# Messaging, Malware and Mobile Anti-Abuse Working Group
# M³AAWG Initial Recommendations: Arming Businesses Against DDoS Attacks

March 2017

The reference URL for this document: www.m3aawg.org/DDoS-Recommendations-Business

## Table of Contents

**Introduction** ..... 1
**DDoS Attacks** ..... 1
**Preparation Before Attacks Occur** ..... 2
**During an Attack** ..... 5
**After an Attack** ..... 5
**Conclusion** ..... 6
**References** ..... 6
**Glossary** ..... 7

## Introduction

Distributed Denial of Service attacks continue to be a major concern for businesses that depend on the internet for email, marketing, commerce, and data storage. Disruptions caused by Distributed Denial of Service (DDoS) attacks range from loss of revenue and higher costs to dramatic brand damage. This guide provides concepts and ideas to help businesses prepare for DDoS attacks. As a side benefit, some of these same techniques can also help businesses who suddenly see a large increase in legitimate customer traffic to their websites.

## DDoS Attacks

Distributed Denial of Service (DDoS) attacks encompass a wide variety of techniques and can range from IP layer 3 volumetric attacks to layer 7 application attacks. Sources of the attacks extend from compromised systems directly sending attack traffic to uncompromised reflective sources that are responding to spoofed IP packets.

DDoS attacks can be broken into four main categories:[1]

- Volumetric
- Application
- State Exhaustion
- Control Plane

There are dozens of attack types within these four main categories. The vast majority of DDoS attacks leverage compromised computer systems that are under a central command and control system. These

[1] Fonash and Glenn 2014

infected computers are generally referred to as "bots." A network of bots under a single command and control system is referred to a "botnet." Nonprofit security organizations track thousands of botnets operating on the Internet at any point in time.[2]

**Volumetric DDoS attacks** can come either from direct sources or from a reflective service where the source IP of the packet is forged with the victim's IP address. Typically, miscreants leverage reflective services to amplify the attack traffic and greatly increase the attack size. Until recently, the largest volumetric attacks seen on the internet to date were reflective amplification DDoS attacks. However, direct attacks from a large number of insecure IoT devices have pushed the largest DDoS attacks over the 1 Tbps threshold.[3]

Attacks can also be categorized as **direct** or **indirect**. Direct attacks target a victim (different than the direct sources described above), while indirect attacks target critical network services needed by the victim for their service to operate. An example of this type of attack is for the miscreant to target the DNS authoritative or recursive service that the victim uses.

In general, **application-level attacks** are lower volume attacks; they leverage compromised computers to send application-level requests to systems in order to overload the victim with legitimate-looking requests. Attacks can move forward or in reverse. A forward application-style attack may try to overwhelm a web server by sending a large number of CPU- and memory-intensive search requests to the website, while a reverse-style attack might make a high number of requests for large-size documents located on the website in order to consume all the available upstream bandwidth of the website.

A new type of high-volume, application-level attack was recently observed starting on March 18, 2015.[4] Dubbed the "Great Cannon," it was a "man-on-the-side" type of attack. After analytic JavaScript code for the Chinese search engine Baidu was modified, legitimate website requests entered Chinese networks and sent attack requests from non-compromised computers using the modified code. This type of attack is unusual; it must be performed either by a network operator or an organization having access to most network traffic transiting operators' networks.

Another form of indirect attack targets the DNS service of an ISP. Either the recursive or the authoritative servers can be targeted, which can cause large-scale customer outages. DNS service interruption can have wide-ranging impact on an ISP or DNS provider's customer base.

## Preparation Before Attacks Occur

Businesses must take steps to prepare for DDoS attacks that could significantly impact their activities. These steps include internal preparations for their networks and servers along with additional DDoS mitigation services from their ISP or from a dedicated DDoS mitigation company. The steps listed below are general guidelines and will vary based on the size of the company, the size of the company's network (including internet uplink capacity) and the DDoS skill level of employees.

### Management Support

Probably the most important first step in preparing for a DDoS attack is to get management buy-in. Estimate the business impact that would occur if a DDoS attack hit the company's operations. How long can services be down before different levels of customer impact occur? What happens if customers cannot

[2] https://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts
[3] "Mapping Mirai: A Botnet Case Study," 2016.
[4] "Using Baidu to steer millions of computers to launch denial of service attacks," 2015

pay their bills or order products? What is the impact of employee email and internet connectivity being down for an extended period of time? Does the company have out-of-band communications? Remember—during a DDoS attack, VoIP phone service running over the same internet circuit will not be working.

**Assess Internet-dependent Services**
The next step a company should take is an assessment of all its internet-dependent services. Consider the impact and potential revenue loss the company would experience should these services become unavailable. Typical services include:

- Customer-facing ecommerce web portals – for many industries, these sites can significantly impact company revenue if not available to customers
- Corporate email systems
- Corporate internet-facing DNS systems
- Employee remote access systems
- VPN networks that could be impacted by internet DDoS attacks

Companies should evaluate the impact that loss of these systems would have on revenue and employee productivity.

**Set Up DDoS Attack Monitoring Systems**
For important or critical internet-facing services, systems should be in place to monitor for DDoS attacks and perform logging and packet capture when attacks occur. During the early stages of an attack, information about the attack can help mitigation efforts. The ability to see web requests, connection requests, firewall logs, IPDS logs and perform full-packet capture on the incoming traffic will allow the company and its DDoS mitigation provider to get a handle on attack traffic. In addition, DDoS attack monitoring from the company's service provider can be very helpful.

**Key points to remember:**
1. Capture date and time stamps for all logs and packet captures.
2. Run an NTP client on your systems to ensure you have accurate times.
3. Capture source IP addresses of offending packets.
4. Where possible, perform full-packet capture of attacking traffic.

**Ecommerce Site Preparation**
Organizations that may be significantly impacted by an attack on their ecommerce web infrastructure should prepare the site for a DDoS attack. This preparation includes:

- Prioritizing the most important functions of the site
- Creating a plan where the site can operate in a state of minimal functionality to serve the most important functions while removing features to make the website more resilient to DDoS attack or resource exhaustion attacks

DDoS attacks come in many varieties. Things to consider for a minimized website:

- **Reduced or eliminated dynamic functionality**. Search functions, dynamically generated webpages, and any functionality requiring access to back-end resources like databases make it easy for an attacker to exhaust CPU, disk or memory resources. Even a website architected to be enhanced with CDN (Content Delivery Networks) or DDoS mitigation service will not work if the attacker finds a URL that can only be served by a single dynamic back-end resource. As much as possible, present static web content to customers that will continue to be served if under attack—especially the main page.

- **Reduced graphics.** Smaller-sized graphics or elimination of most graphics can help webservers function more efficiently during an attack.

- **Limit access to large documents or files.** One type of DDoS attack involves making thousands of requests from the website for large documents. This can flood the upstream link from the website and interfere with other legitimate traffic.

- **Rate limit the number of incoming connections allowed to the website.**

**Not all high-volume events are DDoS attacks**. Linking from a widely-viewed website to an organization's website can also look like an attack.[5]

As an unexpected benefit, all this preparation can also help businesses manage sudden large increases in *legitimate* traffic.

**Network and Server Preparation**
Additional preparation work should be considered including:

1. Adding more local capacity (bandwidth or servers) to the attacked service.

2. Deploying DoS/DDoS-specific premise-based mitigation devices and/or using antiDoS capabilities in local hardware. This can include load balancers, local DDoS data scrubbers, DNS servers with DDoS mitigation capabilities and other specialized devices.

3. Coordinating with software and hardware vendors for guidance on optimal device configuration.

4. Using Content Delivery Networks (CDN) to help mitigate attacks by distributing attack volumes across a wide CDN infrastructure.

5. Considering an offsite secondary or tertiary email server to store email during an attack and for off-site retrieval.

6. Ensuring that network control plane traffic has priority over DDoS traffic.

7. Ensuring that website administration management traffic is either transmitted on an out-of-band network and server interface(s) that will not be affected by DDoS attack traffic, or that proper Quality of Service (QoS) prioritization and management traffic Access Control Lists (ACLs) are in place to ensure that the website can be managed during an attack.

8. Lowering the company's DNS TTLs so that IP addresses can be quickly changed if it plans to use blackhole techniques to mitigate an attack.

Do not be part of the problem. Find any NTP or DNS servers and other UDP-based services that should not be exposed externally and remove them from the network or locate them to an internal network so these services are not participating in reflective DDoS attacks.

[5] https://en.wikipedia.org/wiki/Slashdot_effect

**Third-Party DDoS Mitigation Providers**
On-site preparation cannot defend against large-scale volumetric attacks that are larger than your network connectivity bandwidth to the internet. These attacks must be mitigated by your upstream ISP, hosting provider or third party DDoS mitigation provider. Plan ahead and have a mitigation service in place prior to an actual attack. In addition, some attack traffic-scrubbing services work better if normal traffic is baselined prior to the attack. It is best to negotiate legal and pricing contracts prior to an attack.

**Coordination with Central Resources**
Businesses should proactively identify and have contacted appropriate points of contact in external organizations prior to a DDoS attack including:

- Upstream ISP
- Third-party DDoS mitigation provider
- Law enforcement agency
- National Community Emergency Response Team (CERT)
- Hosting provider
- Other organizations who can help before, during and after a DDoS attack.

**Test the Company's Preparation**
Test the company's preparation to see how well it has been planned. First start with a paper exercise to see if the organization is actually ready for an attack. How will they contact customers? Will the communications group be ready to distribute a press statement on the issue? What mitigations will be deployed to stop or reduce the attack?

## During an Attack

- **Capture attack traffic**
  Be prepared to capture traffic during the attack. Full-packet captures can provide great insights into the attack and the changing nature of an attack.

- **Implement mitigation strategies**
  Based on the characteristics of the attack, implement planned predefined mitigation strategies. These can include:
  - website changes
  - blackholing
  - filtering and changes to DNS entries
  - upstream scrubbing with the company's ISP or third-party DDoS mitigation service
  - on-site data scrubbing.

## After an Attack

Share captured hostile/attack code, tactics, techniques, attack sources and procedures with other organizations who may experience similar types of attacks and with central coordination organizations such as national CERT organizations, information-sharing organizations and possible law enforcement, where appropriate. Work with the network operator, hosting provider, information sharing organization or national CERT to identify attacking computers and clean up the machines on the distant end to minimize the possibility of future attacks.

## Conclusion

DDoS attacks will continue to impact many internet businesses and users for the foreseeable future. Businesses that do not prepare for attacks could experience a substantial impact on operations, customers, and, ultimately, loss of revenue. Businesses that prepare for DDoS attacks can significantly reduce these impacts. Proper planning and preparation in coordination with service providers can not only help mitigate attacks, but can also prepare businesses to better handle legitimate increases in website traffic.

## References


Fonash, Peter, and Michael Glenn. "Remediation of Server-Based DDoS Attacks Final Report." Communications Security, Reliability and Interoperability Council (CSRIC) IV Working Group Report, FCC, Washington DC: FCC. http://docplayer.net/16237406-September-2014-working-group-5-remediation-of-server-based-ddos-attacks-final-report.html

"Mapping Mirai: A Botnet Case Study." October 3, 2016. Accessed October 7, 2016. https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fiflield, Sarah McKune, Arn Rey, John Scott-Railton, Ronand Deibert, and Vern Paxson. April 10, 2015. "China's Great Cannon." *Citizen's Lab.* University of Toronto. Accessed September 3, 2015. https://citizenlab.org/2015/04/chinas-great-cannon/

"Using Baidu to steer millions of computers to launch denial of service attacks. March 25, 2015. Accessed September 3, 2015. https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1.h

# Glossary

| | |
|---|---|
| **AntiDoS** | Techniques and devices used to mitigate DoS/DDoS attacks. |
| **Blackhole/Blackholing** | Also known as "null routing," blackholing network traffic drops malicious traffic at a properly configured router. The ISP or customer sends out a route announcement that identifies the destination IP address to be dropped. That announcement can drop traffic across a group of blackhole-configured routers. [A variation of the technique can drop traffic based on source IP address. ISPs have found this technique less effective due to a.) the large number of attacking source IP addresses in a normal DDoS attack; b.) router limitations; and c.) collateral damage from inadvertently dropping legitimate traffic.] |
| **Bot** | A device infected with malicious software that can be remotely controlled. |
| **Botnet** | A group of bots that are remotely controlled by a single entity. |
| **CERT** | Computer Emergency Response Team. |
| **Content Delivery Networks (CDN)** | A system of geographically distributed servers that replicate files and content and deliver that content to end users from the closest or best server. A CDN can help distribute and minimize the impact of DDoS attacks, especially on web traffic. |
| **Data scrubbing** | Activity in which a server differentiates between legitimate traffic and illegitimate attack traffic, dropping the illegitimate traffic and allowing the ISP to deliver legitimate traffic to the appropriate destination. |
| **Denial of Service (DoS) Attack** | Malicious traffic that attempts to deny access to network, server, or application resources. |
| **Distributed Denial of Service (DDoS) Attack** | A DoS attack in which the attack traffic comes from (is distributed across) multiple sources, which might be anything from computers to smartphones to IoT-connected devices. |
| **Domain Name System (DNS)** | A critical internet service that translates alphanumeric names to IP addresses. |
| **Internet Service Provider (ISP)** | A company or organization that provides internet access to its subscribers. |
| **Internet Protocol (IP)** | The main protocol used to deliver packets across the internet. |
| **Internet of Things (IoT)** | A term used to describe adding network connectivity to a variety of physical objects for local communication or communication across the internet. Examples of devices include light bulbs, refrigerators, washing machines, home fitness equipment, vehicles, traffic signals, soil moisture sensors and much more. Major categories of IoT devices include consumer, smart cities, industrial, healthcare, government, financial and more. |
| **Intrusion Detection System (IDS)**<br>**Intrusion Prevention System (IPS)** | An Intrusion Detection System (IDS) monitors networks or systems for malicious or unusual activity. An Intrusion Prevention System (IPS) has the capability to stop, block or respond to identified packets. An IPDS (or IDPS) combines an IDS and an IPS. |

| | |
|---|---|
| **Network Time Protocol (NTP)** | A protocol used to synchronize clocks across the internet and other packet-switched networks. |
| **Reflective Amplification Distributed Denial of Service (DDoS) Attack** | A DDoS attack in which the IP packets' source address is changed from the actual sender to the victim's IP address. The IP packets are then sent to a service on the internet that amplifies their effect. The original IP packets are "reflected" off the legitimate service and the response goes to the DDoS attack victim, flooding the victim with IP packets they did not request. Common vulnerable protocols include DNS, NTP, SSDP, SNMP and approximately 10 others. Some of the largest DDoS attacks seen on the internet have used this technique. |
| **Tbps** | Terabits per second |
| **Time to Live (TTL)** | A field in the IP packet header. The TTL field is normally decremented at each IP router. When the IP packet TTL reaches zero, the router discards the packet. This prevents routing loops where the packet loops forever. |
| **Transmission Control Protocol (TCP)** | A network protocol that runs on top of the IP protocol to provide a reliable method of delivering ordered data packets. |
| **User Datagram Protocol (UDP)** | A network protocol that runs on top of the IP protocol to provide packet delivery for loss-tolerant applications. An example application is a broadcast television stream. |
| **Voice over IP (VoIP)** | A group of technologies and protocols for delivering voice and multimedia communications across a packet-switched network such as the internet. |
| **Virtual Private Network (VPN)** | A private network that isolates packets transiting a public network such as the internet. A VPN can make it appear as if the user or system is connected to a private network. |

As with all best practices that we publish, please check the M³AAWG website (www.m3aawg.org) for updates to this document.