CYBER THREATS & TRENDS

SECURING YOUR NETWORK PANDEMIC-STYLE

neustar Security | csc

TABLE OF CONTENTS

SUFFERING FROM ACRONYM FATIGUE?

The year 2020 was dominated by new terms that have burst onto the scene and taken over our lives. Chief among them is Coronavirus Disease 2019, better known as COVID-19. We've also heard a lot about SARS, N95, CDC, WHO, and more.

As these acronyms have wreaked their havoc, however, a few others have come into the realm of cybersecurity. One such is ransom-related denial of service, or RDoS—and its distributed cousin, ransom-related distributed denial of service (RDDoS). Using the threat of a denial of service (DoS) attack to hold a company for ransom is not a new phenomenon in certain industries, such as online gambling, but it has gotten a whole new grip on mainstream business in 2020. Not only are the usual suspects involved here, but a number of well-known nation-state actors have popped up as well. We've seen expanded use of some lesser used protocols to carry out DDoS attacks too, some of which reflect changes in internet traffic overall.

As you might expect, the accelerated drive to digital transformation has not been without casualties either. Web applications must be open in order to function, and some well-known attacks from the Open Web Application Security Project (OWASP) have been ready and waiting for the rush to the internet. Adding to the prospective chaos is the ongoing move from monolithic application architecture to a microservices model, complete with virtual machines, containers, and geographically disparate assets. While the motivations toward microservices are good—resilience, availability, and ease of innovation—the devil is often in the details, or in this case, the application program interfaces or APIs.

Still another acronym, and one many of us take for granted, has risen in the area of cybersecurity: DNS or the Domain Name System. This acronym frequently shows up in reports like this one as an amplification vector for DDoS attacks, but its foundational impact on web traffic as a whole has led to attacks in this last year.

As we look back across what occurred in 2020, it's important to remember that many of the largest security risks are a direct result of companies having to fundamentally change the way they do business at an extraordinarily accelerated pace. Estimates of how the pandemic has accelerated adoption of digital business ranges from six to seven years in more developed regions to more than ten years in those that were not as far along. Now, however, it is time to use the lessons that we have learned to prepare for the next "new" normal, which will be upon us as COVID-19 begins to loosen its grip. One emerging concept is that of holistic web protection. This evolution, driven by the retail, financial, and technology sectors, is an emerging category of security solutions that includes DDoS mitigation, web application firewalls (WAFs), and bot risk management (BRM). Such solutions could provide consolidated management capabilities that could shrink the gap between disparate legacy providers.

Regardless of how your business adapts, the most important realization is that you will have to do so. And the best way to move forward is to determine your most important assets and look at every possible way to guard them. Throughout this report, we'll look at what has happened in this tumultuous time and how best to protect yourself moving forward.

—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 program in Russia.

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

CYBER THREATS & TRENDS 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 in 2020, as well as customers for whom we offer Security Operations Center (SOC)-as-a-Service.

Comparing 2020 with 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 ever seen on the internet. The longest duration for a single attack was also the longest Neustar has mitigated, at 5 days and 18 hours.

154%

or over 2.5 times

Increase in number of attacks 2020 vs 2019

1.17 Tbps

Largest attack size in 2020

192%

Increase in the largest attack size in 2020 compared to 2019

5 DAYS | 18 HRS

Longest attack duration

Comparing the number of attacks by size category in 2020 with the number of attacks in 2019, the number of attacks in all size categories increased. In perspective, the biggest change was in the 5-to-25-Gbps category.

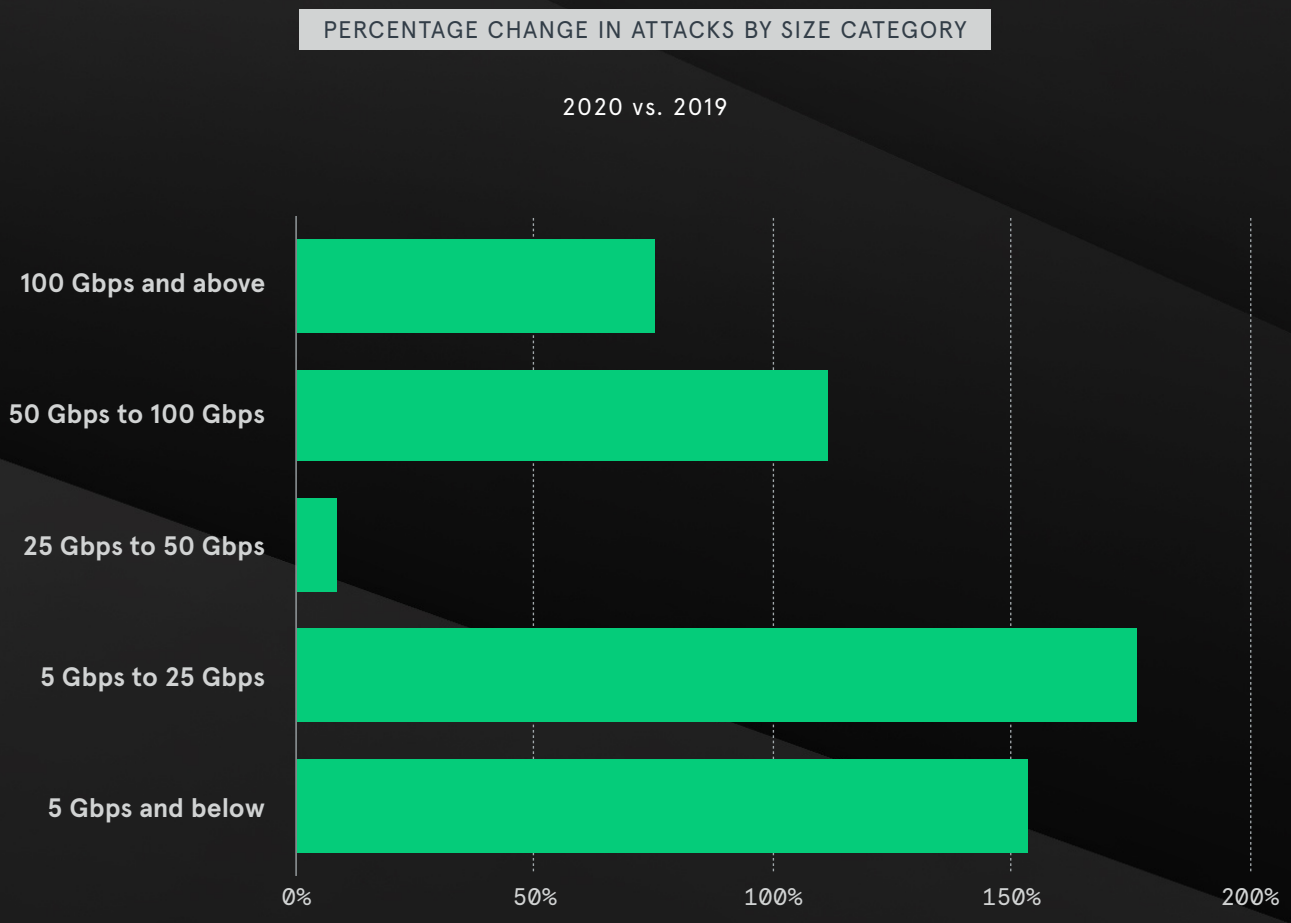

Figure 1: Percentage change in number of attacks by size category, 2020 vs. 2019

ATTACK VOLUME

In 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 in every size category.

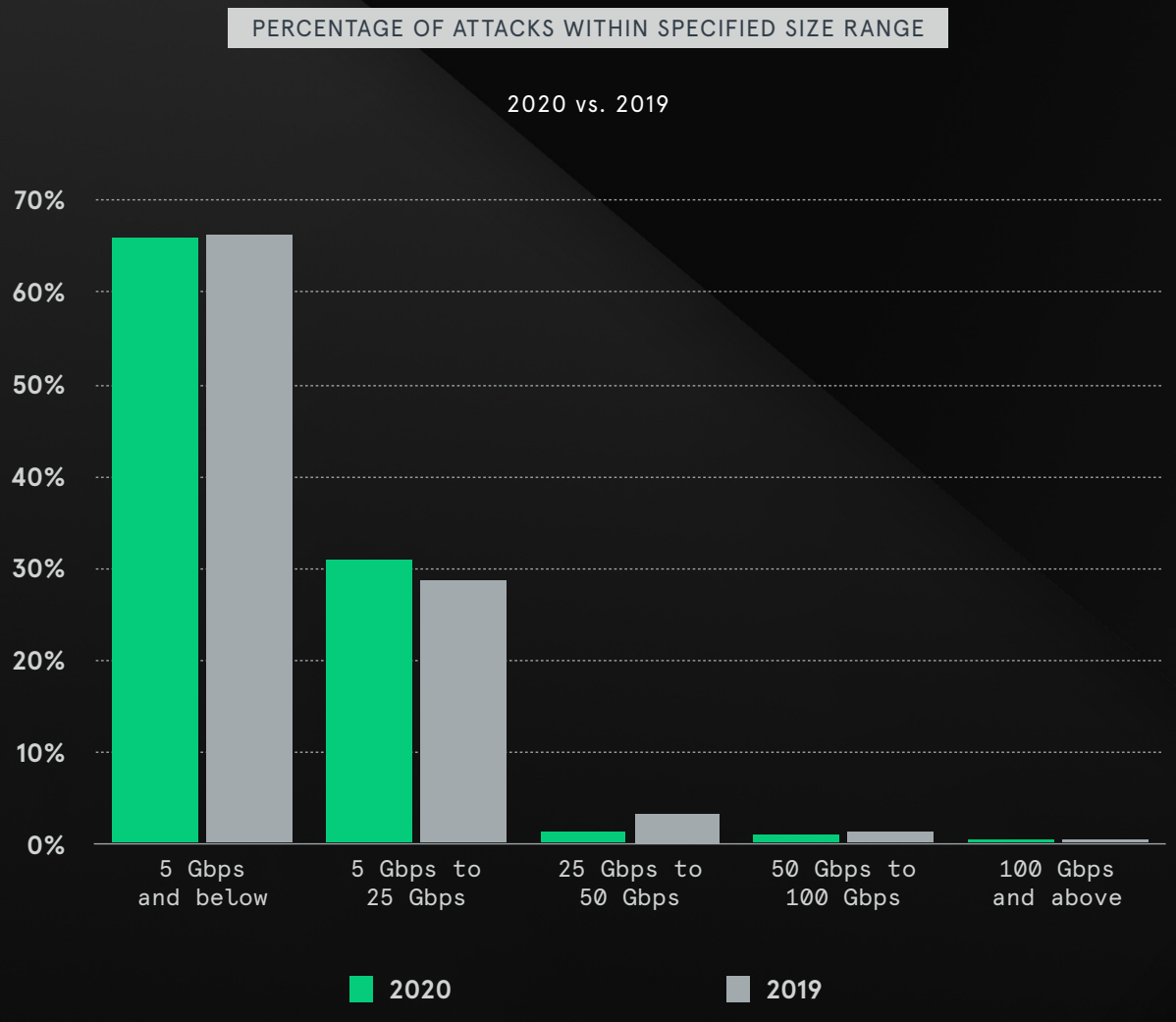

Figure 2: Percentage of attacks within specified range, 2020 vs. 2019

ATTACK INTENSITY

Comparing the intensity of attacks in 2020 to the intensity of attacks in 2019, Neustar observed that the maximum intensity was relatively unchanged.

2020 VS 2019

350 Mpps
Most Intense in 2020

342 Mpps
Most intense in 2019

Over
↑ 2%
Increase in maximum intensity year over year

THREAT VECTORS

The number of attacks featuring a single vector in 2020 was fairly low, as were the number of extremely complex attacks featuring more than four vectors.

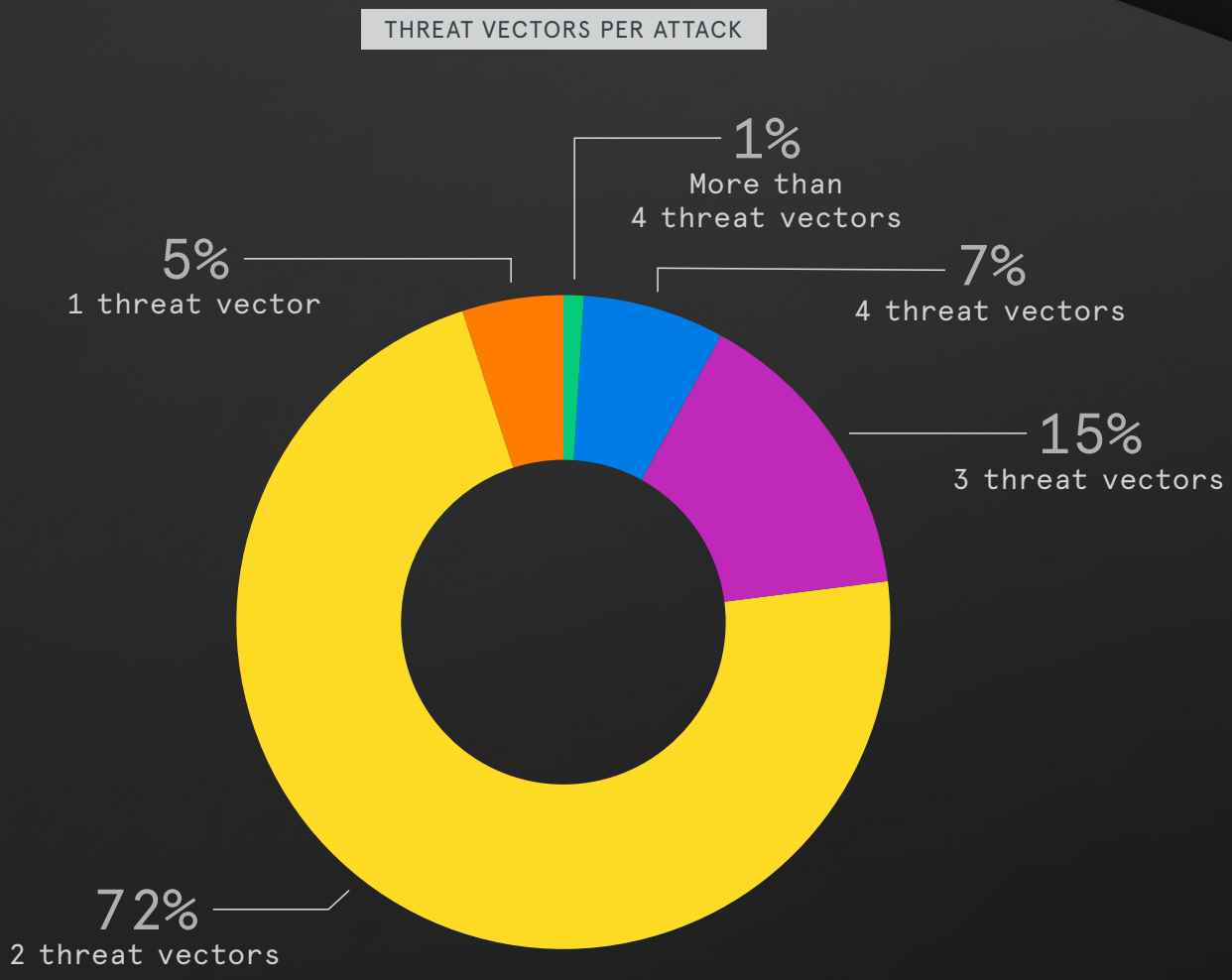

Figure 3: Threat vectors per attack, 2020

DDoS 2020

With its new dependence on e-commerce, 2020 could be considered a comeback year for DDoS attacks, if they had ever gone away in the first place. DDoS, which has long been top of mind for security executives, rose up the rankings to the number one concern, as shown in the November survey conducted by the Neustar International Security Council (NISC).

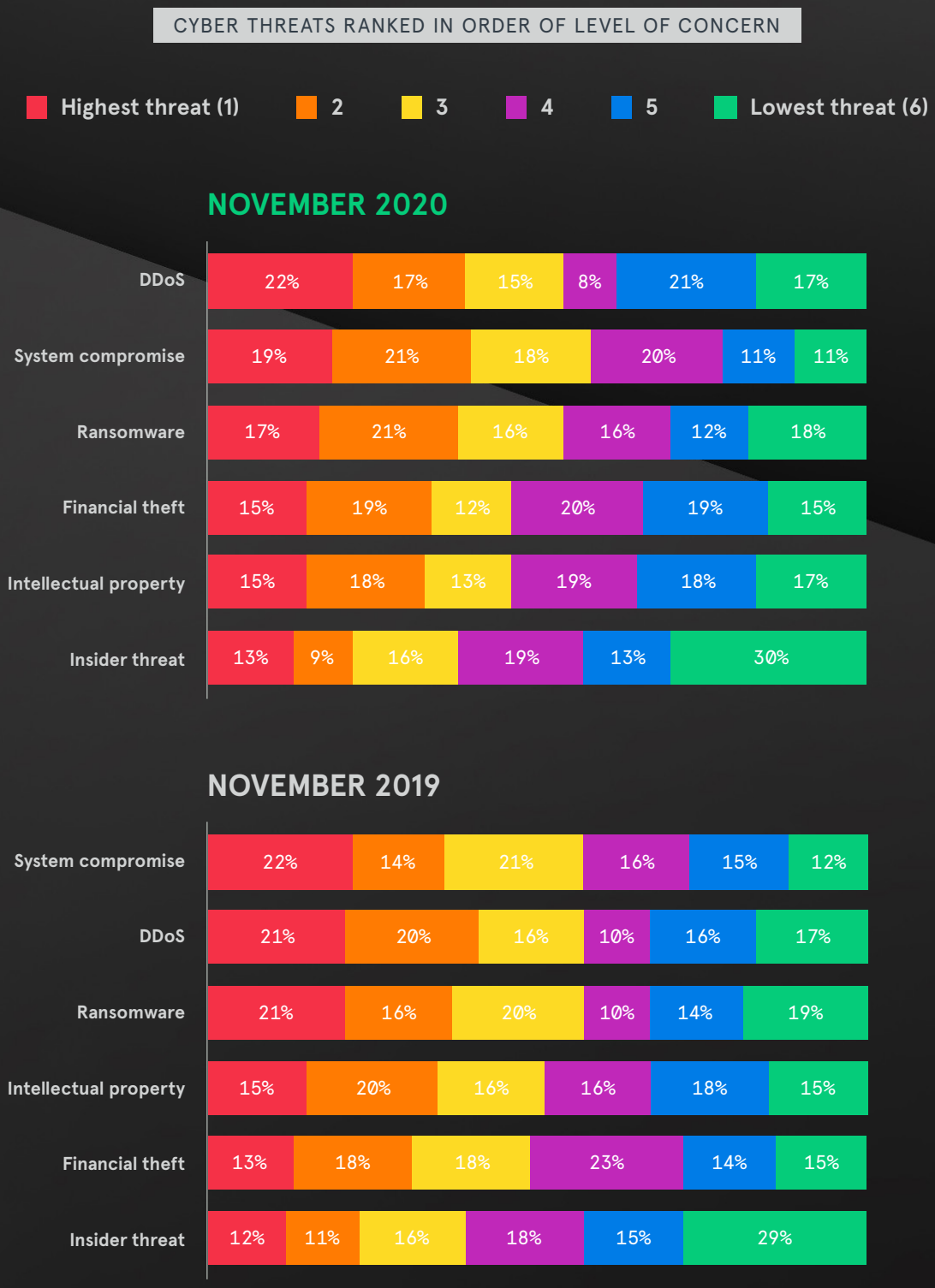

Figure 4: Cyberthreats ranked in order of level of concern, NISC Survey, Q4 2020

The number of respondents that acknowledge being on the receiving end of a DDoS attack has also gone up, when compared to answers to the same question in the NISC November 2019 survey.

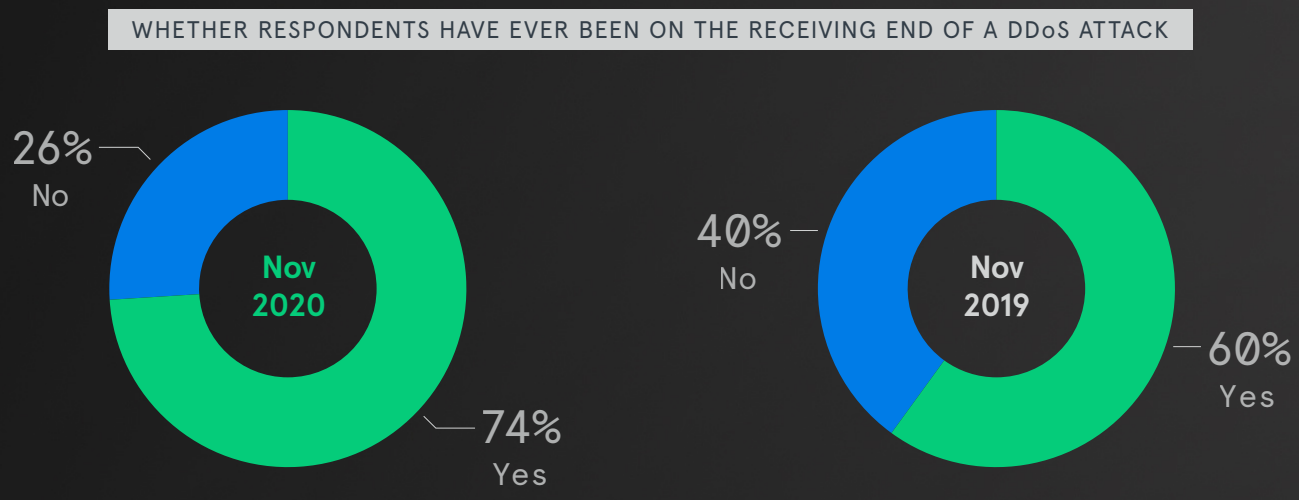

Figure 5: Percentage of respondents who have been on the receiving end of a DDoS attack, NISC Survey, Q4 2020

As a result, companies surveyed reported a rise in outsourcing for DDoS mitigation, adding several percentage points when comparing November's survey results to answers to the same question in 2019.

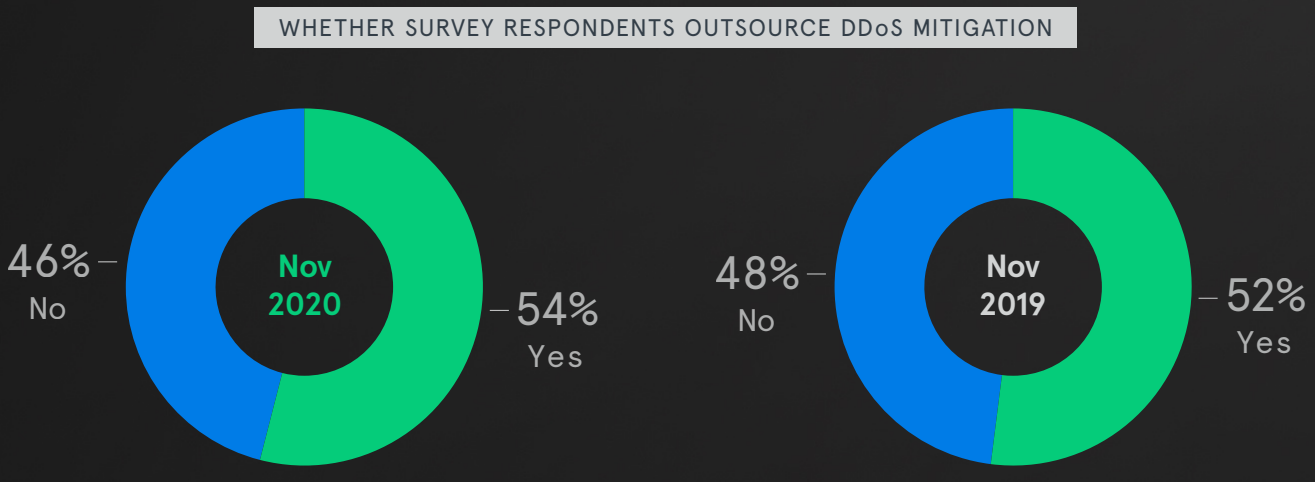

Figure 6: Percentage of respondents who outsource DDoS mitigation, NISC Survey, Q4 2020

While response time to mitigation appears to have gone down, mitigations within 5 minutes may well be too long for many businesses.

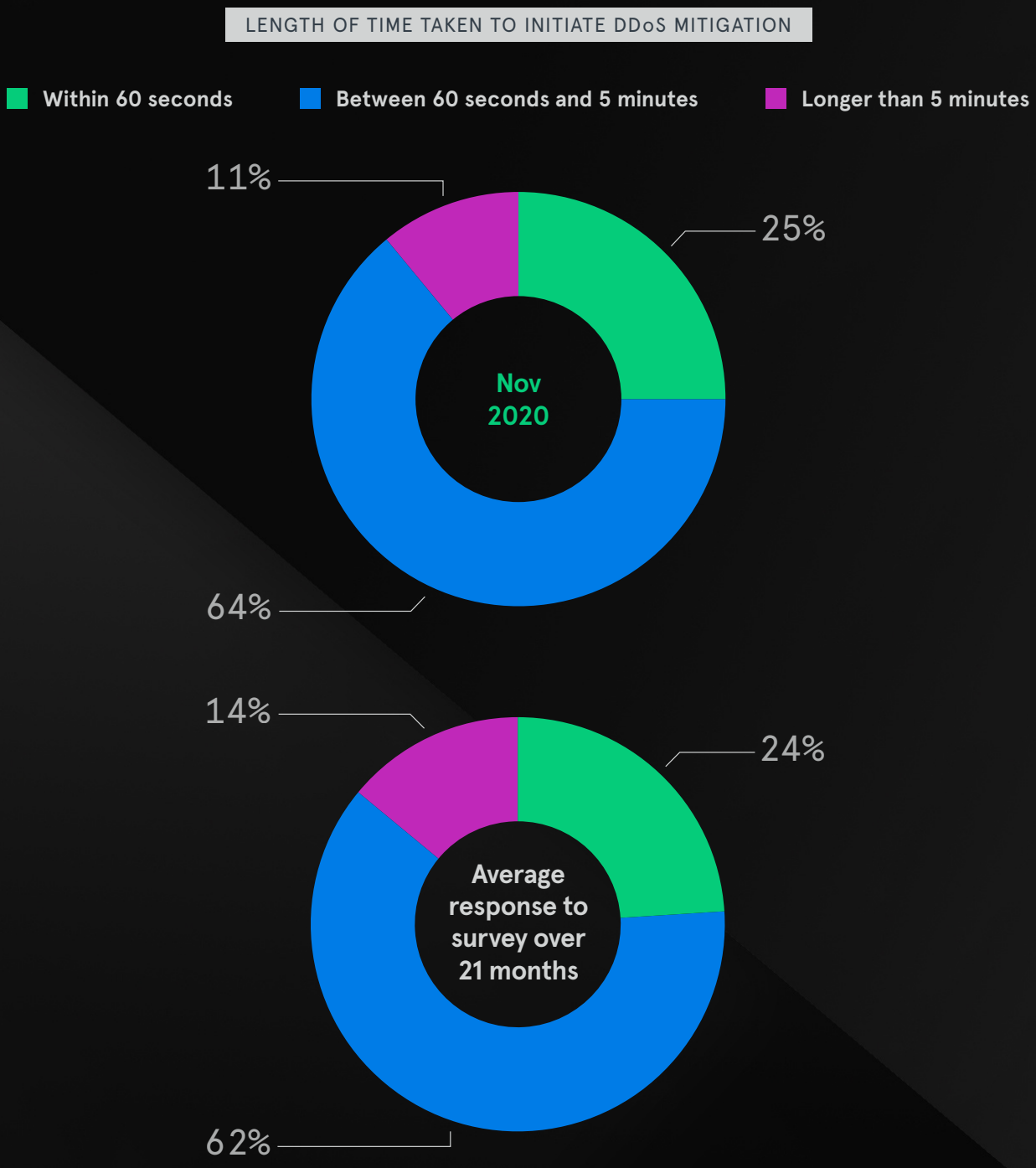

Figure 7: Length of time taken to initiate DDoS mitigation, NISC Survey, Q4 2020

Ransom-Related DDoS

RDDoS is not a new phenomenon for many online industries. The differences between those attacks and the ones we've seen in 2020 can be seen in terms of persistence and sophistication, as well as target. These attackers are aiming at a wide variety of organizations, including those in financial services, government, telecom, and more. Extortion demands have been signed by a number of well-known threat groups, including Fancy Bear and Lazarus Group, both of which are established bad actors that are perhaps better known for other types of attacks.[1] It is important to note that even though extortion emails are "signed" by these groups, they may actually have been originated by others.

Clients that receive extortion threats are typically sent a demand letter that follows an almost templatized format. In the letter, users are threatened with a DDoS attack unless the demands for payment, usually in Bitcoin, are met. The attackers say that they will send a sample attack the next day and threaten a high volume—up to 2Tbps—of attack traffic if the ransom is not paid.[2]

An INTERPOL assessment of cybercrime throughout the pandemic has shown "a significant target shift from individuals and small businesses to major corporations, governments, and critical infrastructure."[3] This dovetails with an FBI notification in July[4] warning of cyber actors exploiting built-in network protocols to carry out larger, more destructive DDoS attacks. It is further validated by warnings from the Cybersecurity & Infrastructure Security Agency (CISA), which issued a warning about DoS and DDoS attacks against multiple sectors in September of 2020, saying that the agency is "aware of open-source reporting of targeted denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks against finance and business organizations worldwide."[5]

It has been postulated that one reason for the adoption of DDoS as a ransom vector, as opposed to using malware, is the ease with which such attacks can be carried out. Inserting malware or ransomware into organizations takes time and careful planning. Launching a DDoS attack, in comparison, has become relatively simple and has the added benefit of being harder to trace back to its origin.

WHIMSICAL NAMES; SERIOUS ATTACKS

These organizations are well known, and their names have shown up in connection with many RDDoS attacks in 2020. These attacks may not have been committed by these organizations but rather by other bad actors seeking to capitalize on the fear of high-profile nation-state attacks.[6]

Fancy Bear, APT28, Sofacy Group: Typically targets government, military, and security groups. Believed to have ties with the Russian military intelligence agency, GRU, and to be sponsored by the Russian government.

This group does not typically use DDoS attacks, instead using zero-days, spear phishing[7], and disguised malware drop websites. They join another group, CozyBear (among other names), believed to be Russian-sponsored.

Lazarus Group, APT38, BeagleBoyz: Targeting mostly financial services. Believed to have close ties with the North Korean government. Typically relies on malware frameworks and compromised payment networks and servers.

What's Your Vector, Victor?

Perhaps 2020 didn't see any dramatically new attack vectors emerge, but it certainly saw a greater use of existing ones.

The built-in access protocols that were discussed as possible amplification vectors in 2019 and earlier reports came up again; in fact, a number of them were called out specifically by the Federal Bureau of Investigation (FBI) in a warning in July 2020. These included:

- Apple Remote Management Services (ARMS)
- Web Services Dynamic Discovery (WS-D)
- Constrained Application Protocol (CoAP)

While the FBI acknowledged the misuse of these protocols, they also noted that disabling them could cause a loss in business productivity. The FBI's first recommendation is that companies "enroll in a denial-of-service mitigation service that detects abnormal traffic flows and redirects traffic away from your network."[8] As we've observed earlier in this report, the results of the latest NISC Survey indicates that the market was listening, with the respondents who indicated that they outsourced DDoS mitgation went from fifty two percent in November 2019 to fifty four percent in 2020.

In addition to built-in discovery protocols, some DDoS threats are taking advantage of TCP-based attacks, including TCP SYN and fragmented packet floods. TCP floods are typically used to generate high-intensity attacks, measured in packets per second (or, more typically, millions of packets per second). High-intensity traffic used in DDoS attacks is not designed to saturate a network circuit but rather aims to overwhelm the infrastructure that has to process the packets. Because of the cycles required to go through a TCP handshake, these traffic floods are well suited to generate high-intensity attacks. Also because of the handshake process, TCP-based communications are more difficult to spoof, implying that large attacks may come from botnets derived from devices that have their own source IP address. Generic Routing Encapsulation (GRE) traffic is a similar protocol that has been seen in DDoS attacks this year.

REMOTE WORKERS BRING THEIR OWN KINDS OF THREATS

The pandemic, and the corresponding explosion in employees working remotely, has made organizations' virtual private networks—or VPNs—business-critical. Known DDoS techniques that target the VPN have also risen to prominence.

One such attack features a blend of TCP packets, including those with the SYN flag checked, to make it look as if a remote session was being initiated; packets with the ACK flag checked, to make it look as if a session was already in process; and some with an URG flag to raise the urgency. Because VPNs and VPN firewalls were not typically built to handle the huge volume of traffic that they've been forced to ingest, the infrastructure can be overwhelmed relatively easily. IPsec VPNs can also be attacked via IPsec Internet Key Exchange (IKE) floods, in which spoofed IKE requests are sent to the VPN server, which is then forced to send an IKE response. These attacks used to be more prevalent, but the advent of IKEv2 has eliminated many of them. It is vital to note that SSL VPNs are not free from the potential for DDoS attacks, either. SSL VPNs are as susceptible to SSL flood attacks as any web server. In these attacks, a high volume of SSL handshake requests are used to try to exhaust resources.

The majority of attack vectors for DDoS attacks continue to feature UDP protocols, which, unlike TCP, are easily spoofed, as they lack a "handshake." UDP-based traffic is commonly used for amplification attacks, in which a small request can generate a massive amount of traffic. UDP protocols are usually behind large, high-bits-per-second (or, more likely, gigabits-per-second) volumetric attacks. Vectors include:

Network Time Protocol (NTP): This attack, which can yield an amplification factor of up to 200:1, makes use of open NTP servers.

Connection-less Lightweight Directory Access Protocol (CLDAP): These attacks take advantage of exposed Active Directory servers. CLDAP uses the UDP version of this service, unlike LDAP, which uses TCP. Amplification factors can be over 50 times.

Internet Control Message Protocol (ICMP): This attack makes use of the "ping" function to flood an attacker with echo-request and echo-reply messages. There have been incidences of "sympathetic" attacks caused by pings that are being sent to ensure that a service is functioning.

Domain Name System (DNS): This attack features spoofed requests designed to elicit very large responses, which are sent to open DNS servers. The spoofed requests use the victim's address instead of the attacker's, so all the DNS servers' responses go to the victim.

The attack vectors that we have seen correlate broadly with the activity observed by the Cambridge Cybercrime Centre. They note that some of their results have to do with how they collect stats, saying: "LDAP-based DoS attacks have become popular because of LDAP's large amplification factor[9]. However, there are relatively few LDAP reflectors in the real world and, therefore, our sensors (honeypots) are often used in attacks, making our data representative of worldwide traffic[10]. Similarly, there are very few NTP reflectors, and, hence, we think our data is highly representative of total activity. However, for DNS, the attackers have many millions of potential reflectors to choose from and, thus, our data collection is rather less complete and our figures are rather less reliable."[11]

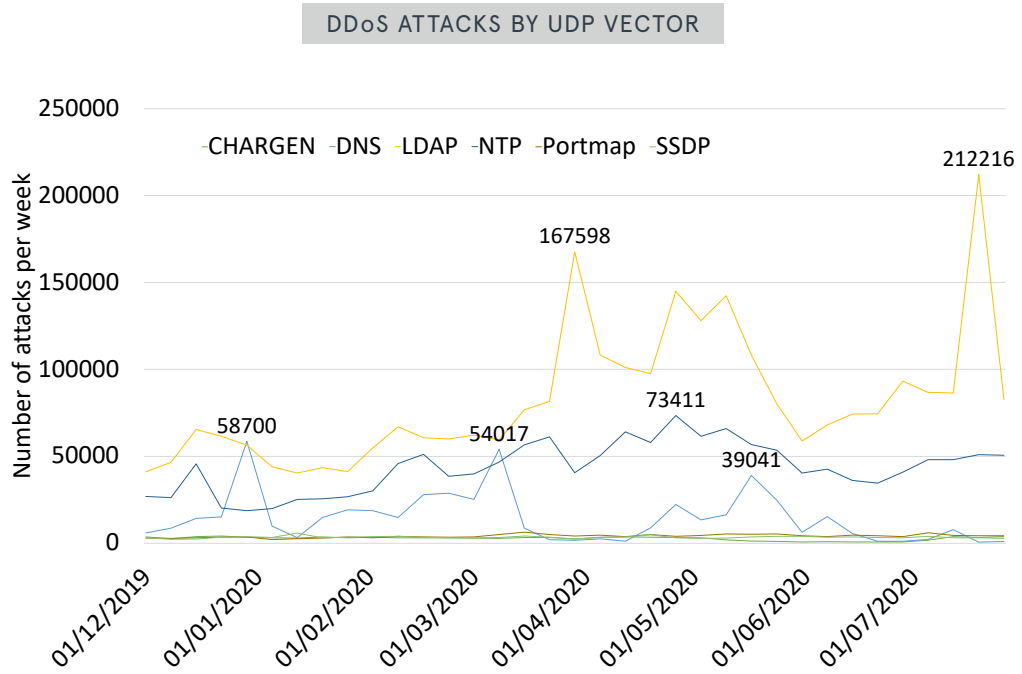

Figure 8: Cambridge Cybercrime Centre, COVID Briefing Paper #11, Analyzing DDoS Attacks by UDP Vector

DIGITAL TRANSFORMATION BRINGS ITS OWN THREATS

If there is one thing that we can all agree on, it is that 2020 is the year that business went digital. According to an Adobe report, "Total online spending in May hit $82.5 billion, up 77 percent year over year; the company estimates that COVID-19 accelerated e-commerce growth 'four to six years.'"[12] At the same time, the number of US store closures by November 15, 2020, was at 14,464, and all kinds of businesses—from restaurants to gyms to car rental agencies—have filed for bankruptcy. Increasingly, those that can move to digital have been pushed to do so, while those who cannot make the move have been pushed out.

The rush to the web has led many companies to get online as quickly as possible. One quick way to get online is to use a content management system (CMS). CMSs allow firms to publish professional-looking content and can enable multiple authors to post. Unfortunately, they are also prone to vulnerabilities. As of August 2020, researchers have identified more than 30 vulnerabilities across 20 popular CMSs,[13] and that's just one type of platform. According to Verizon's Data Breach Incident Report of 2020, web applications are by far the top vector for hacking. The study further notes that is important to reassert that this trend of having web applications as the vector of these attacks is not going away. This is associated with the shift of valuable data to the cloud, including email accounts and business-related processes.[14]

Web applications are the focus of the OWASP. This nonprofit foundation has been dedicated to improving the security of software for 19 years and is known for publishing a top-ten list of application vulnerabilities that can serve as a guidepost for security. The list shows the most common application vulnerabilities, as well as their risks, impacts, and countermeasures. The number-one threat, injection, has occupied the top spot for some time. Verizon showed the relative number of web application attacks graphically, via a block diagram, adding that SQL injection vulnerabilities and PHP injection vulnerabilities are the most commonly exploited. This makes sense, since these types of attacks provide a quick and easy way of turning an exposed system into a profit maker for the attacker. However, in vulnerability data, cross-site scripting (XSS)—the infamous ding popup vulnerability—is the most commonly detected vulnerability, and SQLi attacks are only half as common as XSS.[15]

Complicating matters further is today's move from monolithic applications on massive servers to microservices, in which elements of applications can be separated by functions and located globally, with hardware that could include anything from virtual machines to containers. Such microservices enable innovation by making it easier to make changes, as well as to scale, via allowing assets to be located close to those accessing them. The microservices architecture itself is enabled by application programming interfaces or APIs, with calls often traversing the public network. APIs deliver a unique ability to connect different applications to one another or to connect different functions within a single application. Far from being simple elements of "plumbing," however, APIs should be thought of as vital elements of the applications that they enable, as well as a large and growing attack vector. OWASP actually recognizes APIs as being so significantly different from "typical" web app attacks and their ramifications of such concern that they have created a separate API Security Top Ten list. Even back in 2019 (which, although it seems like a decade past, was only a year ago), approximately 16 percent of organizations said their APIs were subject to daily injection attacks, and 15 percent experienced data leakages at that rate.[16]

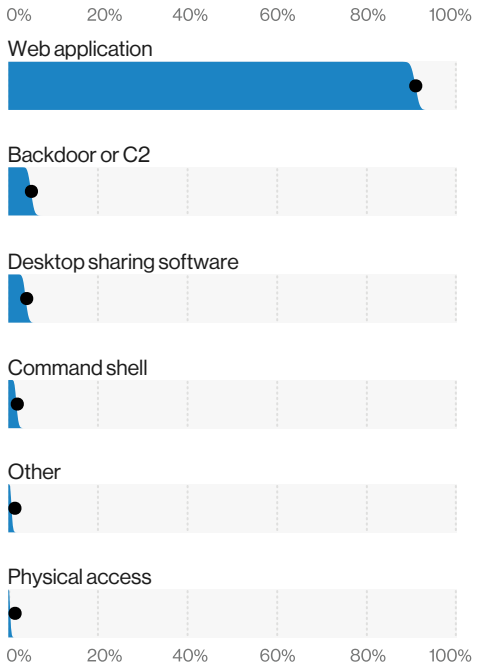

Figure 9: Total hacking vectors, Verizon Data Breach Incident Report, 2020

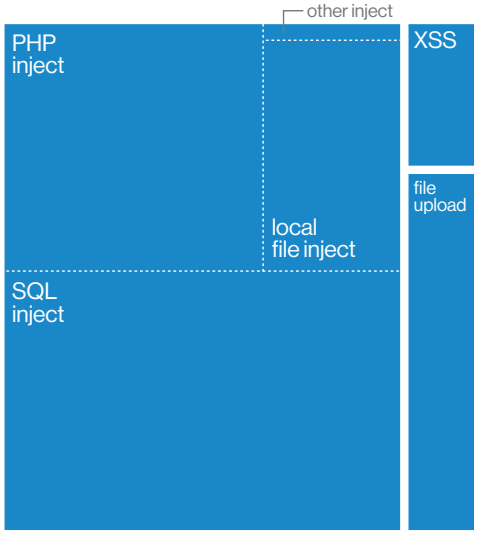

Figure 10: Web application attacks blocks, Verizon Data Breach Incident Report, 2020

Virtual Patching Has Become Vital

Discussion of vulnerabilities leads to another important acronym: Common Vulnerabilities and Exposures (CVE). CVE is a list of publicly disclosed computer vulnerabilities, maintained by MITRE Corporation with funding from the National Cyber Security Division of the US Department of Homeland Security. While there is inevitably some lag between discovery and publish date, these lists are constantly growing.

Patching vulnerabilities is always an ongoing problem, and with the addition of APIs and agile development, it is almost impossible for enterprises to stay on top of this never-ending task. To get an idea of the sheer volume of patches, it is useful to consider just how many are released per month. As you can see below, releases per month range from just over a thousand to double that number. Some of these vulnerabilities are likely minor, but many are not. Note that because of the lag between discovery and posting, some of the most recent vulnerabilities discovered may not have made the list.

Web application firewalls (WAFs) can form a vital part of ongoing defense by enabling virtual patching. OWASP defines virtual patches as a security policy enforcement layer that prevents the exploitation of a known vulnerability. This process can give the enterprise an ability to keep defenses current.

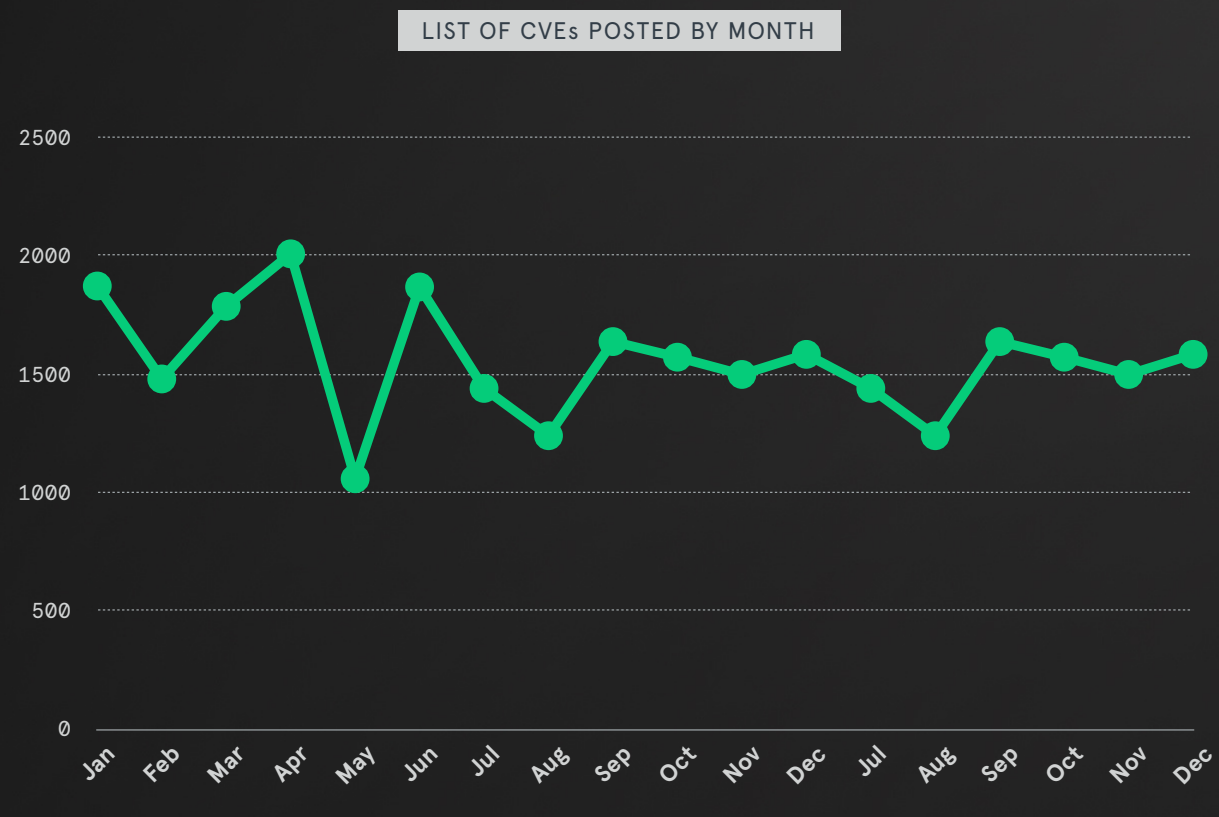

Figure 11: List of CVEs posted by month, National Vulnerability Database

DNS ATTACKS: MORE THAN A VECTOR

In 2020, we also saw an increase in attacks on DNS itself—or what look like attacks, as bad actors abuse the system. "Acting as the internet's address book and backbone of today's digital services, it's unsurprising that DNS is an increasingly appealing vector for malicious actors, particularly as more consumers turn to websites during peak online shopping periods," said Rodney Joffe, Neustar's SVP, Fellow and Cybersecurity Expert.

The majority of respondents to the most recent NISC survey agree. Three in five respondents reported having been the victim of a DNS attack in 2020, and a variety of different threat types have been used.

Figure 12: DNS threats that organizations have been victim of in the past year, NISC Survey, Q4 2020

Even more troubling, over 70 percent of organizations admit to having reservations about their awareness of and ability to respond to DNS attack threats.

ORGANIZATIONS AWARENESS & PREPAREDNESS TO RESPOND TO THREATS LAUNCHED AS PART OF A DNS ATTACK

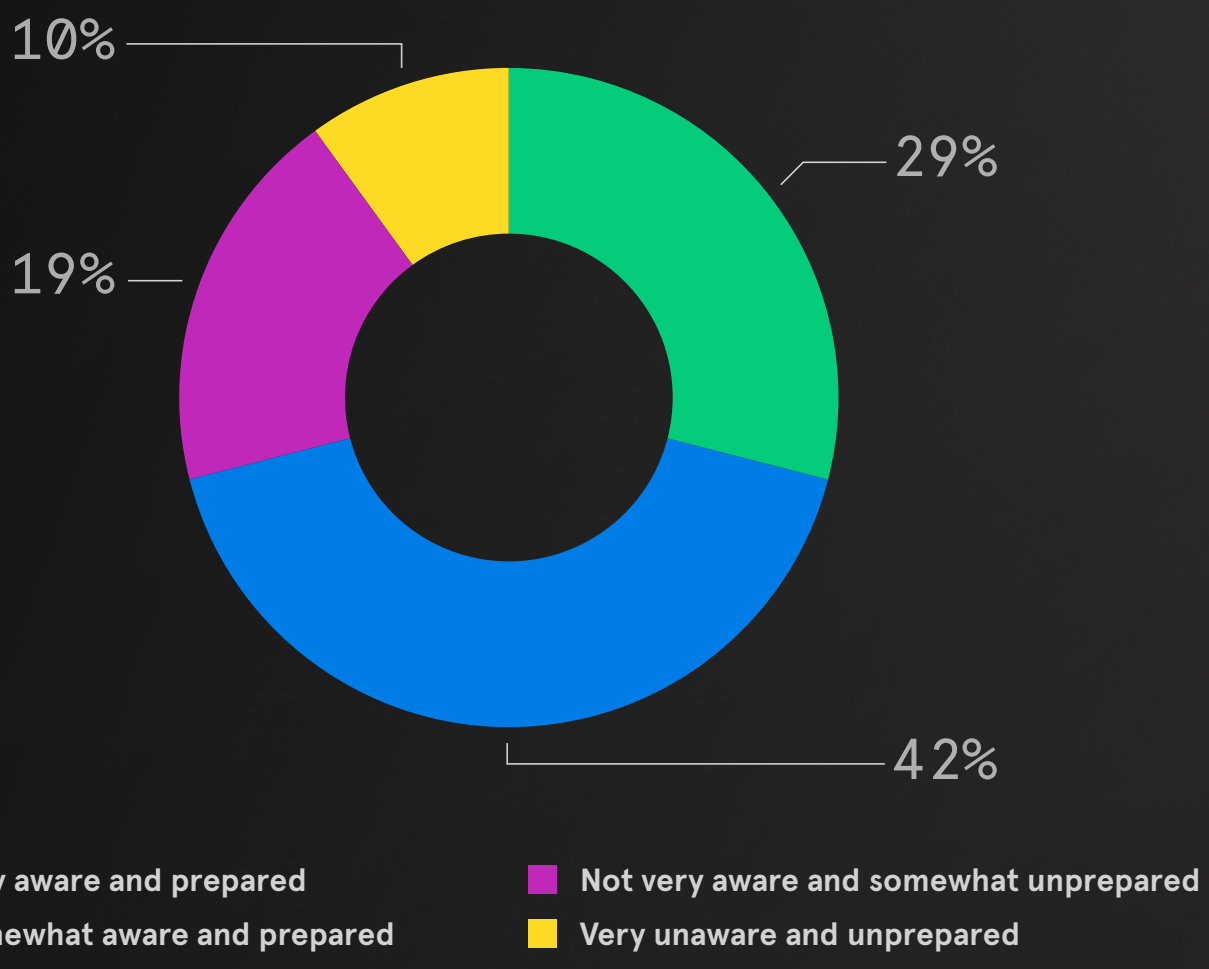

Figure 13: Organizations awareness and preparedness to respond to threats launched as part of a DNS attack, NISC Survey, Q4 2020

Some attacks on DNS, including DDoS, TCP SYN floods, and DNS flood attacks, are familiar from our DDoS discussions. That is because DNS services are meant to be "open," albeit heavily protected. In cases where organizations are running their own DNS servers, however, they will be more susceptible to DDoS attacks such as these. Managed or hosted services are typically protected with always-on DDoS attack mitigation, in addition to being massively overprovisioned, as is the case with Neustar UltraDNS.

While most managed services have built-in protections for many of these attacks, it is worthwhile to consider how each one of them works. Some of the most prevalent DNS-specific attacks seen in 2020 include domain hijacking, DNS cache poisoning, zombie/phantom domain attacks, and DNS tunneling.

Domain hijacking is when a bad actor gains control of a target's DNS information, and then makes unauthorized changes. In many cases, these attacks begin with some type of social engineering to gain access, although they can also result from a successful cache-poisoning exploit. Domain hijacking is one of the most difficult attacks to recover from, as some countries (not to mention customers) will hold the target company responsible for any data leaks or breaches that occur during such events.

DNS cache poisoning is a result of the fact that recursive name servers temporarily store, or cache, information learned during the name resolution process. Cache poisoning can occur when an adversary sends fake (spoofed) DNS responses to a recursive name server, pretending they came from an authoritative name server. When malicious information is cached on the recursive name server, the server is considered "poisoned." If the "bad route" is followed successfully, it will result in the bad address being cached on the user's computer and can make its way into the local resolution DNS system. These bad addresses can be the result of a "man in the middle" attack. These attacks can be fairly easily defeated by the use of Domain Name System Security Extensions (DNSSEC). DNSSEC is not enabled by every managed DNS provider, and the threat of DNS cache poisoning is a major reason to consider this facet of cybersecurity.

Phantom, zombie, or botnet-based domain attacks could be considered a form of DDoS, as they use a botnet to submit requests to local or self-managed DNS services for domains that do not exist. The DNS system nonetheless has to try to resolve these domains, wasting resources as they do. A managed DNS service, which should be protected by DDoS mitigation, will see these threats for what they are and can quickly offload the traffic. Another mitigation technique that can be used is to require clients to use TCP, with its attendant handshake process, rather than the common UDP form, which does not use the handshake process.

DNS tunneling takes advantage of the fact that, although most organizations block or filter HTTP or FTP traffic to restrict access to malicious sites, they are unlikely to apply the same techniques to DNS traffic. Attackers take advantage of this open and established pathway to sneak other programs or code inside packets, which are crafted to be interpreted by security devices as legitimate DNS queries and responses. In doing so, they can enable and obscure both data exfiltration and infiltration and establish "command-and-control" (C2) channels without being detected.

DNS-based attacks are extremely costly, not just to the bottom line but also to brand and reputation. A recent IDC study stated that the average cost of a DNS attack is $924K, with the biggest impact coming from application downtime as assets move to the cloud. Neustar's Rodney Joffe says "When successful, DNS attacks can have damaging repercussions to an organization's online presence, brand, and reputation. A domain hijacking attack, for example, can result in hackers taking control of a company's domain and using it to host malware or launch phishing campaigns that evade spam filters and other reputational protections. In a worst-case scenario, this type of attack can even lead to an organization losing its domain altogether."

Even more ominous, DNS attacks can take a long time to repel, and that's important, since the bulk of the costs from DNS attacks are application downtime. According to IDC, the average time taken to mitigate DNS attacks is over 5 hours.[17] Joffe says it's a positive sign that organizations are aware of the severity of DNS attacks, but it is also important that they continue to take proactive steps to protect themselves and their customers against the different threats. "This should involve regular DNS audits and constant monitoring to ensure a thorough understanding of all DNS traffic and activity," he said.

WHEN BUSINESS CLOSURE BECOMES BIG BUSINESS

We all know that many businesses have had to close their doors in 2020, either temporarily or for good. As of August 2020, Yelp reported that 163,735 businesses had indicated that they have closed. Of that number, 97,966 or 60 percent have indicated that their closures are permanent. This represents a 23-percent increase since previous results were listed in mid-July.[18]

While this news represents a sad reality for businesses, it is a huge boon to cybercriminals for whom abandoned domains can represent a direct way into sensitive corporate and personal data. Cybercriminals can obtain a wealth of data on customers via the abandoned domains that businesses may leave behind. Attackers can also potentially regain access to Office 365 or G Suite accounts and hijack personal user accounts. These data sources can include:

- Confidential documents of former clients
- Confidential documents of a former practice
- Private email correspondence
- Personal information of former clients

Abandoned second-level domain names pose an additional threat to other companies as well. That's because most security systems have some form of contextual categorization in which frequently visited domains have been categorized as safe to visit; examples could include restaurants or retailers. Based on the categorization, you may be unaware that the business went under. Given that you have trusted that company in the past, you have no reason not to trust it going forward—until you get more up-to-date information that tells you otherwise. This can lead to the acquisition of domains for phishing campaigns, as these may not be picked up by firewalls, given that many categorization lists may not be up to date.

WHAT WILL THE "NEXT NORMAL" LOOK LIKE?

No matter what comes next, we can be sure that it won't be anything like what has gone before, particularly in the world of cybersecurity. The digital world will not return to a 2019 state and will almost certainly incorporate elements of what may have been stopgap moves in 2020. That means looking at cybersecurity at a scale that may be new.

Where to Begin?

Whether you have moved (or been pushed) to digital transformation, it is important to consider that security solutions that have worked in the past may not work in today's environment. Take nothing for granted and start from ground zero to the extent that you can. This process is really just a reframing of security industry best practices, although the high stakes and compressed timeframe provide a charged backdrop.

What Are You Protecting?

A good place to start is by understanding what you have to protect. It's likely that employee connectivity is close to the top of the list. Your business has moved from having to protect a corporate infrastructure to now having to protect a largely remote infrastructure. The attack surface that security teams face has not doubled, as it would if you added one remote office, but rather increased exponentially. For example, if your company has 1,000 employees that are now working remotely, your security team is now in charge of 1,000 small remote offices. Not only do you have the remote workers themselves to contend with, but you must also consider the other unprotected devices that could be in use on the network at the same time, as education has moved online and IoT devices have boomed. The corporate VPN has suddenly become essential. Online collaboration tools that might be appropriate from inside a company may not be suitable for use when all users are remote and depend upon varying types of "last mile" connections.

From there, consider your most business-critical assets, as well as attackers that could be drawn to them. Once you have determined what the business cannot live without, it's time to go further. Where is the asset/application/service located? Is it in the public cloud, private cloud, your datacenter, or some combination? Each location type could be vulnerable to threats that are specific to the infrastructure; for example, the same application housed in a corporate datacenter will have a different attack profile than an application that is served in a containerized microservice on the public cloud. And remember to look hard at the foundational CMS as well as any APIs that are in use.

Once you've considered the asset and where it is housed, you must look at what is going on in your industry. For example, while online gaming companies have long been susceptible to RDDoS attacks, the threat may have spread to your vertical market as well. As companies have had to rapidly move business online, it is not uncommon for the firms within a vertical to use the same framework as one another. Attackers look for that, and a successful attack in one space usually leads to more.

How Can You Protect It?

A good place to start applying protection once you've considered your assets' vulnerabilities is by taking the FBI's advice. If you don't currently have a DDoS mitigation vendor, this is a great time to consider getting one. If you do work with a vendor, you might want to consider always-on mitigation. This is especially the case if you're in an industry that has attracted RDDoS attacks.

If you have web apps, you also have vulnerabilities; they are unavoidable, particularly in today's microservices architecture. Be sure that your WAF(s) protect your apps from the OWASP top vulnerabilities and support virtual patching. You may want to consider augmenting on-prem appliances with a cloud-based WAF to lighten the load. And whatever you do, don't forget your APIs!

Another element that should be considered for fortification is your DNS. Even if you have never considered a managed DNS service, now may be the time to look more closely, because the risk is greater than ever. At Neustar, DNS traffic was 220 percent higher in the first three quarters of 2020 than in all of 2019. Cache poisoning or other such exploits could irreparably ruin your brand. These attacks can be prevented by the use of DNSSEC, but these protections can be tricky to implement on your own. If you do have—or decide to try—a managed DNS vendor, make sure that they support the DNSSEC specification, because not all do.

Finally, as employees begin to return to the office, make sure that domains that were trusted in the past are still in (the same) business. A good way to do that is to look for newly observed or revived domain names. Threat feeds will show domains that have suddenly become active after a period of inactivity and also keep you abreast of recently removed or recently registered domains.

There Is No Silver Bullet

Finally, consider that there is no one solution that will secure everything, and anyone who tells you different is trying to sell you a bag of magic beans. There is not a single panacea. For that reason, it's essential to look at security holistically, rather than in a piecemeal, point-product fashion. Additionally, look for vendors that can tailor their offering to your requirements, rather than those that try to shoehorn you into their standard offering.

GLOSSARY

ACK – Acknowledgement
AI – Artificial Intelligence
API – Application Programming Interface
ARMS – Apple Remote Management Service
C&C – Command and Control
CDC – Centers for Disease Control and Prevention
CHARGEN – Character Generator Protocol
CoAP – Constrained Application Protocol
CVE – Common Vulnerabilities and Exposures
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
GRU – Russian Main Intelligence Directorate
HTTP – HyperText Transfer Protocol
IoT – Internet of Things
IP – Internet Protocol
IPsec – Internet Protocol Security
ISP – Internet Service Provider
IT – Information Technology
LAN – Local Area Network
LDAP – Lightweight Directory Access Protocol
M3AAWG – Messaging, Malware and Mobile Anti-Abuse Working Group
Mbps – Megabits per second
Mpps – Million packets per second
N95 – A government efficiency rating usually used in connection with facial masks. The rating indicates that the mask blocks about 95 percent of particles that are 0.3 microns in size or larger
NISC – Neustar International Security Council
NIST – National Institute of Standards and Technology
NTP – Network Time Protocol
NVD – National Vulnerability Database
NXNS – Non-eXistent Name Servers Attack
PII – Personally Identifiable Information
Portmap – An Open Network Computing Remote Procedure Cal
POST – An HTTP method which sends data to a server to create/update a resource
RDoS/ RDDoS – Ransom Related Denial of Service/ Distributed Denial of Service
SaaS – Software as a Service
SARS – Severe acute respiratory syndrome
SIEM – Security Information and Event Management
SOC – Security Operations Center
SQL – Structured Query Language
SQLi – An injection attack that makes it possible to execute malicious SQL statements
SSDP – Simple Service Discovery Protocol
SSL – Secure Sockets Layer
SYN – Synchronize
Tbps – Terabits per second
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
URG – A flag that is used to inform a receiving station that certain data within a segment is urgent and should be prioritized
URL – Uniform Resource Locator
WHO – World Health Organization
WS-DD – Web Services Dynamic Discovery

REFERENCES

1 https://www.wired.com/story/ddos-extortion-hacking-fancy-bear-lazarus-group
2 https://www.techrepublic.com/article/ransomware-campaign-threatens-organizations-with-ddos-attacks
3 https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
4 FBI Private Industry Notification; PIN 20200721-002, July 21, 2020
5 https://us-cert.cisa.gov/ncas/current-activity/2020/09/04/dos-and-ddos-attacks-against-multiple-sectors
6 https://www.wired.com/story/ddos-extortion-hacking-fancy-bear-lazarus-group/
7 https://www.wired.com/story/russias-fancy-bear-hackers-are-hitting-us-campaign-targets-again/
8 FBI Private Industry Notification; PIN 20200721-002, July 21, 2020
9 University of Cambridge, Cambridge Cybercrime Centre, September 15, 2020
10 University of Cambridge, Cambridge Cybercrime Centre, September 15, 2020
11 University of Cambridge, Cambridge Cybercrime Centre, September 15, 2020
12 https://www.forbes.com/sites/johnkoetsier/2020/06/12/covid-19-accelerated-e-commerce-growth-4-to-6-years/?sh=236d0ea8600f
13 https://www.securityweek.com/over-30-vulnerabilities-discovered-across-20-cms-products#:~:text=Researchers%20have%20identified%20more%20than,Microsoft%20SharePoint%20and%20Atlassian%20Confluence
14 https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
15 https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
16 https://businessinsights.bitdefender.com/api-security-a-top-concern-for-cybersecurity-in-2020
17 IDC 2020 Global DNS Threat Report
18 https://www.cnbc.com/2020/09/16/yelp-data-shows-60percent-of-business-closures-due-to-the-coronavirus-pandemic-are-now-permanent.html

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-267252-07.28.21