IMPERVA®

DDOS REPORT

Global DDoS Threat Landscape

Q1 2017

More and more assaults occurred in bursts

80 percent of all attacks lasted less than an hour. 90.5 percent of network layer attacks lasted under 30 minutes.

Network layer attacks grew more complex

40.5 percent of all attacks were multi-vector assaults, compared to 29 percent in Q4 2016.

74 percent of targets suffered repeat assaults

19 percent were attacked 10 times or more, up by 13.1 percent from Q4 2016.

The US, South Korea and China topped the attacking country list

The three countries accounted for 68.8 percent of all DDoS attack requests.

Overview

For the fourth quarter in a row we saw a decrease in the number of network layer assaults, which fell to 269 per week compared to 568 in Q2 2015. In contrast, we saw yet another spike in the number of application layer assaults, which reached an all-time high of 1,099 per week.

The largest application layer attack we mitigated this quarter peaked at over 176,000 RPS—already higher than the largest attack we saw in 2016, which peaked at approximately 173,000 RPS.

On a macro level DDoS assaults grew shorter, but also more complex and persistent. 80 percent of all attacks lasted less than an hour, and for the first time more than 90 percent of network attacks lasted under 30 minutes. Meanwhile, the number of repeat assaults reached an all-time high with 74 percent of targets attacked on multiple occasions.

The increase in attack complexity was reflected in the rise in multi-vector threats, which accounted for 40.5 percent of all network layer DDoS assaults—a steep increase from "just" 29 percent in the previous quarter.

China, the United States and South Korea continued to top the attacking country list, serving as points of origin for 68.8 percent of all DDoS attack requests. Most of the attacks (50.8 percent) originated in China, followed by South Korea (10.8 percent) and the United States (7.2 percent).

Highlights

Network Layer Attacks

- Largest attack peaked at 270 Gbps and 85 Mpps
- Number of attacks decreased to 280 a week
- Multi-vector attacks were up to 40 percent

Application Layer Attacks

- Number of attacks increased to 1,099 a week
- Largest attack peaked at 176,393 RPS
- 74 percent of targets were hit by repeat assaults

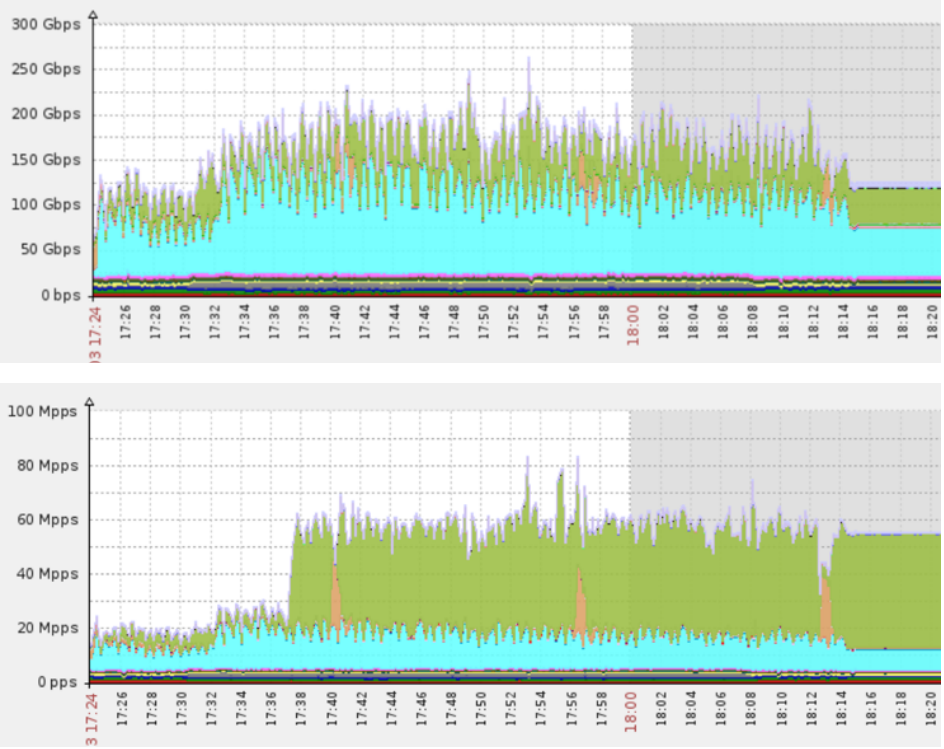
DDoS Botnet Activity

- 50.8 percent of assault traffic originated from China
- 10.8 percent of assault traffic originated from South Korea
- US, UK and Japan were the top three attacked countries

Network Layer Attacks

In Q1 2017, Imperva Incapsula mitigated an average of 266 network layer attacks per week, a slight decrease from the 280 attacks per week we saw in the previous quarter. This was the third consecutive quarter of declining network layer assaults after they peaked in Q2 2016.

In contrast to Q4 2016, when we mitigated a record-high 650 Gbps assault, Q1 2017 saw a decrease in network layer attack sizes. While we continued to mitigate multiple 100+ Gbps assaults, the largest peaked at 270 Gbps and 85 Mpps.



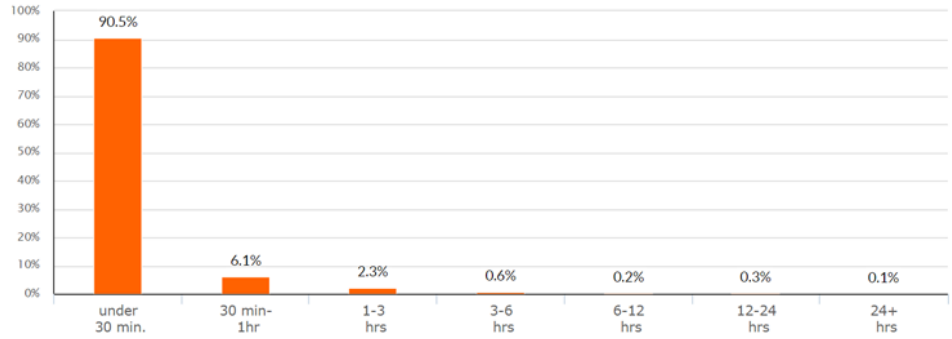
The largest network layer attack in Q1 2017 peaked at 270 Gbps and 85 Mpps

Average attack duration dropped from 100 minutes in Q4 2016 to 29 minutes in Q1 2017—a result of the steep increase in short burst attacks.

For the first time, over 90 percent of all attacks lasted under 30 minutes (12.3 percent higher than Q4 2016), while only 0.1 percent of attacks continued for more than 24 hours. The longest attack of the quarter persisted for less than nine days, compared to the over 29-day assault we saw in Q4.

In addition, Q1 2017 was characterized by a marked increase in multi-vector assaults. Over 40 percent of attacks employed two or more vectors, as opposed to 29 percent in Q4 2016.

Attack duration



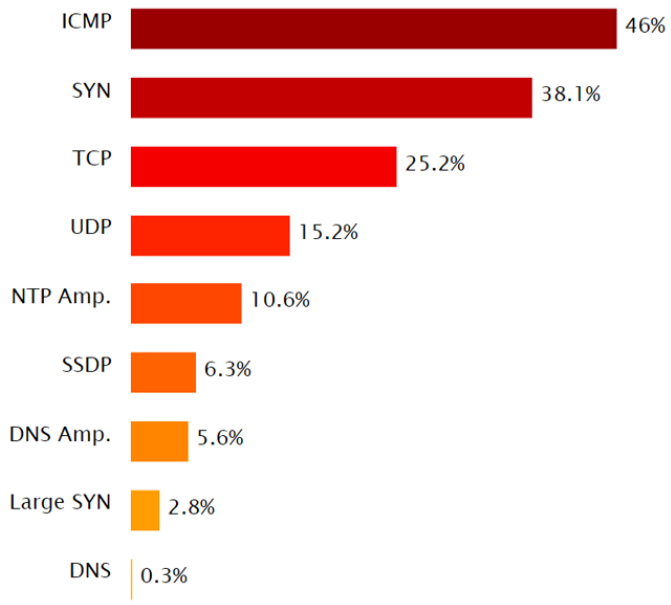
Distribution of network layer DDoS attacks, by duration

In Q1 2017, we saw a continuation of the trend toward short attack bursts, with 96.6 percent of DDoS events lasting under one hour.

This was the first quarter in which over 90 percent of attacks lasted less than 30 minutes, compared to 78.2 percent in Q4 2016. This can be attributed to the widespread availability of botnet-for-hire (a.k.a. stresser or booter) services, which are used by non-professionals to launch short-lived assaults for as little as five dollars per assault.

Consistent with this trend, the relatively few persistent attacks that we mitigated also decreased in duration. In Q1 2017, the longest attack lasted approximately 204 hours, compared to Q4 (approximately 700 hours) and Q3 (483 hours) of 2016.

Attack vectors



Distribution of network layer DDoS attacks, by attack vector

Similar to previous quarters, perpetrators continued to use a wide variety of payloads (network packets) to carry out network layer assaults in Q1 2017. ICMP floods continued to be the most prevalent attack type, appearing in 46 percent of all network layer assaults. SYN floods were used in 38.1 percent of attacks—an increase of more than 16 percent from last quarter. SSDP floods increased from 4.2 percent in Q4 2016 to 6.3 percent in Q1 2017.

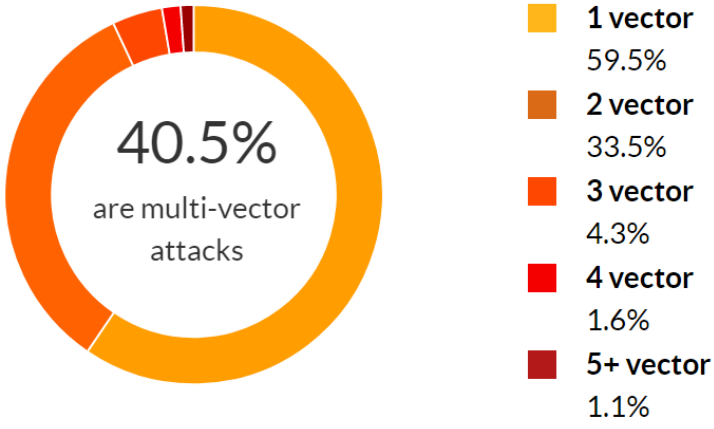
After trending down for the entirety of 2016, NTP amplification attacks made a comeback, growing by 3.7 percent as compared to Q4 2016.

Multi-Vector Attacks

For the first time since Q3 2015, over 40 percent of network layer attacks were multi-vector assaults. By comparison, the figure came in at 29 percent in Q4 2016.

The bulk of these sophisticated attacks were two-vector attacks (33.5 percent), with ICMP and SYN floods the most common combination (24.8 percent).

The rise in multi-vector assaults reflects the sophistication and technical know-how of today's tech-savvy offenders.



Distribution of network layer DDoS attacks, by number of vectors used

Application Layer Attacks

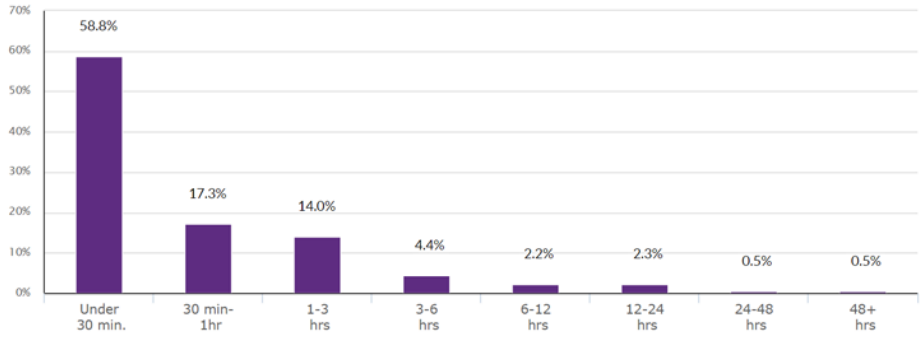
The largest application layer attack this quarter peaked at 176,393 RPS (requests per second), exceeding last year's high in Q3 of 173,633 RPS. The longest assault lasted "only" 19 days, compared to the 47-day DDoS barrage in Q4 2016 and the record-setting 67-day assault in Q2 2016. offenders Such attack tools are commonly used by non-professional offenders, often internet trolls who use DDoS to settle a personal dispute or to simply harass their victims.

On average, the Incapsula service mitigated 1,099 application layer attacks per week in Q1 2017. This marks a significant 28.4 percent increase from Q4 2016 (after factoring in our user base growth) and the fourth consecutive quarter in which we recorded an increase in application layer attacks.

The rise in attacks was partially driven by a large number of hit-and-run assaults on a small number of sites. Specifically, ten customers experienced over 200 attacks throughout the quarter. One of these customers—a popular science news website—was hit 1,046 times, mostly by low-volume bursts lasting 10 minutes or less.

Extreme cases aside, Incapsula recorded an all-time high for attack frequency, with 74 percent of targets attacked more than once during the quarter. Notably, 19 percent of all targets were attacked 10 times or more—the highest level we've ever seen in this category.

Attack duration and frequency



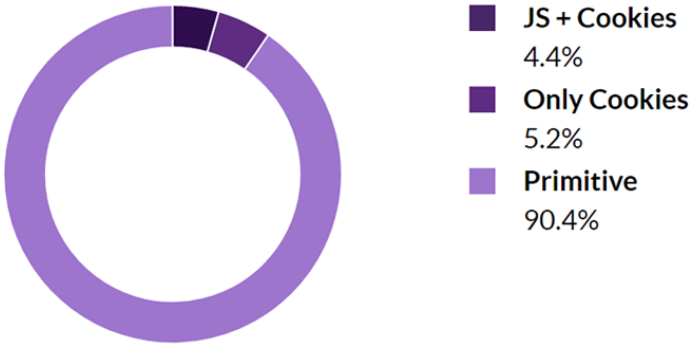
Distribution of application layer DDoS attacks, by duration

Consistent with the above-mentioned trend, average attack duration fell to 53 minutes in Q1 2017. This was the first quarter ever that average attack duration was less than two hours. Still, the overall duration distribution continued to resemble that of Q4 2016.

The decrease in attack duration correlated neatly with the steep increase in attack frequency. When combined, these trends point to yet another increase in the number of short-lived attack bursts, resulting from DDoS-for-hire activity and hit-and-run attack tactics.

Distribution of application layer attacks, by frequency

DDoS bot capabilities and assumed identities



Distribution of application layer attack sessions, by bot capabilities

In Q1 2017, almost 10 percent of bots showed some type of advanced capabilities for bypassing security countermeasures. This represents a slight decrease from the previous quarter, in which 13.6 percent of bots were able to retain cookies and/or execute JavaScript.

Primitive bots remained dominant, reflecting the type of attacks typically associated with botnet-for-hire services.

Assumed Identities

	Q1
Internet Explorer	48.8%
Firefox	29.1%
Chrome	7.7%
Baidu Spider	7.7%
Android Browser	0.6%
Opera	0.3%
Safari	0.2%
Googlebot	0.1%

To evade detection by less sophisticated mitigation services, DDoS bots use fake user agents to assume legitimate tool and browser identities.

While Microsoft's Internet Explorer browser bot continued to be the most impersonated tool, its share of the pie became much smaller, dropping from 72 percent in Q4 2016 to 48.8 percent in Q1 2017. In contrast, the use of fake Firefox browser bots grew from 5.5 percent in Q4 to 29.1 percent this quarter.

Botnet Activity and Geolocation

Top Targeting and Attacking Countries

Top Attacking Countries

China	**50.8%**
South Korea	10.8%
United States	7.2%
Egypt	3.2%
Hong Kong	3.2%
Vietnam	2.6%
Taiwan	2.4%
Thailand	1.6%
United Kingdom	1.5%
Turkey	1.4%

Top Targeted Countries

United States	**92.7%**
United Kingdom	2.3%
Japan	1.8%
Netherlands	1.6%
Singapore	0.8%
Germany	0.4%
Israel	0.3%
Australia	0.2%
Hong Kong	0.1%

While the United States remained the most attacked country, its predominance in Q1 2017 was clearly influenced by the hit-and-run barrage against a small number of US-based websites, including the previously mentioned science news site. Notably, many of the US-based websites used AWS-hosted services.

For the first time in the past year, Singapore and Israel joined the most attacked countries list. The United States, United Kingdom and Japan continued to top the list, as they generally have since our report was first issued in Q3 2015.

Once again China led the list of attacking countries, however its share of total attacks dropped by 27.7 percent from Q4. This vacuum was filled by the resurgence of South Korea and the United States, whose powerful internet infrastructure and widespread broadband connectivity are attractive to DDoS perpetrators.

While it's rare to see Middle Eastern countries on this list, both Egypt and Turkey were among the top ten attacking countries in Q1 2017.

Methodology

Our analysis is based on data from 3,457 network layer and 14,122 application layer DDoS attacks on websites using Imperva Incapsula services from January 1, 2017, through March 31, 2017—referred to herein as the first quarter of 2017 or Q1 2017.

Information about DDoS bot capabilities and assumed identities comes from a random sample of 22.49 billion DDoS bot requests collected from such assaults over the same period.

Definitions

DDoS attack – A persistent, distributed denial of service event against the same target (e.g., IP address or domain). It's usually preceded by a quiet (attack free) period of at least ten minutes, and followed by another quiet period of the same duration or longer.

Network layer attack – An assault against either the network or transport layers (OSI layers 3 and 4). Its goal is to cause network saturation by expending much of the available bandwidth. It's typically measured in gigabits per second (Gbps), referring to the amount of bandwidth it can consume per second.

Application layer attack – An assault occurring on OSI layer 7. Its goal is to bring down a server by exhausting its processing resources (e.g., CPU or RAM) with a high number of requests. It's measured in requests per second (RPS)—the number of processing tasks initiated per second. Such attacks are executed by DDoS bots able to establish a TCP handshake to interact with a targeted application.

Botnet – A cluster of compromised, malware-infected devices remotely controlled by an offender. Device owners are unaware of their system participation.

DDoS bot – A malicious software application (script) used by a perpetrator. So-called bad bots only come into play in application layer attacks, where a TCP connection is established. They typically masquerade as browsers (human visitors) or legitimate bots (e.g., search engine crawlers) to bypass security solutions.

Payload – In the context of this study, a payload is a packet type used in a network layer assault. It's fabricated by an attack script and can often be altered on the fly. In many cases, multiple payload types are used simultaneously during the course of a single event.

What's next

- To learn more about the business effects of DDoS attacks, read this free DDoS Impact Report.
- To estimate the potential cost of DDoS to your business, use our free DDoS Cost Calculator.
- For more information about Incapsula DDoS protection services, visit www.incapsula.com.

IMPERVA INCAPSULA

About Imperva Incapsula

Imperva Incapsula is a cloud-based application delivery service that protects websites and increases their performance, improving end user experiences and safeguarding web applications and their data from attack. Incapsula includes a web application firewall to thwart hacking attempts, DDoS mitigation to ensure DDoS attacks don't impact online business assets, a content delivery network to optimize web traffic, and a load balancer to maximize the potential of web environments.

Only Incapsula provides enterprise-grade website security and performance without the need for hardware, software, or specialized expertise. Unlike competitive solutions, Incapsula uses proprietary technologies such as client classification to identify bad bots, and big data analysis of security events to increase accuracy without creating false positives.