enough to temporarily disrupt the victim's operations. For example, in online games, a short offline window of a few minutes can be enough to settle the odds on who will win the game. These short attack bursts increase the difficulty in mitigating these campaigns, as some of the mitigation tactics need some time to start working and most can only cope with a medium attack volume. The average attack duration reported by Prolexic was 17 hours [1].

DOS MALWARE TRENDS



“ Most of the current bots are multipurpose weapons that can perform different tasks... ”

DoS malware trends

Most of the current bots are multipurpose weapons that can perform different tasks, including downloading new modules that expand their capabilities. This makes it difficult to assess if a specific botnet will be used for DDoS attacks or not. Basic DDoS capabilities are part of the majority of today's bots, however, some advertised DDoS modules are actually flawed and will not generate much impact due to implementation errors. Some of the most common dedicated DDoS bots are Darkness/Optima, Dirt Jumper/Ruskill, BroBot and BlackEnergy. The average lifespan of a bot in the United States in 2013 was 13 days, with 20 percent of all bots being located in this country. The infection numbers for bots with a DDoS focus are quite low, with only a few hundred detections per month, but most of them have a constant install base.

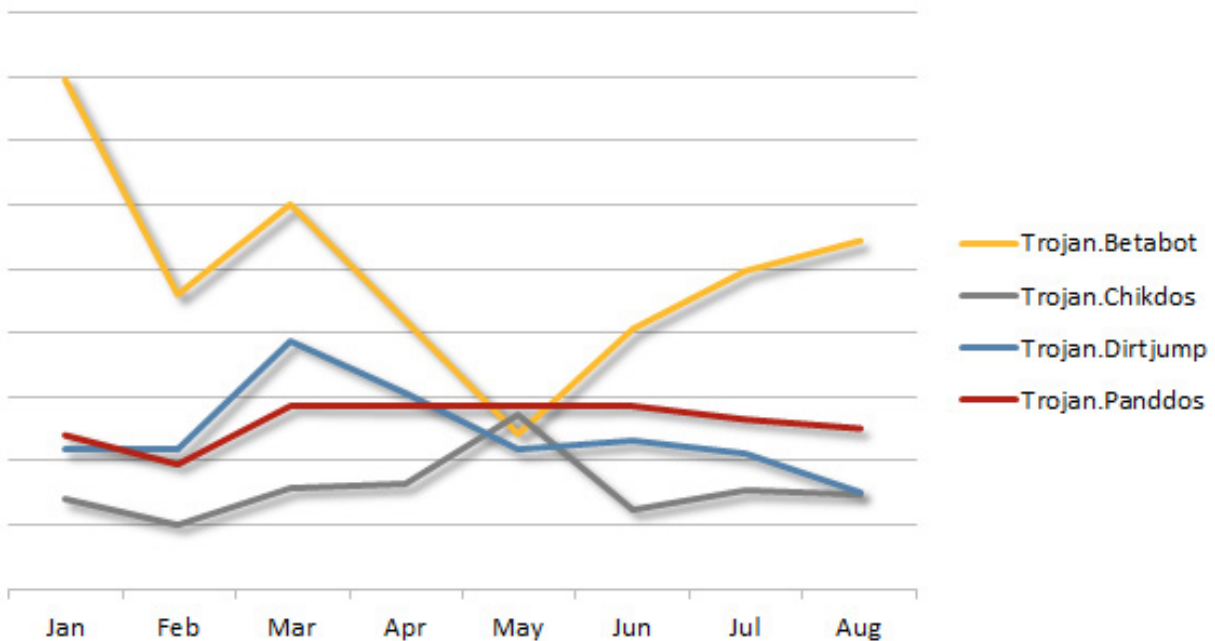


Figure 3. DoS malware infections per month in 2014

For example, the Beta Bot threat appeared in early 2013 and has a plethora of features at its disposal. Besides infostealer capabilities, it has multiple DoS attacks features. The global infection numbers for Beta Bot ([Trojan.Betabot](#)) are only a few hundred per month.

Linux server malware

At the end of 2013, we noticed an [increase of servers](#) getting compromised with malware. The attackers used a public exploit for the [Elasticsearch Arbitrary Java Code Execution Vulnerability](#) (CVE-2014-3120) to issue custom commands on the targeted Linux server, which ultimately lead to the installation of remote shell scripts. [Java.Tomdep](#) is a similar example with a focus on Tomcat Web servers. Another example was when attackers exploited the zero-day [Apache Struts ClassLoader Manipulation Security Bypass Vulnerability](#) (CVE-2014-0094) to hijack Linux servers. Attackers primarily used these servers to perform DDoS attacks through DNS and SYN flood attacks. The botnet was dubbed IptabLex and is detected by Symantec as [Backdoor.Piltabe](#). First, the infections concentrated on China but now, servers all around the globe are getting compromised. The malware is an ELF binary that comes in two server versions—limited and advanced. Both will be installed on the Linux server to allow the threat to automatically start when the server starts. We have seen various versions of Linux getting infected with this malware. These servers all have high bandwidth at their disposal and are often not protected by security software. But the threat no longer solely focuses on servers, as the group behind these attacks has started to infiltrate routers as well.

Within 24 hours after news about the ShellShock Bash vulnerability was published, we saw the first use of an exploit against the issue, where attackers aimed to install DDoS malware scripts on Unix servers. This shows once more how attackers are fast adapting their methods to new opportunities to expand their botnets.

Another example is the BroBot botnet running on compromised servers, which first appeared at the end of 2012. This bot was used by hacktivists in Operation Ababil against US financial institutions. Brobot's active attacking infections seen per day increased from 109 in July to 145 per day in August, which was a rise of more than 33 percent. The PHP-based bot can execute remote modules and use the following methods for DDoS attacks: UDP, TCP, DNS, HTTP and SSL.

Dirtjumper

Dirtjumper ([Trojan.Dirtjump](#)) is another example of a DDoS bot which is widely used. It was very active in 2013, experiencing a massive peak in August. In 2014, infection rates remained at a constant level of around 27 percent of the average level seen in 2013. The tool was initially released in 2009 under the name RussKill and evolved into its current state in 2011. The bot offers multiple DDoS options, including HTTP GET and POST flood requests. The bot will randomize the browser user-agent and referrer string of any request that it sends by default.

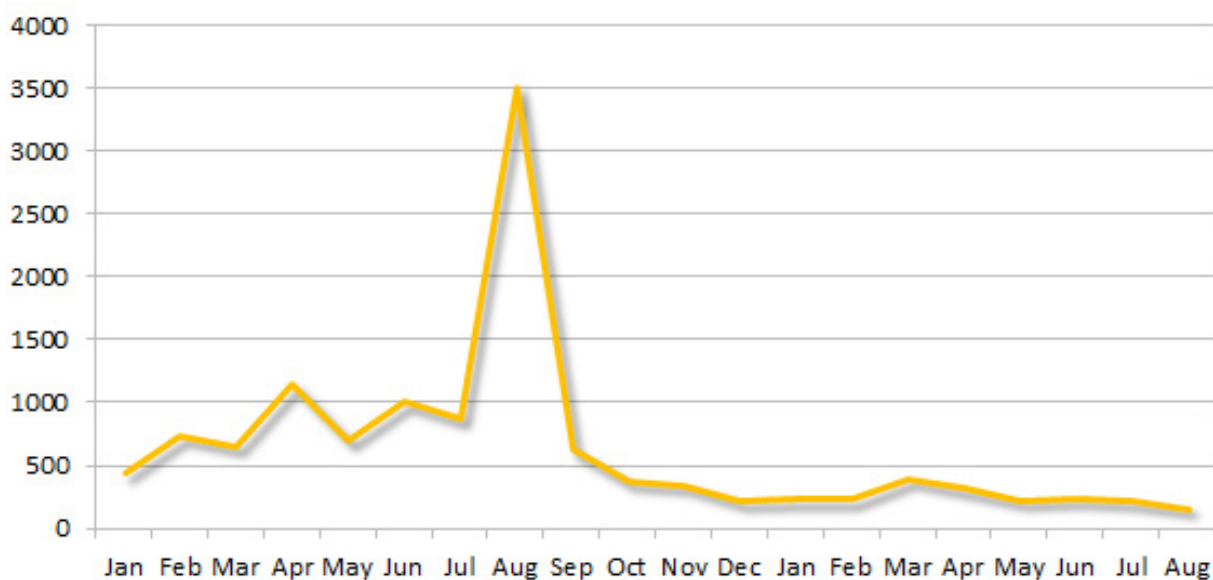


Figure 4. Infection rate for Trojan.Dirtjumper

DDoS as a service trends

It is now easier than ever for someone to carry out a DDoS attack, regardless of their technical knowledge. DDoS as a service is sold online on underground hacking forums. These “booter” or “stresser” services are sometimes advertised as legitimate products for infrastructure stress tests. Other providers are more blatant about their services and do not hide their intention. The sellers promote the services with fancy videos as ways to knock competitors offline.

The prices range from US\$5 to over \$1,000, depending on the attack’s duration and size. While the sellers offer amplification attacks that could generate more than 100 Gbps of attack traffic, in reality the generated traffic seen is usually around 20-40 Gbps.

These services are commonly offered in the gaming community to temporarily get rid of competing teams. There are a few specialized services that will take on any target, even heavily protected ones, but the price can go up to a few thousand dollars.

Most of the services are very similar and there is some rivalry between the sellers. As a result, many of the booter sites actually use DoS-protected hosting to defend themselves. However, their services sometimes do get hacked, resulting in the leak of their customer database.

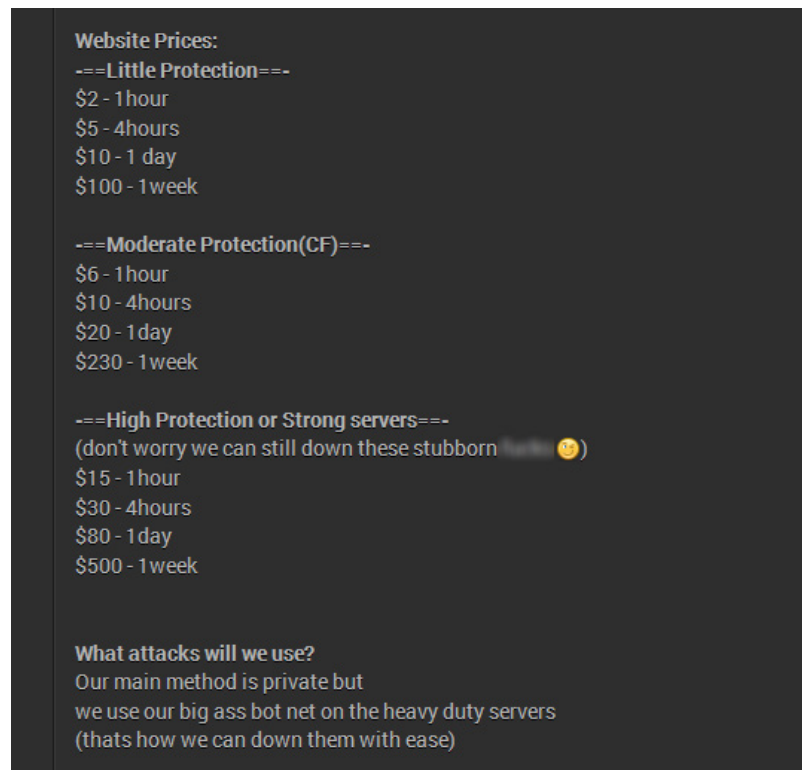


Figure 5: DDoS pricelist

Hello today i would like to offer you my DDos services 😊

Supported attack methods : Udp , Xudp , Chargen , Essyn , Ssyn , Ntp , Amp and Udplag

Monthly price Updated @05/2014 :

Bronze Monthly : 30 Days membership - 30 Seconds Stress - Unlimited stress per day. > 5 Euro <

Silver Monthly : 30 Days membership - 60 Seconds Stress - Unlimited stress per day. > 7 Euro <

Gold Monthly : 30 Days membership - 90 Seconds Stress - Unlimited stress per day. > 10 Euro <

Platinum Monthly : 30 Days membership - 120 Seconds Stress - Unlimited stress per day. > 12 Euro <

Ultimate Monthly : 30 Days membership - 200 Seconds Stress - Unlimited stress per day. > 15 Euro <

Extreme Monthly : 30 Days membership - 1200 Seconds Stress - Unlimited stress per day. > 30 Euro <

Lifetime price Updated @05/2014 :

Bronze Lifetime : Endless membership - 45 Seconds Stress - Unlimited stress per day. > 40Euro <

Silver Lifetime : Endless membership - 80 Seconds Stress - Unlimited stress per day. > 50 Euro <

Figure 6. DDoS booter service advertisement

We offer you the services to eliminate competitors websites and servers using DDOS attack.

About Us:

- Produce an attack on sites / servers / IP 's / Ports
- Anonymity • 100%
- In case of failure of the order is available for the remaining time manibek
- Undertake the serious purpose, as well as goals from DDoS-protection.
- Make a free test for 5-10 minutes.

Prices:

- > \$ 50 night
- > From \$ 300 week
- > \$ 900 a month

Loyalty discounts.

The final price depends on the purpose of the order, as well as from its protection.

Figure 7. DDoS service for offer

TARGETS & MOTIVATION

“The extortion demand is accompanied with a short DDoS burst to demonstrate the attacker’s capabilities...”

”

Targets

The most commonly targeted sector of DDoS flood attacks is the gaming industry, followed by the software and media sectors. These sectors have been in the focus for the past few years. [Verisign](#) reported that 43 percent of DDoS attacks targeted the media and 41 percent targeted IT services in the second quarter of 2014. The rest of the top five list includes the public sector, financial institutions, and telecommunication providers. According to Prolexic, the gaming industry was the most attacked sector, experiencing 46 percent of attacks, followed by IT services with 22 percent, media, entertainment with 15 percent, and financial services with ten percent of attacks [1]. During political crises, we often see an increase in DDoS attacks being used against government websites, such as, for example, in summer 2014 during the crisis in Ukraine.

The most offending countries for flood attacks, which means where Symantec has seen most of the DoS attacks originate from in our GIN, was India with 26 percent, followed by the US, with 17 percent.

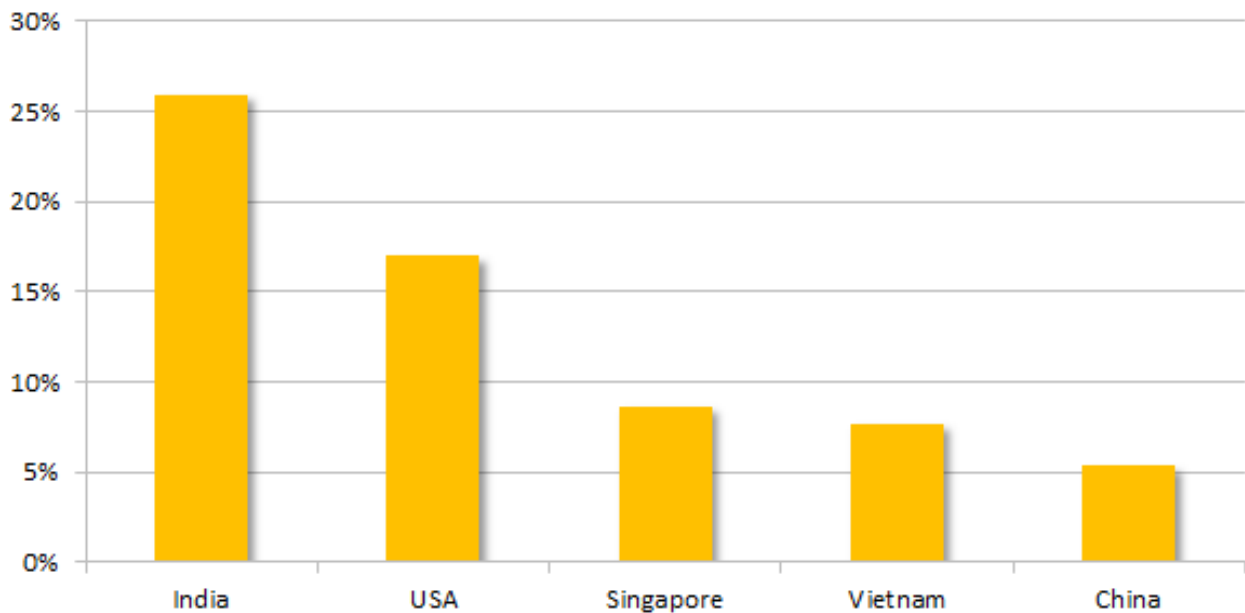


Figure 8. DDoS source countries in 2014

As a reference, the Prolexic Q2/2014 report lists USA, Japan, and China as the top three sources. The sources for DoS attacks are often countries that have a high number of bot-infected computers and a low adoption rate of filtering of spoofed packets. Combining this with a high amount of unpatched, open amplifiers for DNS or NTP attacks make these regions an ideal launching platform for DDoS attacks. It should be noted that this does not mean that the people behind the attack are located in the same country, as the attacks are often orchestrated remotely.

Motivation

The most obvious consequence of a DDoS attack is that the targeted service will be unavailable for legitimate customers. The motivations of the attackers, on the other hand, are often not so clear and can vary a lot.

Extortion and Profit

One of the most easy-to-comprehend motivations for DDoS attacks is the desire to gain profit through extortion. In this kind of scam, attackers blackmail victims by email, demanding that they pay a fee or else their online presence will be knocked offline for hours by a DDoS attack. Sometimes, the extortion demand is accompanied with a short DDoS burst to demonstrate the attacker's capabilities and to amplify the significance of the looming threat. The targets are often companies that heavily rely on their Web presence, such as online shops, online gambling or betting sites, and media and gaming services. Surprisingly, the attackers often demand quite a small amount of money. For example, during an attack against a [US company](#) in April 2014, the attacker demanded US\$300.

Of course, attackers sometimes request a small amount to test if the victim is willing to pay, and if so, they may demand even more after the victim sends the money. There have also been reported cases where the demanded money was more than six figures. Unfortunately, this kind of cybercrime is considerably easy to perform and has attracted quite a few copycats who want to get easy money. For example, in Germany, five people between the age of 16 and 22 were [arrested](#) and convicted in 2014 for blackmailing more than 40 online stores by threatening them with DDoS attacks. On average, the attackers demanded US\$150 from the store owners. Most of them did not pay the ransom and faced loss of millions due to inflicted damage.

The timing of attacks varies a lot. A DDoS attack may be more effective if it starts on Friday afternoon, as there might be less staff in the office to mitigate the attack. However, for extortion attempts, major events are often chosen as a starting point. For example, attackers may target online gambling sites during a soccer final or attack online retailers on Black Friday.

There are many ways to profit from DDoS attacks. It is easy to see how competitors could profit if the DDoS attack victim's customers have to order from a different online store due to downtime. In 2013, we noticed [another tactic](#) being used against the cryptocurrency bitcoin. A group carried out multiple DDoS attacks against larger bitcoin trader platforms. This generated enough chaos and panic that the exchange rate dropped significantly by 60 percent, allowing the attacker to buy bitcoins cheaply and sell them later at a high profit.

Diversion

DDoS attacks can also be used in targeted attacks to [distract](#) the victim from the real attack or to keep the victim's resources busy. The idea behind this is to distract the local CERT team with a DDoS attack while a targeted attack is conducted. Researchers have speculated on this tactic for a long time as it can serve multiple purposes. Besides keeping the victim's incident response team busy, a DDoS attack can also be used to prevent users, for example online banking customers, from logging into the service and discovering that their funds are missing. Servers may get restarted, which could result in the loss of forensic evidence that once was in memory.

The DDoS attack may also cause log files to grow larger, making it difficult for the firm's security team to find the right entries. Of the companies that experienced a DDoS attack in 2013, 55 percent were also victims of data theft or another attack at the same time, according to a survey from [Neustar](#). These DDoS attacks are usually smaller in volume and only last for a short amount of time, as they do not want to destroy the target.

Hacktivism

When discussing hacktivist collectives, one of the first groups that come to mind is Anonymous. While this loosely associated network of individuals and groups are still making their mark, their campaigns are failing to create the impact that they once did. While attacks under the Anonymous banner still pose a major risk, it is other hacktivist groups that have somewhat taken the limelight in recent times. The al-Qassam Cyber Fighters, Cyber Berkut, or #OpHackingCup groups are good examples of the use of DDoS attacks to protest in favor of particular ideologies

and generate media attention. Hacktivist groups often leak their intention before the attack in order to maximize publicity during the attack. The attacks follow a specific timing, because if the customer and the media notice the attack, the gain for the attacker is larger. Attackers are also using media coverage as a means to validate that the attack actually worked.

Another example of this motivation is the [DarkSeoul group's](#) DDoS attacks against South Korea. At the 63rd anniversary of the start of the Korean War, multiple government sites were hit by DDoS attacks. During the campaign, a multi-staged Trojan was distributed through compromised Web servers. Once the timestamp of a downloaded image file was matched, [Trojan.Castov](#) started flooding the DNS server with DNS requests to bring the server to its knees. This group, which conducted various targeted attacks in the past, is also known to have wiped large numbers of computers during US Independence Day. The performed attacks were intelligently coordinated and required good level of knowledge about the target.

Disputes

Short DDoS attacks against competing players are unfortunately very popular among online gamers. Booter services are traditionally used directly against the other player's computer, keeping them from connecting to the online game. As a result, the game will continue unhindered on the server without the victim. But most large online gaming networks have already experienced at least one disruptive DDoS attack against their infrastructure as well.

Of course this is not limited to gamers, as any individual with a personal grudge might be a candidate for a DDoS attack. In the past, we have seen cases where a harmless dispute that started in a chat channel or forum escalated and one of the parties started to use DDoS attacks to force their rival offline.

Due to the fact that DDoS services can be rented cheaply and do not require sophisticated knowledge to perform, we are unfortunately seeing an increase in the use of DDoS services to settle arguments online.

Collateral damage

Sometimes, the DDoS attack is unintentional and was not performed with a malicious intent. A classic example is when a small company's website is featured in a major news article, which generates a lot of interest.

This could lead to tens of thousands of users visiting that particular website, resulting in an application-level DDoS attack. In other instances, a malware sample might use a domain-generating algorithm (DGA) to generate URLs from where to download updates. If a legitimate business happens to share the same domain, they will get an unintentional DDoS attack from all of the clients trying to download the update from their site. Such a case happened at the beginning of 2014 in [South Korea](#), when a threat attempted to download an update from 16 media websites which massively slowed down the sites.

DDOS SERVICE

about

You have up to '3' targets choices:
 - Game Servers
 - Home-connections
 - Websites

The power is more then mostly other peoples DDoS Service.
 I dont have any dstat on the power..
 But I can guarantee that my service wont let you down.
 I only accept paypal.

prices

- ✓ Game Server: 2\$ every 30 minutes.
- ✓ Home Connection: 15\$ each 24h/ 2\$ every 2h
- ✓ Website 2\$ every 30 minutes.

PM me
 Or add me on skype:

Figure 9. DDoS service for gamers

EXAMPLES OF RECENT DDOS ATTACKS

“ There are constant
DDoS attacks
happening around
the globe... ”

Examples of recent DDoS attacks

Besides the large NTP DDoS attack in February that peaked at 400 Gbps, which we already mentioned, there are constant DDoS attacks happening around the globe. Often, companies give minimal details about these attacks. Even if a group takes responsibility for the attack, it is often unclear what exact methods were used and how successful they were. The following are a few examples of recent attacks that we have seen.

Attacks against gaming sites

In December 2013, a group under the name of Derp or DerpTrolling came up with a new mission to disrupt online games played by a user named PhantomL0rd, who regularly streams videos of his gaming sessions. The group previously accepted requests for new targets, usually big companies, and advertised attacks on Twitter. But this time, the target was an individual gamer. The group went after different online gaming servers in an attempt to disrupt this player's gaming activities. Through chat, PhantomL0rd was in contact with the attackers, who followed him from game to game. The group was successful in bringing down major online game servers. This series of

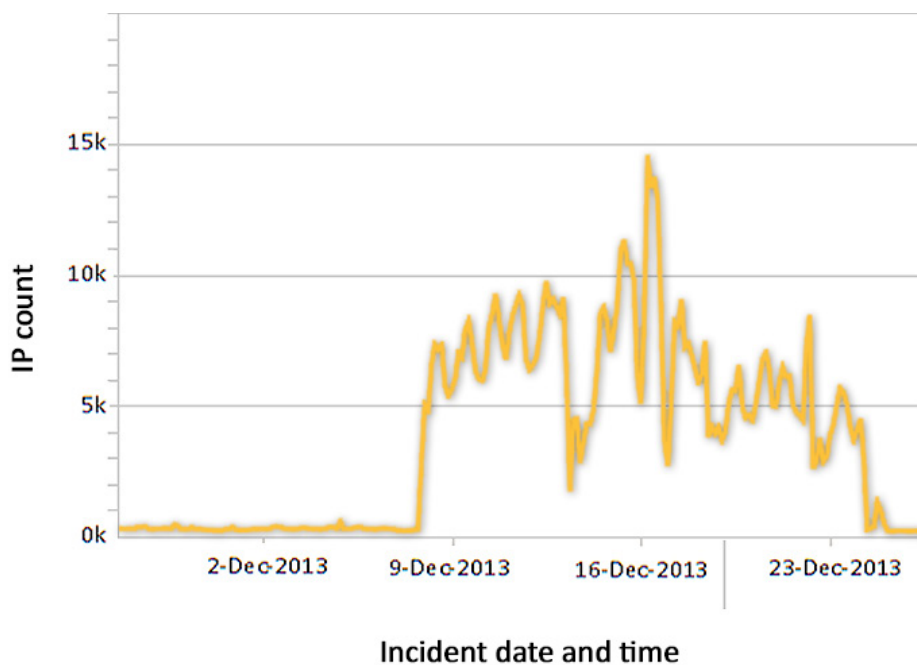


Figure 10. NTP amplification attack by DerpTrolling

attacks also saw the attackers harassing PhantomL0rd in real life, such as by ordering massive amount of pizzas to be delivered to PhantomL0rd's house and even having the police raid his house under a false allegation. Such real life disturbances have increased lately against gamers who are popular on video streaming sites.

In January 2014, reports indicated that an alleged member of the Derp group was arrested in New York. Despite this, the remaining members of the group continued to perform attacks. These attackers used [NTP amplification](#) DDoS attacks, which spiked in December, as seen by Symantec's global intelligence network (GIN) in Figure 11.

It is not always clear who is behind an attack, as sometimes, multiple groups claim responsibility. For example, in August, the Sony PlayStation Network and Microsoft's Xbox Live [experienced massive disruptions](#) after being attacked with DDoS floods. Shortly after they went down, a group called Lizard Squad took credit for the attacks. But they weren't the only ones to do this, as a user with the moniker FamedGod claimed in a video that he was actually responsible for the NTP attack, providing some details on how he did it.

This started an escalating feud between the two parties, where the Lizard Squad group raised the bar by hinting that there might be a bomb on board the Sony's Online Entertainment president's flight. The airline responded and diverted the plane, but the security check revealed no explosives. Later, the group continued to take down other gaming sites.

These are just two examples of attacks against the gaming industry. As previously mentioned in this report, attackers commonly conduct smaller burst attacks against competing gamers, often using booter services.

Attack against bitcoin traders

A large European bitcoin payment processor was [attacked at the end of 2013](#). The attackers carried out a DDoS attack to weaken the company's network and set some systems offline due to overload. Once this happened, the attackers accessed some of the wallets stored on the service, stealing bitcoins worth for more than US\$1 million. In the past year, we have seen [many attacks](#) against cryptocurrency trading platforms. These attacks often try to influence the exchange rate in order to gain profits. Even if the attacker doesn't generate any direct profit, they can [prevent](#) other users from accessing their online wallets, which could lead to a potential loss for the targets.

Hactivist attacks

During the World Cup in Brazil, hactivists from Anonymous brought down multiple government sites with DDoS attacks and website defacements ([#OpHackingCup](#)). The group's protest was directed at the Brazilian government for spending hundreds of millions on stadiums for the World Cup instead of helping the poor with hospitals and schools.

During the summer of 2014, a collective called "Cyber Berkut" performed several DDoS attacks against NATO websites and various targets in Ukraine. The attacks are linked to the tensions in Ukraine and are a protest against the NATO's involvement in the region.

Since 2012, the "cyber fighters of Izz Ad-Din Al Qassam" used DDoS attacks against multiple targets in multiple waves, most commonly against financial institutions in the United States. Operation Ababil resulted in around 65 Gpbs of traffic, which generated multiple hours of downtime at various banks. The attacks were in response to various statements against Muslims, such as the release of a controversial film by an American pastor. The group used the BroBot botnet ([PHP.Brobot](#)) with high bandwidth servers to conduct TCP, UDP, and HTTP flood attacks. A part of the botnets is still active and continues to grow today.


Impacts of DDoS attacks

Besides the obvious downtime that a DDoS attack generates, there might be other impacts to the victim. Of course, downtime and the issues caused in all of the dependent systems can be devastating enough, but the attack may generate additional costs, as some hosting solutions, including DDoS-protected ones, bill the user for the traffic used by its clients. Therefore, even if the DDoS attack was not successful in bringing down the website, the victim may still have to pay a substantial amount of money for the used bandwidth. This is in addition to the maintenance and operational costs of the site.

Depending on the sector of business that the victim is in, DDoS attacks might lead to customer frustration. If, for example, the online store goes down, customers may lose confidence in the brand and go somewhere else to shop. This could result in a loss of revenue or in some cases, even repression, depending on the granted service-level agreements (SLAs). This loss is very hard to measure. In addition, such attacks might generate a higher call volume in the call center from the store's customers, which can lead to more costs and customer frustration due to waiting times.

Some servers and network devices might start to reboot when they exhaust their resources. This can lead to the loss of log files. Other devices may start to overwrite log files or drop data in order to cope with the huge load of packages. This potentially means that a simultaneously executed attack could go unnoticed as the log file is missing.

MITIGATION



“ A DDoS attack scenario should be part of every incident response plan.

”

Mitigation

Mitigating a DDoS attack is often not easy and depends on how critical the online presence and service uptime is for the company. Unfortunately, there is no silver bullet that can fully remove the risk of being affected by a DDoS attack. The best solution is to have a layered protection approach that allows for filtering at various levels, depending on the type of attack.

There are different approaches for DoS protection services, some which are always on, others which are enabled on demand. Depending on the business' requirements, there are different advantages to consider. The time to live (TTL) value on your DNS records is important to note when considering DDoS defenses. If you have a long TTL value, you will not be able to switch your DNS records quickly to a new, protected location in the case of an attack. This all shows the importance of being prepared. It is essential to think about mitigation before an actual attack happens, as during the DDoS attack, the pressure on staff and resources may be high.

Be prepared

A DDoS attack scenario should be part of every incident response plan. A companies' CERT or IT staff needs to check their exposure before an actual attack happens. Know who to call. Businesses should create a plan with the required contact information for ISPs and Web hosting providers. Most ISPs are interested in keeping their network bandwidth unclogged and will help mitigate the attack where they can. [ICANN](#) has created an article that explains what an organization can do when they are under attack.

Best practices

The best advice to follow is to be prepared for the next attack. Considering the increase of DDoS attacks and how easy they are to perform, it is only a matter of time until an exposed online service will get hit. The following is a list of some advice that can help companies better prepare themselves against DDoS attacks.

Be prepared for the next attack

- Have an incident response plan ready and know who to call in an emergency
- Discuss DoS mitigation strategies with your upstream provider and ensure that they are aware of this threat
- Utilize DDoS protection services where beneficial

Monitor your network and detect abnormal behavior patterns

- Know what your normal network behavior looks like
- A NetFlow analysis can be a good way to detect attacks
- Include enterprise-wide security monitoring from edge to endpoint

Design your network with scalability and flexibility in mind

- Load balancers, reverse proxies, and content delivery networks (CDN) can help flatten small network peaks
- Know the bottlenecks in your infrastructure

Do some basic traffic filtering, layered where possible

- Firewalls, blackhole routing, and traffic shapers can help drop some of the unwanted traffic
- Be aware that firewalls themselves can be targets of resource-exhausting attacks
- Utilize Web application firewalls (WAF) as a front-line defense against layer 7 attacks
- Close/block unnecessary ports and disable unused services
- Block inbound ICMP and UDP traffic if not used with a rule early in the rule set

Verify configuration on servers and network

- Patch and harden your servers and external exposed systems
- DNS, NTP, and Web servers should particularly be periodically checked for configuration issues
- Check the options for aggressive connection aging and TCP window size enforcement

Blacklist sources

Blacklisting IP addresses can be difficult or even useless if an attacker uses spoofed sources. Often, attackers change their source pool over time in order to make it more difficult to blacklist the sources, but it can still help mitigate part of the attack. The same holds true for blackhole routing, where IP addresses are intentionally null routed and not forwarded.

Over-provisioning bandwidth

A DDoS prevention strategy which is sometimes suggested is to buy more bandwidth. Unfortunately, this is not really a cost-efficient method and if the attackers really want to harm your business, they will always find more bandwidth. This is generally an arms race, which the targeted company will lose.

Pure CDNs are often not designed to protect resources from DDoS attacks, even though they provide larger bandwidth. Attackers might simply bypass the cache and send requests directly to the backend servers. It makes more sense to partner up with anti-DoS services before an attack happens.

Insurance

In recent years, insurance for cyberrisks has been gaining in popularity. The scope of coverage and the prices vary widely. Such insurance policies allow companies to insure part of the damage associated with DDoS attacks. Each enterprise has to assess how big the risk of a DDoS attack is for them and how large their risk appetite is. Of course, the attacks will still happen and companies cannot simply insure away all of the risks.

Don't become the source

Protect your servers and configure them according to best practice guidelines. Install patches and harden your systems so that they will not be compromised and added to a botnet. You should also prevent your DNS server from acting as an open resolver and disable the "Monlist" command on any NTP servers in your organization. Most gateways allow a bandwidth throttle that can help reduce the damage you may inflict if your network is compromised. Set up some monitoring alerts that inform you once outbound traffic spikes.

Stop spoofing

For many years, ISPs have tried to prevent people from spoofing the source address of IP packets. RFC2827, along with its implementation [BCP38](#), advise providers to adjust their in and outbound traffic rules. Simple firewall rules can check if packets that have been received on an interface impersonate other internal resources. This would help to prevent some of the attacks, especially amplification attacks. Surprisingly, a lot of providers have not yet implemented BCP38, meaning that attackers can still spoof packets. According to the [Spoofer Project](#), more than 25 percent of all computers are still able to send spoofed packets to the network.

Unfortunately, preventing spoofing would not eliminate the problem of all DDoS attacks, as compromised servers and botnets could still flood victims using their real IP address. But it would make it much harder for attackers to hide and reduce the chances for amplification attacks.

CONCLUSION



“ In the future, we might see more DDoS attacks coming from mobile devices or even the Internet of Things... ”

Conclusion

DDoS attacks are rising as a threat. Over the last few years, these attacks have grown in intensity and now have traffic volumes of up to 400 Gbps. These attacks are easy to carry out and do not require great knowledge or access to zero-day vulnerabilities. The duration of the attacks is often just a few hours or even minutes, but this can be enough to inflict a lot of damage at the target site. Currently, amplification or reflection attacks are the most popular attack. These attacks use DNS or NTP servers to amplify the attack traffic by a factor of 50-100 times. This allows small botnets to conduct huge volumetric attacks. Many initiatives can help to protect reflection servers, but there are still more than enough open amplifiers that can be misused. In 2014, we have noticed an increase in compromised Unix servers being used to launch attacks. They are of great interest to the attacker, since they provide a large bandwidth. DDoS botnets can be rented as a service starting at \$5 for small attacks.

Application-layer attacks, which target the Web application, are gaining in importance as well as they are difficult to mitigate. They will become even more important in the future as often, attackers adapt their methods during an attack in an attempt to bypass any short term defense mechanism. In the future, we might see more DDoS attacks coming from mobile devices or even the Internet of Things, but this is currently not happening on a large scale.

The motivation of the attacker can vary widely, with hacktivism, profit, and disputes being the main reasons. Considering the ease of conducting large DDoS attacks, Symantec expects that the DDoS growth trend will continue in the future. The likelihood of being targeted by short but intensive DDoS attacks is rising.

Some companies try to over-provision bandwidth resources to defend themselves against potential DDoS attacks. However, this arms race is very expensive to win. It is more important to be prepared for DDoS attacks and have an incident response plan ready. Talk to the upstream provider and ensure that they are aware of this threat and check what benefits the utilization of DDoS protection services can bring.

APPENDIX

Appendix

Types of DDoS attacks

Most attacks try to overwhelm the victim's network with packets and saturate their network bandwidth. Twenty-six percent of the attacks in the second quarter of 2014 were SYN flood attacks that tried to saturate the victim's infrastructure [1]. But it is also possible to reach the limitation of an application or at the OS level when too many packets are sent. Some observed DDoS attacks generated more than one million packets per second (Mpps), which can bring down many network devices just by the numbers as well. Often, attackers use a combination of multiple attack types, which can also vary over time.

Volumetric attacks

Volumetric attacks commonly use Layer 3 and Layer 4 protocols to generate high volumes of traffic. This is the most common type of DoS attack and can saturate the target's infrastructure, such as the network link, router, and server. These attacks include UDP, ICMP, and TCP floods. The packet source can be spoofed to make it harder to mitigate. These attacks are often carried out through botnets in order to maximize the impact.

In addition, tools like the LOIC are used. LOIC received some publicity after being heavily used by participants of the Anonymous hacktivist collective to perform DoS attacks. Such tools will use a local computer to perform various types of network flood attacks. In many cases, the source of the traffic was not spoofed, which led to arrests and convictions in the past. For instance, there was the case involving a man from the United States, who was given [two years federal probation and a fine of US\\$183,000](#) for taking part in a DDoS attack against a multinational corporation. The sentence may seem severe, considering that the man used the LOIC DDoS tool for approximately 60 seconds as part of a larger group of hacktivists taking part in an Anonymous campaign.

Protocol attacks

In addition to pure volumetric attacks, attackers have also been trying to consume the actual resources on the server or intermediate network equipment like firewalls and routers. An example is TCP connection floods, where the attacker tries to use up all of the possible open connections on the targeted Web server.

The increased use of reflection attacks doesn't mean that other methods have disappeared. An attack against one of the world's largest bitcoin exchanges used a TCP SYN flood attack and reached over 100 Gbps. Rather than using a huge botnet of compromised computers for this attack, it is believed that those responsible used a network of compromised servers, which is another tactic that is increasingly being utilized. Compromising insecure servers gives hackers access to far more bandwidth than they would get from even a modest sized botnet with DDoS functionality. Some attackers hijack servers in cloud infrastructure, which often have high bandwidth and might have a good IP reputation.

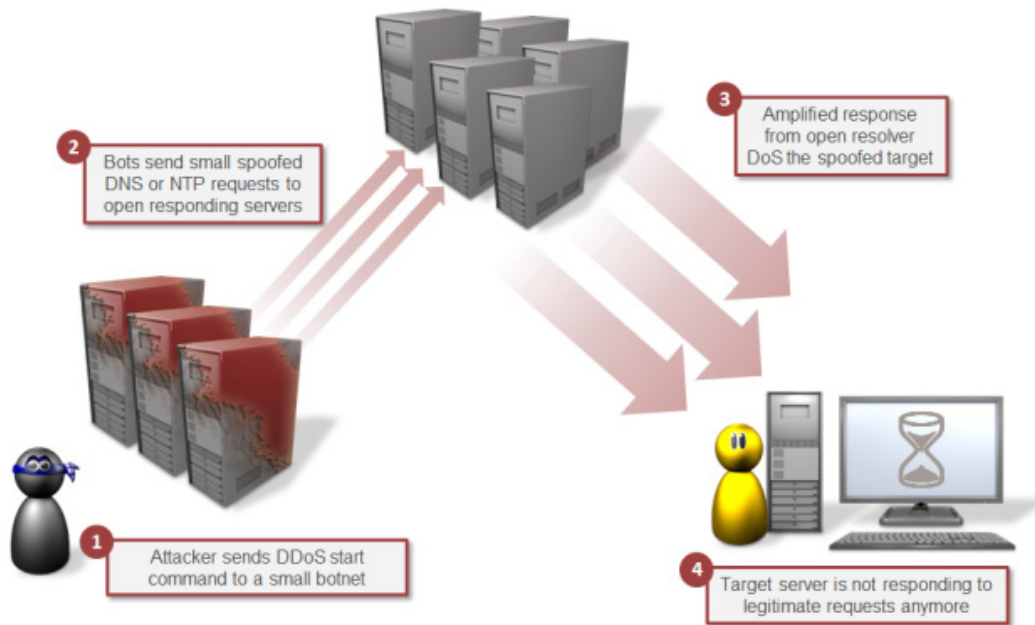
Amplification/reflection attacks

The idea behind amplification attacks is simple. Through the misuse of weaknesses in Internet services and protocols, an attacker can amplify their own traffic by a given factor by reflecting it at the third-party server. This means, for example, that the attacker only needs to control 1Gbps of traffic to allow a third-party amplifier to generate 20 Gbps of traffic, which is then redirected to the target. The reflection is achieved by sending packets with a spoofed sender address that appears to be the victim's, so that the response will flood the victim. There are a handful of services which are currently used to generate such amplification attacks, including DNS, NTP, SNMP, simple service discovery protocol (SSDP), and Chargen.

DNS amplification

DNS amplification DDoS attacks hit the news in March 2013 after a massive DDoS attack hit the antispam organization Spamhaus. The reported attack traffic volume was 300 Gbps, which at the time was the largest DDoS attack recorded.

Amplification DDoS Attacks



Symantec Security Response

Figure 11. DDoS amplification attack schema

In this type of attack, an attacker sends a request with a spoofed source IP address, matching that of the target, to a large number of recursive DNS resolvers. The resolvers then respond to the request, but the response is much larger in size, which means the attacker can effectively amplify their attack from 10 to 50 times that of the bandwidth they have available. This should not be confused with DoS attacks against DNS servers, where the attacker attempts to bring down the DNS server itself and does not care about any reflected traffic.

DNS reflection attacks are made possible by misusing poorly configured domain name servers that have recursion enabled and will respond to anyone. These are referred to as open resolvers or open DNS recursors. There are [28 million open DNS resolvers](#) online that need to be locked down and secured. Until this problem is addressed, DNS reflection attacks will continue to be used for large DDoS attacks. In the past, we have also noticed that some attackers set up their own deliberately vulnerable DNS servers and then misused them for reflection attacks.

NTP amplification

Amplification attacks [using NTP](#) have been on the rise since end of 2013 and were the most common UDP-based DDoS attack methods for the first half of 2014.

Using the MON_GETLIST command on a NTP server will return a list of up to 600 IP addresses that last accessed that NTP server. This can generate more than 200 times the amount of traffic. The US-CERT released [an advisory](#) in January 2014, warning about NTP amplification and urging users to implement an update which disables the Monlist feature by default. You can verify if you are running a vulnerable open NTP server at <http://openntpproject.org/>

NTP reflection attacks were down significantly in the second quarter of 2014. This could be a result of an awareness and clean-up campaign, where many people upgraded to newer NTP versions that were not vulnerable by default. [NSFocus](#) reported that out of the 430,000 vulnerable NTP servers found in February, all but 17,000 had been patched by May.

This study was conducted after a large NTP amplification attack hit a Cloudflare customer at the beginning of 2014.

According to a report, the attack traffic reached [400 Gbps](#) by using around 4,500 open NTP servers. This is the largest volumetric DDoS attack in history so far. Such a high network load is sufficient to blast any unprotected resource off the Internet.

SNMP reflection

The UDP-based SNMP can also be used to amplify attack traffic, similar to DNS and NTP amplification attacks. Usually, older versions of SNMP, such as version 2, are targeted because they are not safe against this kind of reflection attack. There are a few tools freely available that make use of this weakness. For example, a script from 2011 from the [TeamPoison](#) group still works today. The tool uses “GetBulk” requests against an SNMP server that use the community string “public”, resulting in an amplification of the traffic of up to 1,000 times or more. There are still quite a lot of old, accessible devices that can be used for such reflection attacks. We have seen attackers experimenting with SNMP instead of NTP in 2014, but it is too early to say if they will completely switch to this type of attack in the future.

Blogs and social media

Over the last few years, we have seen attackers using content management systems and social media sites to generate indirect DDoS attacks as well. For example, in March 2014, more than 100,000 websites were misused through the [XMLRPC pingback](#) feature in WordPress to initiate various DDoS attacks. This resulted in an application-layer attack that sent thousands of HTTP GET requests. Other social media features have been misused for DDoS attacks as well. Any feature that can be tricked into sending traffic to a third-party address can be misused. Even a simple but popular social media post that uses JavaScript to automatically send HTTP GET requests can result in a DoS attack.

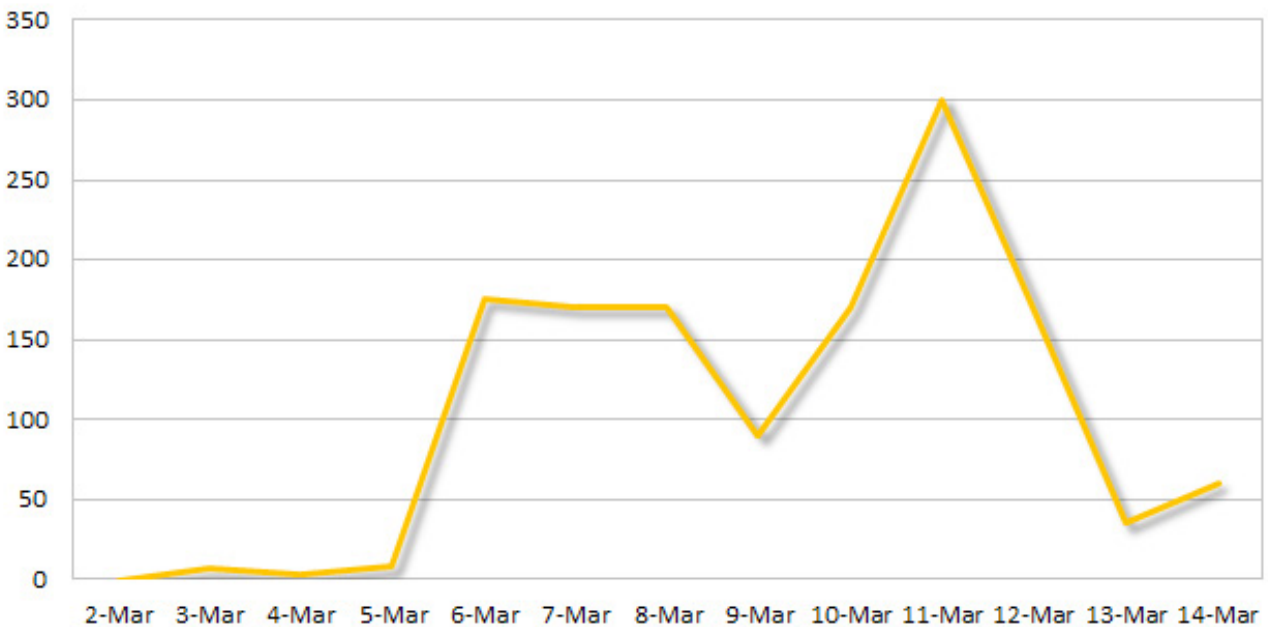


Figure 12. Daily WordPress pingback DoS activity

Application-level attacks

Sometimes we see DoS attacks targeting Web applications directly with simple HTTP GET and POST requests instead of targeting the hosting Web service. For example, targeting Web forms, such as search fields, to post random strings and take advantage of flaws in the application can slow down the Web server drastically. Attackers can even slow down the posting of data to keep the connection open as long as possible by sending the requested data with a very small packet window. The same applies to requesting large images but setting a very small TCP window for receiving them. Submitting complex queries can generate a higher CPU load on the backend server that performs the database look up for the request. As a result, even if the Web server remains responsive, the queries may flood the database server. Sending a few dozen search requests can already be enough to trigger a DoS on a Web application. It can be challenging to distinguish bot traffic from legitimate user requests. At the end of 2013, a group used a [browser automation tool](#) to conduct a DDoS attack from 180,000 endpoints, imitating normal user browsing requests.

Other tactics try to target vulnerabilities in the Web application themselves. For example, older versions of the commonly used scripting languages PHP, ASP.NET, and Python suffered from the [PHP Web Form Hash Collision Denial Of Service Vulnerability](#) (CVE-2011-4885). An attacker could send a specially crafted HTTP request to trigger a hash collision, which would cause the server to reach 100 percent CPU utilization for a few minutes. The recently discovered ShellShock Bash vulnerability allows for many types of DoS attacks against applications as well. One simple example that we have seen in the wild is attackers making the server execute long sleep commands, using up the server's cycles. Even if developers try to do the right thing, they can sometimes cause a DoS condition in their servers. Last year, the Django framework suffered from a weakness in the way it protected against password brute-force attacks. If an attacker repetitively [submitted large passwords](#) for verification, they could considerably slow down the server.

Of course, using of SQL injections to delete all data in a database could be considered an application-level DoS attack, as most Web applications will no longer work if the backend database has been deleted.

These application-layer attacks do not need large bandwidth on the attacker side. With enough knowledge about the target application, the attackers can adjust requests to inflict the maximum amount of damage with only a handful of packets. But even without background knowledge, attackers have been seen using easy-to-use tools like Slowloris, SlowPost, RUDY, and LOIC against Web applications.

Resources

1. <http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q2.html>
<http://www.verisigninc.com/assets/report-ddos-trends-Q22014.pdf>




Authors

Candid Wueest
Principal Software Engineer

About Symantec

Symantec Corporation is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings - anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of \$6.7 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

 Follow us on Twitter
@threatintel

 Visit our Blog
<http://www.symantec.com/connect/symantec-blogs/sr>

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.