Corero DDoS Trends Report

Q2–Q3 2017

corero

Executive Summary

Organizations around the globe have become increasingly dependent on the Internet as a means to conduct business, and the Internet-connected world has grown more complex due to faster throughput, larger connections, the Internet of Things, and public and private clouds. Simultaneously, **Distributed Denial of Service (DDoS)** threats have become more sophisticated and common.

Internet reliability can come down to a fraction of a second; since its inception, the Internet has been all about availability. When the Internet goes down, businesses that rely on that service go down with it, and DDoS attacks are considered one of the most serious threats to Internet availability today.

Downtime or latency significantly impacts brand reputation and ultimately, revenue. When you combine the frequency and duration of attacks, and the low volume, sub-saturating nature of the threats, victims are faced with a significant security and availability challenge. Automated, real-time mitigation techniques must be in place to eliminate the repercussions of a DDoS attack.

This report contains observations from DDoS attack attempts against Corero customers in Q2 2017 and Q3 2017, as well as comparisons against previous quarters. **The data represents the frequency and sophistication of DDoS attacks that organizations face today.**

KEY TREND

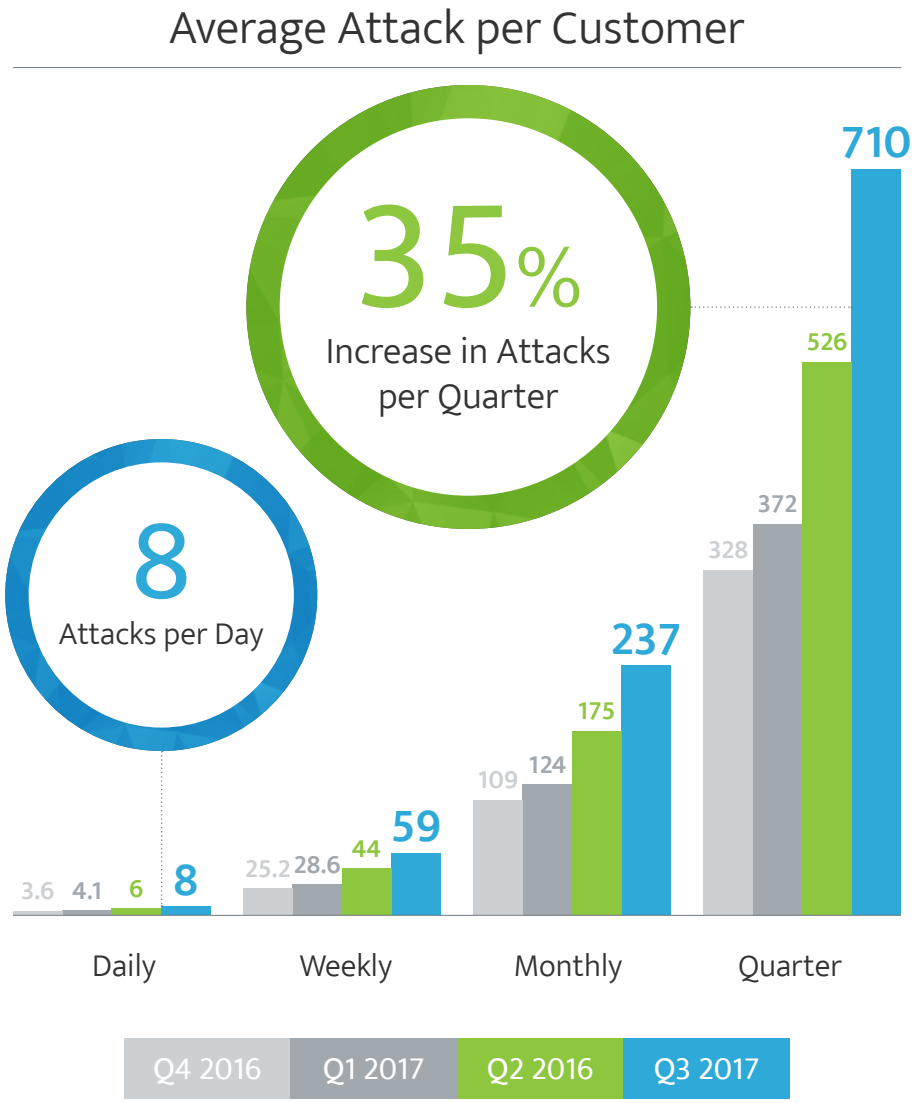
Increase in frequency

We have just passed the one-year anniversary of what many believe to be one of the largest DDoS attacks recorded. Domain Name Service Provider Dyn came under attack by two large and complex DDoS attacks against its managed DNS infrastructure. Because of the attacks, dozens of Internet platforms and services — including major brands such as Twitter, Spotify, Reddit, Netflix and others — felt the significant ripple effect of service outages. Since that incident, other various large-scale DDoS attacks have made national or even global headline news. However, those large-scale attacks are atypical of the types of disruptions that companies suffer from day-to-day.

Frequent, modest-sized, short duration DDoS attacks are the modern-day problem, as they regularly cause the most damage. It's these types of attacks on which businesses should focus.

Corero has observed a jump in the frequency of attack attempts against customers. In the last quarter (Q3 2017), Corero customers experienced an average of 237 attacks per month, an increase of 35% compared to Q2 2017 (175 attacks).

Worryingly, we saw an average of 8 attack attempts per customer, per day in Q3 2017 — double what was observed in Q1 2017.



KEY TREND

Low volume, short duration attacks

While the frequency of attacks is concerning, the size and duration of attacks are also important to call out. Roughly 96 percent of mitigated DDoS attacks were less than 5 Gbps in volume, in both Q2 and Q3 2017.

The average duration of DDoS attacks is also cause for concern. 65 percent of attacks in Q2 2017 lasted 10 minutes or less, and in Q3, 71% percent were 10 minutes or less.

Average Size of DDoS Attacks

SIZE	Q4 2016	Q1 2017	Q2 2017	Q3 2017
<1G	79%	80%	82%	81%
1G–5G	18%	15%	15%	15%
5G–10G	4%	4%	2%	3%
>10G	1%	2%	1%	1%

Average Duration of DDoS Attacks

MINUTES	Q4 2016	Q1 2017	Q2 2017	Q3 2017
0–5	57%	56%	51%	58%
6–10	17%	16%	14%	13%
11–20	7%	6%	13%	11%
21–30	11%	12%	7%	6%
31–60	4%	5%	8%	6%
>60	5%	5%	7%	6%

While attacks lasting 5 minutes or less make up the majority of the attack attempts, we noticed that the attacks lasting 21-30 minutes dropped by 50 percent (Q1 vs Q3).

KEY TREND

Attack Types

Corero has observed a wide range of DDoS attack types over the last two quarters. Two distinct attack types stand out:

1. Sophisticated, multi-vector attacks, aimed to deceive and overrun traditional IT security measures made up a significant portion of the attacks observed this year.
2. Service Flood attacks aim to saturate the bandwidth target victim, resulting in service outages, downtime and latency.

Multi-vector Attacks

20% in Q2 2017 **>** **15%** in Q3 2017

Service Floods

39% in Q2 2017 **<** **41%** in Q3 2017

Cyber-criminals are also switching methods, from simple volumetric attacks to multi-vector DDoS attacks. Modern toolkits can launch both infrastructure-based and application-based DDoS payloads, and attacks include SYN flood, UDP flood, **Domain Name System (DNS)** query flood and GET floods. Attackers are implementing techniques to profile the nature of the target network's security defenses, and utilizing subsequent techniques to implement second or third attacks designed to circumvent an organization's layered protection strategy. Corero has found that multi-vector attack attempts are used regularly (see figure 1) against Corero customers. More frequently, we see Service Flood attacks as shown in figure 2, comprised of TCP or UDP attacks such as SYN flood, ACK flood, Reset flood etc.

Multi-Vector Attack Mitigation

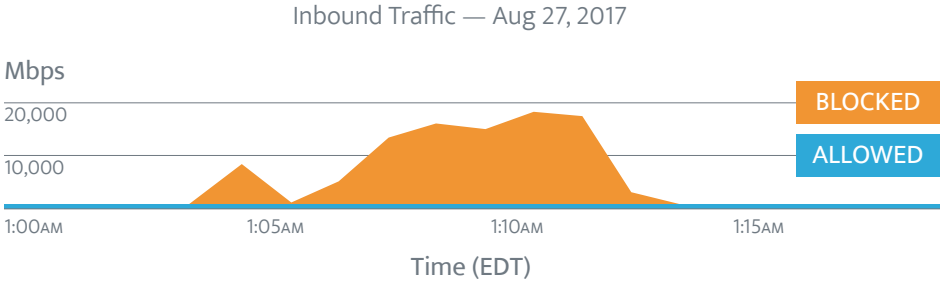


FIGURE 1

Corero SecureWatch® Analytics visualization of a multi-vector attack mitigation. Attack lasting 15 minutes in duration, peaking at 17 Gbps.

Service Flood DDoS Attack Mitigation

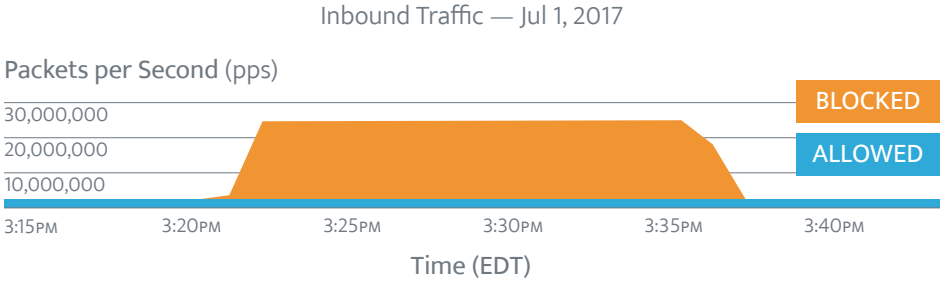


FIGURE 2

Corero SecureWatch® Analytics visualization of a service flood attack mitigation. Attack lasting 15 minutes in duration, peaking at 22.5 million pps.

KEY INSIGHT

RDoS

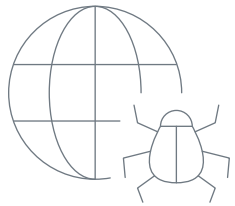
Ransom Denial of Service (RDoS) made a significant comeback in Q3 2017. A widespread wave of RDoS threats from the Phantom Squad hacker group kicked off in September. These threats targeted companies throughout the US, Europe and Asia. **This extortion campaign launched messages demanding Bitcoin payment, with promise to execute attacks on September 30 unless the demands were met.**

Recent examples span across industries — from banking and financial institutions, to hosting providers, online gaming services and SaaS organizations. Unfortunately, most cyber security solutions focus on recovery from criminal extortion attacks, rather than defeating one. DDoS mitigation technology has evolved to deal with these attacks, automatically and instantaneously to eliminate the threat to your business.

KEY INSIGHT

IoT Botnets should be a grave concern

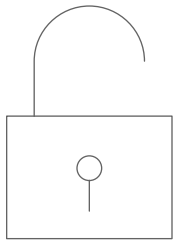
Despite its advantages, the IoT comes with a host of security disadvantages. IoT devices are usually poorly managed, patched and secured; thus they are prime targets for hacker infiltration and takeover. Aside from the personal privacy and security concerns that result from these security gaps, **the bigger danger is that these connected devices can be harnessed by hackers for a variety of nefarious purposes; in many cases hackers use them to form a botnet to carry out DDoS attacks.** The latest IoT botnet plague making headlines is the "Reaper" botnet. Reportedly having infected over a million devices, this botnet is much more dangerous than the Mirai botnet of late last year. It leverages known security flaws in the code of unsecured machines, taking over unsecured IoT devices with the use of hacking tools and then spreading itself further. At the time this paper was authored (Nov 2017) the botnet was in the recruitment phase, and DDoS security experts have yet to see an attack executed with this new powerful bot. The potential scale and power of this botnet has the ability to create Internet chaos and dire results for target victims.



KEY INSIGHT

DDoS distraction; data exfiltration

Once a DDoS attack is underway, security personnel are often distracted by the DDoS traffic, which allows hackers to use whatever means at their disposal to penetrate a network or plant ransomware or malware. **Such attacks are not designed to deny service, but to deny security, by acting as a camouflage that masks more sinister activities — usually data theft and network infiltration.** These attacks act as a diversion tactic, distracting IT teams from the breach that's taking place, which could involve data being exfiltrated, networks being mapped for vulnerabilities, or a whole host of other potential risks.



RECOMMENDATION

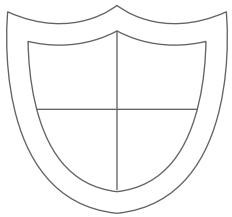
Understand the evolving threat landscape

The DDoS threat landscape will continue to evolve just as it has for the last couple of decades. **We continue to see an increase in attack attempts against our customers quarter over quarter, with some of our customers experiencing thousands of attack attempts per day.** The sophistication of DDoS attacks continues to evolve, with multi-vector attacks being used more often than not. These attacks are used to profile existing security solutions and infrastructure, to probe and determine which vectors and techniques will prove successful. These attacks are also sophisticated enough to leave just enough bandwidth available for other cyber attacks to make their way undetected into the network, past weakened network security layers. There would be little to no trace of these additional attack vectors infiltrating the compromised network, as the initial DDoS had accomplished its purpose of distracting all security resources from performing their intended functions.

RECOMMENDATION

Talk DDoS with your ISP

Organizations that once had DDoS protection projects on the back burner are now re-prioritizing their security strategies to place DDoS mitigation at the forefront. This shift in precedence puts increased pressure on Internet and cloud providers to enable this protection for their customers, and eliminate DDoS threats closer to the source. Providers are now accepting a greater responsibility for defending their customers and networks against DDoS attacks. This approach allows for new security service offerings that protect and increase customer satisfaction.



RECOMMENDATION

Enable real-time threat detection and mitigation mechanisms

To keep up with the growing sophistication and organization of well-equipped and well-funded threat actors, **it's essential that organizations maintain comprehensive visibility and automated mitigation capabilities across their networks to instantly detect and block any potential DDoS attacks as they arise.** Proactive DDoS protection is a critical element in proper cyber security against loss of service availability and data breach activity. The everyday DDoS attack that Corero has highlighted in this report cannot be properly defeated with traditional Internet gateway security solutions such as firewalls, Intrusion Prevention Systems and the like. Similarly, cloud based DDoS scrubbing alternatives cannot achieve successful mitigation with the low volume, short duration attacks that are impacting organizations every day. As organizations develop their DDoS resiliency plans, and choose their methods of DDoS protection, time-to-mitigation must be a critical factor.

Summary

About Corero Network Security

Corero Network Security is the leader in real-time, high-performance DDoS defense solutions. Service providers, hosting providers and digital enterprises rely on Corero's award winning technology to eliminate the DDoS threat to their environment through automatic attack detection and mitigation, coupled with complete network visibility, analytics and reporting. This industry leading technology provides cost effective, scalable protection capabilities against DDoS attacks in the most complex environments while enabling a more cost effective economic model than previously available. For more information, visit www.corero.com.

US Headquarters
225 Cedar Hill Street Suite 337
Marlborough, MA 01752
+1 978-212-1500
info@corero.com

EMEA Headquarters
Regus House, Highbridge, Oxford
Road Uxbridge, England UB8 1HR, UK
+44 (0) 1895-876579