corero

2021

DDoS THREAT INTELLIGENCE REPORT

Table of Contents

Executive Summary

The internet is integral to organizations' operations and it is relied on to conduct business and deliver services. As consumers we are dependent on the internet now more than ever - and we expect an always-on, accessible-anywhere service.

This Internet-first world is growing more complex each year with faster connections, new technologies like 5G and 6G, Internet of Things (IoT), and the expansion of cloud services. The entire threat landscape is also changing. As the DDoS (Distributed Denial of Service) attack surface grows, we're seeing these cyber attacks grow in frequency and sophistication. As experts in DDoS protection, Corero has seen rising numbers of recorded attacks as well as significant shifts in attackers' motives and goals.

Service Providers and Hosting Providers are central to the internet-providing eco system and are increasingly expected to be responsible for maintaining their customers' Internet availability. For them, protection against real-time DDoS attacks is critically important - when the Internet goes down, the organizations that rely on Internet service go down with it. Expectations for Internet response and resilience come down to seconds; not minutes.

DDoS attacks are one of the favorite tools of today's cyber criminals - 'DDoS-for-hire' services make it cheap and easy to launch attacks.

Downtime and Internet disruption have a direct affect on revenue and customer loyalty and trust.

This report contains data and observations from DDoS attacks against Corero customers in 2021 and the first Quarter of 2022 with comparisons against previous years. We are seeing 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. Our take-away is that awareness and prevention tools are not practical countermeasures for today's DDoS threat. Fast-acting, real-time automatic detection and mitigation continue to be the best line of defense.

2021 DDoS Trends Summary

82%
of Attacks last less than 10 minutes

29%
Increase in number of attacks per day*

297%
Increase in openVPN Attacks**

97%
Attacks are less than 10 Gbps

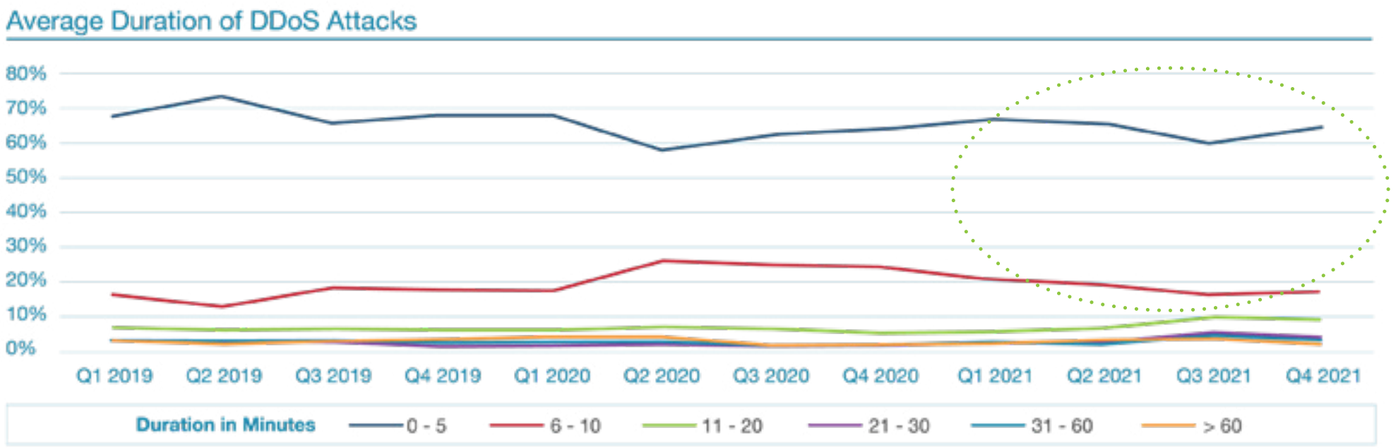
29%
Likelihood of a repeat attack within a week

** Corero reports that our Service Provider and Hosting Provider customers face an average of 11 attacks per day, an increase of 29% from last year.*
*** since Q1 2019; at the start of the COVID-19 pandemic*

Key Trend

01

Short Duration DDoS Attacks Dominate



86%
of Attacks
<10 mins

The greatest DDoS risk to organizations is a barrage of short duration, low volume attacks. Here, the damage is often done before the attack is even reported and can go unnoticed by security teams. Cybercriminals are known to use these shorter attacks to experiment and test for vulnerabilities within a network, looking for opportunities for further follow-up. Corero has observed that 82 % of attacks last less than 10 minutes with a 29% likelihood of a repeat attack occurring after the initial one has taken place.

Even a few minutes of downtime can prove costly with lost revenue, reduced customer confidence, increased customer churn, and overall reputation damage. While shorter duration, sub-saturating DDoS attacks don't grab headlines like larger ones, they can be damaging enough to knock a firewall or intrusion prevention (IPS) system offline, potentially allowing hackers to infiltrate networks and do further damage.

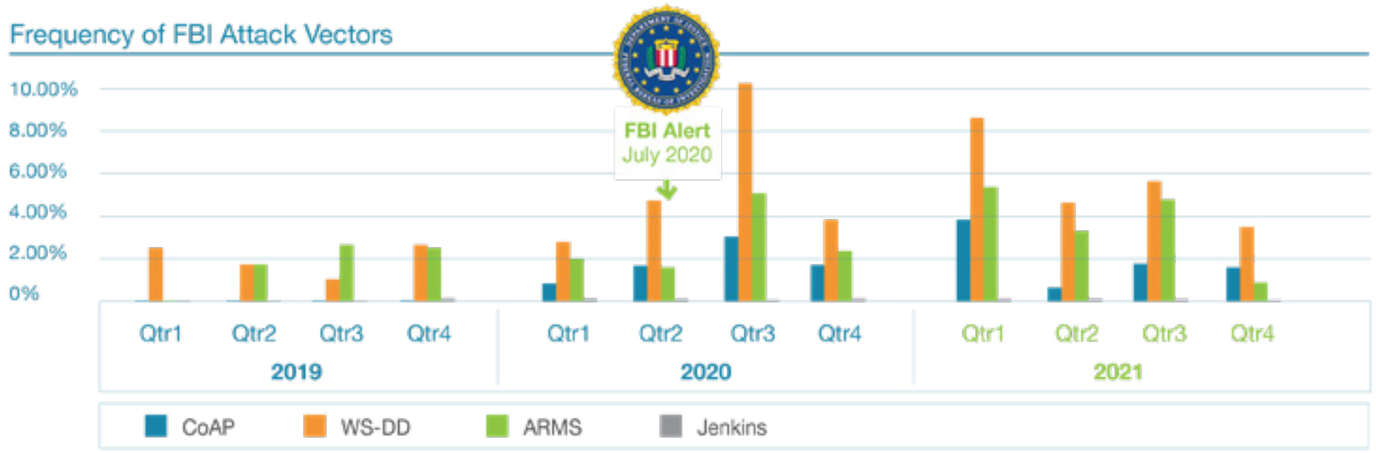
It is important that organizations have appropriate security measures in place to identify and mitigate these short, low-volume DDoS attacks before damage can be done. Corero reports that our Service Provider and Hosting Provider customers face an average of 11 attacks per day, an increase of 29% from last year.

Key Trend

02

New Attack Vectors are Inevitable

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.



Awareness alone is not a practical countermeasure against DDoS attacks. A zero-day solution is required to mitigate the ongoing risk.

In July 2020 the FBI alerted private industry to 4 new DDoS attack vectors. However, Corero Threat Intelligence data found that these vectors had already been active in the wild for at least 12 months before and despite the FBI warning, their use grew throughout 2020 and was still extremely prevalent in 2021. We're seeing that attackers will capitalize on opportunity and that even though attacks have tailed-off very slightly, they remain a significant threat.

Corero's Threat Intel team is constantly on the lookout for new exploits and emerging techniques that cybercriminals could leverage to launch new and more sophisticated DDoS attacks. Some of the latest research includes the new **TP240PhoneHome** and **Hikvision SADP vulnerabilities** which can be exploited to launch damaging reflection and amplification attacks. With the threat landscape constantly evolving, solutions that deliver zero-day protection continue to be the best form of defense.

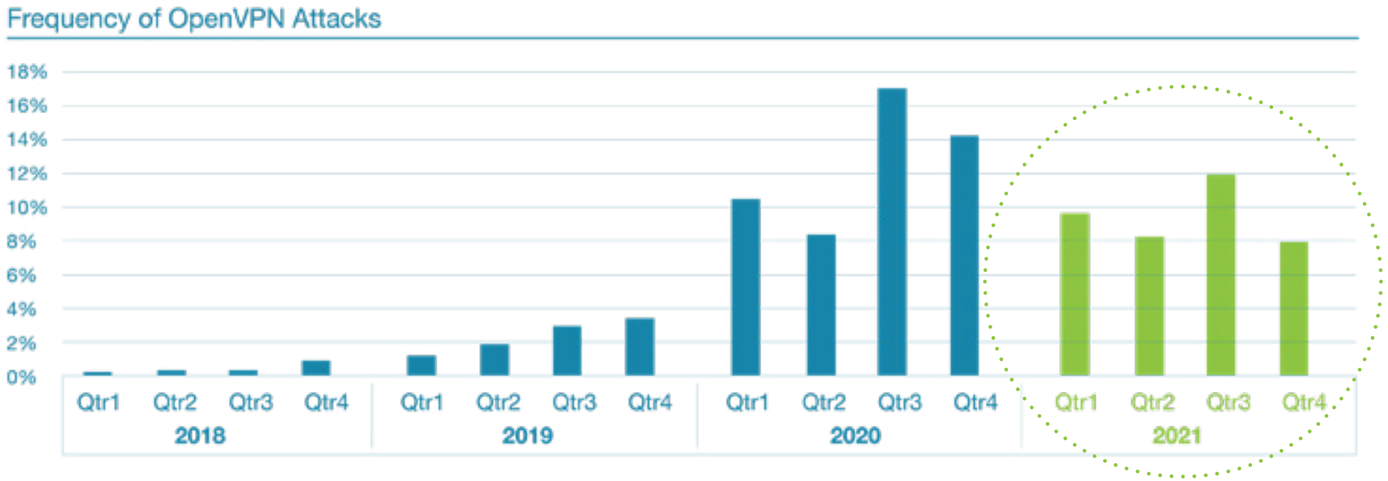
FBI reference: https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/fbi-private-industry-notiication-20200721-002.pdf

Key Trend

03

OpenVPN Attacks Remain High

The COVID-19 pandemic forced a huge shift in behavior and placed more reliance on the internet than ever before. Many of these behaviors like remote or hybrid working patterns and reliance on the internet for shopping and banking are now normal. These behaviors have proven lucrative for DDoS attackers using OpenVPN reflections as an attack vector. As the pandemic starts to wane, the preference for hybrid working prevails and Corero has seen use of this attack vector remain high - significantly higher than pre-COVID-19 levels.



297%

increase in OpenVPN Attacks since start of COVID-19 pandemic

OpenVPN as a reflection DDoS vector is bad news for both the victim being attacked as well as the organization whose infrastructure is being used to launch the attack, since remote workers will experience a degraded, possibly unusable, service, impacting productivity and potentially business continuity.

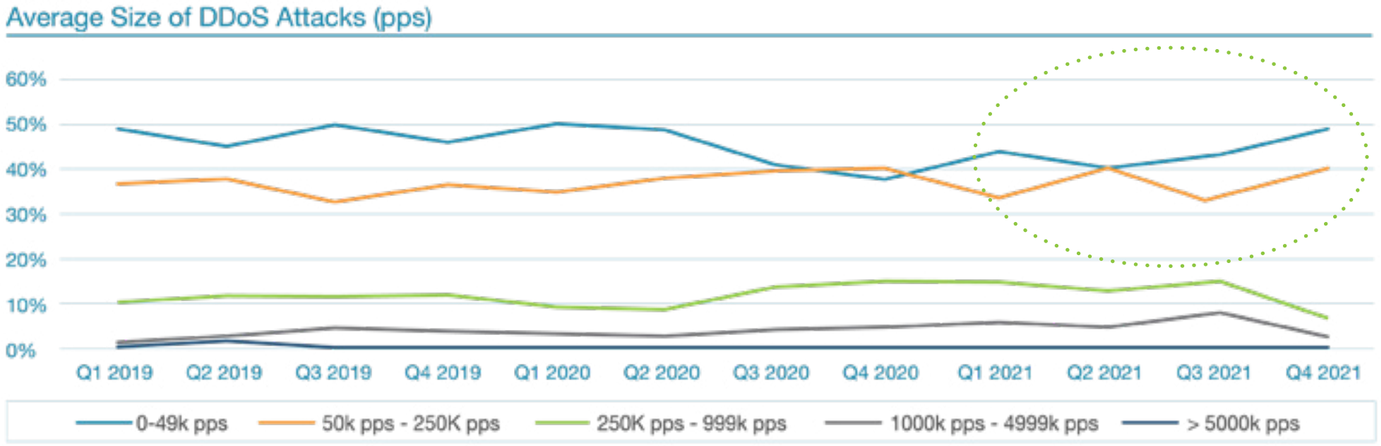
While patches and additional network security measures can be added to protect against attack, Corero's Security Operations Centre (SOC) are seeing compromised systems in the field being patched for extra network security as protection, however the threat from this kind of attack remains critically high.

Key Trend

04

Lower Packet Rate Attacks Dominate

Small, lower packet rate, short duration attacks should be a cause for concern, as they can pass under the radar of traditional DDoS solutions and go unnoticed by security teams, causing significant disruption.



81%
of attacks are low packet rate

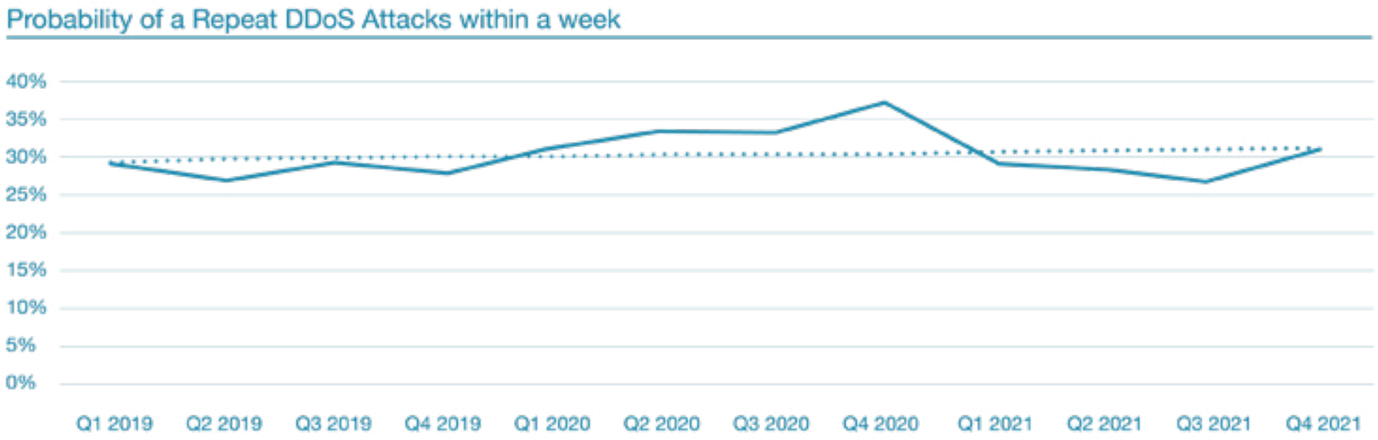
DDoS attacks are often thought of in terms of high bandwidth consumption and high packet rates. While this type of attack persists, combinations of small packets a high rates and large packets at lower rates are also used. In fact, Corero consistently sees the vast majority of attacks are under 250,000 packets per second. These DDoS attacks often behave in similar ways to normal traffic and are therefore capable of bypassing standard DDoS defenses. For this reason, they pose one of the biggest cyber threats and we advise that threat intelligence teams should check that they are adequately covered for DDoS protection with specialist support and ensure that DDoS mitigation forms part of any cyber risk assessment.

Key Trend

05

Significant Chance of Repeat Attack

The probability of a repeat DDoS attack within a 7-day span remains significant.



29%

Probability of Repeat Attack within a Week

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.

For this analysis, we have treated so-called ‘pulse’ or ‘saw-tooth’ DDoS as single attacks. These are characterized by attack traffic that repeatedly switches on for just a few minutes, switches off, and then re-appears a few minutes later, in a similar or modified form.

This technique is primarily used to evade on-demand scrubbing mitigation services, as the ‘pulses’ can be too short to trigger the required traffic redirection. It also enables DDoS-for-hire services to multiplex their attack resources across a number of victims and support more cybercriminal customers paying to launch damaging 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, 82% of which lasted less than 10 minutes, in 2021. 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. For 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. This can result 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 Provider Transit Links

Corero has observed, for many years, that the vast majority of DDoS attacks are less than 10Gbps in volume. This is a significant factor for Service and Hosting Providers, as they typically connect to other providers using 10Gbps, and increasingly 100Gbps, transit links. As a result, nearly all DDoS attacks do not saturate their upstream connections, or their backbone networks.

However these attacks are still significant enough to have damaging effects on the tenant customers of these providers. It's therefore vital that providers employ an effective DDoS protection solution to keep this junk traffic out and help to keep their customers online and productive.

The key significance of most DDoS attacks not being large enough to saturate providers' transit links, is that it enables them to benefit from using the latest generation of on-premises DDoS protection solutions. These enable attacks to be blocked much more effectively than on-demand cloud-based approaches. With an on-premises solution, the offending traffic can be dropped in real-time and with such accuracy, that the end-users are not even aware they were being targeted.

Why 2022 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 risk of unwanted downtime without having 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. With each new vector we often see a long tail, measured in years, of subsequent exploitation and related attacks. For example, the vulnerabilities referenced in the 2020 FBI DDoS alert and the leverage of OpenVPN reflections which ramped during the COVID-19 pandemic, continue to appear in present day attacks.

At the same time, the novel weaponization and abuse of internet facing applications or devices continues with recent examples including the **TP240PhoneHome** test feature and **Hikvision SADP** response. It is important to be aware of the evolving threat landscape and not to simply assume that your Service / Hosting Provider has effective counter measures in place to combat the latest DDoS attack vectors and keep your business online.

As cyber criminals continue to find new vectors to launch assaults on organizations, the best defense against potential downtime is to utilize real-time protection. Solutions which detect and redirect traffic to the cloud often result in downtime. On-demand, cloud-based scrubbing services cannot practically mitigate the short, frequent attacks that many organizations now 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 and less than 10 Gbps. These findings question of the effectiveness of traditional detect, redirect and mitigate solutions that may need up to 10 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 detection and mitigation services with on-premises DDoS protection, 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 Internet bandwidth. On-demand cloud mitigation can never be truly real-time, so it cannot deliver protection without some 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 10Gbps) 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 already 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.

Recommendations

DDoS Considerations for the Digital Transformation journey.

Postpone protection at your peril.

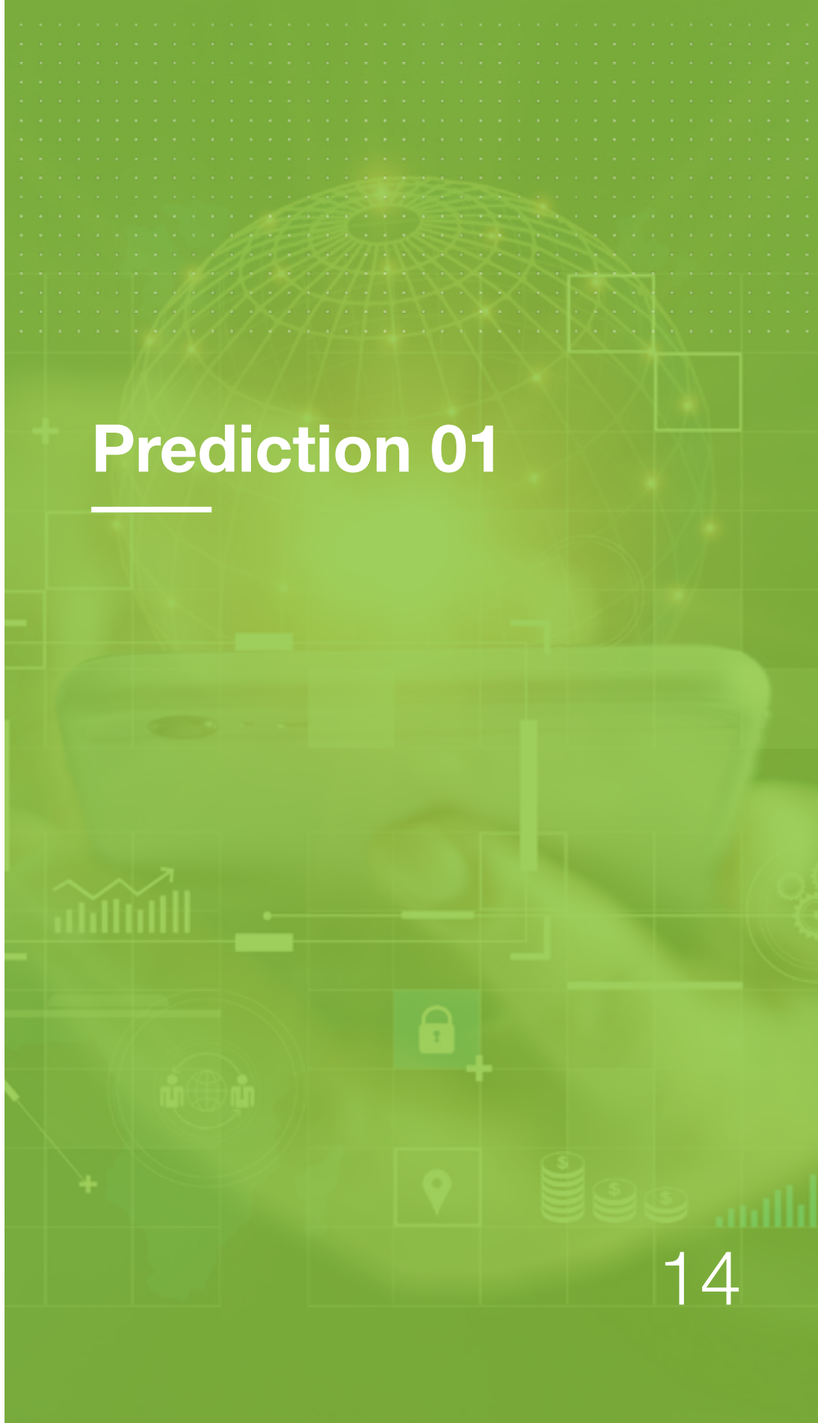
While the increasingly popular and necessary Digital Transformation trend does not explicitly imply the use of public Internet services, it is common for corporations to take advantage of online services that can automate the solution of business problems and improve the competitiveness of their offerings 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 & Synergy Six Degrees:

The Need for Always-On, Real-Time DDoS Security Solutions



Prediction 01

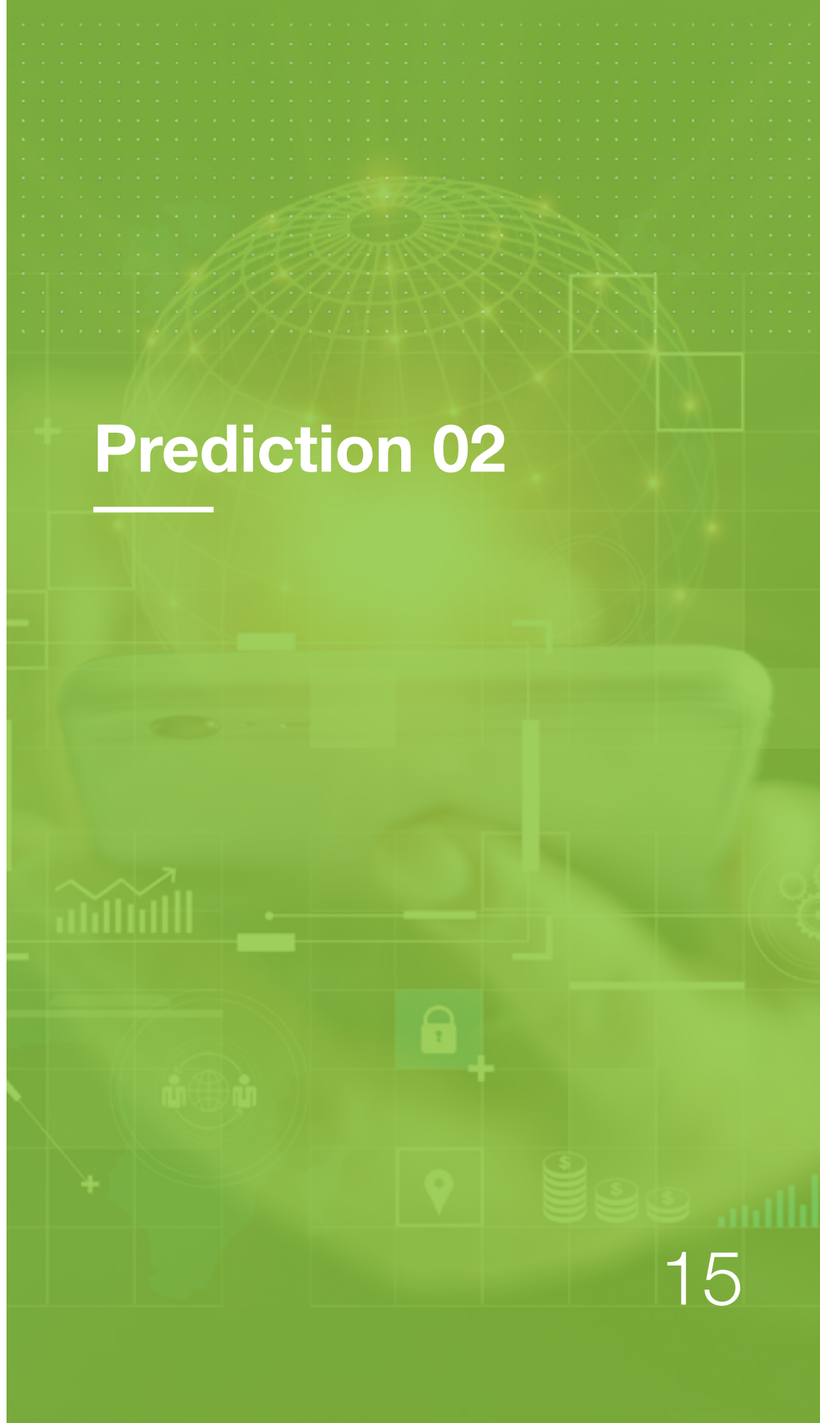
Prediction 02

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 offoad 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 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.



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