Threat Report

Distributed Denial of Service (DDoS)

Q4 2018

Contents

NEXUSGUARD®

Q4 2018 Threat Report

Key Observations

Crackdown on DDoS-for-hire services helps alleviate DDoS activity, but growing botnets and demand promise comeback

Thanks to the eradication of 15 of the world's biggest "Booters" (DDoS-for-hire websites), the web-based services designed for customers to launch distributed denial-of-service attacks against sites on demand, by the FBI in December 2018, the number of attacks as well as the maximum and average attack sizes decreased by 10.99%, 23.91%, and 85.36%, respectively, year-over-year (YoY).

Conversely, due to the continued exploitation of the "Bit-and-Piece" technique carried over from the previous quarter, the number of attacks and the maximum and average attack sizes increased by 36.08%, 49.15%, and 3.75%, respectively, quarter-on-quarter (QoQ). Widely adopted in Q3 2018, the "Bit-and-Piece" tactic avoids detection by contaminating legitimate traffic across hundreds of IP prefixes with small-sized junk.

Q4 2018 also saw conventional attacks like UDP, TCP SYN, and ICMP drop significantly on a YoY basis. However, SSDP Amplification attacks — the most popular "Bit-and-Piece" attack vector — increased by 3,122.22% YoY and 91.21% QoQ. Moreover, attackers were more persistent than before, as evidenced by a month-long attack case in which the target was hit by as many as 13 attacks a day for 28.95 minutes and 1493.93 minutes throughout most days of December.

Total Attacks

vs. Q4 2017	10.99% ▼
vs. Q3 2018	36.08% ▲

Attack Sizes

176 Gbps Maximum Attack Size	vs. Q4 2017	23.91% ▼	vs. Q3 2018	49.15% ▲
1.008 Gbps Average Attack Size	vs. Q4 2017	85.36% ▼	vs. Q3 2018	3.75% ▲

DDoS Attack Type

	SSDP	Amplification	HTTPS Flood	UDP	TCP SYN	ICMP
vs. Q4 2017	3,122.22% ▲	118.90% ▲	2.18% ▲	17.10% ▼	77.12% ▼	46.41% ▼
vs. Q3 2018	91.21% ▲	78.80% ▲	194.17% ▲	33.16% ▼	19.34% ▼	20.99% ▼

Quarter Highlights

FBI's Takedown of “Booter” Sites Severely Reduces Attack Activity

Q4 2018 was quite different from Q4 2017. YoY, the total attack count fell by 10.99%. The decrease was largely attributed to the FBI’s successful takedown of 15 large **“Booter”** websites that were alleged to be responsible for having generating more than 200,000 DDoS attacks since 2014. The FBI’s highly effective crackdown not only suppressed the number of total attacks YoY, but also the average and maximum attack sizes, decreasing both by 85.36% and 23.91%, respectively.

More about “Booters”

First, the availability of booter service sheds light on the legal loophole in website or network ownerships. Second, it raises concerns over the security vulnerabilities of a sheer number of unsecured and unpatched IoT devices as well as misconfigured computers and network devices. They entail rapid changes in the technological infrastructure in which hackers and cybercriminals can exploit countless vulnerabilities before they are even known to the manufacturer or owner. Last but not the least, we believe that DDoS attack-as-a-service, made easy with booter service, is poised to make a comeback despite the recent crackdown.

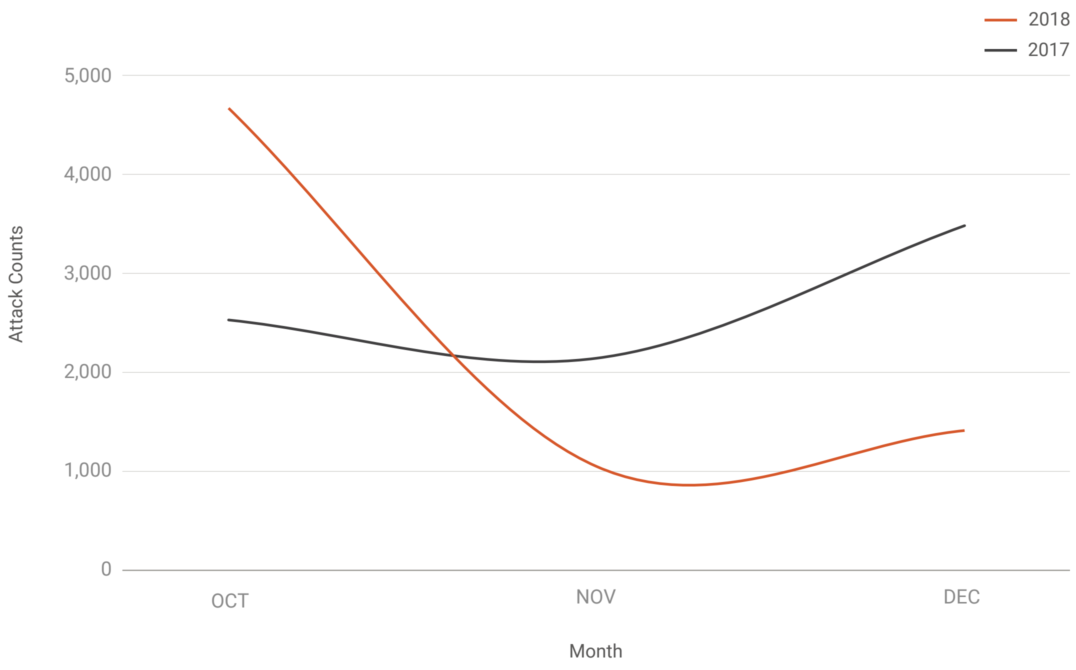

Figure 1. YoY Attack Counts, Q4 2017-2018

The concentration of HTTPS attacks has also caught our attention. In a rampant attack case, one of our customers was targeted throughout most days of December except two days. The durations of attacks on the victim network ranged from 28.95 minutes to 1493.93 minutes. An average of 13 attacks were logged within a day. It is believed that the attacker meant to take the network down throughout December—a traditional peak season for retail and entertainment.

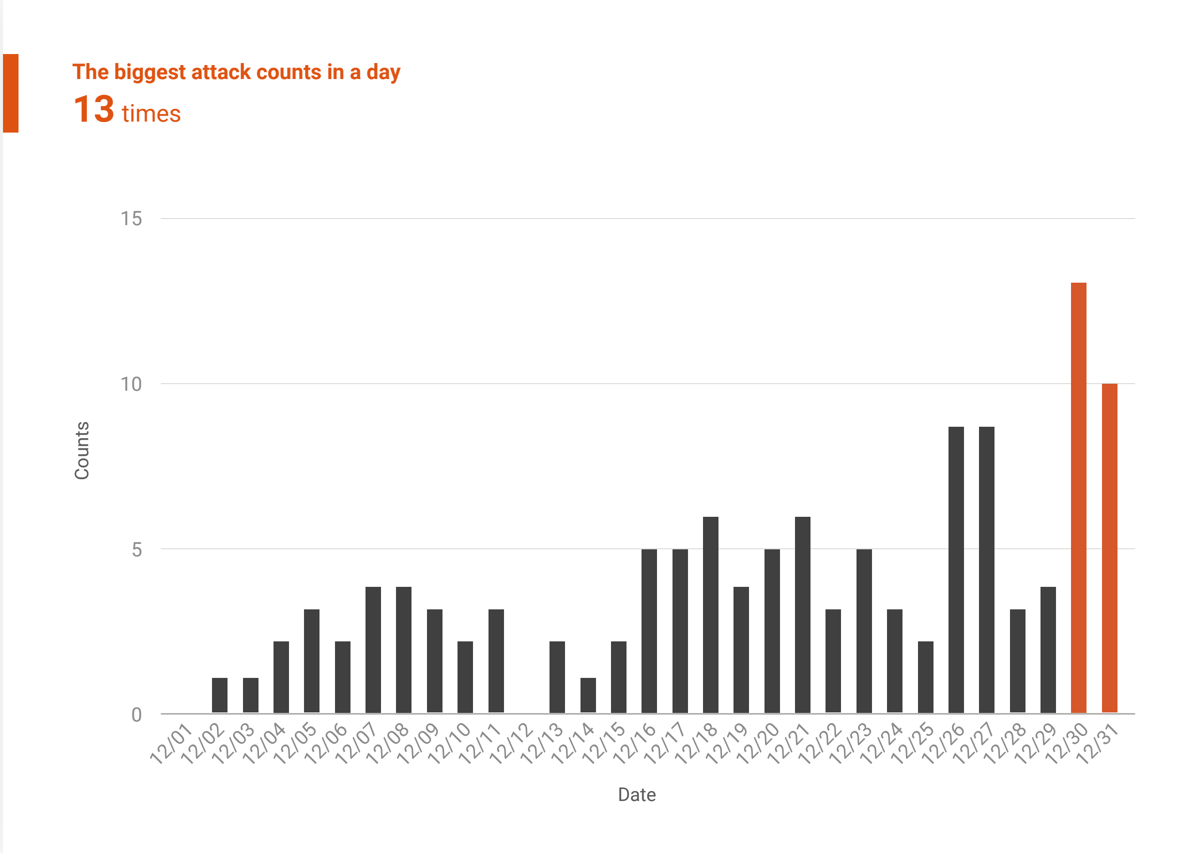

Figure 2. Daily Frequency of HTTPS Flood, Dec. 2018

DDoS Activities

Types of Attack Vectors

The “Bit-and-Piece” tactic popularized in Q3 continued in Q4 and was adopted by many attackers, regardless of the attack vector utilized. SSDP Amplification attacks constituted 48.26%, growing by 91.21% QoQ and a whopping 3,122.22% YoY. UDP followed with 14.26%, while HTTPS Flood clinched the third spot with 9.10% (an increase of 194.17% QoQ and 2.18% YoY). ICMP attacks accounted for 6.00% and HTTP Flood for 5.84% in the quarter (An increase of 239.52% QoQ, or a decrease of 52.48% YoY).

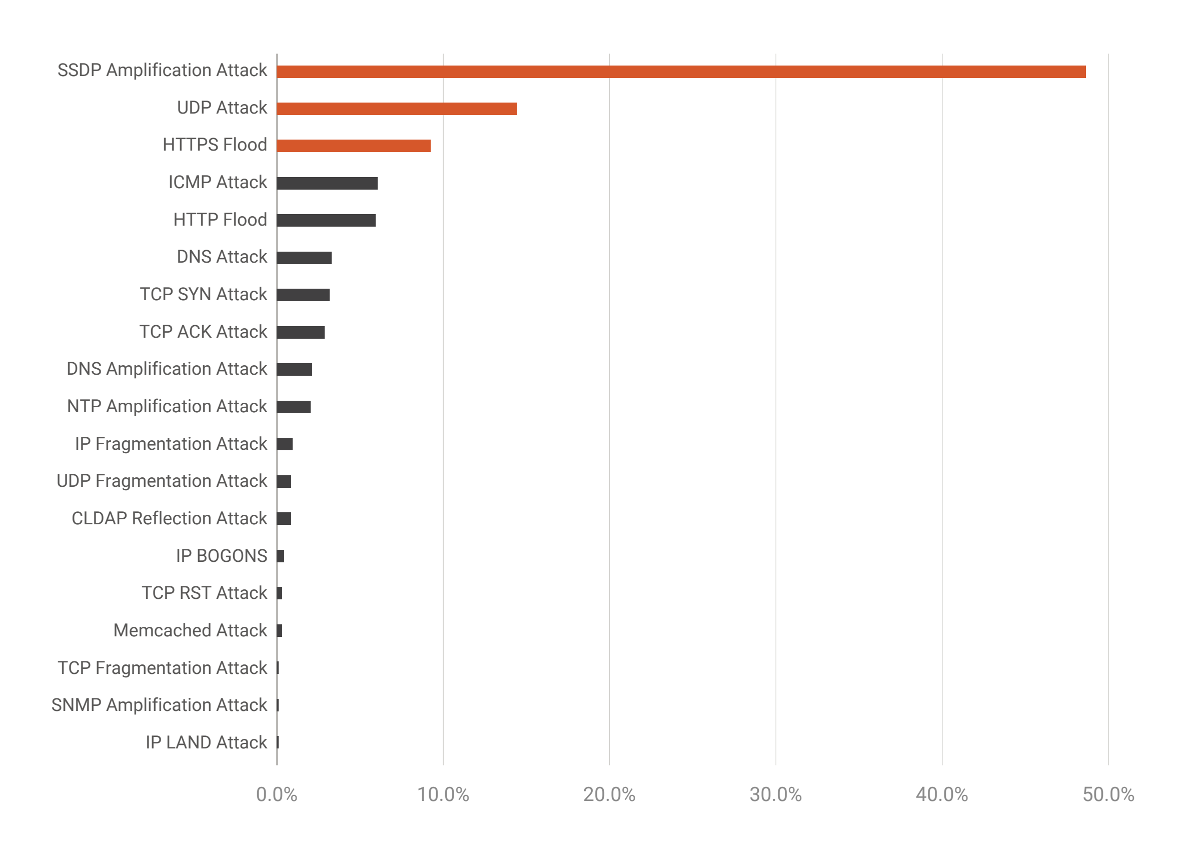

Figure 3. Distribution of DDoS Attack Vectors

Top 3 Attack Vectors

No.1 SSDP Amplification Attack

48.26 %

3,480

SSDP (Simple Service Discovery Protocol) attacks are launched over UDP via Universal Plug and Play devices such as printers, web cameras, routers, and servers. Perpetrators first discover and scan all exploitable devices and then use botnets to send UDP packets with a target's spoofed IP address to UDP Port 1900 of all exploitable devices. In turn, the devices respond massively, causing the target to become inundated with a large volume of replies. According to US-Cert, the bandwidth amplification factor during such attacks can be as high as 30.8x.

No.2 UDP Attack

14.26 %

1,028

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.3 HTTPS Flood

9.10 %

656

Attackers attempt to exhaust server resources by generating valid, volumetric HTTPS requests or sessions. The sessions are typically HTTPS GET, which overwhelm the victim's web servers by flooding them with answer requests (ACK). The process forces servers to allocate maximum resources to handle the volumetric attack traffic. As a result, legitimate requests cannot get through.

Number of Attack Vectors

Single-vector attacks (73.11% of the total) were prevalent in the quarter, while 26.89% leveraged multiple vectors. The maximum number of attack vectors utilized in Q4 was 11. UDP figured prominently as the lead vector in the vast majority of multi-vector attacks.

Single-vector attacks
73.11 %

Multi-vector attacks
26.89 %

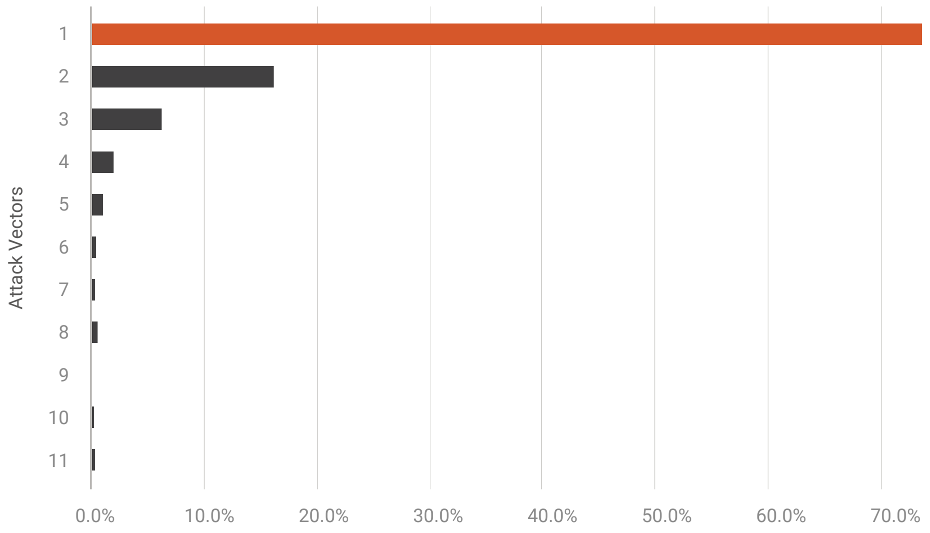

Figure 4. Distribution of DDoS Attack Vectors

Rankings	Attack Vector 1	Attack Vector 2	Attack Vector 3	Distribution of Multi-vectors
1	UDP	DNS	N/A	29.50%
2	UDP	DNS Amplification	NTP Amplification	7.55%
3	UDP	DNS Amplification	N/A	6.47%
4	HTTP	TCP SYN	N/A	4.32%
5	UDP	ICMP	N/A	2.52%
5	TCP SYN	ICMP	N/A	2.52%
5	UDP	CLDAP Reflection	N/A	2.52%

Table 1. Ranking of Multi-vector Attacks

Attack Durations[1]

Attacks lasting fewer than 90 minutes accounted for 42.80% of the total, while those lasting longer were 57.20%. Attacks spanning 1,200+ minutes clocked in at 15.58%. The quarterly average duration was 452.89 minutes, while the longest attack lasted 18 days, 21 hours, and 59 minutes. The average and maximum durations bumped up considerably in the quarter (145.82% QoQ and 175.61% YoY).

Attacks in the quarter were routinely targeted to occur during peak service hours. In one extreme case, the victim was hit by as many as 13 attacks in a day, each spanned from 28.95 minutes to as persistent as 1493.93 minutes in duration. Such concerted attack was obviously intended to cause total outage especially to the target network during peak service hours.

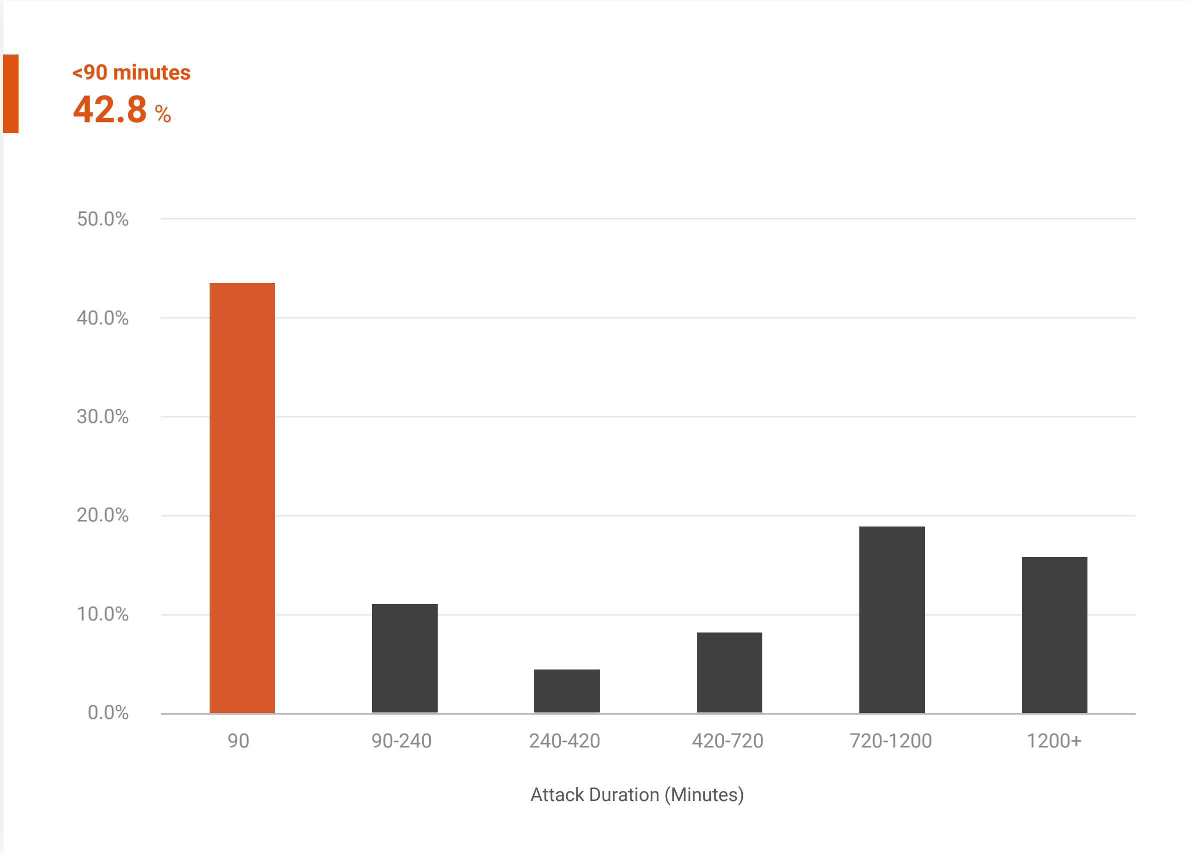

Figure 5. Attack Duration Distribution

[1] Attack duration measures the timespan of a series of attacks on the same destination IP within an interval of five minutes, regardless of the number of attack vectors. If no further attacks occur following the five minute interval, the end of the last attack is considered the cut-off time. The "ceasefire breaks" between attacks are excluded from attack duration time.

Attack Size Distribution[2]

In the quarter, 96.84% of attacks were smaller than 10Gbps and a full 90.37% smaller than 1Gbps; those ranging between 1Gbps and 10Gbps accounted for only 6.47%. The occurrence of “Bit-and-Piece” attacks and the negligible size of application attacks combined to keep the overall attack sizes relatively small in the quarter.

The largest attack in the quarter

176.00 Gbps

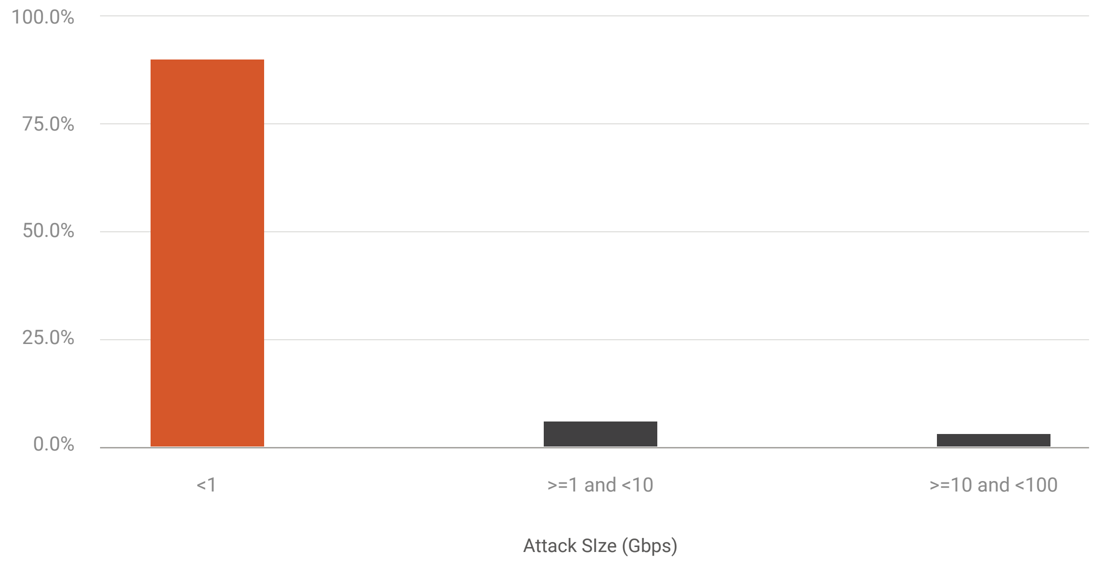

Figure 6. Attack Size Distribution

DDoS attacks in Q4 2018 saw a drop in both maximum and average size YoY (down 85.36% and 23.91%, respectively), while both rose QoQ (up 3.75% and 49.15%, respectively).

Attack Size in Gbps	Q4 2018	Q3 2018	Q4 2017
Maximum	176.00	118.00	231.32
Average	1.008	0.97	6.89

Table 2. Attack Size Quarterly Variations

[2] Attack size measures the aggregate size of a series of attacks on the same destination IP within a time interval of five minutes, regardless of the number of attack vectors. The peak size of each attack within the attack interval is counted in the aggregation. If no further attacks occur after five minutes, the aggregation ends.

Global Attack Source Distribution[3]

As often is the case, China was No.1, followed by the US. France and Russia placed third and fourth. As they account for nearly one-third of the world's Internet users, it's no surprise that China and the US also the lead the pack as top sources of DDoS attacks worldwide.

Regions	Percentage
China	22.68%
United States of America (US)	18.01%
France	7.06%
Russian Federation	4.14%
Brazil	3.53%
Vietnam	3.53%
South Korea	2.78%
India	2.72%
Netherlands	2.48%
Italy	2.37%
Other (135 Regions)	32.07%

Table 3. Global Attack Source Distribution

[3] Untraceable volumetric attacks transmitted with spoofed IP addresses such as TCP SYN, ICMP, and DNS are not included in our sampling. Only traceable attacks like HTTP Flood with real source IP addresses are counted.

APAC Attack Source Distribution

As the top global attack source, China, as expected, is also the leader of the pack in APAC, followed by Vietnam, India, and Indonesia.

Regions	Percentage
China	61.16%
Vietnam	9.52%
India	7.33%
Indonesia	4.06%
Thailand	3.63%
Taiwan	2.95%
Singapore	2.19%
Hong Kong	1.62%
Japan	1.55%
Malaysia	1.33%
Others (12 Regions)	4.50%

Table 4. APAC Attack Source Distribution

Global Attack Sources by Autonomous System Number (ASN)

Unsurprisingly, attacks emanating from ASNs in the US and China top the list. France, Vietnam, and Korea are also key contributors.

ASN	Network Name	Percentage
14061	DIGITALOCEAN-ASN - DigitalOcean, LLC, US	9.18%
45090	CNNIC-TENCENT-NET-AP - SHENZHEN TENCENT COMPUTER SYSTEMS CO LTD, CN	7.24%
16276	OVH, FR	6.07%
4134	CHINANET-BACKBONE - NO.31, JIN-RONG STREET, CN	3.50%
45899	VNPT-AS-VN - VNPT CORP, VN	2.29%
38365	CNNIC-BAIDU-AP BEIJING BAIDU NETCOM SCIENCE AND TECHNOLOGY CO., LTD., CN	2.02%
4766	KIXS-AS-KR KOREA TELECOM, KR	1.70%
4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	1.65%
16509	AMAZON-02 - AMAZON.COM, INC., US	1.56%
4808	CHINA169-BJ CHINA UNICOM BEIJING PROVINCE NETWORK, CN	1.52%
Others	1,460 ASNs	63.28%

Table 5. Top Ten ASN Attack Rankings

End Note

On Cybercrime Law Enforcement

In 2018, the FBI cracked down on 15 of the world's largest DDoS-for-hire websites, which are believed to have mounted more than 200,000 attacks since 2014. The enforcement efforts against these "Booters" caused attack counts to drop around 11% in Q4 2018 versus the same period in 2017, while average and maximum attack sizes went down 85% and 24%, respectively.

Cracking down on "Booters" and seizing the command-and-control (C&C) servers of botnets have long been part of the FBI's campaign for fighting cybercrime. In 2011, the FBI obtained a court order authorizing the seizure of 29 domain names used to control the notorious Coreflood botnet. Early last year, it seized the control of a C&C server behind a botnet of 500,000 hacked routers, allegedly controlled by Russia. But despite collaborative law enforcement efforts conducted by international agencies, it's not likely that the headache of DDoS attacks will fade away.

Botnet builders will continue to find ways to exploit security vulnerabilities of Internet-connected devices. The spread of the source code of Mirai, a malware that turns networked devices running Linux into bots, amply demonstrates this eventuality. The release of the Mirai source code immediately fuelled the exponential growth of botnets. The Satori malware, evolved from Mirai, was advanced to exploit the zero-day vulnerabilities of other types of IoT devices.

In contrast to tracking down C&C servers and alerting the owners of compromised devices, less effort is required to shut down "Booter" websites since they are more visible and accessible via search engines. That said, Nexusguard believes that the FBI's December crackdown only scratched the surface of a global problem. Since a DDoS-for-hire attacks can easily be launched against a victim in another country, law enforcement entities across national boundaries will need to intensify cross-border intelligence sharing, for example via Interpol.

The root cause of botnets stems from hardware/software vulnerabilities and human ignorance or negligence that leave the door open for malware to enter and take control. Patching all vulnerabilities and raising security awareness across all levels of users, in theory, is a way out. But in reality that's easier said than done — so botnets and DDoS-for-hire services are not likely to disappear any time soon.

For the novice, carrying out a DDoS attack no longer requires coding or hacking skills; it's now just a few clicks away. More bandwidth, faster connection speeds, and unpatched and unknown hardware/software vulnerabilities will continue to make DDoS attacks a persistent headache — despite the best efforts of law enforcement agencies.

Research & Methodology

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

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

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

20190311-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