IMPERVA®

The Top 10 DDoS Attack Trends

Discover the Latest DDoS Attacks and Their Implications

Introduction

The volume, size and sophistication of distributed denial of service (DDoS) attacks are increasing rapidly, which makes protecting against these threats an even bigger priority for all enterprises. In order to better prepare for DDoS attacks, it is important to understand how they work and examine some of the most widely-used tactics.

What Are DDoS Attacks?

A DDoS attack may sound complicated, but it is actually quite easy to understand. A common approach is to "swarm" a target server with thousands of communication requests originating from multiple machines. In this way the server is completely overwhelmed and cannot respond anymore to legitimate user requests. Another approach is to obstruct the network connections between users and the target server, thus blocking all communication between the two – much like clogging a pipe so that no water can flow through. Attacking machines are often geographically-distributed and use many different internet connections, thereby making it very difficult to control the attacks. This can have extremely negative consequences for businesses, especially those that rely heavily on its website; E-commerce or SaaS-based businesses come to mind.

The Open Systems Interconnection (OSI) model defines seven conceptual layers in a communications network. DDoS attacks mainly exploit three of these layers: network (layer 3), transport (layer 4), and application (layer 7).

Network (Layer 3/4) DDoS Attacks: The majority of DDoS attacks target the network and transport layers. Such attacks occur when the amount of data packets and other traffic overloads a network or server and consumes all of its available resources.

Application (Layer 7) DDoS Attacks: Breach or vulnerability in a web application. By exploiting it, the perpetrators overwhelm the server or database powering a web application, bringing it to its knees. Such attacks mimic legitimate user traffic, making them harder to detect.

Why You Need To Read This White Paper

This white paper presents the top ten current methods and trends in DDoS attacks based on real-world observation and data. It provides insight regarding:

- Volumetric attacks
- SYN flood attacks
- NTP amplification attacks
- 'Hit and Run' attacks
- Browser based bot attacks
- Multi target DDoS botnets
- Spoofed user-agents
- Multi-vector attacks
- Attacks from mobile devices
- Geographic locations for attack origination

This white paper concludes with an actionable plan and solutions you can implement to prevent these types of attacks.

Large Scale, Volumetric Attacks Are Getting Bigger

What Are Volumetric Attacks?

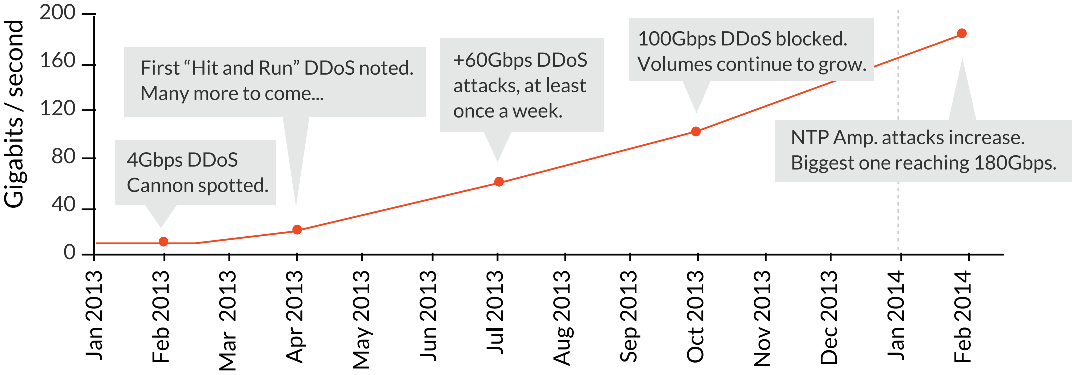
Volumetric attacks flood a target network with data packets that completely saturate the available network bandwidth. These attacks cause very high volumes of traffic congestion, overloading the targeted network or server and causing extensive service disruption for legitimate users trying to gain access.

Volumetric attacks are getting larger, more sophisticated, and are lasting for a longer duration. They can bring any business server down within a few minutes. These network-level (layers 3 and 4) attacks are designed to overwhelm a server's internet link, network resources, and appliances that are not able to absorb the increased volumes.

Latest Trends

- There was a 350% increase in large-scale volumetric DDoS attacks in the first half of 2014 when compared to the previous year.
- Attacks of 20 Gbps and above now account for more than 1/3rd of all network DDoS events.
- DDoS attacks of over 100 Gbps increased to an overwhelming 100+ events in the first half of 2014 alone.

Application (Layer 7) DDoS Attack Overview



Implications

As volumetric DDoS attacks continue to evolve, organizations will need ever more network resources to battle them. Even companies with significant amounts of internet connectivity and bandwidth could see their capacity exhausted by these attacks and buying significant additional bandwidth can be very expensive.

Combo SYN Flood Attacks Are Most Common

Latest Trends

- Combo SYN flood attacks account for 75% of all large scale (above 20Gbps) network DDoS events.
- Half of all network DDoS attacks are SYN flood attacks.
- Large SYN flood are the single most commonly used attack vector, accounting for 26% of all network DDoS events.

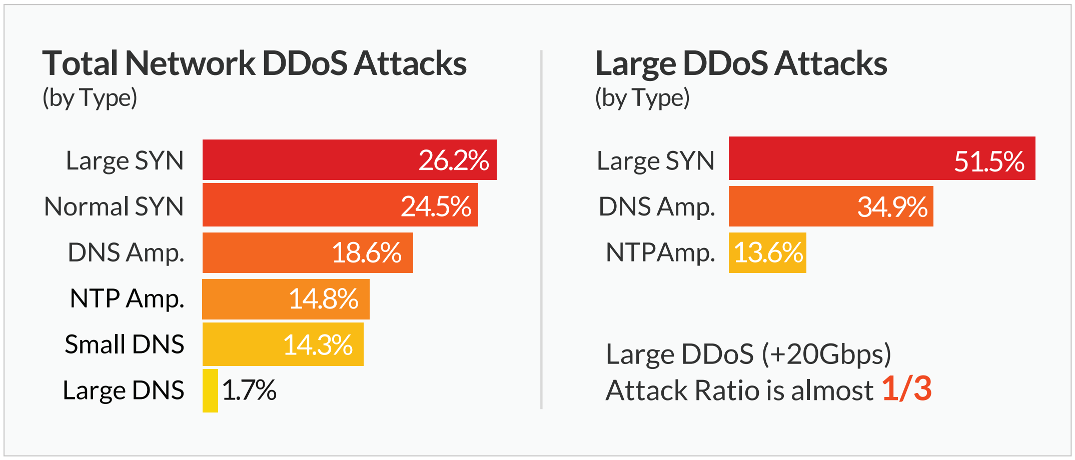
What Are Combo SYN Flood Attacks?

In the TCP connection sequence (the "three-way handshake"), the requester first sends a SYN message to initiate a TCP connection with a host. The server responds with a SYN-ACK message, followed by receipt confirmation of the ACK message by the requester. This opens the network connection.

In a SYN flood attack, the requester sends multiple SYN messages to the targeted server, but does not transmit any confirmation ACK messages. The requester can also dispatch spoofed SYN messages, causing the server to send SYN-ACK responses to a falsified IP address. Of course, it never responds because it never originated the SYN messages. The SYN flood binds server resources until no new connections can be made, ultimately resulting in denial of service.

A combo SYN flood comprises two types of SYN attacks – one uses regular SYN packets, the other large SYN packets above 250 bytes. Both attacks are executed at the same time; the regular SYN packets exhaust server resources (e.g., CPU), while the larger packets cause network saturation.

Multi-Vector Attacks Facilitate Hyper Growth



Implications

A combo SYN flood attack remains the "weapon of choice" for perpetrators. These attacks quickly consume resources of a target server, or of intermediate communications equipment (e.g., firewalls and load balancers), making them difficult to combat using traditional DDoS mitigation strategies.

NTP Amplification Attacks Are Significantly Increasing

What Are NTP Amplification Attacks?

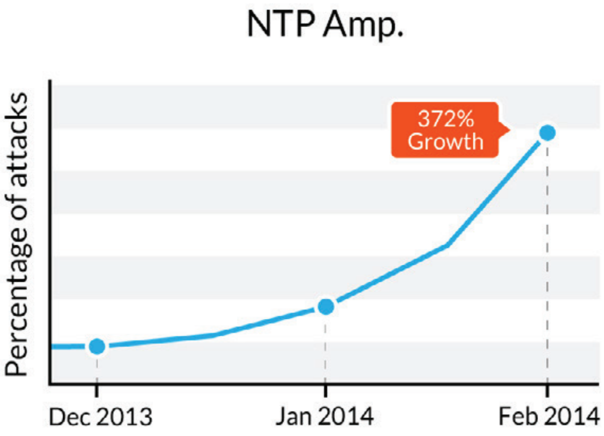
Computers use the Network Time Protocol (NTP) to synchronize their clocks over the internet. NTP amplification attacks exploit a feature on NTP servers; called MONLIST, it returns a list of the last 600 IP addresses that communicated with the server. Attackers send out MONLIST requests to NTP servers using a target server's spoofed IP address. Thus the NTP server response is much larger than the original request. By using numerous vulnerable NTP servers, attackers are quickly able to compromise the target server, it being overwhelmed with multiple data packets.

In part, NTP amplification attacks can be massive because the underlying UDP protocol does not require any handshaking.

Latest Trends

- 400 Gbps NTP amplification attack in February 2014 is the largest DDoS attack ever reported.
- In Q1 2014, the number of NTP amplification attacks increased by an astonishing 372% compared to Q4 2013.
- NTP amplification is now the primary attack vector and is starting to surpass SYN flood attacks.

On The Rise - NTP Amplification Attacks



Implications

There are more than 400,000 NTP servers around the world that can potentially be used in an NTP amplification attack. Some are capable of amplification factors up to 700 times, which could result in a huge blow to internet traffic.

“Hit and Run” Attacks are Ever Persistent

What Are “Hit and Run” Attacks?

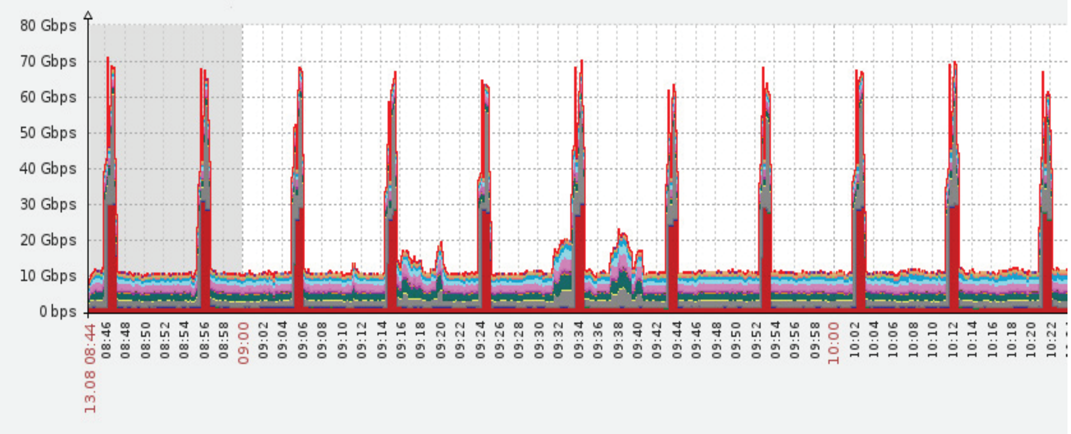
As their name suggests, hit and run attacks consist of short packet bursts at random intervals over a long period of time. What makes these threats different from other DDoS attacks is that they can last for days or even weeks. Also, unlike other attacks, they are not continuous and are designed to specifically exploit slow-reacting anti-DDoS solutions.

Despite the sophistication of other kinds of DDoS threats, hit and run attacks continue to be popular because of their low cost and ease of deployment.

Latest Trends

- Hit and run attacks typically last 20 – 60 minutes in duration.
- After causing some collateral damage to a target server, hit and run attacks usually occur again after another 12 – 48 hours.
- Traditional DDoS prevention solutions, such as GRE tunneling and DNS rerouting, have become ineffective in dealing with these types of attacks.

Hit and Run Attacks



Implications

Hit and run attacks wreak havoc with “on-demand” DDoS mitigation solutions that need to be manually engaged/disengaged with every burst. Such attacks are changing the face of the anti-DDoS industry, pushing it toward “always on” integrated solutions. Any mitigation that takes more than a few seconds is simply unacceptable.

The Sophistication of Browser-Based Bots

What Are Browser Based Bots?

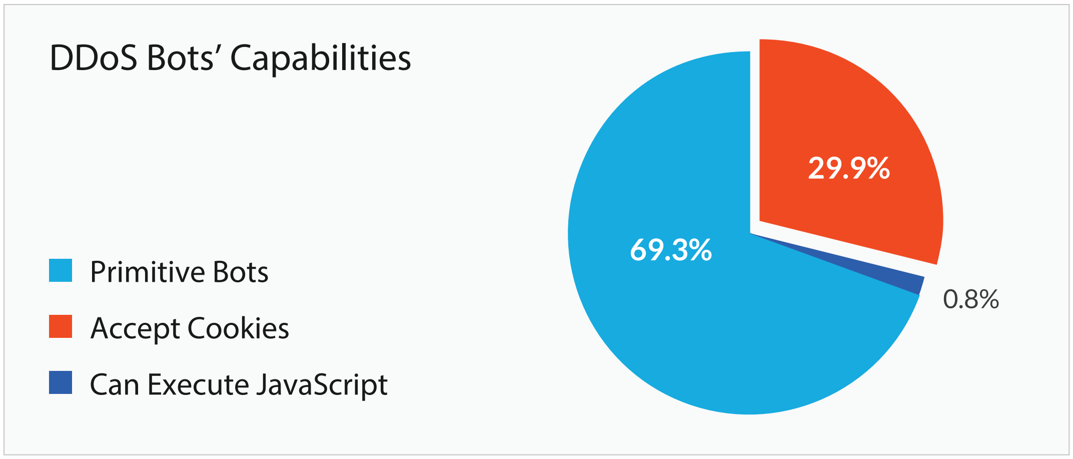
Browser-based bots consist of malicious software code segments running inside a web browser. The bots run during a legitimate web browsing session; once the browser is closed, the bot session automatically terminates. Browser-based bots are surreptitiously installed on unsuspecting users' computers upon visiting a malicious website. Multiple bots can then simultaneously launch an attack against a targeted server from compromised machines.

Some DDoS bot types imitate browser behavior, such as support for cookies, in order to evade anti-DDoS defenses. DDoS bot attacks target the application layer and are extremely dangerous because they don't require high volumes to succeed. It only takes 50 – 100 targeted requests per second to bring down a mid-size server. Bot attacks are hard to detect and often revealed only after the damage has been done.

Latest Trends

- Browser-based DDoS bots are becoming more sophisticated and are now able to bypass both JavaScript and cookie challenges – the two most common methods used for bot filtering.
- 30% of all DDoS bots encountered in 2014 were able to accept and store cookies, while 0.8% of them could also execute JavaScript.

Bots are Evolving - Developing Immunity to Cookie and JavaScript Challenges



Implications

Identifying layer 7 attacks requires an understanding of the underlying application. It also requires proper differentiation between malicious bot traffic, regular bot traffic (such as search engine bots), and human traffic. The ability to analyze incoming traffic and assign a contextual risk score based on the visitor's identity, behavior, and reputation is an additional factor.

Spoofed User-Agents Used In Most Bot Sessions

What Are Spoofed User Agents?

Good bots, such as "Googlebots" are critical to ensuring that websites are properly indexed by search engines. It is therefore important not to accidentally block them.

Spoofing user agents is a frequently-used attack technique. Here the DDoS bots masquerade as "good" bots from reputable sources such as Google or Yahoo, in order to evade detection. Using this method, the bots are able to pass through low-level filters and proceed to wreak havoc on target servers.

Latest Trends

- The top five spoofed agents shown in the list below account for 85% of all malicious DDoS bot sessions.
- Bot traffic accounts for 62% of all website traffic, half of which consists of search engines and other good bots – the other half comprising malicious bots.

Common Spoofed User-Agents

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)

Implications

The list is dominated by malicious bots masquerading as search engine bots. From a mitigation point of view, they represent the easiest of all application layer challenges, due to the highly-predictable behavior patterns of legitimate search engine bots, as well as their predetermined points of origin.

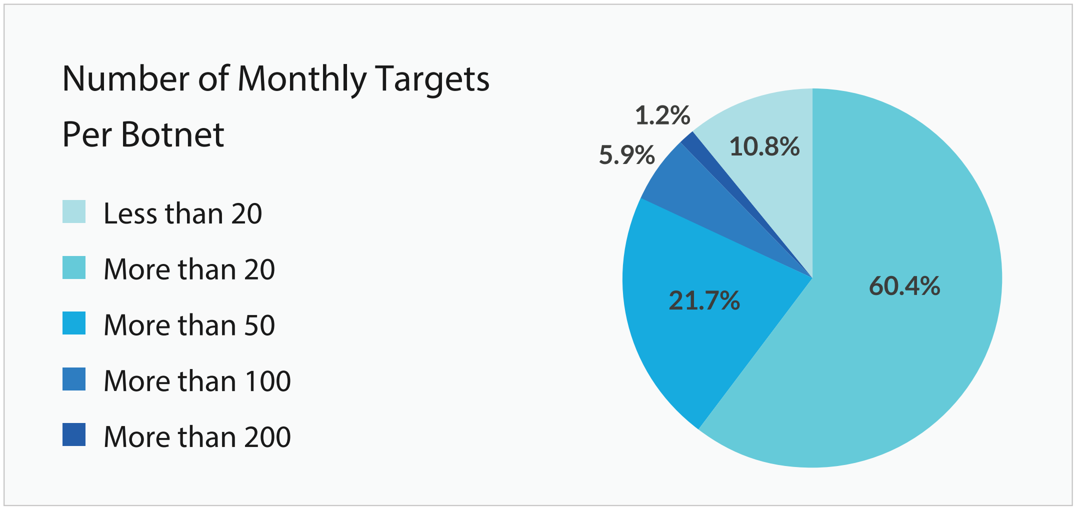
30% of DDoS Botnets Attack 50+ Targets Per Month

What Are Shared Botnets?

A botnet is a group of compromised computers on the internet, taken over by malware. Machine owners are usually unaware of malicious software infiltration, thereby allowing attackers to control their "zombie" machines remotely and launch DDoS attacks. In addition to personal computers, botnets can also include hijacked hosting environments and various internetconnected devices (e.g., CCTV cameras which often have easy-to-guess default passwords).

Botnets are frequently shared between hackers or rented by one attacker from another. They can have multiple owners and use the same compromised machines for launching attacks against different targets. Shared botnets are available for hire on the internet and can be easily launched by non-technical users.

29% of Botnets Attack More than 50 Targets a Month



Implications

Shared botnet attacks continue to significantly increase, because they can be accessed cheaply and easily utilized without any technical knowledge. DDoS mitigation systems must be proactive and use reputation-based security methods to anticipate user intentions (and be able to red flag them as necessary).

Latest Trends

- DDoS botnets are being reused to attack multiple targets. On average, 30% of botnets attack more than 50 targets each month.
- 1.2% of botnets attack over 200 targets each month; both of these numbers are increasing.
- Marketplaces are available across the internet, increasingly selling access to sophisticated botnets for very low prices.

Over 80% of Attacks Use Multi-Vector Approach

What Are Multi-Vector Attacks?

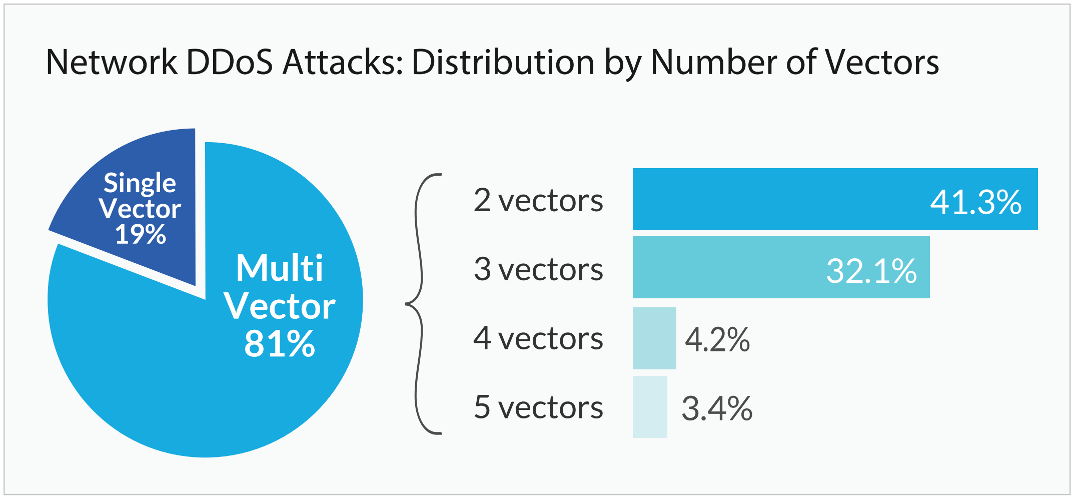
Traditionally, DDoS attack campaigns used a single attack type, or vector. However, there is a rise in DDoS attacks using multiple vectors to disable a network or server(s). Called multi-vector attacks, they consist of some combination of the following: (1) Volumetric attacks; (2) State-exhaustion attacks; and (3) Application layer attacks.

The multi-vector approach is very appealing to an attacker, since the tactic can create the most collateral damage to a business or organization. These attacks increase the chance of success by targeting several different network resources, or using one attack vector as a decoy while another, more powerful vector is used as the main weapon.

Latest Trends

- 81% of DDoS attacks employed at least two types of vectors.
- 40% of DDoS attacks used three or more different vectors at the same time.
- In order to mount large-scale attacks, more than 75% of multi-vector attacks used a combination of SYN methods (such as using regular SYN packets and much larger SYN packets greater than 250 bytes).

Over 81% of Attacks Are Multi-Vector Threats



Implications

The fact that multi-vector attacks are so prevalent now indicates the level of familiarity attackers have developed with website security and DDoS protection products. These attacks can be extremely difficult to mitigate because they require a multi-layered approach across the entire data center/enterprise and a highly-skilled IT team to combat them.

Attacks from Mobile Devices Are Increasing

What Are Mobile Device Attacks?

As markets have become saturated with mobile devices, the number of attacks has dramatically increased. With cellular networks providing more internet bandwidth and faster connectivity, it has become easier for mobile devices to be hijacked and unwittingly used to launch DDoS attacks. Mobile phones and tablets are not impervious to malware, and can be easily infected without the knowledge of their owners. They can then be used to download malicious software and launch DDoS attacks together with other, similarly-hijacked mobile devices, all secretly-controlled by the attacker.

Mobile devices have weaker security protection compared to PCs. Most users do not install any type of anti-virus application on them. Owners also download apps more freely on mobile devices without much thought regarding security. This makes it easier for malicious apps to compromise these devices.

Latest Trends

- More powerful mobile devices and downloadable attack apps (especially on Android-based devices) have made it much easier for attacks to be launched from them.
- New tools, such as Low Orbit Ion Cannon (LOIC), are freely available and let individuals intentionally "opt in" to participate in attacks.

Implications

With mobile devices becoming more ubiquitous and powerful, the number of attacks from mobile devices will likely rise sharply. There is an additional layer of complexity in mitigating attacks from mobile devices; cellular networks cannot use traditional firewalls to block source IP addresses since they would also affect legitimate traffic.

52% of Attacks Originate From Only Ten Countries

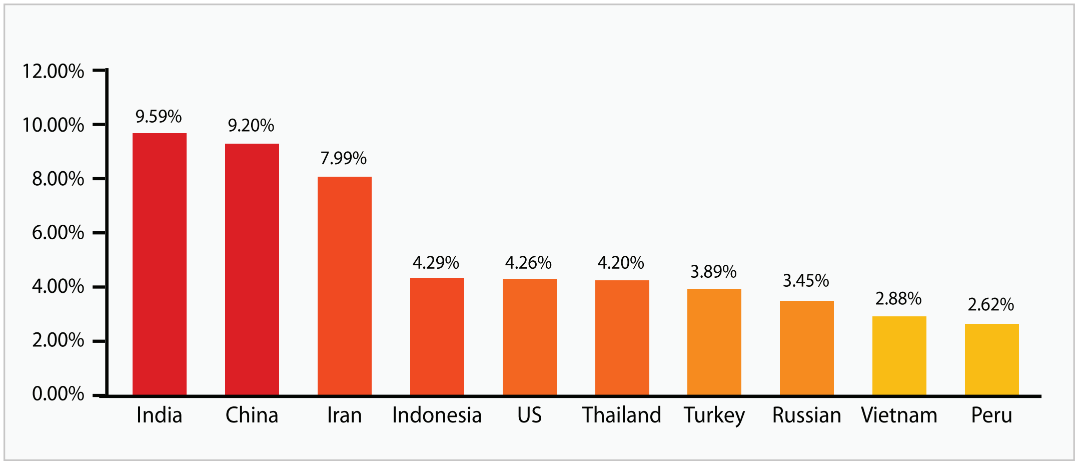
In Which Geolocations Do DDoS Attacks Originate?

DDoS attacks are frequently routed through hijacked hosting environments or internet connected devices in regions having an insecure infrastructure. The attacks may originate in another country, but are then amplified through other environments. IT infrastructures in these countries tend to have weaker security measures in place, which is why computing resources located therein are used more frequently to commit attacks.

Latest Trends

- The top five spoofed agents shown in the list below account for 85% of all malicious DDoS bot sessions.
- Bot traffic accounts for 62% of all website traffic, half of which consists of search engines and other good bots – the other half comprising malicious bots.

Top Attack Originating Countries



Implications

Attacks will likely continue to increase from these regions as IT infrastructures and the number of internet-connected devices therein is increasing at a much larger rate than other locales. The implementation of stronger regulation and security controls within these regions could significantly reduce the number of attacks originating from within their borders.

Conclusion

DDoS attacks are constantly evolving in terms of their technology, sophistication level, and tactics. New attack tools are being regularly released, and – what is particularly alarming – some of them are so user-friendly they require little-to-no technical knowledge to initiate attacks. Highly-disruptive botnets, powered by thousands of servers, are also now available for rent, and at very low prices. As a consequence, the number, magnitude, and disruption level of DDoS attacks is expected to scale to new levels.

Traditional anti-DDoS products are no longer sufficient to meet these challenges. These consist of appliance-based solutions having bandwidth limitations; "on demand" mitigation requiring manual activation; rate-limiting solutions that are ineffective against IP spoofing; and delay/splash screens that impair the user experience.

Effective DDoS Mitigation Solution Requirements

To protect against all current and future DDoS attacks, an all-encompassing mitigation solution requires the following:

- Cloud-based DDoS mitigation
- A high-capacity network
- Automatic/instant detection and mitigation
- Visitor identification, risk analysis, and progressive challenges
- Minimal disruption to website user experience
- Always-on DDoS protection

Imperva Incapsula – Protecting You Against All the Latest DDoS Attack Trends

Incapsula DDoS protection solution exceeds all of the above requirements. Being a cloud-based, "always-on" solution, it protects against attacks on any level, be they network (layer 3), protocol (layer 4), or application (layer 7).

Incapsula offers a unique capability set specifically designed to address the latest trends in the DDoS threat landscape. Being a cloud-based service running over a high-capacity global network, it scales on demand to counter multi-gigabyte, network layer 3 DDoS attacks. Advanced traffic analysis algorithms block malicious traffic at the protocol layer (4), and an enterprise-grade web application firewall employs user classification, granular mitigation rules, and progressive challenges to thwart sophisticated layer 7 application attacks.

Incapsula CDN evenly distributes traffic between data centers while simultaneously accelerating legitimate traffic to decrease latency. Each data center holds several interconnected, high-powered scrubbing servers, used for real-time DDoS traffic profiling and blocking.

With Imperva Incapsula DDoS protection solution you get:

- An "always-on" service having instant detection and mitigation.
- Cloud-based platform that is swiftly updated to address the latest attack types.
- Powerful network of globally-positioned data centers to block the largest of attacks.
- Blanket DDoS protection for all types of services (UDP/TCP, SMTP, HTTP, FTP, SSH, VoIP, etc.)
- Backed by a 24 × 7 security team and a 99.999% uptime SLA

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance. Over 3,500 customers in more than 90 countries rely on our SecureSphere platform to safeguard their business. Imperva is headquartered in Redwood Shores, California.

Learn more at www.imperva.com.

IMPERVA®

www.imperva.com