IMPERVA®

DDOS REPORT

Global DDoS Threat Landscape

Q2 2017

Overview

The number of network layer attacks continued to fall in Q2 2017, the fourth consecutive quarterly drop since peaking in Q2 2016. After reaching a record high in Q1 2017, application layer assaults fell to 973 a week this quarter.

We also saw an increase in the frequency of repeat application layer attacks. In total, 75.8 percent of target websites were hit by repeat assaults, the largest percentage we have on record. This was especially true for US based websites, 80.3 percent of which suffered multiple assaults. Moreover, of the 45 targets that suffered 50 or more attacks, 34 were hosted in the US.

Q2 2017 saw the emergence of a new attack tactic, which we nicknamed "pulse wave DDoS" due to the traffic pattern it generates—a rapid succession of attack bursts that split a botnet's attack output, enabling an offender to go after multiple targets. One such attack was also the largest network layer assault we mitigated this quarter, peaking at 350 Gbps (gigabits per second).

China was responsible for 63 percent of attack traffic, once again topping our list of attacking countries. The US (6.4 percent) came in second. Turkey (2.1 percent), Ukraine (1.9 percent) and India (1.8 percent) respectively came in third, fourth and fifth place after each saw a significant increase in DDoS attack traffic originating from their territories.

Highlights

Network Layer Attacks

- Largest attack peaked at 350 Gbps and 70 Mpps
- Number of attacks declined to 196 per week
- Multi-vector attacks dialed back to 21 percent

Application Layer Attacks

- Largest attack peaked at 89,134 RPS
- Number of attacks declined to 973 a week
- 75.8 percent of targets hit by repeat assaults

DDoS Botnet Activity

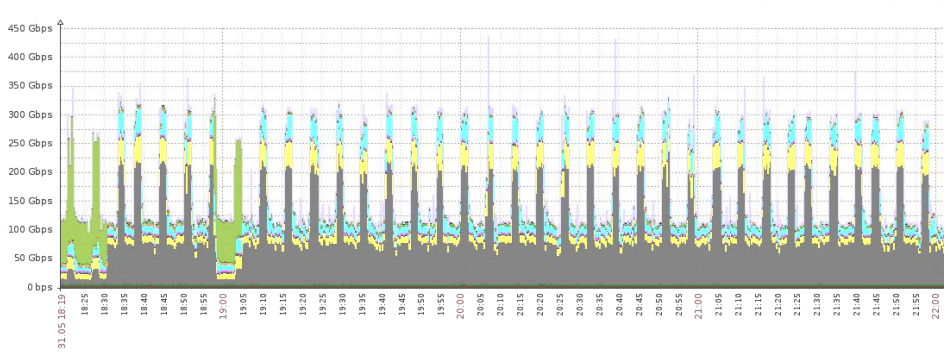
- 63 percent of attack traffic originated in China
- Significant uptick in attack traffic out of Turkey, Ukraine and India
- The US, UK and Spain were the top three attacked countries

Network Layer Attacks

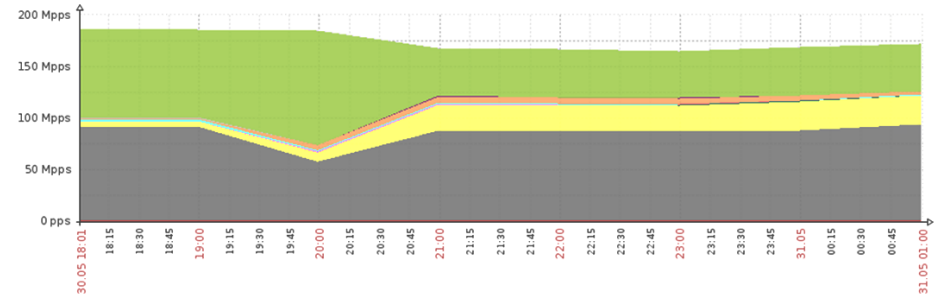
In Q2 2017, Imperva Incapsula mitigated 2,618 network layer attacks, an average of 196 per week, compared to 269 per week in Q1. This represented a 35.9 percent decrease from Q1 2017 and was the fourth consecutive quarterly drop in network layer assaults since they reached their highpoint in Q2 2016.

The trend toward short-lived attacks continued, although at a slightly decreased rate. 82.5 percent of network layer attacks lasted under 30 minutes this quarter, compared to 90.5 percent in Q1 2017.

While the primary reason for these attacks remains botnet-for-hire activity, the emergence of pulse wave DDoS was a contributing factor. One of the pulse wave assaults mitigated in Q2 2017 was also the largest attack of the quarter, peaking at over 350Gbps. The highest rate attack peaked at 200Mpps.



Total Incapsula TRAFFIC - Total Incoming Traffic all Incapsula

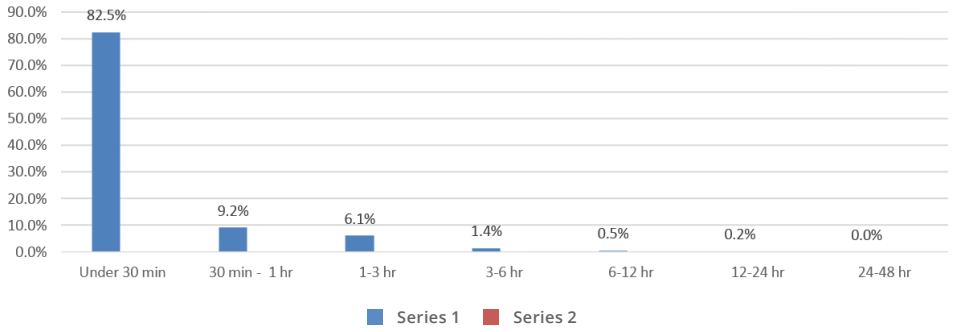


Total Incapsula TRAFFIC - Total Incoming Packets all Incapsula (6h 59m 50s)

The longest attack of Q2 2017 lasted for more than 147 hours, a decrease from the 204-hour assault we mitigated in Q1 2017. Average attack duration, however, increased from almost 29 minutes last quarter to more than 34 minutes this quarter.

After reaching a record high in Q1 2017, the use of multi-vector attacks fell in Q2 2017, largely resulting from a decrease in 2-vector assaults.

Attack duration



Distribution of network layer DDoS attacks, by duration

Q2 2017 saw a continuation of the trend toward short burst attacks (91.7 percent of assaults lasted less than an hour) albeit at a slightly decreased rate from last quarter.

82.5 percent of attacks this quarter were under 30 minutes, down from 90.5 percent in Q1 2017. While the bulk of these attacks can be attributed to botnet-for-hire (a.k.a., stresser or booter) services, pulse wave and probing attempts that occurred before or in between attacks were contributing factors.

The number of attacks lasting more than three hours in Q2 2017 increased to 2.1 percent from 1.2 percent last quarter. Conversely, only eight assaults lasted for more than 12 hours this quarter, compared to 14 last quarter.

Attack vectors

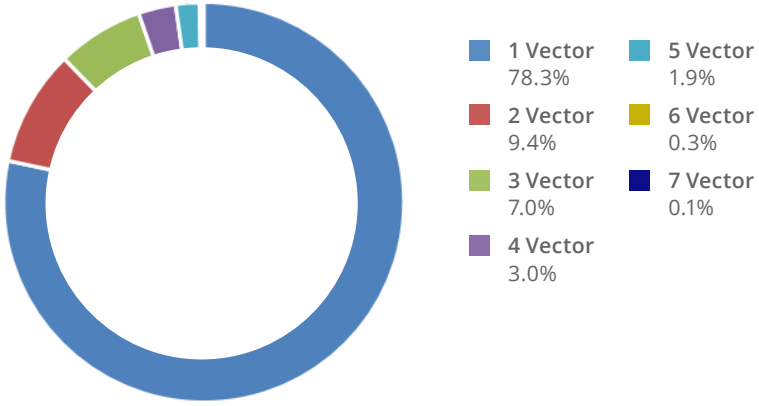
VECTORS	Q2
DNS	1.0%
DNS Amp.	5.0%
ICMP	29.9%
Large SYN	7.1%
NTP Amp.	9.9%
SYN	23.0%
TCP	31.6%
UDP	27.1%
SSDP	5.0%

Distribution of network layer DDoS attacks, by attack vector

Similar to Q1 2017, a variety of payloads were used this quarter to execute network layer attacks, the bulk of which were a combination of ICMP, TCP, UDP and SYN floods. The use of UDP and generic TCP floods increased while ICMP and SYN floods declined.

While NTP and DNS amplification tactics were still used, they were only present in 14.9% percent of attacks.

Multi-Vector Attacks



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

Multi-vector assaults dropped to 21.7 percent in Q2 2017, following last quarter's record high 40.5 percent. This can be attributed to the sharp decrease in 2-vector assaults, which fell from 33.5 percent to 9.4 percent quarter over quarter.

Sophisticated attacks, however, continued to increase. This quarter, 12 percent of assaults consisted of three or more attack vectors, compared to seven percent last quarter. From these, 2.3 percent used five or more vectors, compared to just 1.1 percent in Q1.

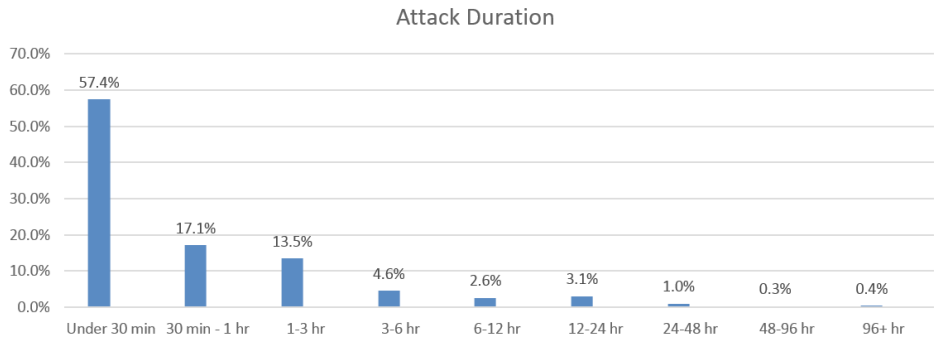
Application Layer Attacks

In Q2 2017, the Incapsula service mitigated 12,825 application layer attacks, an average of 973 attacks per week, compared to 1,099 in Q1. This represented an 18 percent decrease from last quarter, after factoring in the growth in our user base.

The largest application layer attack this quarter peaked at 89,134 RPS (request per second), which was significantly smaller than last quarter's 176,393 RPS attack. This quarter's attack, however, lasted for 48 days, more than twice as long as the one in Q1 2017.

Q2 2017 was notable for the spike in the number of targets (75.8 percent) that suffered from repeat application layer assaults, the highest number that we've ever recorded.

Attack duration and frequency

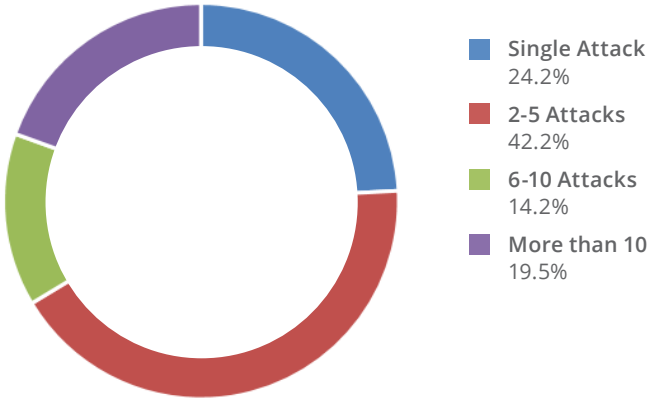


Distribution of application layer DDoS attacks, by duration

Similar to Q1 2017, more than half of all application layer assaults lasted for less than 30 minutes this quarter, albeit at a slightly decreased rate (57.4% in Q2 compared to 58.8% in Q1). That said, the number of persistent attacks increased—7.4 percent lasted more than six hours, compared to 5.5 percent in Q1 2017. Of these attacks, 1.7 percent lasted longer than 24 hours.

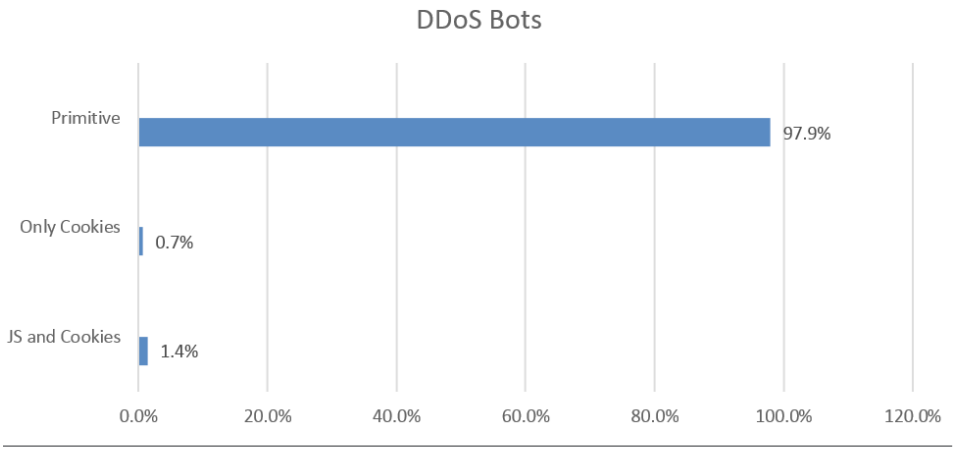
In addition to the increase in persistent attacks, Q2 2017 saw attack frequency reach a record high. On average, a single target was attacked 11.5 times throughout the quarter, while 19.5 percent of targets were hit more than ten times.

Attack frequency



Distribution by frequency of attacks against a target

DDoS bot capabilities and assumed identities



Distribution of application layer attack sessions, by bot capabilities

In Q2 2017, the number of advanced bots capable of bypassing security countermeasures, i.e., retain cookies and/or execute JavaScript, fell to 2.1 percent from 9.6 percent in Q1 2017. Experience shows that this number tends to fluctuate depending on the nature of the botnets used for attacks in a particular month.

In contrast, the number of primitive bots grew from 90.4 percent 97.9 percent quarter over quarter, reflecting an increase in non-sophisticated application layer attacks typically associated with botnet-for-hire services.

Assumed Identities

	Q2
Internet Explorer	55.4%
Chrome	19.1%
Firefox	17.6%
Baidu Spider	3.1%
Safari	1.8%
Opera	0.8%

DDoS bots often try to evade detection by using fake user agents to disguise themselves as legitimate tools and browsers

In Q2 2017, the number of bots masking themselves as browsers, i.e., Internet Explorer, Google Chrome and Firefox increased from 85.6 percent last quarter to 92.1 percent.

The adoption of these 'default' identities is yet another sign of a lack of sophistication among the application layer assault encountered this quarter.

Instead of trying to bypass security measures, attackers preferred to wage wars of attrition with persistent assaults by rudimentary bots.

DDoS Botnet Activity

Botnet Activity and Geolocation

Attacked Countries

United States	**79.7%**
United Kingdom	2.1%
Spain	2.1%
Singapore	1.9%
Hong Kong	1.9%
Ireland	1.8%
Netherlands	1.7%
Japan	1.4%
Australia	1.2%
Czech Republic	1.2%

Attacking Countries

China	**63.0%**
United States	6.4%
Turkey	2.1%
Ukraine	1.9%
India	1.8%
South Korea	1.8%
Vietnam	1.7%
Hong Kong	1.7%
Japan	1.6%
Taiwan	1.2%

In Q1 2017, attacks against the US accounted for over 92 percent of all attack traffic due to a barrage of hit and run attacks against a relatively small number of sites. In Q2 2017, this trend continued, albeit on a slightly smaller scale.

38 percent of DDoS targets in the US were exposed to six or more DDoS attacks in the span of the quarter, with 23 percent targeted by ten or more assaults. Also, of the 45 targets that suffered more than 50 attacks, 34 were US-hosted sites.

As a result of these repeat assaults, the US was still the target for over 79.7 percent of all attacks, despite being home to "only" 61.4 percent of targets.

Conversely, the UK was home to 5.7 percent of targets but was hit by just 2.1 percent of attacks. Similarly, the Netherlands was home to 4.3 percent of targets but was hit by 1.7 percent of attacks.

China continued to lead the attacking country list, with more than 360,000 attacking devices and 63 percent of attack traffic.

Noticeably, in Q2 2017 we saw a significant increase in attack traffic out of Turkey, Ukraine and India. In Turkey, we recorded over 3,000 attacking devices that generated over 800M attack requests, more than double from what we saw last quarter. In Ukraine and India, we recorded 4,300 attacking devices, representing a roughly 75 percent increase from Q1 2017. The combined attack output of Ukraine and India was 1.45 billion attack requests per quarter.

Methodology

Our analysis is based on data from 2,618 network layer and 12,825 application layer DDoS attacks on websites using Imperva Incapsula services from April 1, 2017, through June 30, 2017—referred to herein as the second quarter of 2017 or Q2 2017. Information about DDoS bot capabilities and assumed identities comes from a random sample of 39.1 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.