IMPERVA®

DDoS Threat Landscape Report

2015 - 2016

Contents

Highlights

- DDoS attacks increased by 211 percent year over year. This uptrend is fueled by DDoS-for-hire services.
- Network layer attacks hit a new high. Largest assault on our record peaks at 470 Gbps.
- Offenders experiment with new attack methods in an attempt to circumvent security solutions.
- The increase in attacks against UK businesses made it the second-most targeted country.
- South Korea dethrones China as the main hub for DDoS botnet activity.
- Half of all targeted businesses were attacked more than once.

Preface

Distributed denial of service (DDoS) attacks are amongst the most common cyber threats facing online organizations today. Every week there is news about a prominent business disrupted by an assault. For every big name brand that succumbs to an attack, many smaller ones fall prey to DDoS offenders.

With no signs of abating, understanding the threat is essential for business owners and network and security ops charged with DDoS protection strategy. In this report, we share unique research data collected in the course of mitigating thousands of DDoS assaults against Imperva Incapsula customers.

Leveraging this real-world data, the report profiles the current evolution of DDoS threat landscape–preparing for the threats of today and predicting the challenges of tomorrow.

Overview

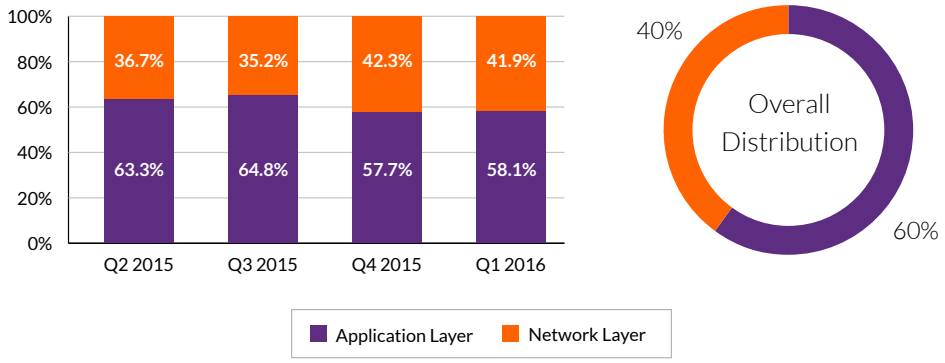

Fig. 1 – Distribution of network and application layer DDoS attacks

From April 1, 2015, through March 31, 2016, Imperva Incapsula mitigated an average of 445 attacks targeting its customers per week.

Overall, application layer assaults accounted for the majority (60 percent). However looking closer, their relative number has been trending downward—dropping by more than five percent year over year. If this continues, network layer attacks could be as commonplace as their application layer counterparts by 2018.

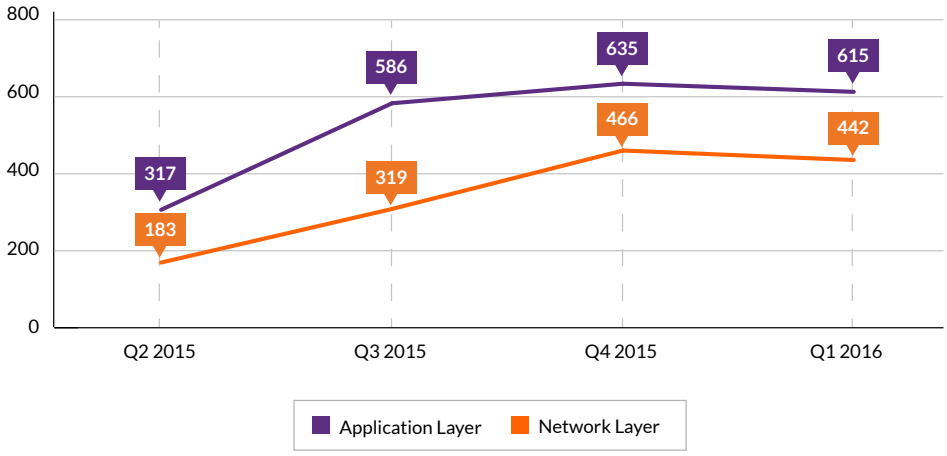

Fig. 2 – Average number of DDoS attacks per week

As evidenced by the graph in figure 2, the number of both network and application layer attacks doubled during the year. This trend is a result of three factors:

- The continual growth of the Incapsula user base has correspondingly increased the network's attack surface. (Many new customers onboard our service after receiving threats from DDoS extortionists or in the midst of a DDoS assault.)
- The increased use of DDoS-for-hire services (a.k.a., stressers or booters). These services let anyone launch a short-duration attack—typically an unsophisticated network layer burst of under 30 minutes. The assaults climbed from 63.8 percent in Q2 2015 to 93 percent in Q1 2016, driving the uptrend in overall DDoS activity.
- The use of hit-and-run tactics such as consecutive bursts launched against a target to:
  - Exhaust mitigation teams by keeping them on high alert around the clock for weeks.
  - Force prolonged activation of on-demand mitigation solutions, often leading to service degradation.
  - Create a state of stress and confusion to draw attention away from other malicious activities (e.g., network breach, data extraction).

Whatever the goal, a single hit-and-run event translates into a series of multiple assaults, thereby driving the total number of DDoS attacks upward.

Network Layer Attack Trends

Attack Size

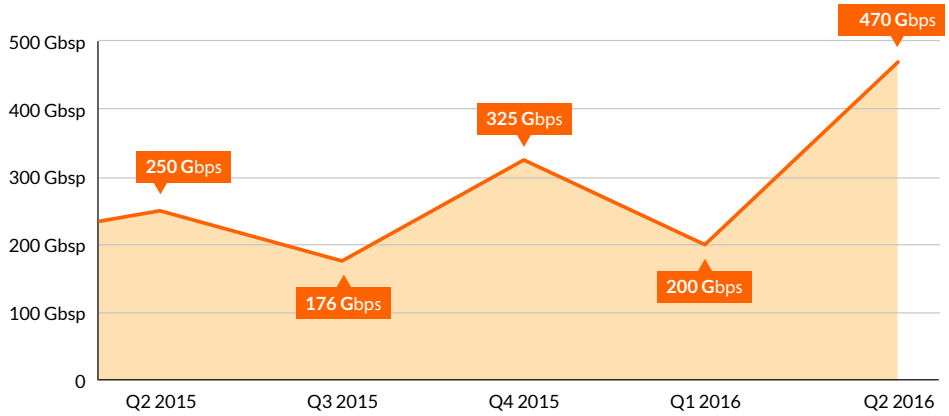

Fig. 3 – Top network layer attack sizes

Attack size (measured in Gbps) is the primary metric used in comparing network layer attacks. It's also an indicator of the evolution of botnet resources, with which such barrages are executed. During the year, we mitigated many more attacks that exceeded the 200 Gbps mark, making them almost a regular occurrence.

Additionally, the bar was raised in the second quarter as we protected one customer from a 470 Gbps multi-vector attack–the largest we've seen to date. Its details provide an interesting case study of just how complex network layer DDoS attacks can be.

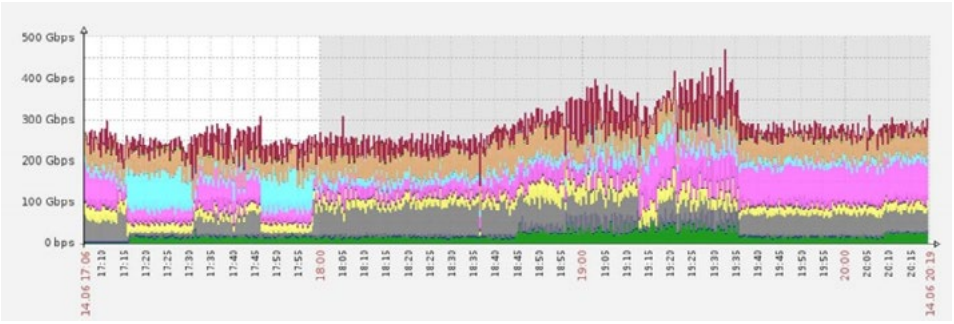

Fig. 4 – DDoS attack peaking at 470 Gbps, the largest so far on record

One of the things that the case study shows is how perpetrators have taken to using small payloads (network packets) to achieve high packet forwarding rates, in addition to high throughput capacity.

Such high attack rates present a new type of threat to our customers and Imperva Incapsula has been increasingly fending off such attacks during the year.

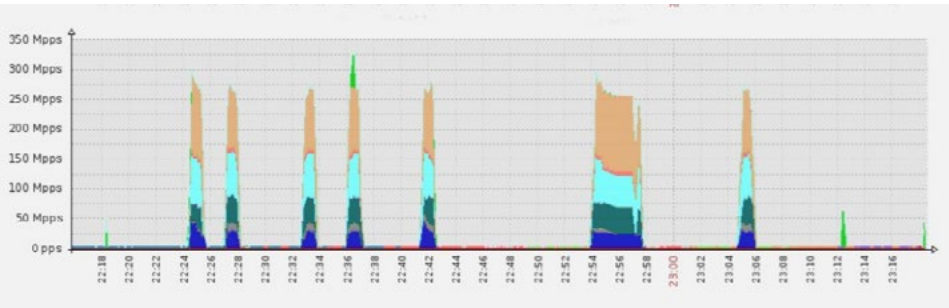

Fig. 5 – The face of a new threat – high rate attack peaking at 300 Mpps

In using packet forwarding rates, perpetrators are attempting to exploit a design oversight in current-generation mitigation appliances, the majority of which can't handle such high Mpps (million packets per second) processing loads. Moving forward, we expect to see an ever-increasing number of such assaults since these appliances are still in their mid-life cycle.

In Q1 2016 we found ourselves mitigating an 80+ Mpps attack every eight days. More than a few exceeded 100 Mpps, with the largest peaking at 300 Mpps (figure 5).

Attack duration

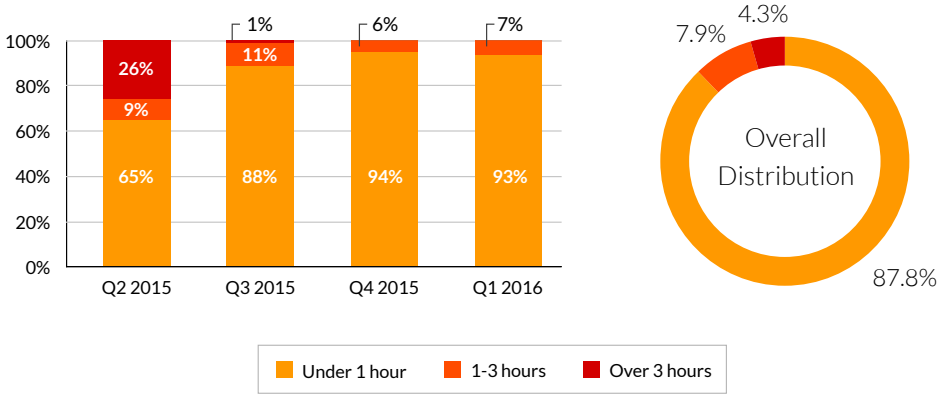

Fig. 6 – Network layer attack duration

During the year, we mitigated our share of lengthy assaults with the longest occurring in Q2 2015 and lasting 54 days. However, we saw a decrease in attack duration with a majority of threats involving short bursts of under 30 minutes.

The steep increase in the number of network layer attacks can be traced to the growing popularity of DDoS-for-hire services. These services enable anyone to launch minute-long attacks for as little as $5 per pop.

Additionally, the fact that DDoS-for-hire now accounts for over 90 percent of all assaults paints a new profile of top bad actors. These are non-professionals who use DDoS for racketeering or to instigate attacks out of boredom or spite.

The existence of such unpredictable offenders poses a new threat to many online entities that traditionally didn't consider themselves a potential target.

Attack Complexity

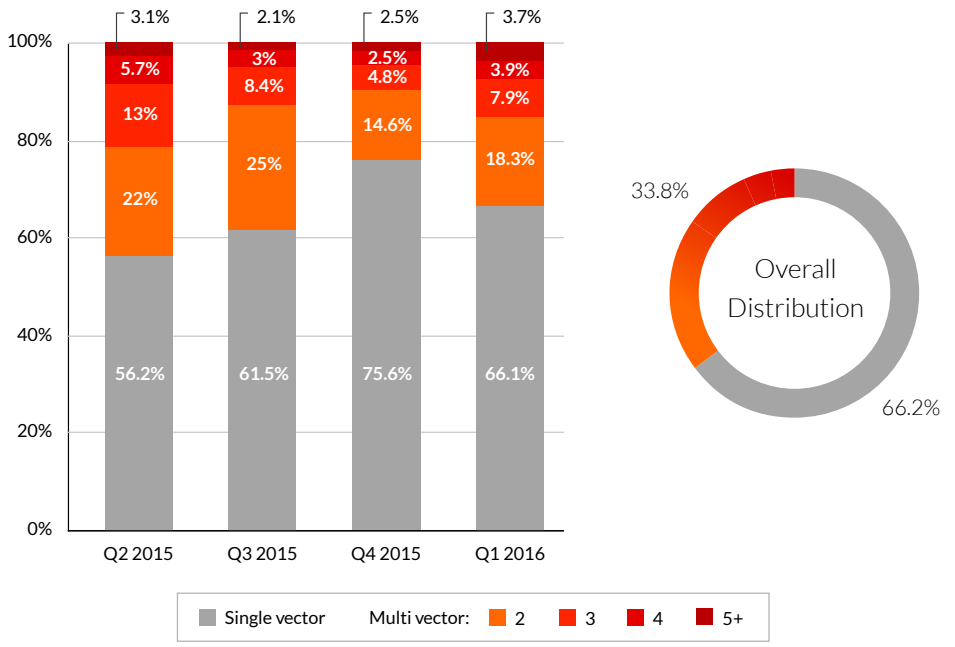

Fig. 7 – Network layer attack complexity

The use of multiple payloads in a single attack is a sign of the attack's complexity. The approach, which uses a mix of different attack vectors, is also a testament to the capabilities of the orchestrator(s) and their choice of tools.

Starting in Q2 2015, we recorded a decrease in multi-vector attacks. Again, this points to increased activity by casual offenders. Interestingly, in Q1 2016, we also saw an increase in the volume of assaults using five or more payloads.

This countertrend reminds us that—in parallel with the increased "hobbyist" activity—more capable cybercriminals continue to improve their methods. As per the first rule of the DDoS mitigation industry, attacks continue to get larger and more sophisticated on the high-end of the scale.

Attack Vectors

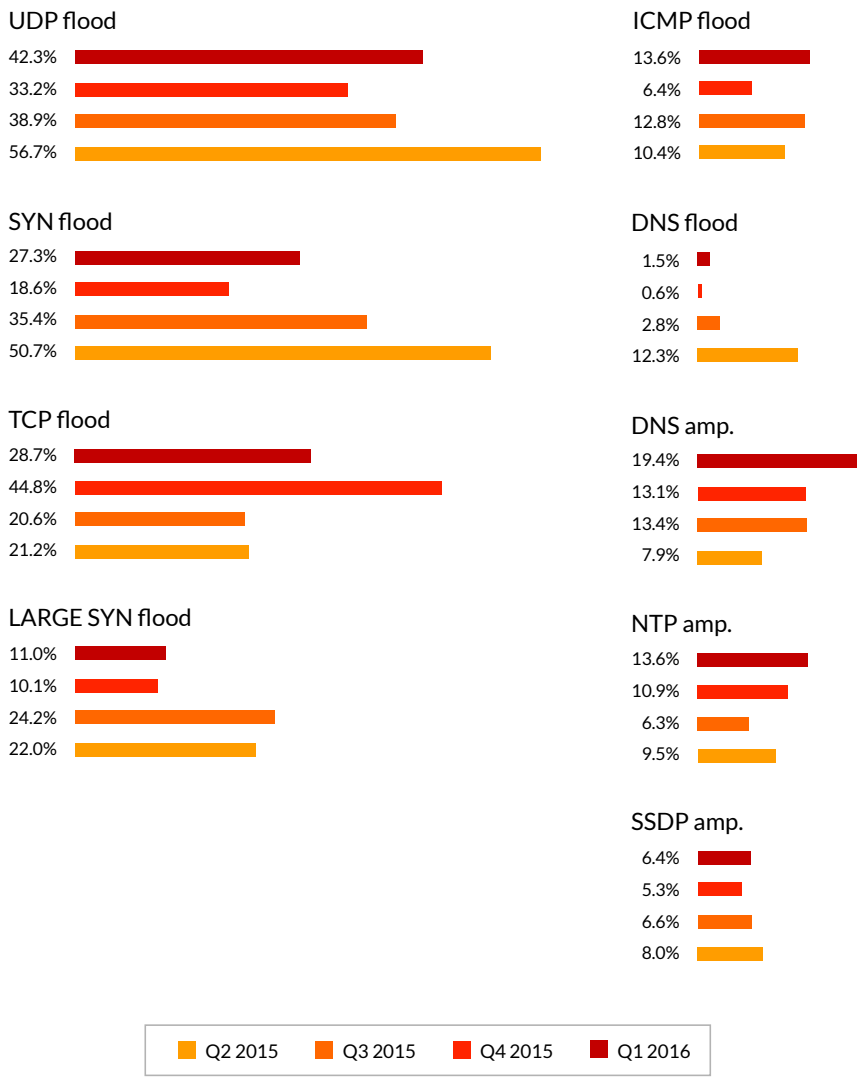

Fig. 8 – Network layer attack vectors

Figure 8 shows attack vectors used in network layer assaults over the past year. The lack of a single vector preference suggests a diversification in attack tactics. Perpetrators apparently don't subscribe to a "silver-bullet" approach.

This reminds us that the high end DDoS perpetrators have moved away from simply trying to take down a target–a feat that doesn't require diversification or complexity. Instead, the variety in attack vectors reveals that bad actors are expecting to be challenged; they're trying different methods in an attempt to circumvent mitigation solutions.

Application Layer Attack Trends

Attack Size

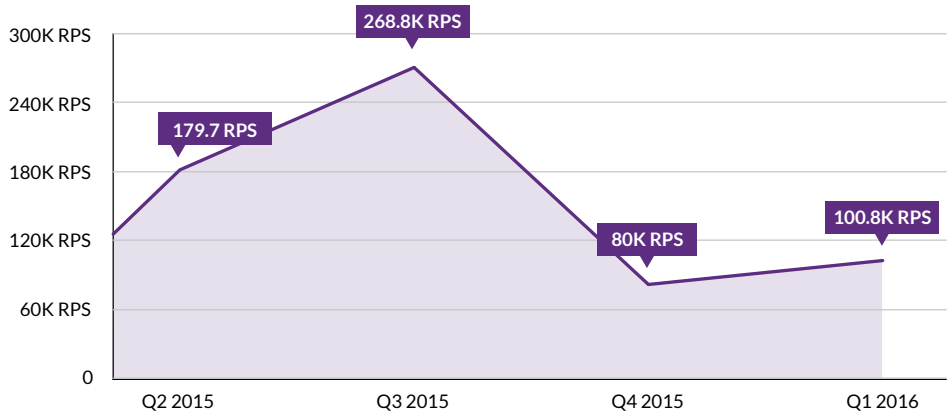

Fig. 9 - Top application layer attack sizes

The sheer size of application layer attacks is a secondary factor as most servers can be brought down with just a few hundred requests per second (RPS).

Still, over the course of the year, we saw application layer attacks reaching new heights. One soared above 268,000 RPS–the largest we've ever recorded. The intent of these massive assaults is to blow a hole in a security perimeter, not just take down a target.

Similar to high-rate network layer assaults (page 5), this is part of the larger trend of DDoS attacks being crafted to bypass mitigation solutions. As part of that trend, we also saw attackers experiment with rare and unique methods. One prominent example is a uniquely executed HTTP flood attack, in which the target was bombarded by abnormally large POST (upload) requests.

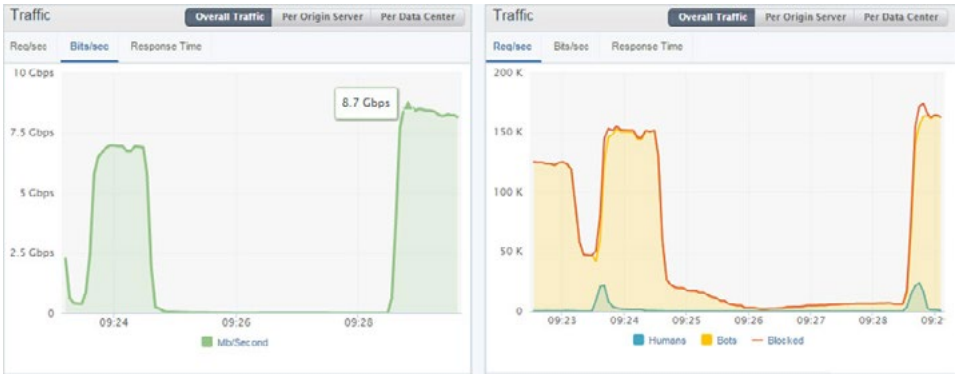

Fig. 10 – HTTP flood peaking at record-breaking 8.7 Gbps

Figure 10 shows that at a rate of 163,000 RPS, the attackers were able to generate 8.7 Gbps of DDoS traffic. This is unheard of in relation to application layer assaults, which rarely exceed 0.5 Gbps. This attack, exploiting nuanced soft spot of a hybrid DDoS mitigation setups, highlights the degree of understanding some perpetrators now have about the inner workings of anti-DDoS solutions.

Attack Duration

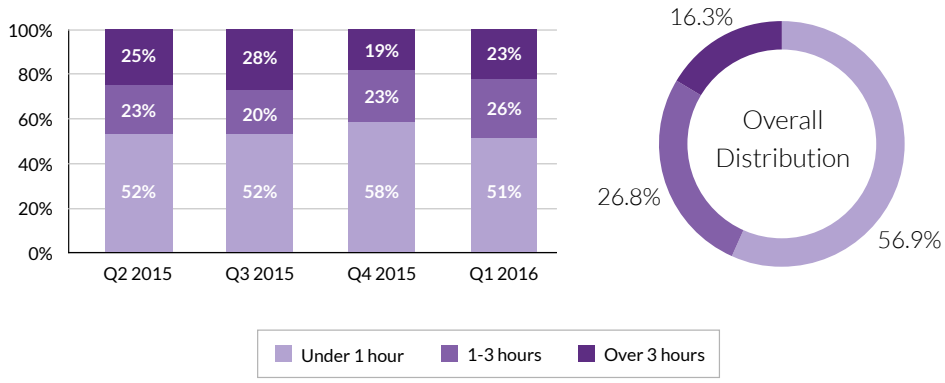

Fig. 11 – Application layer attack duration

Compared to network layer assaults, application layer attacks are significantly easier to sustain because they require far fewer botnet resources. As a result, more than 44 percent of application layer attacks lasted more than one hour as compared to just 12.2 percent of network layer attacks.

In Q3 2015, we saw a trend develop regarding an increase in application layer assaults lasting between one and three hours.

Attack Frequency

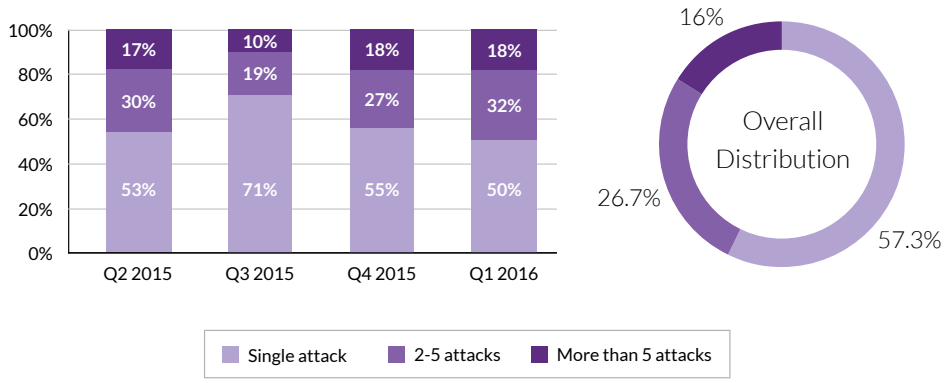

Fig 12 - Application layer attack frequency

Unlike network layer assaults, which often target the Incapsula network, every application layer attack can be linked to its specific target. This enables us to measure the frequency by which any given organization is repeatedly hit by DDoS assaults.

On average, our data shows that more than 40 percent of targets are attacked more than once with 16 percent targeted more than five times. Looking at quarter-by-quarter data, one can also observe an uptrend in repeat attack events. These have increased from 29.4 percent in Q3 2015 to 49.9 percent in Q1 2016.

This ties into the increased use of hit-and-run tactics (page 4)–yet another reminder that DDoS is a long-term security issue. Once sighted by tenacious offenders, even protected businesses are likely to be persistently hit, as perpetrators seem unfazed by multiple failed attempts.

DDoS Bot Capabilities

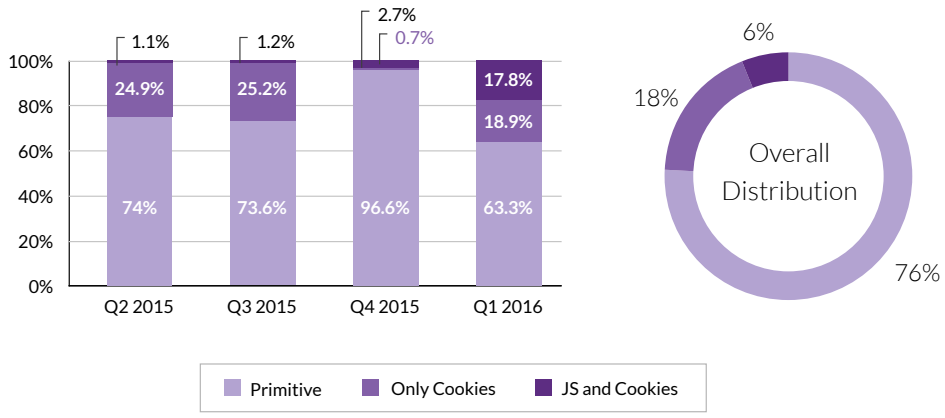

Fig. 13 – DDoS bot capabilities

Application layer attacks use bad bots to make numerous TCP connections with a server in an attempt to exhaust its resources. Bots of this type use fabricated user-agent HTTP headers–most commonly those of popular web browsers–to mask their true identity.

To complete the charade, more advanced bots also exhibit browser-like traits including being able to retain cookies and parse JavaScript. These bots can circumvent bare bones security solutions that test solely for such criteria when trying to identify fake/malicious visitors.

Bad bot advancements hint at an evolution in application layer attack tools. On average, our records show that 24 percent of DDoS bots were so called advanced attackers–able to bypass at least some of these rudimentary security tests. In Q1 2016, the number of advanced attackers rose to a record high of 36.6 percent.

Botnet Activity

Top Attacking Countries

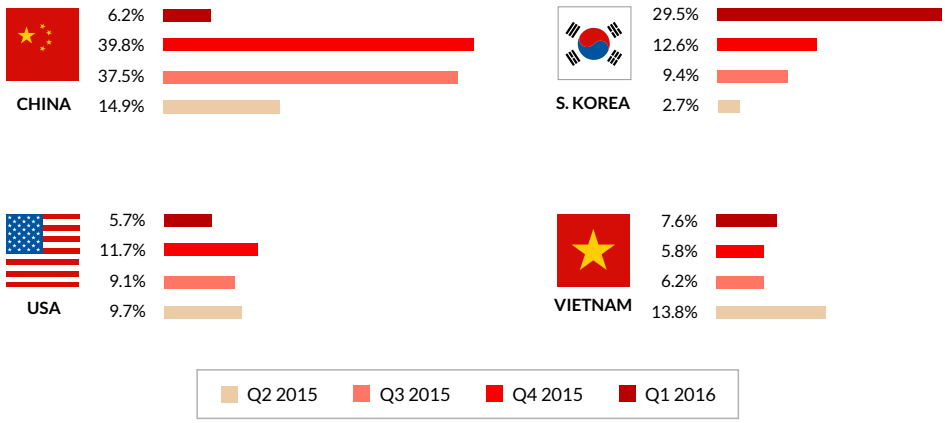

Fig. 14 - Top attacking countries

We track botnets used to launch assaults against Incapsula-protected networks, web applications and cloud environments as part of our ongoing security research. Amongst other things, this enables us to keep a record of repeat offenders so as to improve the accuracy of our traffic- scrubbing solutions.

On a higher level, information provides a view of macro trends in DDoS botnet activity including common countries of origin. As in our previous reports, China remains the leader on the list as the main point of origin for botnet activity in three out of the four quarters.

More intriguing, however, is the steep increase in botnet traffic emanating from South Korea. By Q1 2016, it had become the point of origin for almost one-third of all application layer DDoS traffic. Although this situation is new, it's not surprising given that country's powerful Internet infrastructure.

South Korea's high-speed Internet backbone enables botnet shepherds to increase compromised device output. However, its window of opportunity might be short-lived as the country mobilizes more resources for its cyber security investment.

The most recent example of that effort is its K-ICT 2020 initiative—a five-year plan to turn South Korea into a global cyber security power. This effort will nearly triple that government's investment and create 19,000 new jobs. It also allows the country to buff its resilience against the spread of malware in the corporate and civilian sectors where botnet operators do most of their "recruiting."

Top Attacked Countries

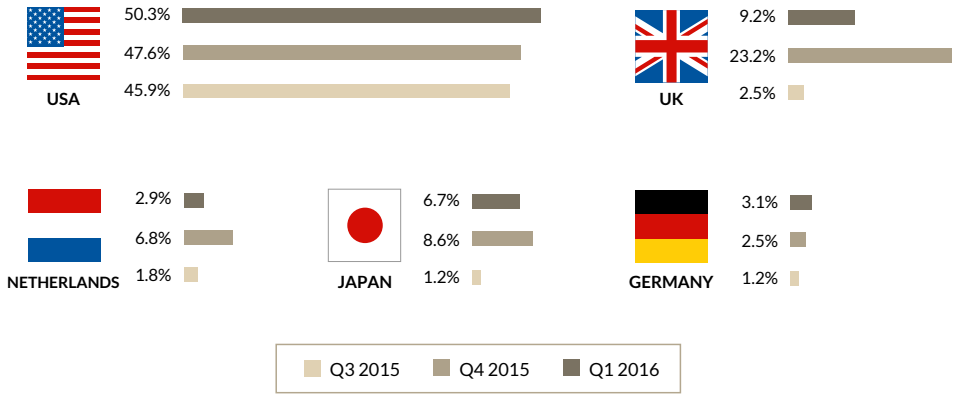

Fig. 15 - Top attacked countries

Even as points of origin for botnet activity have shifted, geographical targets have essentially remained the same during the past year, which is to be expected. With the goal of using DDoS for extortion or attention-grabbing vandalism, most perpetrators target successful online businesses more often than highly developed industrial countries.

Deserving a special mention, one trend result is the increase in DDoS attacks on UK-based businesses during the final six months of this study. This number first spiked in Q4 2015 during a holiday season when increased cyber extortion attempts caused a boom in criminal activity.

In Q1 2016, attacks on the UK trended downward, yet still accounted for 9.2 percent of all assaults making the UK the second-most attacked country for two succeeding quarters.

While the majority of attacks in the UK targeted small and medium sized organizations, this trend also translated into several high-profile assaults, including the takedowns of the BBC, HSBC UK and the Irish National Lottery.

Botnet malware types

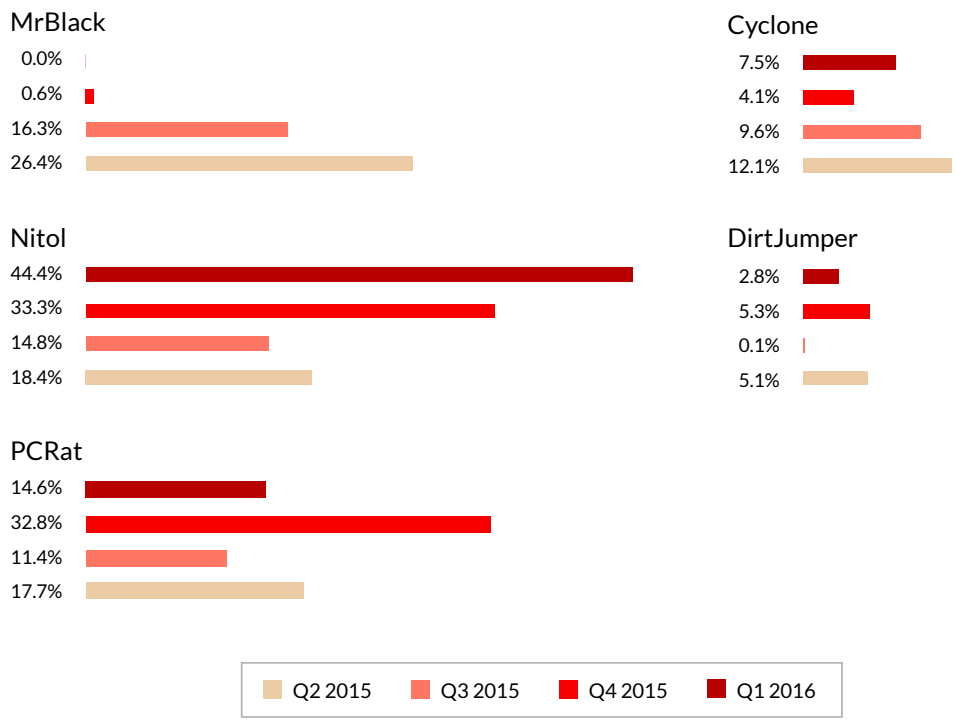

Fig. 16 - Most common botnet malware types

During the study period, the majority of attacks came from botnets running variants of Nitol, Cycloe and PC Rat malware. On average, these attacks accounted for 55.1 percent of all botnet activity.

In Q2 and Q3 of 2015, we also monitored numerous attacks from (mostly) SOHO routers infected with MrBlack malware which we documented in detail. Attackers also used Sentry MBA, a password cracking tool which can be used in a DDoS attack when run at a high rate.

Finally, in Q1 2016 we saw an activity spike from botnets running Generic!BT variants, originating mostly in Russia and Ukraine. Overall they accounted for 12.8 percent of botnet activity in that quarter.

Incapsula DDoS Protection:

- Global cloud network with over 2 Tbps capacity easily handles even the largest attacks
- Advanced scrubbing algorithms mitigate complex attacks without challenging legitimate users
- Protect DNS, network devices and Web servers
- Supports Anycast DNS and Unicast DNS routing
- Supports on-demand BGP routing
- Monitors attacks in real time
- Supported by 24/7 operations center
- Backed by the Imperva security research team
- Part of a comprehensive solution that includes web security, high availability and content delivery

What's next

- Read our DDoS Impact Report to learn more about the business effects of DDoS attacks.
- Use our DDoS Response Playbook to create your DDoS response plan.
- Visit www.Incapsula.com for addition information about Incapsula DDoS protection services.

Questions?

CONTACT US

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.

Unlike the competition, Incapsula uses proprietary technologies in its solutions. Our client classification technology identifies bad bots, and our big data analysis of security events increases accuracy without creating false positives.

Incapsula services include:

- A web application firewall (WAF) to thwart hacking attempts
- DDoS mitigation to ensure attacks don't impact online business assets
- A content delivery network (CDN) to optimize load speed and user experience
- A cloud-based load balancer to enable flexible scalability

Only Incapsula provides enterprise-grade website security and performance—without the need for hardware, software, or specialized expertise.

Sources

The above analysis is based on data from the following Imperva reports:

- Q2 2015 Global DDoS Threat Landscape Report – Jun 9, 2015
- Q3 2015 Global DDoS Threat Landscape Report – Nov 2, 2015
- Q4 2015 Global DDoS Threat Landscape Report – Jan 28, 2016
- Q1 2016 Global DDoS Threat Landscape Report – Apr 20, 2016

These represent a combined record of 12,092 network layer and 18,444 application layer DDoS attacks on websites, networks and cloud environments protected by Imperva Incapsula services.

Definitions

DDoS attack – Defined as 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 occurring 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. The impact of network layer assaults is measured in bits per second (bps), tested against total network capacity. The impact is also measured in packets per second (pps), tested against the processing capacity of the networking devices (e.g., switches or routers).

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), tested against the maximum number of requests that can be handled by a server(s). 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 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 attack. 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 attack.