DDoS Trends and Analysis
QUARTERLY REPORT
Service Providers, hosting providers and the online enterprise are all impacted by the challenges of DDoS attacks. These threats have grown in size, frequency and sophistication in recent years. Not surprisingly, customer expectations for improved service availability and security have risen in unison.

The following report highlights the DDoS trends and analysis derived from Corero’s protected Service Providers, hosting providers and online enterprise customers across the globe. Corero’s state-of-the-art Security Operations Center (SOC), combined with sophisticated DDoS event visibility, analytics and reporting has allowed for a complete picture of the DDoS threats Corero’s protected customers are continually facing. This first edition is intended to highlight the key trends and subsequent analysis of DDoS attack data, and implications for organizations today and in the future.

## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS Attacks are Increasingly Rampant</td>
<td>3</td>
</tr>
<tr>
<td>Duration and Scale: Blink and You’ll Miss It, But the Damage Has Been Done</td>
<td>4</td>
</tr>
<tr>
<td>Multi-Vector and Adaptive DDoS Attack Techniques are Becoming More Common</td>
<td>6</td>
</tr>
<tr>
<td>The Case for Real-Time DDoS Defense</td>
<td>7</td>
</tr>
<tr>
<td>Key Observations and Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
DDoS ATTACKS ARE INCREASINGLY RAMPANT

Today’s DDoS threat landscape is complex and increasingly sophisticated. Opportunistic DDoS attacks remain a menace, but targeted attacks are a rapidly growing threat. Each vertical market reveals variations in the motivations behind DDoS attacks, including cyber terrorism, political or ideological intentions, fraud, ransom, monetary gain, data exfiltration attempts or even for gaining a competitive advantage. The drivers are endless, and the attacks keep coming.

In Q4 2014, Corero customers experienced an average of 3.9 DDoS attack attempts per day, per customer.

One customer in particular, experienced an average of 12 attacks per day across its multi-datacenter environment during the three month time period.

Previous attempts to capture this information by DDoS mitigation vendors have been focused on a cloud only view. While those reports offer very interesting data points about large scale DDoS attacks, they represent only a fraction of DDoS traffic an organization faces on a daily basis.

Service degradation, outages and downtime CAN BE EXPONENTIAL

**3.9 attacks per DAY**

**27 attacks per WEEK**

**117 attacks per MONTH**

**351 attacks per QUARTER**

*Fig 1. Example of one Corero customer, experiencing roughly four attacks per day as depicted with the blue spike in Internet traffic. Yellow lines depict user traffic flowing unimpeded during attack with the Corero SmartWall® Threat Defense System (TDS) for real-time DDoS Defense.*
According to industry research, conducted by the Ponemon Institute, average data center downtime due to a DDoS attack is 86 minutes, and the cost per minute during this downtime is $8,000 USD. With the frequency of attacks observed, and the average outage time being close to 90 minutes; the cost of unplanned outages due to DDoS attacks can be exponential and fiscally damaging to any organization relying on the Internet to conduct business.

**DURATION AND SCALE: BLINK AND YOU’LL MISS IT, BUT THE DAMAGE HAS BEEN DONE**

With significant DDoS attacks making the headlines regularly, many believe that there’s only one type of DDoS attack to worry about—high volume, long duration attacks.

However, the majority of the attacks targeting Corero customers were less than five minutes in duration, with 96% of attacks lasting less than 30 minutes.

These findings highlight a new trend in DDoS attack activity: short bursts of damaging attack traffic versus prolonged events.
These Corero customer data points highlight out the quick hitting DDoS attacks, however there is a second, almost more dangerous trend: partial link saturation attacks. These DDoS attacks do not fully consume the Internet link, nor are they largely volumetric in nature. The danger in partial link saturation attacks is not the ‘denial of service’ as the acronym describes, but the attack itself. The attack is designed to leave just enough bandwidth available for other sophisticated multi-vector attacks with data exfiltration as the main objective, to fly in under the radar, while the distracting DDoS attack consumes resources. In Q4 2014, 87 percent of attack attempts against Corero’s customers were less than 1Gbps in peak bandwidth utilization. While another 10 percent of attacks were between 1-5Gbps.

If these types of DDoS attacks are not mitigated or blocked at the network level they may have gone completely undetected by traditional security solutions.

Organizations looking to out-of-band defenses and anti-DDoS scrubbing-lane approaches for re-routing traffic once an attack has been identified (most often after an outage or service degradation has been experienced) is a game of cat and mouse. Once these short bursts of attack traffic have been identified, engaging a human analyst for intervention is required. The analyst must then decide to enable the transition to the Cloud based anti-DDoS service. The time of detection to the time of mitigation could range to upwards of one hour with this approach to protection. Given the previously mentioned 96% of DDoS attacks lasting 30 minutes or less; by the time your on-demand defenses are engaged the damage has been done. And, not surprisingly the costs associated with this approach are substantial; switching to the Cloud in each instance of a sub saturating, short duration DDoS attack will break the bank.

Of attacks were less than 5Gbps and lasted 6-10 min

13%

Of attacks were less than 1Gbps and lasted 0-5 min

66%

79%

Of attacks were less than 5Gbps and under 10 min in length
MULTI-VECTOR AND ADAPTIVE DDoS ATTACK TECHNIQUES ARE BECOMING MORE COMMON

Many equate DDoS with one type of attack vector – volumetric. It is not surprising, as these high bandwidth-consuming attacks are easier to identify, and defend against with on-premises or cloud based anti-DDoS solutions, or a combination of both. The attack attempts against Corero’s customers in Q4 2014 not only employed brute force multi-vector DDoS attacks, but there was an emerging trend where attackers have implemented more adaptive multi-vector methods to profile the nature of the target network’s security defenses, and subsequently selected a second or third attack designed to circumvent an organization’s layered protection strategy.

While volumetric attacks remain the most common DDoS attack type targeting Corero customers, combination or adaptive attacks are emerging as a new threat vector.

Fig 2. Example of one Corero customer, experiencing a multi-vector DDoS attack event. Pink is SSDP/UPnP reflection, purple (third from top of screen capture) is SYN flood, green is (bottom of the screen capture) is NTP reflection.
THE CASE FOR REAL-TIME DDoS DEFENSE

Given the nature of the highly available networks, precise enforcement of mitigation policies against DDoS attack traffic must be accomplished without incurring false positives, with line-rate performance and maximum security efficacy. On-premises or in-line technology is designed to handle all categories of DDoS attacks in real-time.

DDoS attacks and cyber threats continue to pose a major challenge, more so for service providers given their bandwidth capacity and volume of customers.

In a Hosting Provider environment, in-line DDoS prevention solutions allow providers to offer comprehensive DDoS and cyber threat protection to their hosted customers as an extension of their current service offerings, improving their overall value proposition and providing an opportunity to offer differentiated value added security services.

Internet Service Providers can address the DDoS challenge, protecting their infrastructure and that of their customers with always on, DDoS threat protection and visibility; no longer relying on black-hole routing techniques or scrubbing lanes as a solution.

In an Enterprise deployment, the on-premises DDoS protection is deployed in front of traditional or next generation firewalls, IPS, ADC and other IT security infrastructure devices, preventing access to the network by untrusted and unwanted attack traffic, enhancing Enterprise networks risk profile and reducing service outages on their web properties as a result of a DDoS attack.

---

<table>
<thead>
<tr>
<th>DDoS ATTACKS &amp; TECHNIQUES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Level DDoS</strong></td>
</tr>
<tr>
<td>SYN, TCP, UDP, ICMP Floods</td>
</tr>
<tr>
<td><strong>Reflective Amplified DDoS</strong></td>
</tr>
<tr>
<td>DNS, NTP, SNMP, QOTD Floods</td>
</tr>
<tr>
<td><strong>Fragmented Packet DDoS</strong></td>
</tr>
<tr>
<td>Overlapping, Missing, Too Many</td>
</tr>
<tr>
<td><strong>Application Layer DDoS</strong></td>
</tr>
<tr>
<td>HTTP GET/POST Floods, App Scripts</td>
</tr>
<tr>
<td><strong>Exhaustion DDoS</strong></td>
</tr>
<tr>
<td>Low &amp; Slow Reads, Too Many Connections</td>
</tr>
</tbody>
</table>
1 **CORERO CUSTOMERS ARE EXPERIENCING AN AVERAGE OF 3.9 DDoS ATTACKS PER DAY.**
Protecting against these frequent attacks requires protection at the very edge of your network or peering points. Detection, analysis and mitigation of attacks before entering your network is necessary in order to maintain service availability while experiencing DDoS attack activity. Deploying technology that detects analyzes and responds to DDoS attacks by inspecting raw Internet traffic, at line rate and identifying the threat within the first few packets of any given attack is the recommendation. In addition to comprehensive DDoS protection the solution must offer a do-no-harm approach, allowing good user traffic to flow uninterrupted, while attack traffic is immediately blocked; false positives cannot be tolerated.

2 **79% OF DDoS ATTACKS TARGETING CORERO CUSTOMERS PEAK AT 5GBPS, AND LAST LESS THEN 10 MINUTES IN DURATION.**
In order to properly defeat these sub saturating, short bursts of DDoS attack activity, organizations cannot rely on cloud based scrubbing solutions, or black-hole routing as a solution for proper defense. With real-time protection and visibility into the DDoS attack traffic targeting the network, the Internet connected business can better protect themselves against the onslaught of DDoS attacks aiming to degrade or completely take down Internet services. Including Short duration, small bandwidth attacks, not visible to cloud based anti-DDoS services.

3 **MULTI-VECTOR AND ADAPTIVE DDoS ATTACKS ARE EMERGING AS A SIGNIFICANT THREAT.**
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. To defeat these sophisticated attacks, real-time analysis is required to determine the need to customize detection filters and block the attack immediately. To defeat these sophisticated attacks, sophisticated analysis is required to determine the need for customizing detection filters and blocking the attack immediately.
Corero Network Security is dedicated to improving the security of the Internet through the deployment of its innovative First Line of Defense® DDoS protection solutions. The Corero SmartWall® Threat Defense System (TDS) provides organizations with real-time protection against a continuously evolving spectrum of DDoS attacks that have the potential to impact any Internet connected business. Corero provides the opportunity to enhance defense-in-depth security architectures with an important additional layer of security capable of inspecting traffic arriving from the Internet and alerting and or blocking attack traffic before it impacts your environment.

Corero solutions are designed to be always on providing automatic attack mitigation with continuous threat visibility and network forensics.

Award-winning DDoS protection products and services from Corero are securing hosting providers, service providers and online enterprises around the world, allowing them to guarantee accessibility and ensure business success. In addition to the Corero on-premises appliances, the Corero SecureWatch® Service offers our customers 24/7 security monitoring and access to the Corero SOC staffed by experts in the mitigation of sophisticated cyber-attacks.