NEXUSGUARD®

Threat Report

Distributed Denial of Service (DDoS)

Q1 2020

Contents

NEXUSGUARD®

Q1 2020 Threat Report

Key Observations

Total Attacks

vs. Q1 2019	278.17% ▲
vs. Q4 2019	542.46% ▲

Attack Sizes

Maximum			Average		
176.29 Gbps	vs. Q1 2019	21.25% ▲	1.385 Gbps	vs. Q1 2019	68.20% ▲
	vs. Q4 2019	11.85% ▼		vs. Q4 2019	4.11% ▼

Top 5 DDoS Attack Types

	UDP	DNS Amplification	CLDAP	Application	Amplification
vs. Q1 2019	5777.47% ▲	7.66% ▼	3390.59% ▲	65.59% ▼	10.68% ▼
vs. Q4 2019	10438.40% ▲	32.17% ▲	2572.97% ▲	26.21% ▲	87.02% ▲

Quarterly Focus

In March and April, we recorded the most unusual increase in DDoS attacks ever. Compared with 2019 Q1, YoY, the number of attacks increased by 278.17%, and QoQ increased by 542.46%. Q1 is generally considered the “off season” for DDoS attacks and hence it is rather unusual to observe such behaviour during this period. While it is a surprising observation, we believe that the occurrence of such spikes could be related to the COVID-19 pandemic.

DDoS attacks have increased significantly amid the COVID-19 pandemic

On March 15, the U.S. Department of Health and Human Services was hit by DDoS attacks which severely impacted its online services. On April 30, the European Union’s High Representative, Josep Borrell, singled out attacks on “critical infrastructures that are essential to managing this crisis” as particularly egregious in a press release. He also noted the proliferation of “malware distribution campaigns, scanning activities and distributed denial-of-service (DDoS) attacks” since the outbreak. Virtual private network (VPN) provider Atlas also recorded more than 175,000 DDoS attacks targeted at the US within a month.

Whatever the motives behind DDoS attacks, DDoS attacks impact everyone

DDoS Attacks have already become a global risk around the world. The motives behind attacks can be categorized into three types. The first type is politically motivated, while the second type is commonly instigated as a form of retaliatory attack by dismissed employees or someone dissatisfied with society during times of economic recession. The last type is always active, namely associated with online crime and competition between rival industries.

ISPs have become the major focal point of attack

The spread of the COVID-19 pandemic has had a profound impact on our everyday lives in many ways. Due to social distancing measures and in an effort to curb the spread of the virus, working from home has become the new norm and home internet connectivity has never been more important. The heavy use and reliance of online services has given rise to a trend of attacks which have been employed to overwhelm ISPs.

There's more to ISP traffic patterns than meets the eye

In addition to the traditional DDoS attacks, we identified various abnormal traffic patterns from ISPs such as traffic generated from infected devices and abnormal traffic generated by exploiting open resolvers (DNS, DLAP, etc) to produce a small-sized and short period of attack. We do not dismiss such abnormal traffic from ISPs as its impact could pose a greater threat than that produced by say a 57 Gbps DDoS attack for 2 hours.

Analyzing the ISP traffic, we found that attacks larger than 5Gbps only accounted for 0.99%, namely those which were detectable and long-lasting. Detection of a DDoS attack sized at 57 Gbps for example would instantly be scrubbed at our scrubbing centres and prevented from heading to customers' networks.

Small but deadly: An invisible killer

As can be seen in Figure 1, 67.12% of the attacks are characterized in the size range of 1Gbps and 5Gbps which from our experience often last less than 15 mins and create less than 200 events per day. We dub this proportion of attacks an "invisible killer". Since this type of attack occurs almost on a day-to-day basis and often does not provide detrimental service degradation to the customer or ISP, it is often overlooked. Due to the lack of size concentration and being overlooked as insignificant relative to overall traffic, it normalizes historical traffic behaviour and gives the invisible killer access to the networks of websites and onlines services to cause havoc. If too intensive however, it would not only be powerful enough to exert an adverse effect on the ISP's network, but also impair connectivity of customer networks. In other words, overlooking it, despite being negligible in size, may lead to a bottleneck that not only cripples the ISP's network but also slows down or even shuts down the downstream customers' networks.

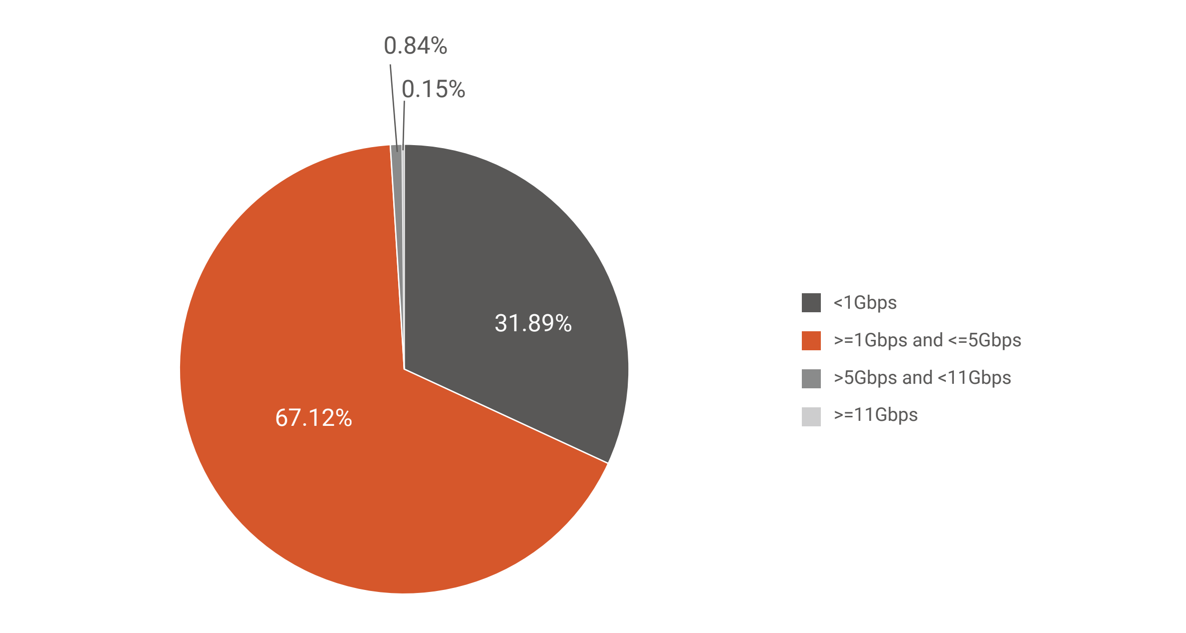

Figure 1. Distribution of event count by attack size. Q1 2020

We believe that this is not an isolated case but an ongoing trend. And as such, these attacks at ISP level can no longer be dismissed because the ISP's network infrastructure would suffer a deluge of attacks if not dealt with properly. It is therefore imperative that ISPs take the initiative to address any malicious or suspicious traffic irrespective of size or quantity to protect their networks against DDoS attacks.

Another observation is that 31.89% of traffic less than 1Gbps was not being utilized as direct attacks and instead it was being harnessed to launch reflected attacks. In fact, most of them are targeted at open resolvers. For ISP's in this scenario, their size is so small that they may not be headed off until they are manifested as reflected attacks resulting in saturation of bandwidth. After reflection, ongoing traffic in the case of DNS amplification attacks can be amplified by 28 to 54 times, whereas for Memcached amplification attacks, traffic can be can be amplified by 10,000 to 51,000 times.

Botnet Activities

Delving into the source IPs, we also observed that the attack traffic originated from DVR Bots because some traffic had NATed IPs signifying that these are fixed IPs. Some of them emanated from 3876 DVRs. Since we run our own IP reputation database, any traffic with suspicious IPs are closely monitored including those originating from IoT botnets such as open resolvers, home routers, etc.

Rankings	Region	Count	Percentage
1	Taiwan	1,428	36.84%
2	Vietnam	820	21.16%
3	South Korea	457	11.79%
4	United States	312	8.05%
5	Italy	147	3.79%
6	Malaysia	92	2.37%
7	United Kingdom	84	2.17%
8	Greece	83	2.14%
9	Romania	58	1.50%
10	Israel	46	1.19%
11	Other(49 Regions)	349	9.00%

Table 1. Sources of Botnets, Q1 2020

As with the above-mentioned case, by monitoring traffic with 9791 active IPs, we discovered that most IoT botnets built in Jan 2019 are based on Bz. Similarly, running the IP reputation database can facilitate in dropping most of the attack traffic. Moreover, the abundance of DDoS-for-hire services has made it easy for anyone to launch deadly attacks via online services and websites. As hackers span from country to country, it is becoming increasingly difficult for law enforcement authorities to keep track of them thus enabling them to continue their malpractice below the radar.

Follow-up on Bits-and-Pieces Attacks

Bits-and-Pieces Attacks

ASN-level CSPs around the world, especially ISPs, continue to be impacted by the stealthy, sophisticated bits-and-pieces 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 110 ASNs were impacted by bits-and-pieces attacks. The total number of IP prefixes (Class C) attacked was 528.

Targeted ASNs
110

Total No. of IP Prefixes (Class C) Under Attack
528

Attack Types

- DNS Amplification Attack (91.86%)
- SSDP Amplification Attack (4.73%)
- NTP Amplification Attack (2.65%)
- CHARGEN Attack (0.76%)

Targeted Geo-locations

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

Category	Minimum	Maximum
No. of Targeted IP Addresses per IP Prefix /24	5	40
Attack Durations (Minutes)	0.02	1,433.85
Attack Count per IP	40	70,442
Attack Count per IP Prefix	222	178,209

Table 2. Information about Attack Traffic with “Bit and Piece” Pattern, Q1 2020

Source Distribution of Application Attack[1]

MacOS devices contributed to about 0.46% of all application attack traffic, whereas Windows-powered PCs and notebooks contributed to about 85.42%. Mobile iOS devices such as iPads and iPhones made up about 5.82% of all application attack traffic, whereas android devices accounted for about 5.02%.

Devices	OS	Percentage
Computers & Servers	Windows OS	85.42%
	Other OS	3.07%
	Macintosh OS	0.46%
Mobile	iOS	5.82%
	Android	5.02%
	Other OS (BlackBerry, DoCoMo)	< 0.01%
Others (including IoT)	Other OS e.g. PSP, Nintendo Wii, Nintendo DS	< 0.01%

Table 3. Distribution of OS and Device Types as Sources of Application Attacks, Q1 2020

[1] 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.

DDoS Activities

Types of Attack Vectors[2]

UDP and DNS Amplification attacks were in the predominance of vectors, representing 75.00% and 10.49%, respectively. UDP attack increased 10438.40% QoQ while drastically climbing by 5777.47% YoY. DNS Amplification Attack surged by 32.17% QoQ and decreased 7.66% YoY. CLDAP Reflection attack was ranked third with 5.27%, showing the increases of 2572.97% QoQ and 3390.59% YoY.

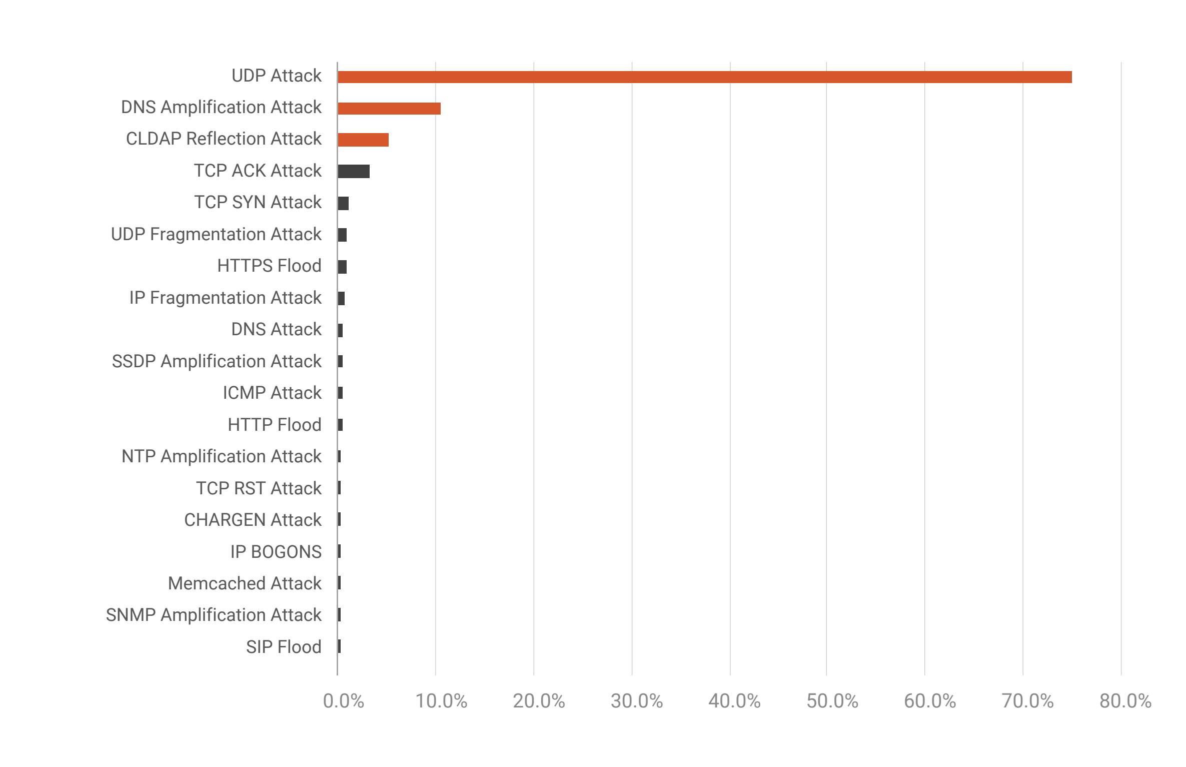

Figure 2. Distribution of DDoS Attack Vectors, Q1 2020

[2] 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

75.00 %

42,259

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

10.49 %

5,908

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

5.27 %

2,967

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 91.88% while the multi-vectors shared the rest of 8.12%. The 2nd and 3rd vectored attacks contributed 6.67% and 0.74%, respectively. The maximum attack vector was 8.

Single-vector attacks

91.88 %

Multi-vector attacks

8.12 %

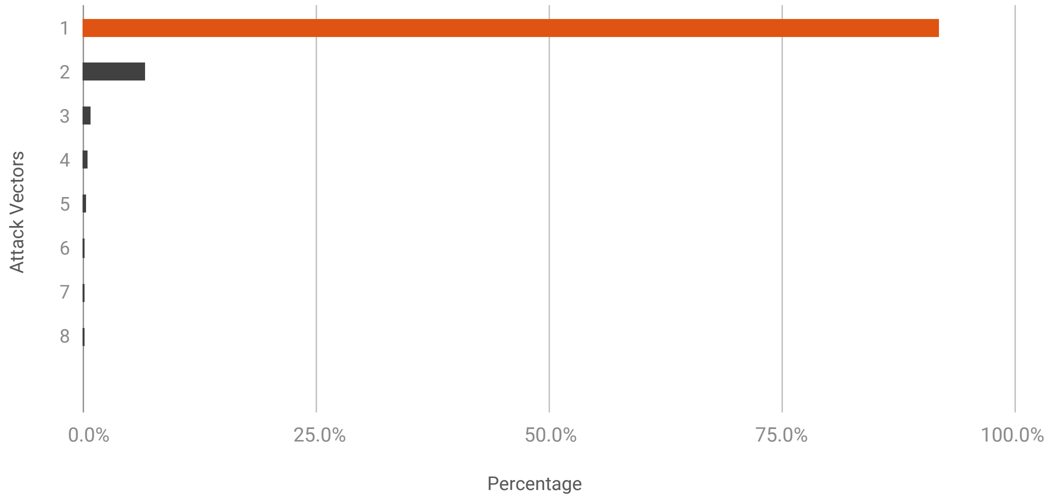

Figure 3. Distribution of DDoS Attack Vectors, Q1 2020

Attack Durations[3]

96.78% of the total attacks lasted fewer than 90 minutes, the rest of which was longer than 90 minutes. 0.19% of attacks are longer than 1200 minutes. The quarterly duration averaged 47.69 minutes, while the longest attack lasted 13 days 17 Hours and 18 minutes. QoQ, both the maximum and average duration increased by 173.91% and dropped by 63.76%. YoY, the maximum duration dropped by 58.44% while the average duration significantly dropped by 91.02%.

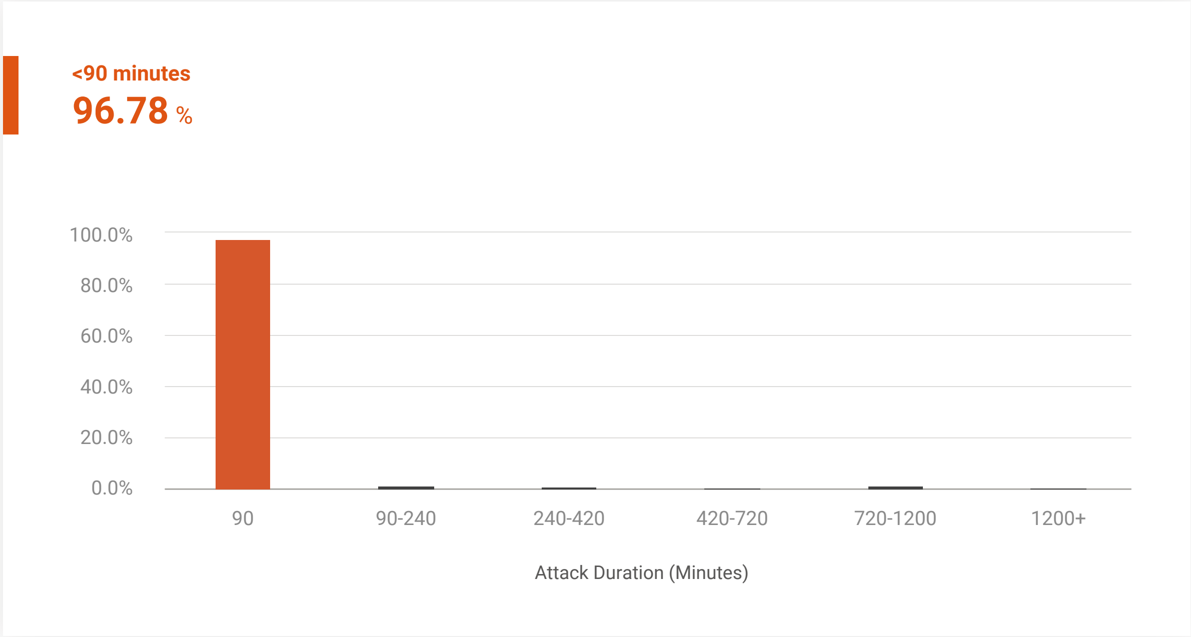

Figure 4. Percentage of Attack Duration, Q1 2020

[3] 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[4]

During the quarter, 38.42% of attacks were smaller than 1Gbps and 99.43% smaller than 10Gbps. Those ranging between 1Gbps and 10Gbps accounted for 61.45%. The maximum size decreased by 11.85% QoQ and increased by 21.25% YoY, and so did the average size decreased by 4.11% QoQ and increased by 68.20% YoY, respectively.

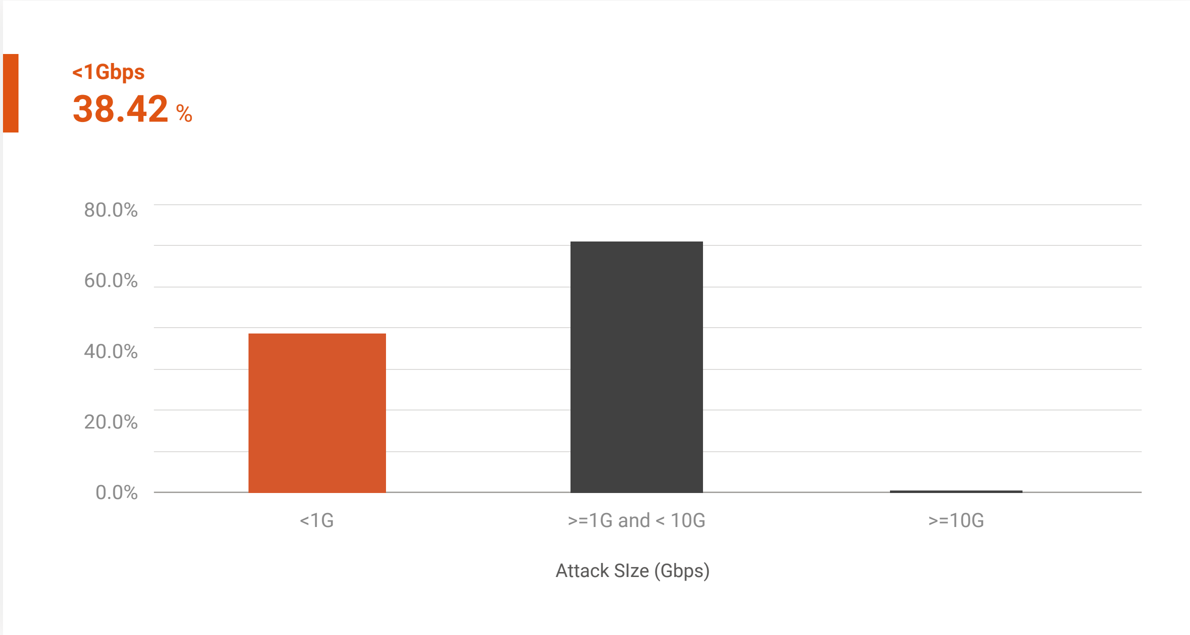

Figure 5. Attack Size Distribution, Q1 2020

[4] 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.

Attack Source Distribution — Global & Regional

Global	Percentage
China	53.63%
United States	13.62%
Russian Federation	8.58%
Taiwan	7.76%
Netherlands	3.26%
Brazil	2.50%
Germany	1.53%
Vietnam	1.04%
South Korea	0.91%
Indonesia	0.87%
Other (117 Regions)	2.76%

Table 4. Top 10 Global Attack Sources, Q1 2020

APAC	Percentage
China	81.52%
Taiwan	11.79%
Vietnam	1.59%
South Korea	1.38%
Indonesia	1.32%
Australia	0.63%
Thailand	0.47%
India	0.40%
Singapore	0.28%
Bangladesh	0.16%
Other (15 Regions)	0.17%

Table 5. Top 10 Sources in APAC, Q1 2020

EMEA	Percentage
Russian Federation	50.45%
Netherlands	19.16%
Germany	9.00%
France	4.82%
Italy	3.66%
United Kingdom	2.06%
Turkey	1.66%
Sweden	1.48%
Ukraine	1.22%
Spain	0.66%
Other (69 Regions)	5.83%

Table 6. Top 10 Sources in EMEA , Q1 2020

The Americas	Percentage
United States	79.11%
Brazil	14.53%
Canada	1.81%
Argentina	1.11%
Mexico	1.11%
Panama	1.03%
Colombia	0.45%
Chile	0.36%
Ecuador	0.23%
Dominican Republic	0.07%
Other (13 Regions)	0.19%

Table 7. Top 10 Sources in Americas, Q1 2020

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

Global ASNs	Network Name	Percentage
4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	45.81%
3462	HINET Data Communication Business Group, TW	7.67%
15169	GOOGLE, US	5.60%
42610	NCNET-AS, RU	2.67%
57043	HOSTKEY-AS, NL	2.39%
9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN	2.35%
14061	DIGITALOCEAN-ASN, US	1.84%
53667	PONYNET, US	1.57%
23650	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN	1.35%
48817	RELDAS-NET, RU	1.13%
Others	983 ASNs	27.61%

Table 8. Top 10 Global ASNs, Q1 2020

APAC ASNs	Network Name	Percentage
4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	69.63%
3462	HINET Data Communication Business Group, TW	11.66%
9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN	3.57%
23650	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN	2.06%
4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	1.38%
38365	CNNIC-BAIDU-AP Beijing Baidu Netcom Science and Technology Co., Ltd., CN	1.21%
9318	SKB-AS SK Broadband Co Ltd, KR	0.92%
17974	TELKOMNET-AS2-AP PT Telekomunikasi Indonesia, ID	0.82%
45090	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	0.51%
4808	CHINA169-BJ China Unicom Beijing Province Network, CN	0.42%
Others	294 ASNs	7.83%

Table 9. Top 10 ASNs in APAC, Q1 2020

EMEA ASNs	Network Name	Percentage
42610	NCNET-AS, RU	15.71%
57043	HOSTKEY-AS, NL	14.08%
48817	RELDAS-NET, RU	6.65%
38994	ERAHOST-AS, NL	6.25%
202425	INT-NETWORK, SC	4.96%
201912	FCLOUD-AS, DE	4.84%
48642	KTEL-AS Ekaterinburg, Russia, RU	4.55%
207083	HOSTSLIM-GLOBAL-NETWORK, NL	4.48%
16276	OVH, FR	3.42%
12389	ROSTELECOM-AS, RU	2.79%
Others	393 ASNs	32.25%

Table 10. Top 10 ASNs in EMEA, Q4 2019

AMERICAS ASNs	Network Name	Percentage
15169	Google, US	32.53%
14061	DIGITALOCEAN-ASN, US	10.69%
53667	PONYNET, US	9.14%
264942	Alcantara Net LTDA, BR	4.50%
15169	GOOGLE - Google LLC, US	4.06%
262717	NET ARTUR INDUSTRIA E COMERCIO DE CAIXAS HERMETICA, BR	3.93%
13490	BUCKEYECABLEVISION, US	2.84%
14061	DIGITALOCEAN-ASN - DigitalOcean, LLC, US	2.57%
393499	ONLINE-TECH-LLC3, US	2.05%
266385	TR Servicos de Telecomunicacoes LTDA-ME, BR	1.81%
Others	276 ASNs	25.88%

Table 11. Top 10 ASN Rankings in the Americas, Q1 2020

Conclusion

This quarter saw an abnormal surge in DDoS attack activities compared to Q1 records over the past decade. YoY, the number of attacks catapulted by 278.17%, and QoQ increased by 542.46%. The rampant DDoS attacks during this first quarter are believed to be linked with the COVID-19 pandemic.

Abnormal traffic patterns detected from ISPs drew our particular attention. Traffic of abnormally small size and short duration was generated by exploiting open resolvers (DNS, DLAP, etc). For 0.99% of the traffic larger than 5Gbps, ISP networks detected and subsequently eliminated it before it could pose any possible threats to customers' networks.

It was discovered that 67.12% of the traffic in the 1Gbps to 5Gbps range, dubbed the "invisible killer" was overlooked by ISPs who are commonly faced with traffic of this size which seldomly impacted them or their customers. If disregarded, it has the potential to not only paralyze the ISP's network but also saturate the downstream customers' networks. 31.89% of traffic less than 1Gbps resembled requests destined for open resolvers. While small in size prior to reflection, this traffic was not blocked until it amplified into a reflected attack.

We believe that the "invisible killer" trend won't go away anytime soon, accentuating the key role of ISP's in the prevention and mitigation of attacks in the long run. Serving on the frontline of DDoS attacks, ISPs must hasten to effectively protect both its own networks and customer networks from either "invisible killer" or traditional attacks. Furthermore, as smart devices and IoT devices continually fall prey to hacking via DDoS-for-hire services, wreaking havoc on our cyberworld, cross-government collaboration with law enforcement should step up their efforts to crack down on such services. A concerted effort would be needed to safeguard the connectivity and service uptime of customer networks from risks and threats of DDoS attacks.

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

20200629-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