CYBER THREATS & TRENDS: JAN–JUN 2020

IS THIS THE NEW NORMAL?

neustar Security

TABLE OF CONTENTS

COVID-19 CHANGES EVERYTHING

The last time we examined the data from our Security Operations Center (SOC), the world was in the midst of the first wave of COVID-19. It is almost hard to recall that, at the time, many of us thought that the pandemic was almost over. As we have become increasingly aware, however, the effects of the virus will be with us for quite some time.

While each of us has experienced vast changes in our everyday lives as the result of the pandemic, the world online has also gone through a radical transformation. Internet use is up between 50 and 70 percent, and streaming media jumped more than 12 percent in the first quarter of 2020, according to Forbes.[1] A recent study by eMarketer estimates that US e-commerce alone will go up 18 percent this year.[2] Sixty-two percent of employed Americans currently say they have worked from home during the crisis, a number that has doubled since mid-March.[3] And many of these changes appear to be here to stay. According to a recent Gallup poll, "Three in five US workers who have been doing their jobs from home during the coronavirus pandemic would prefer to continue to work remotely as much as possible, once public health restrictions are lifted."[4]

Work Has Changed

Business workers' rapid transition away from the corporate office has resulted in a number of shifts for networking and security teams all over the world. IT departments have had to put more emphasis on collaboration and remote connectivity tools while ensuring that their employees and their businesses remain protected. The change from local area network (LAN) or office-based connectivity to a virtual private network (VPN) or virtualized environments has caused a myriad of problems on its own. While businesses enjoy some protection through the external hosting of some public services, such as their websites or email systems, they need to carefully consider their VPNs as well as the other services that aren't externally hosted or protected. If a business's corporate connection is attacked, specifically targeting its VPN, and this goes down, its entire workforce is offline.

The challenge with using VPNs to allow global workforces to log on remotely is that cybercriminals understand that the hardening of connectivity from a distributed denial of service (DDoS) point of view has not been done. This makes VPNs an easy target for these attacks. The fact that most businesses use "vpn" as part of the URL or host name also makes it simple for an attacker to identify the server. With a single Domain Name System (DNS) lookup, the attacker has the IP address and can launch a conventional volumetric DDoS attack via a rented bot network to swamp circuits, or use a network protocol attack to paralyze system resources.

The Internet Has Changed

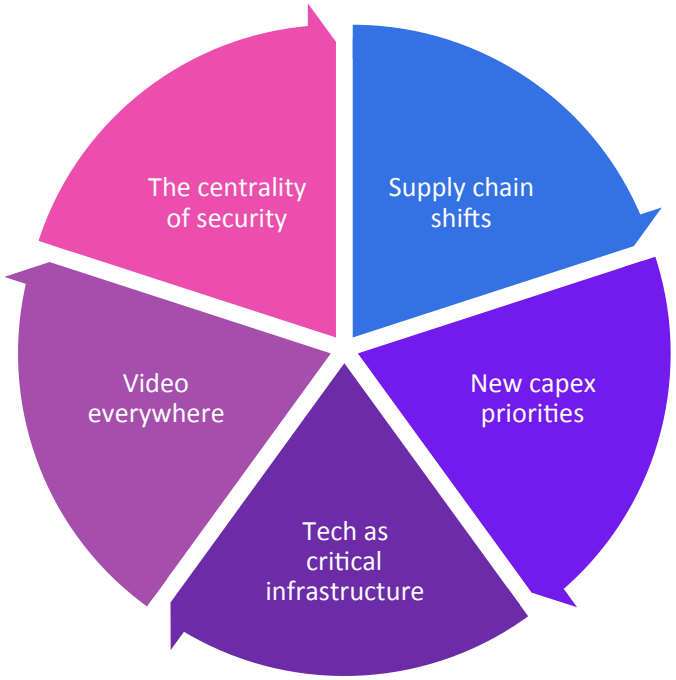
All industries have seen an effect from the novel coronavirus pandemic. Internet traffic is up and, as you will see later in this report, so are attacks. Attackers of all types, whether serious cybercriminals or bored teenagers stuck at home, likely have more screen time than ever. And not only is there explosive growth in the number of people using the Internet, there is also a spike in the number of machines online. Business Wire predicts that "Amid the COVID-19 crisis and the looming economic recession, the Internet of Things (IoT) market worldwide will grow by a projected US $876.5 billion, during the analysis period, driven by a revised compounded annual growth rate (CAGR) of 31.4 percent."[5]

As our world changes, so too must our priorities. While a poorly performing website could reflect increased traffic, it is possible that the traffic bogging down your site could actually be from a DDoS attack. Highlighting this fact, the US Federal Bureau of Investigation (FBI) released a notification in late July saying that one way to identify a DDoS attack is "unusually slow network performance (opening files or accessing websites)."[6]

Even worse, failure to correct the problem in these times could cripple your business, rather than just annoy more impatient customers. A dropped connection or poor-quality streaming experience could be enough to cause customers to consider changing services or providers. Services that used to represent a portion of your revenue may now constitute the majority.

Business Has Changed

Analysts at Omdia have identified five key trends that they expect to cut across technology sectors during and after the pandemic.[7]



Source: Omdia ©2020 Omdia

If You Can't Change the Offense, Change the Defense

Cybercriminals rarely cause disruption just for the sake of it. One of the most likely objectives for DDoS incursions is to make a path for a targeted attack. Many of these can be stopped by examining and filtering traffic, which should be doable by whatever mechanism is used to defend against DDoS attacks targeting corporate infrastructure. By examining traffic, looking at headers and content, and scoring the combination by also assessing reputation, it's possible to pass all the good traffic while minimizing the bad traffic that gets through.

Organizations should also strongly consider a managed service option. It's much easier to mitigate an attack when a solution is already in place, before it actually needs to be used. At a time when many businesses could do with one less worry, fully managed services can take the pressure off and ensure digital assets are safe and secure.

Another thing to consider is the benefit of a DDoS mitigation solution that is vendor-neutral and strongly focused. As Forrester mentioned in a recent report, "Pure plays bring DDoS and security expertise. Enterprises and service providers that are concerned with maintaining uptime but lack large security teams with deep DDoS expertise can outsource DDoS mitigation to a focused provider, giving them access to dedicated DDoS expertise should they require it."

Network security is more important than ever in these uncertain times. As always, carefully examine the assets you are concerned about, as well as the various resources that support them. Consider the loss to your revenue and ultimately your brand, should there be an issue, because you may be playing with higher stakes than ever before. Then look for a vendor that you trust, preferably one that offers different service options to meet your needs. Finally, act, because if you have not been hit yet, it is likely just a matter of time.

—Michael Kaczmarek

Michael Kaczmarek

Vice President of Security Product Management

Neustar

Michael Kaczmarek is the VP of Product Management for Neustar's Security Solutions business unit. He is responsible for evangelizing the vision, strategies, and tactics for the successful launch and expansion of products into new and existing markets.

Prior to joining Neustar, Michael was with Verisign for more than 18 years where he served in various capacities including VP of product management and marketing for Verisign Security Services. Prior to joining Verisign, Michael was a systems engineering manager for Lockheed Martin in charge of their Solid Rocket Motor Disposition in Russia Program.

Michael holds a Bachelor of Science in aerospace engineering from the University of Maryland and a Master of Engineering in environmental engineering from Johns Hopkins University.

CYBER THREATS & TRENDS: JAN-JUN 2020

This section contains the observations and insights derived from DDoS attack mitigations enacted on behalf of, and in cooperation with, customers of Neustar DDoS Protection Services from January to June of 2020, as well as customers for whom we offer SOC-as-a-Service.

Comparing January to June of 2020 with the same period in 2019, the total number of attacks has increased by more than two and a half times. The largest attack size observed during this period is also the largest that Neustar has ever mitigated and, at 1.17 Terabits per second (Tbps), among the largest seen on the Internet. The longest duration for a single attack was also the longest we've ever seen, at 5 days and 18 hours.

151%

Increase in number of attacks from Jan-Jun 2020 vs the same period in 2019

1.17 Tbps

Largest attack size from Jan-Jun 2020

192%

Increase in the largest attack size from Jan-Jun 2020 compared to the same period in 2019

5 DAYS | 18 HRS

Longest attack duration from Jan-Jun 2020

Comparing the number of attacks by size category from Jan-Jun 2020 with the number of attacks in the same time period in 2019, in perspective, the biggest changes happened at opposite ends of the scale. While attacks of all sizes increased across the board, the category that grew the most featured the largest attacks of 100 gigabits per second (Gbps) or more.

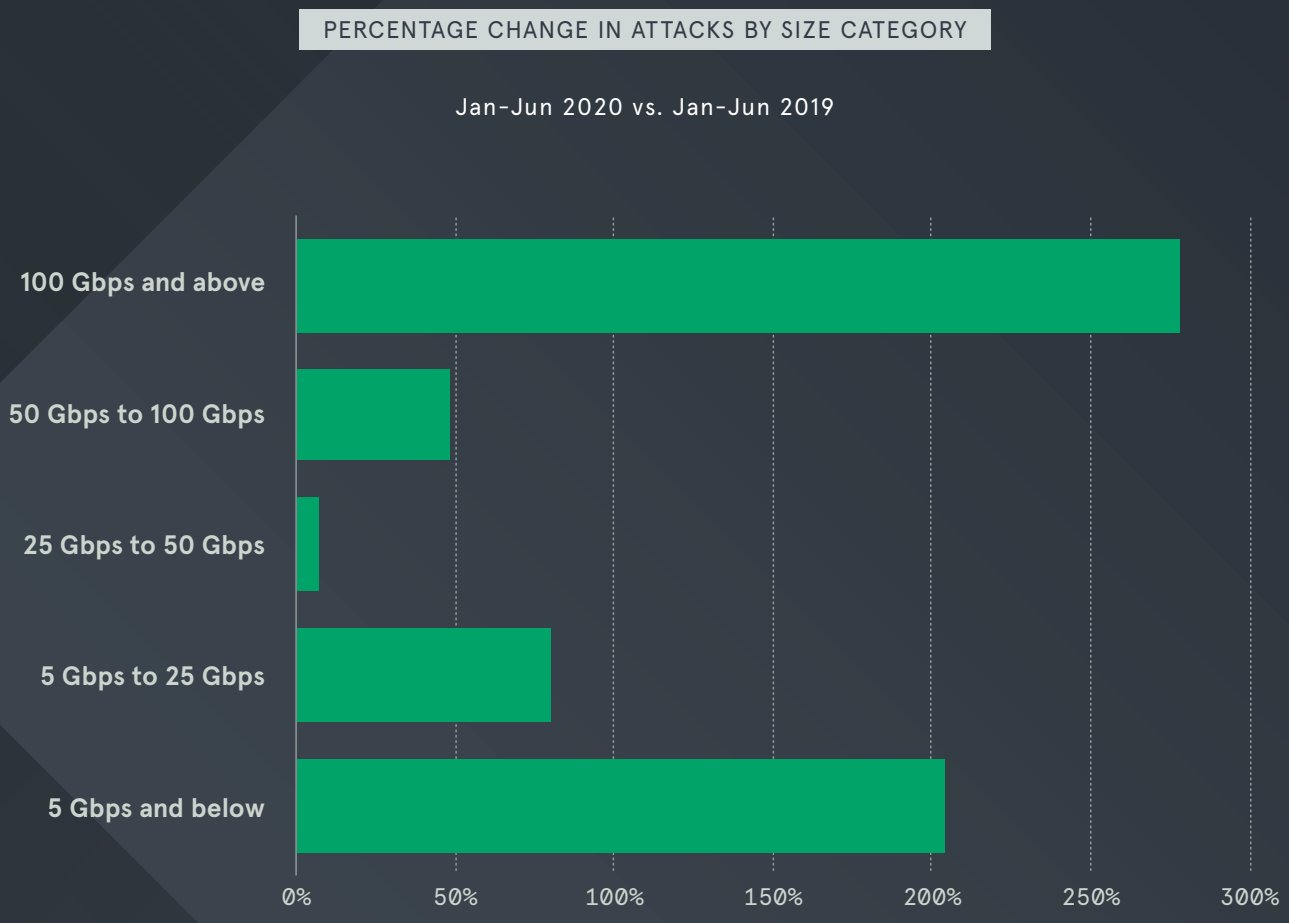


Figure 1: Percentage change in number of attacks by size category, Jan-Jun 2020 vs. Jan-Jun 2019

ATTACK VOLUME

From Jan-Jun 2020, over 70 percent of attacks mitigated by Neustar were 5 Gbps or less. It is important to note that this comparison looks at the composition of traffic for each time period, rather than the number of attacks. The total number of attacks, of course, increased dramatically.

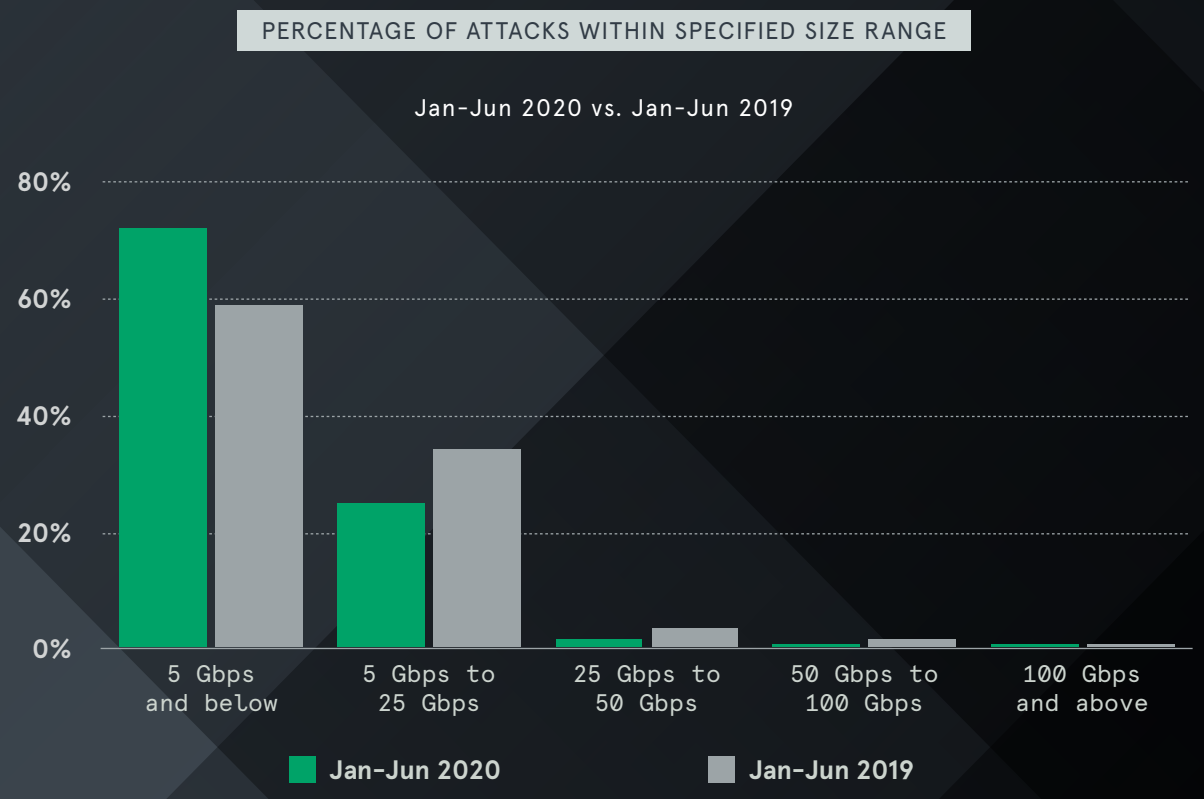


Figure 2: Percentage of attacks from Jan-Jun 2020 vs. same period in 2019

12 Gbps
Average attack size from Jan-Jun 2020

11 Gbps
Average attack size from Jan-Jun 2019

ATTACK INTENSITY

Comparing the intensity of attacks from Jan-Jun 2020 to the intensity of attacks for the same period in 2019, Neustar observed that, at 350 million packets per second (Mpps), 2020's most intense attack was dramatically higher than the most intense attack of the same period in 2019. This attack represents more than an 81 percent increase in intensity, while the overall average intensity of attacks for these periods was virtually unchanged.

2020	VS	2019

350 Mpps
Most intense from Jan-Jun 2020

193 Mpps
Most intense from Jan-Jun 2019

Over
↑ 81%
Increase in maximum intensity YoY

3 Mpps
Average intensity from Jan-Jun 2020

2 Mpps
Average intensity from Jan-Jun 2019

THREAT VECTORS

The number of attacks featuring a single vector from Jan-Jun 2020 was fairly low, as were the number of extremely complex attacks featuring more than 4 vectors. These results may point to the fact that a larger number of attackers than ever before have "gotten into the DDoS game." Such bad actors may purchase/control threats with more than a single vector, but the number of attackers with the expertise to wield increasing numbers of changing vectors goes down as the complexity goes up.

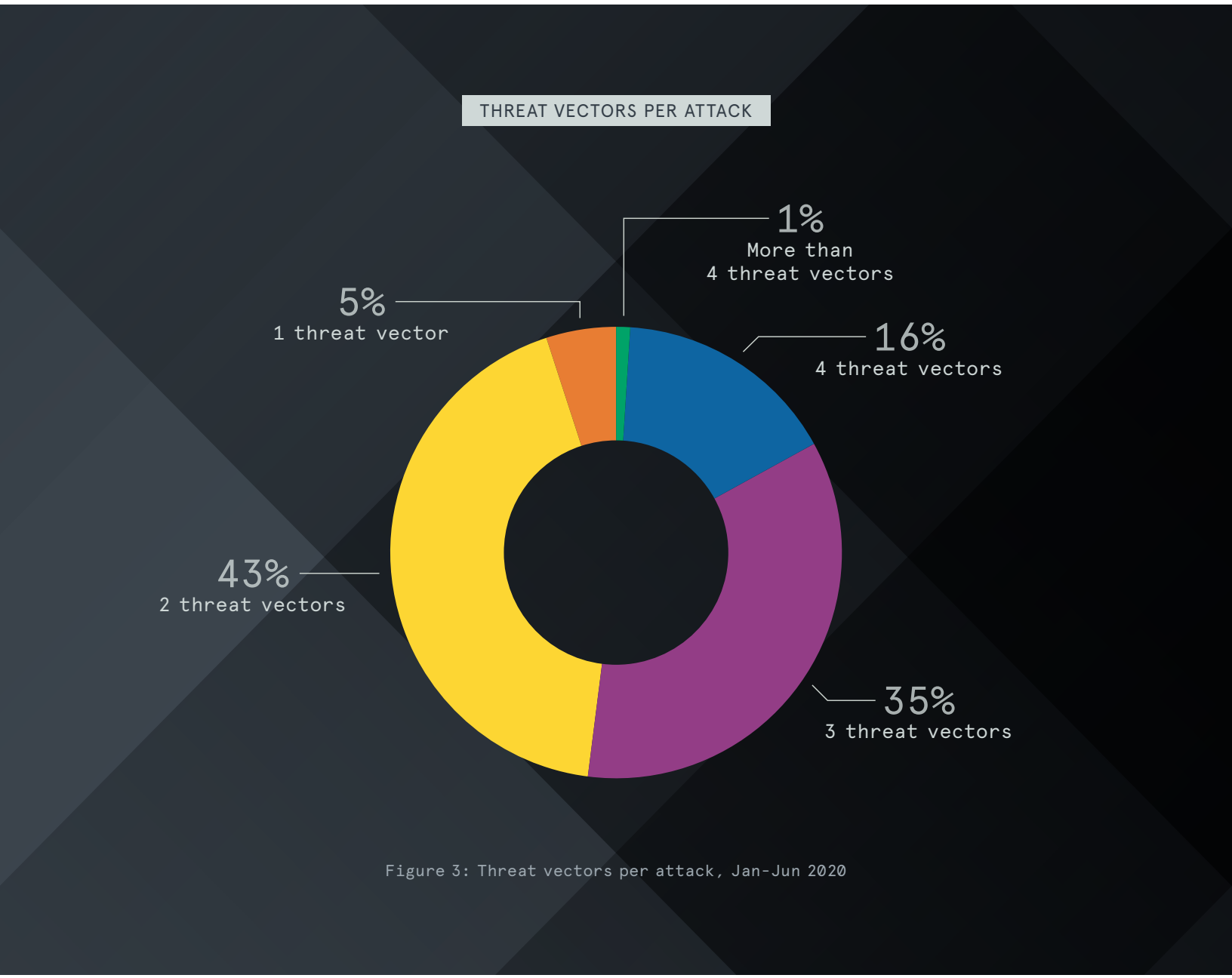


Figure 3: Threat vectors per attack, Jan-Jun 2020

RETURN OF THE BIG ATTACKS

DDoS attacks are nothing new. They have been around for decades. Every now and then, they make headlines, including the attacks on GitHub (where most of us first wondered how to pronounce "Memcached") and Dyn (where we all learned how an obscure Japanese anime character named Mirai could wreak havoc). There have been DDoS attacks on media outlets, banks, schools, and even government offices, not to mention the myriad "service outages" or "network failures" that were really DDoS attacks in disguise. In fact, one could argue that DDoS attacks have been around for so long that they have become a sort of background noise.

From Jan-Jun 2020, however, that outlook has changed decidedly. DDoS attacks are back in the news, and they are bigger, more intense, and happening in greater numbers than ever before. In this report, we'll consider recent DDoS events and take a look at the secret ingredients that make them powerful, including amplification vectors and bots. We will then examine vertical industries and look at what makes attackers do what they do.

The Big News

Attack Volume

This year marks the advent of the largest volumetric DDoS attack on record. Amazon Web Service (AWS) reported that an unidentified customer on their network had been hit by a 2.3 Tbps attack that continued for days. While the attackers themselves are not known, it appears that the basis was an amplification attack that used hijacked Connection-less Lightweight Directory Access Protocol (CLDAP) servers.

Amplification attacks are based on the same premise as reflection attacks. In a reflection attack, the instigator spoofs their source IP address, substituting it for the IP address of the victim. The attacker then sends a request to a service that will return information ... except the unwitting service returns that information to the spoofed address belonging to the target. As a result, the target gets an answer to a question that they did not ask, sort of like the '90s prank of signing another person up to receive an unwanted catalog or solicitation. An amplification attack works the same way, except in this case, the attacker sends a request to a service that is known to send back a lot of data, thus amplifying the volume of return traffic. To build on the '90s example cited above, this attack is like signing someone up with a junk mail clearinghouse instead of a single unwanted catalog.

One of the best-known amplification attacks used unprotected Memcached servers to amplify traffic. This attack was used to bring down GitHub in 2018 and, because of the volume of traffic generated by a single request, did not require the use of bots to generate a then-record-setting 1.3 Tbps. The attack also served to highlight the number of Memcached servers, which were designed to be behind firewalls, that were open to the Internet. Many of those servers have since been reconfigured, but there remain many available protocols—which we will consider in a later section—that are open by design and can thus be used as amplification vectors.

Attack Intensity

We are accustomed to thinking of DDoS attacks in their volumetric form, with measurements in Gbps or (now) Tbps. We refer to these attacks in terms of size, as the large volume of traffic is designed to saturate a circuit by using up its capacity. The other type of attacks we are hearing more about are high-intensity attacks, which are measured in Mpps. These attacks are targeted at a specific piece of infrastructure that incoming traffic must traverse on its way to a target. The previous high-water mark of 500 Mpps has also been topped this year, with an attack of over 800 Mpps.

Attack Numbers

While the huge threats above capture attention and headlines, the really big news in the world of DDoS mitigation is the overall number of these attacks. Neustar, along with the industry as a whole, has seen a dramatic jump in the number of attacks, especially those on the smaller side. When considering the reason for this ongoing trend, it is helpful to consider the intent of such attacks, which may not be large enough to completely saturate a circuit. Put simply, an attacker can do a lot of damage to a site or resource if they can remain undetected. A good way to remain undetected is to keep attack traffic high enough to do damage but low enough to bypass any traffic thresholds that would automatically signal an incursion. This is particularly true as Internet Service Providers (ISPs) become increasingly savvy about DDoS threats. By keeping the volume low and the pressure on, hackers can accomplish a variety of goals.

Attack Trends

Among the large numbers of attacks, we have observed several growing trends.

Burst and Pulse Attacks

There are a number of types of DDoS attacks where the relatively short gaps between an attack being detected, a mitigation being triggered, and a full redirect to the mitigation provider's scrubbing center enacted can be exploited. One such attack is called a burst attack. These threats feature an intense amount of attack traffic that appears suddenly and disappears just as quickly. A similar attack type is called a pulse attack or a pulse wave attack. This type of threat initially looks like a burst attack, but the bursts just keep coming. Pulse attacks, which are often aimed at ISPs or large enterprises, may include carpet bombing attacks in which a burst of traffic hits a particular subnet and then disappears, only to pop up again on another subnet. Still another twist is to change the attack vector or vectors while a DDoS is underway.

Both attack types pose the same problem: By the time a customer is aware that they're being attacked and they move to mitigation, the attack is over. Even worse, the target may be completely unprotected during the period that a route swing/propagation is underway. A savvy attacker will wait until this period to hit hardest.

The length of time that a customer is undefended depends upon what sort of DDoS mitigation they have. In the case where a customer has no active detection, it could take 5 minutes or more to start a mitigation. In situations in which a customer might not want to pay for always-on protection but does have their network set up for detection and alerting with automatic mitigation, the route swing and propagation could still take about 3 minutes. Many customers with mission-critical networks have moved to always-routed solutions, where mitigations are in the order of seconds, to avoid this downtime.

By the time a customer is aware that they're being attacked and they move to mitigation, the attack is over.

Vectors and Bots

Vectors: Amplification Factors

We have already discussed the basic function of any amplification attack when considering the AWS attack that used hijacked CLDAP servers. The CLDAP protocol has been around for years and has recently been used for DDoS amplifications, as have a number of others. Given the security industry's response to Memcached servers being used in a similar way, one might think that the logical defense is to remove protocols that are open to the Internet. Unfortunately, this is not practical in the case of built-in protocols, as noted by a recent warning by the FBI.

"Cyber actors increasingly are likely to abuse built-in network protocols for DDoS attacks against US networks. While a defense-in-depth strategy calls for the disabling of built-in features, such as ARMS, WS-DD, and CoAP, the loss of functionality to business productivity and connectivity may make implementing these strategies challenging. Moreover, device manufacturers are unlikely to disable such features by default because it would interfere with the user experience."[8]

Another such vulnerability was discovered in February of this year in Jenkins servers. Jenkins servers are free/open-source servers that are typically employed by DevOps teams, which use them to build, test, and deploy apps running in the cloud. The servers feature a built-in auto-discovery protocol that is enabled by default and exposed on public-facing servers. Unlike some other vectors, the option to disable the auto-discover protocol is possible by the teams that are using these servers.

According to the FBI, "Cyber actors' abuse of built-in network protocols may enable DDoS amplification attacks to be carried out with limited resources and result in significant disruptions and impact on the targets. In the near term, cyber actors likely will exploit the growing number of devices with built-in network protocols enabled by default to create large-scale botnets capable of facilitating devastating DDoS attacks."[9]

Of course, not all amplification vectors use built-in protocols. Q2 of 2020 saw the release of several new threats. The first, which exploits a DNS server vulnerability, is called NXNSAttack. The research team who discovered the attack reported that an attacker using NXNSAttack can amplify a simple DNS query from 2 to 1,620 times its initial size, creating a massive spike in traffic that can crash a victim's DNS server.[10] Patches have been made available. This vulnerability likely poses the most serious threat to server administrators who run their own DNS service, rather than managed DNS providers, such as Neustar, who began rollout of validated mitigations and patches the day after the threat was announced. Neustar's UltraDNS is further protected by the UltraDDoS Protect service.

Another amplification method, called RangeAmp, was also discovered in May of this year. Attackers can use several different types of malformed packets to bring down websites and large chunks of content delivery networks (CDNs). The exploit takes advantage of range requests, a HTTP standard that was designed to allow a client to request only a specific portion, or range, of a file from a server. Such partial requests are used when sending large media or downloading files with pause and resume functions. While any website could be affected by this attack, it is most dangerous to CDNs and is said to be able to increase the traffic load on CDNs by anywhere between 724 and 43,300 times.[11] Most large CDN vendors have already been made aware of this vector and have taken steps to prevent its use.

Here Come the Bots

As we have all become painfully aware, the spread of bots, which can then be used in DDoS attacks, grows proportionately to the deployment of IoT devices. Many of us were introduced to the recruitment of unsecured IoT devices into botnets with the Mirai attacks that affected Dyn. Unfortunately, although that attack received substantial press, it did not serve to eliminate Mirai (or its variants) or to persuade all users to secure IoT devices. In fact, since 2018, the Open Web Application Security Project (OWASP) has dedicated a specific site detailing weak, guessable, or hardcoded passwords as the first link.[12]

According to recent research from Palo Alto Network's Unit 42, there has been a resurgence of malware like Gafget, a Mirai variant, which is continuing to build up botnets.[13] And hackers are not standing still either. In February of 2020, hardware maker Zyxel fixed a zero-day vulnerability that has later been exploited by another new variant of Mirai.[14] This information, coupled with projections that there will be more than 41 billion IoT devices in use by 2027,[15] fuels the growing need for enterprises to implement a robust DDoS solution.

Traffic Changes as a Result of COVID-19

Much of the precipitous rise in DDoS attacks mirrors the growth in Internet traffic we've seen during the pandemic. Buyers have moved a large percentage of their spending online, as shown in the figure below.

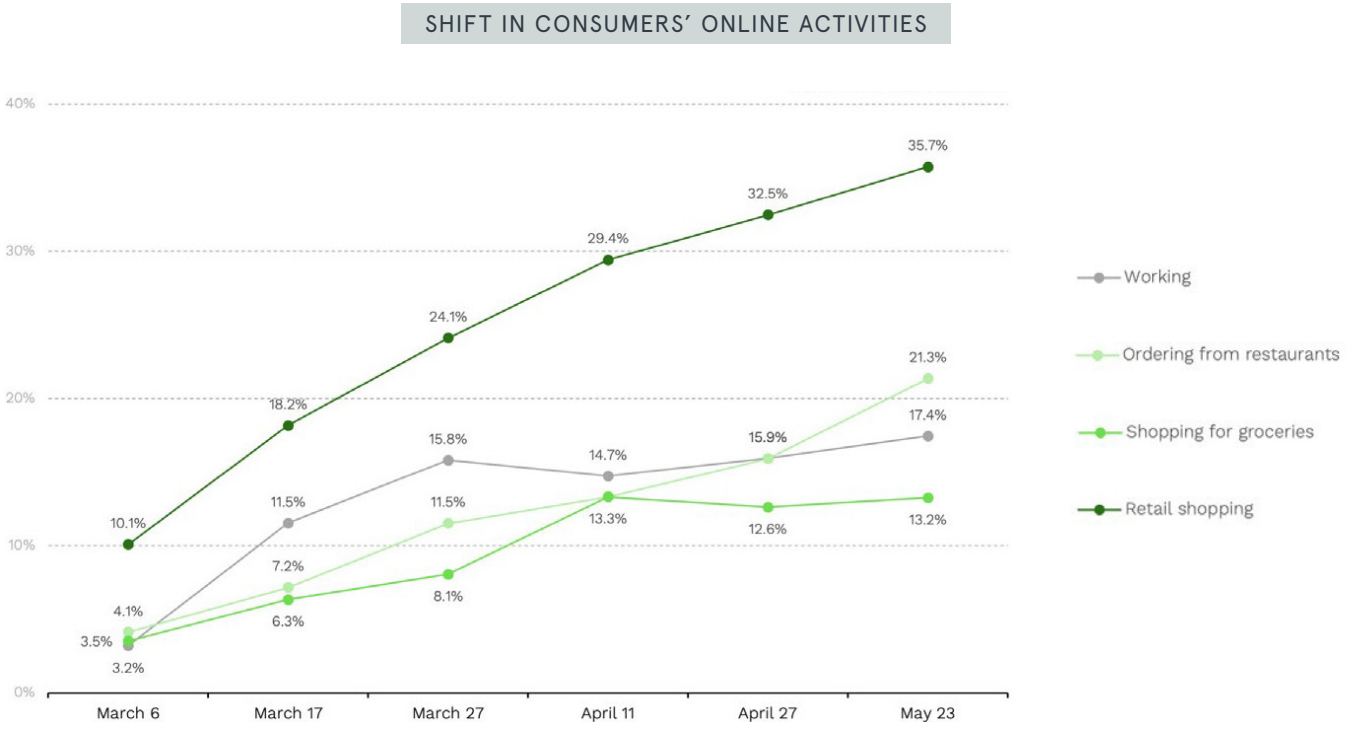


Figure 4: Share performing select activities who have gone online to do them, PYMNTS.com, June 2020

Per a June 2020 report from e-commerce provider Profitero, "COVID-19 has caused 10 years of consumer behavior change in just eight weeks,"[16] regarding the explosion of e-commerce and direct-to-consumer business models as one of those major transitions. Many of these changes in buying behavior are likely to be lasting ones. A report from the US Chamber of Commerce states that "Retailers will be feeling the impact of the coronavirus crisis long after the quarantines, store closings, and social distancing rules have ended. It is likely to create permanent shifts in consumer behavior that retailers need to start preparing for...."[17]

These findings highlight the importance of keeping online assets up and running, but a deeper look shows the potential for long-term trouble, should e-commerce sites not perform to user's expectations. Consumers have always been quite willing to change brands should they feel that their needs are not being met, and site performance has long been a guide for user satisfaction online. Nearly 70 percent of consumers admit that page speed impacts their willingness to buy from an online retailer,"[18] as reported by Unbounce. Website stress testing monitor Dotcom-Monitor goes even further, saying that "75 percent of all users will typically bounce as page load time passes the 3-second mark."[19] Business.com reports that for an online business, a slow load speed on a webpage can lead to a lack of sales conversions and a general loss of traffic and that modern consumers would prefer to search for a new page than spend time waiting for a page to load.[20] If consumers have historically been willing to switch sites when their first choice does not perform as expected, the stress of the pandemic is unlikely to make users more patient. The Profitero report probably says it best when it quotes the old adage, "if you want loyalty, get a dog." Now more than ever, brands need to look closely at optimizing site performance to keep the users that they have. One of the easiest ways to do this is ensure that all DDoS threats are mitigated, including the lower-level attacks that may not stop a site from running, but will certainly sap performance.

ATTACKS BY INDUSTRY

This year's attacks, like this year's Internet traffic, have not been evenly spread across all sites. Some industries have been extremely hard hit. And while the challenges faced by some vertical markets, like e-commerce or gaming, are covered well, some others you may hear less about.

ISPs, Registries, and Hosting Sites

Neustar has a unique perspective when considering DDoS mitigations. The company's offerings are cloud-based and vendor-neutral, which has led to UltraDDoS Protect being chosen the mitigation provider of choice for many ISPs, registries, and website hosts.

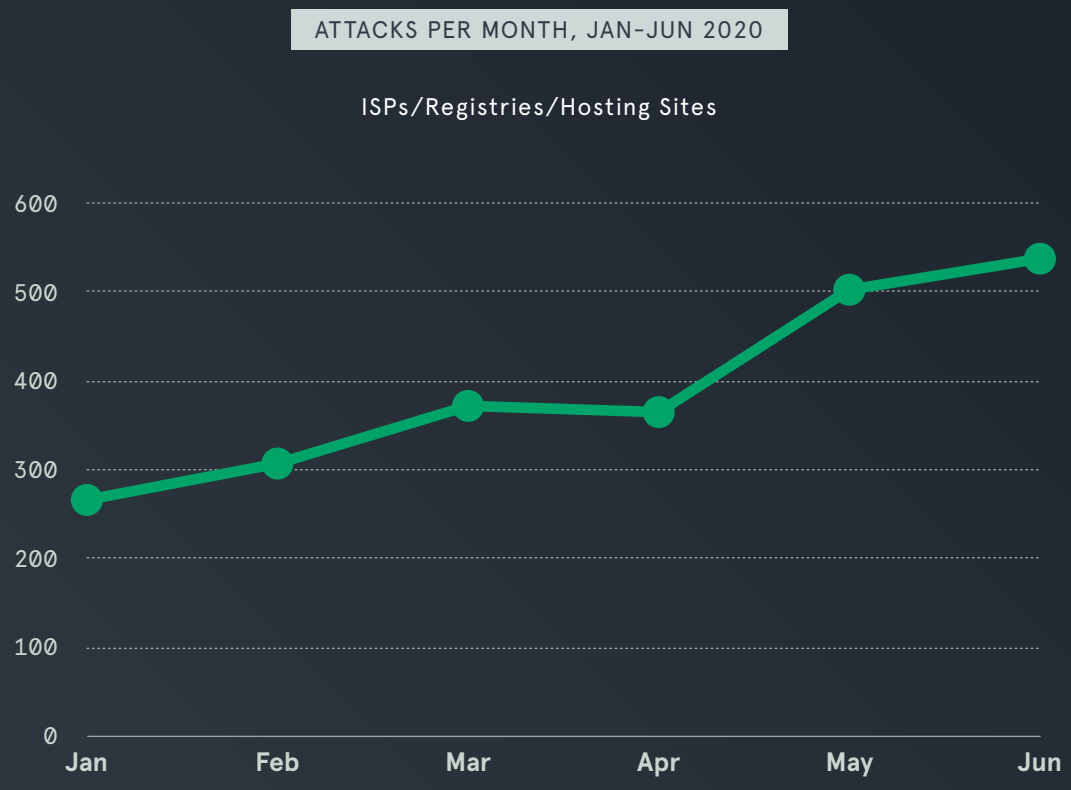


Figure 5: Attacks per month on ISPs/registries/hosting sites, as observed by Neustar

These companies are typical targets, given their essential nature. They are built to absorb attacks at some level, but the increase in sheer numbers (a 102-percent increase between January 2020 and June 2020) is noteworthy.

Gaming, Gambling, and Media

It is no surprise that gaming sites have seen high rates of growth throughout 2020 as lockdowns took hold. According to Forbes, "The increases in gaming revenue has been huge, month to month, since March. In March of this year, gaming, over March of 2019, is up 34 percent in spending. In April of this year, gaming was up 73 percent over last year, same month. And this past month, May, was up 53 percent over May of 2019."[21] And since those of us in the security industry know that gaming sites have long been among the top targets for attackers, it is also no surprise that attacks on these sites has grown as well. One of the largest DDoS attacks happened to video game company Electronic Arts (EA) in mid-April, when a series of DDoS attacks took servers offline.[22]

The online gambling industry is one of the potential sectors that may make it through the pandemic with the least possible damage. In fact, according to a study by the Grand View Research, online gambling is about to witness massive growth, and in the US alone, it will reach a value of $102.9 billion by 2025, as stated by Security Boulevard.[23] That also makes this industry ripe for cyberthreats. DDoS attacks can be used to hold a site for ransom, while other types of malware can be used to steal everything from cryptocurrency to personal identity.

Media, specifically online video, rounds out this trio of targets. Omdia forecasts that "video will account for up to 1.9 zettabytes (ZB) – equal to 1 billion terabytes – of Internet traffic this year, up by 0.2ZB or 12 percent on our pre-COVID-19 forecast. That's equal to an extra 200 billion hours of Netflix viewing or Zoom video calls. Even in 2021, when Omdia expects restrictions to ease, traffic will to be up to 9 percent higher than previously forecasted, as video remains part of the 'new normal.'"[24] As we have seen, where traffic rises, so too do attacks, although the majority of attacks observed in this sector have trended toward credential stuffing attacks.

Neustar attack mitigations for this vertical increased sharply, with a rise of 461 percent.

Figure 6: Attacks per month in gaming/gambling/media as observed by Neustar

Retail/E-Commerce

Retail and e-commerce have received a lot of attention since the beginning of the pandemic, as the urgency to move from brick-and-mortar shops to online offerings is perhaps greater than in any other industry. These numbers in a late April story from Forbes[25] tell the story:

- US retailers' online year-over-year (YoY) revenue growth is up 68 percent[26] as of mid-April, surpassing an earlier peak of 49 percent in early January.
- There's been a 129-percent year-over-year growth in US and Canadian e-commerce orders as of April 21 and an impressive 146-percent[27] growth in all online retail orders.
- Online conversion rates increased by 8.8 percent in February, reflecting a level of shopping urgency typically seen during Cyber Mondays, according to QuantumMetric.[28]

These numbers could signal a bonanza … if your site is robust enough to handle the traffic and to do so without a sacrifice in performance. That means that DDoS threats are a clear and present danger to a retailer's bottom line. According to a recent report, "Retail sites and applications rely directly on incoming traffic for revenue; thus, distributed denial-of-service (DDoS) extortion is potentially lucrative. A sophisticated DDoS attack can bring down a site in a matter of minutes." The same report noted that DDoS assaults account for 21 percent of all cyberattacks against online retailers.[29]

Healthcare

The combination of literally life-or-death stakes, made even more urgent in this time of COVID-19, increase the criticality of DDoS attacks on healthcare institutions. Hospitals or healthcare organizations always feature a host of IoT devices, many of which can be exploited. And finally, patient information is among the richest source of data to exist anywhere. All of these factors have combined to make healthcare one of the most desirable targets for attackers.

Attacks on healthcare providers started almost as soon as the pandemic was publicized. The Brno University Hospital in the Czech Republic was hit in March with a cyberattack that forced the hospital to shut down their entire network, resulting in the cancellation of surgeries. Assistance Publique–Hôpitaux de Paris, the university hospital trust managing 39 public hospitals in the Paris area, was hit on March 22, 2020. While the attack itself did not last long, it did impact Internet access, which blocked remote workers from email, Skype, and other remote locations. Just days later, the US Department of Health and Human Services (HHS) was the victim of a foiled DDoS attack. Meanwhile, the World Health Organization (WHO) revealed that it was experiencing double the usual number of cyberattacks against its systems, including hackers running malicious sites that impersonated the WHO's internal email system.[30]

WHY IS THIS HAPPENING?

It is worthwhile to consider why the number of DDoS attacks has risen so dramatically in such a short period of time. At Cambridge University in the UK, the Cambridge Cybercrime Centre pondered this question in a series of COVID-19 briefings and began by studying activity on one of the largest "booter/stressor" sites.[31] As you can see on the following charts, the number of attacks enacted by the site had been increasing steadily since 2018 but went up sharply around the time of the pandemic and associated lockdown.

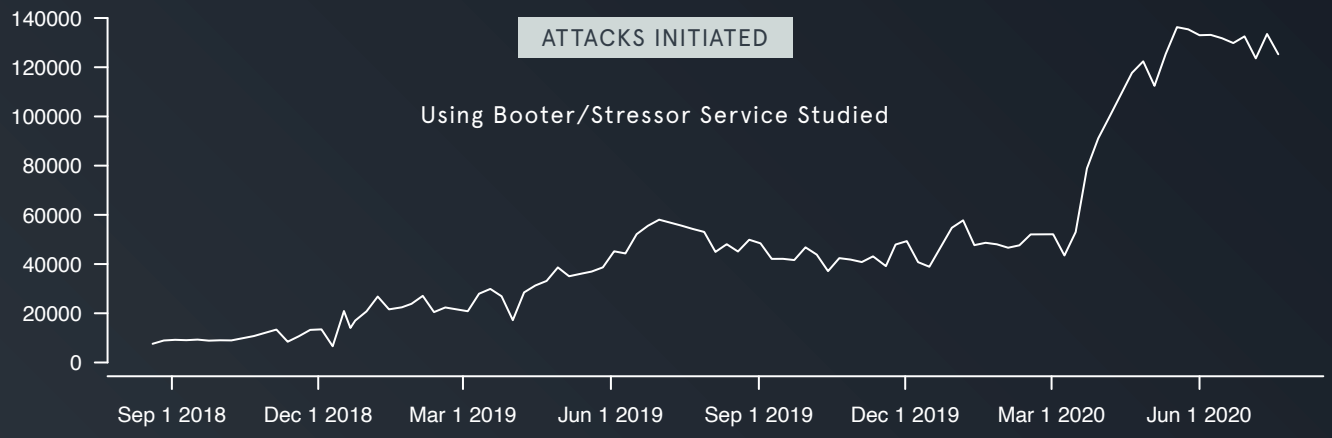


Figure 7: Attacks initiated by booter/stressor firm studied by Cambridge Cybercrime Centre

The next logical question is: Who is behind these attacks? Are cybercriminals staging more attacks, or are new attackers getting into the game? Analysis of new users on the same site provides insight.

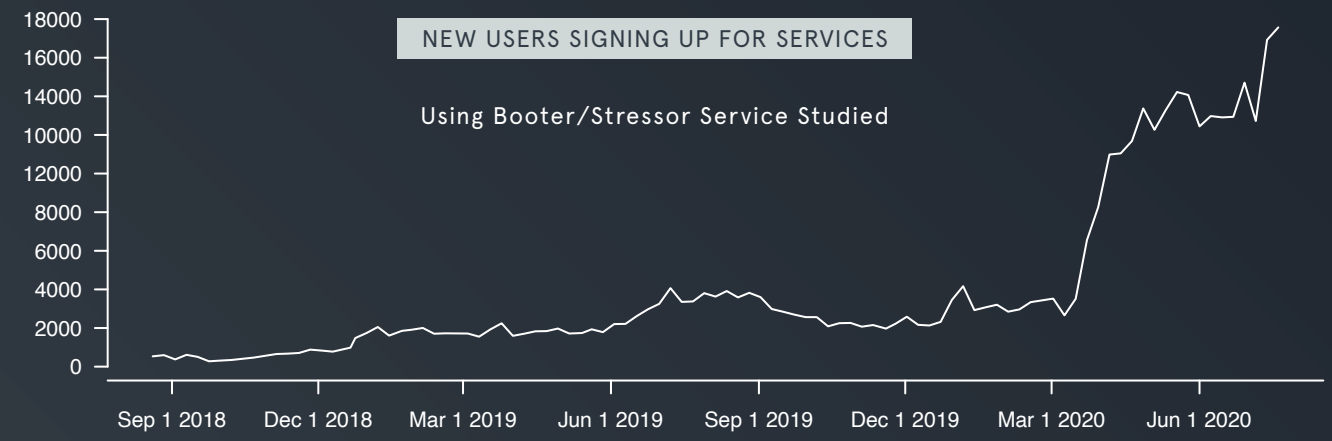


Figure 8: New user sign-up for booter/stressor firm studied by Cambridge Cybercrime Centre

The Cambridge group concluded their examination of this question by saying, "There is a clear change to activity patterns on cybercrime forums, with increased posting linked to activity being spread into working and school hours. This indicates that lockdown, and the associated increases in boredom and free time, are having significant effects on the routine activities of the users of cybercrime forums."[32]

SUMMARY

SO NOW WHAT?

While 2020 has brought radical changes in behavior to consumers and criminals alike, it is naïve to assume that actions of either audience will revert completely to pre-pandemic norms after this crisis passes. The FBI simply suggests, "Enroll in a Denial of Service mitigation service that detects abnormal traffic flows and redirects traffic away from your network."[33]

More detailed advice for coping with "the new normal" comes from industry analysts at Forrester.[34]

Choose a DDoS Mitigation Solution That Aligns with Your Strategy

Any organization with an Internet presence is at risk of a DDoS attack. Certain industries, like financial services and gaming, have historically been at higher risk than others. Just because your organization has never been targeted doesn't mean you're immune from a future attack. We recommend that security and risk pros:

- **Be proactive.** Be prepared for a DDoS attack before it occurs. DDoS attacks can saturate networks and applications with malicious traffic, making it difficult to put the required defenses in place. Document your plan in a codified DDoS runbook, so all parties involved understand what needs to happen when an attack occurs. With advance preparation, defenses can kick in immediately, avoiding a gap in protection.

- **Know the DDoS attack risk.** Use your own or vendor-provided threat intelligence to understand attacker campaigns and risks to your industry. Many DDoS vendors provide threat intelligence as part of their service, so consider this if you don't have threat intelligence from other sources. DDoS attackers typically don't pick targets at random. They may target companies within your industry as part of a campaign or may talk about an attack involving your organization before the attack occurs.

- **Limit the attack surface.** Prioritize the criticality of your applications and determine the level of acceptable risk for each. Limit the application's attack surface by minimizing the resources that are exposed to the Internet and can be discovered by a malicious actor. Ensure that you have DDoS coverage for your mission-critical and revenue-generating applications.

- **Build in redundancy to maintain availability.** Map the dependencies that your critical applications have on third parties, storage arrays, and DNS services, and then build in redundancy. In 2016, a volumetric attack against the DNS provider Dyn disrupted the availability of applications for which Dyn was the sole provider. Organizations with multiple DNS providers were unaffected.

- **Choose a solution that fits your digital transformation strategy.** As we predicted in our previous Now Tech on DDoS mitigation solutions, the major public cloud providers, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, have added DDoS protection to their portfolio of services. Firms hosting applications in a single public cloud provider should evaluate the cloud's built-in DDoS protections. Most organizations, however, are choosing a hybrid strategy with multiple public cloud providers and on-premises workloads. Those firms should choose a solution provider that can provide DDoS protection across their hybrid architecture.

COVID-19 has fundamentally changed what organizations must do to succeed, both during lockdowns and possibly long after. There is no one-size-fits-all solution for security, but a hard look at current activities suggests that rethinking your attack mitigation strategy may be in order. It could mean the difference between barely surviving and thriving in this rapidly changing environment.

GLOSSARY

ACK – Acknowledgement
AI – Artificial Intelligence
API – Application Programming Interface
ARMS – Apple Remote Management Service
C&C – Command and Control
CoAP – Constrained Application Protocol
DBIR – Data Breach Investigations Report
DDoS – Distributed Denial of Service
DoE – Department of Energy
DoS – Denial of Service
DNS – Domain Name System
FBI – Federal Bureau of Investigation
Gbps – Gigabits per second
GET – An HTTP method which requests data from a specified resource
GRE – Generic Routing Encapsulation
HTTP – HyperText Transfer Protocol
IoT – Internet of Things
IP – Internet Protocol
ISP – Internet Service Provider
IT – Information Technology
LAN – Local Area Network
M3AAWG – Messaging, Malware and Mobile Anti-Abuse Working Group
Mbps – Megabits per second
Mpps – Million packets per second
NISC – Neustar International Security Council
NIST – National Institute of Standards and Technology
NTP – Network Time Protocol
NXNS – Non-eXistent Name Servers Attack
PII – Personally Identifiable Information
POST – An HTTP method which sends data to a server to create/update a resource
SaaS – Software as a Service
SIEM – Security Information and Event Management
SOC – Security Operations Center
SYN – Synchronize
Tbps – Terabits per second
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
URL – Uniform Resource Locator
WS-DD – Web Services Dynamic Discovery

REFERENCES

1 https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-Internet-use-70-streaming-more-than-12-first-figures-reveal/#439a03dd3104, Forbes, March 23, 2020

2 https://www.emarketer.com/content/us-retail-sales-drop-more-than-10-2020?ecid=nl1014

3 https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx

4 https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx

5 https://www.businesswire.com/news/home/20200527005557/en/Global-Internet-Things-IoT-Market-Insights-Report

6 https://image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+PIN+-+7.21.2020.pdf

7 http://images.intelligence.informa.com/Web/InformaUKLimited/%7B19960528-e373-433d-a24c-51a03c5ce9e2%7D_Connecting_the_Dots_Key_Strategic_Opportunities_in_a_Post-COVID-19_World.pdf

8 https://image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+PIN+-+7.21.2020.pdf

9 https://image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+PIN+-+7.21.2020.pdf

10 https://www.zdnet.com/article/nxnsattack-technique-can-be-abused-for-large-scale-ddos-attacks/

11 https://threatpost.com/ddos-attacks-cresting-pandemic/158211/

12 https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

13 https://threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609/#:~:text=For%20one%2C%2098%20percent%20of,low%2Dhanging%20fruit%20for%20attackers.

14 https://krebsonsecurity.com/2020/03/zxyel-flaw-powers-new-mirai-iot-botnet-strain/

15 https://www.businessinsider.com/Internet-of-things-report

16 https://insights.profitero.com/TheCheatingConsumerReportLP.html

17 https://www.uschamber.com/co/good-company/launch-pad/changes-in-consumer-buying-after-coronavirus-pandemic

18 https://unbounce.com/page-speed-report/

19 https://www.dotcom-monitor.com/

20 https://www.business.com/articles/website-page-speed-affects-behavior/

21 https://www.forbes.com/sites/mikevorhaus/2020/06/22/gaming-industry-continues-big-growth-due-to-stay-at-home-americans/#63a64c6a43a1

22 https://www.pcgamesinsider.biz/news/70908/ea-servers-taken-out-by-ddos-attacks/

23 https://securityboulevard.com/2020/06/online-casino-and-gambling-industry-is-gaining-momentum-so-is-the-cyber-threat/

24 http://images.intelligence.informa.com/Web/InformaUKLimited/%7B19960528-e373-433d-a24c-51a03c5ce9e2%7D_Connecting_the_Dots_Key_Strategic_Opportunities_in_a_Post-COVID-19_World.pdf

25 https://www.forbes.com/sites/louiscolumbus/2020/04/28/how-covid-19-is-transforming-e-commerce/#4b38842d3544

26 https://ccinsight.org/observations/us-retailers-see-online-growth-yoy-in-april-similar-to-recent-holiday-season/

27 https://ccinsight.org/

28 https://www.quantummetric.com/covid-19-online-sales-impact/

29 https://www.mytotalretail.com/article/cyberattacks-on-online-retailers-the-top-3-threats-facing-companies-today/

30 https://www.medicaldevice-network.com/features/cyberattacks-healthcare-covid-19/

31 https://www.cambridgecybercrime.uk/COVID/

32 https://www.cambridgecybercrime.uk/COVID/

33 https://image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+PIN+-+7.21.2020.pdf

34 https://www.forrester.com/report/Now+Tech+DDoS+Mitigation+Solutions+Q2+2020/-/E-RES158436?objectid=RES158436

About Neustar.

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in Marketing, Risk, Communications, and Security that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100. Learn how your company can benefit from the power of trusted connections.

www.home.neustar

RPRT-SEC-244268-09.10.2020