corero

2020

DDoS THREAT INTELLIGENCE REPORT

Table of Contents

Executive Summary

Organizations around the world depend on the Internet now more than ever to conduct business and deliver services.

This Internet-first world grows more complex each year due to the demand for faster connections, 5G, Internet of Things (IoT), and cloud services. Distributed Denial of Service (DDoS) threats are growing in sophistication, size, and frequency. Each year, we see a rising number of total recorded attacks.

Service Providers and Hosting Providers are increasingly expected to assume the responsibility for upholding their customer's Internet availability. Real-time DDoS protection has become more critical now than ever before. Unfortunately, DDoS-for-hire services, that make it cheap and easy to launch attacks, have become increasingly common. Expectations for Internet response and resilience come down to seconds not minutes. When the Internet goes down, organizations that rely on Internet service go down with it.

DDoS attacks are considered one of the most serious yet most common threats to Internet availability.

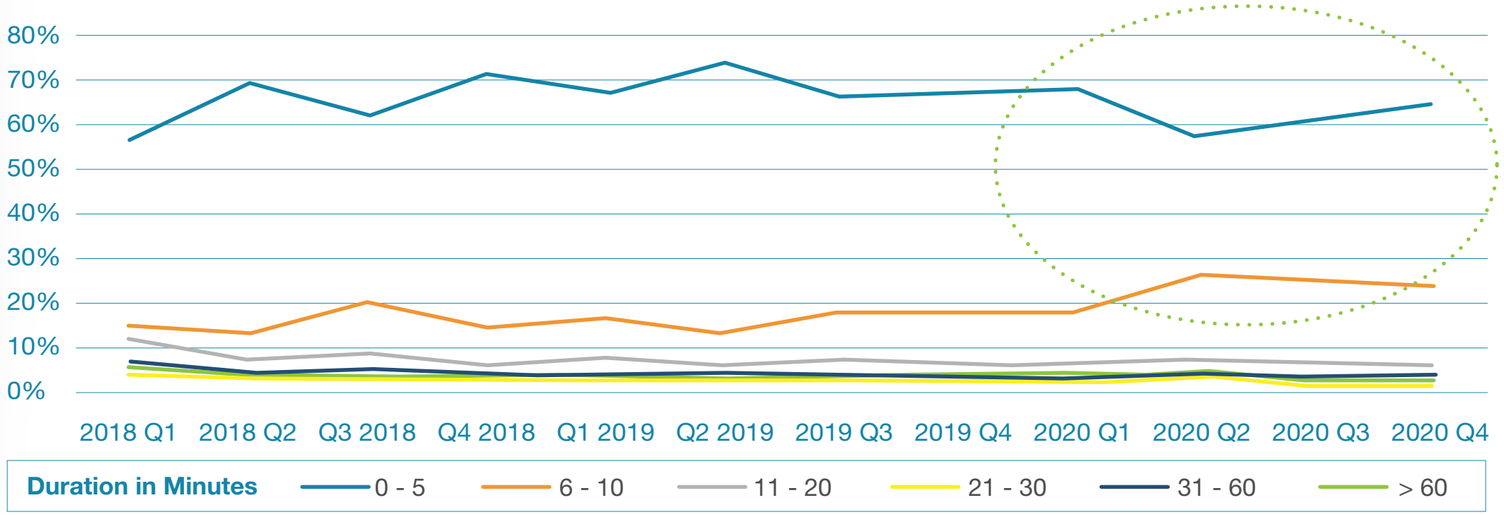
Downtime and Internet disruption can damage brand reputation, customer trust and revenue. This report contains observations from DDoS attacks against Corero customers in 2020, as well as comparisons against previous years. Once again we are reporting a net increase in the number of unique DDoS attack vectors seen in the wild and in the level of year-over-year DDoS activity. Awareness and prevention are not practical countermeasures for DDoS. Detection-and-mitigation continues to be the best defense.

Key Trend

01

Increase in Shorter Duration Attacks

Average Duration of DDoS Attacks



86%
of Attacks
<10 mins

If there is a problem that goes on for just a few minutes there is quite a good chance that it will fly by under the radar, making short duration attacks dangerous. Those quick little glitches in the performance of systems are often unnoticed by security teams, which allows cybercriminals to test for vulnerabilities within the network. Even a few minutes of downtime can prove extremely costly for lost revenue, reduced customer confidence, and overall reputation damage.

With such significant, and easily calculable, revenue at risk for every minute of downtime, organizations need to ensure they have the right security measures in place, which can identify and mitigate even small and low-volume DDoS threats before damage is done. Corero reports that customers face an average of 9 attacks per day, a 13% increase from last year.

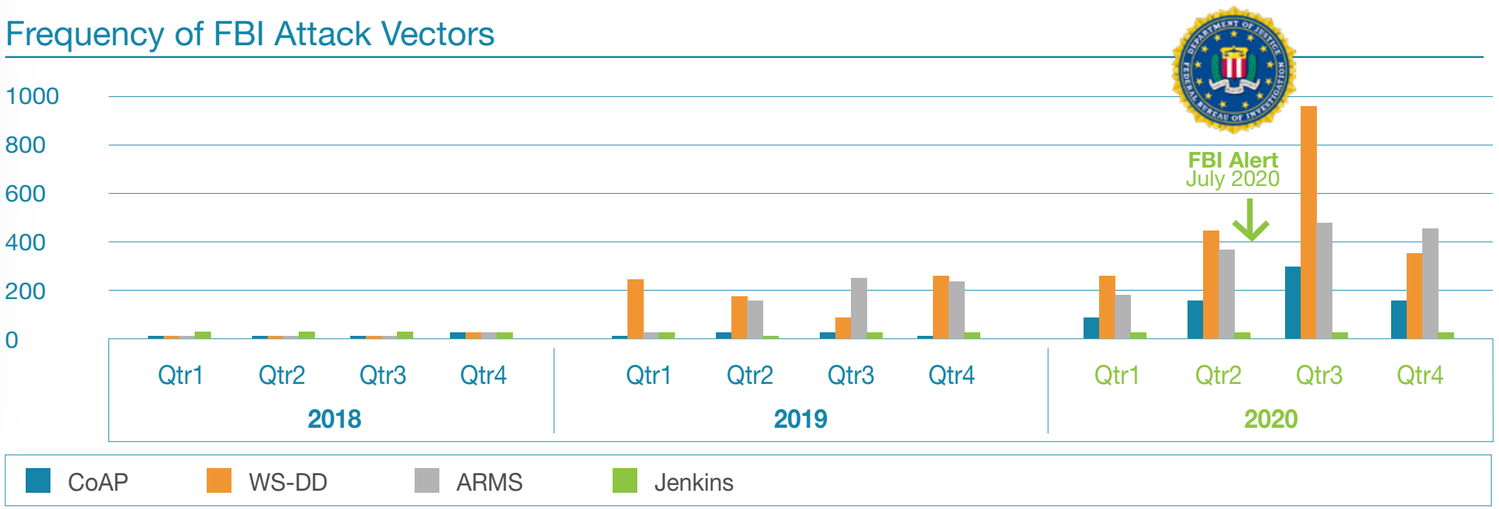
Key Trend

02

New Attack Vectors are Inevitable but not Preventable

New attack vectors are being discovered all the time. As their existence becomes known, more and more booter/stresser services include these vectors in their DDOS-for-hire attack suites. This leads to an increasing presence of the new attack vectors in the wild.

Frequency of FBI Attack Vectors



Awareness and prevention alone are not practical countermeasures for DDoS.

In July 2020 the FBI alerted private industry about 4 new DDoS attack vectors. However, our Threat Intelligence data shows they had already been active in the wild for at least the prior 12 months and despite the mid-year FBI warning their use continued to grow in the remainder of 2020. This demonstrates that awareness and prevention are not practical countermeasures for DDoS. Detection and mitigation continues to be the best defense as illustrated by the zero-day protection provided against these attacks for Corero customers.

FBI reference:

https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/fbi-private-industry-notification-20200721-002.pdf

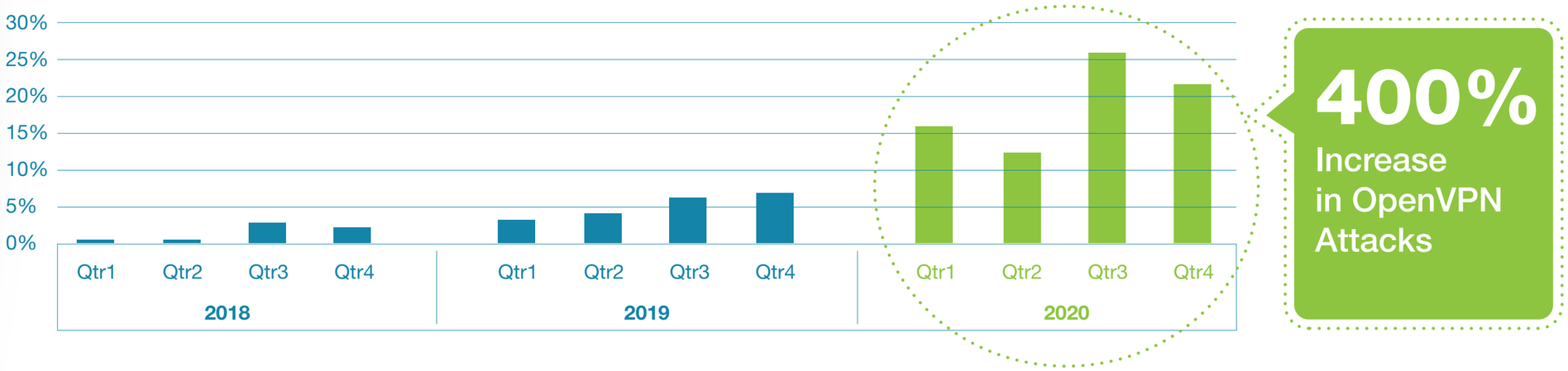
Key Trend

03

Increase in OpenVPN Attacks

With businesses continuing to encourage employees to work from home during the COVID-19 pandemic, Corero has seen a year-over-year increase of nearly 400% in the use of OpenVPN reflections as an attack vector.

Frequency of OpenVPN Attacks



OpenVPN as a reflection DDoS vector is bad news for the victim being attacked but, also for the organization whose OpenVPN infrastructure is being used to launch the attack as their remote workers will suffer from a degraded, or possibly unusable, service, impacting productivity and, potentially, business continuity.

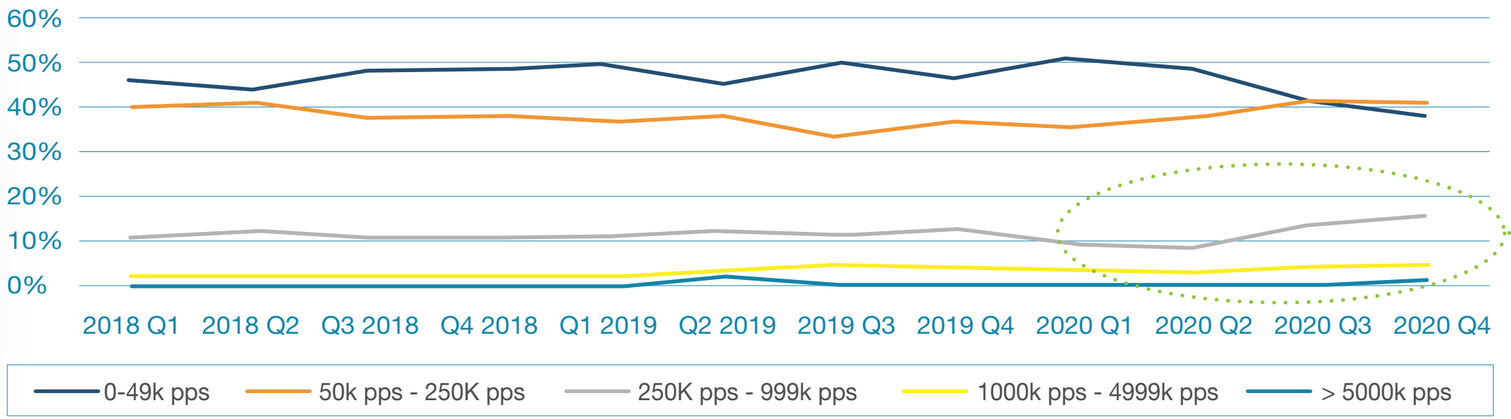
Key Trend

04

High Packet Rate Attacks on the Rise

Increases in higher packet rates suggests a focus on state exhaustion, rather than saturation, type attacks.

Average Packet Rate of DDoS Attacks (pps)



17%
Increase in High Packet Rate Attacks

These smaller attacks are a cause for concern. Even though they are sub-saturating and don't steal as much bandwidth on their own, the impact due to the increased frequency of such DDoS packets hitting a network can still be costly, in terms of network infrastructure downtime and maintenance. Additionally, reputations are at stake here, as we've previously reported, many organizations are under the impression that their providers are already protecting them from such attacks.

Small attacks that Corero has been seeing can easily take down a company's firewall in a matter of seconds, either blocking the flow of legitimate traffic or, possibly worse, leaving the network wide-open to infiltration, mapping, malware, or stealing of sensitive data. Clearly, this has the potential to be much more damaging than taking a website or service offline.

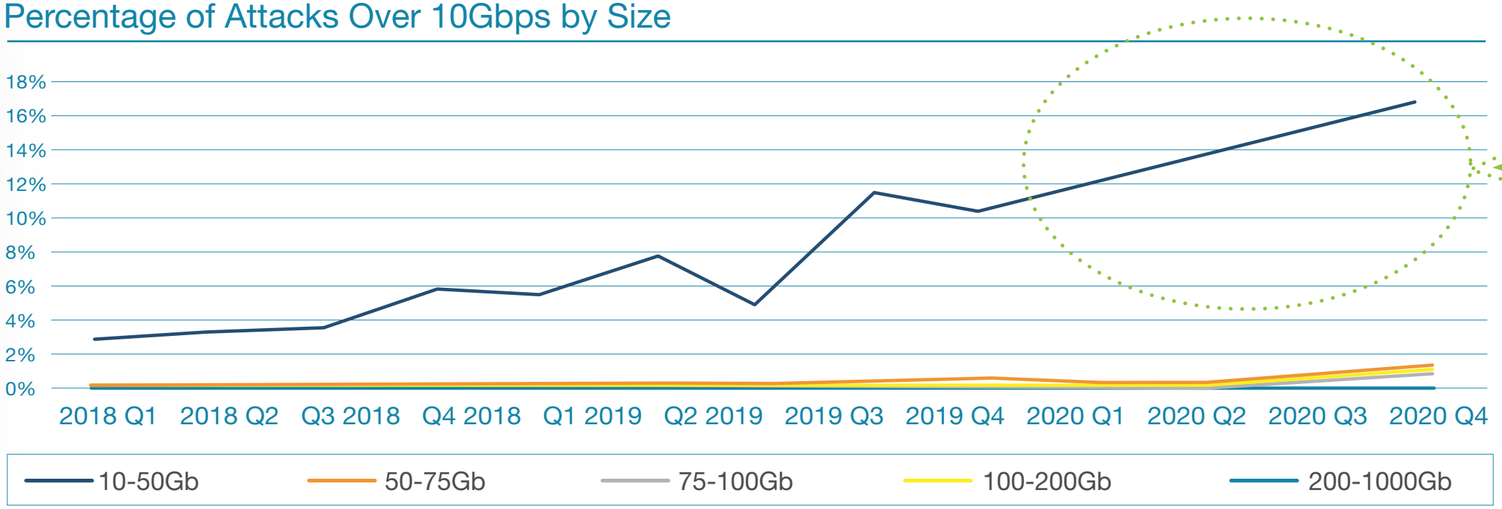
Key Trend

05

Increase in Attacks over 10Gbps

Suggests the increasing shift to 100Gbps Internet connectivity is accompanied by a trend indicating more everyday DDoS attacks to be larger than for 10G.

Percentage of Attacks Over 10Gbps by Size



70%
Growth in Attacks over 10Gbps

While the frequency of attacks has increased, their small size and duration continues to demonstrate why organizations must invest in real-time, automatic DDoS Protection. As consistently reported, the vast majority (98%) of mitigated DDoS attacks are still less than 10Gbps in volume.

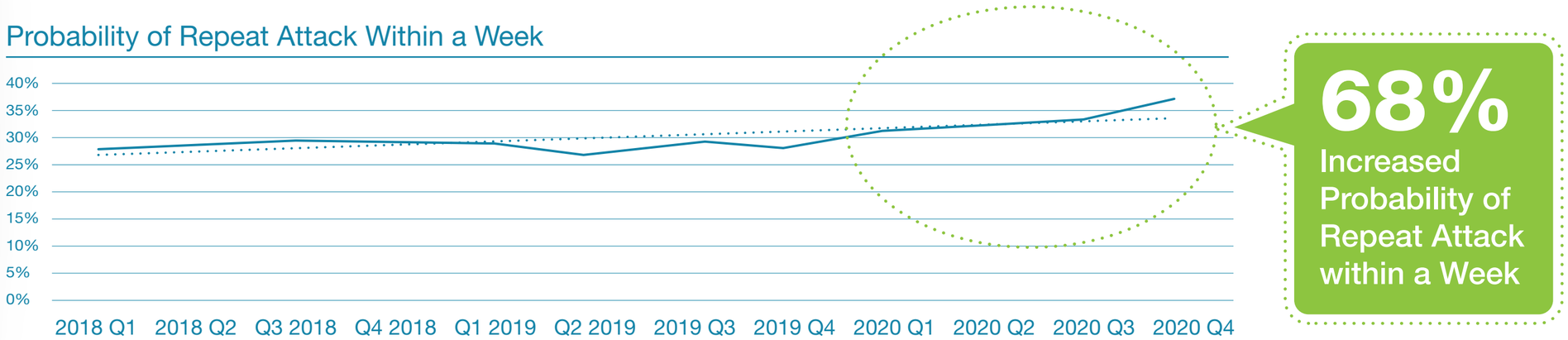
In summary, smaller attacks, below 10Gbps, and those of short duration continue to dominate. These attacks are particularly difficult to detect and mitigate with manual and legacy systems.

Key Trend

06

Increased Chance of Repeat Attack

The probability of a repeat DDoS attack within a 7-day span has increased noticeably since 2019.



The only way to avoid repeat outages as a result of these attacks is to deploy active real-time protection against DDoS that can detect and mitigate in seconds or less.

We have excluded so-called “saw tooth” or “pulse” attacks from this data, which are characterized by attacks which switch-on for sometimes just a few minutes and then reappear several minutes later in a similar or mutated form.

Corero counts these as a single attack scenario 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 victims and support more dark web customers paying for DDoS attacks.

Key Insight

Don’t Pay for Downtime

If your DDoS protection system takes minutes to respond then it will not detect and block the majority of attacks, 86% of which lasted less than 10 minutes. This is potential downtime for your business.

DDoS attacks have become harder to detect and mitigate as they are increasing in frequency and sophistication. In today’s online world, even seconds of downtime can cost an organization thousands of dollars and tarnish brand reputation. The only way to ensure business continuity when faced with the growing threat of attacks, is by investing in a real-time, always-on DDoS detection and mitigation solution.

There are a variety of protection options available, on-premises, in the cloud or a combination of the two commonly referred to as hybrid DDoS protection. However, be sure to assess your risk tolerance and that of your customers. If any amount of downtime cannot be tolerated, you should invest in an always-on solution. Like many organizations, even a minute of downtime is too much. Relying on a cloud solution alone can disrupt Internet availability. Many cloud services advertise “always-on” however, that often means just always-routed through their cloud, it does not mean you are always protected, resulting in additional delays for time-to-mitigation that may still be measured in minutes.

For the best of both worlds, consider investing in a hybrid solution that combines your existing Cloud-based DDoS protection with on-premises DDoS detection and mitigation. These hybrid solutions will handle the vast majority of attacks locally in real-time without requiring your traffic to be redirected to the cloud.

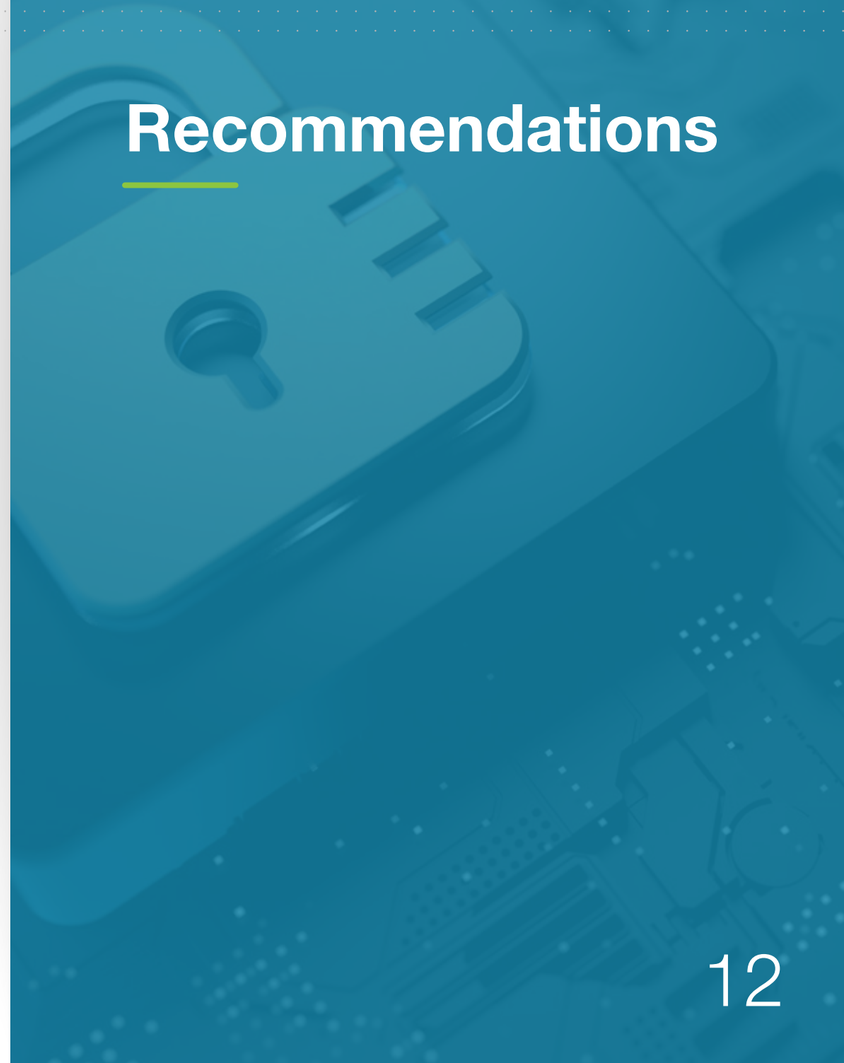
Key Insight

Majority of DDoS Attacks Do Not Saturate Uplinks

With a 2020 estimate that 99% of observed attacks are coming in below link saturation there is a real opportunity to detect and block many DDoS attacks in real time without requiring expensive and time consuming traffic redirection to cloud solutions.

This means that most attacks can be addressed by on-premises solutions without the disruption, risk or cost of re-routing customer traffic across the Internet to third party cloud scrubbing centers.

Recommendations



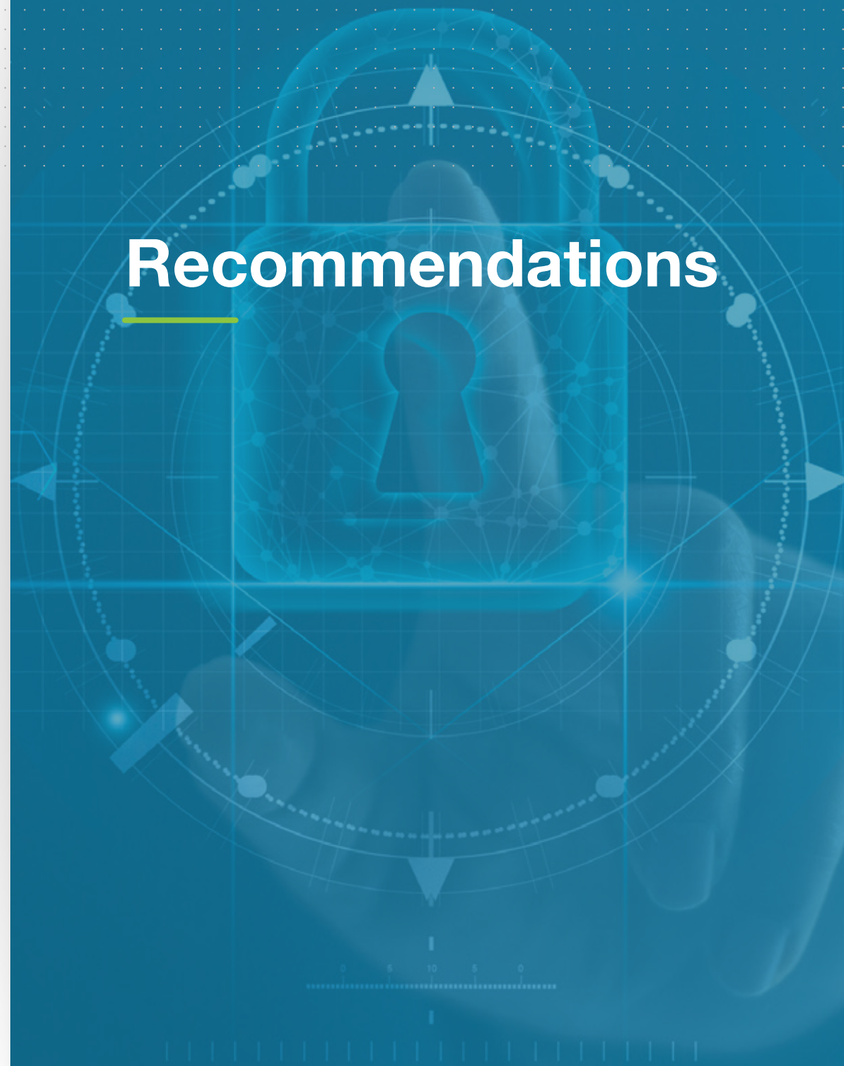
Why 2021 is the year to invest in real-time, always-on DDoS protection

A decade long trend tells us that DDoS attacks and threats are not going away anytime soon and your organization, along with your customers, are at significant risk of unwanted downtime without real-time, always-on DDoS protection in place.

Once again we are reporting a net increase in the number of unique DDoS attack vectors seen in the wild and in the level of year-over-year DDoS activity. The specific example of the mid-year FBI alert regarding the malicious use of built-in network protocols for DDoS attacks demonstrates that new vectors are inevitable and not preventable and that awareness and prevention are not practical countermeasures for DDoS. These exploits were already being used in attacks before the FBI alert and their use continues to grow to this day. Detection and mitigation continues to be the best defense.

As hackers continue to find new vectors to launch assaults on organizations, the best defense against potential downtime is to utilize real-time protection. Traditional solutions which detect and redirect traffic, often result in downtime. These on-demand cloud-based scrubbing services cannot practically mitigate the short, frequent attacks that many of our customers face. As organizations plan their strategy for effective DDoS protection, the relationship between time-to-mitigation and potential downtime is a vital consideration.

Recommendations



The majority of attacks are less than 10 minutes, these findings present the question of the efficacy of traditional detect, redirect and mitigate solutions that may need up to ten minutes or more to begin protecting.

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.

Hybrid Protection

Depending on your risk tolerance in regard to business continuity, you should consider enhancing existing Cloud-based DDoS protection with on-premises DDoS detection and mitigation to create a hybrid solution. This hybrid solution will handle the majority of attacks in real time without swinging attack traffic to the cloud.

Cloud-based mitigation is needed to defend against DDoS attacks that are larger than your bandwidth. With that being said, on-demand cloud mitigation can never be truly real-time, so it cannot deliver protection without downtime. This can be from minutes, to tens-of- minutes, depending on the provider. Corero research continues to show that most DDoS attacks are short (less than ten minutes) and sub-saturating (less than 1Gbps) and are on the rise. Organizations must take into account that the typical time to swing traffic to cloud DDoS protection means the attack is often already over and the damage may be done.

The benefit of a hybrid DDoS protection approach is that the on-premises solution will significantly reduce the number of times an organization is faced with engaging cloud protection. This lowers costs for the entire organization, and keeps you protected while delivering a real-time, comprehensive and consistent form of defense. Hybrid protection ensures that during the minutes, and sometimes even tens of minutes, that the cloud service is engaging, the attack will still be stopped by the on-premises solution.

Prediction 01

DDoS Considerations for the Digital Transformation journey.

Postpone protection at your peril.

While the increasingly popular and necessary Digital Transformation trend does not explicitly imply the use of public Internet services, it is common for corporations to take advantage of online services that can automate the solution of business problems and improve the competitiveness of their offerings in the marketplace. For this reason it is important to recognize the need for a robust cyber-security posture to protect these newly transformed business processes. A key cyber-defense component of any Internet accessible business should be DDoS protection.

Corporations that have previously relied upon traditional security techniques, maybe even physical security or personal recognizance, to protect their assets or transactions are now presented with a wide range of unseen shadowy virtual threats. For these reasons it is especially important to specify DDoS protection as an attribute of any new networks, services, or customer engagement products that are used by the newly transformed business.

However, it is inevitable that with the high volume of businesses making this transition, coupled with the rush to deliver results, DDoS protection will be delayed or worse still be forgotten. This will lead to unexpected impacts to transformed commercial businesses, institutions, or critical infrastructure.

To learn more about mitigating DDoS risk on the road to Digital Transformation, download our report powered by analyst firms Omnisperience & SynergySix Degrees:
The Need for Always-On, Real-Time DDoS Security Solutions

Prediction 02

5G & IoT

Fuel for the Fire, expect new DDoS attack vectors to spread in the wild.

The groundbreaking deployments of 5G and IoT based networks are pushing the frontier of edge-oriented communications, data collection and compute. The increased bandwidth needed to support these advances creates favorable economics for Internet offload as close to the edge as possible. While this alleviates cost and congestion in back-haul networks and reduces latency, it also multiplies the number of Internet access points by several orders of magnitude, sometimes requiring growth from a handful of transit/peering points to tens even hundreds of locations, closer to the edge. These locations are also new DDoS entry points, bypassing legacy core DDoS protection mechanisms.

At the same time, the new 5G & IoT communities of connected and capable devices such as sensors or smart phones are green fields for bot herding and DDoS exploitation.

It will be challenging to keep pace with the malicious actors seeking to create potentially harmful botnets from these resources unless the industry simultaneously deploys the necessary cyber security controls. We would be wise to expect DDoS disruption on this new frontier until the roll out of DDoS detection and mitigation solutions can catch up.

86%
of Attacks <10 Mins

New Attack Vectors are Inevitable but not Preventable

400%
Increase in OpenVPN Attacks

2020 DDoS Trends Summary

17%
Increase in High Packet Rate Attacks

70%
Increase in Attacks Over 10Gbps

68%
Increase in Chance of Repeat Attack within a Week

Ready to learn more?

Visit Website

Schedule a Demo

Corero Network Security is a global leader in real-time, high-performance, automatic DDoS defense solutions. Service and Hosting providers, alongside digital enterprises across the globe rely on Corero's award winning cybersecurity technology to eliminate the threat of Distributed Denial of Service (DDoS) to their digital environment through automatic attack detection and mitigation, coupled with network visibility, analytics and reporting.

Corero's industry leading SmartWall and SecureWatch technology provides scalable protection capabilities against external DDoS attackers and internal DDoS botnets in the most complex edge and subscriber environments, while enabling a more cost-effective economic model than previously available. Corero's key operational centers are located in Marlborough, Massachusetts, USA and Edinburgh, UK, with the Company headquarters in Amersham, UK. The Company is also listed on the London Stock Exchange's AIM market under the ticker CNS.L.

For more information, visit **www.corero.com**, and follow us on LinkedIn and Twitter.

US HEADQUARTERS

Corero Network Security Inc.
293 Boston Post Road West, Suite 310
Marlborough, MA 01752
Tel: +1 978 212 1500
Email: info@corero.com

EMEA HEADQUARTERS

Corero Network Security (UK) Ltd.
St Mary's Court, The Broadway,
Amersham, Buckinghamshire, HP7 0UT, UK
Tel: +44 (0) 1494 590404
Email: info_uk@corero.com