NEXUSGUARD®

Threat Report

Distributed Denial-of-Service (DDoS)

Q1 2017

Contents

1. Methodology

As the 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. Data is gathered via botnet scanning, Honeypots, ISPs, and traffic moving between attackers and their targets. The analysis conducted by Nexusguard and our research partner, attackscape.com (https://www.attackscape.com/), identifies vulnerabilities and measures attack trends worldwide to provide a comprehensive view of DDoS threats.

Attacks and hacking activities exert a sizeable 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 our quarterly reports.

2. Key Observations for Q1 2017

- In Q1 2017, the number of DDoS attacks observed by Nexusguard registered a 380% year-on-year growth, suggesting that DDoS attacks occurred more frequently than the same period a year ago. It can be concluded that the impact of seasonal factors on attack frequency has become less apparent.
- Uncommonly fierce attacks were observed in Q1 2017 — much more so than in preceding quarters. An enormous 275Gbps attack took place during Valentine's Day and a lengthy attack spanning 4,060 minutes occurred over the Chinese New Year.
- The percentage of days with sizeable attacks (larger than 10Gbps) grew considerably between January (48.39%) and March (64.29%).
- HTTP attack counts and total attack counts increased over Q4 2016 by 147.13% and 37.59% respectively.

3. Quarterly Focus: Attackers Don't Go on Vacation During Holidays

As noted in our Q4 2016 report, 200+Gbps attacks have become commonplace. Such large-scale attacks continued this quarter, but now with more frequency, longer durations, and greater complexity, especially with the increased use of HTTP GET/POST flood to target the application layer. Multi-vector attacks in the form of advanced persistent threats (APT) also became more common. During Q1, attackers didn't take a break for any holidays.

3.1 Holidays Are No Longer Peaceful

Prior to 2017, attacks were not common in the year's first quarter. This year, however, the magnitude and frequency of attacks reached an unprecedented level. Two attacks with the largest size and duration ever were tracked during Q1 holidays in APAC and the West.

3.2 A New Years Nightmare

In APAC, a lengthy attack January 28-31, the period of Chinese New Year, lasted 2 days, 19 hours, and 40 minutes. It was a widespread, disruptive event that left celebrants weary and exhausted upon returning to work.

3.3 Heavy Hits on the Day of Romance

In the West, an attack over Valentine's Day (February 14-15) lasting 21 hours and 31 minutes spiked up to 275.77Gbps. It was an unusual event in that Valentine's Day had not been targeted previously.

3.4 Attack Frequency Changes

Q1 2017 saw increased frequency of DDoS attacks compared with corresponding quarters in 2015 and 2016, during which attacks were less scalable and frequent. 2017 attack counts increased by 231.12% over Q1 2015 and 379.84% over Q1 2016. The turning point, when gigantic, continuous attacks began to wreak havoc, appears to be Q4 2016, reflecting a ripple effect of increased Botnet activity that occurred in the year's final quarter.

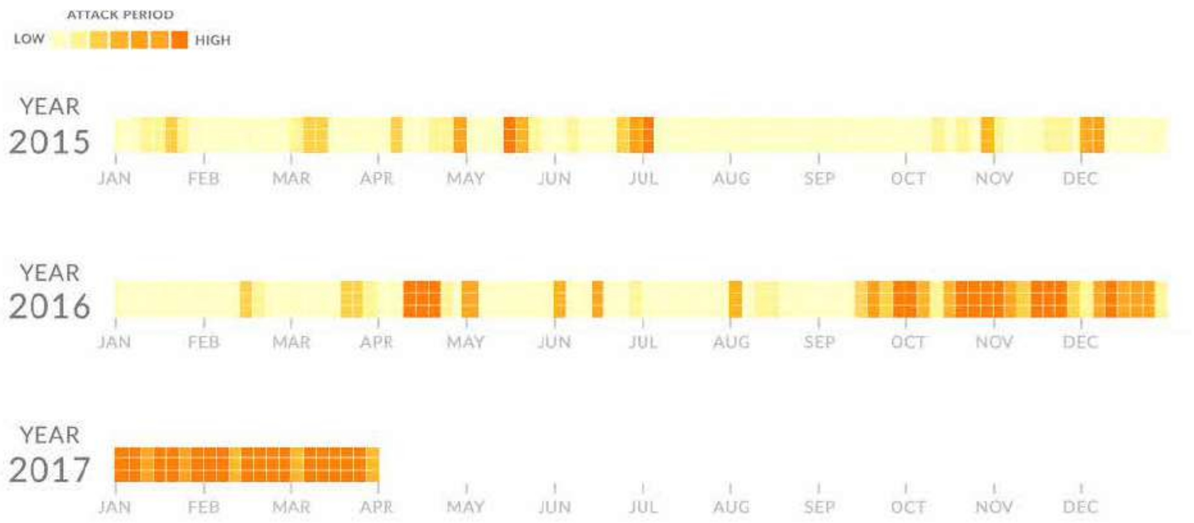

Figure 1. Attack Frequency in Q1 — 2015 through 2017

4. DDoS Activities

4.1 Types of Vectors

In Q1 2017, 21 attack vectors were identified in 16,641 attacks. HTTP Flood was the predominant type, contributing 24.36%. TCP Flag Invalid Attack took second place at 20.28%. TCP SYN Attack and UDP Attack were the third and fourth leading vectors with 17.17% and 13.85% respectively.

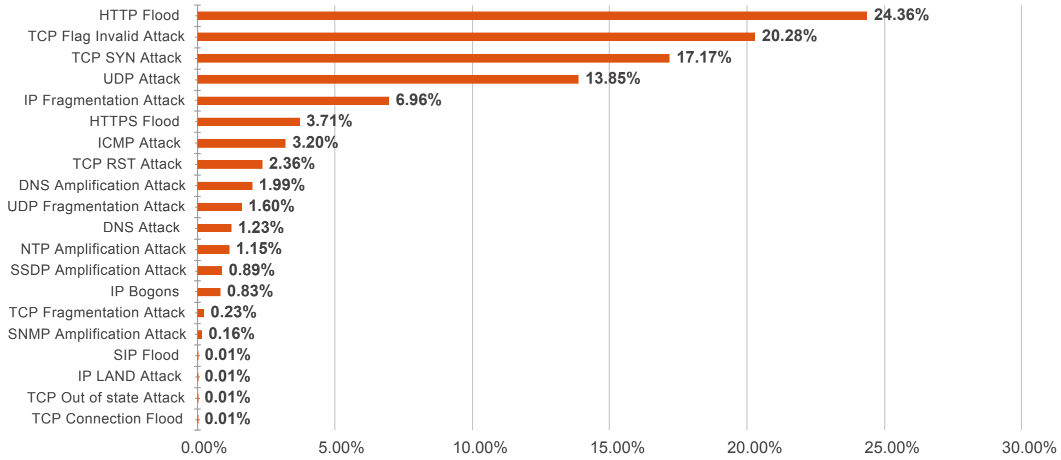

Figure 2. Distribution of DDoS Attack Vectors

The total number of attacks in Q1 2017 jumped 37.59% over Q4 2016. HTTP attacks proliferated, showing an increase of 147.13% in the quarter. Application layer attacks encompassing HTTP Flood (86.77%) and HTTPS Flood (13.23%) soared as predicted in our Q4 2016 threat report. 93.75% of the attacks were mixed with volumetric and application aspects, whereas only 6.25% were pure application attacks. Since they call for multi-layered defense mechanisms, which are costly and, therefore, target enterprises have yet to upgrade their DDoS attack mitigation solutions to in order protect their online resources from the growing threat of multi-vector DDoS attacks.

	Q4 2016	Q1 2017	Percentage of Attacks Q1 2017 over Q4 2016
HTTP Attack Counts	1640	4053	147.13%
Total Attack Counts	11514	15842	37.59%

Table 1. Comparison of Attacks - Q4 2016 and Q1 2017

4.2 Quantity of Attack Vectors

Multi-vector attacks played the leading role in Q1 2017. 31.08% of attacks were single vector, while the rest were multi-vector.

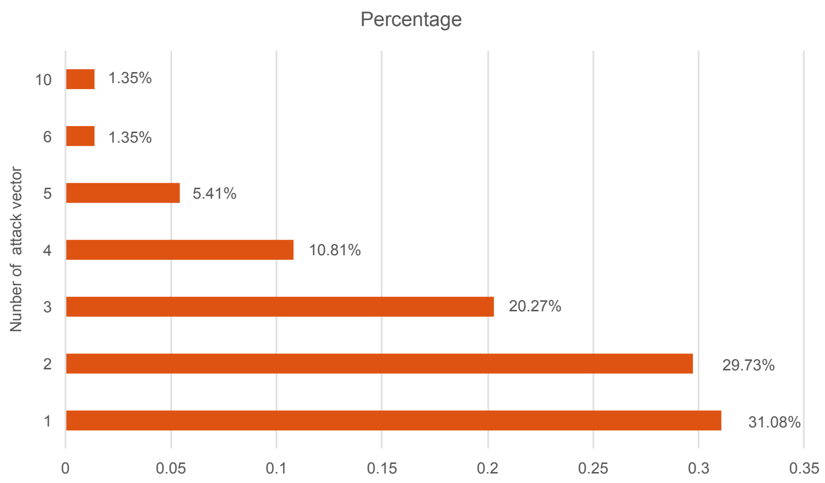

Figure 3. Distribution of Attack Vectors in Q1 2017

4.3 Attack Duration

More than 48% of attacks lasted longer than 90 minutes: 22.97% were between 91 and 240 minutes, and 12.16% between 241 and 420 minutes. 4.05% of attacks exceeded 1,400 minutes.

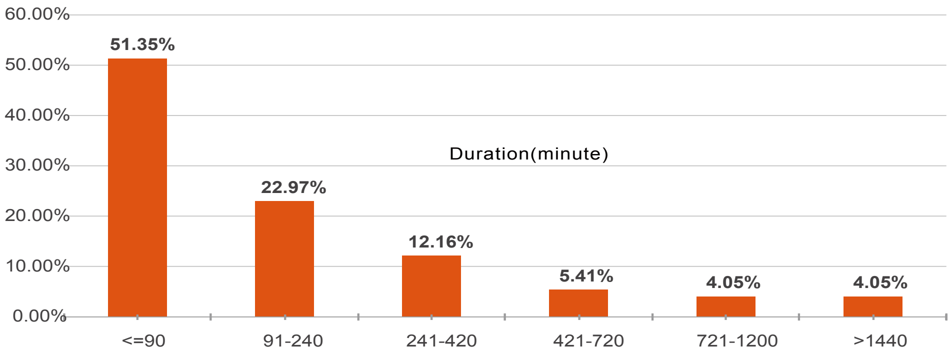

Figure 4. Distribution of Attack Duration

4.4 Attack Size Distribution

Of the attacks recorded in the quarter, more than 22% were sizeable (larger than 10Gbps): 20% ranging between 10Gps - 200Gps, and 2.67% larger than 200Gps.

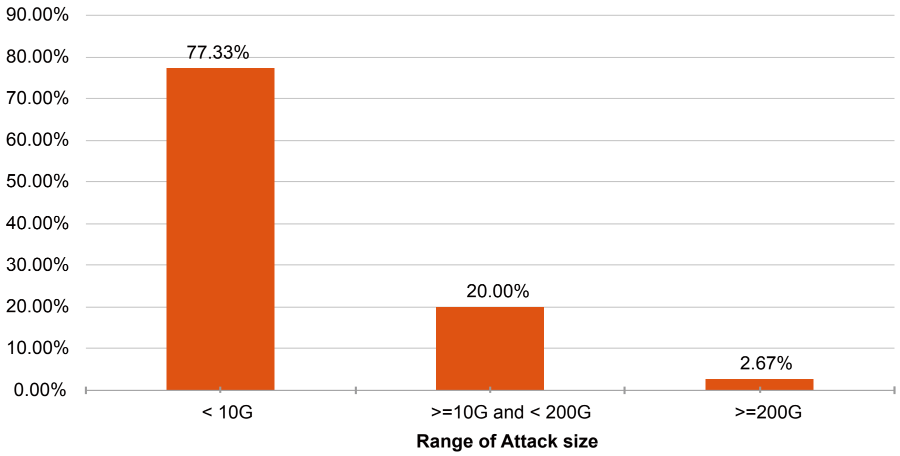

Figure 5. Distribution of Attack Sizes

4.5 Global Attack Source Distribution

The US was the leading source of attacks, being the originating point of 23.75% of attacks in Q1. China and Japan followed, with 17.83% and 15.35% respectively. Germany and France vied for a spot in the Top 5, accounting for 7.78% and 6.69%.

Country	Percentage
United States	23.75%
China	17.83%
Japan	15.35%
Germany	7.78%
France	6.69%
Netherlands	3.90%
Russian Federation	3.72%
United Kingdom	2.48%
Canada	2.37%
Romania	2.16%
Others (Including 96 countries)	13.96%

Table 2. Percentage of Attack Source over Worldwide

4.6 APAC Attack Source Distribution

In APAC, China was ranked No. 1, being the source of 50.34% of attacks in the region. Japan took the second place with 43.34%. Vietnam, Singapore, South Korea and Taiwan followed Japan with 1.82%, 1.28%, 1.23% and 1.09% respectively.

Country	Percentage
China	50.34%
Japan	43.34%
Vietnam	1.82%
Singapore	1.28%
South Korea	1.23%
Taiwan	1.09%
Hong Kong	0.81%
Malaysia	0.04%
Indonesia	0.02%
Philippines	0.01%
Others (Including 4 countries)	0.02%

Table 3. Percentage of Attack Source among Asian Countries

4.7 Reflective DDoS Attacks by Autonomous System Number (ASN)

AS-PNAPTOK placed first among all network ASNs with 30.58%. Second and third were PROXAD and CHINANET-BACKBONE with 11.96% and 11.17% respectively.

AS Number	Network Name	Percentage
17675	AS-PNAPTOK	30.58%
12322	PROXAD	11.96%
4134	CHINANET-BACKBONE	11.17%
9808	CMNET-GD	8.21%
23650	CHINANET-JS-AS-AP	7.72%
7922	COMCAST-7922	7.32%
7018	ATT-INTERNET4	5.96%
16276	OVH	5.79%
63949	LINODE-AP	5.66%
31400	ACCELERATED-IT	5.64%

Table 4. ASN Rankings with Attack Size

5. Conclusions

DDoS attacks are no longer concentrated over predictable periods. Holiday or long weekend — no matter, the attackers never rest. The patterns are more erratic, the techniques more complex, and the attacks last longer and tend to target multiple vectors. During Q1 2017, application-layer attacks like HTTP GET/POST Flood predominated, overtaking volumetric-based attacks.

Furthermore, over the past few years, the increasing adoption of Internet of Things (IoT) has resulted in a massive number of poorly guarded, unsecured devices. The exploitation of the resulting vulnerabilities has fueled the rapid growth of Botnets, which in turn are supplying attackers with myriad hijacked IP addresses, enabling them to launch more long-lasting, sophisticated attacks.

To combat these increasingly complex DDoS attacks, which often target multiple vectors at the same time, a multi-layered mitigation platform that leverages a large, redundant scrubbing network with the support of a 24x7 security operations center (SOC) is much needed.

NEXUSGUARD®

Global Leader in DDoS Mitigation

About Nexusguard

Founded in 2008, Nexusguard is the global leader in fighting malicious Internet attacks. Nexusguard protects clients against a multitude of threats, including distributed denial of service (DDoS) attacks, to ensure uninterrupted Internet service. Nexusguard provides comprehensive, highly customized solutions for customers of all sizes, across a range of industries, and also enables turnkey anti-DDoS solutions for service providers. Nexusguard delivers on its promise to maximize peace of mind by minimizing threats and improving uptime. Visit www.nexusguard.com for more information.

456 Montgomery Street, Suite 800 San Francisco, CA 94104 USA | +1 415 299 8550

nexusguard.com

20170809-EN-A4