corero

Full Year 2018 DDoS Trends Report

Table of contents

Organizations have become dependent on the Internet as a means to conduct business and deliver consumer/citizen services.

The Internet-connected world has grown more complex due to faster connections, the widespread adoption of Internet of Things (IoT) devices, and cloud services. Simultaneously, **Distributed Denial of Service (DDoS)** threats have become more sophisticated and frequent. Whilst unlawful in many countries, DDoS-for-hire services are commonplace and inexpensive.

Internet resilience can come down to a fraction of a second. 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 can significantly impact brand reputation, customer trust and revenue. Within Europe, the introduction of the GDPR and NIS legislation has significantly increased the risk of punitive fines for cyber-resilience failures.

This report contains observations from DDoS attack attempts against Corero customers in 2018, as well as comparisons against previous years.

The key highlights are:

- Low volume, sub-saturating attacks continue to dominate (98% less than 10Gbps)
- The average number of attacks per customer is up 16% year over year
- The number of attacks over 10Gbps have doubled
- The average attack is becoming even shorter with 81% of attacks lasting less than 10 minutes
- 1 in 5 victims are attacked again within 24 hours of an initial attack

Other notable events within the reporting period included:

The Memcached exploit gained notoriety by smashing the record for the largest DDoS attacks ever reported.

National intelligence and law enforcement agencies took proactive, well publicized measures to take down DDoS-for-hire services.

Governments became increasingly vocal about Nation State sponsored cyber attacks and the threat these pose to critical national infrastructure.

KEY TREND

Attacks per customer up 16% in last 12 months

In February and March 2018, the record for the largest DDoS attacks ever reported was smashed by the 1.3Tbps attack on Github and a subsequent 1.7Tbps attack on an unnamed US-based Service Provider. Both of these attacks and others that followed exploited vulnerable Memcached servers to amplify the attacks to these unprecedented levels. However, those large scale attacks are atypical of the types of disruptions that companies suffer from day-to-day. In this case, much of that vulnerable Memcached infrastructure has now been closed down by its owners, reducing the likelihood of a repeat of such attacks using this particular technique.

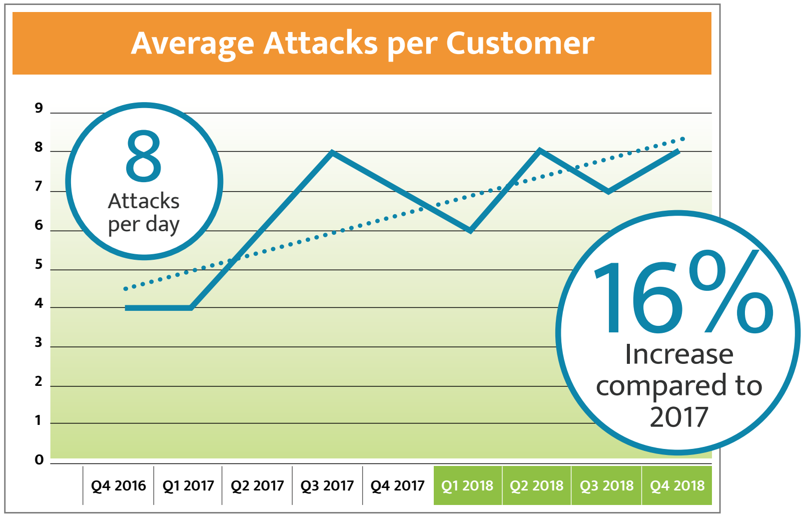
Frequent, modest-sized, short duration attacks are the most common modern-day DDoS problem as they regularly cause damage to more victims. It is these types of attacks that a business is more likely to encounter.

Corero has once again observed a year-over-year increase in the frequency of attack attempts against customers. In the last year, Corero customers experienced an average of 8 attacks per day, an increase of 16% compared to 2017.

> “The average number of attacks per customer in 2018 increased 16% over 2017”

Average Attacks per Customer

	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018	Q2 2018	Q3 2018	Q4 2018
DAILY	4	4	6	8	7	6	8	7	8


Average Attacks per Customer

KEY TREND

Increase in DDoS attacks over 10Gbps

Average Size of DDoS Attacks

SIZE	2015	2016	2017	2018
< 1G	87%	77%	82%	82%
1G - 5G	9%	18%	14%	13%
5G - 10G	3%	4%	3%	3%
> 10G	1%	1%	1%	2%

100%
Increase in DDoS attacks over 10Gbps

> “The percentage of attacks over 10Gbps has doubled in 2018 compared to 2017”

KEY TREND

Low volume, short duration attacks dominate

While the frequency of attacks has increased, the size and duration of attacks remains the primary factor in organizations choosing a DDoS Protection solution. As previously reported, 98% of mitigated DDoS attacks were less than 10Gbps in volume. The vast majority (98%) of mitigated DDoS attacks were less than 10 Gbps in volume.

The continuing trend is that attacks are getting shorter. In 2018, 81% of attacks lasted less than 10 minutes; up from 71% in 2017.

The long-term trend of a reduction in the percentage of attacks over 20 minutes continues with further decline in average duration. In 2018, only 12% of attacks lasted longer than 20 minutes; down from 19% in 2017.

In summary, attacks below 10Gbps and short duration attacks continue to dominate with these attacks trending larger and shorter to evade traditional protection methods.

Average Duration of DDoS Attacks

MINUTES	2015	2016	2017	2018
0 - 5	63%	54%	58%	65%
6 - 10	17%	18%	13%	16%
11 - 20	7%	8%	10%	8%
21 - 30	8%	11%	7%	4%
31 - 60	3%	4%	6%	4%
> 60	2%	5%	6%	4%

81%

Attacks lasted less than 10 minutes

KEY TREND

Probability of repeat attacks

We continue to report on the chance of repeat attacks in this report.

We observed that approximately 60% of DDoS victims did not experience repeat attacks during the 90 day reporting period following the initial attack, suggesting they were one-shot victims.

Within a 90 day window of an attack, the trend is that victims have a 1 in 5 chance (22%) of being attacked again within 24 hours. During the remainder of the 90 day period, the probability of follow-up attacks rises to 1 in 3 (36%).

We have excluded so-called "saw tooth" or "pulse" attacks from this data, which are characterized by attacks which switch-on for, say, 5 minutes and then reappear several minutes later in a similar or mutated form. Corero counts these as a single attack that has presumably been designed to evade traditional redirection to scrubbing center defenses and/or to allow DDoS-for-Hire services to multiplex their attack resources between different attack victims and support more dark web customers paying for DDoS attacks.

Probability of Repeat DDoS Attacks by Elapsed Time

DAYS	2017 Q1	2017 Q2	2017 Q3	2017 Q4	2018 Q1	2018 Q2	Q3 2018	Q4 2018
< 1	25%	23%	23%	22%	20%	21%	22%	23%
2 - 7	9%	8%	9%	8%	7%	7%	7%	6%
8 - 30	4%	8%	7%	7%	6%	6%	5%	5%
31 - 90	2%	4%	3%	3%	3%	3%	2%	2%

> "Victims have a 1 in 5 chance (22%) of being attacked again within 24 hours"

corero

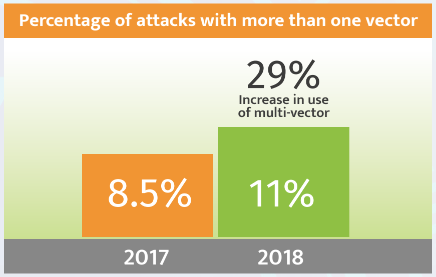
KEY INSIGHT 1

Increase in the use of multi-vector attacks

Multi-Vector vs. Single-Vector Attacks

There is an increase of 29% in the use of multi-vector attacks in 2018 compared to 2017.

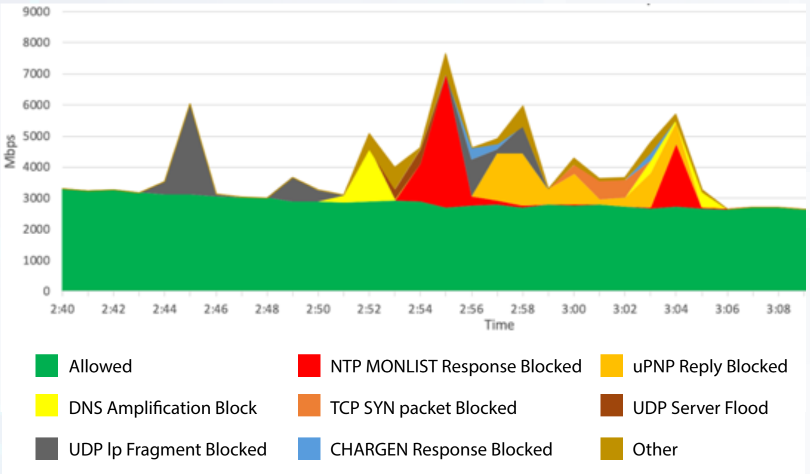
During the reporting period we observed a 16% increase in the use of multi-vector attacks. Multi-vector attacks present several additional challenges for both detection and mitigation for the following reasons.



- For complete mitigation it is necessary to recognize each and every vector and respond with the appropriate mitigation without impacting legitimate traffic.
- Multi-vector attack rates are usually additive in terms of bandwidth and packet rate. The total attack rate will be the sum of vector1 + vector2 + vector3, etc.
- Multi-vector attacks often exhibit more variability in attack rate during the attack period as different vectors join and leave the multi-vector attack. This presents challenges for many traditional detect and redirect DDoS solutions that typically provide partial mitigation capacity. Making a decision on the mitigation method (e.g. redirection vs. blackhole) based on the current attack rate is flawed as it can vary on a minute by minute basis.

Multi-Vector Attack Example

- The most common contributors to multi-vector attacks continue to be volumetric UDP amplification vectors including DNS, NTP, Chargen, SSDP and CLDAP.
- Attackers frequently mix resource exhausting TCP SYN floods from spoofed sources to make tracking more challenging.
- These vectors and more variants are added or subtracted multiple times during a typical 10 minute attack period. The aggregate attack amplitude may vary up to 10X during the attack as vectors surge and fade.



KEY INSIGHT 2

Repeat DDoS attacks continue

Repeat attacks against the same victim (by IP address) continue in 2018 at approximately the same probability reported during the past year, 2017, when measured over time spans of one day, one week, one month and one quarter. DDoS attacks target victims for various reasons.

Whatever the motivation, current data suggests that there is a 22% chance of a repeat attack within 24 hours and a 36% chance of a repeat attack within 90 days.

When combined with the data indicating that the majority of attacks are also less than 10 minutes, these findings call into question the efficacy of traditional detect, redirect and mitigate solutions that may need up to ten minutes or more to initiate mitigation.

Clearly for the vast majority of the attacks described in this report this would be ineffective. The only way to avoid repeat outages as a result of these repeat attacks is to deploy active real-time protection against DDoS that can detect and mitigate in seconds or less.

> “If you are attacked, there is a 22% chance the same IP address will be attacked again in the next 24 hours”

KEY INSIGHT 3

Majority of DDoS attacks do not saturate uplinks

A new insight for this report is the tracking of link saturation by DDoS attacks. Corero analyzed hundreds of thousands of attacks during the period and found that less than 0.6% resulted in one 10G link being saturated, which is judged as more than 95% utilization, also known as “full pipe”.

99.4% of attacks do not reach 95% link saturation levels.

Furthermore, of those 0.6% of attacks that caused a link to reach saturation of 95% utilization, the large majority (>95%) of those saturated attacks lasted less than 10 minutes.

> “99.4% of attacks do not reach 95% link saturation levels”

Attacks That Caused a Link to Reach Saturation

	%
Non Saturation Attacks	99.4%
Link Saturation Attacks	0.6%

KEY INSIGHT 4

DDoS amplification resources are global

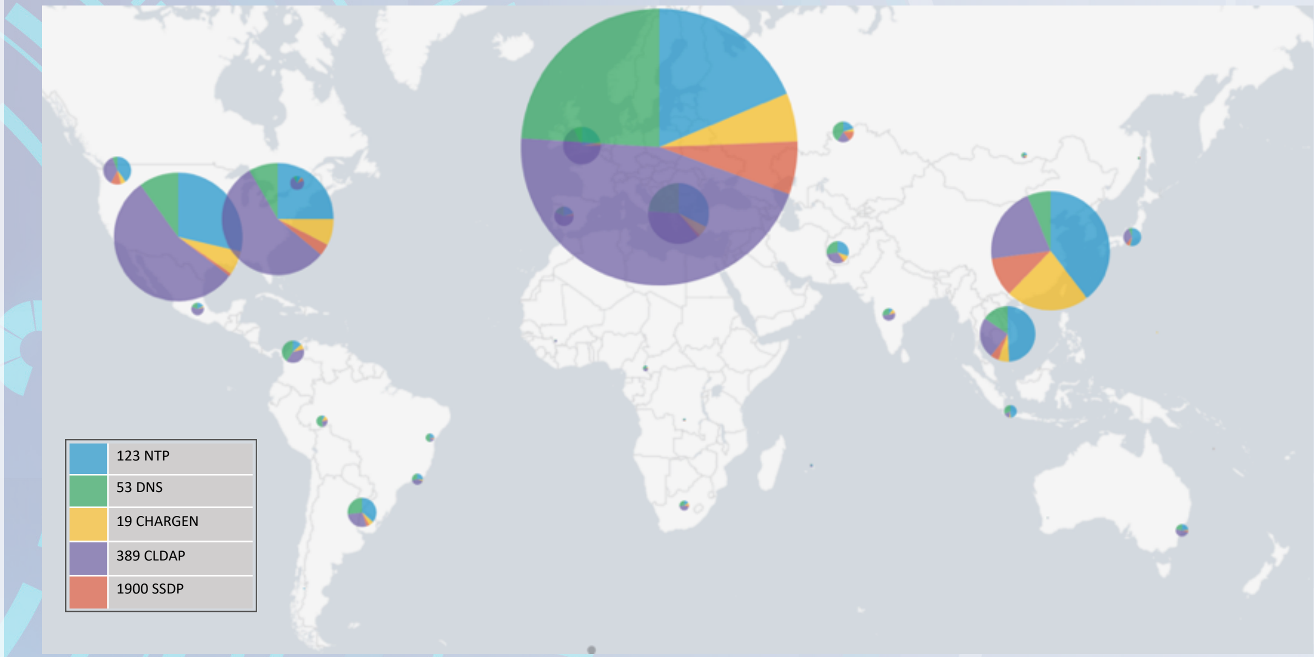
A review of DDoS Amplification sources during 2018 reveals that the availability of vulnerable UDP servers continues to be a worldwide problem.

Different geographies are observed hosting a variety of amplifiers that can be leveraged by DDoS attackers from anywhere in the world. These include open DNS resolvers, monlist NTP servers, Windows CLDAP servers, SSDP/uPnP servers, and CHARGEN servers to name a few.

There is a difference in the mix of available amplifiers but the overall situation appears to indicate every region is still home to a large number of problematic resources.

CLDAP dominated in North America and central Europe while NTP and CHARGEN lead in Asia. NTP is second in the US while DNS takes second place in Europe.

Volume of DDoS attacks by amplification type and geolocation during December 2018



> The overall findings suggest that individual DDoS attack amplification vectors will continue to originate from around the world

KEY INSIGHT 5

Emerging evidence of indiscriminate DDoS attacks

- During the last year we observed evidence of attacks that disrupt larger numbers of victims but exhibit no obvious or specific targeting.

- Questions being asked are:
  - Are the attacks trying to disrupt the Internet in general?
  - Are they broad anti-establishment or anti-nation attacks?
  - Are the attacks spread out over wide ranges to avoid legacy detection techniques?
  - Are the attacks a side effect of increased use of more aggressive scanning tools?
  - Are the observed traffic levels side effects of targeted campaigns causing indirect damage as they are leveraged to attack third parties?

- Interim conclusion:
  - Most likely a mix of several of the above scenarios.

- In November 2018, during an approximate 24 hour period, tens of thousands of IP addresses spanning a wide range of unrelated sites, were observed to be the target of excessive traffic rates from the Internet.

  The suspicious traffic appeared to part of the same event. The traffic levels were sufficiently elevated to cause an unprotected site to suffer a service impact or an outage. It was not possible to account for the number of victims impacted by this incident but it is considered likely that the vast majority of target sites were not explicitly selected.

RECOMMENDATION 1

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 year over year.**

The sophistication of DDoS attacks continues to develop, with multi-vector attacks being used more frequently in the past year. These attacks often present a more challenging detection and mitigation task due to their varying amplitude, ports and protocols.

The average attack is getting shorter with the majority now lasting less than 10 minutes. Real-time detection and mitigation is an essential requirement to provide comprehensive protection.

More targets and therefore victims are being caught up in the malicious activity resulting in DDoS risk to innocent bystanders.

> “The sophistication of DDoS attacks continues to develop, with multi-vector attacks being used more frequently in the past year”

RECOMMENDATION 2

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 also 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 3

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 we have 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 frequent, 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

2018 DDoS Trends

16%
increase in
the average number
of attacks

100%
increase in number
of attacks over
10Gpbs

81%
of attacks last
10 minutes or less

22%
chance of repeat
attack on same victim
within 24 hours

About Corero Network Security

Corero Network Security is a 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, with comprehensive visibility, analytics and reporting. This industry leading technology delivers flexible protection that scales to tens of terabits, with a dramatically lower cost of ownership than previously possible. For more information, visit www.corero.com

Copyright 2019 Corero Network Security, Inc. All rights reserved. 867-5309-003

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

corero