NEXUSGUARD®

Threat Report

Distributed Denial of Service (DDoS)

Q3 2021

Contents

Key Observations 02

DDoS attacks rise sharply with increased ferocity and volume in Q3 2021 03

Attack statistics reveal major shift in attack trend 03

Attackers target specific services using large volumetric attacks 04

Impact to CSP networks 07

Challenges faced by CSPs 07

Attack Statistics 08

Types of Attack Vectors 08

Top 3 Attack Vectors 09

Quantity of Attack Vectors 10

Attack Durations 11

Attack Size Distribution 12

Bit-and-Piece Attacks 13

Source Distribution of Application Attack 14

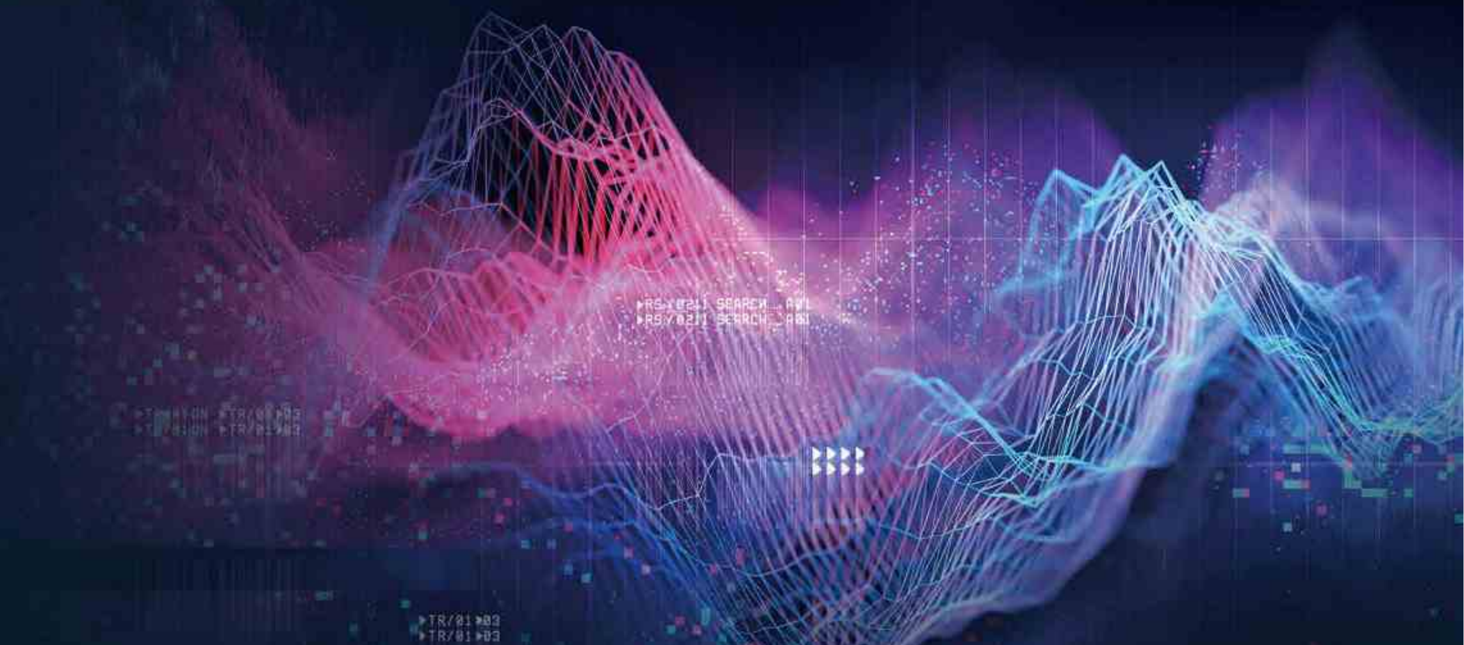
Application Attack Source Distribution (IP Reputation) — Global & Regional 15

Application Attack Source by Autonomous System Number (ASN) – Global & Regional 17

Conclusion 19

Research & Methodology 20

NEXUSGUARD®



Q3 2021 Threat Report

Key Observations

Total Attacks

vs. Q2 2021	-28.03% ▼
vs. Q3 2020	18.71% ▲

Attack Sizes

Maximum		
586.00 Gbps	vs. Q2 2021	544.66% ▲
	vs. Q3 2020	232.41% ▲

Average		
1.13 Gbps	vs. Q2 2021	105.12% ▲
	vs. Q3 2020	-25.78% ▼

Top 6 DDoS Attack Types

	UDP	TCP ACK	UDP Fragmentation	Application	Amplification	Bit and Piece
vs. Q2 2021	-48.44% ▼	188.49% ▲	145.43% ▲	35.96% ▲	-64.01% ▼	-82.75% ▼
vs. Q3 2020	32.54% ▲	811.45% ▲	308.56% ▲	67.72% ▲	-48.39% ▼	-92.43% ▼

DDoS attacks rise sharply with increased ferocity and volume in Q3 2021

Q3 saw a notable trend in which attackers launched DDoS attacks at single targets within a CSP, attributing an attack size increase of 544% QoQ and 232% YoY. DDoS attacks against infrastructures on the other hand saw a significant reduction, particularly attacks through Bit-and-Piece tactics widely used in previous quarters, decreased by 82% QoQ and 92% YoY.

Over 55% of attacks focused on hitting a specific service with high volumes of traffic simultaneously, and according to our research, several 500 Gbps plus attack events were recorded, peaking at 586 Gbps. Due to the dramatic increase in attack size, this shift to employing high-penetration volumetric attacks can potentially lead to additional impact to CSP networks, regionally.

Attack statistics reveal major shift in attack trend

Table 1 shows the top 10 CSPs under DDoS attack, of which over 10,000 attack events targeted a single CSP. Over 98.72% of the attacks targeted the same destination IP and corresponding destination port simultaneously, and the duration of each attack ranged between 35.87 and 79.25 minutes. The attacks were launched with an obvious purpose in mind. Attackers concentrated their resources on single targets using heavy fire attacks for sustained periods to inflict maximum damage.

Rank	Attack Event	Percentage	Attack Count	Percentage
1	11,752	35.45%	13,243	27.44%
2	9,475	28.58%	18,152	37.61%
3	3,950	11.91%	3,963	8.21%
4	3,068	9.25%	3,103	6.43%
5	755	2.28%	864	1.79%
6	618	1.86%	1,658	3.44%
7	498	1.50%	498	1.03%
8	469	1.41%	3,383	7.01%
9	385	1.16%	385	0.80%
10	360	1.09%	489	1.01%

Table 1 - Top 10 attack cases at targeted CSPs

Attackers target specific services using large volumetric attacks

Our records show that 2962 attack cases were over 100 Gbps and 291 attack cases exceeded 400 Gbps. As shown in Table 2, the targets under attack were primarily web services and mobile app services. Without a robust DDoS mitigation strategy in place, these attacks are enough to knock most online services offline. Moreover, large volumes of attack traffic causes an overload on network equipment and saturation of core network devices.

Rank	Protocol	Service	Count	Percentage
1	TCP	HTTPS	995,676	43.04%
2	UDP	HTTPS	140,089	6.06%
3	UDP	DNS	28,223	1.22%
4	UDP	NTP	10,793	0.47%
5	UDP	HTTP	3,616	0.16%
6	UDP	Mobile App service	5,544	0.24%
7	TCP	HTTP	1,878	0.08%
8	UDP	VPN	1,034	0.04%
Other			1,126,601	48.70%

Table 2 - Top 10 attack cases against specific services

Why attackers are choosing to employ high-penetration volumetric attacks

In Q3, attackers opted to employ high-penetration volumetric attacks, such as TCP ACK and UDP attacks, rather than amplification attacks since the signatures can be easily blocked by source IP blacklists. Of the volumetric attacks that were employed, TCP ACK and UDP attacks accounted for 55.62% of all attacks. One of the reasons behind adopting such attacks lies in the design of CSP networks - TCP ACK and UDP traffic can be transmitted from the attack source to the target CSP very efficiently. And aside from attacks with obvious signatures, upstream ISPs tend not to interfere with passing traffic.

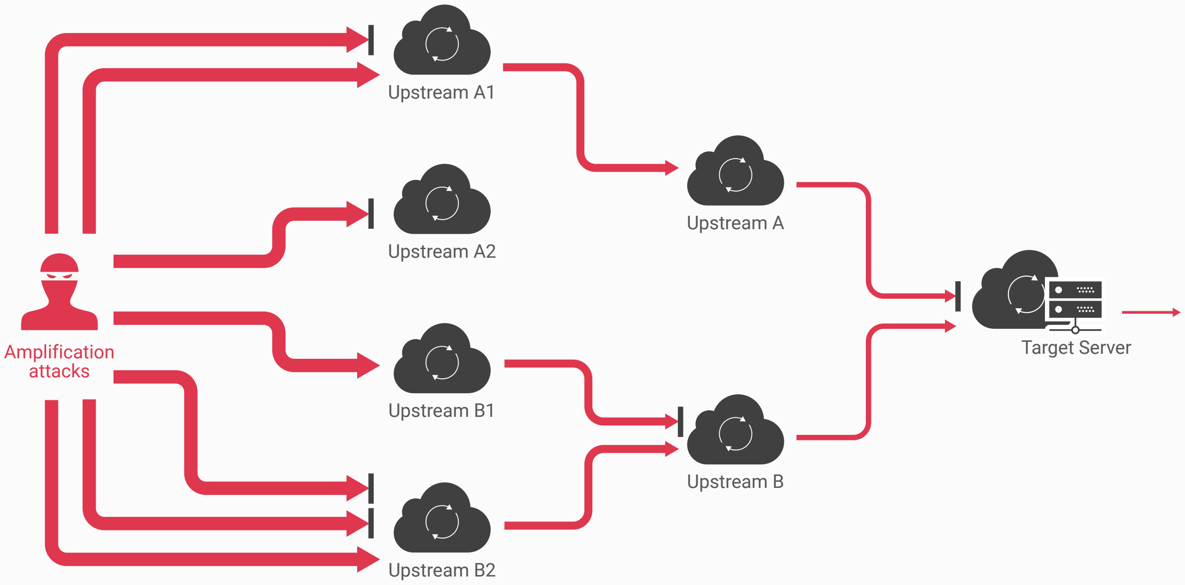


Figure 1 - Amplification attacks blocked by upstream ISPs

Leveraging TCP ACK packets to launch attacks

One of the smallest packets commonly seen on networks is a TCP ACK. A TCP ACK packet has a 20 byte IP header and a 20 byte TCP header, adding up to 40 bytes. Because this is smaller than the Ethernet's minimum payload size of 46 bytes, it is automatically padded prior to transmission to bring it up to size. TCP ACK packets are mainly used in the TCP Three-Way handshaking process to establish a reliable connection. The connection is full-duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other. The exchange of these four flags is performed in three steps—SYN, SYN-ACK, and ACK. The first ACK sent by each end acknowledges the other end's initial sequence number itself but has no data.

Attackers abused TCP ACK packets to launch DDoS attacks - two types of TCP ACK attack packets ranging between 46-1498 bytes were identified as follows:

1. TCP ACK packets without payload

Commonly seen on networks, these types of TCP ACK packets are not blocked and allowed to pass through ISPs. Although this type of packet can only generate small-sized attacks, it can still have an impact on network devices, particularly ones that need to process every TCP ACK packet. High packet-rate loads of traffic ultimately drains the resources of network devices, routers and switches.

2. TCP ACK packets with random data

According to our findings, several Gbps of malformed TCP ACK attack packets passed through upstreams, targeting various services of CSPs. Surprisingly, upstreams did not interfere with nor inhibit these packets, allowing them to pass to targeted CSP networks, resulting in saturation of bandwidth.

Generating malformed UDP packets to pass through ISPs

User Datagram Protocol (UDP) is one of the core Internet protocols commonly used to establish host-to-host communications for applications such as streaming audio and video, DNS and NTP. As a connectionless protocol, UDP transmits data in one direction from source to destination without verifying the readiness or state of the receiver.

Attackers generated UDP-like application traffic using malformed UDP packets with random payloads between 1024-1440 bytes. The mechanics of UDP is such that only the receiver knows how an application works - upstreams as well as hosting CSP networks have no idea whether the UDP packets being sent are normal, abnormal or malformed. Moreover, some UDP applications are customized or encrypted, resulting in UDP attack packets being allowed to pass unhindered.

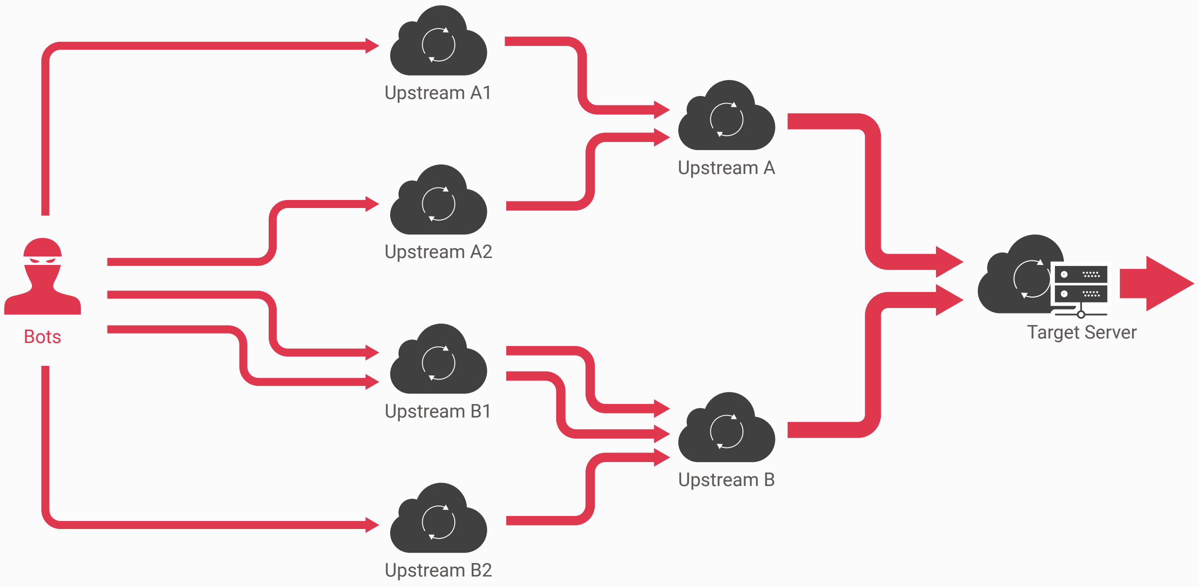


Figure 2 - Attack traffic passing through ISPs to targeted CSPs

Impact of high-penetration volumetric attacks

Owing to upstream ISPs' lack of transparency and knowledge of the TCP and UDP services that pass through them and arrive at their peers, attackers have been successful in launching TCP ACK and UDP attacks. In the case of targeted CSPs, concentrated influxes of large volumes of attack traffic flooded CSP networks after passing through a number of upstream ISPs, cutting off access to services of downstream customers.

Impact to CSP networks

Large volumes of traffic hitting a CSP not only denies access to various services but also causes considerable impact to the CSP network.

TCP ACK attacks begin by hitting network devices before they arrive at the targeted service. Since network devices process incoming packets one by one through Network Address Translation (NAT) or Port forwarding, the processing of large volumes of TCP ACK traffic eventually results in the outage of these devices. To safeguard against malformed and large TCP ACK traffic from saturating the bandwidth of CSP networks, it is vital that DDoS traffic once detected is dropped instantly and never allowed to reach the network devices.

CSP networks are complex environments in which to apply appropriate security policies to control incoming traffic. Attack traffic with obvious signatures, however, is dropped at the first instant so as to protect service owners within the CSP against unforeseeable consequences. Common UDP applications such as DNS and NTP have specific DDoS mitigation policies in place. However, most UDP applications today are customized and therefore difficult to classify and apply packet validation.

UDP packets are one of the most difficult to apply security policies, and since it is extremely difficult to classify normal traffic packets among large volumes of attack traffic, UDP attacks are able to effectively saturate the bandwidth of CSPs, denying users access to services.

Challenges faced by CSPs

When CSP networks have been severely affected by an attack, the first port of call is to blackhole the destination IPs. However, if the corresponding service has no DDoS mitigation backup plan in place, the attack will still cause online services to become unavailable.

For critical online services and VIP customers under attack, offering only a blackholing method is not the ideal solution given that this would give competitors who are able to offer whole suites of DDoS mitigation solutions a competitive advantage. That being said, DDoS mitigation solutions do have limitations particularly when it comes to dealing with large-sized attacks. Therefore, blackholing is still practiced when a CSP’s network is gravely impacted by an attack, even though it is not the most suitable option.

Attack Statistics

Types of Attack Vectors[1]

UDP and TCP ACK attacks were in the predominance of vectors, representing 33.61% and 22.01%, respectively. UDP attack decreased by 48.44% QoQ while increased by 32.54% YoY. TCP ACK Attack increased by 188.49% QoQ and 811.45% YoY. UDP Fragmentation Attack was ranked third with 18.57%, showing an increase of 145.43% QoQ and 308.56% YoY.

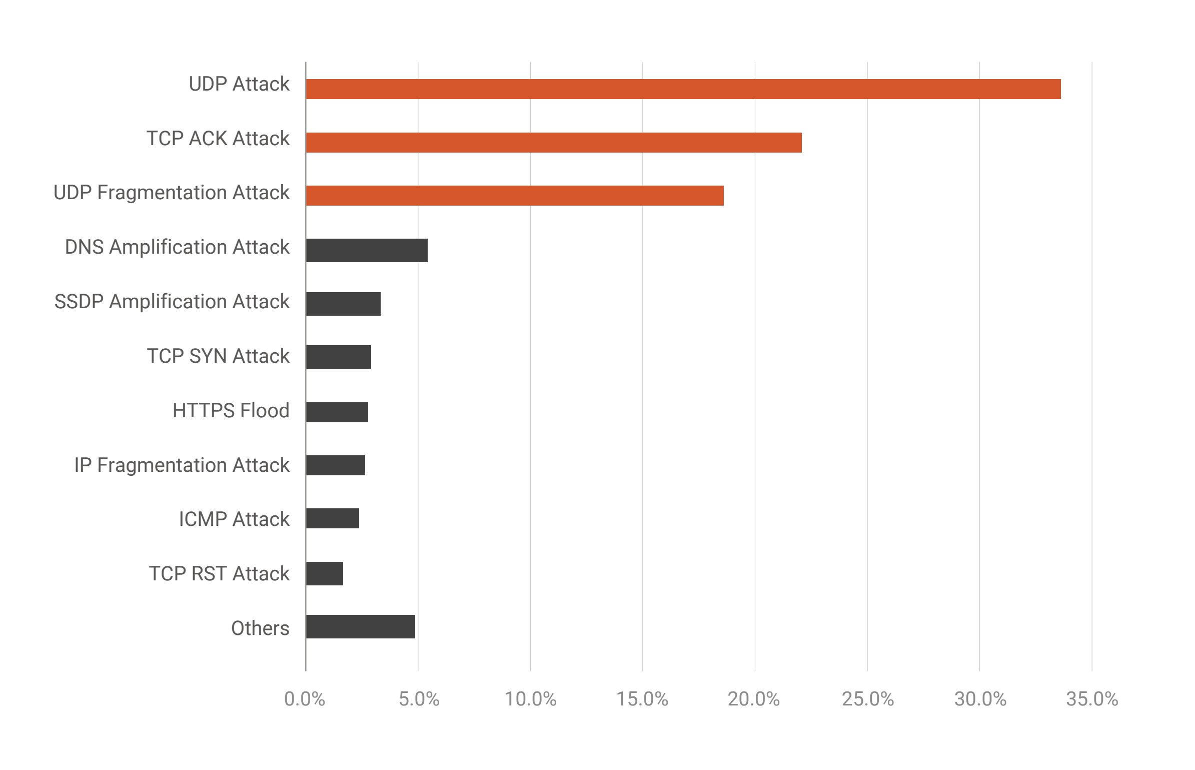


Figure 3 - Distribution of DDoS Attack Vectors

[1] Attacks on network Layers 3 and 4 lasting for at least five minutes at a size equal to or larger than 100Mbps were counted as volumetric attacks. Attacks targeting applications lasting for at least five minutes with at least 500 requests per sec were counted as application attacks. Attack vector measures the number of vectors exploited by the same attack on the same destination IP. An attack is defined as one attack or more than one attack that occurred within a time interval of five minutes in between. In the same attack, each attack vector is counted once no matter how many times it is targeted as long as the attacks occurred within a time interval of five minutes in between. 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.

Top 3 Attack Vectors

No.1 UDP Attack

33.61 %

15,201

UDP (User Datagram Protocol) attacks can quickly overwhelm the defenses of unsuspecting targets. Speed in detection and response is key to thwarting attackers using this volumetric strategy. UDP frequently serves as a smokescreen to mask other malicious activities such as efforts to compromise personal identifiable information (PII) or the execution of malware or remote codes. When large numbers of UDP packets hit a targeted network, bandwidth is congested and a server's resources sapped, ultimately making them inaccessible.

No.2 TCP ACK Attack

22.01 %

9,953

A DNS Amplification at stack 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 sizeable 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.3 UDP Fragmentation Attack

18.57 %

8,396

UDP fragmentation attacks are launched by transmitting fraudulent UDP larger than a network's maximum transmission unit (MTU), usually around 1,500 bytes. Because the fake packets cannot be reassembled, the resources of target servers are consumed very fast, bringing about their unavailability.

Quantity of Attack Vectors

The dominant attack vector was single with 45.65% while the multi-vectors shared the rest with 54.35%. The 2nd and 3rd vectored attacks contributed 36.12% and 4.65%, respectively.

Single-vector attacks
45.65 %

Multi-vector attacks
54.35 %

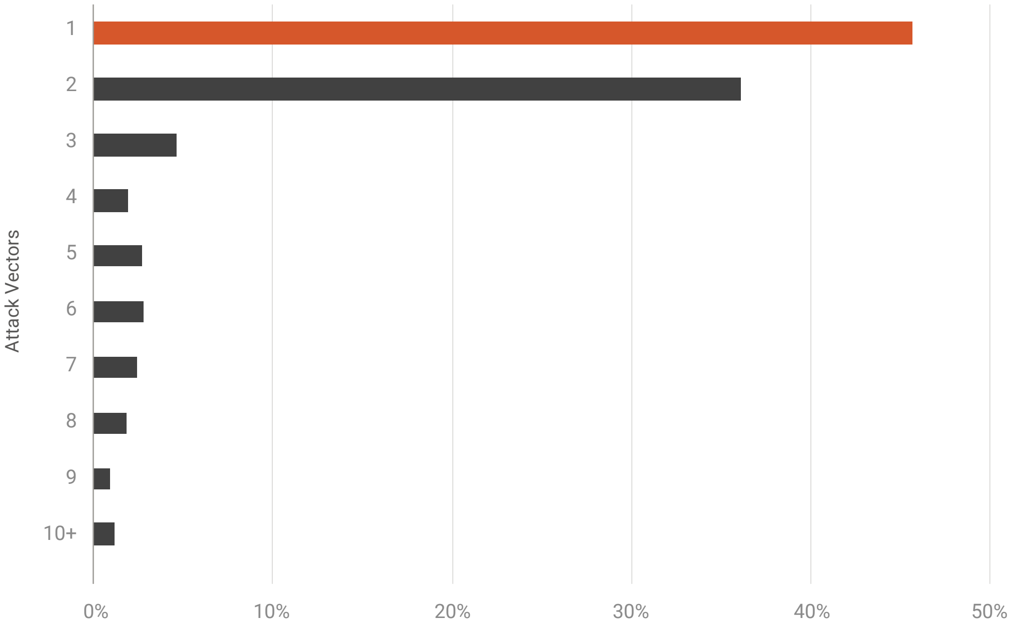


Figure 4 - Distribution of DDoS Attack Vectors

Attack Durations[2]

84.45% of the total attacks lasted fewer than 90 minutes, the rest of which was longer than 90 minutes. 3.73% of attacks are longer than 1200 minutes. The quarterly duration averaged 159.69 minutes, while the longest attack lasted 11,173 minutes. QoQ, both the maximum and average duration decreased by 74.79% and 6.84%. YoY, the maximum duration decreased by 82.48% while the average duration increased by 16.08%.

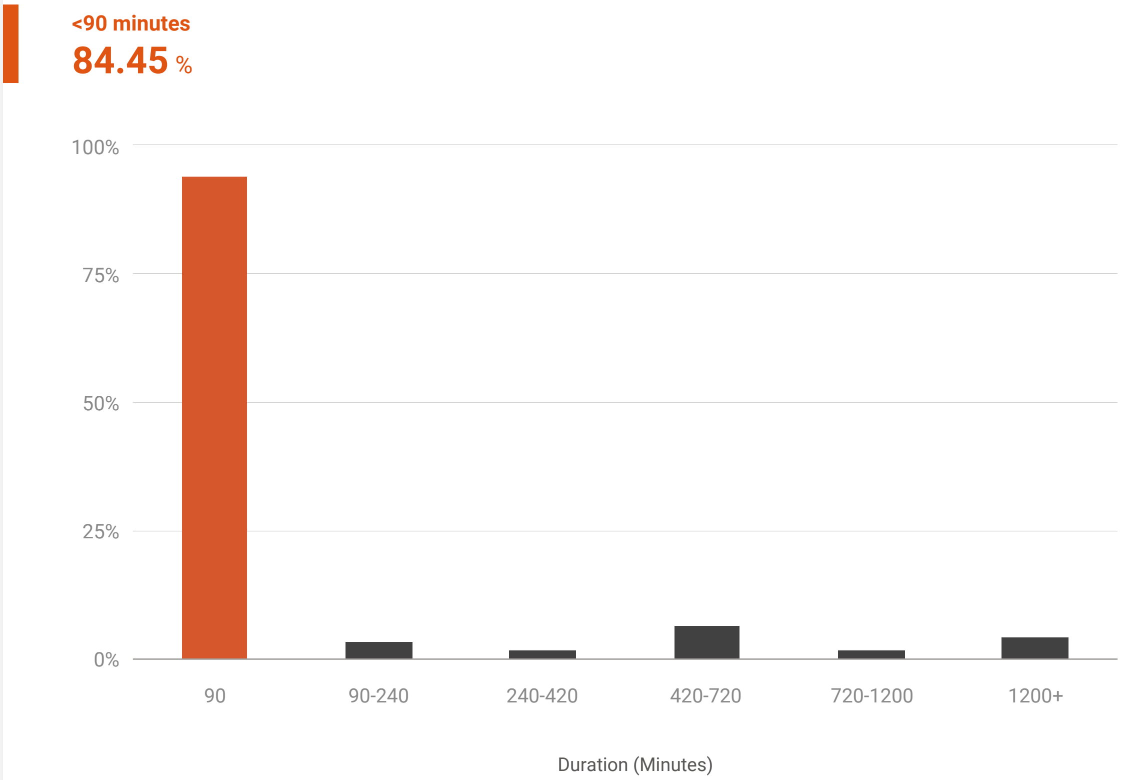


Figure 5 - Percentage of Attack Duration

[2] Attack duration measures the timespan of a series of attacks on the same destination IP within a time interval of five minutes in between but regardless of the number of attack vectors. If no more attack occurs after five minutes, the finish time of the last attack is considered to be the cut-off time. The "truce" between attacks are excluded from attack duration. 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.

Attack Size Distribution[3]

During the quarter, 67.37% of attacks were smaller than 1Gbps and 84.54% smaller than 10Gbps. 15.45% of attacks were equal and larger than 10Gbps. The maximum size increased by 544.66% QoQ and 232.41% YoY, and so did the average size increased by 105.12% QoQ and decreased by 25.78% YoY, respectively.

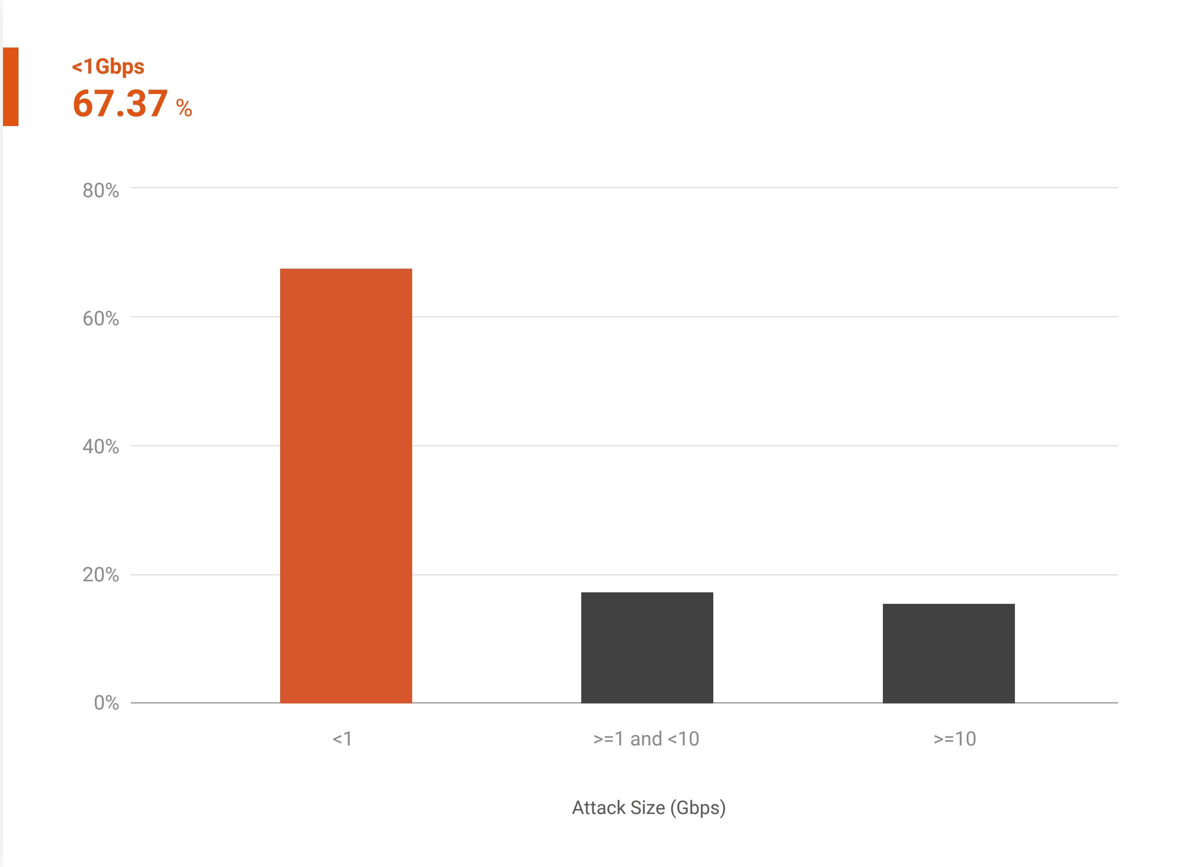


Figure 6 - Attack Size Distribution

[3] Attack size measures the aggregate size of a series of attacks on the same destination IP within a time interval of five minutes in between but regardless of the number of attack vectors. The peak size of each attack within the same attack is counted in the aggregation. If no more attack occurs after five minutes, the aggregation stops. In order for the traffic patterns and behavior 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.

Bit-and-Piece Attacks

ASN-level Communications Service Providers (CSPs) around the world, especially ISPs, continue to be impacted by the stealthy, sophisticated bit-and-piece attacks, which are carried out by drip-feeding doses of junk traffic into a large IP pool. Within each IP space, the junk traffic is small enough to bypass traditional threshold-based detection, but is big enough to clog the target when the bits and pieces are accumulated from different IPs. During the quarter, a total of 17 ASNs were impacted by bit-and-piece attacks. The total number of IP prefixes (Class C) attacked was 143.

Targeted ASNs	Total No. of IP Prefixes (Class C) Under Attack
17	143

Attack Types

- UDP Attack(33.04%)
- TCP ACK Attack(15.86%)
- SSDP Amplification Attack(12.78%)
- DNS Amplification Attack(9.69%)
- UDP Fragmentation Attack(9.25%)
- CLDAP Reflection Attack(6.17%)
- ICMP Attack(5.73%)
- TCP SYN Attack(2.64%)
- NTP Amplification Attack(1.76%)
- HTTPS Flood(1.32%)
- DNS Attack(0.44%)
- IP BOGONS(0.44%)
- TCP Null Attack(0.44%)
- TCP RST Attack(0.44%)

Targeted Geo-locations

Bangladesh, Brazil, Germany, Hong Kong, Philippines, Thailand, United Kingdom, United States

Category	Minimum	Maximum
No. of targeted IP addresses per /24 network	10	256
Attack Size by IP (Gbps)	Less than 0.0001	51.58
Attack Size by /24 network (Gbps)	0.0020	295.83
Average Attack Size(Gbps)	Less than 0.0001	3.68
Attack count per IP	41	1602
Attack count per IP prefix	813	20791
Duration (minutes)	28.07	678.00

Table 3 – Summary of Bit-and-Piece Attacks

Source Distribution of Application Attack[4]

MacOS devices contributed to about 22.43% of all application attack traffic, whereas Windows-powered PCs and notebooks contributed to about 48.08%. Mobile iOS devices such as iPads and iPhones made up about 4.98% of all application attack traffic, whereas android devices accounted for about 24.19%.

Devices	OS	Percentage
Computers and Servers	Windows OS	30.54%
	Other OS	17.54%
	Macintosh OS	22.43%
Mobile	iOS	4.98%
	Android	24.19%
	Other OS(BlackBerry, DoCoMo)	0.07%
Others (including IoT)	Other OS e.g. PSP, Nintendo Wii, Nintendo DS	0.24%

Table 4 – Source Distribution of Application Attack

[4] 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 mobile 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.

Application Attack Source Distribution (IP Reputation) — Global & Regional

Name	Percentage
China	17.42%
Turkey	16.43%
United States	14.33%
Hong Kong	11.18%
Germany	6.27%
Indonesia	5.79%
Cambodia	4.78%
Singapore	4.74%
Taiwan	1.97%
Vietnam	1.84%
Others(217 Regions)	15.25%

Table 5 - Top 10 Sources Ranking

APAC	Percentage
China	32.66%
Hong Kong	20.95%
Indonesia	10.86%
Cambodia	8.96%
Singapore	8.89%
Taiwan	3.70%
Vietnam	3.45%
Thailand	2.93%
Philippines	1.84%
Australia	1.42%
Others(32 Regions)	4.34%

Table 6 - Top 10 Sources in APAC

EMEA	Percentage
Turkey	56.52%
Germany	21.59%
France	3.61%
United Kingdom	3.50%
Netherlands	2.83%
Cyprus	2.00%
Russian Federation	1.06%
Ukraine	1.05%
Albania	0.74%
Bulgaria	0.73%
Others(119 Regions)	6.37%

Table 7 - Top 10 Sources in EMEA

America	Percentage
United States	81.44%
Canada	7.21%
El Salvador	2.87%
Ecuador	2.41%
Brazil	2.10%
Mexico	0.71%
Colombia	0.68%
Argentina	0.48%
Panama	0.37%
Chile	0.28%
Others(44 Regions)	1.45%

Table 8 - Top 10 Sources in Americas

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

ASN(Global)	Network Name	Percentage
4837	CHINA UNICOM China169 Backbone	5.56%
24940	Hetzner Online GmbH	5.50%
4134	Chinanet	4.93%
15897	Vodafone Telekomunikasyon A.S.	3.51%
33387	NOCIX	3.12%
16135	Turkcell Iletisim Hizmetleri A.s.	2.98%
9121	Turk Telekom	2.98%
18450	WEBNX	2.65%
23693	PT. Telekomunikasi Selular	2.64%
4760	HKT Limited	2.59%
	Others(19150 ASNs)	63.54%

Table 9 - Top 10 ASN Attacks Rankings

ASN(APAC)	Network Name	Percentage
4837	CHINA UNICOM China169 Backbone	10.43%
4134	Chinanet	9.25%
23693	PT. Telekomunikasi Selular	4.96%
4760	HKT Limited	4.86%
9381	HKBN Enterprise Solutions HK Limited	3.50%
9269	Hong Kong Broadband Network Ltd.	3.44%
45498	SMART AXIATA Co., Ltd.	2.95%
9808	China Mobile Communications Group Co., Ltd.	2.54%
17976	CAMGSM Company Ltd	2.31%
17408	AboveNet Communications Taiwan	2.05%
	Others(2559 ASNs)	53.71%

Table 10 - Top 10 ASN Rankings in APAC

ASN(EMEA)	Network Name	Percentage
24940	Hetzner Online GmbH	18.94%
415897	Vodafone Telekomunikasyon A.S.	12.10%
16135	Turkcell Iletisim Hizmetleri A.s.	10.27%
9121	Turk Telekom	10.26%
20978	TT Mobil Iletisim Hizmetleri A.S	7.83%
12978	Andromeda Tv Digital Platform Isletmeciligi A.s.	4.08%
34984	Tellcom Iletisim Hizmetleri A.s.	3.48%
47524	Turksat Uydu Haberlesme ve Kablo TV Isletme A.S.	2.55%
8386	Vodafone Net Iletisim Hizmetleri Anonim Sirketi	2.06%
43242	Aydogan Communication LTD.	1.84%
	Others(2610 ASNs)	26.60%

Table 11 - Top 10 ASN Rankings in EMEA

ASN(Americas)	Network Name	Percentage
33387	NOCIX	17.73%
18450	WEBNX	15.06%
174	COGENT-174	5.53%
7922	COMCAST-7922	4.29%
63005	NEXUS-22-63005	3.15%
7018	ATT-INTERNET4	2.53%
32097	WII	2.40%
15169	GOOGLE	2.08%
8075	MICROSOFT-CORP-MSN-AS-BLOCK	2.02%
23033	WOW	1.98%
	Others(2520 ASNs)	43.23%

Table 12 - Top 10 ASN Rankings in Americas

Conclusion

In recent years, attackers have devised numerous ways to magnify DDoS attack size to cause maximum damage to their targets. UDP-based amplification attacks were commonly employed, with memcached attacks clocking amplification factors of up to 51,000, while other attacks through DNS and NTP racked up amplification factors ranging between 51 and 556.9. However, since amplification attacks use amplifiers to reflect attacks, these along with their signatures once identified can be easily blacklisted and dropped. To circumnavigate this, attackers shifted their focus away from amplification attacks by sending high-penetration attack packets across ISP networks to paralyze targeted CSPs with high influxes of traffic. These attack packets were also able to bypass the DDoS mitigation defences of the CSP network.

As 2021 draws to a close, CSPs will need to focus on improving and adopting best industry practices in order to maintain the availability of CSP services when faced with attackers' constantly changing attack strategies. These practices should include deploying advanced protection strategies that respond quickly to a multitude of attacks, as well as regularly testing DDoS defences to confirm they can fully protect networks from attacks.

Furthermore, to minimize the risk of DDoS attacks, the ideal solution is to drop all attack traffic coming from ISPs well before it is allowed to reach the targeted CSP network. Whether or not an ISP forwards traffic to a CSP, the CSP will eventually be impacted if large volumes of traffic are not prevented from reaching a certain level.

For ISPs, internal botnets, bots, and amplifiers are difficult to avoid - to limit the risk of DDoS from these sources, ISPs must shore up the security policies of outgoing traffic, so that attacks can be detected at the source and stopped as early as possible to significantly weaken the power of an attack. ISPs can also set up DDoS filtering policies for better DDoS prevention and incident response through BGP FlowSpec. Routes configured automatically or manually can be converted into firewall filters which block attacks more effectively.

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 the quarterly Threat Report produced by Nexusguard's research team:

- Tony Miu, Editor, Research Direction, Threat Analysis and Content Development
- Ricky Yeung, Research Engineer, Data Mining & Data Analysis
- Kitson Cheung, Technical Writing

20220106-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 communications 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

Copyright 2021 Nexusguard Limited. All rights reserved.