Global DDoS Threat Landscape
Understanding the latest DDoS attack trends, methods and capabilities
What’s inside

Introduction 3

Report Highlights 3
Network Layer Attacks
Application Layer Attacks

Methodology 4

Network Layer Attacks 5
Overview
Attack Duration
Attack Vectors
Multi-Vector Attacks
Botnet-for-Hire

Application Layer Attacks 11
Overview
Attack Duration and Frequency
Botnet Activity and Geolocation
DDoS Bot Capabilities and Assumed Identities

Conclusion 17
Shady Economy of DDoS Attacks

What’s next 18

About Imperva Incapsula 18
Introduction

Distributed denial of service (DDoS) assaults continue to be a nuisance for online businesses and their customers. Worse, the downtime caused by attacks is costly for organizations and frustrating for consumers. With no signs of abating, understanding the methods and capabilities of perpetrators is essential to maintaining good defenses.

In this document you’ll find unique research data, collected in the wild in the course of mitigating thousands of DDoS assaults against Imperva Incapsula-protected domains and network infrastructures. Leveraging this large dataset, we are able to produce statistical research of DDoS events—one which provides a bird’s-eye view of the current state of the DDoS threat landscape. It is supplemented by granular information about the identity and tactics of DDoS bots, collected by our application layer security solutions.

This Q2 2015 DDoS Threat Landscape Report examines trends in both network and application layer DDoS attacks. Assaults against network infrastructures continue to grow in size and duration. Those aimed at applications are both long in duration and likely to be repetitive. The upshot for organizations of all sizes is that simply weathering the storm is no longer a viable strategy—the impact will be big, durable, and likely recurring.

As indicated by its title, this is our premier quarterly report on this topic. It marks our new commitment to producing a periodic DDoS landscape study which discloses quarter-to-quarter and cumulative annual trends in DDoS attack patterns.

Report Highlights

Network Layer Attacks
- Largest attack peaks at 253Gbps
- Longest attack lasts 64 days
- 20.4 percent of all attacks last over five days
- UDP is the most common attack vector
- Large-SYN flood is the most high-damage attack vector
- Multi-vector attacks are less common
- Botnet-for-hire fingerprints are on roughly 40 percent of all attacks

Application Layer Attacks
- Largest attack peaks at 179,712 RPS
- Longest attack lasts eight days
- On average, targets are hit every ten days
- Nitol botnet was used in 59 percent of all attacks
- MrBlack botnet was the most aggressive, despite not being the largest
- 56 percent of DDoS bot traffic emerged from China, Vietnam, US, Brazil and Thailand
- Botnet operators have abandoned the use of search engine impersonator bots
- DDoS bots display more diversity in assumed identities to counter signature-based security methods
Methodology

Our analysis is based on data from 1,572 network layer and 2,714 application layer DDoS attacks on websites using Incapsula services from March 1 through May 7, 2015 which we will refer to this in report as the second quarter of 2015 or Q2 2015. Information about DDoS bot capabilities and assumed identities comes from a random sample of 60 million DDoS bot sessions collected from such attacks over the same period.

DDoS traffic flow often uneven and inconsistent, thus escaping definitive characterization. Consequently, any study of multiple DDoS events should start with a question of what constitutes a singular attack.

For this research, an attack is defined as a persistent DDoS event against the same target (IP address or domain). It is preceded by a quiet (attack-free) period of at least ten minutes and succeeded by another such period of the same duration or longer.

The following study also makes a distinction between two DDoS event types: network layer and application layer attacks. These definitions refer to the OSI model, which conceptualizes the process of data transmission by segmenting packets into seven layers.

Thus, network layer attacks target the network and transport layers (OSI layers 3 and 4). Such high-volume assaults have the ability to cause network saturation by utilizing much of the available bandwidth resources.

Network layer attacks are typically measured in Gbps (gigabits per second), for the amount of bandwidth they’re able to consume per second.

Application layer attacks, on the other hand, target OSI layer 7. Unlike their network layer counterparts, these can bring down a server by overbearing its processing resource (e.g., CPU) with a high number of requests.

Application layer assaults are measured in RPS (requests per second), for the amount of processing tasks initiated per second. They are executed by bots—inhuman visitors that are able to establish a TCP handshake to interact with a targeted application.
Network Layer Attacks

Overview

In the second quarter of 2015, we continued to see an increase in DDoS attack volumes from 2014, with the largest network layer assault peaking at over 253Gbps. Concurrently, we also continued to notice an increase in attack duration from 2014, with the longest network layer event lasting over 64 days, and 20.4 percent of attacks lasting over five days.

Of attack vector types, large-SYN flood (packet-size of 250 bytes and above) currently displays the most damage potential, followed by UDP flood. The latter is the most common type, used in over 55 percent of all documented DDoS attacks on the Incapsula network during the period of the report—partly due to an increase in the number of SSDP assaults.

Many of the events mitigated in the second quarter of 2015 carry the markings of botnets-for-hire services (a.k.a., booters or stressers), which we associate with many of the shorter and more rudimentary DDoS attacks against Incapsula clients.
**Introduction**

**Report Highlights**

**Methodology**

**Network Layer Attacks**

**Overview**

**Attack Duration**

**Attack Vectors**

**Multi-Vector Attacks**

**Botnet-for-Hire**

**Application Layer Attacks**

**Overview**

**Attack Duration and Frequency**

**Botnet Activity and Geolocation**

**DDoS Bot Capabilities and Identities**

**Conclusion**

**Shady Economy of DDoS Attacks**

---

**Attack Duration**

As evidenced by the graph below, most network layer DDoS events mitigated in this period were either very short attacks or extremely prolonged barrages, with roughly 71 percent of DDoS occurrences lasting under three hours and 20.4 percent occurring over five days.

---

![Network layer DDoS Attack (by duration)](image)

**Figure 2: Distribution of network layer DDoS attacks, by duration**

The polarity illustrated in the distribution of these assault types makes a discussion about average duration fairly impossible. It does, however, point to the existence of two common DDoS scenarios:

1. A short single-vector attack, usually of a duration under 30 minutes, likely used for probing a target’s defenses or for **hit-and-run** tactics. These are more likely to be launched by inexperienced assailants by way of DDoS-for-hire services, the latter offering their users the ability to launch n minute-long attacks per month.

2. An extended day-long DDoS event, in which perpetrators relentlessly pound at an objective using different attack vector mixes to punch a hole through target defenses. These are very likely the work of skilled cyber thugs, wielding their own botnet resources.
Single and Multi-Vector DDoS Attacks (by duration)

<table>
<thead>
<tr>
<th>Duration</th>
<th>Single Vector Attack</th>
<th>Multi Vector Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short attacks</td>
<td>28.2%</td>
<td>71.8%</td>
</tr>
<tr>
<td>Long Attacks</td>
<td>10.9%</td>
<td>89.1%</td>
</tr>
</tbody>
</table>

**Figure 3: Distribution of single and multi-vector DDoS attacks, by duration**

**Attack Vectors**

By far, UDP and SYN floods are the most common “weapons of choice” for DDoS attacks against the Incapsula network in Q2 2015, having been used in over 56 percent of all attacks. Of these, eight percent are SSDP DDoS attacks, launched from “Internet of Things” devices.

**Network Layer DDoS Attack Vectors (by commonness)**

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>56.7%</td>
</tr>
<tr>
<td>SYN</td>
<td>50.7%</td>
</tr>
<tr>
<td>Large SYN</td>
<td>22.0%</td>
</tr>
<tr>
<td>TCP</td>
<td>21.2%</td>
</tr>
<tr>
<td>DNS</td>
<td>12.3%</td>
</tr>
<tr>
<td>ICMP</td>
<td>10.4%</td>
</tr>
<tr>
<td>NTP</td>
<td>9.5%</td>
</tr>
<tr>
<td>DNS Amp.</td>
<td>7.9%</td>
</tr>
</tbody>
</table>

**Network Layer DDoS Attack Vectors (by peak attack volume)**

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Peak Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>61.1 Gbps</td>
</tr>
<tr>
<td>SYN</td>
<td>28.2 Gbps</td>
</tr>
<tr>
<td>Large SYN</td>
<td>73.9 Gbps</td>
</tr>
<tr>
<td>TCP</td>
<td>17.6 Gbps</td>
</tr>
<tr>
<td>DNS</td>
<td>33.5 Gbps</td>
</tr>
<tr>
<td>ICMP</td>
<td>6.0 Gbps</td>
</tr>
<tr>
<td>NTP</td>
<td>39.7 Gbps</td>
</tr>
<tr>
<td>DNS Amp.</td>
<td>18.8 Gbps</td>
</tr>
</tbody>
</table>

**Figure 4: Distribution of DDoS attack vectors, by commonness**

**Figure 5: Distribution of DDoS attack vectors, by peak attack volume**
Notably, we see DNS and NTP amplification attacks falling out of favor, when compared to their popularity in early 2014. This is likely the combination of several factors, including:

- Ongoing efforts to harden the security of NTP servers and open DNS resolvers.
- The relative ease with which amplification attacks can be detected.
- The inflation of botnet resources, which enables the launching of large-scale attacks without the need for amplification.

To address the last point, analysis of peak volumes generated by each attack vector shows that large-SYN floods are the single most-damaging attack type.

### Multi-Vector Attacks

Historically, we’ve always considered multi-vector usage to be the hallmark of a more sophisticated attacker. In light of that, it’s interesting to note that in this period only 56 percent of all network layer attacks were multi-vector, compared to 81 percent in the period from November 30, 2013 to February 27, 2014.\(^1\)

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{multi-vector_attacks.png}
\caption{Distribution of single-vector vs. multi-vector attacks, compared to 2014}
\end{figure}

While this could be short-lived, this downward trend may also be the result of increased activity by botnet-for-hire services. These typically offer a limited number of attack scripts, often used to launch uncomplicated DDoS attacks (a large number of which could tip the statistical scale).

This notion is reinforced by the relative prominence of short, single-vector attacks [see Figure 3], many of which are also attributed to botnets-for-hire.

Network Layer DDoS Attacks [by number of vectors]

Figure 7: Distribution of network layer DDoS attacks, by number of vectors

Botnet-for-Hire

The growing botnet-for-hire industry offers the option to execute rudimentary DDoS attacks to anyone willing to pay for such a service.

As mentioned, the telltale marks of botnet-for-hire services appear on many DDoS assaults directed against our clients. Specifically, we associate these with many of the shorter and more rudimentary DDoS events—a description that fits roughly 40 percent of all mitigated network layer attacks in the second quarter of 2015.

This assumption is solidified by the nuances of the botnet-for-hire business model—a subscription scheme that provides each user with limited access to the botnet resources (usually for a cumulative duration of no more than 60 minutes per month).

During these short periods, individuals with little or no DDoS skill are able to execute assaults using one of the few available scripts (which are reminiscent of our definition of attack vectors).

Pricewise, our review of 20 botnets-for-hire shows that the average subscription fee for a one hour/month DDoS package is roughly $38.
with fees as low as $19.99. The services vary in damage potential, with some advertised attack volumes reaching above 200Gbps. Such numbers, however, are unlikely to reflect actual volumes generated by these botnets.

Even with actual capacity being much lower, however, these still pose a serious threat to most under-protected infrastructures.
Introduction

Report Highlights

Methodology

Network Layer Attacks
Overview
Attack Duration
Attack Vectors
Multi-Vector Attacks
Botnet-for-Hire

Application Layer Attacks
Overview
Attack Duration and Frequency
Botnet Activity and Geolocation
DDoS Bot Capabilities and Identities

Conclusion

Shady Economy of DDoS Attacks

Application Layer Attacks

Overview

In Q2 2015 we saw spike activity from devices infected with MrBlack, Nitol, PCRat, and Cyclone malware, with 15 percent of all attacks originating from China. The largest application layer assault against our clients peaked at nearly 179,712 requests per second (RPS).

The longest application layer attack lasted for eight straight days, with the average duration stretching for just over two and a half hours. Once initially targeted, a website will be hit again every ten days on average.

![Figure 9: Largest application layer attack this past quarter, peaking at 179,747RPS](image)

Compared to data collected during the past twelve months, we notice a shift in DDoS bot populations. More and more impersonator bots are assuming non-generic identities in an effort to bypass rudimentary, signature-based security solutions.

As part of that trend, in Q2 2015 we encountered a significantly lower number of DDoS bots trying to pass themselves off as search engine crawlers—where the two most common impersonator (Google and Baidu) instances didn’t even amount to one percent of all DDoS bot traffic combined.
**Introduction**

**Report Highlights**

**Methodology**

**Network Layer Attacks**

**Overview**

**Attack Duration**

**Attack Vectors**

**Multi-Vector Attacks**

**Botnet-for-Hire**

**Application Layer Attacks**

**Overview**

**Attack Duration and Frequency**

**Botnet Activity and Geolocation**

**DDoS Bot Capabilities and Identities**

**Conclusion**

**Shady Economy of DDoS Attacks**

---

**Attack Duration and Frequency**

Illustrated in the graph below, most application layer attacks (just under 98 percent) lasted under 24 hours, with 52 percent being no more than one hour.

![Distribution of Application Layer DDoS Attacks](image)

Unlike network layer attacks, application layer events can always be accurately associated with their targets. This provides us with the opportunity to correctly assess the number of concurrent attacks launched against the same target.

That analysis shows that nearly half of all websites targeted by an application layer barrage were assaulted more than once, with over 17 percent being attacked more than five times and ten percent being targeted more than ten times during the 72-day period.

![Distribution of Application Layer Attacks](image)

---

*Figure 10: Distribution of application layer DDoS attacks, by duration*

*Figure 11: Distribution of application layer attacks, by frequency of assault against a target*
The image that emerges is that of repeated, medium-length attack bursts, continuously launched against any target unlucky enough to grab the attention of perpetrators. With application layer events being relatively less resource-demanding, it only makes sense for DDoS offenders to try and try again.

**Botnet Activity and Geolocation**

IP spoofing is a common practice in network layer attacks; it helps perpetrators mask their real IP and, as a result, their geolocation. Spoofing, however, is not an option in relation to application layer assaults, which require the attacking device to complete a full three-way TCP handshake. Here its true IP address is always unveiled.

Consequently, tracing back application layer attacks to their countries of origin is the best way to obtain accurate data about botnet geolocations around the globe.

In Q2 2015, we saw nearly 15 percent of all application layer DDoS traffic emerging from China—followed by Vietnam, US, Brazil and Thailand. The latter was home for most of the MrBlack-infected routers, used in a mass-scale DDoS campaign we reported about one month ago.
Introduction

Report Highlights

Methodology

Network Layer Attacks

Overview
Attack Duration
Attack Vectors
Multi-Vector Attacks
Botnet-for-Hire

Application Layer Attacks

Overview
Attack Duration and Frequency
Botnet Activity and Geolocation

DDoS Bot Capabilities and Identities

Conclusion
Shady Economy of DDoS Attacks

Shown in the next graph, MrBlack-infected devices were also the most active in attacks against our clients, followed by Nitol, PCRat, Cylone, and DirtJumper.

![Application Layer Attack Requests](image1)

![Application Layer Attacking IPs](image2)

Interestingly, the number of MrBlack-infected devices is relatively small, with the DDoS malware appearing on no more than 5 percent of botnet devices used in attacks against or clients (Figure 14).

However, due to the relative high capacity of the routers it compromised, it was able to generate much higher attack volumes, even when compared to the expansive Nitol botnet which accounted for 59 percent of all botnet IPs attacking our clients in Q2 2015.

**DDoS Bot Capabilities and Assumed Identities**

The evolution of DDoS bots is a hot topic for us and others in our industry. It epitomizes the constant tug-of-war between the bot herders and security providers, with any newly-introduced penetration capabilities reflecting the perpetrators’ understanding of mitigation technology.

In Q2 2015, we continued to see roughly the same percentage of primitive bots as we saw in the period from November 30, 2013 to February 27, 2014, as published in our previous DDoS Threat Landscape Report of 2014. These “primitives” are categorized as such for their inability to mimic any browser-like capabilities. As a result, all of these can be weeded out by moderately-advanced bot detection mechanisms, including JavaScript (JS) and cookie challenges, out one month ago.
Having said that, it would be wrong to assume that no progress has been made by DDoS offenders. Analysis of HTTP headers, used by DDoS bots to proclaim their identity, reveals a shift from previously popular practices. Specifically, our data shows that many botnet operators have abandoned the use of search engine impersonator bots, which were common throughout 2014.

Overall, search engine user-agents were spotted in less than one percent of all DDoS bots blocked by Incapsula—a steep downward trend from last year when Baidu and Google impersonators alone accounted for 57.7 percent of DDoS bot traffic.
This shift is likely to be a result of wider adoption of IP-based mitigation techniques that can effectively spot bogus search engine clients via ASN verification.

Interestingly, we’ve noticed higher overall diversity in DDoS bots’ user-agent variants, with the top ten most-common types used by only 43 percent of attacks in the data set. This is yet another shift from the period from November 30, 2013 to February 27, 2014, when the most common user-agents appeared in more than 90 percent of all attacks.

Assuming that these trends reflect the hardships with which botnet operators are faced, it looks like many mitigation solutions still rely on very rudimentary, signature-based heuristics.

<table>
<thead>
<tr>
<th>User-Agent Used by DDoS Bots</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)</td>
<td>25.6%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Windows NT 6.2; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0</td>
<td>4.8%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Linux; U; Android 1.5; en-us) AppleWebKit/528.5+ (K-HTML, like Gecko) Version/3.1.2 Mobile Safari/525.20.1</td>
<td>3.7%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1</td>
<td>3.2%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko</td>
<td>1.2%</td>
</tr>
<tr>
<td>Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C)</td>
<td>1.0%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.97 Safari/537.11</td>
<td>0.9%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.11) Gecko/2009082115 Firefox/3.0.11</td>
<td>0.9%</td>
</tr>
<tr>
<td>Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36</td>
<td>0.9%</td>
</tr>
<tr>
<td>Mozilla/5.0 (compatible; Baiduspider/2.0; <a href="http://www.baidu.com/search/spider.html">http://www.baidu.com/search/spider.html</a>)</td>
<td>0.9%</td>
</tr>
</tbody>
</table>

Figure 17: User-agent used by DDoS bots, by commonness
Introduction

Report Highlights

Methodology

Network Layer Attacks
Overview
Attack Duration
Attack Vectors
Multi-Vector Attacks
Botnet-for-Hire

Application Layer Attacks
Overview
Attack Duration and Frequency
Botnet Activity and Geolocation
DDoS Bot Capabilities and Identities

Conclusion

Shady Economy of DDoS Attacks

Traditionally, much of the conversation about DDoS threats has been focused on rising assault volumes and increased attack sophistication. While highlighting those does help raise awareness to the problems posed by DDoS attacks, it does not paint a full picture of the business implications.

In this report, we’ve made an effort to highlight attack duration and frequency data. Combined with an understanding of downtime cost, IT decision-makers can assess potential DDoS risks.

On average (according to our 2014 DDoS Impact Survey) an unmitigated attack costs a business $40,000 per hour. Implications go beyond lost business opportunities to include loss of consumer trust, data theft, intellectual property loss, and more. Today, with top attack percentiles lasting for days, and half of all targets being repeatedly hit, a worst-case scenario entails significant financial losses.

What is most disconcerting is that many of these smaller assaults are launched from botnets-for-hire for just tens of dollars a month. This disproportion between attack cost and damage potential is the driving force behind DDoS intrusions for extortion and vandalism purposes.

For Q2 2015 we estimate that roughly 40 percent of our clients were exposed to attacks from botnets-for-hire. While these were mitigated, there is no reason why online organizations should face such dangers at all.

Perhaps putting a price tag on the damage caused by such services will bring more public attention to their activity, and to the danger posed by the shady economy behind DDoS attacks.
What’s next

- To learn more about the business effects of DDoS attacks, read this free 2014 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.

Sign up for a free trial
No software to download or equipment to hook up

Get Started Today

About Imperva Incapsula

Incapsula’s cloud-based Application Delivery gives online businesses a complete solution for maximizing the security, speed and availability of their websites. Tens of thousands of businesses worldwide—from e-commerce sites to high-profile SaaS providers, Fortune 500 companies and large financial institutions—use Incapsula’s service to secure and accelerate their websites and web applications.

Founded in 2009 by a group of security industry veterans specializing in web application security, Incapsula was spun out of and subsequently acquired by Imperva, a world-leading provider of data security solutions.