WHITE PAPER

DDoS Report: The Escalating Threat of DDoS Attacks

Table of Contents

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

Introduction

With increasing frequency and scale, some of the world's largest data center and network operators are suffering from crippling Distributed Denial of Service (DDoS) attacks. Virtually every commercial and governmental organization today is largely – if not entirely – reliant on its online services, and service availability is completely at risk from the rising tide of DDoS attacks. DDoS attacks are growing in a variety of ways:

- **Frequency**: 50% increase in DDoS attacks year-over-year[1]
- **Size**: 1 in 3 attacks is over 20 Gbps; 60 Gbps attacks are regularly seen and even 100 Gbps attacks are not uncommon[2]
- **Severity**: the biggest impact is the staggering increase in the average packets per second rate in typical DDoS attacks; in fact, DDoS attack rates have skyrocketed 1,850% percent to 7.8 Mpps between 2011 and 2013[3]
- **Sophistication**: 81% of attacks are multi-vector threats and botnets are getting smarter[4]
- **Persistence**: average attack duration is 17 hours[5]

The growing volume and scale of DDoS attacks impairs services used by hundreds of millions of people around the world. This includes users of services like e-commerce, financial services, gaming, social media and even governmental and healthcare services. Even well-funded networks of the largest U.S. banks have experienced outages due to DDoS attacks. Bank of America, Wells Fargo, US Bank, JP Morgan Chase, Sun Trust, PNC Financial Services, Regions Financial and Capital One have all purportedly lost service availability for extended periods as a result of large-scale DDoS attacks. And they are not alone. Smaller credit unions have also had their share of DDoS attacks.

These trends have resulted in new guidelines from the U.S. Federal Financial Institutions Examination Council (FFIEC), as well as the Monetary Authority of Singapore (MAS) to require all banking entities to put infrastructure in place to handle these cyberattacks. Gartner, renowned analysts for the enterprise space, recommends that an eight step program[6] be put in place to control DDoS damage.

New, focused and targeted DDoS attacks are a devastating contrast to security threats such as worms, phishing and virus attacks. A DDoS attack launched by a criminal or vicious competitor can take an entire business offline for an extended period, and the ease with which an attack can be generated makes every organization vulnerable. Criminal syndicates and commercially motivated hackers have built "for hire" botnet networks that can be "rented" on-demand over the Internet. These criminals shamelessly promote their DDoS services, also known as "booters" and often marketed as web performance test tools or "stressers." For example, for under $30 these organizations will launch an hour-long attack, and of course more money provides higher degrees of havoc. While individual DDoS attacks were historically launched by gamers to gain control of an online game session (a.k.a. "booting the host"), the booters have come within easy reach of the masses, such as disgruntled ex-employees who want to disrupt the services of their previous employer. Extortion by criminal syndicates is another common motivation. And more recently, DDoS attacks have been used as a foil for criminals who use the havoc created in response to an attack as an opportunity to exfiltrate data from the target organization.

There are many elements that are involved in DDoS attacks and the measures against them, but they all share one common element: ***large-scale zombie networks or botnets sending traffic at very high packet per second rates***. Protecting against these massive botnets requires equally powerful tools.

Large-Scale Concerns

With the backdrop of an unparalleled growth in DDoS attacks, the common thread is that everything happens at large scale. The main elements that form the DDoS problem are the increasing scale of botnets, bandwidth and connection rates.

In 2012, Spamhaus, an organization that tracks and lists known spammers in a database, suffered from what is still one of the largest attacks in Internet history, reportedly clocking in at 300 Gbps. This attack followed a dispute with CyberBunker, a hosting company where virtually everything is allowed to be hosted. CyberBunker's IP addresses were listed in Spamhaus' database and as a result, many email servers would not accept email from these IP addresses (many email systems in the Internet cross-check against Spamhaus' database). After Spamhaus refused

[1] Akamai's State of the Internet 2014
[2] Neustar Annual DDoS Attacks and Impact Report
[3] Verizon data breach report 2014
[4] Incapsula 2013-2014 DDoS Threat Landscape Report
[5] Prolexic Global Attack Report Q1 2014
[6] "Master These Eight Steps to Control the Damage From DDoS Attacks" - Gartner, April 2014
[7] http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

to remove the Cyberbunker IPs, a large-scale DNS amplification attack started, peaking at 300 Gbps.[7]

In February 2014, an undisclosed customer of CloudFlare was under attack trumping the scale of the Spamhaus attack. CloudFlare claims the peak bandwidth was just shy of 400 Gbps, which was made possible by leveraging a Network Time Protocol (NTP) amplification attack.[8]

The Q1 2014 report from Prolexic (now part of Akamai) mentions a 10 hour long DDoS assault, peaking at over 200 Gbps and 53.5 Mpps, making this the record-holder for DDoS attacks on their network to date.

These attacks are possible due to the exploitation of a vast number of poorly configured networks and servers. Older unpatched Content Management Systems (CMS) such as Wordpress, Drupal and Joomla are a popular target to enlist as zombies in a botnet network. These servers have higher bandwidth connectivity compared to private Internet connections and are always on. Many Internet services such as DNS or NTP, if unpatched, can be leveraged in amplification attacks. In fact, the openresolverproject indexed about 28 million open DNS resolvers that can be exploited for DDoS attacks.

In order for these services to send traffic to the DDoS victim, the network has to allow spoofed IPs to exit the network. Properly configured networks do not allow source IPs that are not part of their Autonomous System (AS) to exit the network. Unfortunately, many networks do not check for this; the Spoofer Project shows that almost a quarter of all networks allow spoofing.

Botnets: Unified Attacks

Many computers, or even more powerful web servers, are infected with viruses or malware that allow an attacker to control them remotely. These compromised hosts, known as "zombies" or "bots," are legion and can be controlled in unison, as they are all linked together by "command-and-control" software to form a "botnet." These bots typically "call home" to a command-and-control center, communicating over Internet Relay Chat (IRC) channels. This allows the actual attacker to hide, while traffic from each bot accumulates to gigantic proportions, taking out the intended victim by saturating its Internet connection, or overwhelming the service or supporting infrastructure, rendering the service unavailable to legitimate clients.

The volume of traffic from each individual bot or zombie machine doesn't seem out of the ordinary, so often the malicious traffic flies under the radar (if even monitored) of the service provider where the bot is hosted. It's the aggregation of traffic from thousands or even tens of thousands of bots targeting a host that creates the crippling impact.

Different botnets can also be used in a single attack. With the increase in connected devices (popularly called the "Internet of Things"), the potential botnet sizes are also increasing rapidly. The first reports on Android-hosted bots are already a fact. With 6.8 billion mobile phone subscribers already, this is an area that needs to be monitored, as overall botnet activity has been up 240% already in this first quarter of 2014. As a matter of fact, in 2013, more than 60% of all web traffic was found to be generated by bots. 29% of botnets attack over 50 targets a month, a 26% year-over-year increase[9].

Botnet example

Large-scale attacks against major U.S. financial institutions in 2013 were claimed by the Izz ad-Din al-Qassam Cyber Fighters, a political group with ties to Iran. The attacks leveraged a vulnerability in CMS applications to install toolkits such as *itsonoproblembro*. These toolkits make the webservers unwilling zombies, and in this case they were used to attack the various U.S. banks using a mix of application-layer attacks on HTTP, HTTPS and DNS, as well as network-layer attacks using floods of TCP, UDP and other IP protocols. These multi-vector attacks are designed to break the weakest link in the victim's defenses.

Bandwidth: Increased Attack Volume

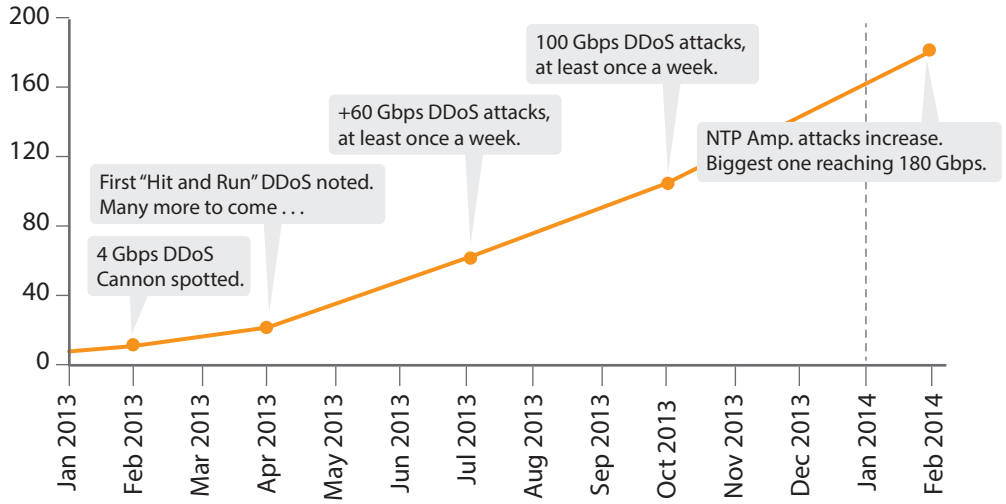
Along with the increasing number of zombie hosts, the bandwidth contributed by each bot is increasing as well. Current botnets are increasingly leveraging compromised commercial servers with high-speed data center network connectivity (e.g., CMS systems such as WordPress) instead of private consumer Internet connections. These servers are equipped with higher bandwidth connectivity, increasing the total botnet capacity.

Amplification and reflection techniques compound this problem even more dramatically. These attacks use forged (spoofed) IP addresses of the victim, and can send queries to DNS or NTP servers, for example. The NTP and DNS servers send all responses to the victim IP with a packet size that can be 200 times the magnitude of the initial query. This of course happens at a whole array of these servers, so the amplified traffic can accumulate to hundreds of Gbps.

The bandwidth used in DDoS attacks is ever increasing. 2014 has already seen a 39% increase in average

[8] http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

[9] Incapsula 2013-2014 DDoS Threat Landscape Report

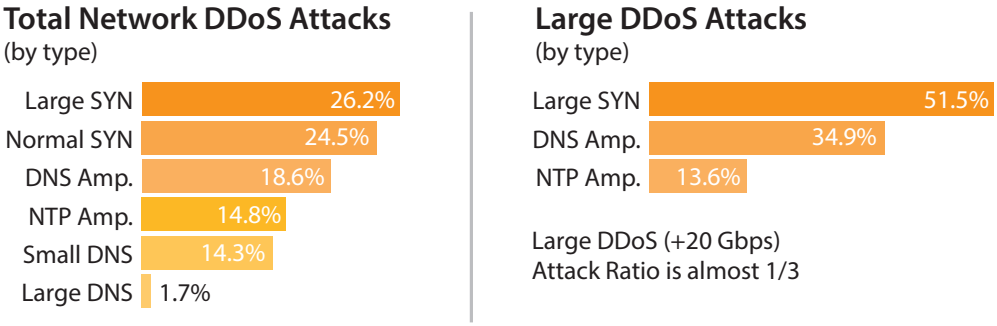


bandwidth and a 35% increase in simple network-layer attacks. Peak traffic is up an astonishing 114%.

Figure 1: Source – Incapsula

Neustar reports that it's not uncommon for attacks to reach 100 Gbps or higher. For example, as of April 2014, the Neustar Security Operations Center has already mitigated more than twice as many 100+ Gbps attacks versus all of last year.

Incapsula decided to include the first quarter of 2014 in its 2013 DDoS report due to the high incidence of newly reported DDoS attacks. As expected, it is seeing the same trends as other DDoS cloud protection providers: Large



size attacks are increasing and account for almost 33% of all DDoS attacks.

Figure 2: Source – Incapsula

Connection Rates: Most Significant Increase

DDoS doesn't just come in the form of massive bandwidth attacks; bots perform a large and growing portion of attacks that use various levels of sophistication to exhaust a service, or the infrastructure of the service. Application-layer attacks are not only identified by their volume, but by their connection behavior. The Slowloris attack, for example, consumes a web server's resources by communicating with it as slowly as possible. Just before a connection times out, it sends another small read request to keep the connection alive. This, of course, is done by a multitude of bots simultaneously, and the web server's resources become so exhausted that it can no longer respond to legitimate requests.

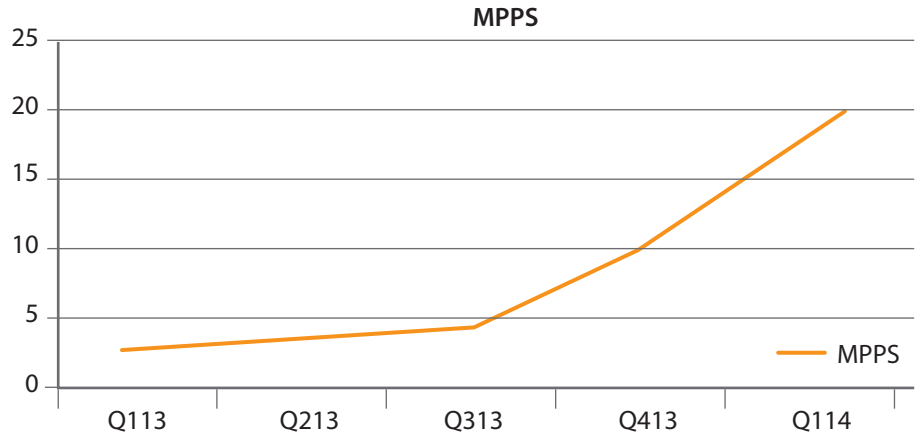
The problem with these large-scale connection rates is often, ironically, the security infrastructure (such as firewalls and intrusion prevention systems) that can also fall victim to resource attacks due to their stateful nature of maintaining session and connection state for each flow. The SYN flood attack, one of the oldest and most prevalent attack types, can be devastating to the stateful security infrastructure, though technically the attack is aimed at exhausting the TCP stack of a node inside the network. More than 50% of large-scale DDoS attacks include a SYN flood component[10]; attacks often consist of both network-layer and application-layer attacks

[10] Incapsula 2013-2014 DDoS Threat Landscape Report

simultaneously, also known as multi-vector attacks.

Because of varying network packet sizes, the packet per second (PPS) rate is the most important metric to use when measuring DDoS attacks, compared to the bandwidth metric that is used in pure volumetric attacks.

Verizon's 2014 Data Breach Investigations Report notes that the mean PPS attack rate is on the rise, increasing 4.5 times compared to 2013. If we carefully extrapolate these numbers, we can expect 37 MPPS in 2014 and 175 MPPS in 2015. These are the mean values to show the trend, but of course this means many higher PPS rates have been seen. For this reason, Prolexic is focusing on the peak values so that network architects can focus on provisioning



networks for the worst case scenario.

Figure 3: Prolexic peak rates

Detection and Mitigation Requirements

As attacks involve high-scale bandwidth, connections and packet rates, you need large-scale power to mitigate them. High-performance, purpose-built hardware can mitigate network-layer attacks very effectively. But as mentioned, DDoS attacks come in many shapes and forms, and are not limited to the network layer. High-performance processors and intelligent software are both required to inspect traffic at the highest packet rates, and then plenty of processing power needs to be available to actually mitigate unwanted traffic. The most effective combination is to leverage dedicated network traffic processors (such as FPGAs) to handle the common network-layer attacks, and also have powerful, multi-core CPUs available for the more complex application-layer attacks. With the clear precedent that the scale of DDoS keeps growing in all directions, plenty of processing headroom is required to prepare your network against future generations of DDoS attacks.

Conclusion

If you are concerned about the possibility of major service outages due to DDoS attacks, you should ensure that your vendor can scale to mitigate the largest multi-vector attacks at your network's edge.

If you want to build a DDoS security infrastructure that can scale to meet the DDoS threats of botnets today and tomorrow, contact A10 Networks® about the A10 Thunder™ TPS product line, the industry's highest performing multi-vector DDoS detection and mitigation solution. Thunder TPS can mitigate the highest PPS rates and bandwidths, and provides various deployment modes and APIs to integrate in any network architecture.

Sources:

Prolexic DDoS reports

www.infosecurity-magazine.com/view/30053/dissection-of-itsoknoproblembro-the-ddos-tool-that-shook-the-banking-world/

www.incapsula.com/images/blog/images/2013-14_ddos_threat_landscape.pdf

http://m.networkworld.com/news/2014/040414-banks-ddos-280425.html?hpg1=bn

http://threatpost.com/volume-of-ntp-amplification-attacks-getting-louder/105763

Verizon Data Breach Investigations Report

http://searchsecurity.techtarget.com/news/2240219793/DDoS-trends-Attackers-vary-DDoS-size-to-cloak-other-attacks?utm_campaign=ssec_security&utm_medium=social&utm_source=twitter&utm_content=1398801110 (Neustar)

www.incapsula.com/blog/cyber-attack-us-banks.html

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-WP-21110-A4-02
Oct 2014

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.

©2014 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, A10 Thunder, Thunder, vThunder, aCloud, ACOS, and aGalaxy are trademarks or registered trademarks of A10 Networks, Inc. in the United States and in other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.