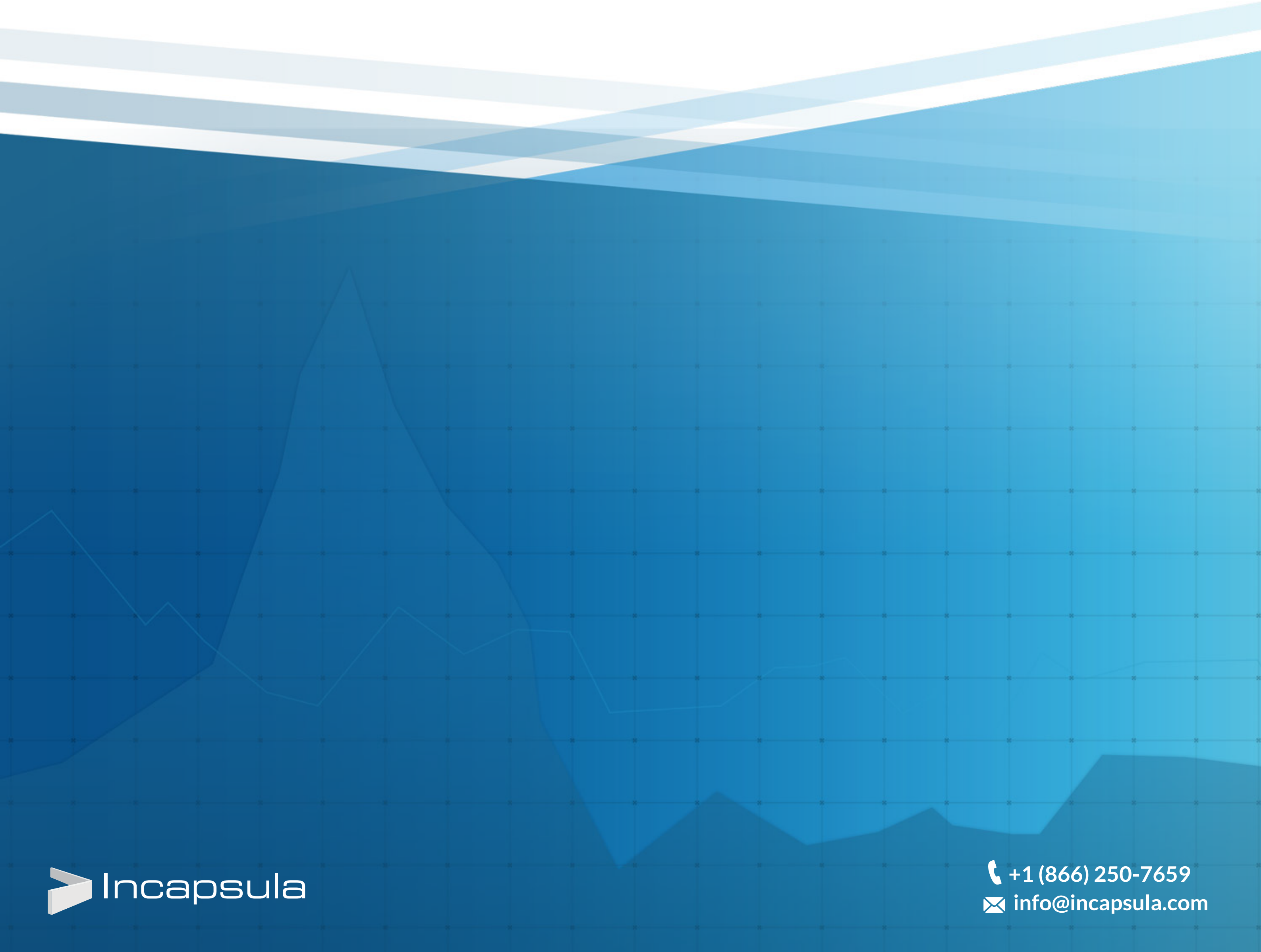
2013-2014

DDoS Threat Landscape Report



Incapsula

☎ +1 (866) 250-7659
✉ info@incapsula.com

Introduction

This report was originally intended to be a 2013 DDoS trends report. However, due to the significant DDoS events in January and February of 2014, we have extended the scope of this report to also include the last 90 days. We believe that the trends discovered during this period, in particular, are essential in order to accurately portray the current state of today's DDoS threat landscape.

The findings below are based on hundreds of attacks perpetrated against websites using Incapsula's DDoS Mitigation service and include the latest Network (Layers 3 & 4) and Application (Layer 7) DDoS trends. We believe that these attacks are a fair representation of the overall DDoS threat landscape and lend valuable insight into the current challenges facing the DDoS protection industry.

At a Glance:

Network (Layer 3 & 4) DDoS Attacks

- Large SYN Floods account for 51.5% of all large-scale attacks
- Almost one in every three attacks is above 20Gbps
- 81% of attacks are multi-vector threats
- Normal SYN flood & Large SYN flood combo is the most popular multi-vector attack (75%)
- NTP reflection was the most common large-scale attack method in February 2014

Application (Layer 7) DDoS Attacks

- DDoS bot traffic is up by 240%
- More than 25% of all Botnets are located in India, China and Iran
- USA is ranked number 5 in the list of "Top 10" attacking countries
- 29% of Botnets attack more than 50 targets a month
- 29.9% of DDoS bots can hold cookies.
- 46% of all spoofed user-agents are fake Baidu Bots (while 11.7% are fake Googlebots)

Research Methodology

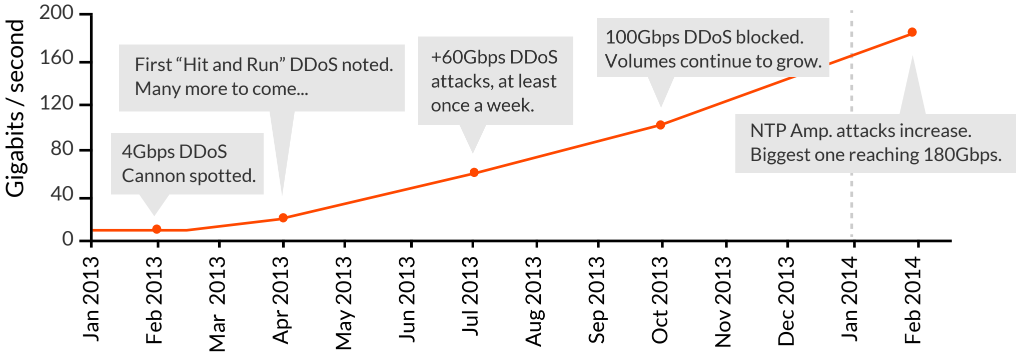
The 2013-2014 trending graphs are based on peak attack volumes and notable DDoS events recorded over this period. Network (Layers 3 & 4) DDoS attack volumes are measured in Gbps (Gigabits per second); Application (Layer 7) peak attack volumes are measured in MRpm (Millions of Requests per minute).

The last 90-days data was collected from November 30, 2013 to February 27, 2014. The network DDoS trending information is based on 237 network DDoS attacks that exceeded 5Gbps, targeting websites on Incapsula's network.

Information about the Application (Layer 7) DDoS attacks is based on records of over 154 million unique DDoS bot sessions on Incapsula's network during this period. (Read more about Incapsula's bot classification techniques.)

Network (Layers 3 & 4) DDoS Attacks

2013: Overview



In 2013 we witnessed a rapid increase in network DDoS attack volumes, which was facilitated by the adoption of new attack methods (NTP Amplification and Large SYN floods) and also by the development of Internet and specifically cloud infrastructures.

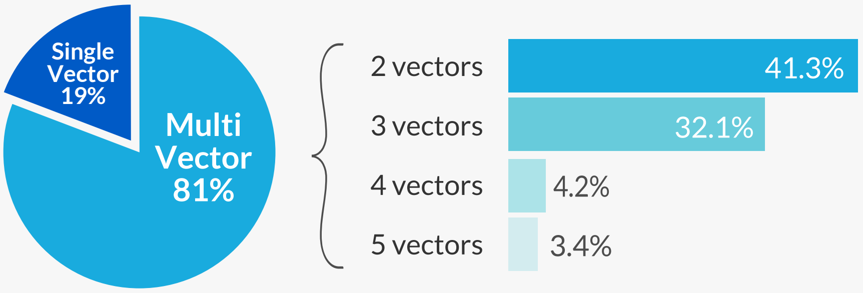
As early as February 2013 we were able to track down a single source 4Gbps attacking server, which – if amplified – could alone have generated over 200Gbps in attack traffic. With such available resources it is easy to explain the uptick in attack volume we saw over the course of the year.

“Hit and Run” DDoS attacks, which were first documented in April 2013 are part of another parallel trend of attacks that were specifically designed to exploit vulnerabilities in DDoS protection services and human IT operators. These attacks, which rely on frequent short bursts of traffic, are specifically designed to exploit the weakness of services that were designed for manual triggering (e.g., GRE tunneling to DNS re-routing). Hit and Run attacks are now changing the face of anti-DDoS industry, pushing it towards “Always On” integrated solutions.

2014: Emerging Trends

Over 81% of Attacks Are Multi-Vector Threats

Network DDoS Attacks: Distribuition by Number of Vectors



The vast majority of network (Layers 3 & 4) DDoS attacks rely on multi-vector offensive tactics. Figures show that in the last 90 days, 81% of all network attacks employed at least two different attack methods, with almost 39% using three or more different attack methods simultaneously.

Multi-vector tactics increase the attacker's chance of success by targeting several different networking or infrastructure resources.

Combinations of different offensive techniques are also often used to create "smokescreen" effects, where one attack is used to create noise, diverting attention from another attack vector. Moreover, multi-vector methods enable attackers to exploit holes in a target's security perimeter, causing conflicts in automated security rules and spreading confusion among human operators.

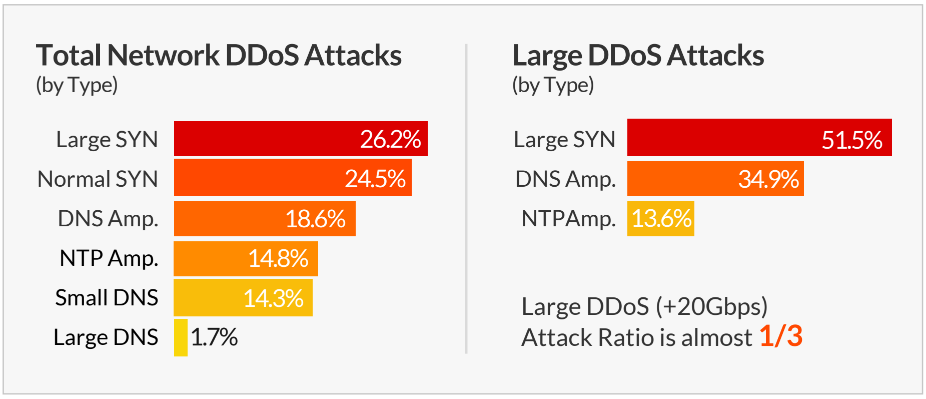
Finally, multi-vector attacks can be used for "trial and error" reconnaissance, gathering the information needed to allow future attacks to weave their way past the defender's layers of security.

Multi-Vector Attacks Facilitate Hyper Growth

The nature of the latest attack trends is a good indicator of the direction in which modern network DDoS attacks are now taking. The multi-vector approach, which is already used by the vast majority of all network attacks, is a clear indication of attackers' familiarity with current DDoS protection methods and the ways in which these methods can be bypassed and overcome.

Another clue comes from the attackers' most common "weapons of choice": i.e., large SYN floods, NTP Amplification and DNS Amplification.

All of these vectors are used to carry out large-scale DDoS
dangerous both due to their size and their ability to clog the



Today large scale DDoS attacks (20Gbps and above) already account for almost 33% of all network DDoS events. There is no doubt that the increasing adoption of these techniques will facilitate the growth of future volumetric network DDoS attacks, which could in turn drive an increase in investment in networking resources.

Weapon of Choice: Combo SYN Flood Attacks

Based on average data from the last 90 days, the most common network attack method was a combination of two types of SYN flood attacks – one using regular SYN packets and another using large SYN (above 250 bytes) packets.

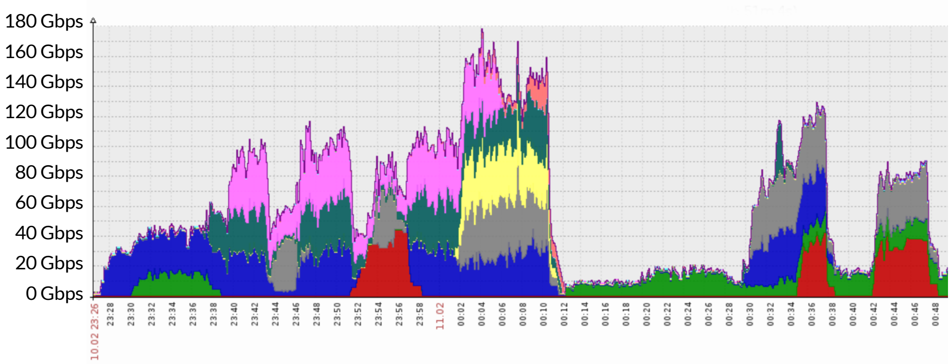


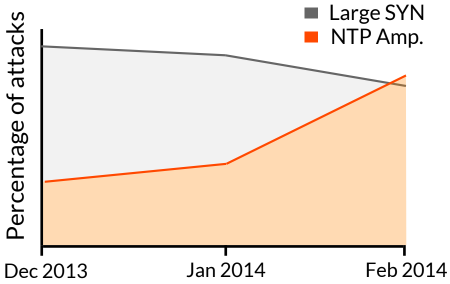
Figure 1: *180Gbps NTP Amplification DDoS Attack (50Mpps)*

In this scenario, both attacks are executed at the same time, with the regular SYN packets used to exhaust server resources (e.g., CPU) and large SYN packets used to cause network saturation.

Today SYN combo attacks account for ~75% of all large scale network DDoS events (attacks peaking above 20Gbps). Overall, large SYN attacks are also the single most commonly used attack vector, accounting for 26% of all network DDoS events.

On The Rise - NTP Amplification Attacks

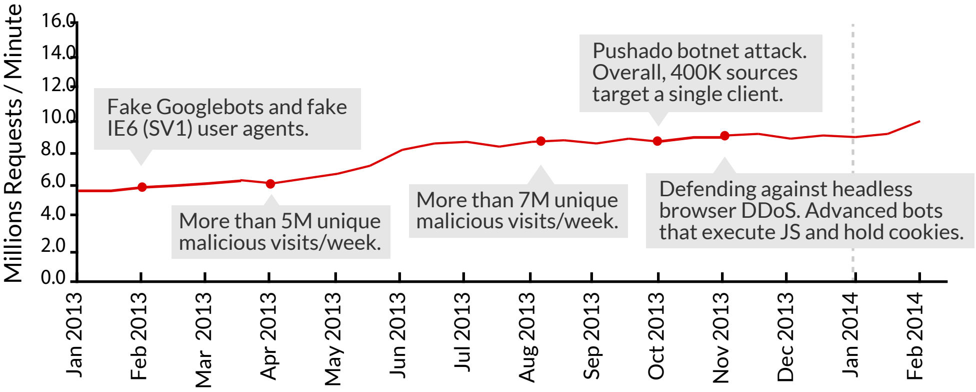
During January and February of 2014 a significant increase in the number of NTP Amplification attacks was noted. In fact, this reached the point where, in February, NTP Amplification attacks became the most commonly used attack vector for large scale network DDoS attacks.



It is still too early to say if this points to a consistent trend or just to a temporary spike, fueled by the public attention given to the recent high profile NTP Amplification attacks.

Application (Layer 7) DDoS Attack

2013: Overview



Fake Googlebots and fake IE6 (SV1) user agents.

More than 5M unique malicious visits/week.

More than 7M unique malicious visits/week.

Pushado botnet attack. Overall, 400K sources target a single client.

Defending against headless browser DDoS. Advanced bots that execute JS and hold cookies.

Over the course of 2013 Incapsula witnessed an evolution of Application (Layer 7) DDoS attack methods. In the first half of 2013 most application DDoS attacks were executed by relatively primitive bots, which could be thwarted with a combination of progressive challenges and signature-based security rules.

However, in the second half of 2013 we began to encounter a much more complex breed of DDoS offenders, including browser-based bots which were immune to generic filtering methods and could only be stopped by a combination of customized security rules and reputation-based heuristics.

The significant evolution of application DDoS tools didn’t translate into an increase in application DDoS attack volumes, which remained relatively unchanged throughout the period. This is because even a rate of 50-100 requests/second would be enough to cripple most mid-sized websites, exceeding typical capacity margins and obviating the need for increased volumes.

2014: Emerging Trends

Locations of Botnets and Vulnerable IT Infrastructures

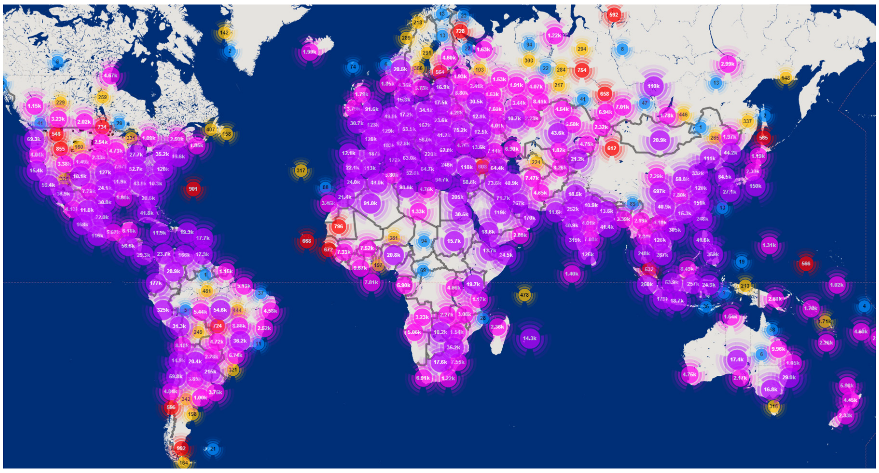


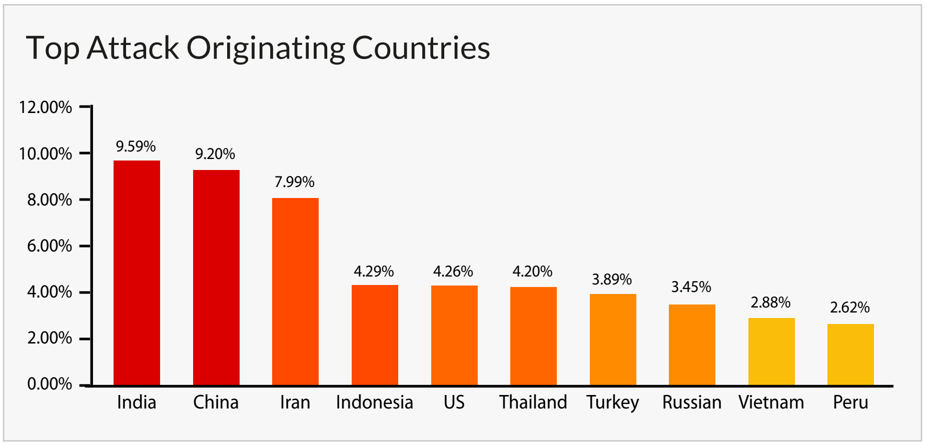
Figure 2: *Application Layer Weekly Attack Map*

On average, Incapsula recorded over 12 million unique DDoS bot sessions on a weekly basis, which represents a 240% increase over the same period in 2013.

Unlike network DDoS attacks, Layer 7 attack sources can’t hide behind spoofed IPs. Instead they resort to using Trojan infected computers, hijacked hosting environments and Internet-connected devices. Large groups of such compromised resources constitute a botnet; a remotely controlled “zombie army” that can be used for DDoS attacks and other malicious activities.

IP records of application DDoS offenders help us pinpoint actual geo-locations of active DDoS botnets and the non-secure infrastructures in which they thrive.

Over the past 90 days, Incapsula’s records show that over 50% of all DDoS bots came from a group of 10 countries - with India, China and Iran accounting for over 25% of all malicious traffic.

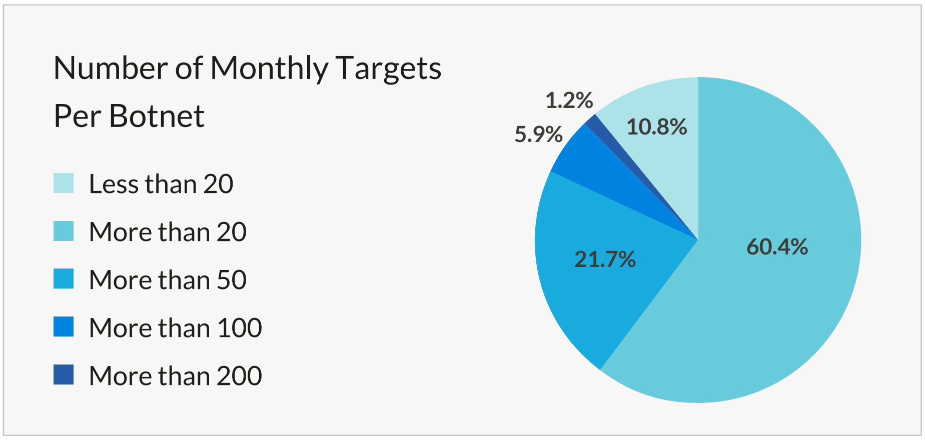


Random sampling of attacking IP addresses uncovers large number of vulnerable privately-owned websites, many of which are using the WordPress CMS platform.

However, it’s also not uncommon to trace the attack back to compromised servers of web hosting companies, websites of commercial organizations and educational institutions (.ac domains) or – in some cases - even government-owned assets (.org domains). The list of compromised resources also includes a wide variety of connected devices, typically CCTV surveillance devices, most of which are open to abuse through easily guessable default passwords.

29% of Botnets Attack More than 50 Targets a Month

Continuous tracking of attacking IP addresses shows that DDoS botnets are being reused to attack multiple targets. On average, almost 29% of all compromised devices will attack more than 50 different targets each month, with 1.2% attacking over 200 different targets during the same period.

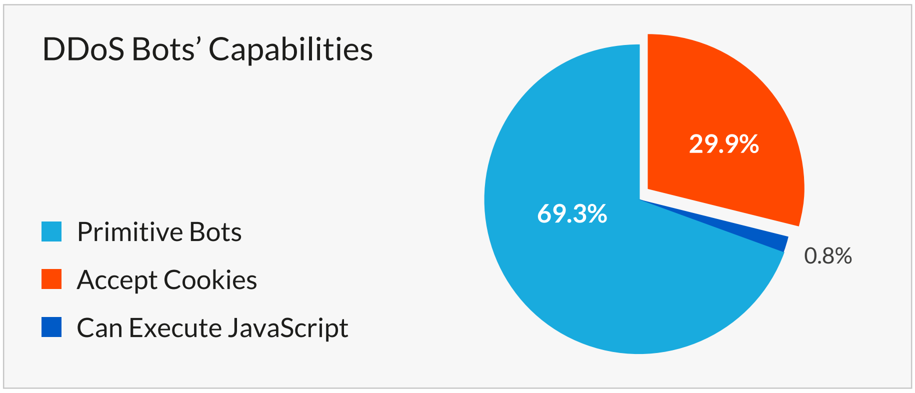

Number of Monthly Targets Per Botnet

These numbers provide an interesting glimpse at the mechanics behind “Shared Botnets”. Looking at the figures, one can clearly see that today DDoS resources are treated just like any other type of rentable infrastructure. At the same time, one can also assume that some of these resources change hands between members of the hacker community. Some even have multiple “owners”, with several "botnet shepherds" using the same compromised machine for several different purposes.

In terms of proactive security, this data further validates the need for reputation-based security methods. Thus, by systematically collecting such data, one can better anticipate the intentions of a visitor, knowing that some should be treated with more suspicion than others.

Bots are Evolving - Developing Immunity to Cookie and JavaScript Challenges

2013 brought abundant evidence of the increased sophistication of DDoS bots and other application DDOS threats. In the fourth quarter of 2013, Incapsula reported the first encounter with browser-based DDoS bots that were able to bypass both JavaScript and Cookie challenges - the two most common methods of bot filtering.



This trend continues in 2014. Overall, in almost 30% of all recorded sessions, the DDoS bots Incapsula encountered were able to accept and store cookies, while 0.8% of these bots could also execute JavaScript.

This data points to the reduced efficiency of these commonly used filtering methods. Even in the case of JS challenges, where the numbers are still typically low, the mere existence of "immune" offenders hints at the evolution we expect to see in the near future.

To counter these challenges, Layer 7 mitigation processes should be based on a combination of more subtle methods, which assign a contextual risk score to the visitor’s identity and behavior patterns. Furthermore, given the reuse of attacking resources, approaches that make use of reputation data are also advised.

Common Spoofed User-Agents

DDoS bots are designed for infiltration. To that end, spoofed user-agents are often used to bypass low-level filtering solutions, based on the assumption that these solutions will not filter out bots that identify themselves as search engine or browsers.

The list below details the ten most commonly spoofed user-agents. The top five entries belong to Baidu and Googlebot impersonators and variant of Microsoft IE browsers. When combined, these appear to be responsible for almost 85% of all malicious DDoS bot sessions. However, it should also be noted that many DDoS offenders will employ “agentless” bots or bots with uniquely crafted headers that were not designed to mimic the signatures of other web clients.

Top 10 Spoofed User-Agents Used by DDoS Bots

33.0%	**Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)**
16.0%	**Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)**
13.0%	**Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)**
11.7%	**Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)**
10.4%	**Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)**
6.8%	Mozilla/4.0 (compatible; MSIE 7.00; Windows NT 5.0; MyIE 3.01)
6.5%	Mozilla/4.0 (compatible; MSIE 8.00; Windows NT 5.0; MyIE 3.01)
1.6%	Mozilla/5.0 (X11; U; Linux i686; en-US; re:1.4.0) Gecko/20080808 Firefox/8.0
0.2%	Mozilla/4.0 (Windows; U; Windows NT 5.1; zh-TW; rv:1.9.0.11)
0.1%	Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)

Looking at the list, one can immediately notice the prominence of “search engine mimics”. From a mitigation point of view, these represent the easiest of all application layer challenges, due to the highly predictable behavior patterns of real search engine bots as well as their predetermined points of origin.

Looking Forward

2013 was a game-changing year for DDoS attacks, with higher-than-ever attack volumes and rapid evolution of new attack methods. Now, the perpetrators are looking to raise the stakes even higher by introducing new capabilities, many of which are specifically designed to abuse the weaknesses of traditional anti-DDoS solutions. As a result, in 2014, many IT organizations will need to re-think their security strategies to respond to latest Layer 3-4 and Layer 7 DDoS threats.

In case of network DDoS threats, the escalated growth of attack volumes has already established demand for scalable cloud-based solutions. To accommodate that, we now are increasing our investments in Incapsula’s infrastructures; both to keep up with our growing customer base and buff up Incapsula’s network capacity. In Q1 2014 we’ve already activated three new datacenters which increased Incapsula’s network throughput to 630Gbps and we are committed to significantly expand on that over the course of the year.

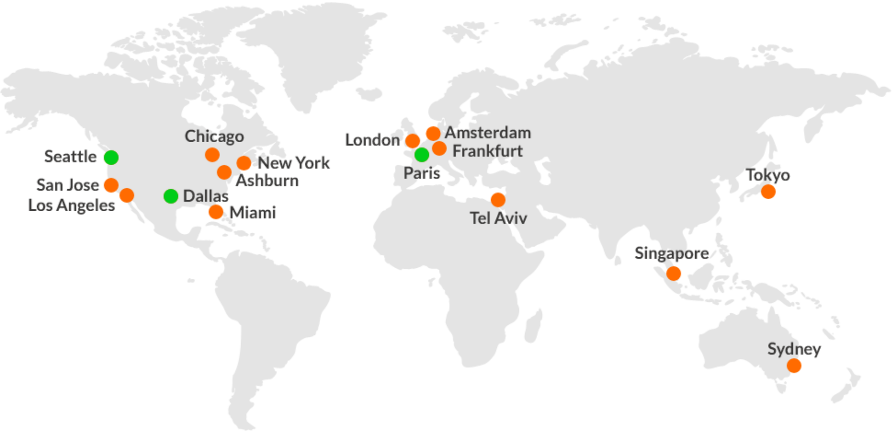


***Figure 3:** Incapsula’s data center deployment map. New facilities are in green.*

With respect to application layer DDoS, we foresee rapid evolution of intelligent traffic filtering solutions, driven by technological sopistication of current-gen DDoS bots. Today, most filtering options still rely on combinations of basic challenges, whose effectiveness is now gradually eroding. And so, it’s only a matter of time before a high-profile application layer attack will expose this issue, compelling organizations to seek better alternatives that rely on combination of challenge based and non-challenge based techniques.

Incapsula is already heavily invested in developing such multi-layered mitigation solution and we are already use behavioral and reputational factors to provide context to visitors’ actions and motivations. Combined with major updated of our backbone infrastructures, these will allow us to provide comprehensive DDoS protection services, helping us clients meet both current and future challenges