IMPERVA®

DDOS REPORT

Global DDoS Threat Landscape

Q3 2017

Highlights

Bitcoin was one of the most targeted industries

Amidst the cryptocurrency price spike, bitcoin was one of the top-10 most targeted industries, despite its relatively small size.

A third of network layer attacks were highly persistent

29.6 percent of network layer targets were hit ten or more times, nearly triple the number of application layer targets.

High packet rate attacks grew more common

Five percent of network layer assaults reached 50 Mpps, while the largest peaked at 238 Mpps.

Botnet activity out of India and Turkey continued to climb

Following an increase in Q2, botnet activity out of the two countries continued to climb, reaching 11.2 percent.

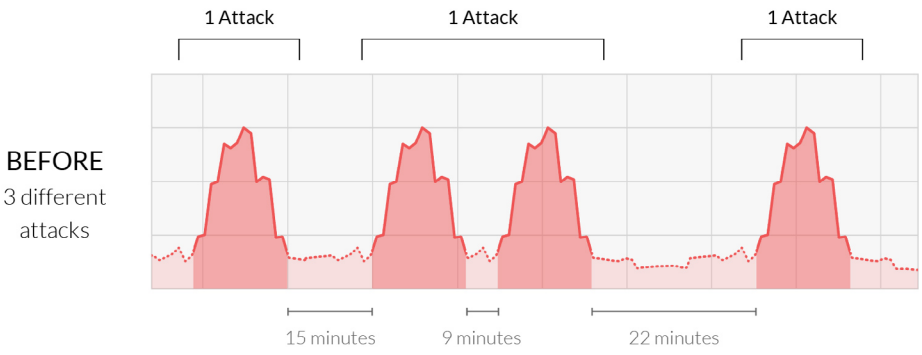
New Methodology

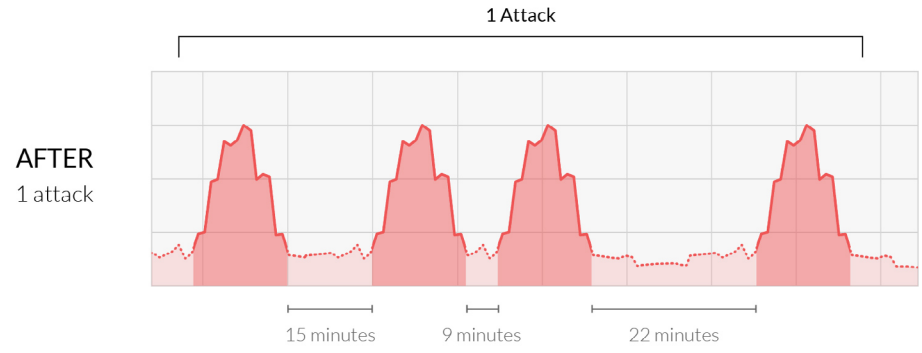
Q3 2017 was marked by an improvement in on our sampling methods and methodology, which changed how we define a single distributed denial of service (DDoS) attack in our quarterly reports.

In prior reports, a DDoS event was defined as a single assault that was preceded by a quiet (attack free) period of at least ten minutes, and followed by another quiet period of the same duration or longer. This quarter, however, we increased the quiet period to sixty minutes in order to aggregate successive attacks.

This was done in response to an increase in the number of short-lived repeat DDoS attacks, such as hit-and-run and pulse wave assaults. Our new sampling method puts these attacks in their proper context, observing them not as a series of independent incidents, but as a single persistent event.

In addition, we expanded on our research to provide additional data and insights. As a result, the scope of our quarterly report has more than doubled from nine to 19 data sets, enabling us to share a more in-depth and detailed view of the DDoS threat landscape.





Overview

In Q3 2017, we saw high packet rate attacks–assaults in which the packet forwarding rate escalates above 50 million packets per second (Mpps)–become more common. So much so that five percent of all network layer assaults came in above 50 Mpps, with the largest attack peaking at 238 Mpps.

This is a cause for concern, as many mitigation solutions are ill equipped to process packets at such a high rate.

Hong Kong topped our list of the most targeted country for network layer assaults in Q3 2017, largely because of a persistent attack on a local hosting service that was hit hundreds of times throughout the quarter. The largest application layer assault targeted a financial services company headquartered in Europe, which was hit multiple times with attacks above 100,000 RPS.

These two attacks illustrate the ongoing macro trend of increased DDoS attack persistence. In Q3 2017, nearly a third of all organizations targeted by network layer assaults were hit more than ten times, as was the case for 11 percent of the domains targeted by application layer assaults.

Target wise, we witnessed a high number of attacks against the bitcoin industry in Q3 2017, which drew 3.6 percent of assaults despite its relatively small footprint.

Finally, botnet activity out of Turkey and India continued to increase for the second quarter in a row. In Q3 2017 these two countries, which typically aren't part of the top-10 attacking countries list, accounted for over ten percent of all botnet activity.

Network Layer Attacks

Attack sizes

In Q3 2017, 8.6 percent of network layer attacks came in above 50 Gbps and five percent were above 50 Mpps.

The largest attack of the quarter peaked at 299 Gbps and targeted Incapsula's own IP ranges, a common occurrence as our IP masking services hide actual customer IP addresses behind our own. The highest attack rate, recorded during an assault targeting a forex company in Asia, came in at 238 Mpps, up from 190 Mpps in Q2 2017.

In contrast, the majority of attacks (90.2 percent) were under 10 Mpps and were predominantly the result of DDoS-for-hire activity.

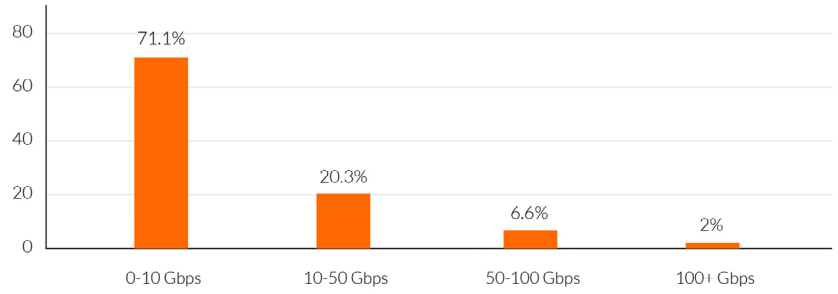


Fig. 1: Network layer attack sizes

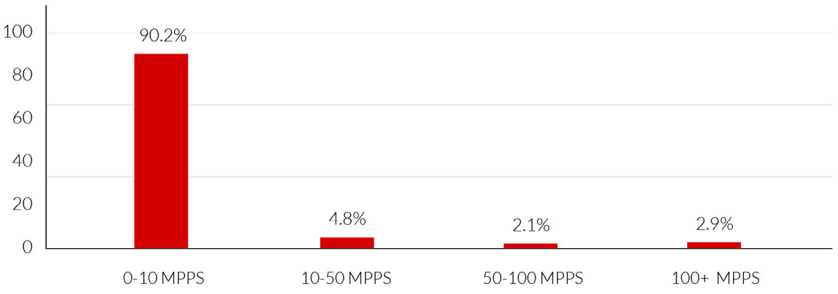


Fig. 2: Network layer attack rates

Top attacked countries

Despite being home to only 5.1 percent of targets, Hong Kong was targeted by almost a third of all network layer attacks in Q3 2017. This was largely due to a large-scale campaign against a local hosting service provider, which was hit more than 700 times throughout the quarter.

Taiwan and the Philippines made an atypical appearance on the top-10 list of attacked countries, following a number of large campaigns targeting gambling websites in their respective regions.

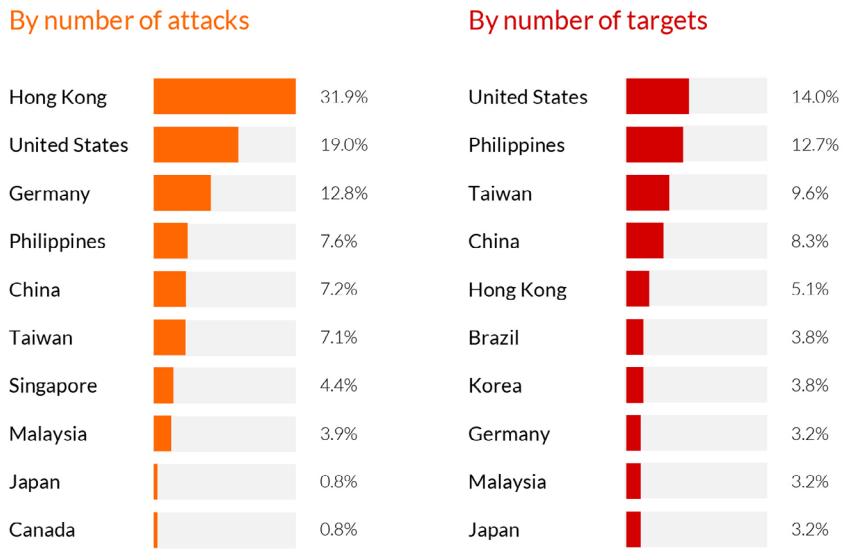


Fig. 3: Network layer: Top attacked countries

Top attacked industries

In Q3 2017, over a third of network layer attacks targeted online gambling sites and related services. This is common, as these sites are reliant on web revenue and exposed to extortion attempts. Additionally, they're highly competitive and are commonly targeted by rival companies.

The online gaming industry was also frequently targeted, although in this case the attacks typically originate from users either attempting to influence a game's outcome or just to vent their frustrations.

The high number of attacks that targeted the internet services industry was driven by the large campaign in Hong Kong. Even if this campaign were to be disregarded, however, internet services would still hold the first place as the most attacked industry.

This is because each of the businesses in this category, such as hosters and ISPs, individually represent hundreds or thousands of domains that use their services. As

such, each represents a large attack surface that can draw multiple attacks from different offenders preying on various targets.

Lastly, in Q3 2017, we saw attacks targeting a relatively high number of cryptocurrency exchanges and services. This was likely related to a recent spike in the price of bitcoin, which more than doubled in the span of the quarter. As a result, bitcoin made the top-10 most targeted industries list, despite its relatively small size and web presence.

This young and exponentially growing industry presents a lucrative opportunity for extortionists and other cybercriminals who are always on the lookout for potentially vulnerable and high-profit targets.

In this specific case, the attacks could have been also launched to manipulate bitcoin prices, something offenders have been known to do.

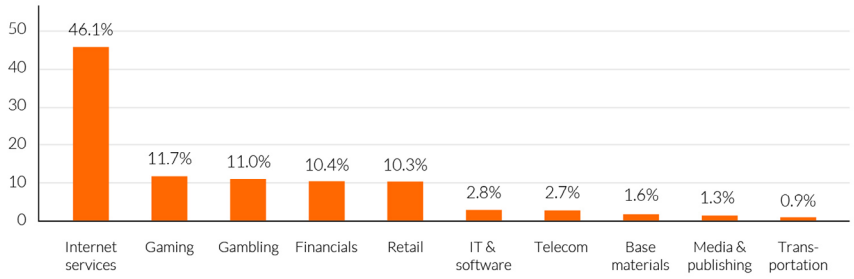


Fig. 4: Network layer: Top attacked industries, according to number of attacks

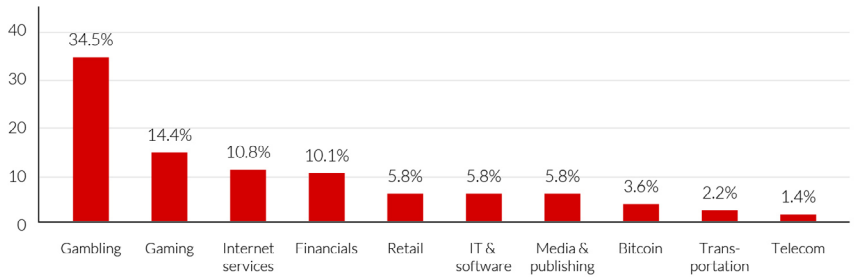


Fig. 5: Network layer: Top attacked industries, according to number of targets

Attack duration

In Q3 2017, our methodology for measuring attack duration was changed to provide a more accurate picture of the current threat landscape. Whereas previously short attacks were counted individually, repeat assaults taking place in the span of an hour are now

treated as a single event. For example, three attacks spaced ten minutes apart are now recorded as one assault.

As a result, the number of attacks lasting more than six hours this quarter increased dramatically to 7.5 percent, from 0.8 percent in Q2 2017. The longest attack of the quarter lasted more than 5.5 days, while average attack duration was 1.2 hours.

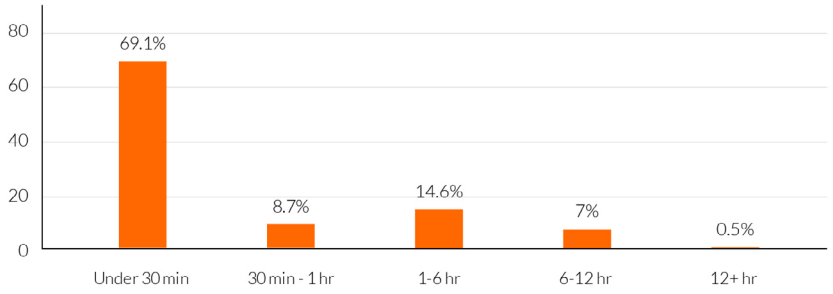


Fig. 6: Network layer: Attack duration

Attack persistence

In Q3 2017, half of network layer targets were hit at least twice, while almost 30 percent were attacked more than ten times. Considering the changes to our methodology, this means that nearly a third of targets were attacked ten or more times, with at least an hour interval in between assaults.

With an average attack duration of 1.2 hours, this also means that—on average—organizations targeted by DDoS offenders spent 12 hours under attack over the course of the quarter.

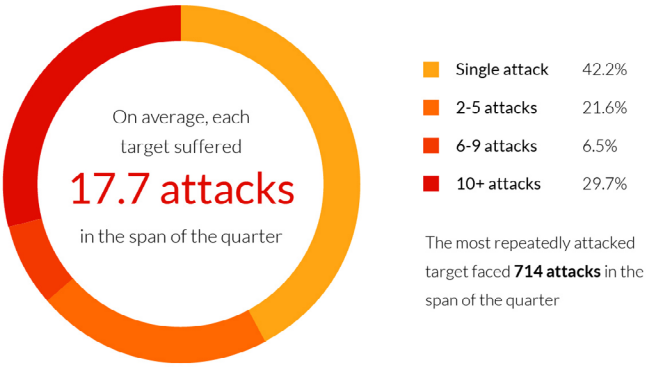


Fig. 7: Network layer: Attack persistence

Attack vectors

In Q3, we saw a steep increase in the number of amplification attacks. DNS-amplification assaults tripled from five percent in Q2 to 15.9 percent this quarter, while NTP-amplification attacks shot up to 36.9 percent from 9.9 percent.

In non-amplified assaults, we continued to see attackers use a variety of fabricated payloads. There was a clear preference towards SYN, TCP and UDP floods, which were often the three payload types used in the course of a single attack.

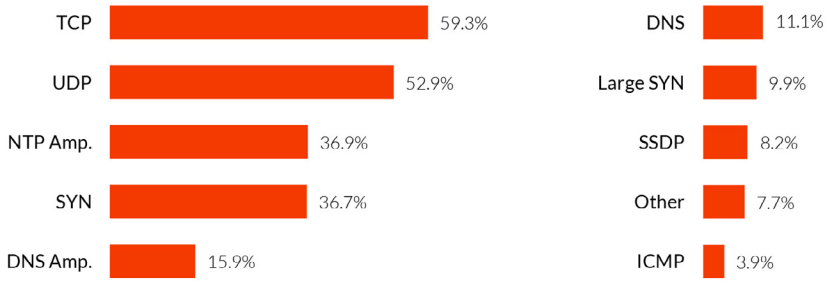


Fig. 8: Network layer: Attack vectors

Multi-vector attacks

In Q3 2017, the number of multi-vector attacks increased to 70.2 percent, from 21.7 percent in the previous quarter. The dramatic increase is closely linked to the changes in how we measure attacks—now, an assault in which an attacker sends out rapid bursts of traffic (e.g., a pulse wave) using different packet types is considered a multi-vector attack.

Measuring attacks in this manner paints a more accurate picture of how sophisticated DDoS assaults have become, and how easily attackers can switch vectors on-the-fly and mix between amplified and non-amplified assaults.

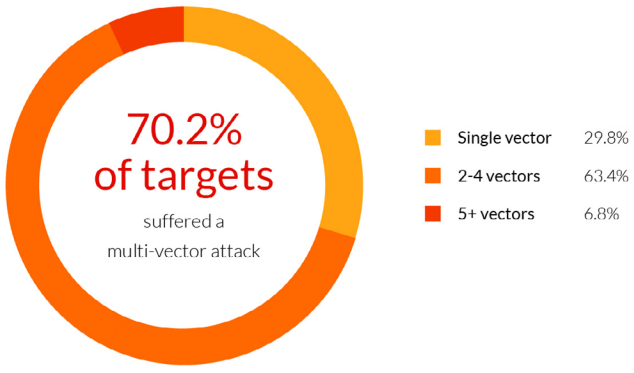


Fig. 9: Network layer: Multi-vector attacks

FAQs

Attack sizes

How are network layer DDoS attacks measured?

Network layer DDoS attacks are measured in Mpps (million packets per second) and Gbps (gigabits per second).

What's the difference between Mpps and Gbps?

Mpps measures the rate at which packets are delivered (a.k.a. forwarding rate) while Gbps measures the total load placed on a network (a.k.a. throughput).

From a mitigation point-of-view, it's important to be aware of both metrics, as they can each be bottlenecked by DDoS traffic.

For example, if your mitigation solution has the capacity to handle 80 Gbps and process packets at a rate of 10 Mpps, a 40 Gbps DDoS attack at a rate of 20 Mpps can still bring down your network, even if it doesn't surpass your total capacity.

Learn more about throughput and forwarding rates.

Top attacked countries

Why are some countries targeted more than others?

Generally, for-profit DDoS perpetrators are interested in targeting wealthy countries with developed digital markets.

A lack of anti-cybercrime legislation or enforcement is also a contributing factor, as some for-profit and non-profit attackers go after local targets. Finally, countries that serve likely-to-be-targeted industries, e.g., gambling, are more prone to attack.

Top attacked industries

Why are some industries targeted more than others?

Attacker motivation typically determines why a specific industry is frequently targeted by DDoS perpetrators.

Motivations can be broken down into the following categories:

- **Business competition** – In a competitive industry, such as gambling, a DDoS attack can be used to take down a rival website.
- **Extortion** – Certain industries, e.g., ecommerce, are very dependent on their online presence and are easy prey for perpetrators extorting money in exchange for keeping a specific website online.

- **Hacktivism** – Hacktivists typically target political, media or corporate websites to protest their actions.
- **Vandalism** – Cyber vandals, typically disgruntled users or random offenders, often attack gaming services or other high-profile targets.

Learn more about DDoS attackers and their motivations.

Attack duration

What influences the duration of a network layer attack?

The length of a DDoS attack largely comes down to the resources at a perpetrator's disposal.

Shorter attacks are typically associated with DDoS-for-hire services (a.k.a. booters or stressers) that can be rented to launch short-lived attacks, usually lasting under 30 minutes.

Longer attacks are almost always the work of more professional bad actors using their own botnets, which can carry out persistent assaults.

Are short attacks a real threat?

Yes. The length of an attack is not correlated with the duration of a site's downtime. While a website (or web service) can be taken down in minutes, it usually takes hours for it to recover.

Additionally, a short attack might be part of a repeat assault, in which a target is hit with multiple short bursts. This method is commonly used to bypass mitigation solutions that rely on manual activation, or are otherwise slow and cumbersome to deploy.

Attack persistence

Why do perpetrators continue attacking a protected target?

There are a number of reasons to repeatedly attack a protected target, including:

- It's common for perpetrators to change methods and try different attack vectors in an attempt to break through a site's defenses.
- The price of executing an attack is extremely low. If a first attempt fails, a perpetrator can try again (and again), even if their chances of success are slim.
- For certain perpetrators, e.g., those executing pulse wave attacks, repeat assaults are part of their MO.

What types of enterprises are more likely to be targeted by persistent attacks?

Generally speaking, large organizations are more likely to be the targets of persistent attacks, which are often initiated by competitors or skilled extortionists.

Attack vectors

Why would a perpetrator use different attack vectors?

For DDoS offenders, switching between different attack payloads (i.e., different types of network packets) is an attempt to bypass a network's filtering mechanisms.

What's the difference between amplified and non-amplified attack vectors?

Amplified attacks vectors, such as DNS and NTP, are executed through a third party, e.g., an open DNS server. Conversely, non-amplified attacks are executed using a perpetrator's botnet.

Multi-vector attacks

Why do perpetrators launch multi-vector attacks?

In a multi-vector attack, different streams of payloads (network packets) are simultaneously sent to a target. This can help a perpetrator bypass an enterprise's security mechanisms, which are not equipped for complex filtering and might allow some of these streams to reach their target.

What do multi-vector attacks tell us about a perpetrator?

A multi-vector assault requires more resources and skill than a single-vector attack. The more sophisticated a bad actor is, the more likely such techniques are to be employed in their assaults.

Application Layer Attacks

Attack sizes

In Q3 2017, one in five application layer assaults went above 1,000 requests per second (RPS). The largest attack was against a financial services company hosted in Europe and clocked in at 134,486 RPS. The site was hit multiple times with attacks above 100,000 RPS, many of which, including the largest one, targeted the organization's API gateways.

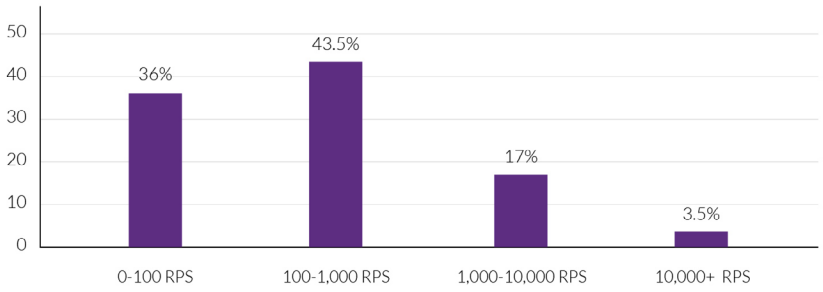


Fig. 10: Application layer attack sizes

Top attacked countries

In Q3 2017, the US topped our list of the most attacked countries, both in terms of hosted targets (40.1 percent) and attacks (53.3 percent). Coming in second place, the Netherlands was home to 10.6 percent of targets and 8.8 percent of attacks.

The remainder of the list consisted of developed countries with mature digital marketplaces, including Singapore, Japan and Australia, which make for attractive targets.

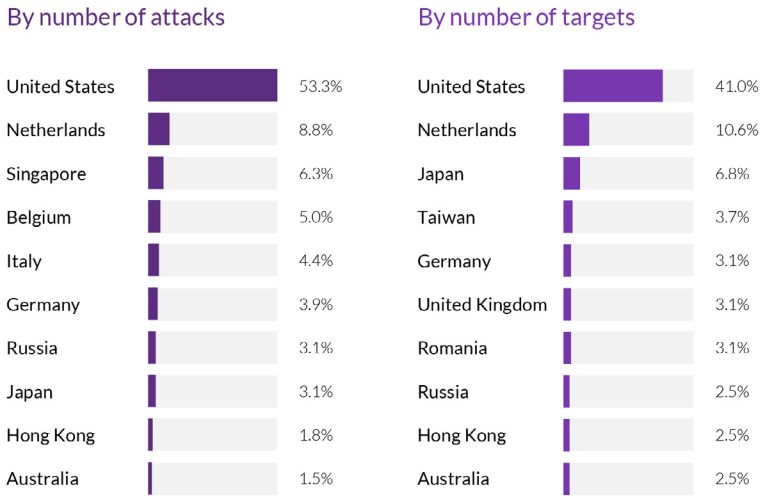


Fig. 11: Application layer: Top attacked countries

Attack duration

The change in our methodology for measuring attack duration, (i.e., aggregating smaller assaults into a single event), allows us to disregard individual assaults that are part of a larger attack.

As a result, the number of attacks under 30 minutes fell from 57.4 percent in the previous quarter to 17.1 percent in Q3 2017. At the same time, attacks lasting between 30 minutes and six hours came in at 73.2 percent in Q3 2017, compared to 35.2 percent in the previous quarter.

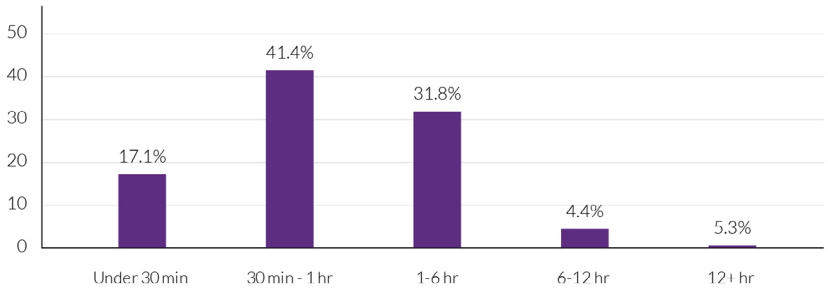


Fig. 12: Application layer: Attack duration

Attack persistence

The change in how we measure DDoS attacks gives us a more accurate view of attack persistence that disregards the "noise" made by short-lived assaults occurring in rapid succession.

As a result, we saw the number of repeat attacks drop from 75.8 percent in the previous quarter to 46.7 percent in Q3 2017. Even with the more precise measurement, however, we still saw that almost 16 percent of targets were exposed to six or more attacks throughout the quarter.

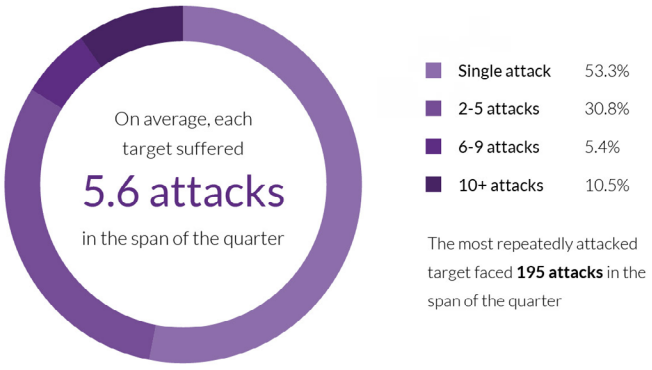


Fig. 13: Application layer: Attack persistence

Bot capabilities

In Q3 2017, application layer attack traffic generated by bots that can bypass cookie challenges increased to 6.4 percent from 2.1 percent in the previous quarter. Of these bots, 1.8 percent were also able to parse JavaScript, an increase from 1.4 percent in Q2 2017.

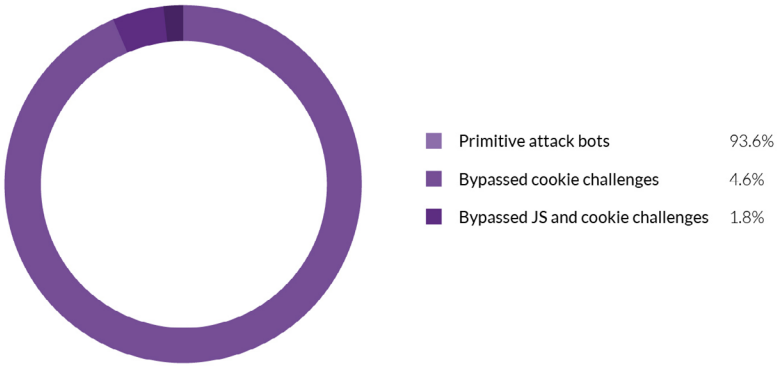


Fig. 14: Application layer: Bot capabilities

FAQs

Attack sizes

How are application layer DDoS attacks measured?

Application layer DDoS attacks are measured in RPS (requests per second).

How many RPS does an attack need to take down a website?

An application layer attack's success depends on the amount of workload that a single request can force on a target server.

For example, a request that downloads an image file is far less resource-intensive than a request that initiates a string of API calls.

That said, many websites work on relatively low operational margins and can be taken offline by just a few dozen well-placed requests. There aren't many that can handle an additional 10,000 RPS, which is equal to 36 million requests an hour.

What is the difference between a network and application layer DDoS attack?

The main difference between the two DDoS attack types is that they target different resources. A network attack attempts to clog network pipes, while an application layer attack seeks to deplete resources, e.g., CPU and RAM.

This translates into further differences in the ways these attacks are executed. It also means that mitigating each of these threats requires a significantly different set of security methods and skills.

In fact, outside of some superficial similarities, application and network layer attacks are two very different types of threats.

Top attacked countries

Why are some countries targeted more than others?

Generally, for-profit DDoS perpetrators are interested in targeting wealthy countries with developed digital markets.

A lack of anti-cybercrime legislation or enforcement can also be a contributing factor, as some for-profit and non-profit attackers go after local targets.

Finally, countries that are home to likely-to-be-targeted industries, such as gambling, are at greater risk of being targeted.

Attack durations

What influences the duration of an application layer attack?

Similar to network layer attacks, the duration of an application layer attack largely depends on the resources at a perpetrator's disposal.

That said, application layer assaults are easier to execute and sustain, as even a sizeable attack of several thousand RPS can be launched from a single computer.

Attack persistence

Why do perpetrators continue attacking a protected target?

Similar to network layer attacks, perpetrators will repeatedly attack a protected target because it's so cheap—many offenders see no point in quitting, even if the chances for success are slim.

Additionally, launching application layer attacks is easy and can even be done from a home PC or a very small amount of botnet devices.

Botnet Location

In Q3 2017, nearly 17 percent of botnet traffic originated in China, despite the fact that it hosted over 40 percent of attack devices. This represented a significant drop from the previous quarter, when China was the source of 63 percent of bot traffic.

After a notable uptick in Q2 2017, botnet activity in Turkey and India continued to increase this quarter.

A staggering 7.2 percent of botnet traffic originated in Turkey in Q3 2017, up from 2.1 percent in the previous quarter. In India, that figure increased to four percent from 1.8 percent in the prior quarter.

These countries, which have rarely appeared in the top-10 attacking country list thus far, accounted for over 10 percent of all botnet activity while serving as home to 5.1 percent of all attacking devices.

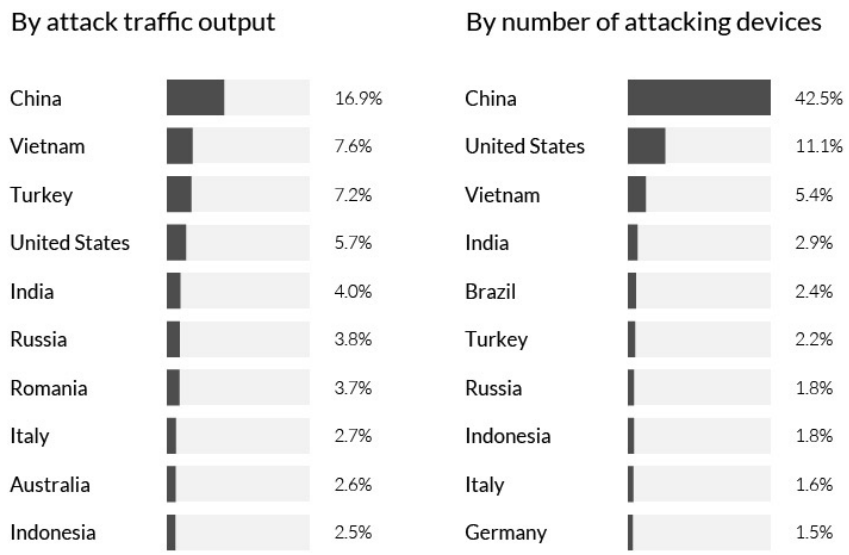


Fig. 15: Botnet location

FAQs

How can you accurately identify botnet geolocation despite IP spoofing?

IP spoofing is the practice of faking a source IP to avoid backtracking and blacklisting. In theory this makes IP geo-data collected during DDoS attacks unreliable.

IP spoofing, however, is only possible with a network layer attack. In an application layer assault, IPs cannot be spoofed, as a full TCP connection has to be established before a request is sent.

This is why we only use data from application layer attacks to identify bot location.

Learn more about IP spoofing.

Why do some countries generate more botnet activity than others?

There are a lot of factors that come into play here. Broadly speaking, however, the two most impactful reasons are:

- **Security awareness** – Countries in which users have adopted digital security policies are better equipped to detect botnets inside their borders.
- **Connected devices** – As a rule, a high number of connected devices open up more opportunities for botnet herders.

Methodology

Our analysis is based on data from 3,920 network layer and 1,755 application layer DDoS attacks on websites using Imperva Incapsula services from July 1, 2017, through September 30, 2017—referred to herein as the third quarter of 2017 or Q3 2017.

Information about DDoS bot capabilities and assumed identities comes from a random sample of 37.4 billion DDoS attack 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). A single attack is preceded by a quiet (attack free) period of at least a sixty 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.