NEUSTAR SECURITY

2019: THE YEAR IN REVIEW

Cyber Threats & Trends Report

neustar® Security

Table of Contents

Knowing Your Enemy Is the Best Defense

It's a typical Monday morning. Bob in marketing arrives at his desk and starts going through his email. Strangely, there is a notice from his bank. It seems that someone has been making high-dollar charges using his credit card. His bank urgently requests that he log in to his online account, using the link they've included, to verify that the purchases are bogus. His bank's name is in the URL, and the website looks legit.

As a security professional, of course, you recognize the email as a likely phishing attempt, rather than a genuine alert from a bank. You might guess that the site did not belong to Bob's bank, but rather to a clever hacker who was able to replicate the real site in almost every respect, starting with the URL in the link. But Bob, in a panic over his credit, may not realize this in time. Bob's credentials are collected, and the individual damage is done, but it doesn't stop there. Just by clicking on the link, Bob triggers a malware download that infects his device and starts to spread inside your network.

This scenario is not one that *might* happen; it's a scenario that has happened and continues to happen around the world millions of times every day. Using tools like DNS Twister, it's easy for bad actors to create permutations of legitimate links that are so close to the real site, they're virtually indistinguishable.

Later, when the breach has been stopped and the attack has been catalogued, you could end up knowing a lot about your enemy via analysis conducted by a provider of threat intelligence. These reports may detail who spearheaded the attack and with which malware. You might even have a new signature to add to your security devices. Other companies may benefit from your breach through the intel yielded. But no matter how beneficial the threat intelligence may be, it's no substitute for preventing the breach in the first place. By the time that pertinent threat intelligence has been compiled, the damage to you—or to another victim—is done.

Prevention, Not Remediation

This approach sounds counterintuitive. After all, if you knew that the request was from a malicious actor or that the link was going to go to a malicious site, you probably would have blocked the delivery of the email altogether! But if the threat analysis was not yet available, how would you know?

The answer is: reliable threat data that's sent to you in as close to real time as possible. Such a feed should include data on newly registered domains (NRDs), since research has shown that 70 percent of NRDs are "malicious" or "suspicious" or "not safe for work."[1] Additionally, the feed should include domain names created by domain generation algorithms (DGAs). It is not uncommon for cybercriminals to use DGAs to mask their true command and control (C&C) points, in order to make their botnet more resilient against takedown efforts and seizures conducted by law enforcement agencies or IT security researchers.[2] Regardless of how these sites are created, it is important to note that most sites set up for malicious purposes are extremely short-lived. By the time you've culled the data, the site may already be gone.

Get the Right Information

Trying to stop innocent users from going to sites that may be malicious is a primary example of how you can use current threat data. But even more nefarious is when the Domain Name System (DNS) is used to "tunnel" data out of the enterprise. This method of exfiltration depends upon the fact that firewalls allow traffic via port 53, which is commonly used for DNS. This same port can be used to set up a tunnel out of the enterprise.

Another element to look out for is traffic coming from anonymous proxies. These servers, which sit between the sender and the target, are designed to disguise the IP address of the sender. While there are legitimate uses for anonymous proxies, such as evading censorship or hiding from oppressive governments, they're also used for malicious purposes. In fact, they've been used to launch amplification Distributed Denial of Service (DDoS) attacks as well as host C&C infrastructure for botnets.

Get the Right Vendor

Identifying sources of potentially malicious traffic for each of these use cases requires a level of expertise and understanding of fraudulent behavior that's difficult to find from a typical threat research organization. A good vendor needs to have the ability to ingest a large amount of data associated with traffic on the internet as well as the knowledge and capability to process and discern patterns within it. Additionally, consider where the raw data came from—is it proprietary, such as DNS exhaust from a system that the vendor owns, or is it purchased? Then look at how the information is refined. What volume of data is being considered? If the datasets are large enough to yield a reliable result, the vendor is almost certainly using some form of machine learning (ML) to process them. Finally, consider the frequency with which data is added. Given the short lifespan of most malicious sites, it's important that the threat data is as fresh as possible.

Make the Best Use of Threat Data

There is a tradeoff between timeliness and accuracy when using near real-time threat feeds to inform security controls. The value is that you can use the information to enhance security almost as soon as something unusual is seen anywhere on the Internet. The downside is that without complete analysis, it can be difficult to be absolutely certain that the site is actually malicious and not just suspicious. One way to use this information, then, is to build safeguards around how the data is used.

Threat feeds can be directed to your Security Information and Event Management (SIEM) system and sent out to your security devices to protect against inbound threats. You may choose to block traffic completely via access control lists (ACLs), or you could take a log-and-watch approach. You could also use the information to catch or flag responses to suspicious sites on their way out of your network, as newly created sites could represent a botnet C&C. This could be significant, as the number of domain names registered and set up by cybercriminals for the sole purpose of hosting a botnet C&C increased by over 100 percent between 2017 and 2018, and the trend shows no signs of slowing.[3]

The methods above are just examples of the way that you can infuse threat data throughout the security devices in your network. Look for a vendor that enables you to choose how and where this data is deployed, because every network is different. One fact remains consistent, however: In the world of security, time is not on your side.

—Rodney Joffe

Rodney Joffe

Neustar Senior Vice President,
Senior Technologist and Fellow

Rodney Joffe serves as Neustar's security chief technology officer, senior vice president, and fellow. His accomplishments include founding the first commercial Internet hosting company, Genuity, as well as the first outsourced and cloud-based domain name system (DNS) company, UltraDNS, where he invented Anycast Technology for DNS. Joffe has served on a number of the US government's cybersecurity intelligence panels and was the leader of the groundbreaking Conficker Working Group. He is one of the first civilians to receive the Federal Bureau of Investigation (FBI) Director's Award, due in no small part to his role in uncovering and taking down the Butterfly Botnet. He has also been honored with the Mary Litynski Lifetime Achievement Award from M3AAWG (the global Messaging, Malware, and Mobile Anti-Abuse Working Group) and was most recently publicly recognized for his years of work and dedication in helping protect against cybercrime, winning The Computing Security Award for his contribution to cybersecurity in 2018. Joffe is also the chairman of the Neustar International Security Council (NISC), which comprises an elite group of cybersecurity leaders across industries and companies who meet regularly to discuss the latest cyberattack trends.

Q4 2019 Threats & Trends

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 during Q4 2019. This report offers a unique view into the attack trends that are unfolding online, including attack statistics and behavioral trends for Q4 2019.

Comparing Q4 2019 to Q4 2018, the number of attacks on directly provisioned customers has increased by 168 percent. The largest attack size observed in Q4 2019 was 349 Gbps in volume, which represents a 22 percent decrease from the largest attack seen in Q4 2018. The longest duration attack lasted for over three days; it is worth noting that this incident was a single, uninterrupted attack, rather than a series of attack waves.

168%

Increase in number of attacks in Q4 YoY

349 Gbps

Largest attack size in Q4 2019

22%

Decrease in the largest attack size in Q4 YoY

3 DAYS | 13 HRS | 8 MIN

Longest attack duration in Q4 2019

The number of attacks by size category in Q4 2019 vs. Q4 2018 shows the largest growth in the 25 to 50 Gbps category.

PERCENTAGE CHANGE IN NUMBER OF ATTACKS BY SIZE

Q4 2019 vs. Q4 2018

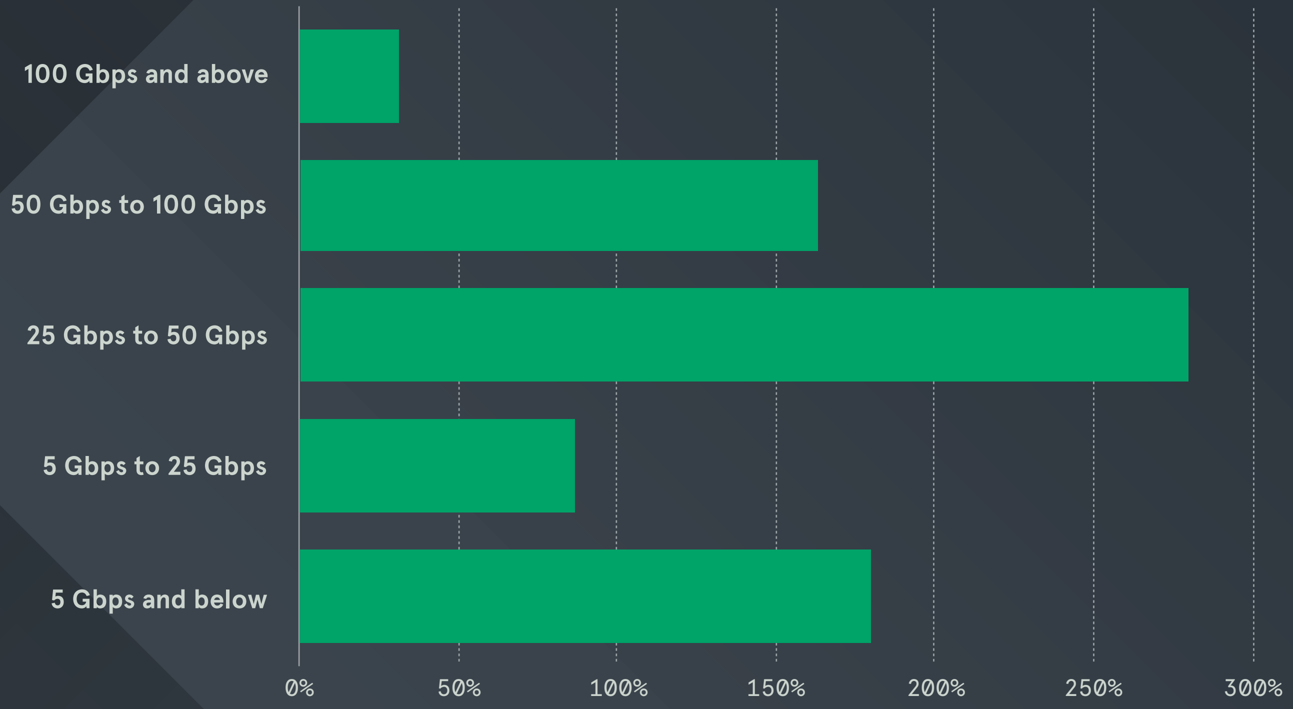
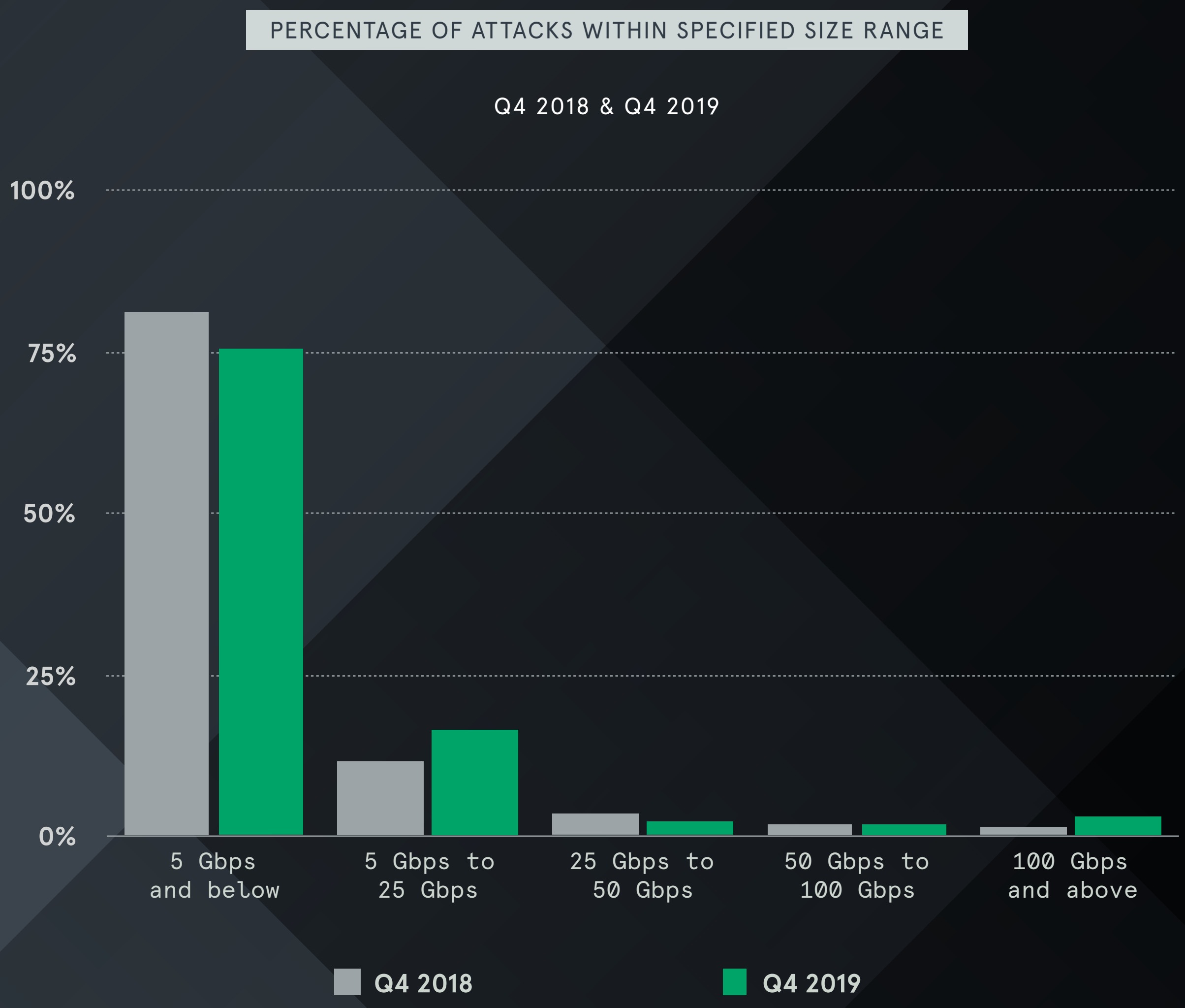


Figure 1: Percentage change in number of attacks by size category, Q4 2019 vs. Q4 2018

ATTACK VOLUME

In Q4 2019, over 80 percent of attacks mitigated by Neustar were 5 Gbps or less. This finding is consistent with what we saw in the same time period of 2018. While the number of attacks in all categories increased in Q4 2019, the composition remained consistent.


PERCENTAGE OF ATTACKS WITHIN SPECIFIED SIZE RANGE

Q4 2018 & Q4 2019

Figure 2: Percentage of attacks within specified size range, Q4 2018 and Q4 2019

ATTACK VOLUME

Q4 2018 VS Q4 2019

12.5Gbps

Average attack size in Q4 2018

7Gbps

Average attack size in Q4 2019

78%

Decrease in average attack size

ATTACK INTENSITY

Comparing the intensity of attacks in Q4 2019 to the intensity of attacks in Q4 2018, Neustar observed that, at 220 Mpps, Q4 2019's most intense attack was dramatically higher than the most intense attack of Q4 2018. This attack represents a 378 percent increase in the most intense attack, while the overall average intensity of attacks for these periods was virtually unchanged.

Q4 2018 VS Q4 2019

46 Mpps

Most intense in Q4 2018

220 Mpps

Most intense in Q4 2019

378%

Increase in intensity in Q4 YoY

1.6 Mpps

Average intensity in Q4 2018

1.7 Mpps

Average intensity in Q4 2019

THREAT VECTORS

In Q4 2019, over 86 percent of all attacks mitigated by Neustar used two or more vectors. Neustar also observed a significant number of attacks that featured more than four threat vectors in that period as well.

NUMBER OF THREAT VECTORS PER ATTACK Q4 2019

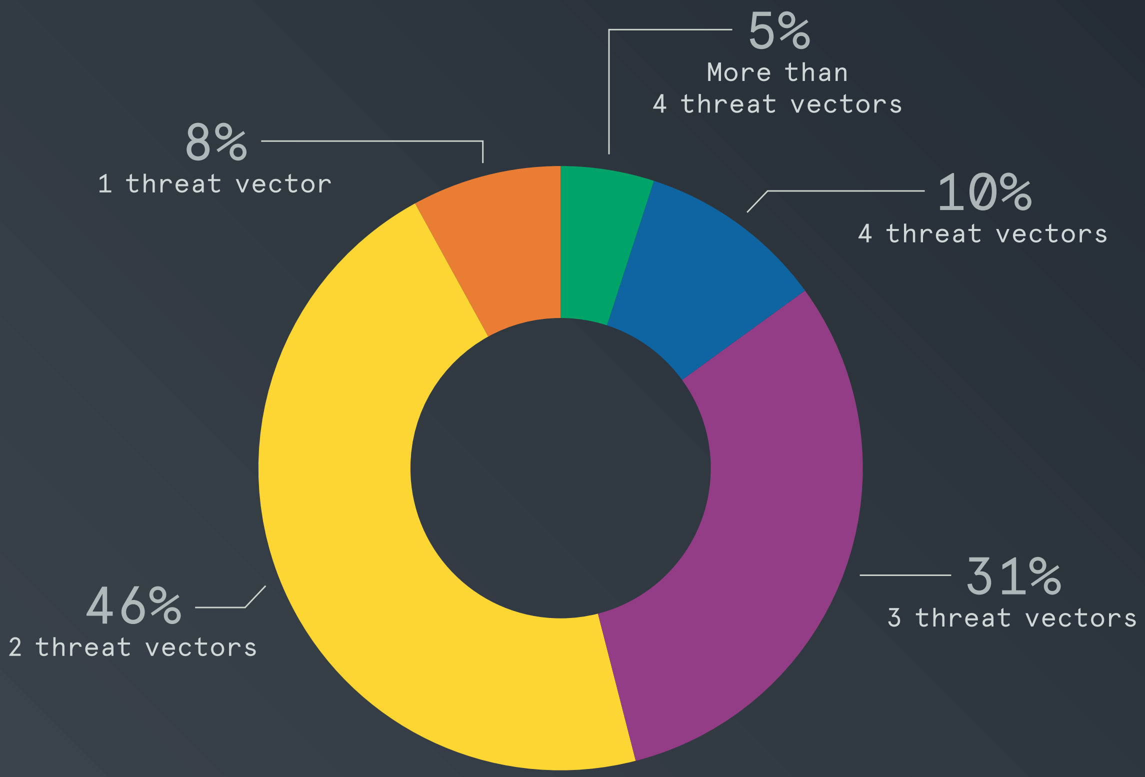


Figure 3: Threat vectors per attack, Q4 2019

2019: The Year in Review

Neustar has mitigated almost three times as many DDoS attacks in 2019 vs. 2018. The largest attack mitigated, 587 Gbps, was 31 percent larger than the largest attack of 2018.

180%

Increase in the number of attacks 2018 to 2019

587Gbps

Largest attack size in 2019

31%

Increase in the largest attack size, 2018 vs. 2019

3 DAYS | 13 HRS | 8 MIN

Longest attack duration in 2019

ATTACK VOLUME

When we consider the number of attacks by size category in 2019 vs. 2018, there is a pronounced increase across the board.

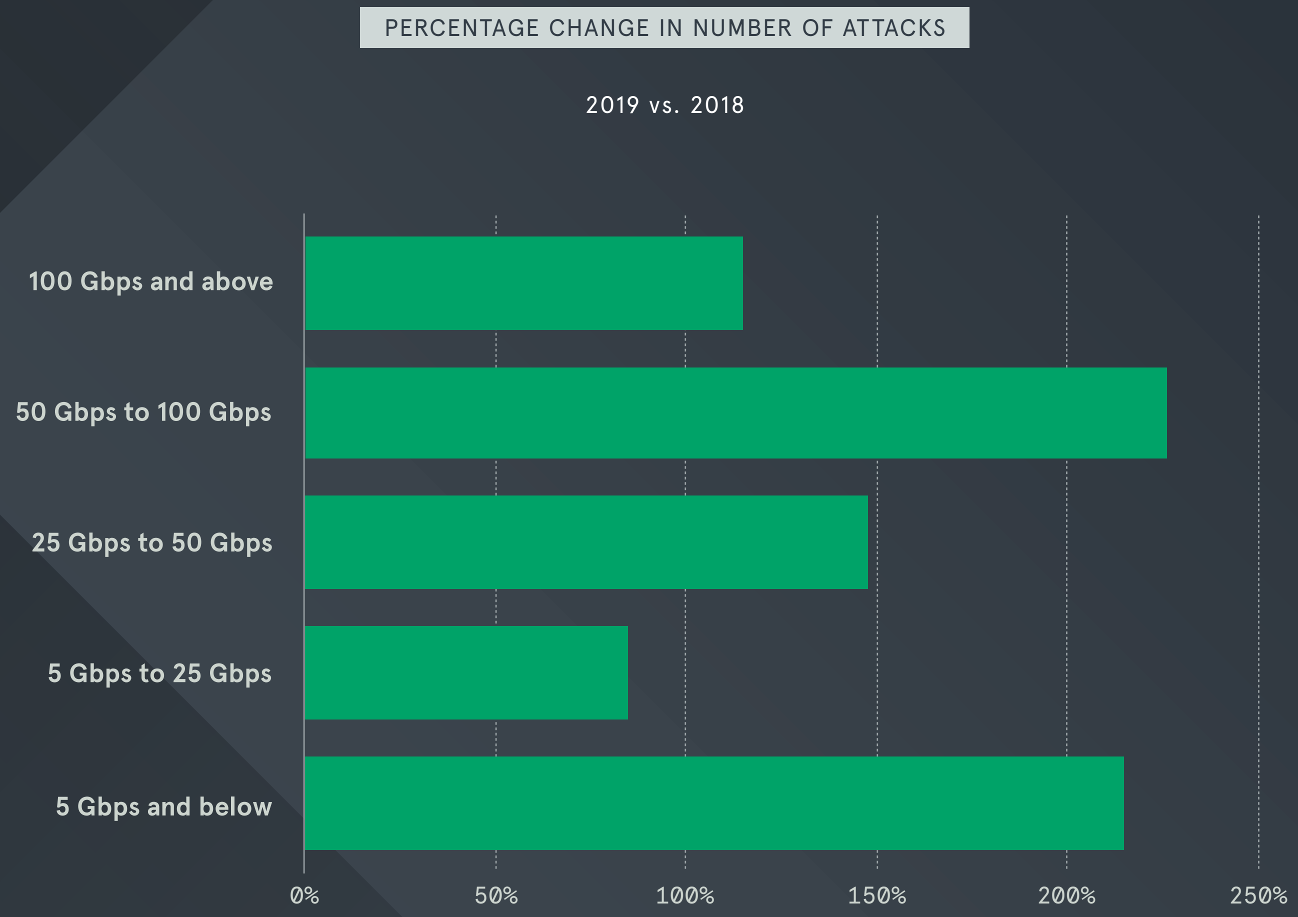


Figure 4: Percentage change in number of attacks 2019 vs. 2018

The number of attacks increased in all categories in 2019. However, when we look at the composition of the attacks that make up the overall numbers, normalized by percentage to account for quantity, the results are consistent.

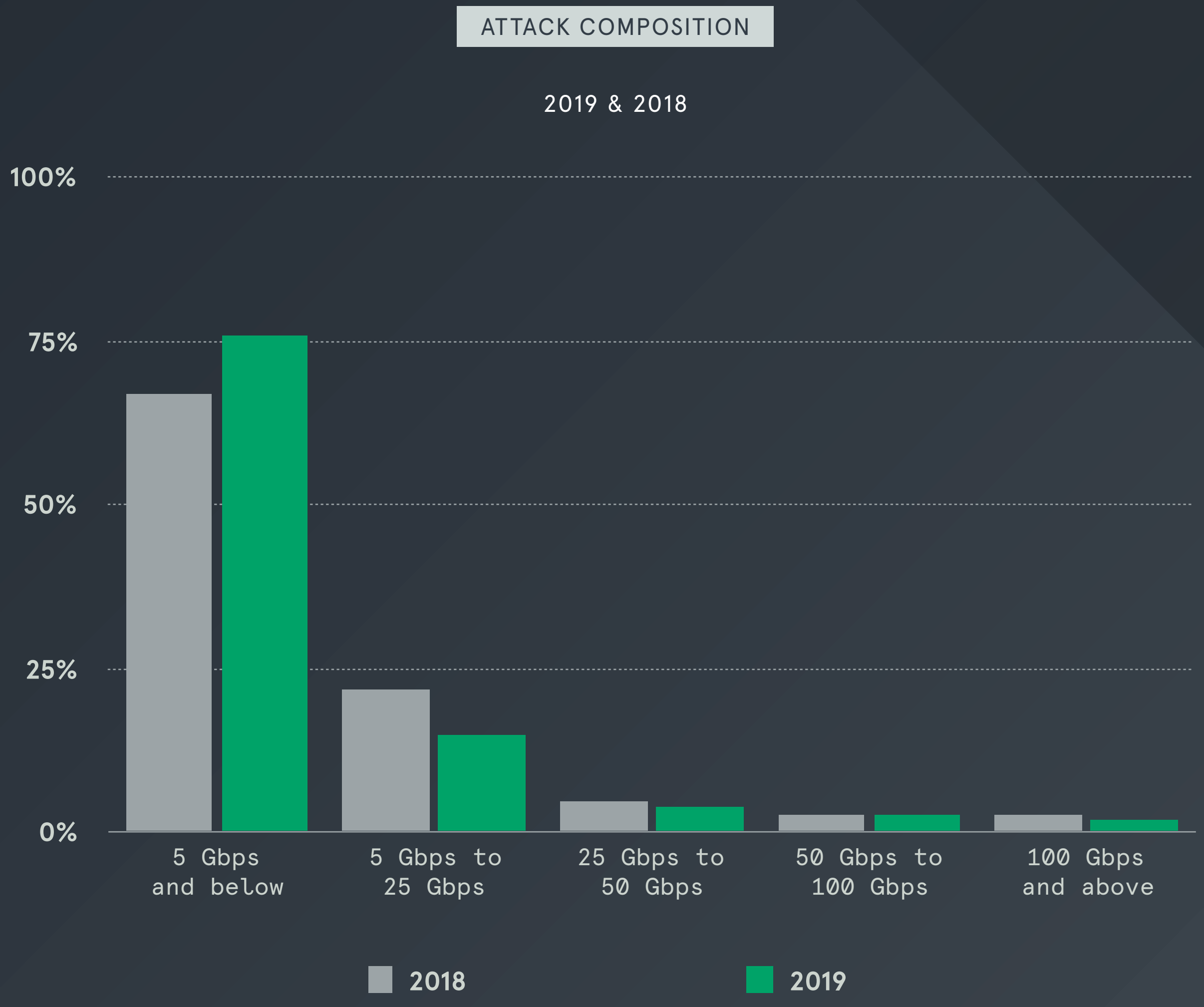


Figure 5: Percentage of attacks within specified size range, 2019 and 2018

12Gbps

Average volume in 2018

12Gbps

Average volume in 2019

ATTACK INTENSITY

When we consider attack intensity, comparing 2018 to 2019, we observed that the most intense attack of 2019 was 252% higher than the most intense attack of 2018. As we observed in the Q4 YoY comparisons, the average intensity remained consistent.

2018 VS 2019

97.5 Mpps
Most intense in 2018

343 Mpps
Most intense in 2019

252%
Increase in top intensity YoY

3 Mpps
Average intensity in 2018

3 Mpps
Average intensity in 2019

THREAT VECTORS

In 2019, over 85 percent of all attacks mitigated by Neustar used two or more vectors. These findings are comparable to what was observed in 2018, with the bulk of attacks mitigated featuring between 2 and 4 threat vectors.

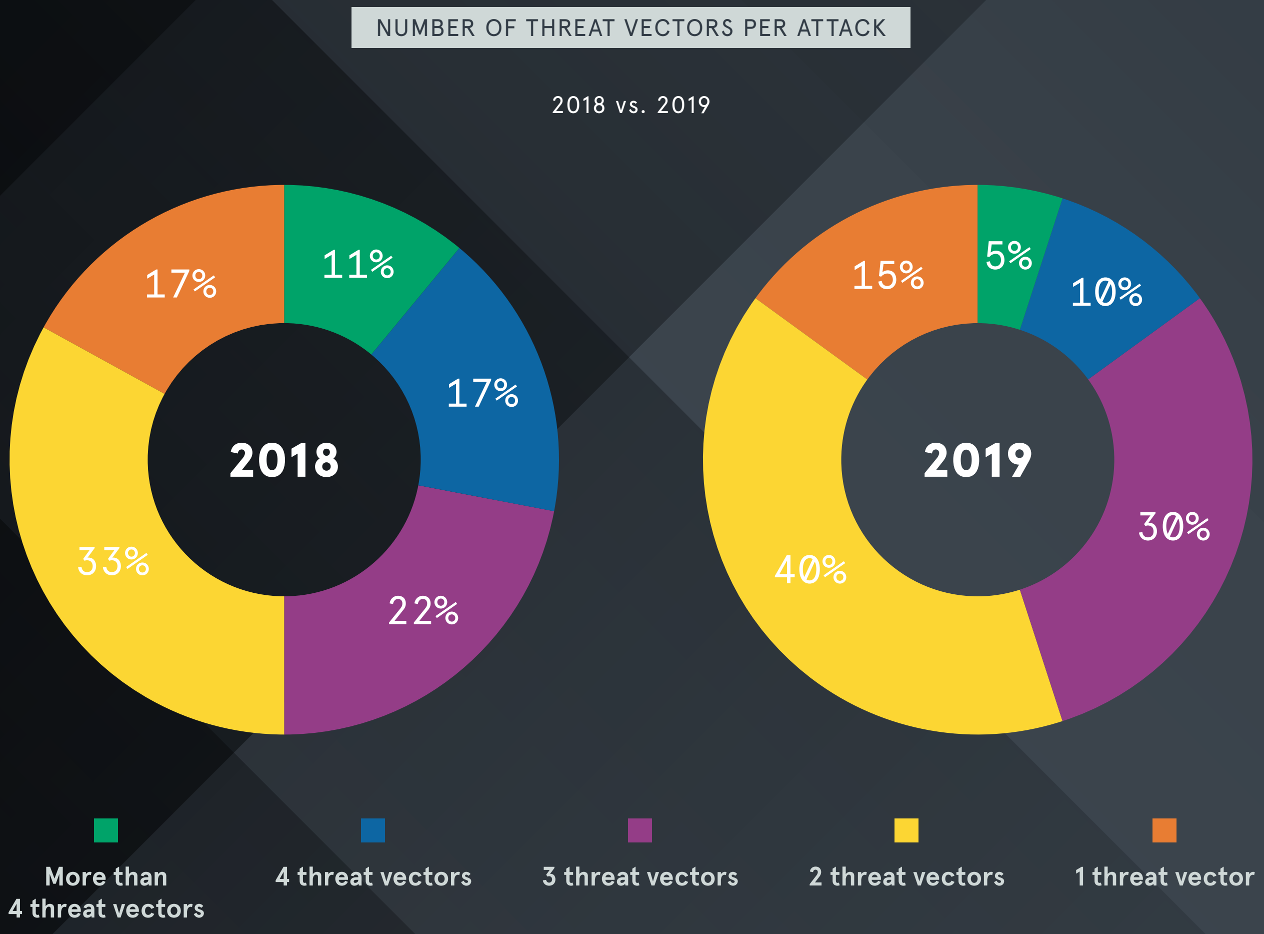


Figure 6: Threat vectors per attack in 2018 vs. 2019

Nobody Knows the Trouble We've Seen...

While Neustar did not observe any terabit-plus DDoS attacks in 2019, we have seen a steady growth of new exploits. Some used vulnerabilities that have existed for some time but had never been exploited, such as those used in 2018 attacks featuring memcached servers. The breakup of some of the larger booter or stressor services put a dent in the DDoS-as-a-service industry in late 2018, and prosecution of both the perpetrators and customers of those services in some jurisdictions has provided something of a cautionary tale.

At the same time, however, the offering of DDoS-for-hire and rent-a-botnet services seems to have rebounded, and a host of "smaller" DDoS episodes may be one result. Web attacks have increased, and bot populations are exploding; Mirai may have gone away, but its descendants live on. On the positive side, these issues have spawned a new awareness of today's security challenges, driving vendors to innovate. One such innovation is the ability to infuse near-real-time threat data across the security stack to enable some degree of proactive protection. We have considered this and other developments as we reviewed the happenings of 2019.

DDoS — An Attack Built to Last

There was coverage of attacks last year that caused some reporters to say, "DDoS? Those attacks are still around?" We saw that reaction in May 2019 during coverage of a report from the US Department of Energy (DoE), regarding DDoS-based disruptions to several power grids. Some reporters mentioned that DDoS attacks are not sophisticated; in fact, some coverage went so far as to say that DDoS attacks are a thing of the past. Unfortunately, security experts recognize the truth. DDoS attacks will always be around.

One of the notable issues around DDoS attacks is the still common assumption that they always feature massive amounts of traffic, such as those we saw in 2016 and again in 2018. Those threats still exist—Neustar mitigated a 587 Gbps attack this year—but such large, headline-making incursions are far from the majority of DDoS attacks. There is speculation that these smaller attacks may be the result of less skilled cybercriminals that are utilizing DDoS-for-hire services, as compared to the largest attacks, which are generally spearheaded by more sophisticated bad actors. These DDoS attacks may also be used as an overlay or smokescreen for other types of cybercrime.

Another type of DDoS attack came to the forefront this year—network protocol attacks, which are rated by packets per second. This measurement is not new, and it also challenges the conventional definition of DDoS as an attack that saturates bandwidth. While volumetric DDoS attacks seek to exhaust bandwidth, protocol or state exhaustion attacks target network infrastructure directly. Both can take a network down.

DDoS attacks have been around for decades, but they continue to evolve. In 2019, we saw a number of amplification attacks that made use of intermediate services to generate large amounts of traffic from small requests. This type of amplification attack was used in the 1.3 Tbps attacks of 2018, which used memcached servers to create an astonishing amount of traffic. Perhaps inspired by the success of this attack, cybercriminals have been busy this year looking for intermediate services that offer an amplification factor. The services under criminal consideration are generally not new—memcached, for example, was introduced in 2003—but are often unprotected and accessible from the Internet. They also typically make use of the User Datagram Protocol (UDP), which is popular with criminals due to the ease with which it can be spoofed. In the case of memcached, this fact, combined with the large amplification factor, made it possible to conduct DDoS attacks without the need for a botnet to generate sufficient traffic to impact the target. Such amplification vectors continue to evolve; in 2019, we saw a few new DDoS vectors, including Apple Remote Management Services (ARMS), Web Services Dynamic Discovery (WS-D), Ubiquiti Discovery Protocol, and the Constrained Application Protocol (CoAP).

Security experts recognize the continuing danger of DDoS attacks, as shown by their responses to the most recent NISC survey.

HOW THREAT OF ATTACK BY VARIOUS VECTORS HAS CHANGED

During November-December 2019, social engineering - email was most likely to be perceived as an increasing threat to organizations, followed by DDoS and ransomware.

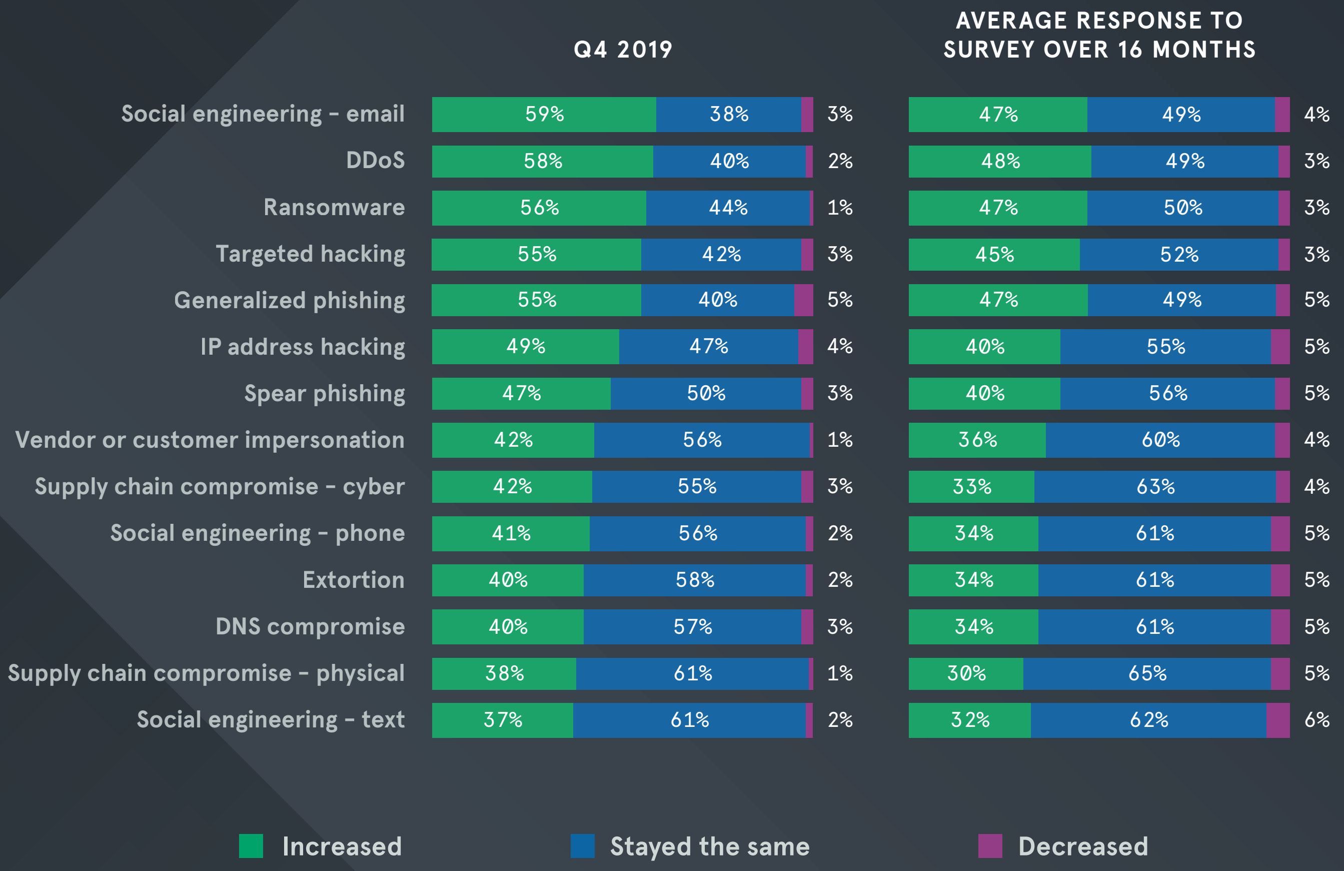


Figure 7: Change in attack threat by various actors, NISC Survey, Q4 2019

While DDoS attacks can be and are used on their own, the ease with which the components of these incursions can be procured makes it even easier to use them as a smokescreen for other activities, such as data theft or network infiltration. The attacker keeps its target busy fighting off the DDoS attack, then sneaks in a piece of malware or exfiltrates important data. It's difficult to tie these events together concretely, but one publication put it best when it said, "Under DDoS attack? Look for something worse."[4] It's interesting to consider that while DDoS attacks are perceived to be at the top of the list of increasing threats, according to the NISC survey, many of the other incursions seen further down may be enabled while using DDoS as a smokescreen.

Botnets

Botnets continued to proliferate and expand throughout 2019, and there is no slowdown in sight. The ability to rent a botnet and purchase DDoS-for-hire services via booters or stressors has created the perfect environment for anyone to craft an attack. Mirai variants remain the "big dog" of botnets and was responsible for massive attacks in 2016.As of July 2019, IBM X-Force says there are now at least 63 Mirai variants[5] and sees them twice as much as the next Mirai-like botnet, Gafgyt.

Not Just for DDoS Anymore

Botnets are often thought of as a key component of DDoS attacks, but the truth is that they can also play a significant role in a variety of web attack types, including web injection, and URL or DNS spoofing. These attacks typically target the users of a website, rather than attempting to deny access to a target company's site or infrastructure. These botnets are now capable of doing everything from collecting and scraping intelligence to doing credential stuffing attacks or initiating HTTP interactions that result in DDoS attacks.[6]

Of course, a botnet is only as good as its command infrastructure. Botnet C&Cs, which started moving to the "dark web" via anonymization services like Tor in 2016, continued that trend in 2019. If you don't choose to block all traffic coming from anonymous sources or aren't sure that you would know exactly what to block, a threat feed can be extremely helpful.

Web Attacks on the Rise

Web attacks were also in the forefront in 2019. Web attacks are often harder to track than straight-up DDoS incursions because some variation in the performance of websites is to be expected. It can also be difficult to determine what "slow" means if you haven't got a baseline for normal performance.

It's important to get a feeling for how things should work, however, because you don't need to be taken offline to be taken out of business.

- 45.5% of consumers are less likely to make a purchase when they experience a slow-loading website
- 36.8% are less likely to return to a retailer if they experience slow-loading pages
- 12% will tell a friend when they experience a slow-loading site[7]

Most companies are aware of the danger to their web resources and have attempted to protect them with devices including web application firewalls (WAFs). In fact, a recent NISC survey shows that close to 100 percent of those surveyed consider a WAF to be an essential component of their security infrastructure.

IMPACT OF CYBERATTACKS

Do you agree that a Web Application Firewall (WAF) is an essential component of your security infrastructure?

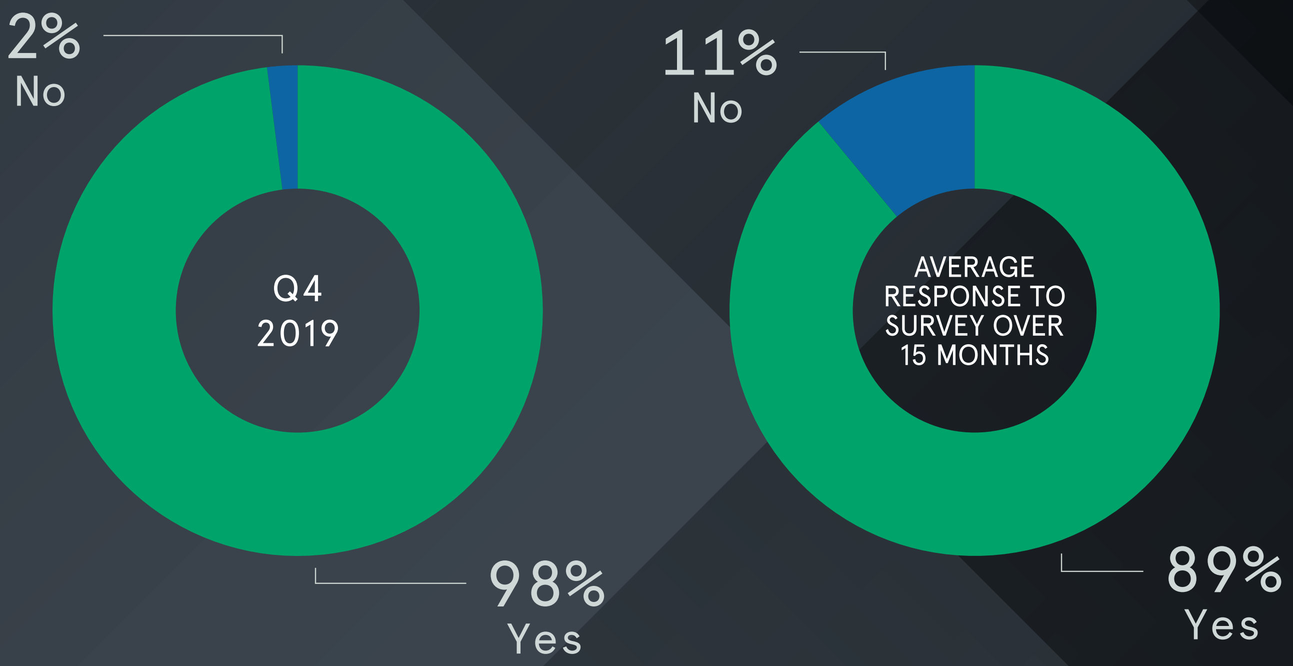


Figure 8: Is a WAF an essential component of your security infrastructure? NISC Survey, Q4 2019

Are All WAFs Created Equal?

Most companies have responded to the requirement for a WAF by installing some kind of security device in front of their applications. Such devices or services can be very specialized and are usually tuned and updated by corporate security experts to keep up with the applications that they protect. As with any infrastructure, however, issues arise as the solution is asked to scale, and specialized WAFs are no exception. Most on-prem WAFs were configured to protect against attacks that are specific to corporate applications but they may also be faced with a firehose of other traffic, which could include application DDoS attacks. Keeping up with the growth of web traffic—both good and bad—is a daunting prospect for any device.

Today, Your Apps Could Be Anywhere; Your Defenses Must Be Too

Another factor in considering application security is the overall move to the cloud. An on-prem device may have made sense when your applications lived in the datacenter, but housing assets in the cloud is becoming a necessity as companies seek economies of scale and superior customer experience. In fact, 84 percent of the respondents to a recent cloud survey report use more than four cloud providers, with a mix of public and private clouds.[8] This means that enterprises must try to find consistent protection for their applications across all platforms. Some have relied on the WAF capabilities offered by each cloud provider, but such protections can be expensive and are not the same across different clouds. And, as security experts are all too painfully aware, security that isn't consistent isn't security.

The logical place to look for such protection is in the cloud, where a vendor-neutral offering could be coupled with DDoS protection and bot mitigation. While such an offering will not erase all application attacks, it can serve to siphon off a large portion of threats, leaving those that are best handled by enterprise application experts. Gartner predicts that by 2024, most organizations implementing multicloud strategies for web applications in production will use only cloud web application and Application Programming Interface (API) protection WAAP services.[9]

Particularly in the case of web services, having always-on protection is vital. One example of the kind of ongoing application threat is also among the oldest—SQL injection (SQLi) attacks. SQLi attacks are several decades old and are well understood; in fact, Malwarebytes Labs ranked SQLi as number three in their "The top 5 dumbest cyber threats that work anyway" list, citing the fact that SQLi is a known, predictable attack with easily implemented countermeasures.[10] Yet SQLi attacks remain one of the most popular attacks, and it currently holds the number-one spot on the Open Web Application Security Project (OWASP) Top Ten list of web application vulnerabilities. This threat is particularly serious because the injection of code into the request can result in the target database forwarding a wealth of unauthorized information to the hacker.

In addition to providing consistent protection from web attacks, a cloud WAF can be coupled with DDoS mitigation. Such an offering should be always-on, providing continuous protection. Additionally, it is important that its defenses are always updated. This is another excellent spot for current updates provided by a threat feed. Such a service can deliver information on bad IPs and botnets to help keep your applications safe and lighten the load on specialized devices.

SUMMARY

Knowledge Is Power

One could sum up 2019 in a single word – More. Neustar mitigated over three times as many DDoS attacks as it did in 2018. The vast majority of those attacks featured more than one threat vector. The average size and intensity remained relatively consistent, though the peaks in volume (Gbps) and intensity (Mpps) were more pronounced. Overall, the biggest difference was the number of attacks.

DDoS attacks were once defined by enormous amounts of traffic that took a site offline by saturating the target's bandwidth. They were uncommon, and they made headlines. As bandwidth has dropped in price and business has moved online, the combination of DDoS-for-hire services and botnet rental have opened up the realm of DDoS threats to anyone with an Internet browser. Ironically, the result appears to be that some commentators have concluded that DDoS attacks aren't happening, when in fact they occur more frequently than ever. The difference is that the perpetrators may be less interested in raising their profile, along with the attendant risk of being caught, and more interested in other goals, such as slowing down a site to gain competitive advantage or distracting the security team in one area while launching an exploit in another.

As the threat landscape becomes more subtle and dangerous, it is vital to know as much about your enemy as possible, and to be able to use that knowledge quickly. That means that the source of any threat feed that you choose to use must be credible and reliable, with proven expertise in delivering large data sets. You should also be free to integrate that threat data throughout your network in any way that you choose. Being able to identify potential threats before they do any damage is a powerful tool in keeping your network – and your business – safe.

GLOSSARY

ACK – Acknowledgement

AI – Artificial Intelligence

API – Application Programming Interface

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

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

REFERENCES

1 https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

2 Spamhouse Botnet Threat Report 2019

3 Spamhouse Botnet Threat Report 2019

4 https://www.networkworld.com/article/2984648/under-ddos-attack-look-for-something-worse.html

5 https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/

6 8 DDoS Attack Trends To Watch For In 2020

7 https://unbounce.com/page-speed-report/?utm_medium=referral&utm_source=press-release&utm_campaign=page-speed-report&utm_content=lp-page-speed-report

8 RightScale 2019 State of the Cloud Report from Flexera

9 Gartner Magic Quadrant for Web Application Firewalls, September 2019

10 https://www.malwarebytes.com/sql-injection/

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 offer industry-leading solution marketing, risk, communication, security, and registry 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