

WHITE PAPER

2017

DDoS of Things

SURVIVAL GUIDE

Proven DDoS Defense in the New Era of 1 Tbps Attacks



Table of Contents

Cyclical Threat Trends.....	3
Where Threat Actors Target Your Business.....	4
Network Layer Attacks	4
Objective.....	4
Types.....	4
Mitigation.....	5
Application Layer Attacks	5
Objective.....	5
Types.....	5
Mitigation.....	6
Amplification Attacks	7
Objective.....	7
Types.....	7
Mitigation.....	7
Multi-Vector DDoS Attacks	8
Objective.....	8
Types.....	8
Mitigation.....	8
Thunder TPS Stops DDoS Attacks	9

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

Cyclical Threat Trends

Cyber attack strategies always evolve. But 2016 witnessed the resurgence of traditional attack strategies, blended with new twists, that the world was ill prepared to defend.

Leading this advancement were IoT-based distributed denial of service (DDoS) attacks. This tactic leverages open-source malware (e.g., Mirai, Leet) that takes advantage of lax security implementations in connected smart devices to build massive botnets able to deploy DDoS payloads that surpass 1 Tbps throughputs.

This is the DDoS of Things.

DDoS attacks have always been an issue for organizations, businesses and service providers, yet for the most part they were kept in check. This was partly due to the majority of threat actors not having the bandwidth to exceed the security measures of large organizations.

That theory played out in the numbers, too. There was a 71 percent year-over-year increase in DDoS attacks from Q3 2015 to Q3 2016, yet the standard attack was still under 100 Gbps. **Akamai reported** that there were 19 “mega-attacks” that topped the century threshold, but the bandwidth at the disposal of threat actors was still somewhat limited.

Since the **Mirai source code was openly published in the second half of 2016** — and soon **followed by rival malware Leet** — DDoS attacks have easily pushed past 600 Gbps thresholds, with some cases exceeding 1 Tbps in bandwidth.

There is good news, however. Mirai and Leet don't change how DDoS attacks work. The malware simply gave malicious groups the means to do it better and faster. Most DDoS attacks still fall into three specific categories: network, application and amplification attacks. This guide dissects each attack type, explains why they work and outlines best mitigation techniques for each.

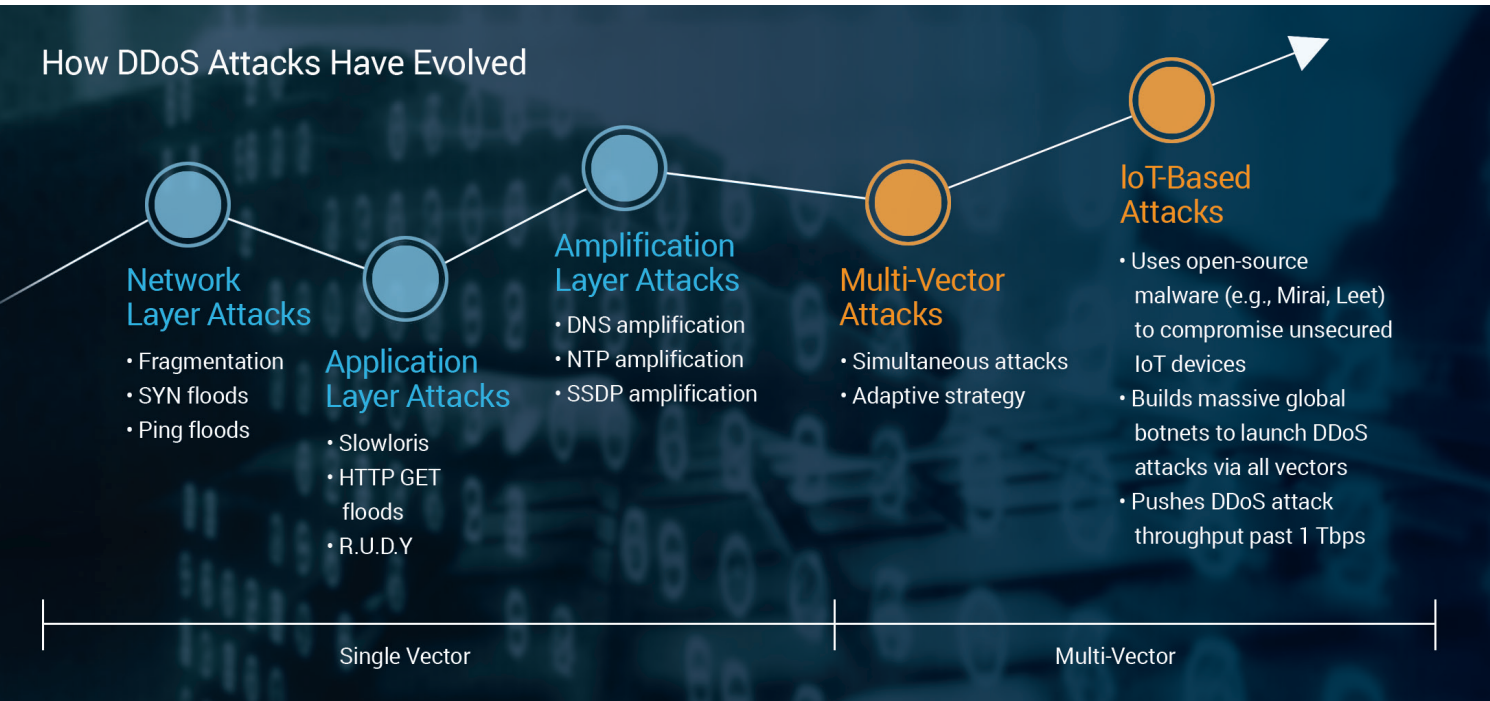
Understanding Mirai

What makes Mirai so powerful? Download the exclusive white paper that dissects the malware that's creating powerful global botnets from unsecured IoT devices.

[READ IT NOW](#)

Where Threat Actors Target Your Business

DDoS attacks are increasing in number, sophistication and capacity. In their infancy, the salvos targeted a single infrastructure layer. Today, threat actors launch various DDoS attacks to exploit and defeat an organization at multiple layers.



Network Layer Attacks

Affected Areas: Physical/Link, Internet & Transport Layer
Examples: UDP Fragment, SYN Floods, Ping Floods, TCP Anomaly

Objective

To overwhelm network resources, including bandwidth (e.g., network links, uplinks), resources (e.g., TCP ports) on intermediate networking devices/gateways (e.g., firewalls, application delivery controllers) or victim servers themselves.

Types

Typically called flood or volumetric DDoS attacks, this type of traffic is easy to create as it can be stateless and/or use spoofed IP addresses. Most are UDP- or ICMP-based packets. The main objective is to overwhelm the network links (bandwidth) and also boost CPU load on the victim device by forcing it to respond to those packets (e.g., unreachable message or echo response).

There are TCP-based attacks, such as TCP SYN and/or RST floods, that exploit the TCP protocol. In addition to overwhelming the bandwidth and CPU load on the victim, these aim to consume transport layer resources, including connection tables on the networking devices or victim servers. Even though these are TCP-based, it's not necessary to establish the TCP session (on the attacker side). As a result, spoofed IPs are often used.

Also, common IP and protocol anomaly attacks — such as XMAS and SYN-FIN packets — exploit IP/TCP/UDP protocol stacks. Invalid protocols require more processing by victim devices than normal packets.


Mitigation

Begin by rate-limiting IP- or ICMP-based traffic to limit attack damage.¹ If protocol-based rate-limiting (e.g., per ICMP, UDP, TCP) is available on the intermediate network device or the server, it will be effective since legitimate traffic using other protocols won't be throttled by the rate-limiting.

Blackholing is another mitigation technique at the ISP level, which protects victims' infrastructure. However, this tactic may interrupt services because it drops all incoming traffic, including legitimate traffic.

For IP and protocol anomaly attacks, and some TCP-based attacks, use filters (or DDoS rules) such as IPtables² (manual configuration) to drop packets based on defined rules. SYN cookie (or SYNPROXY) may also be used for SYN flood mitigation by challenging the sender to verify that they are legitimate.

Note, even if these mitigations are applied to the intermediate network device or the server, it most likely requires CPU processing power (unless it has hardware assist) for activities while serving legitimate traffic.



“The main objective of network layer attacks is to overwhelm the network links (bandwidth) and boost CPU load on the victim device by forcing it to respond to UDP- or ICMP-based packets.”

Application Layer Attacks



Affected Areas: Transport & Application Layers
Examples: Slowloris, HTTP GET Floods, R.U.D.Y.

Objective

To exhaust available application server resources (e.g., session pool, CPU load, etc.) and/or exploit vulnerabilities and default configurations in common applications, including Apache and Windows IIS.

Types

Most application layer attacks are sophisticated and often resemble legitimate traffic because they are able to properly establish a TCP connection with the victim server and operate on high levels, such as HTTP. In most cases, the traffic source originates from infected PCs and IoT devices not using spoofed IPs.

Due to the nature of DDoS reports focusing on size and volume, the most common application layer attacks are HTTP Flood attacks (e.g., GET, POST). These are used to overwhelm CPU resources/capacity of servers with massive amounts of HTTP request packets.

Since HTTP response is compute-intensive to formulate, and typically larger than request packets, it may be possible to saturate computing capabilities and the network (i.e., uplink) with the response packets that interrupts legitimate workloads.

¹ "DDoS Quick Guide" January 29, 2014. <https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf>

² "IPtables DDoS Protection: The Best Rules to Mitigate DDoS Attacks" April 18, 2016. <https://javapipeline.com/iptables-ddos-protection>

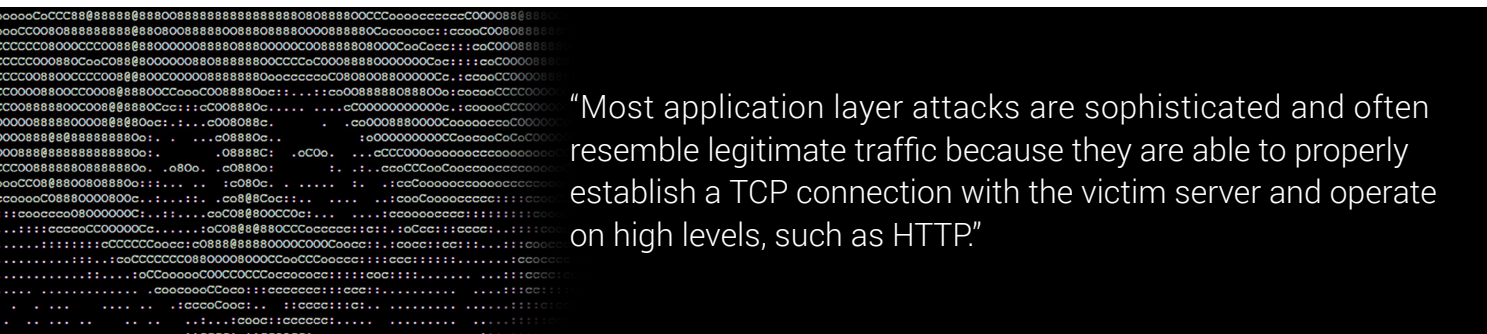
Also, there are more complex application layer attacks; they are so-called “slow and low” attacks like Slowloris, R.U.D.Y, SlowPOST and SlowREAD. At first, a slow-and-low attack device typically establishes a proper TCP session with the target server and then sends HTTP requests very slowly (e.g., utilizing pause frame, etc.) for as long as possible.

This is achieved via hundreds of thousands of bots to open as many concurrent connections to the target server as possible. This eventually overflows the maximum concurrent connection pool and leads to denial of additional connections from legitimate clients.

A well-known type of UDP-based application attack is a DNS attack or DNS flood, which specifically target a DNS service. Because it’s UDP-based, it’s relatively easy to launch in volume even when using spoofed IPs.

Intentional invalid DNS requests may cause more stress on the DNS server. This results in overwhelming the target DNS servers.

The application layer is also vulnerable to many SSL-based DDoS attacks, which try to exploit SSL handshakes to exhaust server resources; SSL-handling processes are very CPU-intensive.



Mitigation

To mitigate application layer attacks, it’s recommended to leverage multi-layer protections due to overall complexity. This could include implementing connection pool limits and traffic rate control at the gateway of server farms (e.g., firewalls and next-generation firewalls) and/or more sophisticated protection at the intermediate devices (e.g., ADC, WAF).

In many cases, leveraging ADCs is the better approach (with L7-based load-balancing enabled). ADCs are tied and configured with specific application services, so they are able to monitor all application service requests and transactions per service type, but also handle all requests as the reverse proxy server.

Therefore, ADCs are able to control connection pool limits and request rates efficiently, and also detect and mitigate more complex slow-and-low DDoS attacks. In addition, WAFs embedded on the ADC can block application attacks, such as cross-site scripting (XSS), SQL injection and buffer overflows, that exploit vulnerabilities.

Firewalls and NGFWs, on the other hand, oversee entire services of a given server farm and can control connection pools and traffic rates per protocol or application services. In many deployment scenarios, these firewalls are also responsible for other critical functions and CPU-intensive tasks, including intrusion prevention, signature-matching and deep packet inspection.

Thus, it may be too much to ask of firewalls to control connection and request rates per service application level as they could tax a network infrastructure, especially if a DDoS attack occurs.

Further, it is better to deploy a DDoS mitigation device in front of firewalls or next-generation firewalls. This serves as a first line of defense to protect application services and other security devices, including NGFWs, IPS, ADCs and WAFs.

Amplification Attacks



Affected Areas: Physical/Link, Internet & Transport Layer
Examples: DNS, NTP, SSDP Amplification Attacks

Objective

To overwhelm network bandwidth by sending enormous traffic volumes that are amplified by proper/legitimate open servers. Amplification is sometimes known as a volumetric attack.

Types

Amplification attacks come in many flavors, but the concept is largely the same: exploit publicly open and available servers to flood a target with more traffic than it can manage. There are two key factors for an amplification attack:

- 1 Use of a spoofed IP address as a source IP of the original request packet sent by thousands of bots, which is actually the IP address of the intended target server/service.
- 2 Use of response packets from an UDP-based application service (e.g., DNS, NTP), which can easily amplify the volume of traffic with greater amounts of response data.

Domain Name System (DNS) amplification DDoS attacks are some of the most common. Due to the nature of the DNS protocol, the size of DNS responses is much larger than the DNS requests.

The attacker intentionally sends DNS requests (with the targets' spoofed IP) that require a large volume of responses (e.g., ANY requests) from thousands of bots. This results in amplifying the volume of the traffic destined to the target system.

In these cases, threat actors leverage open DNS servers to overwhelm actual targets with DNS response traffic.³ This is also commonly known as a reflection attack and the application servers (DNS in this case) are called reflectors.

The same technique is used in a Network Time Protocol (NTP) amplification attack, which exploits older versions of NTP servers by sending "monlist" commands.⁴

Similarly, Simple Service Discovery Protocol (SSDP) amplification attacks leverage UDP traffic, but instead use vulnerable search commands to exceed bandwidth limits of a target.⁵

Mitigation

There are two primary approaches to defend against amplification attacks. The first is to prevent the reflector (e.g., open DNS or NTP servers) from participating in the DDoS attack by denying such requests. This should be considered at the service provider side, who owns the open DNS/NTP servers.

An example of this in practice would be denying/dropping unknown "ANY" requests on the DNS server, and/or patching monlist query vulnerabilities on NTP servers. This solution won't necessarily stop the entire amplification DDoS attack, but may help reduce the volume (and also save the DNS/NTP service itself).

³ "DNS Amplification Attacks": revised October 19, 2016. <https://www.us-cert.gov/ncas/alerts/TA13-088A>

⁴ "NTP Amplification": <https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html>

⁵ "UDP-Based Attacks": revised November 4, 2016. <https://www.us-cert.gov/ncas/alerts/TA14-017A>

However, the most important strategy is to defend the target server or service. Due to the volume of amplification attacks, the best protection is to block traffic (i.e., blackhole) at the closest point on the network edge (e.g., Internet, Internet exchange peering point) or even on the service provider's side.

For example, when blackholing traffic at border gateway routers, it's best to manually apply filters to specify UDP traffic and known source ports (e.g., port 53 DNS, port 123 NTP).



Multi-Vector DDoS Attacks



Affected Areas: All (Physical/Link, Internet, Transport, Application Layer)

Examples: All

Objective

Take down online services by employing any and all available or possible techniques.

Types

Multi-vector DDoS attacks are a strategic combination of all attack types described to this point.

Mitigation

As described in the above sections, many attack types can be leveraged in each specific attack vector. The mitigation and countermeasures for each attack are different, respectively.

Attackers may choose attacks based on target services and size, but also the types of bots he or she can use to cause the attack; the introduction of Mirai and the DDoS of Things provides threat actors with more options and power. By combining multiple attack types in multiple attack vectors, threat actors increase their chance for success due to the complexity and size of attacks.

Therefore, organizations or service providers running application services must deploy a proper and dedicated DDoS protection solution that can mitigate multi-vector DDoS attacks, including those launched from unsecured IoT-based devices. It's important to consider size (i.e., mitigation throughput), deployment flexibility and application-aware countermeasures.

Thunder TPS Stops DDoS Attacks

There is an undeniable increasing trend in DDoS attacks in terms of frequency, size and complexity.

Likewise, organizations are increasingly dependent on the availability of their services, and on their ability to connect to the Internet. Downtime results in immediate revenue loss, brand damage and additional employee labor for mitigation.

To easily integrate into various networking architectures, a flexible DDoS mitigation solution is required: A10 Thunder TPS.

A10 Networks Thunder TPS provides agile, efficient and network-wide protection against the full spectrum of DDoS attacks. This includes challenging multi-vector attacks that use a combination of high-rate volumetric or network protocol attacks and more sophisticated application attacks, as well as 1 Tbps-plus DDoS of Things attacks.

- **Protect against the full attack spectrum**
- **Prepare for growing attack scale and complexity**
- **Scale DDoS protection to mitigate escalating scale from IoT-based attacks**
- **Customize and integrate the solution to meet the specific needs of your organization**



Fight the DDoS of Things
Stop DDoS attacks up to 300 Gbps with
A10 Thunder TPS 14045.

[DOWNLOAD DATASHEET](#)

A10 Thunder TPS

Flood Attack Protection	Application Attack Protection	Resource Attack Protection
• SYN cookies	• Application-aware Berkeley Packet Filter (BPF)	• Fragmentation attack
• SYN authentication	• Regular expression filter (TCP/UDP/HTTP)	• Slowloris
• ACK authentication	• HTTP request rate limit	• Slow GET/POST
• Spoof detection	• DNS request rate limit	• Long-form submission
• SSL authentication	• DNS query check	• SSL renegotiation
• DNS authentication	• HTTP protocol compliance	
• HTTP challenge	• HTTP anomalies	
• TCP/UDP/ICMP flood protection		
• Application (DNS/HTTP flood protection)		

To learn how A10 Thunder TPS can detect and mitigate DDoS attacks against your organization, please visit A10networks.com/TPS.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

©2017 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, Thunder and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.

Part Number: A10-WP-21140-EN-01 JUN 2017

