NEXUSGUARD®

Threat Report

Distributed Denial of Service (DDoS)

Q3 2019

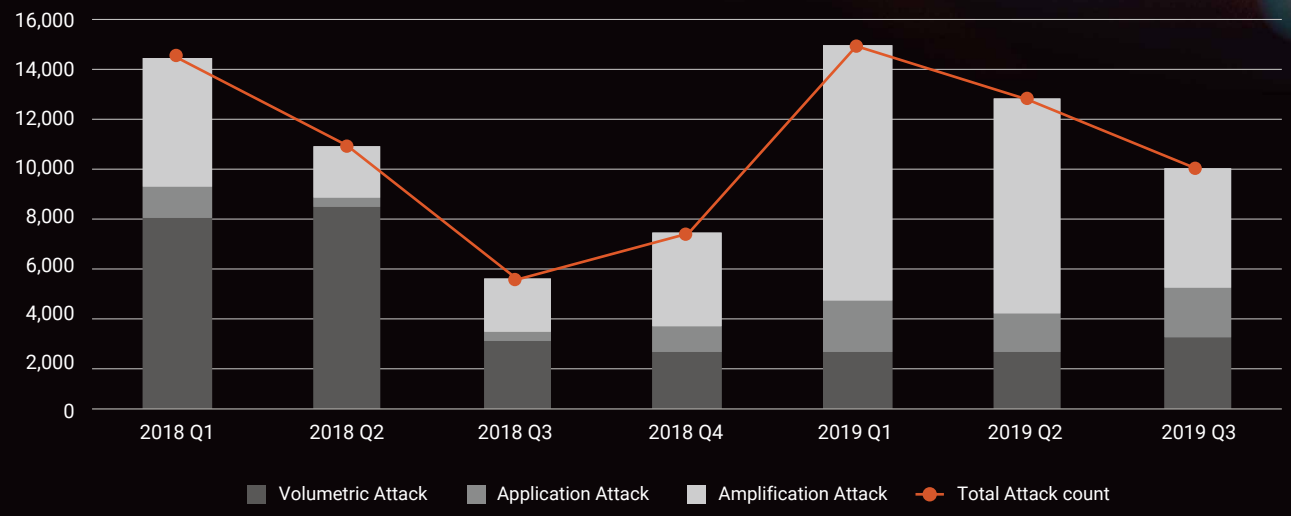
Contents

NEXUSGUARD®

Q3 2019 Threat Report

Key Observations

Attack Trends Q1 2018 – Q3 2019



Total Attacks

vs. Q3 2018	85.66% ▲
vs. Q2 2019	22.60% ▼

Attack Sizes

	Maximum	Average
vs. Q3 2018	137.29% ▲	28.94% ▲
vs. Q2 2019	137.49% ▲	29.34% ▲

DDoS Attack Type

	DNS Amplification	HTTP	TCP SYN Flood	Application	Amplification
vs. Q3 2018	4,787.91% ▲	1017.74% ▲	177.37% ▲	487.61% ▲	125.71% ▲
vs. Q2 2019	46.93% ▼	52.64% ▲	13.60% ▲	27.20% ▲	44.70% ▼

Quarterly Focus - Single Targets, Multiple Innocent Victims

While the ongoing implementation of DNSSEC (Domain Name System Security Extensions) continued to drive the growth of DNS Amplification attacks in the quarter, the sharp rise in TCP SYN Flood attacks is also worthy of considerable attention. TCP SYN Flood isn't new, but our findings suggest that the techniques behind the latest round of attacks have become ever-more sophisticated.

How SYN Flood Attacks Work

To start, let's review how TCP SYN Flood attacks work: In order to establish a TCP connection, the three-way TCP handshake must be completed. It begins with the client requesting a connection by sending a SYN message to the server. Then, the server acknowledges by replying with a SYN-ACK message to the client. Finally, the client responds with an ACK message to establish the connection.

During an attack, an attacker sends repeated SYN packets to every port on a targeted server, often using a spoofed IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each request with a SYN-ACK packet from each open port.

The malicious client doesn't send the expected ACK, or, if the IP address is spoofed, never receives the SYN-ACK. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet. While waiting, the server cannot close down the connection by sending an RST packet. Therefore, the connection remains open. Before the connection times out, another SYN packet comes in. Over time, a large number of half-open connections accumulate until they overflow, denying legitimate clients the ability to establish connections.

Types of SYN flood attacks

Type 1: Multiple, randomized spoofed-source IPs abusing one destination IP:

In Type 1 (56.36% of SYN Flood attacks in Q3), an attacker mobilizes a huge number of random, spoofed IP addresses to send an enormous volume of SYN requests to a single IP, causing the victim server to respond with SYN-ACK packets to voluminous malicious requests. Type 1 attacks are easy to mitigate, since most source IPs are only used a few times, but they all target the same destination. Because of this pattern, a TCP authentication filter can easily flag and drop malicious SYN packets from spoofed source IPs. Also, ISPs deploying preemptive measures are likely to drop malicious source IPs that do not belong to them.

Type 2: Multiple, fixed real-source IPs abusing one destination IP:

In Type 2 (33.24% of SYN Flood attacks in Q3), an attacker leverages a large, fixed pool of real IP addresses (e.g., servers, routers, IoT devices) to generate malicious SYN packets to hit one destination IP per attack. Most Type 2 attacks were smaller than 1Mbps, but in some cases attack sizes were 100Mbps. One extreme case where traffic was diverted from a cloud service provider reached 424.2Mbps.

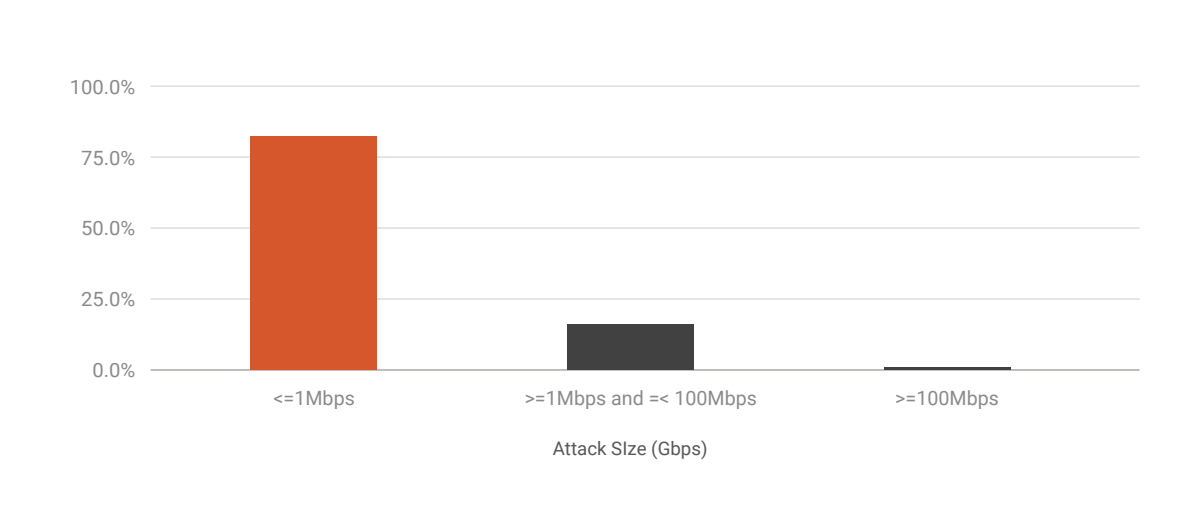


Figure 1. Size Distribution of Single-source IP SYN Flood Attacks, Q3 2019

When targeting an Internet host, an attacker typically prefers to maintain anonymity by spoofing the source IP address. But using real IP addresses of hijacked machines or devices offers certain advantages. Here are the reasons Nexusguard believes that real IP addresses were used in some of the SYN Flood attacks we observed:

To bypass ISP filters

Packet filtering is ineffective if an attack comes from real IP addresses, especially when the IP addresses come from within the same ASN network.

To bypass TCP authentication

TCP authentication uses various methods to check if a client is real or a bot. During authentication, the first and/or first two TCP SYN packets are dropped, until the client sends the second or third packet. If the client passes authentication, the IP is flagged as that of a real user and granted access. If the attacker uses the same pool of IPs to keep sending TCP SYN packets, some will inevitably survive TCP authentication.

To leverage IoT botnets

Traffic sent by IoT botnets isn't spoofed; it corresponds to real IP addresses. Such attacks can have a huge impact on networks and servers. If an attack is large enough, it can incur hefty charges for massive outbound malicious traffic. In some Q3 incidents, botnet-driven SYN Flood attacks bypassed TCP authentication and hit the backend directly.

If malicious SYN traffic threatens to break the defence and hit the target server directly, SYN cookie, a technique used to resist IP spoofing attacks, can be the second layer of defence, which is more effective in mitigating Type 1 attacks. But it is much less so in mitigating Type 2 attacks due to a high volume of malicious traffic.

Type 3: Multiple, fixed real-source IPs abusing two different destination IPs:

In Type 3 (10.40% of SYN Flood attacks in Q3), multiple, fixed spoofed-source IPs are used to abuse two destination IPs. After tracking their sources Nexusguard found that most source IP addresses were valid, leading us to believe that such attacks were **Distributed Reflection Denial of Service (DRDoS)** attacks. Here, an attacker sends a spoofed SYN packet with the original source IP replaced by the victim's IP address to random or pre-selected reflection IP addresses.

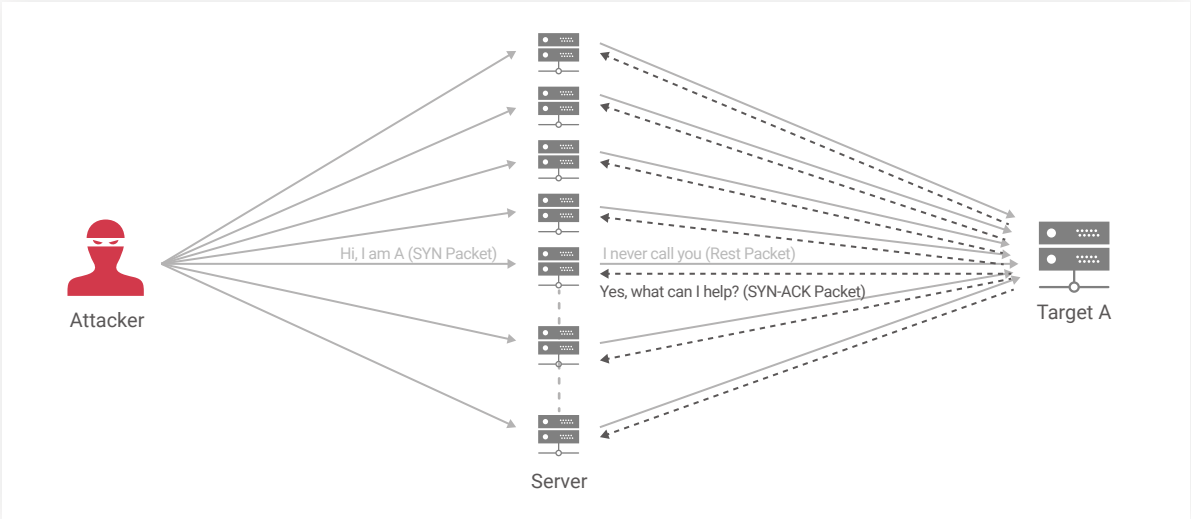


Figure 2. How Distributed Reflection Denial-of-Service (DRDoS) Attacks Work

The service ports at the reflection addresses reply with a SYN-ACK packet to the victim of the spoofed attack. When the victim does not respond with the last ACK packet, the reflection service will continue to retransmit the SYN-ACK packet, resulting in continued reflection.

From the attacker's perspective, this DRDoS is an extremely cost-effective way to launch denial-of-service attacks to the victim by taking advantage of a wide range of innocent addresses to reflect attack traffic. When the attack is distributed through multiple reflectors, the attack vector is called a distributed reflection denial-of-service (DRDoS) attack.

Any server with an open TCP port, which are widely available and accessible, can be leveraged as reflectors, making DRDoS attacks difficult to mitigate. Advanced mitigation techniques are required to address the threat of DRDoS attacks.

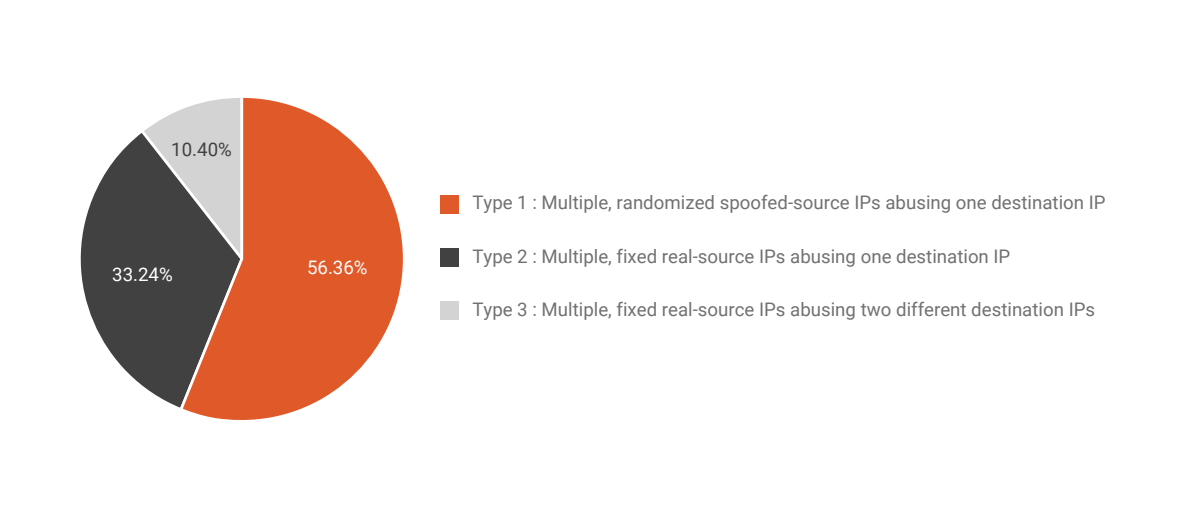


Figure 3. Types of SYN Flood Attacks, Q3 2019

Bit-and-Piece Attacks Continue to Spread

During the quarter, Bit-and-Piece attacks spread to 27 regions, three more than Q2. However, the number of ASNs targeted by such attacks decreased by 31% QOQ, and the number of IP addresses and prefixes selected to transport tiny, Bit-and-Piece traffic fell measurably. The maximum attack counts per IP address and per IP prefix also fell QOQ.

Targeted ASNs
54

Total IP Prefixes (Class C Networks) Under Attack
219 (185 Prefixes)

Attack Types

- CHARGEN (80.2%)
- DNS Amplification (14.63%)
- SSDP Amplification (4.67%)
- NTP Amplification (0.5%)

Targeted Geo-locations

Argentina, Bangladesh, Belgium, Brazil, Bulgaria, Cambodia, Canada, China, Czech Republic, Hong Kong, India, Iran, Islamic Republic of, Netherlands, New Zealand, Palestinian Territories, Philippines, Poland, Portugal, Saudi Arabia, Taiwan, Thailand, Turkey, Ukraine, United Kingdom, United States, Vietnam

Category	Minimum	Maximum
No. of Targeted IP Addresses per IP Prefix /24	5	215
Attack Durations (Minutes)	28.73	1,818.62
Attack Count per IP	40	32,056
Attack Count per IP Prefix	209	139,971

Table 1. Information about Attack Traffic with “Bit and Piece” Pattern, Q3 2019

Application Attack Traffic Emanates from Compromised Windows Systems and iOS Devices

Botnet-hijacked Windows OS computers and servers contributed to about 44% of application attack traffic in Q3, while iOS-powered mobile devices contributed about 31% to application attack traffic.

Overall, mobile and IoT devices contributed to about 8.4% of total DDoS attack traffic, including network and application attacks.

Devices	OS	Percentage
Computers & Servers	Windows	44.05%
	Other	6.66%
	Macintosh	8.58%
Mobile	iOS	30.72%
	Android	9.58%
	BlackBerry, DoCoMo	0.40%
Others (including IoT)	PSP, Nintendo Wii, Nintendo DS, etc.	0.01%

Table 2: Distribution of OS and Device Types as Sources of Application Attacks, Q3 2019

Note: Untraceable volumetric attacks transmitted with spoofed IP addresses such as TCP SYN, ICMP, and DNS were not included in our sampling. Only traceable attacks like HTTP/HTTPS Flood with real source IP addresses were counted. Attack traffic produced by mobiles botnets are identified based on the following criteria: malicious traffic from mobile gateway IP addresses, attack patterns in user-agent, URL, HTTP header, etc. that are unique to mobile botnets.

DDoS Activities

Types of Attack Vectors[1]

DNS Amplification and HTTP Flood attacks were dominant, representing 45.21% and 14.09% of total attacks, respectively. DNS Amplification attacks fell significantly (46.93% QOQ), while climbing dramatically 4,787.91% YOY. HTTP Flood surged 52.64% QOQ and 1,017.74% YOY. TCP SYN ranked third showing increases of 13.60% QOQ and 177.37% YOY. At 6.64% of the total, HTTPS Flood dropped 6.04% QOQ, yet jumped 192.83% YOY.

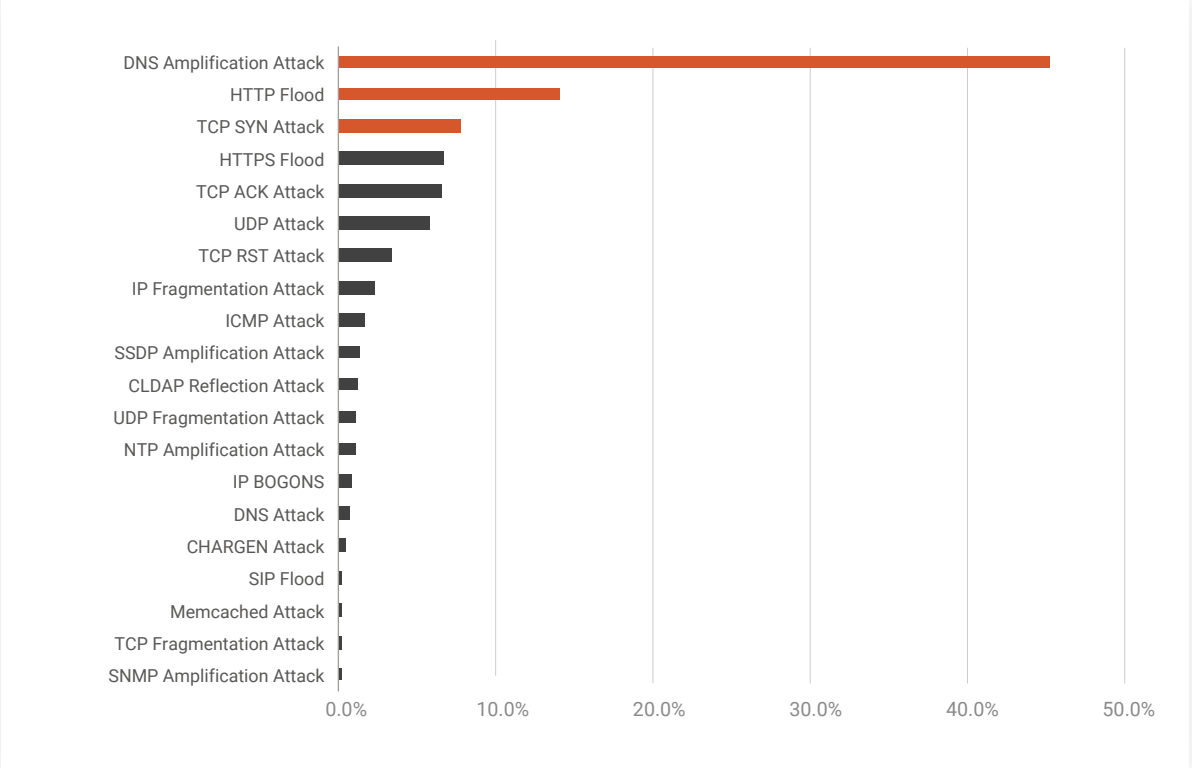


Figure 4. Distribution of DDoS Attack Vectors, Q3 2019

1 Attacks on network Layers 3 and 4 lasting at least five minutes of a size equal to or larger than 100Mbps are counted as volumetric attacks. Attacks targeting applications lasting at least five minutes with at least 500 requests per second are counted as application attacks. Attack vector counts measure the number of vectors exploited by the same attack on the same destination IP. An attack is defined as one or more event occurring within a time interval of five minutes. In the same attack, each vector is counted once no matter how many times it is targeted as long as the attacks occurred within the five-minute interval. As for Bit-and-Piece attacks, they are counted as a single attack based on a network-based destination IP address rather than a host-based destination IP address.

Top 3 Attack Vectors

No.1 DNS Amplification

45.21 %

4,448

A DNS Amplification attack occurs when UDP packets with spoofed target IP addresses are sent to a publicly accessible DNS server. Each UDP packet makes a request to a DNS resolver, often sending an "ANY" request in order to receive a large number of responses. Attempting to respond, DNS resolvers send a large response to the target's spoofed IP address. The target thus receives an enormous amount of responses from the surrounding network infrastructure, resulting in a DDoS attack. Because such a sizable response can be created by a very small request, the attacker can leverage this tactic to amplify attacks with a maximum amplification factor of 54.

No.2 HTTP Flood

14.09 %

1,386

Here attackers attempt to exhaust server resources by generating valid, countless HTTP requests or sessions. The most commonly used method to launch such attacks is HTTP GET flooding. Attackers can either initialize a large number of valid sessions or send a large number of requests in a single session to inundate the victim's web servers with answer requests. The process forces servers to allocate maximum resources to handle traffic so normal requests cannot reach them.

No.3 TCP SYN

7.73 %

760

The attacks take place when voluminous SYN requests with spoofed IP addresses are sent out, triggering targeted servers to respond with SYN-ACK. However, the messages can't be sent back from the targeted server to consummate the Three-way Handshake required to complete the connection. Consequently, with no SYN-ACK or ACK responses, the connection between the perpetrator and the available ports on a targeted server remains half-open, causing the server to malfunction.

Quantity of Attack Vectors

Single-vector attacks dominated with 66.00% of the total, while multi-vectors accounted for the rest. Two- and three-vector attacks accounted for 17.57% and 7.01%, respectively. The maximum number of vectors used was 12.

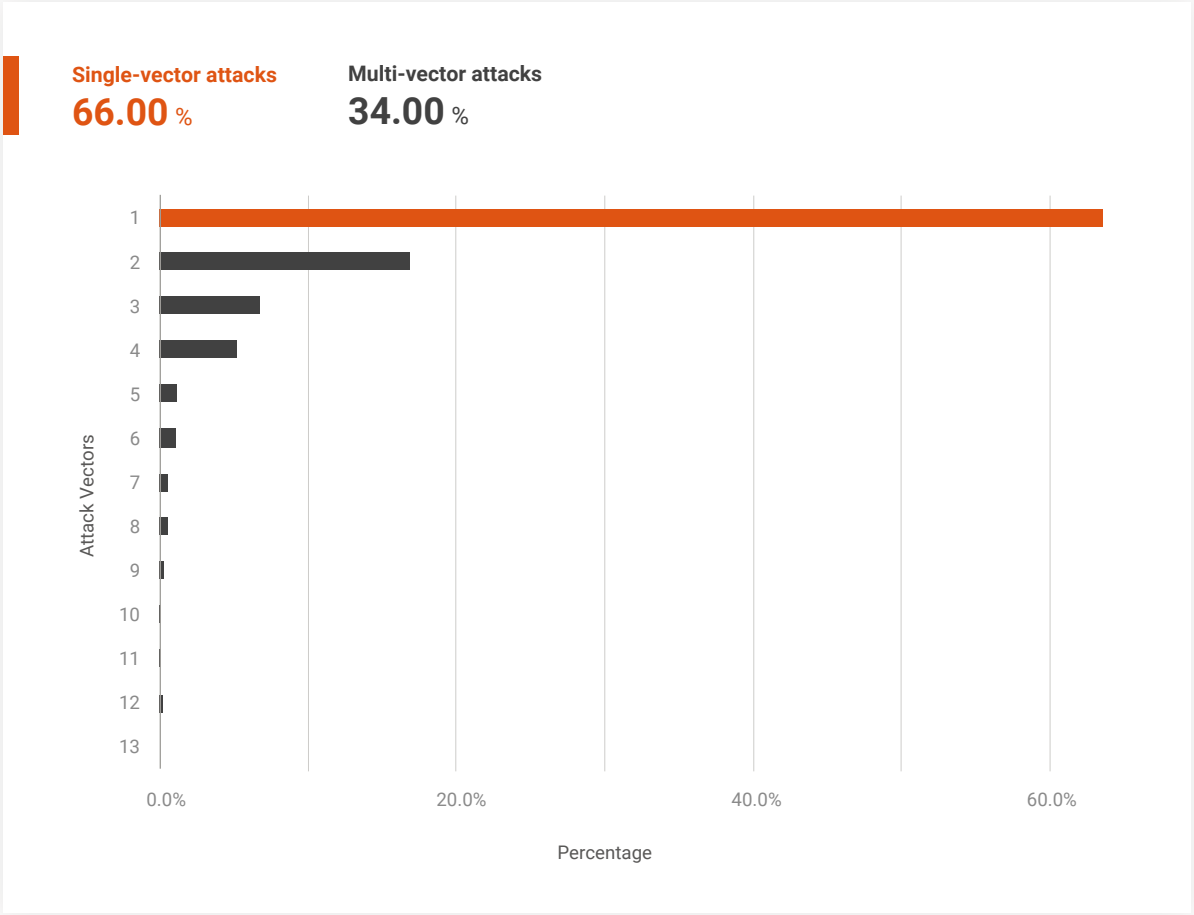


Figure 5. Distribution of DDoS Attack Vectors, Q3 2019

Attack Durations[2]

85.61% of attacks lasted fewer than 90 minutes. 0.02% lasted between 30,000 and 40,000 minutes. The quarterly average was 125.93 minutes, while the longest attack lasted 27 days, 7hours, 10minutes, and 27 seconds. In the quarter, the average duration dropped 31.15% QOQ and 31.65% YOY and the maximum duration fell 24.07% QOQ while rising 898.06% YOY.

<90 minutes
85.61 %

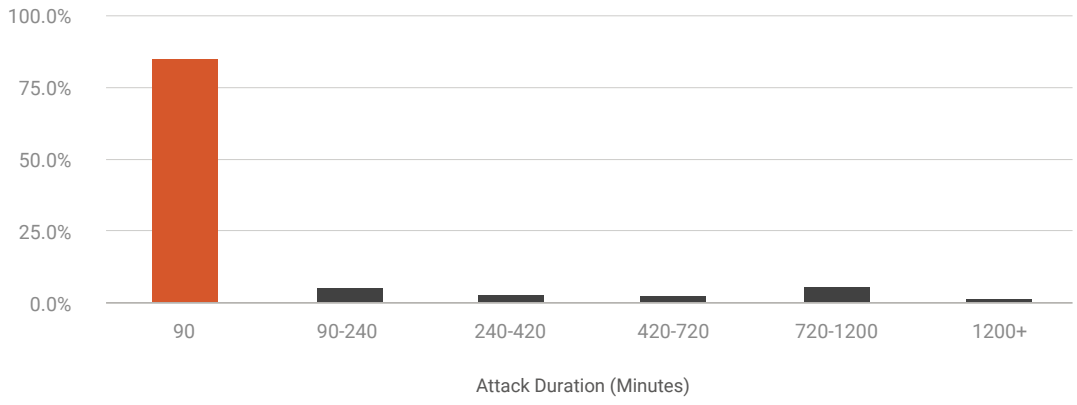


Figure 6. Attack Durations Fewer than 20,000 Minutes, Q3 2019

>1200 minutes
0.78 %

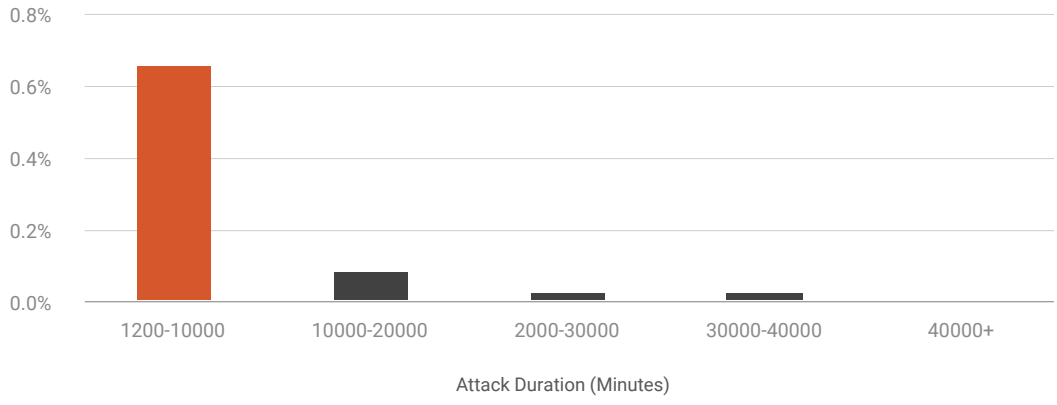


Figure 7. Attack Durations 1,200+ Minutes, Q3 2019

2 Attack duration measures the timespan of a series of attacks on the same destination IP within an interval of five minutes, regardless of the number of attack vectors. If no further attacks occur following the five-minute interval, the end of the last attack is considered the cut-off time. "Ceasefire" breaks between attacks are excluded from attack duration time. As for Bit-and-Piece attacks, they are counted as a single attack based on a network-based destination IP address rather than a host-based destination IP address.

Attack Size Distribution[3]

In the quarter, 96.86% of attacks were smaller than 10Gbps and 89.64% smaller than 1Gbps — those ranging between 1Gbps and 10Gbps accounted for only 7.22%. Maximum size increased 137.49% QOQ and 137.29% YOY. Average size rose 29.34% QOQ and 28.94% YOY.

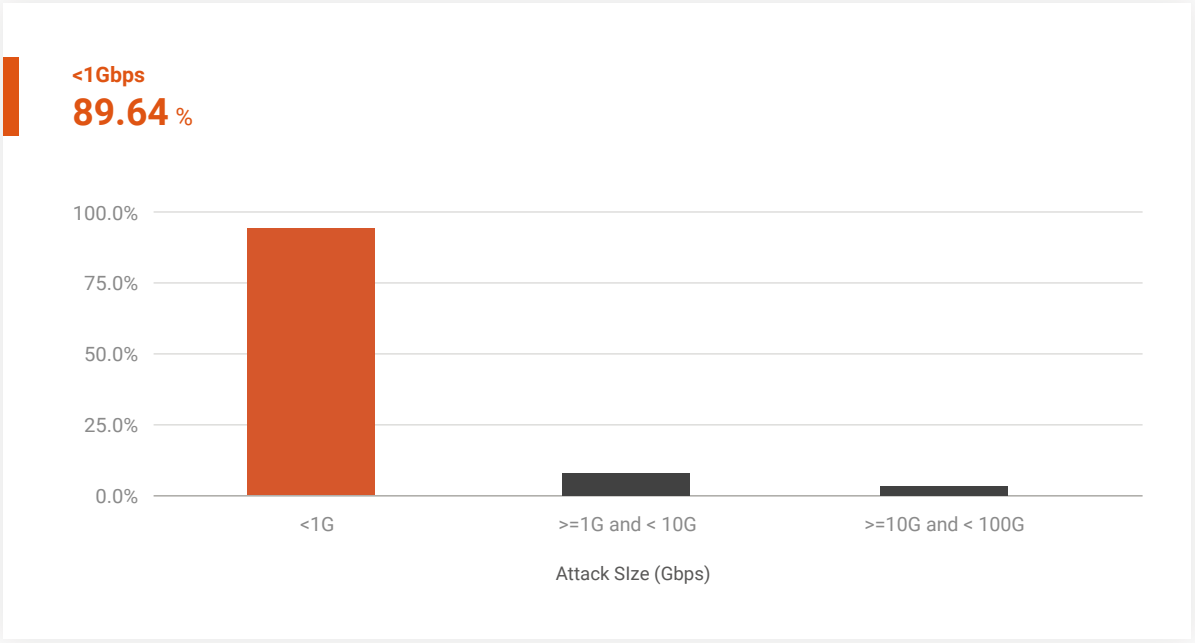


Figure 8. Attack Size Distribution, Q3 2019

3 Attack size measures the aggregate size of a series of attacks on the same destination IP within a time interval of five minutes, regardless of the number of attack vectors. The peak size of each attack within the attack interval is counted in the aggregation. If no further attacks occur after five minutes, the aggregation ends. As for Bit-and-Piece attacks, they are counted as a single attack based on a network-based destination IP address rather than a host-based destination IP address.

Attack Source Distribution — Global & Regional

Global	Attack Counts	Percentage
China	317,628	19.87%
Turkey	243,819	15.25%
United States	243,706	15.24%
South Korea	197,168	12.33%
Netherlands	109,262	6.83%
Germany	108,221	6.77%
France	88,510	5.54%
Sweden	73,320	4.59%
Canada	52,040	3.25%
Russian Federation	40,345	2.52%
Others	124,808	7.81%

Table 3. Top 10 Global Attack Sources, Q3 2019

APAC	Attack Counts	Percentage
China	317,628	58.98%
South Korea	197,168	36.61%
Viet Nam	4,789	0.89%
Mongolia	4,007	0.74%
Singapore	3,962	0.74%
India	3,133	0.58%
Hong Kong	2,870	0.53%
Indonesia	1,805	0.34%
Thailand	700	0.13%
Japan	675	0.13%
Others	1,787	0.13%

Table 4. Top 10 APAC Attack Sources, Q3 2019

Note: Untraceable volumetric attacks transmitted with spoofed IP addresses such as TCP SYN, ICMP, and DNS were not included in our sampling. Only traceable attacks like HTTP Flood with real source IP addresses were counted. In order for the traffic patterns and behaviour to match the bit-and-piece attack's definition, attacks are counted as one attack based on network-based destination IP addresses instead of host-based destination IP address.

EMEA	Attack Counts	Percentage
Turkey	243,819	32.79%
Netherlands	109,262	14.69%
Germany	108,221	14.55%
France	88,510	11.90%
Sweden	73,320	9.86%
Russian Federation	40,345	5.43%
Romania	19,748	2.66%
United Kingdom	12,656	1.70%
Ukraine	10,637	1.43%
Norway	7,954	1.07%
Others	29,189	3.93%

Table 5. Top 10 Attack Sources in EMEA, Q3 2019

The Americas	Attack Counts	Percentage
United States	243,706	76.97%
Canada	52,040	16.43%
Panama	9,189	2.90%
Brazil	4,840	1.53%
Mexico	3,198	1.01%
Jamaica	1,722	0.54%
Argentina	1,043	0.33%
Colombia	220	0.07%
Ecuador	168	0.05%
Peru	146	0.05%
Others	370	0.12%

Table 6. Top 10 Attack Sources in the Americas, Q3 2019

Attack Source by Autonomous System Number (ASN) – Global & Regional

Global ASNs	Network Name	Percentage
205101	AS205101, TR	15.13%
4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	12.21%
4766	KIXS-AS-KR Korea Telecom, KR	12.01%
16276	OVH, FR	6.64%
396507	EMERALD-ONION - Emerald Onion, US	5.32%
37943	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology Co., Ltd, CN	5.26%
200052	FERAL Feral Hosting, GB	4.55%
51815	TEKNIKBYRAN, SE	3.41%
38994	ERAHOST-AS, NL	3.33%
4224	CALYX-AS - The Calyx Institute, US	2.55%
Others	1188 ASNs	29.58%

Table 7. Top 10 Global ASNs, Q3 2019

APAC ASNs	Network Name	Percentage
4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	36.52%
4766	KIXS-AS-KR Korea Telecom, KR	35.92%
37943	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology Co., Ltd, CN	15.74%
23650	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN	1.36%
37963	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN	0.90%
4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	0.85%
9318	SKB-AS SK Broadband Co Ltd, KR	0.77%
133774	CHINATELECOM-FUJIAN-FUZHOU-IDC1 Fuzhou, CN	0.77%
9484	MOBINET-AS-MN Mobinet LLC. AS Mobinet Internet Service Provider, MN	0.75%
4808	CHINA169-BJ China Unicom Beijing Province Network, CN	0.64%
Others	329 ASNs	5.78%

Table 8. Top 10 ASNs in APAC, Q3 2019

EMEA ASNs	Network Name	Percentage
205101	AS205101, TR	30.52%
16276	OVH, FR	13.38%
200052	FERAL Feral Hosting, GB	9.17%
51815	TEKNIKBYRAN, SE	6.89%
38994	ERAHOST-AS, NL	6.72%
43350	NFORCE, NL	3.53%
57043	HOSTKEY-AS, NL	2.68%
9009	M247, GB	2.50%
1101	IP-EEND-AS IP-EEND BV, NL	2.37%
60729	ZWIEBELFREUNDE, AT	1.60%
Others	548 ASNs	20.65%

Table 9. Top 10 ASNs in EMEA, Q3 2019

AMERICAS ASNs	Network Name	Percentage
396507	EMERALD-ONION - Emerald Onion, US	31.37%
4224	CALYX-AS - The Calyx Institute, US	15.01%
14061	DIGITALOCEAN-ASN - DigitalOcean, LLC, US	14.86%
53667	PONYNET - FranTech Solutions, US	13.79%
3	MIT-GATEWAYS - Massachusetts Institute of Technology, US	4.59%
32780	HOSTINGSERVICES-INC - Hosting Services, Inc., US	2.15%
30633	LEASEWEB-USA-WDC-01 - Leaseweb USA, Inc., US	1.94%
21859	ZNET - Zenlayer Inc, US	1.35%
395089	HEXTET - Hextet Systems, CA	1.15%
18451	LESNET - LES.NET, CA	1.01%
Others	302 ASNs	12.78%

Table 10. Top 10 ASN Rankings in the Americas, Q3 2019

End Notes

In Q3 2019, Nexusguard saw perpetrators frequently abuse the three-way TCP handshake to launch three types of SYN Flood attacks, including DRDoS (Distributed Reflection Denial-of-Service). As noted earlier in this report, SYN Flood is a relatively old attack vector and was previously considered to be less effective than UDP Reflection. However, attackers have come to realize that SYN Flood Reflection attacks can also achieve a significant impact.

For DNS Amplification and Memcached Reflection attacks, suitable reflectors/amplifiers are not widely available. However, for SYN Flood Reflection, any server with an open TCP port is an ideal attack vector, and such reflectors are widely available and easy to access. Consequently, intended or not, SYN Flood Reflection not only hits its targeted victims, but also, via randomly selected reflectors, impacts innocent users. Be they individuals, businesses, or other organizations, innocent victims of such attacks end up having to process large volumes of spoofed requests and what appear to be legitimate replies from the attack target. As a result, bystanders can incur hefty fees for bandwidth consumed by junk traffic or even suffer from secondary outages.

Deploying scalable, cloud-based DDoS protection is the most effective solution for mitigating the impact of increasingly complex SYN Flood Reflection and Bit-and-Piece attacks. Nexusguard's mitigation technology employs behavioral and threshold-based detection methods that quickly identify and accurately block anomalies and excessive junk while letting in legitimate traffic, making it an ideal solution for protecting ISPs, their networks, and their customers.

Research & Methodology

As a global leader in Distributed Denial of Service (DDoS) attack mitigation, Nexusguard observes and collects real-time data on threats facing enterprise and service-provider networks worldwide. Threat intelligence is gathered via attack data, research, publicly available information, Honeypots, ISPs, and logs recording traffic between attackers and their targets. The analysis conducted by our research team identifies vulnerabilities and measures attack trends worldwide to provide a comprehensive view of DDoS threats.

Attacks and hacking activities have a major impact on cybersecurity. Because of the comprehensive, global nature of our data sets and observations, Nexusguard is able to evaluate DDoS events in a manner that is not biased by any single set of customers or industries. Many zero-day threats are first seen on our global research network. These threats, among others, are summarized in quarterly Threat Reports produced by Nexusguard's research team:

- Tony Miu, Editor, Research Direction & Threat Analysis
- Ricky Yeung, Research Engineer, Data Mining & Data Analysis
- Dominic Li, Technical Writer & Content Development

20191224-EN-A4

About Nexusguard

Founded in 2008, Nexusguard is a leading cloud-based distributed denial of service (DDoS) security solution provider fighting malicious internet attacks. Nexusguard ensures uninterrupted internet service, visibility, optimization and performance. Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements. Nexusguard also enables communication service providers to deliver DDoS protection solution as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime.

NEXUSGUARD®

www.nexusguard.com