NEXUSGUARD®

Threat Report

Distributed Denial of Service (DDoS)

Q2 2019

Contents

NEXUSGUARD®

Q2 2019 Threat Report

Metrics

Total Attacks

vs. Q2 2018	17.73% ▲
vs. Q1 2019	14.69% ▼

Attack Sizes

Maximum

117.9 Gbps

vs. Q2 2018	67.16% ▼
vs. Q1 2019	18.91% ▼

Average

0.969 Gbps

vs. Q2 2018	96.33% ▼
vs. Q1 2019	17.71% ▲

DDoS Attack Type

	DNS Amplification	HTTP	HTTPS	Application	Amplification
vs. Q2 2018	1040.41% ▲	281.51% ▲	363.33% ▲	313.14% ▲	314.93% ▲
vs. Q1 2019	31.01% ▲	12.78% ▼	36.00% ▼	24.64% ▼	15.87% ▼

Quarterly Focus - Q2 2019

DNSSEC (Domain Name System Security Extensions) Fuels New Wave of DNS Amplification

DNS Amplification[1] contributed to the largest share of attack activities in Q2 2019, accounting for 65.95%, confirmed 8,382 DNS Amplification attacks. During the quarter, Nexusguard's honeypot network captured 144,465,553 malicious DNS queries.

Based on attack patterns, the amplification factor of these incidents ranged between 36X and 72X. Compared with the maximum amplification power of memcached attacks, the destructive power of these attacks is considerably smaller. Nevertheless, the size is more than enough to inflict DDoS effects on victimized networks.

The observation that multiple government domains (as well as paypal.com) fell victim to rampant abuses during the quarter is surprising at first sight. Closer scrutiny, however, suggests that many of these domains had deployed DNSSEC to the top-level .gov domain as required by the U.S. government's OMB mandate. There is a strong causal relation between DNSSEC implementation and increased DNS Amplification because, due to the large size of responses they generate, DNSSEC-enabled servers are at risk of being targeted to reflect amplification attacks.

DNSSEC was designed to protect applications from using forged or manipulated DNS data, such as that created by DNS cache poisoning. The extra security DNSSEC provides relies on a resource-intensive data verification process using public keys and digital signatures.

1 The Domain Name System (DNS) is a fundamental element in Internet technology as it translates domain names into corresponding IP addresses. The DNS queries and responses are UDP-based (User Datagram Protocol). DNS servers are constantly abused to reflect DNS Amplification attacks. Memcached, SSDP or CLDP services are part of the intranet and are not supposed to be accessible to the public. Such services can be turned into weapons for generating amplification and reflection attacks only when they are unsecured or insecure. By contrast, the data provided by DNS is intended to be available to any device on the Internet. The continued adoption of DNSSEC, along with the existence of other vulnerable protocols, suggests that DNS Amplification will remain a mainstream attack method and continue to pose a significant threat to service provider and enterprise networks alike.

Domain	Query Count	Percentage	Included DNSSEC
1x1.cz	16,605,666	11.49%	yes
edu.za	13,524,481	9.36%	yes
aids.gov	12,640,652	8.75%	yes
isc.org	12,541,244	8.68%	yes
eftps.gov	11,423,694	7.91%	yes
mz.gov.pl	10,811,274	7.48%	yes
paypal.com	9,403,514	6.51%	yes
leth.cc	9,118,943	6.31%	yes
dfafacts.gov	7,299,000	5.05%	yes
nel.gov	7,212,696	4.99%	yes
other	33,884,389	23.45%	

Table 1: 10 Most Frequently Abused Domains and Query Counts of DNS Requests

Take the domain aids.gov as an example. As shown in Figure 1, the size of DNS response packets is significantly larger than that of the original query. In this example, a response without DNSSEC data is only 4.53X the size of the original query, while a response that includes DNSSEC is 45.28X larger.

```
XXXXXXXX:~ XXXX$ dig ANY aids.gov +bufsize=8192 +dnssec +notcp @X.X.X.X

; <<>> DiG 9.10.6 <<>> ANY aids.gov +bufsize=8192 +dnssec +notcp @X.X.X.X
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58188
;; flags: qr rd ra; QUERY: 1, ANSWER: 31, AUTHORITY: 5, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;aids.gov.                      IN      ANY

;; ANSWER SECTION:
aids.gov.               14      IN      NSEC    _dmarc.aids.gov. A NS SOA MX TXT RRSIG NSEC DNSKEY SPF
aids.gov.               14      IN      RRSIG   NSEC 8 2 60 20190909000127 20190903230127 30216 aids.gov.
jATB0vv/UTdTZ0STPAcfqro300zdhT1Wmq0WP3LZyPhbiNgDO+mQXDbI Asbkt2rxOCaI+CBWEGbAg3EW/zHm/S1QbUQvAgIGbhRgMoaEpnmJ86hp
75o3BWSnZ5Q7EiMm2nyBF27RzKdtqvFJ8B5MJhJZjnPcQM/D6Kfchz6a tqY=
aids.gov.               2654    IN      RRSIG   DS 8 2 3600 20190911041008 20190904041008 7877 gov.
c8dOaOlk5CIB0INfUGT5BVCD95hrD4VHyhirVjcFmOsbDs7xyp/RpIkh M2FoCUBywQWVRF2BZC/bg9jpc3bmk4vWQyTB0IXDVIdYF8QdN8VW67BC
eYhZ76o7hr7iHRCr1XXYSwRku9liKxf+79QdSCcF1/TqSKOkJoGOBRpE F0M=
aids.gov.               2654    IN      DS      33911 8 2
25E4201580BAD778CEB8CA012798C2F736FD74C0F43D90037D898890 0A31924A
                        .
                        .
                        .
aids.gov.               854     IN      DNSKEY  256 3 8 AwEAAbhx1s507zBoGvr5EjMfm8aLFO8jRHwRiz7nIMU1MsAP65S5C51q
PVygjQzM4YGqg9DxsjJHFSRalj5hRpBQLNk+GbbWbkcsbSn3301ILI3/ IqE9Pcjb1fv/5hTdy2fBcA9r/qW3azJlvmEfkerjD0/BJvxAaAhHfKUU 2MFLxthB
aids.gov.               854     IN      DNSKEY  257 3 8
AwEAAXbzVMd0WJUadXS3iC0Np4ReMGeFfvxBKmznUfNf3soFhYN5HD1Y TyD7AF7t/ojiXDVp5K7L6UxZ+H26zdE+OxsCh4Va6751v+YVR8TpQNIA
bQODITKV8o7BfPsZOMfQbM2MQs2BNNX7LYL5VJdYYNCvUfIVujfM2jMP fcO6R11R0rxIls2loMLahimOVkTQH7LL1D3hLtuUAhwZQrcm8ZjlMUSg
wzZGDHGkf/Y8BXGawk32ovtm8nf1NZhuMUGS7ksc4jvl/747OmKMpfSc 7+tKXLmAYAAQUpgo27/AXvLI86LHYYDYumzh0GGvmKLRxxuqqgVFpd5H
s35lHd/xbts=
aids.gov.               854     IN      DNSKEY  257 3 8 AwEAAboH+KOSR2Mr+qwWBV2xVIWJ2fc1IqSL/nDZo/tJMQr2vHE9i+bB
256/kFjZOYtfbLfM5/+ZBTJhLndmGwRyZxo9q/Ccy4UWIaUMXosOqWcy 0/GjvrNPLwDRHs7QcAA4kgKWl1SVKE+gz+NjRPG/GmKCqff3XOwP75vH
Q64HOMckhDH76/mcuNtlrfJyswuo30v0S7pQqGLZbloL9A6O+PvGdudz Vs1hbweDL7/mMRJeS0x+fjWktRK3J2itF2SWrTHvPyWthdQmvtQEtpqE
INsmdV/07gRxLLmfhDBDmSRodVwndp3iyFqUgYnAHaMKRhVjCqJwcxB5 dRy4s5wvRWM=
                        .
                        .
                        .
;; Query time: 626 msec
;; SERVER: X.X.X.X#53(X.X.X.X)
;; WHEN: Wed Sep 04 15:34:27 HKT 2019
;; MSG SIZE  rcvd: 3716
```

Figure 1: DNS Response is enlarged when DNSSEC Data is Embedded

Table 2 compares the amplification factors of the 10 most frequently abused domains before and after DNSSEC adoption. Again using aids.gov as an example, the domain's DNS server amplification power surged to more than 45.28X (up from 4.53X) after DNSSEC. Clearly, DNSSEC is a very cost-effective resource for attackers seeking to reflect amplification attacks. While intended to be a patch to DNS poisoning, DNSSEC has had the unintended consequence of creating yet another DDoS vulnerability.

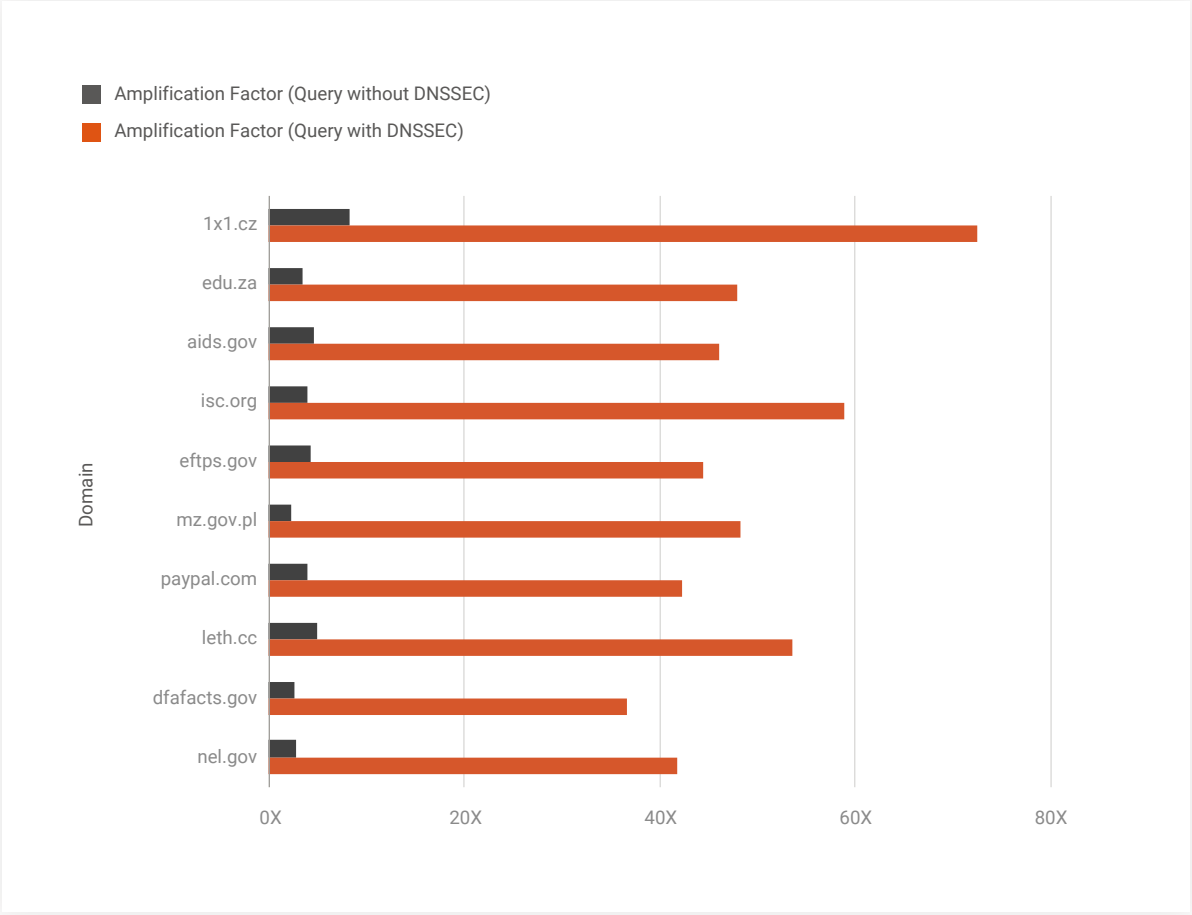

Figure 2: Comparison of amplification factors

Strategic Bit-and-Piece Attacks Continue to Spread

In addition to DNS Amplification, targeted ASN networks were also hit by CHARGEN, SSDP, and NTP Amplification in what are known as Bit-and-Piece attacks. The tactic was widely adopted across Europe, North America, and Africa.

Targeted ASNs
84

Total IP Prefixes (Class C Networks) Under Attack
460 (315 Prefixes)

Attack Types

- CHARGEN (58.76%)
- DNS Amplification (23.26%)
- SSDP Amplification (17.80.%)
- NTP Amplification (0.18%)

Targeted Geo-locations

Belgium, Brazil, Bulgaria, China, Czech Republic, France, Gabon, Germany, Hong Kong, Indonesia, Kazakhstan, Republic of Korea, Latvia, Netherlands, Poland, Portugal, Romania, Russian Federation, Sweden, Taiwan, Turkey, Ukraine, United Kingdom, United States

Category	Minimum	Maximum
No. of Targeted IP Addresses per IP Prefix /24	5	256
Attack Durations (Minutes)	10.22	1,797.95
Attack Count per IP	40	49,246
Attack Count per IP Prefix	200	328,291

Attacks Predominantly Originate from Botnet-hijacked Windows and iOS Machines

48.28% of Windows OS computers and servers and 20.48% of iOS-powered mobile devices were leveraged to launch DDoS attacks.

Devices	OS	Percentage
Computers & Servers	Windows	48.28%
	Other	5.48%
	Macintosh	2.55%
Mobile	iOS	20.48%
	Android	4.38%
Others (including IoT)	Other OS	18.84%

Table 2. Distribution of OS and Device Types as Attack Sources

DDoS Activities

Types of Attack Vectors[2]

DNS Amplification was the leading vector, showing sharp increases of 31.01% QOQ and 1,040.41% YOY, respectively. HTTP and HTTPs Flood followed, dropping 12.78% and 36.00% (QOQ), while increasing 281.51% and 363.33%, respectively, (YOY).

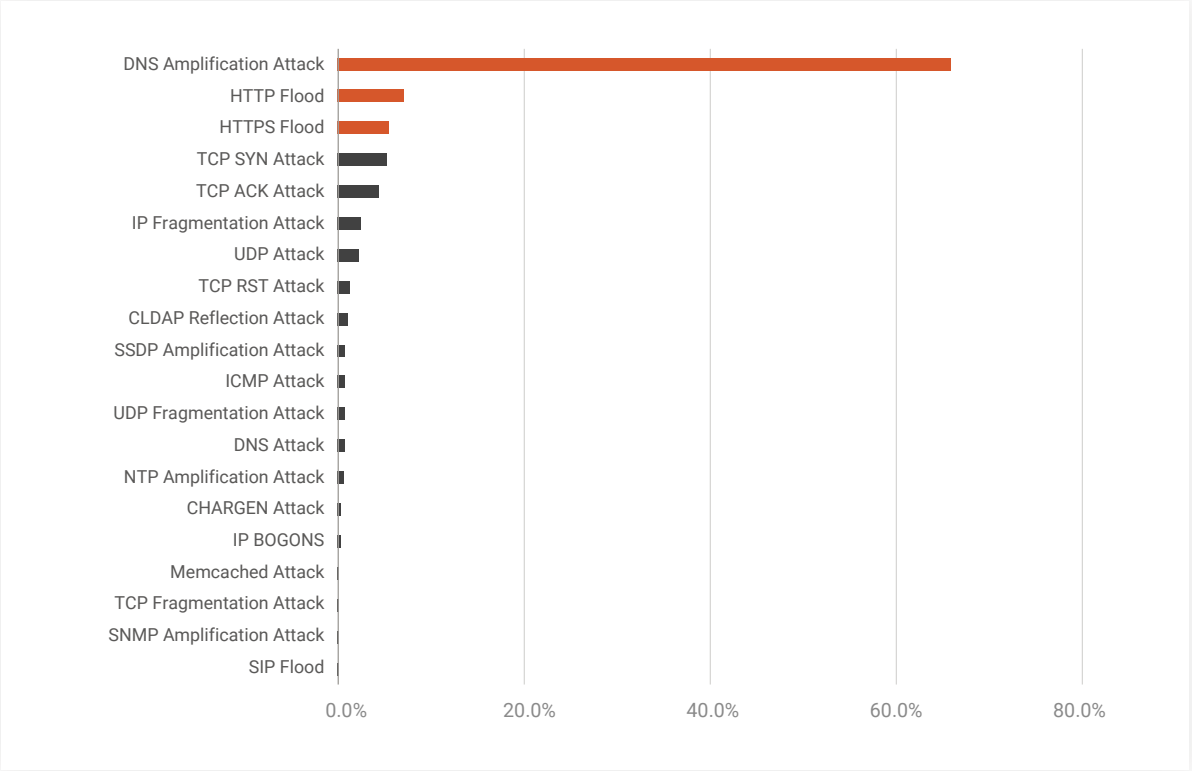

Figure 3. Distribution of DDoS Attack Vectors , Q2 2019

2 Attacks on network Layers 3 and 4 lasting at least five minutes at a size equal to or larger than 100Mbps were counted as volumetric attacks. Attacks targeting applications lasting at least five minutes with at least 500 requests per sec. were counted as application attacks. Attack vector counts measure the number of vectors exploited by the same attack on the same destination IP. An attack is defined as one or more events occurring within a time interval of five minutes. In the same attack, each vector is counted once no matter how many times it is targeted as long as the attacks occurred within the five-minute interval. As for Bit-and-Piece attacks, they are counted as a single attack based on a network-based destination IP address rather than a host-based destination IP address.

Top 3 Attack Vectors

No.1 DNS Amplification

65.95 %

8,382

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 sizable response can be created by a very small request, an attacker can leverage this tactic to amplify attacks with a maximum amplification factor of 54.

No.2 HTTP Flood

7.14 %

908

Here attackers attempt to exhaust server resources by generating valid, volumetric HTTP requests or sessions. The most commonly used method to launch such attacks is HTTP GET flooding. Attackers can either initialize a large number of valid sessions or send a large number of requests in a single session to inundate the victim's web servers with answer requests. The process forces servers to allocate maximum resources to handle traffic so normal requests cannot reach them.

No.3 HTTPS Flood

5.74 %

695

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.

Quantity of Attack Vectors

Single-vector attacks dominated with 63.56% of the total, while multi-vectors accounted for the rest. Two- and three-vectored attacks accounted for 13.56% and 8.71%, respectively. The maximum number of vectors used was 13.

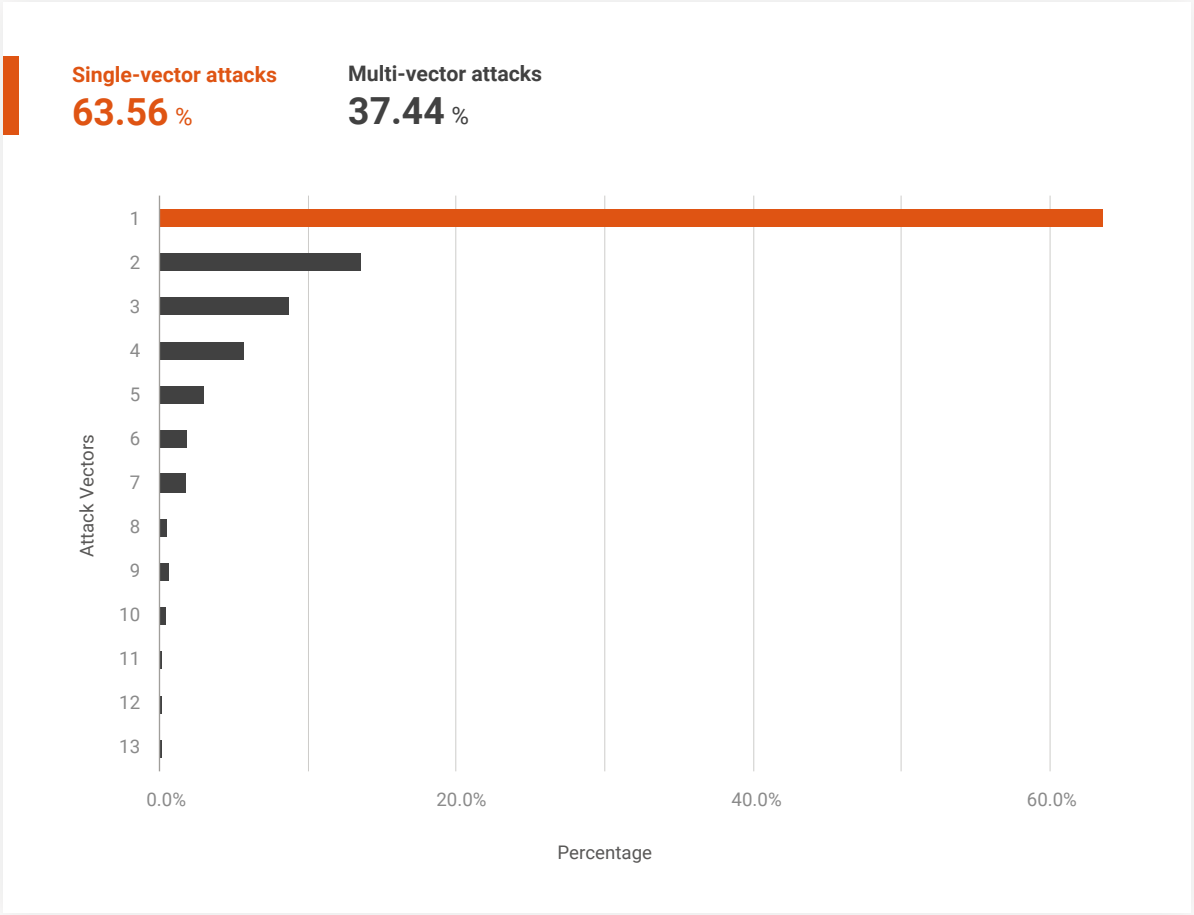

Figure 4. Distribution of DDoS Attack Vectors, Q2 2019

Attack Durations[3]

74.18% of attacks lasted fewer than 90 minutes. 2.42% lasted more than 1,200. The quarterly average was 182.9 minutes, while the longest attack lasted 28 days, 1 hour, and 11 minutes. In the quarter, the average duration dropped by 65.57% (QOQ) and 42.50% (YOY) and the maximum duration fell by 3.76% (QOQ) while rising 467.97% (YOY).

<90 minutes
74.18 %

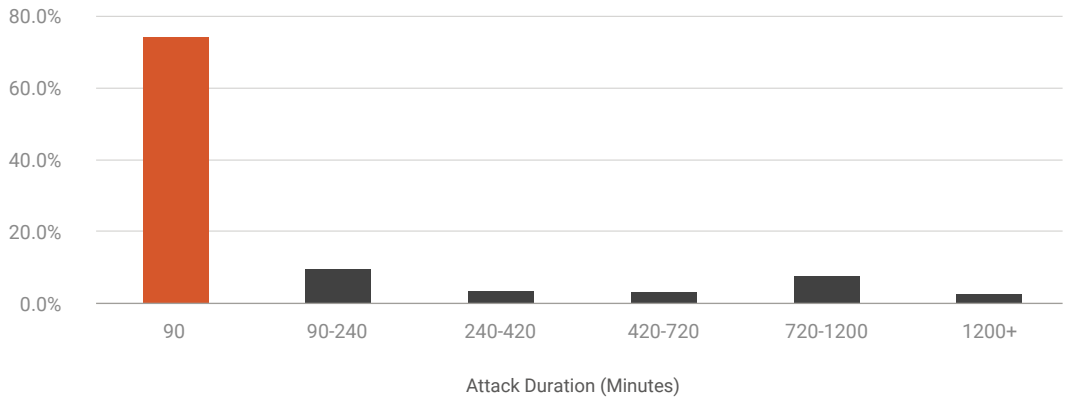

Figure 5. Attack Durations (Shorter than 1,200 Minutes), Q2 2019

>1200 minutes
2.42 %

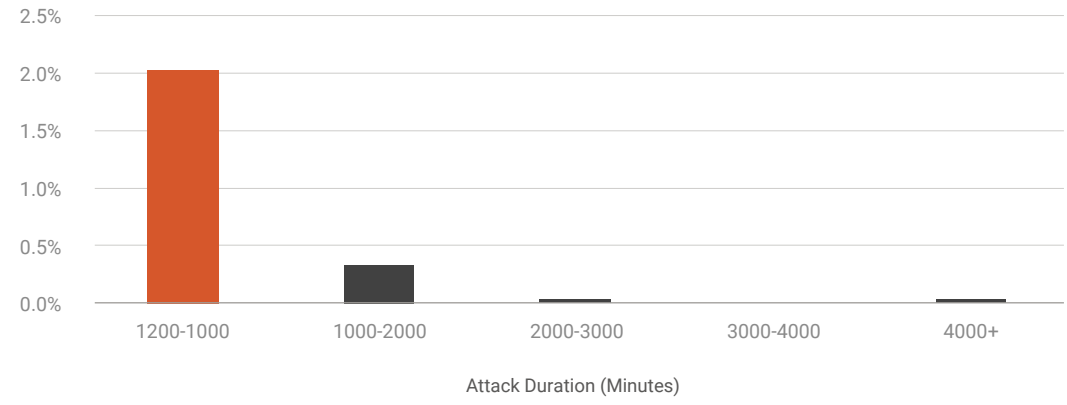

Figure 6. Attack Durations (Longer than 1,200 Minutes), Q2 2019

3 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. As for Bit-and-Piece attacks, they are counted as a single attack based on a network-based destination IP address rather than a host-based destination IP address.

Attack Size Distribution[4]

In the quarter, 97.79% of attacks were smaller than 10Gbps and a full 91.58% smaller than 1Gbps — those ranging between 1Gbps and 10Gbps accounted for only 6.21%. Maximum size dropped by 18.91% while the average rose 17.71% (QOQ). YOY, both maximum and average sizes fell by 67.16% and 98.33%, respectively.

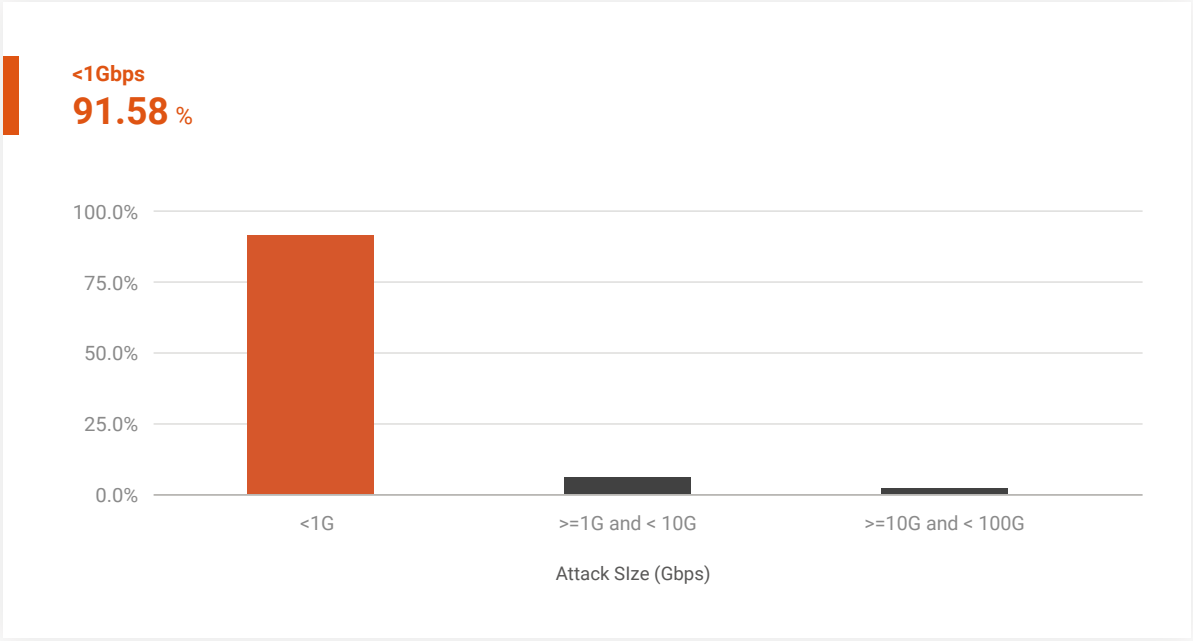

Figure 7. Attack Size Distribution, Q2 2019

4 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. As for Bit-and-Piece attacks, they are counted as a single attack based on a network-based destination IP address rather than a host-based destination IP address.

Global Attack Source Distribution[5]

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

Regions	Percentage
United States of America	22.80%
China	13.70%
Vietnam	8.70%
Russian Federation	5.13%
France	3.83%
Egypt	3.52%
Brazil	3.50%
Germany	3.38%
Netherlands	3.20%
South Korea	2.52%
Others (113 regions)	29.72%

Table 3. Global Attack Source Distribution, Q2 2019

5 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. As for Bit-and-Piece attacks, they are counted as a single attack based on a network-based destination IP address rather than a host-based destination IP address.

APAC Attack Source Distribution[6]

As a leading global attack source, China is also a leader of the pack in APAC, followed by Vietnam, Thailand, and India.

Regions	Percentage
China	43.19%
Vietnam	27.41%
Thailand	5.35%
India	4.96%
Indonesia	4.30%
Singapore	3.59%
Hong Kong	2.15%
Taiwan	2.10%
Lao People's Democratic Republic	1.82%
Malaysia	1.27%
Others (9 regions)	3.86%

Table 4. APAC Attack Source Distribution, Q2 2019

6 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. As for Bit-and-Piece attacks, they are counted as a single attack based on a network-based destination IP address rather than a host-based destination IP address.

Global Attack Sources by Autonomous System Number (ASN)

Attacks emanating from ASNs in the US and Vietnam top the list. China and Egypt are also key contributors.

ASN	Network Name	Percentage
1406	DIGITALOCEAN-ASN - DigitalOcean, LLC, US	16.29%
45899	VNPT-AS-VN VNPT Corp, VN	6.13%
4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	3.66%
8452	TE-AS TE-AS, EG	3.35%
16276	OVH, FR	2.40%
45090	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	2.06%
4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	1.60%
15169	GOOGLE - Google LLC, US	1.57%
42610	NCNET-AS, RU	1.57%
16509	AMAZON-02 - Amazon.com, Inc., US	1.43%
Others	1,131 ASNs	59.94%

Table 5. Top 10 ASN Attack Rankings, Q2 2019

End Notes

The Domain Name System (DNS) is a foundational element of the Internet that translates domain names into corresponding IP addresses. DNS queries and responses are UDP-based, and domain name data is intended to be available to anyone on the Internet. By contrast, Memcached services (SSDP or CLDP) are part of the intranet and are not supposed to be open to the public.

DNSSEC fixes one problem, but creates another: The growing adoption of DNSSEC suggests that DNS Amplification will continue to pose a significant threat to service provider and enterprise networks alike. Long overdue, the deployment of DNSSEC as the ultimate patch for fixing DNS cache poisoning is finally gaining widespread acceptance. The downside is the exceptionally long responses DNSSEC-enabled servers generate. The long DNS responses include records containing cryptographic keys and/or signatures. When a domain is upgraded to support DNSSEC, it returns traditional records as well as DNS records. As a result, the sizes of DNSSEC-enabled DNS responses significantly exceed those of traditional responses. Such responses are often abused by attackers to launch amplification attacks that clog victim networks and hosts. We believe that telcos and DNS providers are inevitably affected the most as they are both vital to public internet access. If history is any guide, the tactics to abuse DNS server vulnerabilities will continue to evolve, suggesting that advanced DNS protection ought to be always in place.

Protection against DNS Amplification is essential: As predicted in Nexusguard's Q4 2017 Threat Report, a new class of powerful botnets has emerged as a result of wider DNSSEC adoption. Its continued deployment exposes DNS servers to an elevated risk of reflecting amplification attacks. When DNS Amplification targets a CSP network, it's not realistic to drop all DNS associated attack traffic — because end-users rely on DNS services to access the Internet. And blocking all incoming DNS response traffic means that legitimate attempts will be denied, thereby having a DDoS effect on paying customers. To distinguish bona fide requests from suspicious attempts, advanced DNS Amplification attack mitigation capabilities, such as those provided by Nexusuguard, must be in place to ensure server availability to legitimate end-users.

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

20190905-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