

Distributed Denial of Service (DDoS)

Annual Threat Report 2020

NEXUSGUARD®

DDoS Protection Made Simple

Table of Contents

Editor's Note	02	Single vector attacks dominate the threat landscape	17
2020: A Year in Review	03	High frequency-short duration attacks increased dramatically	18
COVID-19 drove DDoS attacks to new heights	04	DDoS attacks < 10Gbps are on the rise	19
Attack motives were as varied as the attacks themselves	06	Bit-and-piece attacks continue to wreak havoc on ISPs	20
DDoS attacks are more complex than ever	08	Source Distribution of Application Attack	22
Looking ahead to 2021/2022	09	Application Attack Source Distribution (IP Reputation)	23
• Predictions	09	Application Attack Source by Autonomous System Number	24
• Recommendations	12	(ASN) – Global & Regional	
2020 Attack Statistics	14	Ending Thoughts	26
UDP attacks were the most commonly used type of attack	15	Research & Methodology	27
Top 3 Attack Vectors	16		

Editor's Note

What a year 2020 has been! No one could ever have predicted how the world would have panned out the way it did over the past 12 months. COVID-19 caused a massive transition to work-from-home for millions around the world – and it's a situation that's lasting longer than anyone could have imagined, even though mass vaccination drives around the world have begun in earnest.

This annual report is our attempt to review a year that was defined by arguably the worst pandemic the world has seen in 100 years. We look back at some of the key insights, findings and trends covered in our previous quarterly reports, and how COVID-19 impacted not only cybersecurity, but also the way we now work and live.

We will look into how the threat landscape has evolved in terms of the increase in DDoS attacks over the past year, the increasing complexity and sophistication of attacks, and will compare relevant statistics against those garnered in 2019.

Against the backdrop of the global pandemic, we found that certain sectors, particularly the online gaming industry became instant hotbeds for DDoS attacks. We will also look at the motives behind attacks, as well as the shift in tactics and strategies employed by cybercriminals against their target victims.

Lastly, in view of the challenges faced by CSPs, service providers, enterprises and organizations in these unprecedented times, we will share our foresights on how DDoS attacks will evolve and recommendations on how best to tackle, mitigate and manage the ever-evolving cyber threats in the post COVID-19 world.





2020: A Year in Review

In the following sections, we will revisit some of the stories covered in our previous quarterly reports, review the key insights, findings and trends over the past year, and compare some of those statistics with those recorded in 2019.

- COVID-19 drove DDoS attacks to new heights
- Attack motives were as varied as the attacks themselves
- DDoS attacks are more complex than ever
- Looking ahead to 2021/2022

2020: A Year in Review -

COVID-19 drove DDoS attacks to new heights

On March 11, COVID-19 was officially declared a pandemic by the World Health Organization (WHO), and as the pandemic heightened around the world, so did the reliance on the Internet as the global workforce quickly shifted to remote work. That shift to work-from-home gave attackers fresh impetus to use DDoS as a way to target organizations and networks, putting an enormous strain on telcos, ISPs and CSPs.

A 369.21% year-over-year (YoY) increase in the number of DDoS attacks was recorded in March, accounting for 23.96% of all attacks in 2020. Q2 constituted 38.33% of attacks, representing the highest concentration of attacks in 2020. Interestingly, the number of attacks fell in July to 6.99% and this downward trend continued through till December.

Attack counts in March

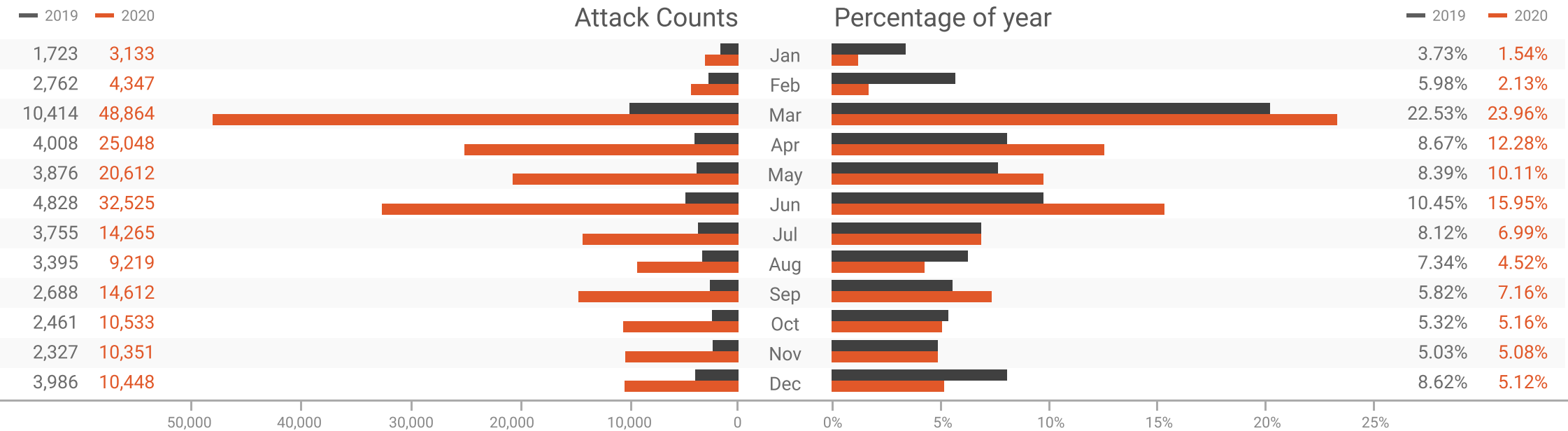


Figure 1 - Attack Distribution in 2020

March to June saw a particularly busy period for attackers as the attack count increased by a massive 449.38% month-over-month (MoM), which peaked in March and accounted for 23.96% of the total number of attacks in 2020. Attackers took advantage of the new reliance on online connectivity for remote working to cripple infrastructures and websites with DDoS attacks to force victims to pay a ransom to stop the attacks.

Prior to July, a large number of cyber crimes involved adversaries using large DDoS attacks or threats of them to extort organizations across a number of sectors. However, from July to September – a time when millions of people had been put under lockdown, stay-at-home entertainment, particularly online gaming started to gather momentum. Amid the global pandemic, attackers set their sights on the online gaming industry given its growing popularity. Of the DDoS attacks recorded during this 3-month period, we found that 31.74% attacks were targeted at the online gaming industry.

Although a downward trend in the number of attacks recorded in 2020 was observed from July through to December, it was still a 270% increase compared to the same period in 2019.

Furthermore, we recorded an 804.57% growth in unique IPs originating from Botnets used to launch application attacks of which 88.96% of the attacks came from computers and servers. And based on the source IPs that we recorded, the infected devices consisted of home computers and newly deployed servers from around the world.



2020: A Year in Review -

Attack motives were as varied as the attacks themselves

The motives and psychology behind each DDoS attack varies – they span financial gains, political and economic benefits, revenge, cyberwarfare or even purely for personal enjoyment. In general, large scale DDoS attacks tend to be the result of group efforts, as opposed to lone actors, with a specific agenda in mind.

From March onwards, according to our findings there was an increase in extortion and ransom DDoS (RDDoS) attacks against a wide range of industries around the world¹. In a RDDoS attack, malicious parties attempt to extort money from an individual or organization by threatening them with a DDoS attack that could knock their networks and websites offline for a length of time, unless the individual or organization agrees to pay a ransom.

Cybersecurity incidents of varying types occurred frequently, among which DDoS attacks increased greatly. Our findings showed that various sectors were hit the most by DDoS attacks in the months of April and June, with the top three sectors being enterprise, online gaming and online gambling, accounting for more than half of all attacks combined.

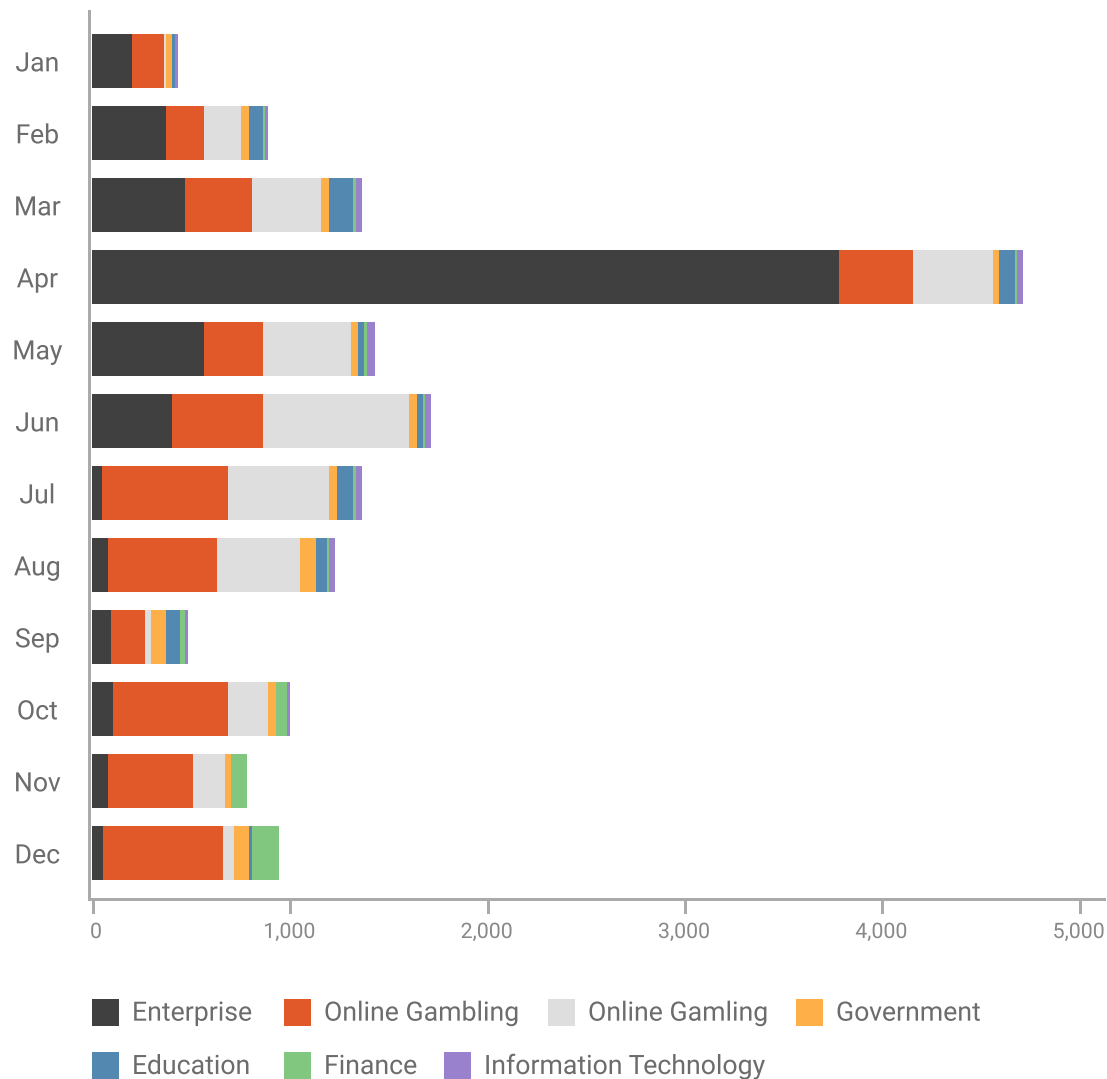


Figure 2 - Top Attacked Sectors in 2020

¹ Refer to Financial Services Information Sharing and Analysis Center (FS-ISAC)

With lockdown and social distancing measures enforced across the world beginning in June in response to the global pandemic, millions of people engaged in stay-at-home entertainment given their increased time at home, which led to an explosion in online gaming². Such heavy reliance on the Internet led to a sharp increase in attacks against the online gaming industry, as cybercriminals capitalised on its high revenue generating potential.

Owing to gamers' willingness to do anything to win, DDoS for-hire-services were also used to launch DDoS attacks to disrupt gaming matches, and gain the upper hand against gaming opponents by knocking them offline in order to earn unearned victories. As the gaming population continues to expand, the online gaming industry is expected to continue its upward trajectory for the foreseeable future.

2020

Jan

Feb

Mar

Apr

May

Jun

Jul

Aug

Sep

Oct

Nov

Dec

**Ransom DDoS
(RDDoS) attacks ▲**

**Top 3 most
attacked industries**

- enterprise
- online gaming
- online gambling

**Increase in attacks
on the
online gaming
industry**

2020: A Year in Review -

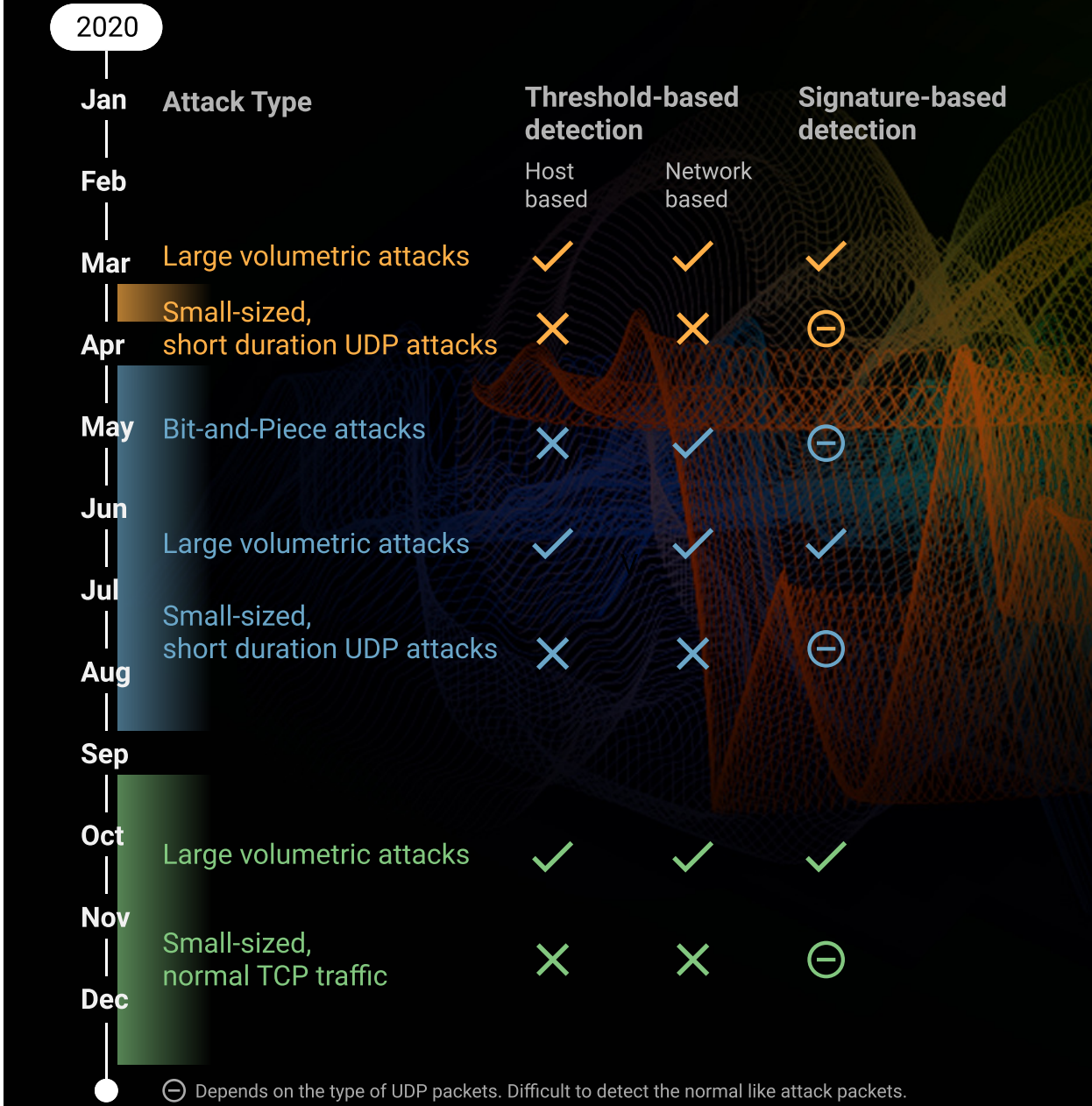
DDoS attacks are more complex than ever

In March, apart from traditional DDoS attacks, we identified other abnormal traffic patterns, including small-sized, short attacks dubbed “invisible killers.” Since these types of attacks occurred almost on a day-to-day basis and often didn’t provide detrimental service degradation to the customer or ISP, they were often overlooked by ISPs, allowing their invisible anomalies access to website and online services networks to cause havoc.

April to August witnessed a shift in tactics which saw attackers opting for a more deceptive and sophisticated approach, by utilizing a more elaborate practise of bit-and-piece attacks to launch amplification and other types of UDP-based attacks to flood target networks with traffic. There was a tendency to employ a blend of attack vectors to launch a wider range of UDP-based attacks, with bit-and-piece attacks taking centre stage.

Attacks launched from September through to December took a more sinister turn with perpetrators concealing TCP-based attacks within volumetric attacks, utilizing the volumetric attack as a cover. Our findings revealed that TCP ACK and SYN-ACK packets were leveraged to generate high packet rates (increased volumes of Packets Per Second – pps) to cause problems for networking equipment attempting to process the deluge of TCP packets. Since the TCP ACK packet is used as a keepalive and SYN-ACK packet is part of the TCP handshaking process, both packets are seen as normal traffic, making detection for signature-based detection methods extremely difficult.

Figure 3 - Summary of Attacks in 2020



2020: A Year in Review -

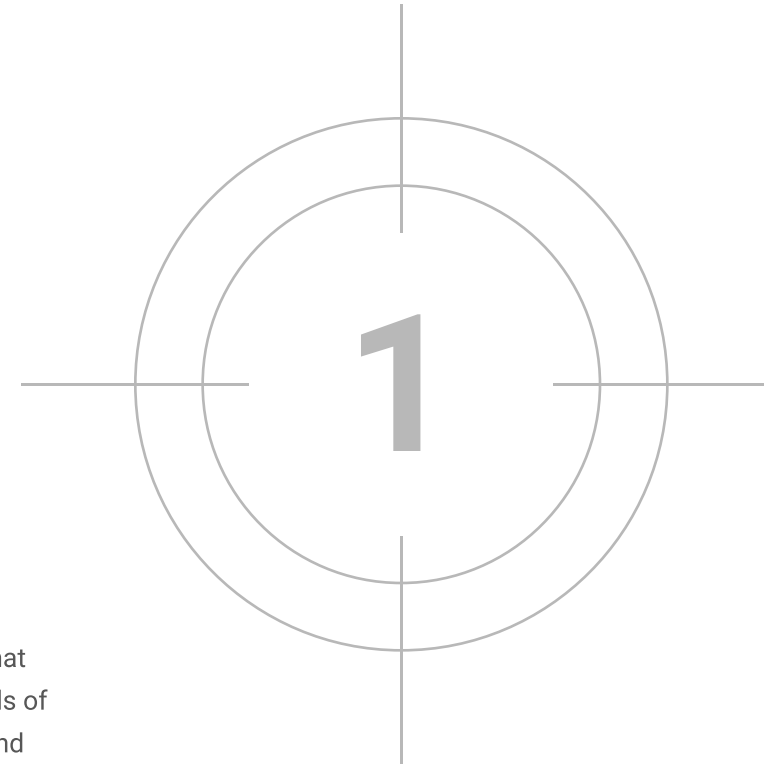
Looking ahead to 2021/2022

PREDICTIONS

Organizations, including CSPs, that rely on threshold and signature-based detection methods will experience severe outages as a result of DDoS attacks

This is because attackers have exploited new ways of leveraging small-sized traffic against the backdrop of a large volumetric attack - that acts as a cover - to overload threshold and signature-based detection systems. We foresee that the employment of high packet-rate loads of small-sized traffic fused with high concentrations of attack traffic will be an increasingly used strategy to overwhelm critical resources and devices.

By and large, threshold and signature-based detection is only geared towards detecting obvious static attack traffic patterns, but because network traffic is dynamic and constantly changes over time, new attack strategies have been able to successfully evade detection by exploiting the limited range of detection parameters inherent in traditional detection systems.



2020: A Year in Review -

t

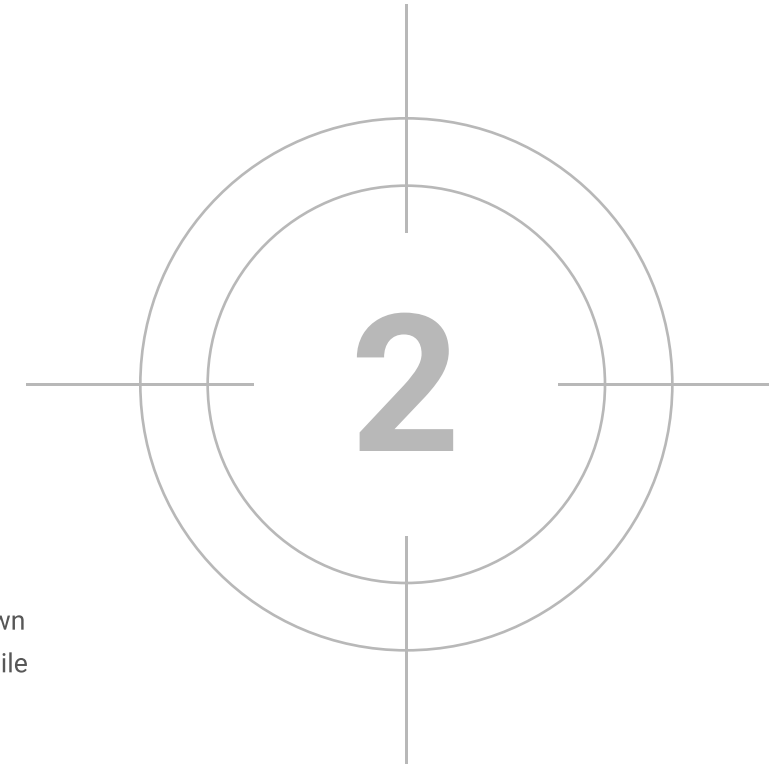
PREDICTIONS

The effectiveness of authentication-based mitigation will be further tested as application attacks are predicted to double in 2021/2022

We predict that enterprises will see more Layer 7 attacks in 2021/2022. These layer 7 attacks will also be much more advanced as they will be designed to bypass authentication-based mitigation. In general, authentication-based mitigation can adequately handle well-known application attacks such as Hulk and Slowloris, as well as more advanced incomplete HTTP request attacks and Slow Read attacks. While this type of mitigation works well with HTTP/HTTPS applications, it does not fare well with other applications, namely application programming interfaces (API) and mobile apps.

The aim of challenge-response authentications is to validate a browser's capabilities to respond to a set of actions which may include URL redirection, handling of cookies or the injection of a HTTP header, which help in identifying whether an actual human user or a bot is behind the browser. Unfortunately, attackers have devised ways to bypass this validation process through the use of highly-intelligent programmed bots that can handle such authentications.

Moreover, perpetrators could potentially tweak their attack strategies further by concealing application attacks within bit-and-piece attacks to overwhelm targeted services with high frequency-short duration attacks to cause a whole new set of problems to CSPs.



2020: A Year in Review -

Looking ahead to 2021/2022

PREDICTIONS

3

Ransom DDoS attacks will increase by 30%

Due to the rise in RDDoS, a significantly larger number of organizations will suffer from DDoS attacks. Such attacks will predominantly be short in duration as attackers cannot possibly launch sustained day-long campaigns on everyone and hope that organizations will pay ransoms.

Given the increasing popularity of such digital tools during the pandemic, we foresee that RDDoS attacks will be targeted at high-profit online businesses such as professional delivery services, video communications platforms, Game Makers and Telehealth services. The accessibility and popularity of cyber currencies, readily available DDoS-for-hire services and the world's continued focus on dealing with the pandemic have had a big hand in allowing perpetrators to extort organizations, using the threat of DDoS attacks against them until a ransom is paid in Bitcoin³. Although some victims are willing to pay the ransom, we strongly recommend against it as those who give in to their demands will find themselves in deeper waters as attackers will feel more assured, knowing their victims have the paying power.

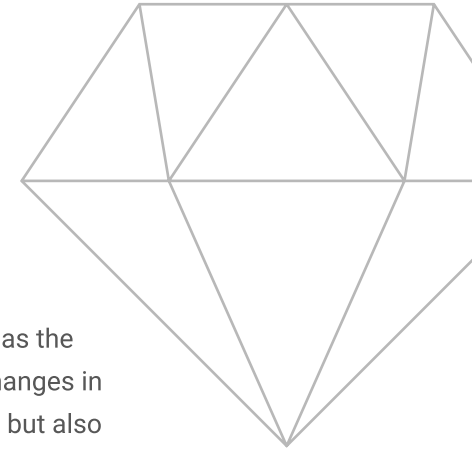
DDoS attacks < 10Gbps will account for 99% of all attacks

In 2021/2022, while we will continue to witness attacks in the order of a few hundred Gbps, we predict that 99% of DDoS attacks will not be bigger than 10Gbps. Rather than launching large bandwidth attacks against enterprises, attackers have opted to employ attacks using high packet-rate loads of small-sized traffic from DDoS-for-hire services, with the aim of evading DDoS mitigation detection systems. These types of attacks are not only extremely effective but also much more economical than employing large bandwidth attacks.

4

2020: A Year in Review -

Looking ahead to 2021/2022



The continued discovery of new attack patterns in recent times, especially small-sized attack traffic that have been able to evade threshold and signature-based detection systems suggests that CSPs need to enhance their security posture and look into employing more effective ways to protect their networks, infrastructures and customers.

RECOMMENDATIONS

Multidimensional DDoS detection

Multidimensional DDoS detection is highly recommended as it takes into consideration a wider range of factors such as the ratios of different protocols compared during peacetime and battletime, network traffic behaviour and the dynamic changes in traffic patterns over time. Taking into account these factors not only helps in identifying and classifying all traffic data but also provides a much more accurate and effective defence system against the constantly evolving DDoS attack trends.

Human behaviour-based detection and mitigation

Application attacks can evade most detection and authentication-based mitigation by manipulating simple HTTP responses such as HTTP redirect, cookies, URL, etc. Some advanced attacks can even manipulate javascript and captcha to achieve the same outcome. However, the nature of malicious HTTP requests such as sending numerous benign HTTP requests is not characteristic of human behaviour. Various robot-like requests or actions such as numerous single page requests from bots around the world, constant downloading of large pictures or repetitive searching of a particular subject to cause heavy loading on databases are designed specifically to exhaust server resources. We therefore recommend using human behaviour-based detection to identify malicious traffic and hosts in order that application attacks can be mitigated with far greater accuracy and efficiency.

Big data and deep-learning

Big data analysis and deep learning-based methods are extremely proficient in analyzing huge amounts of data, overcoming the inefficiencies inherent in threshold and signature-based detection methods. And due to their strengths in perusing large amounts of CSP traffic data automatically, malicious attack patterns can be pinpointed and dropped with speed and precision.

2020: A Year in Review -

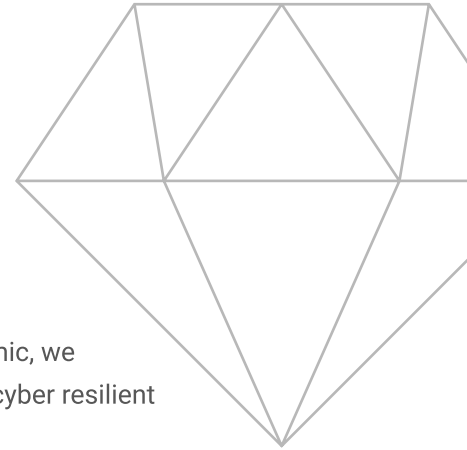
Looking ahead to 2021/2022

RECOMMENDATIONS

Comprehensive defensive measures

In view of the increase in remote work and reliance on various online services and resources amid the global pandemic, we strongly recommend that enterprises and organizations employ the following defensive measures to create a more cyber resilient environment to reduce the risk of cyber attacks:

- **Security Awareness Training:** Train employees to help better understand cyber threats and provide a strong line of defence, especially when working remotely.
- **Defence-in-depth Cybersecurity Strategy:** Implement a defence-in-depth cybersecurity strategy and access controls, including enabling multi-factor authentication (MFA), deploying up-to-date security policies and establishing a comprehensive data backup plan.
- **Device Security:** Ensure devices and routers are up to date, secure, and protected to reduce the risk of unauthorized access.
- **Network and Resource Segmentation:** Distribute servers and critical data in different data centers to ensure they are located on different networks with diverse paths.
- **Vulnerability Assessment and Penetration Testing:** Regularly check for and remediate exploitable security flaws and vulnerabilities.
- **Resiliency Plan:** Implement a comprehensive incident response plan, and regularly conduct rehearsals of incident response drills to improve response time and reduce service disruption during an attack.
- **RDDoS Attacks:** It is strongly recommended that organizations do not pay ransoms and that they notify the Police of the RDDoS threats made against them immediately.



2020 Attack Statistics

- UDP attacks were the most commonly used type of attack
- Top 3 Attack Vectors
- Single vector attacks dominate the threat landscape
- High frequency-short duration attacks increased dramatically
- DDoS attacks < 10GBps are on the rise
- Bit-and-piece attacks continue to wreak havoc on ISPs
- Source Distribution of Application Attack
- Application Attack Source Distribution (IP Reputation)
- Application Attack Source by Autonomous System Number (ASN) – Global & Regional

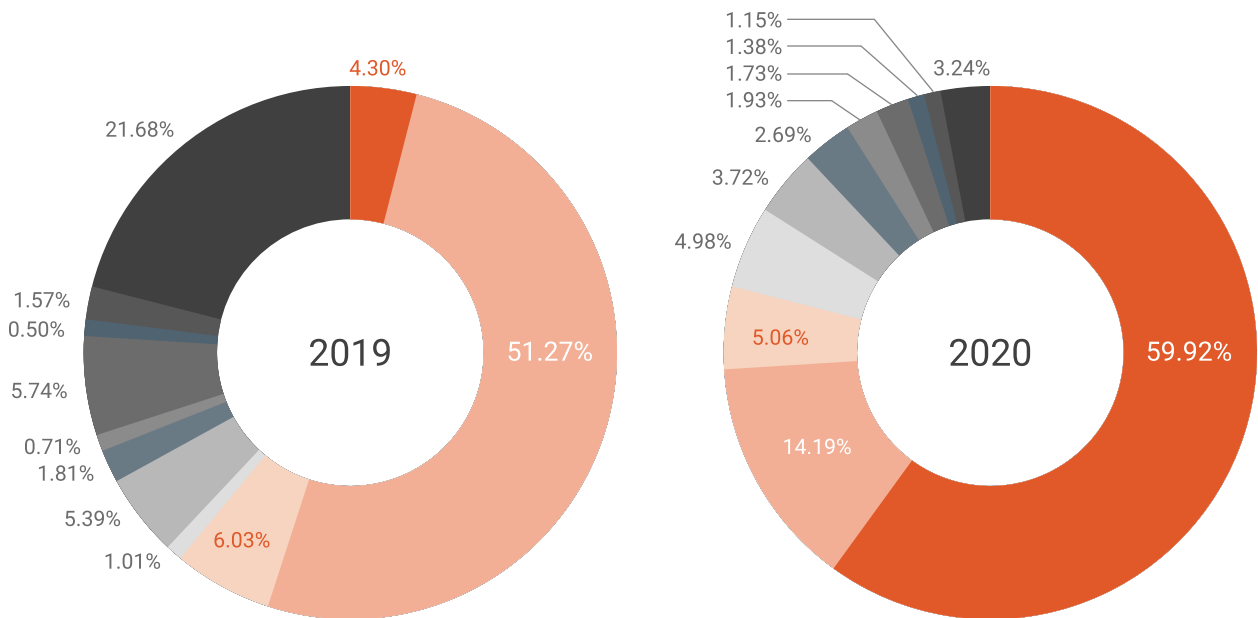
2020 Attack Statistics -

UDP attacks were the most commonly used type of attack

In 2020, UDP and DNS Amplification attacks were in the predominance of vectors, representing 59.92% and 14.19%, respectively. UDP attacks increased by 6,054.08% YoY. DNS Amplification Attacks decreased by 22.13% YoY. TCP SYN Attacks was ranked third with a 270.34% increase YoY. 2020 saw an increase across all attack types compared to 2019.

UDP attacks increased
by

6,054% YOY



Attack Types⁴

	% increase
UDP Attack	6054.08%
DNS Amplification Attack	22.13%
TCP SYN Attack	270.34%
CLDAP Reflection Attack	2067.16%
TCP ACK Attack	204.17%
IP Fragmentation Attack	555.93%
UDP Fragmentation Attack	1100.00%
HTTPS Flood	33.11%
DNS Attack	1126.96%
ICMP Attack	224.38%
Others	-33.98%

Figure 4 - Top 10 Attack Vectors in 2019 and 2020

⁴ 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

1 UDP Attack

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.

2 DNS Amplification Attack

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.

3 TCP SYN Attack

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.

2020 Attack Statistics -

Single vector attacks dominate the threat landscape

In 2020, 86.70% of attacks were shorter than 90 minutes, while the rest exceeded 90 minutes. 0.8% of attacks were longer than 1200 minutes. The quarterly duration averaged 171.42 minutes, while the longest attack lasted 63,756.77 minutes. YoY, both the maximum and average duration increased by 57.85% and decreased by 67.73% respectively.

83%

of recorded attacks were
single vector attacks

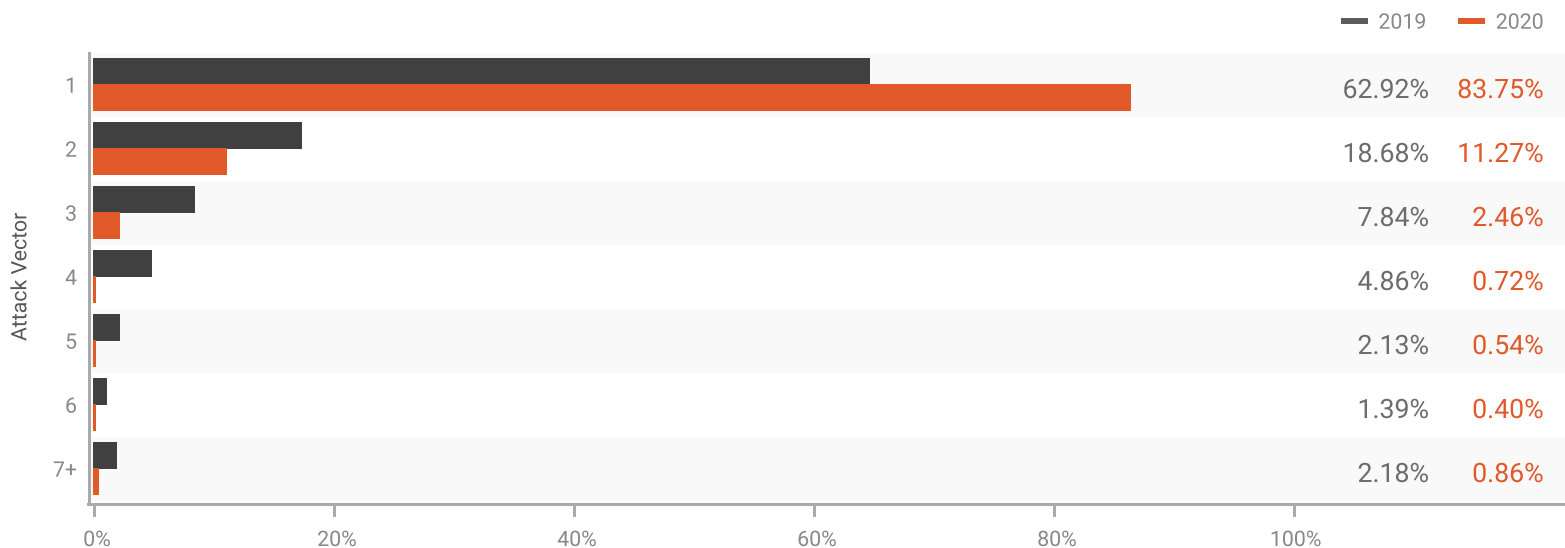


Figure 5 - Distribution of DDoS Attack Vectors in 2019 and 2020

2020 Attack Statistics -

High frequency-short duration attacks increased dramatically

In 2020, 86.70% of attacks were shorter than 90 minutes, while the rest exceeded 90 minutes. 0.8% of attacks were longer than 1200 minutes. The quarterly duration averaged 171.42 minutes, while the longest attack lasted 63,756.77 minutes. YoY, both the maximum and average duration increased by 57.85% and decreased by 67.73% respectively.

86%

of attacks were shorter
than 90 minutes

Duration (Minutes) ⁵			
	2019	2020	% increase
Maximum	40,391.35	63,756.77	57.85%
Average	531.16	171.42	-67.73%

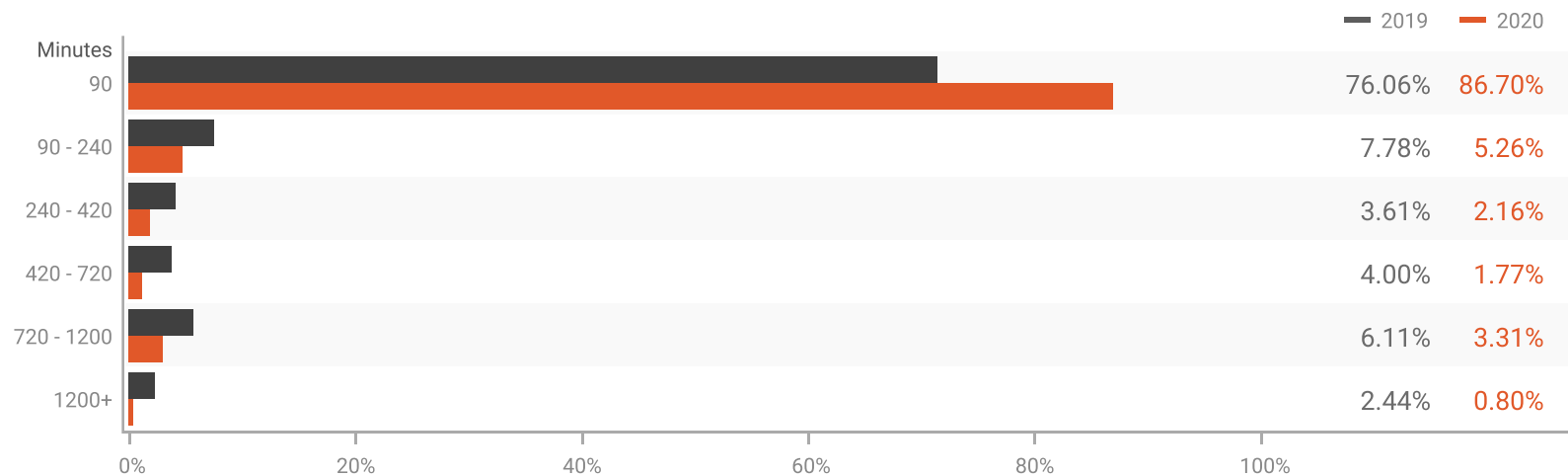


Figure 6 - Percentage Change of Attack Durations in 2020

⁵ 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.

2020 Attack Statistics -

DDoS attacks < 10Gbps are on the rise

In 2020, 66.34% of attacks were smaller than 1Gbps and 98.76% were smaller than 10Gbps. Those ranging between 1Gbps and 10Gbps accounted for 32.42%. The maximum size decreased by 37.04% YoY, while the average size increased by 5.26% YoY.

66%

of attacks were smaller than 1Gbps

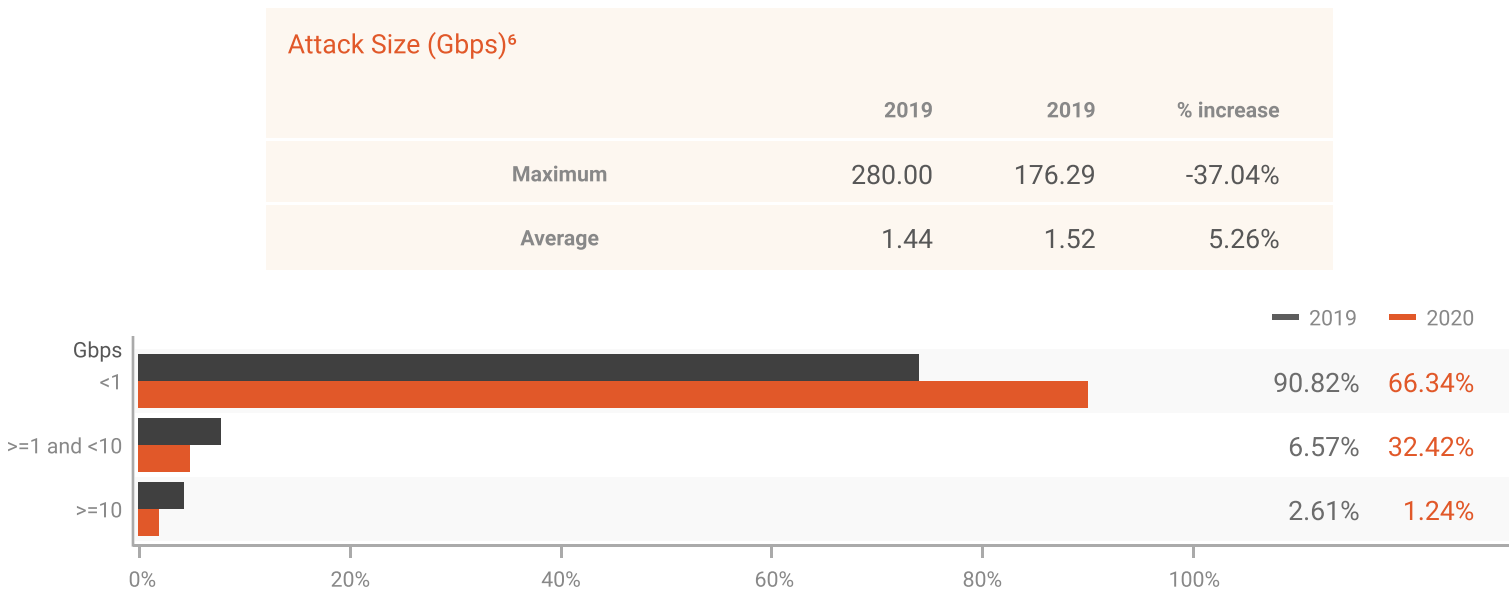


Figure 7 - Attack Size Distribution in 2019 and 2020

⁶ 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.

2020 Attack Statistics -

Bit-and-piece attacks continue to wreak havoc on ISPs

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.

Summary 1 - Bit-and-Piece Attacks in 2019 and 2020

		2019	2020	% increase
No. of Targeted ASN		305	301	-1.31%
No. Target Geolocations		24	23	-4.17%
Total IP prefixes under attack(Class C)		1,207	2,833	134.71%
No. of targeted IP addresses per IP prefix	Minimum	5	10	100.00%
	Maximum	256	256	0.00%
Attack Count per IP	Minimum	15.00	40.00	166.67%
	Maximum	293,907	5,204,092	1670.66%
Attack Count per IP prefix	Minimum	200	222	11.00%
	Maximum	538,127	5,219,918	870.02%
Attack Duration(Minutes)	Minimum	0.90	3.48	286.67%
	Maximum	28.73	48.15	67.59%

Targeted ASNs

301

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

2,833

Summary 2 - Bit-and-Piece Attack Types in 2019 and 2020

2019	2020
CHARGEN Attack(42.59%)	UDP Attack(44.22%)
DNS Amplification Attack(27.85%)	DNS Amplification Attack(33.16%)
SSDP Amplification Attack(26.05%)	CLDAP Reflection Attack(6.58%)
NTP Amplification Attack(3.52%)	IP Fragmentation Attack(6.24%)
	SSDP Amplification Attack(2.49%)
	UDP Fragmentation Attack(1.60%)
	TCP SYN Attack(1.56%)
	ICMP Attack(1.48%)
	CHARGEN Attack(1.05%)
	NTP Amplification Attack(0.68%)
	DNS Attack(0.51%)
	MS SQL RS Amplification(0.13%)
	TCP ACK Attack(0.13%)
	HTTPS Flood(0.08%)
	IP BOGONS(0.04%)
	SIP Flood(0.04%)

Summary 3 - Bit-and-Piece Attack Types in 2019 and 2020

2019		2020	
Belgium,	Romania,	Argentina,	Turkey,
Brazil,	Russian	Bangladesh,	Ukraine,
Bulgaria,	Federation,	Brazil,	United States ,
China,	Sweden,	Canada,	Australia,
Czech Republic,	Taiwan,	China,	Pakistan,
France,	Turkey,	Hong Kong,	Greece,
Gabon,	Ukraine,	Iran,	Kuwait
Germany,	United Kingdom,	Japan,	
Hong Kong,	United States	Lebanon,	
Indonesia,		Netherlands,	
Kazakhstan,		Poland,	
Korea,		Romania,	
Netherlands,		Russian Federation,	
Poland,		Singapore,	
Portugal,		South Africa,	
Republic of Latvia,		Taiwan,	

Source Distribution of Application Attacks⁷

MacOS devices contributed to about 0.5% of all application attack traffic, whereas Windows-powered PCs and notebooks contributed to about 85.41%. Mobile iOS devices such as iPads and iPhones made up about 5.96% of all application attack traffic, whereas android devices accounted for about 5.08%.

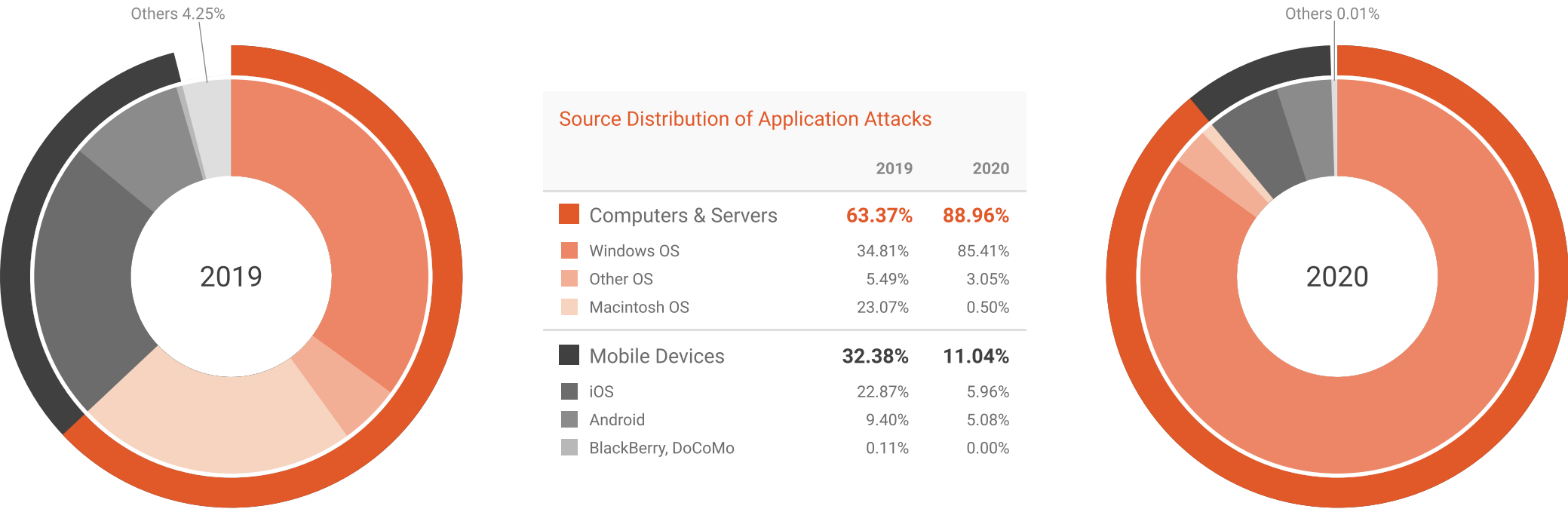












Figure 8 - Source Distribution of Application Attacks in 2019 and 2020

⁷ 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.

2020 Attack Statistics -

Application Attack Source Distribution (IP Reputation)

Application Attack Source Distribution (IP Reputation) in 2019 and 2020

	2019	2020
 China	15.46%	28.80%
 United States	18.58%	13.46%
 Turkey	0.39%	7.90%
 Malaysia	0.57%	6.99%
 Singapore	0.94%	6.71%
 Philippines	0.35%	6.38%
 Indonesia	2.06%	4.38%
 Hong Kong	0.67%	4.16%
 Brazil	3.94%	3.27%
 Thailand	1.85%	3.19%
Others(187 Regions)	55.20%	14.76%

2020 Attack Statistics -

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

Top 10 ASN Attacks Rankings in 2019 and 2020

	Network Name	2019	2020
AS4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	8.89%	15.66%
AS43260	AS43260, TR	Less than 0.01%	4.94%
AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN	32.41%	3.07%
AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	0.30%	2.84%
AS43242	EXTEND, TR	No Record	2.84%
AS45090	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	0.15%	2.20%
AS4788	TMNET-AS-AP TM Net, Internet Service Provider, MY	0.02%	2.12%
AS54994	QUANTILNETWORKS, US	No Record	1.87%
AS23650	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN	0.86%	1.83%
AS45498	SMART-AXIATA-KH SMART AXIATA Co., Ltd., KH	No Record	1.82%

Top 10 ASN Rankings in APAC 2019 and 2020

	Network Name	2019	2020
AS4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	9.96%	24.45%
AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN	36.30%	4.80%
AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	0.34%	4.43%
AS45090	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	0.16%	3.44%
AS4788	TMNET-AS-AP TM Net, Internet Service Provider, MY	0.02%	3.31%
AS23650	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN	0.96%	2.85%
AS45498	SMART-AXIATA-KH SMART AXIATA Co., Ltd., KH	No Record	2.84%
AS3462	HINET Data Communication Business Group, TW	0.03%	2.03%
AS9506	SINGTEL-FIBRE Singtel Fibre Broadband, SG	0.01%	2.01%
AS135354	NBPAP-AS-AP NAVER BUSINESS PLATFORM ASIA PACIFIC PTE. LTD., SG	No Record	1.95%

Top 10 ASN Rankings in EMEA 2019 and 2020			
	Network Name	2019	2020
AS43260	AS43260, TR	0.01%	23.56%
AS43242	EXTEND, TR	No record	11.37%
AS31083	TELEPOINT, BG	Less than 0.01%	7.22%
AS16135	TURKCELL-AS Turkcell A.S., TR	0.02%	6.63%
AS47331	TTNET, TR	0.97%	6.10%
AS15897	VODAFONETURKEY, TR	0.00%	5.56%
AS35047	ABISSNET, AL	Less than 0.01%	3.61%
AS20978	TT_MOBIL Istanbul, TR	No record	3.40%
AS16276	OVH, FR	4.89%	2.48%
AS34984	TELLCOM-AS, TR	0.01%	2.45%

Top 10 ASN Rankings in America 2019 and 2020			
	Network Name	2019	2020
AS54994	QUANTILNETWORKS, US	No record	12.48%
AS174	COGENT-174, US	0.03%	7.92%
AS7922	COMCAST-7922, US	0.43%	7.53%
AS16509	AMAZON-02, US	1.62%	6.71%
AS15169	GOOGLE, US	29.43%	5.91%
AS8075	MICROSOFT-CORP-MSN-AS-BLOCK, US	1.05%	5.87%
AS46664	VDI-NETWORK, US	0.04%	4.35%
AS53813	ZSCALER-INC, US	No record	3.41%
AS20057	ATT-MOBILITY-LLC-AS20057, US	Less than 0.01%	2.58%
AS136800	XIAOZHUYUN1-AS-AP ICIDC NETWORK, US	No record	2.51%

Ending Thoughts

For better or worse, the last year has changed us.

Reflecting on the year and all of its ups and downs, we have learned many lessons, not just about how perpetrators are using COVID-19 as leverage to create havoc, but about how remote working in a digital world can keep our societies functional in a time of lockdowns and quarantines.

2020 reinforced the reality that anything can happen at a moment's notice. Many office-based organizations, reliant on a face-to-face work style, shifted their entire organization to remote overnight. The extraordinary circumstances have forever changed our perspectives on work, health and travel.

Let's hope that our lives will return to some semblance of normalcy soon. In the meantime, always maintain good personal hygiene and remember to change your passwords regularly.

Stay safe!



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 Report produced by Nexusguard's research team:

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

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

