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 Q1 2018 and Q2 2018, as well as comparisons against previous quarters. The key highlights are:

- Low volume, sub-saturating attacks continue to dominate (95% less than 5Gbps)
- The number of attacks is up 40% year-over-year
- Whilst still infrequent, attacks over 10Gbps have doubled
- Attacks are becoming even shorter in duration (82% under 10 minutes)
- 1 in 5 of 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 40% 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. And, in this case, much of that vulnerable Memcached infrastructure has now been closed down by its owners, removing the possibility of a repeat of such attacks using this particular technique.

- 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.

- Worryingly, Corero has observed a year-over-year increase in the frequency of attack attempts against customers. In the last quarter (Q2 2018), Corero customers experienced an average of 8 attacks per day, an increase of 40% compared to Q2 2017 (6 attacks per day).
**KEY TREND**

Low volume, short duration attacks dominate

### Average Duration of DDoS Attacks

<table>
<thead>
<tr>
<th>MINUTES</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018 Q1</th>
<th>2018 Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-5</td>
<td>63%</td>
<td>54%</td>
<td>58%</td>
<td>57%</td>
<td>69%</td>
</tr>
<tr>
<td>6-10</td>
<td>17%</td>
<td>18%</td>
<td>13%</td>
<td>15%</td>
<td>13%</td>
</tr>
<tr>
<td>11-20</td>
<td>7%</td>
<td>8%</td>
<td>10%</td>
<td>12%</td>
<td>7%</td>
</tr>
<tr>
<td>21-30</td>
<td>8%</td>
<td>11%</td>
<td>7%</td>
<td>5%</td>
<td>3%</td>
</tr>
<tr>
<td>31-60</td>
<td>3%</td>
<td>4%</td>
<td>6%</td>
<td>6%</td>
<td>4%</td>
</tr>
<tr>
<td>&gt;60</td>
<td>2%</td>
<td>5%</td>
<td>6%</td>
<td>5%</td>
<td>4%</td>
</tr>
</tbody>
</table>

### Average Size of DDoS Attacks

<table>
<thead>
<tr>
<th>SIZE</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018 Q1</th>
<th>2018 Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1G</td>
<td>87%</td>
<td>77%</td>
<td>82%</td>
<td>77%</td>
<td>85%</td>
</tr>
<tr>
<td>1G-5G</td>
<td>9%</td>
<td>18%</td>
<td>14%</td>
<td>16%</td>
<td>10%</td>
</tr>
<tr>
<td>5G-10G</td>
<td>3%</td>
<td>4%</td>
<td>3%</td>
<td>5%</td>
<td>3%</td>
</tr>
<tr>
<td>&gt;10G</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
<td>2%</td>
</tr>
</tbody>
</table>

**77%** Attacks 10 Minutes or less

**94%** Attacks 5Gbps or less
While the frequency of attacks is concerning, the size and duration of attacks remains the primary concern. Just as we saw in the second half of 2017, in both Q1 and Q2 2018 roughly 95% of mitigated DDoS attacks were less than 5 Gbps in volume.

The principal change is that short duration attacks are getting shorter. In Q2 2018, 82% of attacks lasted less than 10 minutes; up from 71% in 2017. In Q2, we saw a significant change with 69% of attacks lasting less than 5 minutes; markedly up from 58% in 2017 and 57% in Q1.

The long term trend of attacks over 20 minutes being in decline also continued. In Q2, only 11% of attacks lasted longer than 20 minutes; down from 19% in 2017.

Whilst still in the extreme minority, attacks over 10Gbps have “doubled” in the last year from 1% to 2%.

In summary, low volume, short duration attacks continue to dominate with these attacks becoming even shorter.
A new key trend for this version of the report is the probability that victims will suffer from a repeat attack.

While 60% of victims do not experience repeat attacks within 90 days, the long term trend is that victims have a 1 in 5 chance of being attacked again with 24 hours.

We have excluded from this data so-called “saw tooth” or “pulse” attacks 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 which has presumably been designed to evade traditional redirection to scrubbing center defenses and/or to allow DDoS-for-Hire services to multiplex between different attack victims.

the long term trend is that victims have a 1 in 5 chance of being attacked again with 24 hours.
The Memcached reflection vulnerability has been around for longer than 10 years, but the exploit was demonstrated and explained last year at a conference and its usage in the wild ramped up shortly afterwards. Memcached made mainstream news in February and March 2018 as the vector of the largest DDoS attacks ever reported. The attacks were reported as being greater than 1.3 and 1.7 terabits in size, originating from worldwide vulnerable Memcached servers being leveraged as UDP reflection/amplification sources.

Throughout February and March responsible companies scrambled to patch or reconfigure their vulnerable Memcached servers, removing them from the pool being leveraged by the attackers. However, Memcached attacks have continued even after a large percentage of Memcached servers have been secured.

Standalone Memcached attacks still occur as a potent standalone vector while also appearing as part of multi-vector attacks accompanying NTP, DNS and other reflective attacks.

Memcached attacks have continued even after a large percentage of Memcached servers have been secured.
Repeat attacks against the same victim (by IP address) continue in 2018 at the approximately 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 currently a 21% chance of a repeat attack in 24 hours and a 37% 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 detect, redirect and mitigate solutions that may need ten minutes or more to initiate mitigation. The only way to avoid repeat outages from these repeat attacks is to deploy active real-time protection against DDoS that can mitigate in seconds or less.

"The only way to avoid repeat outages from these repeat attacks is to deploy active real-time protection against DDoS"
While governments around the world are cracking down on “darkweb” online DDoS attack websites (known as booter or stresser sites), launching DDoS attacks via third parties continues to be easy and inexpensive.

To counteract the ongoing DDoS threat, Digital Enterprises are increasingly considering DDoS protection a requirement for business continuity.

To maximize the value to their DDoS investment and mitigation effectiveness, the requirement for automated DDoS mitigation is also increasing in importance and manual or human directed mitigation is becoming a last resort effort. This also applies to decisions related to traffic redirection to mitigate attacks.

The time it takes to detect an attack, redirect to a scrubbing center and then manually approve attack vector countermeasures is often longer than most attacks and certainly longer than most servers are able to absorb without a DDoS outage.
Law enforcement agencies around the world are cracking down on the criminals behind DDoS attack services.

In April, Europol supported by the UK National Crime Agency and their Dutch counterparts combined to take-down Webstresser.org. So-called web-stressers have long been suspected as DDoS-for-hire attack services masquerading as a legitimate business.

In May, the US FBI seized an Internet domain allegedly being used by Russian criminals and a botnet of 500,000 hijacked routers. The proactive seizure is believed to have neutralized the threat from this botnet.

Despite these actions, launching DDoS attacks continues to be straightforward and inexpensive. In many jurisdictions, launching a DDoS attack remains a criminal act.

The issue for law enforcement agencies and businesses is that cost of defending against the threat is orders of magnitude more expensive than the cost to launch an attack.
There has been a notable change in tone and rhetoric from governments and government agencies blaming foreign governments and their associates as being the source of cyber-attacks.

In the west, the most frequently cited sources of attacks have been Russia, China, Iran and North Korea.

Whilst these accusations align with the western political narrative, there is plenty of hard evidence to support these assertions including well-publicized DDoS attacks on the Winter Olympics, major banks, energy firms and election infrastructure.

Agencies are also proactively warning of devastating attacks on critical national infrastructure. For example, in January the head of the UK’s National Cyber Security Centre warned that a major cyber-attack on national infrastructure is a matter of “when, not if”.

In May, the FBI somewhat bizarrely warned owners of small office and home routers to power cycle (reboot) the devices citing foreign cyber-actors as having compromised hundreds of thousands of routers worldwide.

"the head of the UK’s National Cyber Security Centre warned that a major cyber-attack on national infrastructure is a matter of “when, not if”"
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 month.

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 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.

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.
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 cybersecurity 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, on-demand 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.
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

H1 2018

- 21% Chance of repeat attack in 24 hours
- 7 Attacks per Customer per Day
- 77% Attacks 10 Minutes or less
- x2 Attacks over 10Gbps has doubled