Q3, 2019 CYBER THREATS & TRENDS REPORT
# TABLE OF CONTENTS

**Does your WAF need a WAF?**
- Generic or Bespoke Attacks
- Real Protection Requires a Layered Defense
- What to Look for in Cloud-Based Application Security
  - Avoid Complexity
  - Eliminate Provider-Based Issues
  - Ensure No Conflict of Interest
  - Insist That Your Vendor Implements Security Best Practices Throughout Their Own Network
  - Look for Quick Access to Expert Support

**Q3, 2019 Threats & Trends**
- Attack Summary
- Attack Volume
- Attack Intensity
- Attack Vectors

**DDoS Attacks – One Consistent Fact in a World Full of Inconsistency**
- This Is Not the Battle That You Signed up For
  - The Wikipedia DDoS
- The Latest Threat Vectors
  - DDoS Reflection/Amplification Attacks
  - Apple Remote Management (ARM) Services
  - Web Services Dynamic Discovery
  - Ubiquiti Discovery Protocol
  - Constrained Application Protocol
  - HTML5 Hyperlink Auditing Ping Redirection
  - Those Bots Just Keep on Coming

**Summary – Get Ready for Q4**

**Glossary & References**

**About Neustar**
DOES YOUR WAF NEED A WAF?

If you’ve been following this report, you’ll know that we have seen a steady climb in the number of lower-volume attacks, particularly those at the application layer. This trend is mirrored across the industry, and it shows no signs of slowing down. Application-layer distributed denial of service (DDoS) attacks use the same basic methodology as other DDoS incursions—degrading or destroying performance of an asset by inundating it with traffic—but do so with a twist. Volumetric or state exhaustion DDoS attacks either do not require protocol handshakes or use that process itself to initiate the attack. Sufficient volumes of traffic to achieve the attack goal can be generated via spoofing. Application-layer DDoS attacks, on the other hand, function in accordance with the application that is being used and cannot typically be spoofed. The lack of sufficient client numbers to overwhelm an application might have been a problem to bad actors in the past, but with the explosive growth of the Internet of Things (IoT) and the botnets that go with them, this is no longer a barrier to entry.
Application attacks often require more analysis than simple “brute force” volumetric attacks, and they are unlikely to be randomly targeted. Some of these DDoS attacks can be custom-tuned to a degree that points to knowledgeable and often extensive reconnaissance. Attacks that target specific software or hardware vulnerabilities are among these crafted threats. Other application-layer attacks, such as generic HTTP/S GET or POST floods, feature a less targeted approach but can be precisely aimed at your assets.

We are accustomed to seeing application security applied via on-prem devices, including Web Application Firewalls (WAFs) and other forms of application security. Such defenses are typically custom-tuned by in-house security staff who know your applications best. These resource-intensive protections are frequently refreshed as applications are updated and business requirements change, and nearly always include the ability to decrypt and inspect encrypted traffic. Unfortunately, as the traffic load grows, you are faced with having to build out your on-prem deployment just to keep up. Decrypting and examining traffic alone can be daunting. And if you move your applications to the cloud, all bets may be off.
Layering your security has always been an industry best practice. In this case, on-prem security devices are often key to providing fine-grained, application-aware defense in front of the apps themselves. One good way to keep your on-prem defenses working at their best is to reduce the amount of traffic that they are required to inspect, and that’s a great place to bring always-on cloud-based application security into play. These defenses in the cloud can dramatically lower the bandwidth that your expensive on-prem devices are hit with, by weeding out generic application-layer traffic with obvious problems, including select traffic that is not standards-compliant. Cloud-based application security can also be used to provide a consistent layer of protection, regardless of where your applications are housed, so apps remain protected, even as you move them to the cloud.
WHAT TO LOOK FOR IN CLOUD-BASED APPLICATION SECURITY

Avoid Complexity
Protecting against volumetric attacks is typically a well-understood process as these attacks are fairly easy to see. That is not always the case when you consider state/protocol attacks, and it certainly is not what you will face with application-layer attacks. You need to ensure that your own team understands the application security that can be provided in the cloud, how best to tune it, and what you could expect it to do in terms of offloading functions from your on-prem devices. It is often useful to provide filtering in the cloud from a vendor other than the one you have on-prem, but this opens up the need for your internal team to learn another user interface (UI). A reliable, managed service can help to ensure that you are reaching your goals and can assist you in providing a consistent level of security no matter where your applications are housed.

Minimize Provider-Based Issues
If you choose to offload your on-prem application security with cloud-based defenses, you should ensure that this change does not lock you into the provider’s network or service. By the same token, you need to ensure that the provider is sufficiently distributed and features enough bandwidth to minimize the effects of mitigation.

Ensure No Conflict of Interest
In the midst of trying to secure your applications, it is important to take a step back and look for any potential conflicts of interest. For example, if you are under attack, is mitigation the first action that the provider would take? To what degree might they be concerned with how an attack on your site impacts their overall network?
Insist That Your Vendor Implements Security Best Practices Throughout Their Own Network

While this point seems self-explanatory, it is important to consider the security posture of the company that is providing your protection. It is worthwhile to ensure that the mitigation vendor is regularly revisiting their own security posture, with activities like third-party penetration tests. Ensure that your passwords and keys are stored in transit and at rest in an appropriate fashion.

Look for Quick Access to Expert Support

Things move fast at the application layer, and when there is an issue, you need to be able to address it quickly, because impact to your apps can directly affect your bottom line. Attacks happen on a 24/7/365 timeline, and sometimes there is no time to deal with a lower tier of support. You should have immediate access to experts who are able to visualize and help you rectify issues as they happen.

DDoS attacks will not stop. With the advent of easily accessed IoT botnets, it is just a matter of time before you feel the impact. While you cannot predict what an attacker will do, you can prepare by ensuring that your assets are defended with a layered security strategy.

- Rodney Joffe

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.
Q3, 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 Q3, 2019. This report offers a unique view into the attack trends that are unfolding online, including attack statistics and behavioral trends for Q3, 2019.

ATTACK SUMMARY

Comparing Q3, 2019 vs. Q3, 2018, the number of attacks on directly provisioned customers has increased by 241 percent. The largest attack size observed in Q3, 2019 was 273 Gbps in volume, slightly smaller than the largest attack size observed in Q3, 2018 at 285 Gbps in volume. The longest duration for a single attack was almost a day and a half at 33 hours.

241% INCREASE IN THE NUMBER OF ATTACKS Q3, YOY

273 Gbps LARGEST ATTACK SIZE Q3, 2019

33 Hours LONGEST ATTACK DURATION

4% DECREASE IN THE LARGEST ATTACK SIZE Q3, YOY
Comparing the number of attacks by size category in Q3, 2019 with the number of attacks in the same time period of 2018, Neustar observed that the greatest change overall was in the class that was 5 Gbps and below. Considered in perspective, however, the greatest difference between numbers of attacks within specific size categories was in the 50 to 100 Gbps category.

Figure 1: Percentage change in number of attacks by category, Q3, 2019 vs. Q3, 2018.
ATTACK VOLUME

In Q3, 2019, over 80 percent of all attacks mitigated by Neustar were 5 Gbps or less. While there is an incidence of attacks between 5 and 100+ Gbps in the third quarter of both 2019 and 2018, the majority of attacks in both periods were 5 Gbps and below. Comparing Q3, 2019 to Q3, 2018, the percentage of attacks in the 5 to 25 Gbps and 25 to 50 Gbps decreased, while there was an increase in attacks between 50 and 100 Gbps. Attacks over 100 Gbps are nearly equal when considered as a percentage of overall attacks in both cases.

Figure 2: Percentage of attacks within specified size range Q3, 2019 vs Q3, 2018.
Q3, 2019 vs Q3, 2018

7.6 Gbps AVERAGE ATTACK SIZE

10.5 Gbps AVERAGE ATTACK SIZE

28% DECREASE IN AVERAGE ATTACK SIZE
ATTACK INTENSITY

Comparing the intensity of attacks in Q3, 2019 vs. the intensity of attacks in Q3, 2018, Neustar observed Q3, 2019’s most intense attack was 24 percent higher than the most intense attack of Q3, 2018, while the overall average intensity of attacks for these periods was down.

Q3, 2019

343 Mpps
MOST INTENSE ATTACK

7.6 Mpps
AVERAGE ATTACK INTENSITY

Q3, 2018

285 Mpps
MOST INTENSE ATTACK

10.5 Mpps
AVERAGE ATTACK INTENSITY
ATTACK VECTORS

In Q3, 2019, over 86 percent of all attacks mitigated by Neustar used two or more vectors. In Q3, 2019, Neustar also observed a significant number of attacks that featured more than four threat vectors.

Figure 3: Threat vectors per attack, Q3, 2019.
The third quarter of 2019 continued to show an impressive number of DDoS attacks against all types of companies. The overall number of attacks dipped slightly in Q3 when compared to Q2 of this year. It is important to note, however, that this small decline is in keeping with the results seen in Q3 of previous years. Think of it as the calm before the storm, because if these trends do mirror last year’s, we could be in for a deluge in Q4. The Q3 NISC survey indicated that the percentage of respondents that have experienced DDoS attacks is now higher than it has been in the 14 months previous.
Despite the relative lull, attacks are obviously still happening. One category that has been hit particularly hard is the area of online gaming.
THIS IS NOT THE BATTLE THAT YOU SIGNED UP FOR

DDoS attacks on online gaming platforms are not new; they have always been a popular target due to the type of users these systems attract. Online gaming sites are much more sensitive to latency than other online platforms, so an incursion can be considered successful even if the site itself is not taken down. In fact, many of these attacks are initiated by other players in an attempt to frustrate legitimate players and force them to log off. Quitting a match has historically included both a penalty to the player that leaves and points for the one that stays, so it is compelling way for unscrupulous players to cheat the game.

The ease with which DDoS services can be hired—even with the arrests we’ve seen in 2019—may entice players who cannot win by “fighting fair.”

Despite the frequency with which they are attacked, DDoS assaults on gaming sites are not always made public, due in part to the gaming companies’ reluctance to warn users away from their platform. Online gaming players can be notoriously fickle, and any hints that a platform may deliver a suboptimal experience can lose a player forever. Several DDoS attacks this quarter, however, came to everyone’s attention.
One of the most impactful attacks was executed on Blizzard, the segment of Activision Blizzard that runs the popular World of Warcraft Classic server-based option for the massively multiplayer online role-playing game (MMORPG). World of Warcraft (WoW) Classic was reintroduced online late this summer only to be hit with a DDoS attack that took it offline for most of a weekend of play in early September.

In an interesting twist, the alleged attackers, coming from an account that goes by UkDrillas, made their actions known before the incursion, as well as claiming responsibility for an attack on Wikipedia during the same timeframe.

There are signs that both attacks were originated in the Europe, Middle East, and Africa (EMEA) region.
THE WIKIPEDIA DDoS

Wikipedia, one of the world’s most popular sites, was intermittently taken offline over the weekend of September 7 and 8—the same weekend that WoW Classic was attacked. The non-profit Wikimedia Foundation, which hosts Wikipedia and other free knowledge sites, was quick to respond, saying "We condemn these sorts of attacks. They’re not just about taking Wikipedia offline. Takedown attacks threaten everyone’s fundamental rights to freely access and share information." These attacks prompted a response from the UK’s National Cyber Security Center, explaining that "When a website suffers a DoS attack, it will appear to users that the site has simply stopped displaying content. However, for businesses it could mean that the online systems they depend upon have ceased to respond." Some estimate that the attack could represent one of the most disruptive DDoS attacks in recent memory.1

Montreal game maker Ubisoft also faced DDoS attacks in this quarter on its platform Rainbow Six Siege, although such attacks have been seen on Ubisoft platforms in the past. Ubisoft announced in response that they will lower the number of matches per server, and also disable penalties against a player who quits a match when the site is attacked. The company has published the steps they are taking to mitigate DDoS incursions, going so far as to promise that they will take legal action against the sites that host DDoS attacks, not only the individuals themselves.

Figure 6: Ubisoft announcement.
THE LATEST THREAT VECTORS

Even as new application-layer threats emerge, the danger of volumetric and protocol/state exhaustion incursions continue unabated. In fact, a few new vectors have recently popped up in that category.

DDoS Reflection/Amplification Attacks

We have observed several new threat vectors coming online in 2019, some of which provide an opportunity for reflection or amplification attack. In a reflection attack, the hacker spoofs the originating IP address, so it appears that the request came from the target site. When the attacker makes a request of a service, such as to DNS servers, the server response goes to the spoofed IP address of the target site, which the service believes to be the originator of the request. Amplification attacks are reflection attacks that return a large amount of data in response to a very small request. This was what we observed in 2017 with the memcached attacks, where hackers saw amplification factors of between 10,000 and 50,000 times. As most security professionals know, the fact that memcached servers could be exploited in this way is not due to what the service does; rather, it is a reflection (no pun intended) of where these devices were located. Memcached servers were never intended to be open to the Internet. Unfortunately, many were, and some still are. And they are not the only example of such services out there.

As we consider the latest attack vectors, it is important to note that reflection attacks themselves are not new. These threats use a well-understood methodology. The difference is all in the intermediate service. Here is a look at what we’ve seen recently.

Apple Remote Management (ARM) Services

Apple has historically gone to great lengths to ensure that its devices can be easily managed from other Apple devices. One such move involves remote management, using Apple Remote Desktop, which the company describes as a feature that “allows
you to manage computers, interact with users, distribute software, create software and hardware reports, and administer several computers at once, all from a single computer.” The need for such protocol is easy to understand, particularly when management is required in venues such as schools, where more sophisticated device management schemes may not be practical. As one might expect given their design, ARM services should not be open to the Internet, but as attacks start to show up, we are seeing that this is not the case. It is actually relatively trivial to find directions on how to get access to an Apple device behind router, firewall, or NAT configurations, and not surprisingly, there are reported cases of DDoS booter services already being written around ARM.

**Web Services Dynamic Discovery**

Web Services Dynamic Discovery, also known as WS-Discovery, WS-DD or simply WSD, is a multicast protocol used by IoT devices to discover others on local networks using a particular protocol or interface. Security researchers at ZDNet, who reported finding the protocol being used to launch DDoS attacks in May of this year, decided not to publish the finding because while the discovery was considered ripe for abuse it had not been fully exploited. The situation has since changed.

WSD has not been a commonly used protocol but was adopted by the Open Network Video Interface Forum (ONVIF) in 2010 as part of a drive to standardize how physical IP-based security devices, such as video or surveillance cameras, can communicate with one another. ONVIF members include Axis Communications, Bosch, Sony and others. ONVIF products that comply with the use of WS-D as part of plug-and-play interoperability fall into the category of IoT devices which can be exploited.

There are two distinct issues with WS-D. First, it uses User Datagram Protocol (UDP), which means that the requestor’s IP address can be spoofed. This makes the protocol a candidate for reflection attacks, in which responses supposedly made to a legitimate request will actually be forwarded to the target. The second issue with WS-D is that it offers an amplification factor—that is, the responses to a request can be larger than the request itself. Although responses in WS-D—based DDoS attacks can theoretically be between 300 and 500 times the size of a request, smaller attacks have been the norm thus far. Unfortunately, the protocol is reportedly in use by over 630,000 devices, and while the threat could be mitigated by simply blocking requests from the Internet to devices using port 3702, this fix is unlikely to be enacted quickly.
These attacks join an assortment of protocols that we’ve seen abused or discussed earlier in the year, which include:

**Ubiquiti Discovery Protocol**

This reflection attack, which also offers some amplification, has been seen for some time. In this attack, bad actors exploit a discovery service in Ubiquiti Networks products, which include Wi-Fi devices, switches, and routers. The service, which runs on port 10,001, is designed to enable Internet Service Providers (ISPs) and others to find Ubiquiti devices on the Internet, as well as inside networks. Like WS-D, Ubiquiti’s discovery service runs on UDP, and can be spoofed. Ubiquiti is said to be issuing a patch for the issue.

**Constrained Application Protocol**

The Constrained Application Protocol, or CoAP, surfaced late last year as a service that could be used as part of a DDoS threat. Although CoAP was formally approved in 2014, it has not seen wide adoption. The protocol was designed to run on platforms that include smartphones, where compute and memory resources are relatively constrained. The protocol functions similarly to HTTP, but instead of running over Transmission Control Protocol (TCP), whose verification processes deliver reliability but consume resources, the “lightweight” CoAP runs over UDP. CoAP can be used to handle HTTP–like functions such as GET and POST commands but consumes fewer resources while doing so, making the protocol a natural fit in the world of smart devices and some IoT products. Once again, however, this comes at a cost, as the requesting packet can feature a spoofed IP address. Amplification is also possible using this vector.

**HTML5 Hyperlink Auditing**

**Ping Redirection**

HTML5 hyperlink auditing is an HTML standard and is typically used by sites to track when users click on a link. The intended functionality includes an intermediate site, usually with a POST command embedded into a site link. The user’s browser will first open the intermediate Uniform Resource Locator (URL), which pings back to a site where clicks are recorded, then opens the intended destination. The new threat uses the same methodology. Attackers use a variety of methods to get users to a site that features an enticing advert with a link. When the user clicks on the link, the intermediate ping function sends traffic to the target site; it can also be written to continue generating these pings as long as the user remains on the page. This functionality has been enabled by default by some browsers, but users who feel it is a violation of privacy have had the ability to disable it in the past. Unfortunately, the ability to disable this functionality is now being eliminated on all but a few browsers.
Those Bots Just Keep on Coming

The nature of botnets makes them among the most popular platforms from which to launch a DDoS attack. When comprised of IoT devices, as most are, the botnet can be highly distributed. While a botnet may have been complex to create, renting one is very easy to do. But it’s not just their ability to launch DDoS attacks that make botnets the threat that they have become.

Consider Mirai, arguably the root of botnet evil; although it was not the first of its kind, Mirai’s success certainly contributed to making “botnet” a household word. Mirai’s source code itself delivers DDoS capabilities by creating an army of remotely controlled devices that each have a legitimate IP address, thus getting past some fundamental protections. The story of how Mirai was originally developed as part of an extortion plan to hold Minecraft servers for ransom makes for fascinating reading and is well covered by Brian Krebs in his popular Krebs on Security blog.7

While the original authors of Mirai have been identified, botnets themselves continue to grow and develop. One of the latest is the Gucci botnet, which began to gain notoriety in October. Gucci targets IoT devices and is said to be able to launch multiple types of DDoS attacks, including HTTP null scans, UDP floods, SYN floods, ACK floods, UDP floods with less protocol options, GRE IP floods, and Value Source Engine specific floods. Researchers traced the bots back to a server in the Netherlands and got into the Command and Control (C&C) panel after getting through the site’s request for a username and password. When the botnet operators discovered the breach, they quickly disabled and moved the service. This botnet appears to be in its youth and is likely targeted for sites in Europe.8
GET READY FOR Q4

With Q4 upon us, it is important to look at the trends we’ve seen over 2019 and 2018. In Neustar’s experience, Q4 has traditionally been the time for the largest number of big DDoS attacks. If you don’t already have a DDoS mitigation service, you should think about employing one now. Consider what it would cost your business in revenue and lost consumer confidence should an attack be successful.

It is also worthwhile to look at what an attacker may consider a successful DDoS attack. A successful DDoS incursion may not mean taking your site down with a volumetric attack, although you should be prepared in case that happens. Q4 and the beginning of Q1 in any year are when the attacks have historically featured the largest volume of traffic.

But preparing for a volumetric DDoS attack no longer covers the most likely scenarios, which are often low volume and aimed at your applications. Users can still get to the site—sometimes—but as seen in the cases of gaming companies, a poorly performing site can be enough to lose customers. While the ramifications of degraded performance are obvious in a real-time game, you should ponder the effect that a poor user experience could have on your business. You may not need protection for all your applications all of the time, but there are always a few whose increase in latency would directly impact your bottom line. In fact, they may already be compromised. Just because you’re running online does not mean that you are running well online, and that can cost you. Now is the time to put your users’ experience first and get ready for Q4.
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
Mbps – Megabits per second
GET – An HTTP method which requests data from a specified resource
GRE – Generic Routing Encapsulation
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
Mtps – 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
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://wikimediafoundation.org/news/2019/09/07/malicious-attack-on-wikipedia-what-we-know-and-what-were-doing/
2 https://www.ncsc.gov.uk/news/wikipedia
4 https://help.apple.com/remotedesktop/mac/3.9/#/ard6250988a1
5 https://how2s.org/index.php/Howto_get_Apple_Remote_Desktop_to_work_behind_a_router
7 https://krebsonsecurity.com/tag/protraf-solutions/
8 https://www.securityweek.com/new-gucci-iot-botnet-targets-europe
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