NEXUSGUARD®

Threat Report

Distributed Denial of Service (DDoS)

Q2 2020

Contents

NEXUSGUARD®

Q2 2020 Threat Report

Key Observations

Total Attacks

vs. Q1 2020	38.76% ▲
vs. Q2 2019	515.15% ▲

Attack Sizes

Maximum			Average		
147.84 Gbps	vs. Q1 2020	16.14% ▼	1.52 Gbps	vs. Q1 2020	9.94% ▲
	vs. Q2 2019	25.39% ▲		vs. Q2 2019	56.41% ▲

Top 5 DDoS Attack Types

	Bit and Piece	DNS Amplification	CLDAP	Application	Amplification
vs. Q1 2020	569.50% ▲	65.05% ▲	35.58% ▲	132.51% ▲	43.00% ▲
vs. Q2 2019	310.43% ▲	3164.67% ▲	338.09% ▲	6.18% ▲	51.81% ▲

About this report

Cyber warfare is not a new concept, it's just a new medium. It's a kind of military operation targeting enemy infrastructure and communications, which involves cleverly thought out strategies to outwit the opponent, and firepower to improve the chances of successfully taking down the targets.

Resembling real-life military operations where a cover-up is put into place to conceal the real target, a large UDP-based attack is employed as a smokescreen to distract in-house security teams from other attacks that are taking place. The tactics behind the operation are Bit-and-Piece attacks which play a major role in contaminating IP pools across numerous IP prefixes with negligible sized junk traffic, while attacks are unleashed in the form of amplification and different types of UDP-based attacks.

In this report, we're going to discuss how bit-and-piece attacks have continued to evolve, and are able to successfully evade DDoS mitigation schemes when blended with multiple attack vectors, and the challenges that these advanced attack tactics present to the cybersecurity world.

We will also explore novel deep-learning based solutions for identifying and predicting complex attack patterns.

Nexusguard recorded a 515.15% YoY and 38.76% QoQ increase in DDoS attacks in Q2 2020. This increase is a continuation of the increasing trend set in Q1 2020. Unlike in Q1 2020 in which over 85.45% of attacks were UDP attacks, 67.16% of UDP attacks this quarter were launched with bit-and-piece attacks, designed to cause maximum damage to target networks.

UDP-based attacks were designed specifically to bypass the volumetric DDoS protection mechanisms of CSPs. In some attack cases, perpetrators targeted 256 IP addresses in the same /24 prefix, non-stop for an entire month. Bit-and-piece attacks, the main impetus behind the recent spate of attacks also saw a 569.5% QoQ and 310.43% YoY increase.

Bit-and-piece attacks are taken to a whole new level through blending multiple attacks

Q2 2020 has seen a shift in tactics with attackers opting for a more deceptive and sophisticated approach, by utilizing a more elaborate practise of bit-and-piece attacks to launch amplification and different types of UDP-based attacks to flood target networks with traffic. The attack tactics and strategies that lend themselves to successfully bypass detection and mitigation are discussed below.

Bit-and-Piece attacks become ever more complex and deceptive

Based on our findings this quarter, smaller and more complex UDP-based and other amplification attacks were often used to maximize the impact of collateral damage on target networks. Bit-and-piece attacks result from injecting doses of junk traffic of negligible size into a large pool of IP addresses across hundreds of IP prefixes, which eventually paralyze the target when the junk traffic starts to accumulate from different IPs.

Figure 1. Summary of Bit-and-Piece Attacks

Interestingly, for every wave of bit-and-piece attack, a random target would be selected to receive a large flood attack, namely a UDP-based attack or amplification attack, in the size range of 300Mbps to 21Gbps. We believe that this acts as a smokescreen to distract in-house security teams from bit-and-piece attacks that are taking place, designed to ultimately take down CSP infrastructures.

In some cases, attacks covered 256 IP addresses in the same IP prefix /24. Perpetrators also spoofed network address (.0) and network broadcast address (.255), with the intent of causing a broadcast storm effect to victim networks.

During this quarter, a total of 112 ASNs were impacted by bit-and-piece attacks. The total number of IP prefixes (Class C) attacked was 1,888.

Targeted ASNs
112

Total No. of IP Prefixes (Class C) Under Attack
1,888

	Minimum	Maximum
No. of Targeted IP Address per IP Prefix /24	10	256
Attack Duration (Minutes)	0.08	5,730.00
Attack Size by IP (Gbps)	0.0003	21.64
Attack Size by IP Prefix /24 (Gbps)	0.0004	103.62
Average Attack Size(Gbps) per IP Prefix /24	0.0200	2.00
Attack Counts per IP	40	5,204,092
Attack Counts per IP Prefix /24	223	5,209,145

Table 1. Summary of Bit-and-Piece Attacks

Harnessing power through blending multiple attack vectors

• UDP-based attacks

In the past, attackers have utilized bit-and-piece attacks with a single attack vector such as a UDP amplification attack to launch UDP-based attacks. However, in this quarter, there has been a tendency to employ a blend of attack vectors to launch a wider range of UDP-based attacks. The combined effect of this tactic is to increase the level of difficulty for CSPs to detect and differentiate between attack and legitimate traffic. Table 2 illustrates the types of attack vectors employed this quarter.

Distribution of Attack Vectors	Targeted Geo-locations
• UDP Attack (44.57%) • DNS Amplification Attack(35.68%) • UDP Fragmentation Attack(6.8%) • CLDAP Reflection Attack(6.24%) • SSDP Amplification Attack(3.87%) • CHARGEN Attack(2.19%), • DNS Attack(0.56%), • IP BOGONS(0.05%), • SIP Flood(0.05%)	Argentina, Bangladesh, Brazil, Canada, China, Hong Kong, Islamic Republic of Iran, Japan, Lebanon, Netherlands, Poland, Romania, Russian Federation, Singapore, South Africa, Taiwan, Turkey, Ukraine, United States

Table 2. Summary of Attack Vectors

As shown in Table 2, 44.57% of attacks were attributed to UDP attacks, though in previous studies and instances of bit-and-piece attacks, they were not common.

We found that UDP-based attacks were characterized in the 4Mbps to 21.64Gbps size range, which is smaller than previously observed. Given their attributes: neither requiring payload, fixed source and destination ports, nor fixed source and destination IPs, UDP-based attacks are still widely adopted. Though smaller in size now, these types of UDP-based attacks can be enlarged by randomly crafting payloads for the purpose of congesting target networks.

Due to the complexity and variety of online applications, organizations need to customize and develop their own protocols to meet their technical needs. As CSPs serve as the nexus across different networks, malicious traffic can be randomly sent to a number of ports instead of just one, greatly hindering the application of CSPs' filtering policies. Furthermore, the unit of magnitude used for threshold-based detection is Gbps, meaning that a few Mbps of UDP traffic would easily go undetected.

- ## Amplification attacks

In this quarter, DNS amplification attacks accounted for 35.68% of bit-and-piece attacks. Despite an amplification factor of 179X, the maximum attack size we recorded was a mere 672Mbps during a wave of the bit-and-piece attacks, indicating that perpetrators are now able to optimize the attack size, in order to maximize the full force of bit-and-piece attacks to cause significant impact to target networks.

Since legitimate DNS response traffic is seen as the same as DNS amplification traffic, albeit different in volume and source, CSPs have to ensure that attack traffic is mitigated, and that legitimate DNS response traffic is allowed to pass to prevent service outage to CSP end users.

Over the last two years we have learned that distributed attacks makes mitigation all the more difficult, therefore it's imperative to ensure that black/white lists are kept up-to-date to help identify attack patterns, and minimize serious impact on CSPs.

Traditional threshold-based detection and mitigation is no longer reliable nor effective

According to our attack analysis, there has been an obvious decrease in attack size, with perpetrators opting to employ small-sized attack traffic to attack more IP prefixes /24. This seriously undermines traditional threshold-based detection and mitigation, given that CSPs now need to detect and identify smaller and more complex attack traffic patterns amongst large volumes of legitimate traffic.

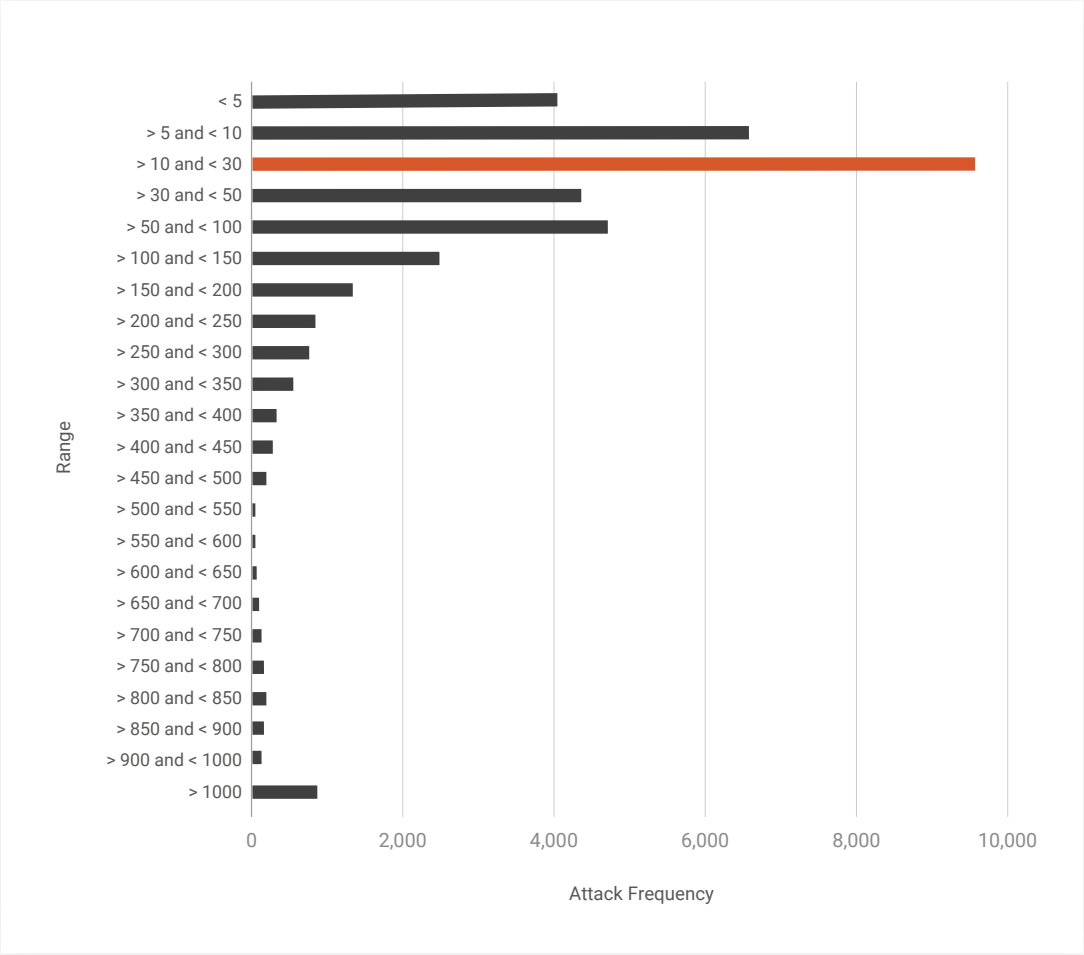
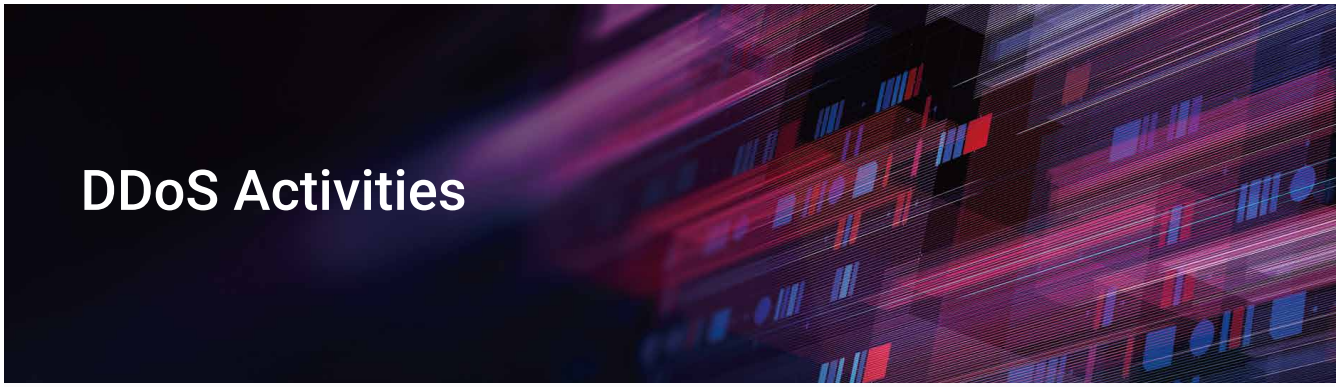


Figure 2. Attack Size Distribution per IP

As can be seen in Fig 2, 51.57% of attacks were smaller than 30Mbps. In addition, 4,080 attacks were smaller than 5Mbps, 6,527 attacks were between 5Mbps and 10Mbps, and 9,637 attacks were between 10Mbps and 30Mbps. Attacks larger than 300Mbps, constituting 11.28% of this quarter's total, were used as smokescreens to distract in-house security staff from bit-and piece attacks, employed to cause havoc to target networks.

Since typical threshold based detection and mitigation solutions are unable to pinpoint the exact attack and subsequently apply surgical mitigation, perpetrators have learned how to exploit this weakness, using volumes of attack traffic often smaller than 30Mbps to force CSPs to subject entire networks of traffic of several Gbps to mitigation. If the mitigation was through an on-site appliance, the capacity of the appliance could be a potential bottleneck. If the mitigation was through a third party cloud service, then there would be performance impacts as the traffic would see increased latencies due to the additional hops.

It's only by using 'deep learning-based' predictive methods to analyze large amounts of CSP traffic data, that malicious attack patterns can be quickly identified and surgically mitigated, before any lasting damage is inflicted.



DDoS Activities

Types of Attack Vectors[1]

UDP and DNS Amplification attacks were in the predominance of vectors, representing 66.76% and 12.43%, respectively. UDP attack increased 23.52% QoQ while drastically climbing by 17775.68% YoY. DNS Amplification Attack surged by 64.51% QoQ and increased 15.95% YoY. CLDAP Reflection Attack was ranked third with 6.26%, showing the increases of 65.05% QoQ and 3164.67% YoY.

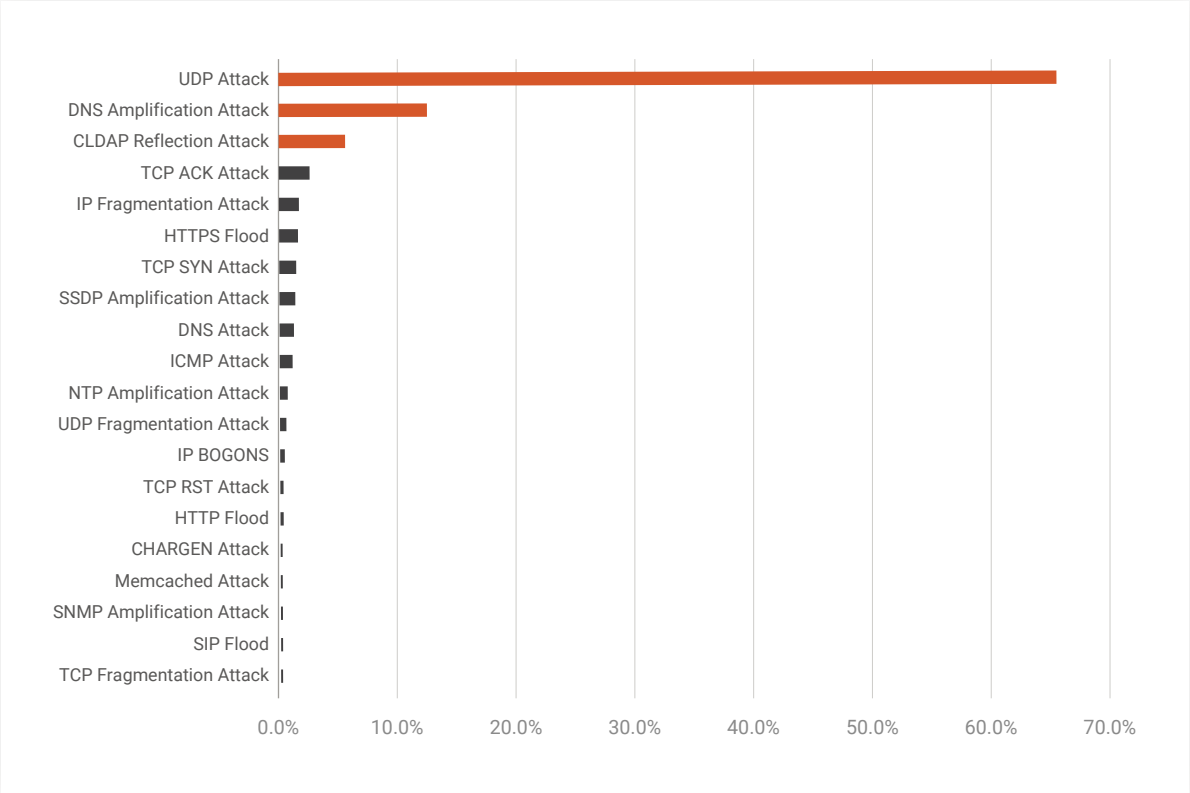


Figure 3. Distribution of DDoS Attack Vectors

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

66.76 %

52,197

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 DNS Amplification Attack

12.43 %

9,719

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 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 CLDAP Reflection Attack

6.26 %

4,897

A Connectionless Lightweight Directory Access Protocol (CLDAP) attack is abuse LDAP queries over UDP, Attacker sends an CLDAP request to a publicly accessible LDAP server with a spoofed victim IP address. The Server responds with a larger response to the victim's IP. 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 70.

Quantity of Attack Vectors

The dominant attack vector was single with 88.42% while the multi-vectors shared the rest with 11.58%. The 2nd and 3rd vectored attacks contributed 8.56% and 1.76%, respectively. The maximum attack vector was 11.

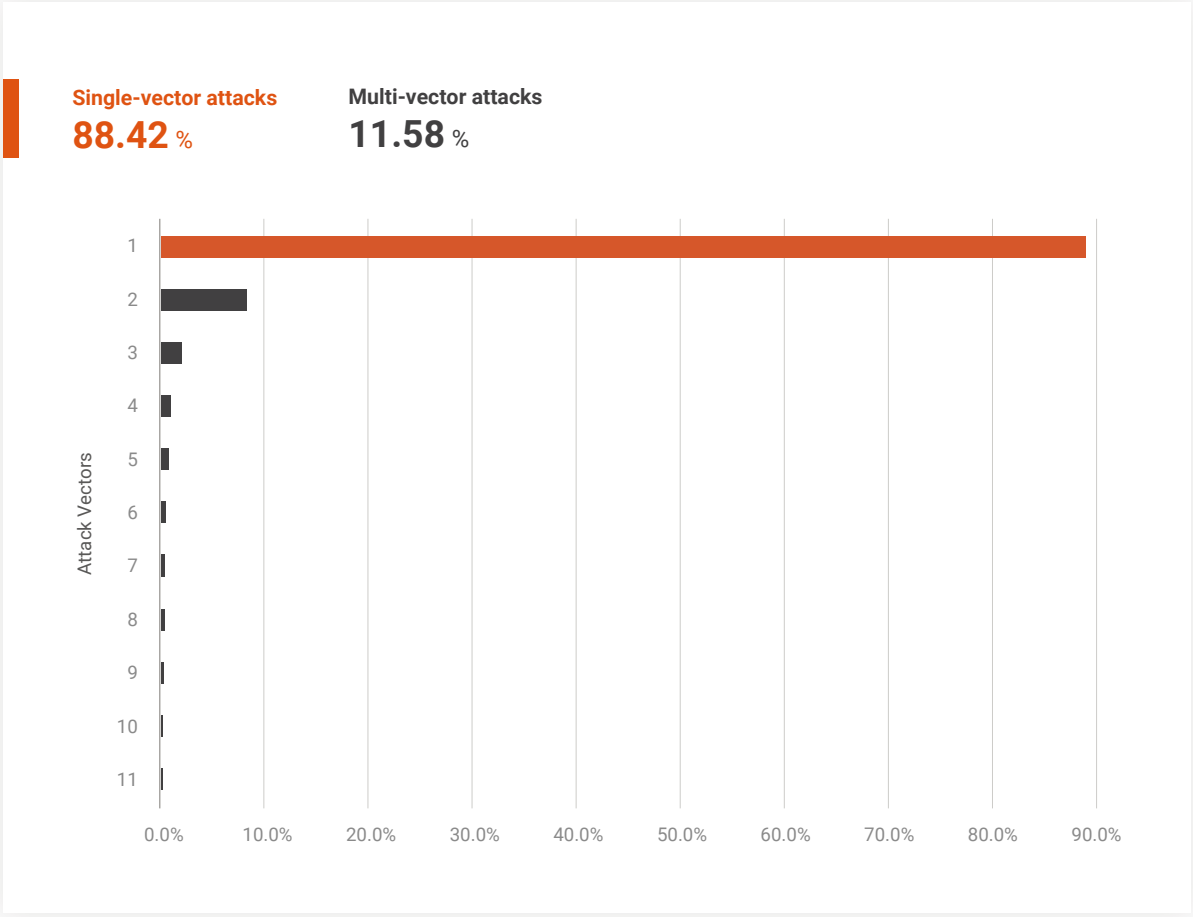


Figure 4. Quantity of DDoS Attack Vectors

Attack Durations[2]

78.89% of the total attacks lasted fewer than 90 minutes, the rest of which was longer than 90 minutes. 1.24% of attacks are longer than 1200 minutes. The quarterly duration averaged 137.57 minutes, while the longest attack lasted 63,756.77 minutes. QoQ, both the maximum and average duration increased by 222.48% and increased by 188.46%. YoY, the maximum duration increased by 57.85% while the average duration significantly dropped by 24.79%.

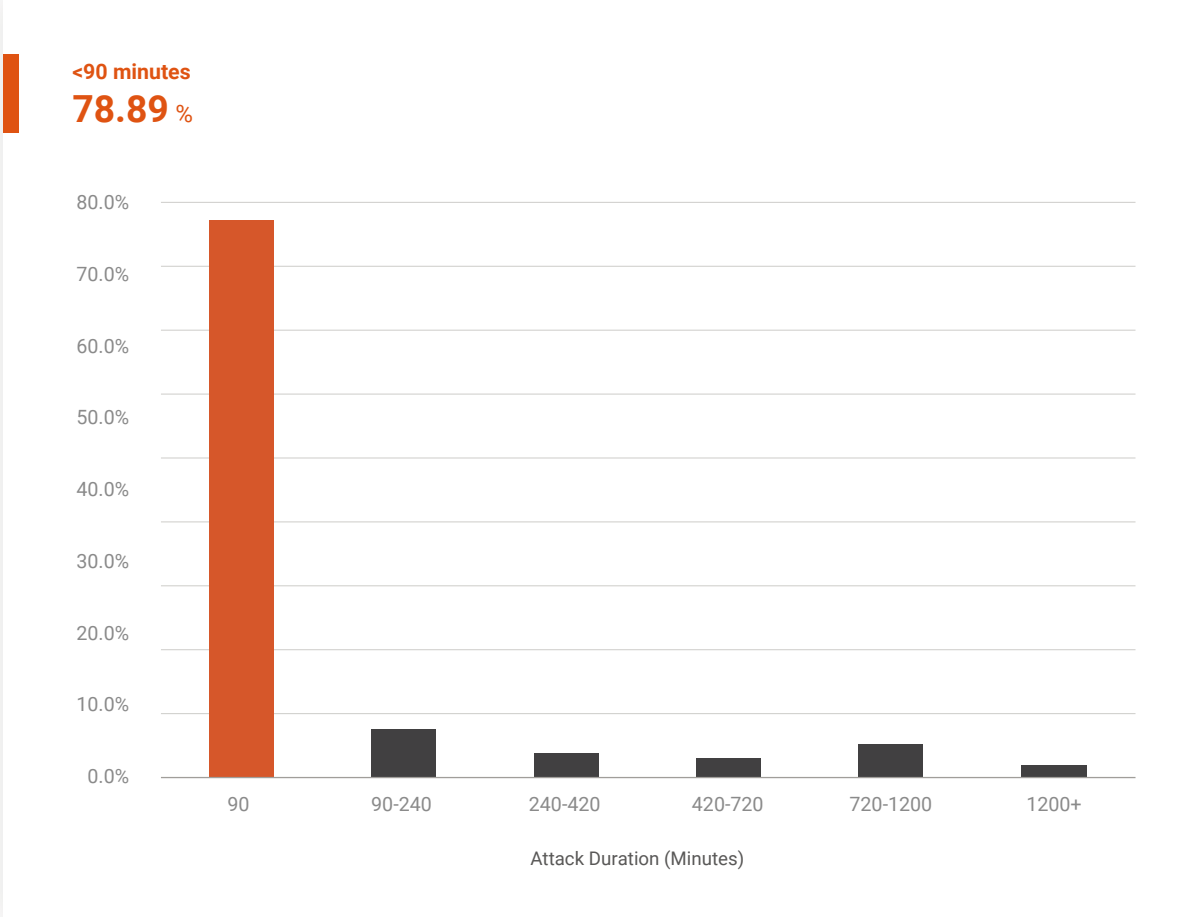


Figure 5. Percentage of Attack Duration

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, 84.67% of attacks were smaller than 1Gbps and 97.07% smaller than 10Gbps. Those ranging between 1Gbps and 10Gbps accounted for 12.20%. The maximum size decreased by 16.14% QoQ and increased by 25.39% YoY, and so did the average size increased by 9.94% QoQ and increased by 56.41% YoY, respectively.

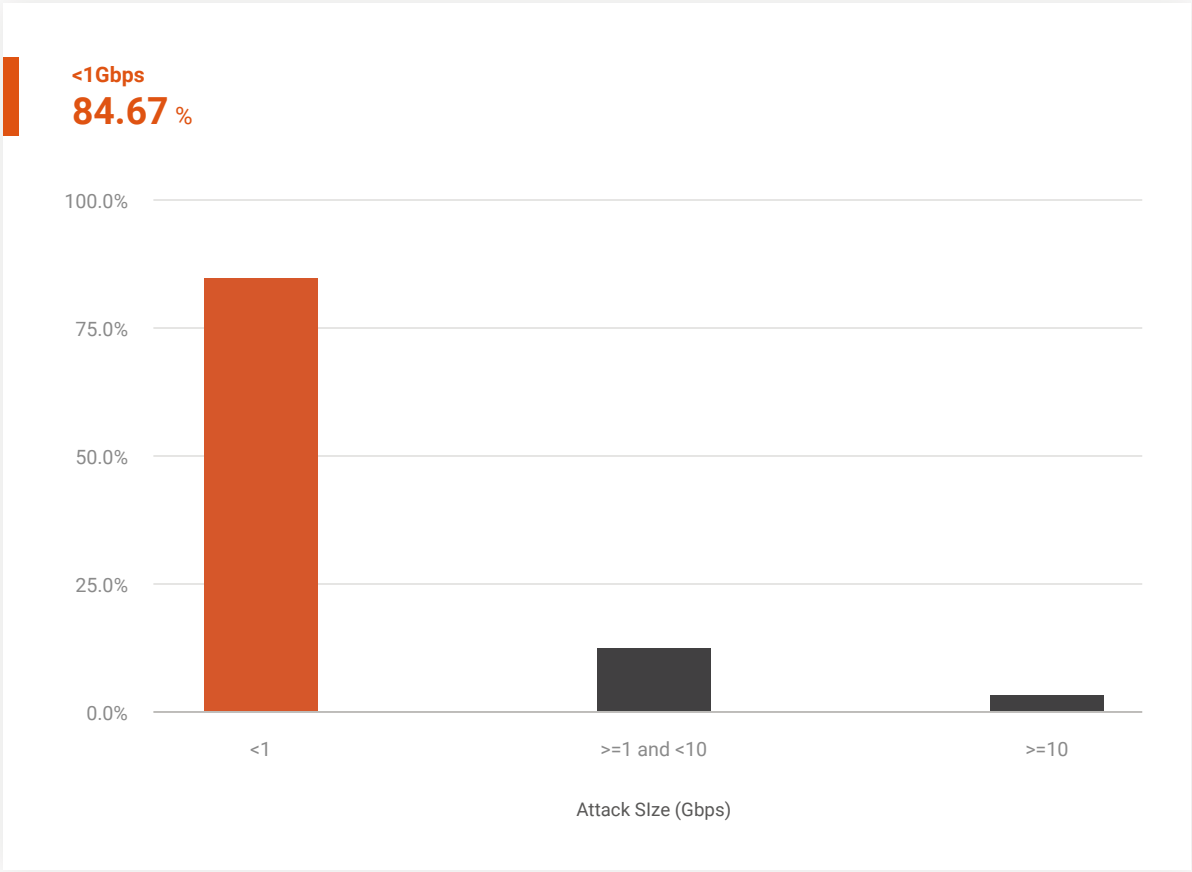


Figure 6. Percentage of Attack Sizes

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.

Source Distribution of Application Attack[4]

Devices	OS	Percentage
Computers and Servers	Windows OS	85.55%
	Other OS	2.53%
	Macintosh OS	1.19%
Mobile	iOS	8.48%
	Android	2.25%
	Other OS (BlackBerry, DoCoMo)	Less than 0.01%
Others (including IoT)	Other OS e.g. PSP, Nintendo Wii, Nintendo DS	Less than 0.01%

Table 3. 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 — Global & Regional

Global	%
China	72.43%
Brazil	5.18%
Indonesia	2.93%
United States	2.72%
Thailand	2.29%
Taiwan	1.81%
Russian Federation	1.51%
France	0.96%
Malaysia	0.93%
India	0.69%
Others (43 Regions)	8.55%

Table 4. Top 10 Sources Ranking

APAC	%
China	85.96%
Indonesia	3.48%
Thailand	2.72%
Taiwan	2.15%
Malaysia	1.10%
India	0.81%
Vietnam	0.65%
Pakistan	0.60%
Philippines	0.57%
Bangladesh	0.48%
Others (6 Regions)	1.48%

Table 5. Top 10 Sources in APAC

EMEA	%
Russian Federation	21.67%
France	13.79%
Turkey	9.35%
United Kingdom	8.63%
Ukraine	7.29%
Germany	4.74%
Sweden	4.15%
South Africa	3.73%
Netherlands	3.35%
Poland	3.02%
Others(19 Regions)	20.28%

Table 6. Top 10 Sources in EMEA

The Americas	%
Brazil	59.09%
United States	30.98%
Mexico	3.43%
Argentina	2.50%
Canada	2.03%
Peru	1.03%
Paraguay	0.57%
Curaçao	0.37%

Table 7. Top 8 Sources in Americas

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

ASN (Global)	Network Name	%
AS4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	27.23%
AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN	9.36%
AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	7.14%
AS24444	CMNET-V4SHANDONG-AS-AP Shandong Mobile Communication Company Limited, CN	6.17%
AS56040	CMNET-GUANGDONG-AP China Mobile communications corporation, CN	3.36%
AS56041	CMNET-ZHEJIANG-AP China Mobile communications corporation, CN	3.30%
AS24445	CMNET-V4HENAN-AS-AP Henan Mobile Communications Co.,Ltd, CN	2.07%
AS56046	CMNET-JIANGSU-AP China Mobile communications corporation, CN	1.91%
AS24547	CMNET-V4HEBEI-AS-AP Hebei Mobile Communication Company Limited, CN	1.73%
AS7713	TELKOMNET-AS-AP PT Telekomunikasi Indonesia, ID	1.04%
Others	2798 Regions	36.70%

Table 8. Top Ten ASN Attacks Rankings

ASN (APAC)	Network Name	%
AS4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	32.95%
AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN	11.32%
AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	8.64%
AS24444	CMNET-V4SHANDONG-AS-AP Shandong Mobile Communication Company Limited, CN	7.47%
AS56040	CMNET-GUANGDONG-AP China Mobile communications corporation, CN	4.06%
AS56041	CMNET-ZHEJIANG-AP China Mobile communications corporation, CN	3.99%
AS24445	CMNET-V4HENAN-AS-AP Henan Mobile Communications Co.,Ltd, CN	2.50%
AS56046	CMNET-JIANGSU-AP China Mobile communications corporation, CN	2.32%
AS24547	CMNET-V4HEBEI-AS-AP Hebei Mobile Communication Company Limited, CN	2.09%
AS7713	TELKOMNET-AS-AP PT Telekomunikasi Indonesia, ID	1.25%
Others	687 Regions	23.41%

Table 9. Top Ten ASN Rankings in APAC

ASN (EMEA)	Network Name	%
AS12876	Online SAS, FR	11.31%
AS9121	FRANCISCO WESLEY GOMES FERREIRA -ME, BR	4.51%
AS45011	SE-A3 http://www.a3.se/, SE	2.32%
AS13285	VIETTEL-AS-VN Viettel Corporation, VN	2.12%
AS16276	OVH, FR	1.56%
AS29695	ALTIBOX_AS Norway, NO	1.35%
AS12389	ROSTELECOM-AS, RU	1.32%
AS9105	SAKURA-A SAKURA Internet Inc., JP	1.28%
AS24940	TRIOLAN, UA	1.14%
AS48430	FIRSTDC-AS, RU	1.11%
Others	960 Regions	71.97%

Table 10. Top Ten ASN Rankings in EMEA

ASN (AMERICAS)	Network Name	%
AS28573	CLARO S.A., BR	2.44%
AS54994	QUANTILNETWORKS, US	1.91%
AS15169	GOOGLE, US	1.40%
AS396253	IBOSS-8-ASN, US	1.24%
AS20473	AS-CHOOPA, US	1.12%
AS209	Redenilf Servicos de Telecomunicacoes Ltda, BR	1.10%
AS7922	COMCAST-7922, US	0.93%
AS28210	PEICITY-AS-TW Peicity Digital Cable Television., LTD, TW	0.50%
AS18881	CHINATELECOM-HLJ-AS-AP asn for Heilongjiang Provincial Net of CT, CN	0.47%
AS14061	PUNTONET S.A., EC	0.47%
Others	1131 Regions	88.42%

Table 11. Top Ten ASN Rankings in Americas

Conclusion

During the last two years, we observed that typically for every wave of bit-and-piece attacks, the attack duration to every IP prefix /24 was almost the same, and usually lasted for around one minute. However, the longest wave that we recorded recently lasted for almost 4 days. Attackers have been implementing specially customized attack patterns to launch waves of 10-15 minute bit-and-piece attacks, every 30 minutes, every day, that last for a whole month. By doing this, the botnet's integrity is preserved and can be used for a longer period of time. This is an observation, not so much a difference in the bit-and-piece attacks; attackers have craftily optimized their attack resources so that a much longer attack can be sustained. Moreover, the adoption of various tactics to ramp up attacks shows that perpetrators have revised their battlefield tactics and rewritten their cyberattack playbooks.

Detecting and mitigating small-sized attack traffic has become an uphill struggle at CSP level, in comparison to the traditional volumetric attack on a small number of targeted IPs, especially since bit-and-piece attack traffic does not match any consistent patterns and has become ever more complex, making identification an extremely difficult task.

Deploying deep-learning methods would be an effective solution for mitigating the impact of increasingly complex bit-and-piece attacks. Nexusguard's Smart Mode detection applies Machine Learning techniques to predict whether network traffic coming from a source is legitimate or part of a malicious DDoS attack. Compared to traditional threshold-based detection methods, Nexusguard's novel AI-driven Smart Mode is able to identify more complex traffic patterns with improved speed and accuracy, making it an ideal solution for protecting CSP networks and infrastructures.

To combat these new and evolving generations of attacks requires organizations to respond in kind and consistently rethink their cyber defence playbook. Just like attackers would deploy all tools at their disposal to achieve an end, organizations should also ensure their defence strategy encompasses not just any part of their assets and always assert that the worst possible scenarios will happen. The mistaken belief that there exists a single foolproof strategy or solution will only bring about catastrophic outcomes that others in the industry will learn from as case studies on exactly what not to do.

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
- Dominic Li, Technical Writing

20200918-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