CompTIA

THE WHO, WHAT, WHY AND HOW OF DDoS ATTACKS: A GUIDE FOR IT PROS

LEARN HOW TO IDENTIFY WARNING SIGNS AND THE TOOLS FOR MITIGATION

DDoS Guide for IT Pros

The IT industry has seen a major increase of Distributed Denial of Service (DDoS) attacks over the past several years. The December 2019 New Orleans cyberattack is such an example: This attack combined a classic ransomware deployment with a DDoS attack. The DDoS upward trend promises to continue.

DDoS attacks date back to the dawn of the public internet, but the force is strong with this one. According to a 2018 report from International Data Group (IDG), the median downtime caused by a DDoS attack is 7 to 12 hours. Using an estimate from Gartner of $5,600 per minute of downtime, that means the average cost of a DDoS attack is in the $2.3 million to $4 million range. These losses are incurred due to a loss of business operations and does not account for staff time or other associated costs.

As technology evolves, so do DDoS attacks. And attackers are continually using these types of attacks to achieve their objectives. This guide will help IT pros understand everything from the basics of detection to tools for combatting attacks, along with the skills one needs to develop to prepare for cybersecurity incidents of this kind.

THIS GUIDE WILL COVER THE FOLLOWING:

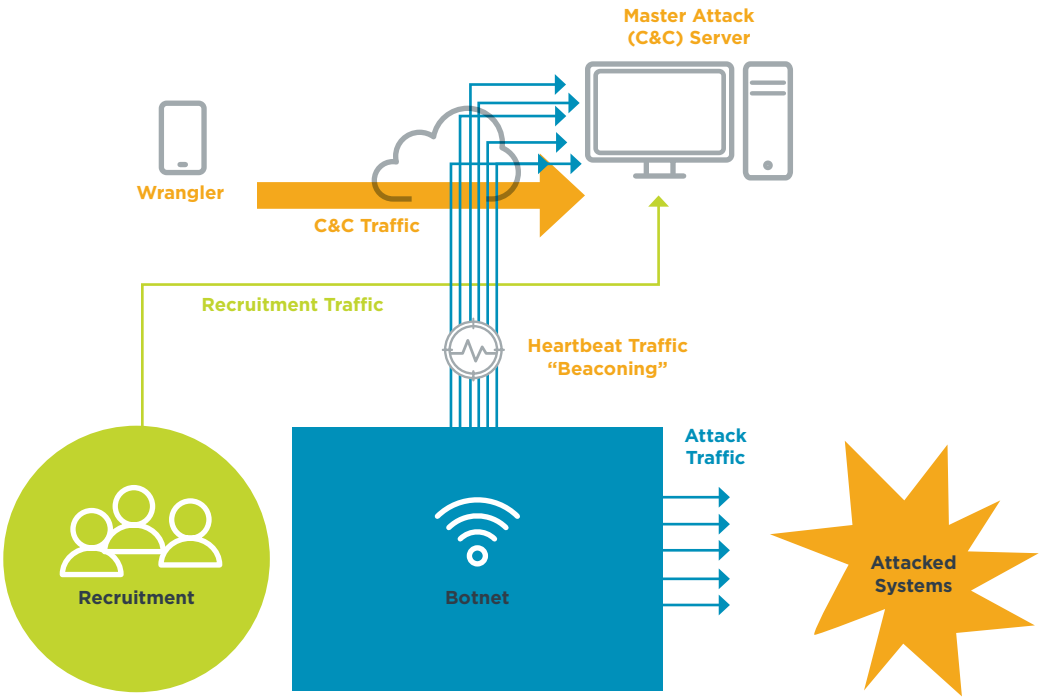
- Definition of DDoS attack
- Types of DDoS attacks
- Explanation of botnets
- Organizational vulnerabilities
- Who, what, why and how of DDoS attacks
- DDoS warning signs and tools for mitigation
- Tools for detecting and responding to DDoS attacks
- DDoS attack best practices and response procedures

Raging IT Warfare:
What Is a DDoS Attack?

DDoS stands for distributed denial-of-service attack. DDoS attacks occur when servers and networks are flooded with an excessive amount of traffic. The goal is to overwhelm the website or server with so many requests that the system becomes inoperable and ceases to function.

Botnets, which are vast networks of computers, are often used to wage DDoS attacks. They are usually composed of compromised computers (e.g., internet of things (IoT) devices, servers, workstations, routers, etc.) that are controlled by a central server.

DDoS attacks can also originate from tens of thousands of networked computers that are not compromised. Instead, they are either misconfigured or simply tricked into participating in a botnet, in spite of operating normally.



Gathering Intel:
Why You Need to Know About DDoS Attacks

DDoS attacks have become increasingly problematic and IT pros need to be ready.

- **DDoS attacks are becoming more common.** In the first part of 2019 alone, TechRepublic saw a whopping 967% increase in volumetric attacks designed to clog networks and deny access to resources.
- **The sheer size of these attacks has increased to overwhelming proportions.** InfoSecurity reports that the average attack grew in size by 500% in 2018 alone. This figure got worse in 2019, and 2020 data is showing us that the problem is not abating on its own.
- **Attacks have become more sophisticated.** They're not limited to layer 3-level attacks. Attackers have developed massive application-layer attacks, as well. Neustar reported that 77% of all the attacks mitigated in Q1 2019 used two or more vectors.
- **DDoS attackers have adopted sophisticated artificial intelligence (AI) and machine learning methods.** For example, DDoS botnets apply machine learning methods to conduct sophisticated network reconnaissance to find the most vulnerable systems. They also use AI to reconfigure themselves at times to thwart detection and change attack strategies. Modern attacks will likely manifest as, both defenders and attackers pit AI-informed systems against each other.
- **DDoS attackers have adopted a blended attack strategy.** They combine various attack methods with social engineering, credential stealing and physical attacks, making the DDoS attack only a single factor in a multifaceted approach.

Even though automation, orchestration and AI are now commonplace, humans are still the ones that make final decisions on how to defend companies.

A More Sophisticated Digital Enemy:
The Evolution of the DDoS Attack

One of the realities of cybersecurity is that most attackers are moderately talented individuals who have somehow figured out how to manipulate a certain network condition or situation. Even though there is often discussion about advanced persistent threats (APT) and increasingly sophisticated hackers, the reality is often far more mundane.

For example, most DDoS attackers simply find a particular protocol. They'll discover that they can manipulate the transmission control protocol (TCP) handshake to create a SYN flood or a particular type of server, such as the memory cache daemon (memcached). Or they'll discover that they can compromise IoT devices, such as webcams or baby monitors. But today, attackers have more help.

Recent advancements have given rise to AI and connective capabilities that have unprecedented potential. Like legitimate systems administrators, attackers now have voice recognition, machine learning and a digital roadmap that can allow them to manipulate integrated devices in your home or office, such as smart thermostats, appliances and home security systems.

Attack Strategy:
Two Types of DDoS Attacks

There are two primary ways a DDoS attack can take form.

Bombardment (volumetric)

This strategy involves a coordinated attack on the targeted system from a collective of devices. Another term for this type of attack is volumetric, coined as such because of the sheer volume of network traffic used to bombard systems. This type of traffic focuses on Layer 3 of the open systems interconnection/reference model (OSI/RM), for the most part and is usually measured in packets per second (PPS) or megabits per second (Mbps).

Volumetric attacks can be long term or burst:

- **Long-Term Attack:** An attack waged over a period of hours or days.
- **Burst Attack:** Waged over a very short period of time, such as a minute or even a few seconds.

Despite being very quick, burst attacks can still be extremely damaging. With the advent of IoT-based devices and increasingly powerful computing devices, it is possible to generate more volumetric traffic than ever before. As a result, attackers can create higher volumes of traffic in a very short period of time. This attack is often advantageous for the attacker because it is more difficult to trace.

A coordinated attack on the targeted system from a collective of devices.

Technological Infection

In this strategy, attackers manipulate applications. They are often called Layer 7 attacks, because attackers and botnets co-opt applications to do their bidding. These applications then become unwitting DDoS attack vectors.

This could involve using IoT-connected devices – such as baby monitors, phones or hubs – to send traffic at the target. This strategy can be more easily understood when you think of the Borg, assimilating others against their will to be part of a larger system of attackers.

Layer 7 attacks can also disable critical web and cloud applications on a massive scale. Today, more companies are using microservices and container-based applications. Layer 7 DDoS attacks are also increasingly popular against cloud-based resources; simply migrating to a cloud provider won't solve the problem.

As the world moves to containers, Kubernetes and more cloud-based services, it's expected that DDoS attack methods will naturally move to and exploit these elements.

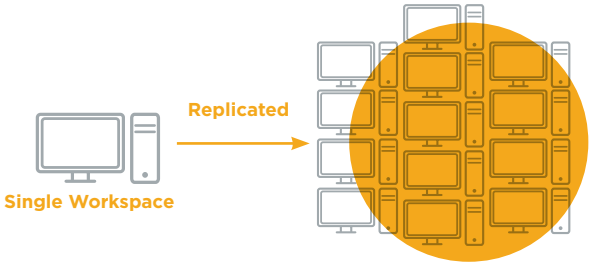
Attackers and botnets co-opt applications to do their bidding.

Strategic Gaps:
How Vulnerabilities are Created

DDoS and other attacks arise as a result of three vulnerabilities: monocultures, technical debt and system complexity.

1. Monocultures: The first vulnerability is created because of our interest in automating and replicating systems. In this age of the cloud and hyper-virtualization, it is a common practice for IT departments to create once and deploy often. This means that once you have created a particular service, such as an Amazon Web Services (AWS) workspace, or a web server, you will replicate it and use it multiple times. This creates a monoculture, or a situation where dozens, or even hundreds, of the same instance exists.

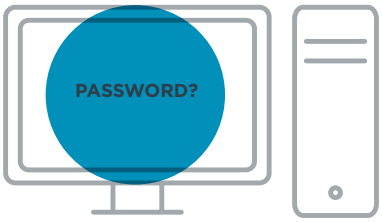
Attackers focus on these types of situations because they can exploit a small vulnerability to achieve maximum damage. This is ideal for attackers because one piece of malware can be used to target many systems.



2. Technical Debt: Companies often skip development steps as they implement a new business solution – a piece of software, a cloud implementation or a new web server. The IT industry long ago identified critical steps that organizations should take to create secure software and services. But these steps take time. Too often, organizations neglect security best practices in the interests of saving time and money.

Whenever a company skips essential steps, they are said to incur a technical debt. The resulting software represents an obligation that the organization eventually needs to re-pay. If an organization doesn't pay this debt back by fixing the software or properly configuring and securing a critical service, that organization will suffer consequences that range from lost business to becoming the target of a successful cyberattack.

One example of technical debt can be found in IoT devices that have powerful networking ability, but no default password. As a result, attackers have been able to easily enlist these devices into their botnets or other DDoS schemes. What makes this situation particularly disturbing is that consumers end up paying the price for a technical debt.



3. Complexity: Complex systems are difficult to manage and monitor, especially if these systems are hastily created. Sophistication is often good and necessary, but as we create more interconnected systems, this complexity can cause us to lose control of our information. In many cases, issues occur because essential steps of the software development lifecycle or the platform development lifecycle are skipped. It's one thing to create buggy software, but when that software connects to multiple cloud instances, it creates a larger, more scalable problem.

Plan of Attack:
The Anatomy of a Botnet Attack

DDoS traffic comes in quite a few varieties. Understanding the types of traffic will help you select proactive measures for identification and mitigation.

1

Command and Control (C&C)

A botnet administrator (i.e., wrangler) uses a central server or network of servers to control the thousands of members of the botnet. Whenever a wrangler issues a command to control the botnet, this is called Command and Control (C&C) traffic. The actual administrator is usually far removed from the botnet or C&C server, and the network traffic is usually spoofed, often making detection difficult.

2

Coordination

The most effective DDoS attacks are highly coordinated. The best analogy for a coordinated attack involves comparing a DDoS botnet to a colony of fire ants. When a fire ant colony decides to strike, they first take a position and ready themselves for the attack. Acting under a single directive and without obvious warning, they wait for the signal and then act simultaneously.

3

Beaconing/Heartbeat Traffic

Whenever a compromised system calls home to a C&C server, it is said to be beaconing. This traffic passing between a botnet member and its controller often has specific, unique patterns and behaviors. As a result, it is possible for security analysts to identify this traffic and treat it as a signature. If this is the case, analysts can then identify compromised systems, as well as manage or block this type of traffic and even trace this traffic to isolate and eradicate botnet infections.

4

Attack Traffic

- **TCP:** In a DDoS attack of this variety, the attacker capitalizes on a vulnerability in the TCP connection. Sometimes that vulnerability exists due to weak or completely non-existent encryption. Normally, a client sends a SYN packet, the server responds with an ACK and the client returns the ACK packet. This communication verifies a connection. An attacker can spoof IP addresses and send a connection request that is never acknowledged, leaving a port open for response. Continued sending of SYN packets compromises all open port connections, disabling the server.
- **UDP:** UDP packets are often sent to servers in normal computing. Each time a UDP packet is sent, the server must use resources to process the request. When large amounts are sent at one time, the server becomes overwhelmed and is unable to process legitimate traffic.
- **ICMP:** ICMP is utilized for diagnostic purposes on networks. During an attack, ping requests flood the servers with illegitimate traffic so that the server can no longer process legitimate requests.
- **Layer 7:** Many modern attacks use floods of (HTTP) GET and POST traffic. They also focus on vulnerabilities found in various servers, including Apache and NGNIX servers. This type of DDoS traffic is often measured in requests per second (RPS). A common example of this type of attack is the age-old Slowloris attack.
- **Amplified:** DDoS attackers, including botnets, often take advantage of legitimate service and protocol behaviors. For example, attackers often use ICMP traffic and NTP servers to amplify attacks.

5

Operational Technology (OT)/IoT

- **OT:** This involves physical items that have programming and an IP address associated with them. This could be devices such as those that are used to control electrical grids, pipelines, automobiles, drones or robots.
- **IoT:** These devices contain individual systems that can communicate with one another or be integrated. Some examples include video doorbells, smart thermostats, smart watches, IP-enabled light bulbs and printers.

6

Memcached

Memcached is an often-used service that distributes memory caching on multiple systems. It is used to help speed up websites by caching information in Random Access Memory. Botnets have often exploited Memcached implementations that are not properly secured.

7

Unusual Traffic

Atypical traffic involves using strategies such as reflection and amplification.

- **Reflection:** Sending traffic through devices, or reflectors, to divert attention away from the attacker's systems.
- **Amplification:** Occurs when the botnet sends traffic through devices, which respond normally while multiplying the outgoing traffic to compromise the target.

8

Monoculture

A collection of similarly configured systems that all contain the same flaw. Here are some examples of compromised monocultures:

- Decades ago, the creators of the Melissa and I Love You worms realized that the Windows systems of that era were identical and open to a particular type of attack. They created malware to manipulate the flaw.
- In more recent times, IoT devices such as webcams and baby monitors, have created monoculture conditions that led to the Mirai botnet. Other IoT devices create potentially dangerous monoculture conditions which are vulnerable to DDoS attacks.
- The 2010 Stuxnet incident in Iran is another example of a monoculture attack. Iranian centrifuges all fell victim to the Stuxnet worm, damaging the SCADA system responsible for processing their nuclear fuel processing plant.

9

Multivector

Modern attacks combine different attack strategies, including Layer 7, volumetric and even ransomware. In fact, these three attack types have become something of a trifecta in the DDoS attack world.

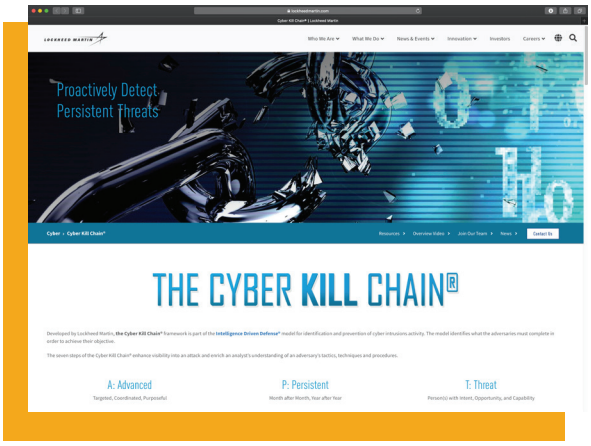
Assembling Weaponry: Tools for Understanding How Botnets Work

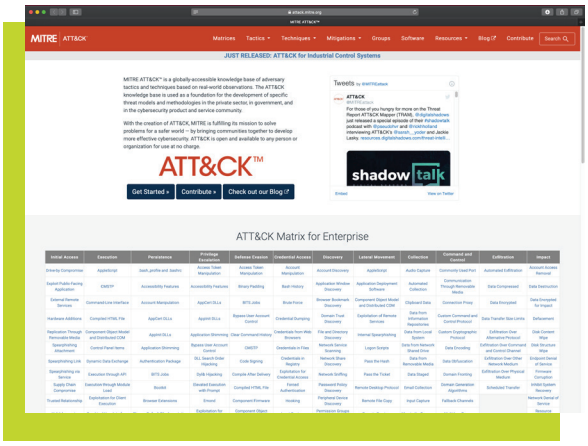
Botnets are often used as malicious tools to help conduct the work of a DDoS attack. It's essential that IT pros equip themselves with the knowledge of how that occurs to help them stay ahead of the onslaught.

There are two models that can help provide insight:

- **Lockheed Cyber Kill Chain:** This model outlines seven steps a hacker might take to conduct a long-term persistent DDoS attack. This model does not account for the use of botnets to compromise systems.
- **Mitre ATT&CK Model:** This model profiles real-world attacks and inventories those into a collective of information to help IT pros analyze and prevent future incidents. This model is particularly useful to individuals who wish to defend themselves against DDoS attacks because it allows you to profile attackers and identify their strategies.

As an IT pro, knowing how to approach a DDoS attack is of vital importance. Security analysts and threat hunters often use the ATT&CK model and the Mitre ATT&CK Navigator to help identify botnets. It is very likely that your organization may have to deal with an attack of one variety or another.





Who, Why, How of DDoS: The Details

One way to raise awareness about DDoS attacks is to understand who is committing these hacks, why they are targeting organizations and how they are accomplishing their goals.

A Brief History of Major Attacks:
DDoS Examples

Let's begin with a short list of major DDoS attacks, the motivations behind them and the lasting impact they have on our digital world.

Estonia: April 27, 2007
The DDoS attacks on Estonia occurred in response to the movement of a politically divisive monument to a military cemetery. To Russian-speaking Estonians, the statue represented Nazi liberation, but to ethnic Estonians, the monument symbolized Soviet oppression. Russian Estonians began rioting, and many were publicly outraged. The week of April 27, a barrage of cyberattacks broke out, most of them of the DDoS variety. Individuals used ping floods and botnets to spam and take down many financial institutions, government departments and media outlets. This attack is still regarded as one of the most sophisticated to date and is a solid example of a state-run attack.

Republic of Georgia: July 20, 2008
In 2008, the Republic of Georgia experienced a massive DDoS attack, mere weeks before it was invaded by Russia. The attack appeared to be aimed at the Georgian president, taking down several government websites. It was later believed that these attacks were an attempt to diminish the efforts to communicate with Georgia sympathizers. Not long thereafter, Georgia fell victim to Russian invasion. This attack is considered to be the textbook example of a coordinated cyberattack with physical warfare. It is studied around the world by cybersecurity professionals and military groups to understand how digital attacks can work in tandem with physical efforts.

Spamhaus: March 18, 2013
Infamously known as the "Attack that Almost Broke the Internet," the Spamhaus incident was, at the time, the largest DDoS attack in internet history. The attack was prompted when a group named Cyberbunk was added to a blacklist by Spamhaus. In retaliation, the group targeted the anti-spam organization that was curtailing their current spamming efforts with a DDoS attack that eventually grew to a data stream of 300 Gbps. The attack was so compromising that it even took down Cloudflare, an internet security company designed to combat these attacks, for a brief time..

Occupy Central: June 2014
The DDoS attacks that occurred during Occupy Central were an effort to cripple the pro-democracy protests that were occurring in Hong Kong in 2014. Two independent news sites, Apple Daily and PopVote, were known for releasing content in support of the pro-democracy groups. Much larger than the Spamhaus attack, Occupy Central pushed data streams of 500 Gbps. This attack was able to circumvent detection by disguising junk packets as legitimate traffic. Many speculate the attack was launched by the Chinese government in an effort to squash pro-democracy sentiments.

Dyn: October 21, 2016
A massive DDoS attack was launched against the DNS provider Dyn. The attack targeted the company's servers using the Mirai botnet, taking down thousands of websites. This attack affected stock prices and was a wake-up call to the vulnerabilities in IoT devices. The Mirai botnet comprised a collection of IoT-connected devices. The botnet was assembled by exploiting the default login credential on the IoT consumer devices which were never changed by end users. The attack impacted the services of 69 companies, including powerhouses such and Amazon, CNN and Visa.

GitHub: February 28, 2018
One of the largest DDoS attacks in history was launched against GitHub, viewed by many as the most prominent developer platform. At the time, this was the largest DDoS attack in history. However, due to precautionary measures, the platform was only taken offline for a matter of minutes. Attackers spoofed GitHub's IP address, gaining access to memcaching instances to boost the traffic volumes aimed at the platform. The organization quickly alerted support, and traffic was routed through scrubbing centers (see page 30 for more information) to limit the damage. GitHub was back up and running within 10 minutes.

Sector-Specific Attacks: 2019-2020
Multiple sectors, from manufacturing to retail to financial entities and governments are all reporting increasingly directed and specific attacks.

The Attacker Profile:
Who Performs DDoS Attacks

You often see images of nefarious, dark-hooded individuals to symbolize the malicious threat actor. In reality, groups of attackers are often well known to authorities and use DDoS tactics to gain influence, disrupt government and military operations or cause people to lose confidence in a market sector, company brand or long-established institution.

Regardless of the motivations that power these attacks, hackers can easily be hired to help launch a DDoS attack. Individuals or entire commercial groups are available for hire on the dark web, often under a service model, similar to that of infrastructure as a service (IaaS) or software as a service (SaaS). Understanding motivation can help uncover causes, but perpetrators are often simply guns for hire.

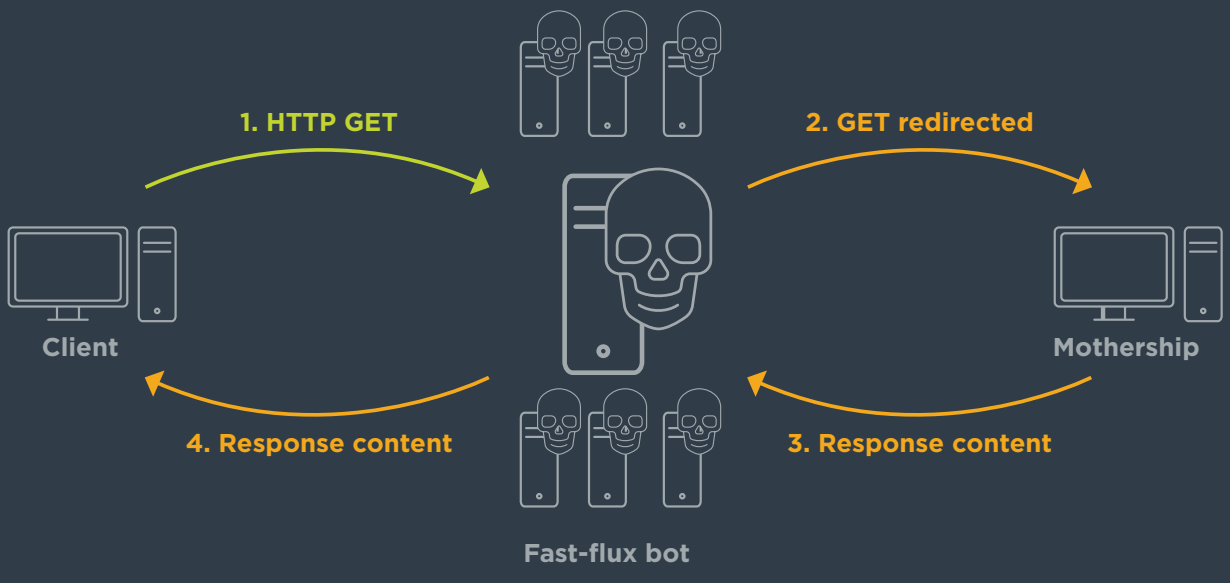
In fact, in December 2019, two Russian hackers were indicted for unleashing a DDoS attack on a U.S.-based bank that were allegedly operating on a DDoS-for-hire model. The attack is being touted as "one of the biggest bank robbery schemes of the past decade."

Tools of the Attacker:
How Attackers Avoid Detection

Attackers have long used IP spoofing to avoid attacks. Most IT professionals know that the IPv4 protocol has no inherent safeguards against spoofing. Most implementations of IPv6 don't fully use the protocol, which invites spoofing attacks.

Attackers are now using another method to hide their activity: Fast Flux DNS. By manipulating DNS traffic, DDoS botnets use multiple IP addresses assigned to a resource. The botnets then swap IP addresses at random, which occurs very quickly. As a result, it is more difficult for incident responders to trace attack traffic.

A variation of Fast Flux DNS is Double Flux DNS, which involves the use of multiple DNS names and manipulating the HTTP GET commands. This strategy is extremely effective for avoiding detection.



What Motivates an Attack:
The Reasons Behind a DDoS Attack

In order to thwart DDoS attacks, it's important to understand what motivates an attack. These motivations often spur a cyber threat.

As of late, DDoS attackers have the following motives:

Financial: DDoS attacks are often combined with ransomware attacks. The attacker sends a message informing the victim that the attack will stop if the victim pays a fee. These attackers are most often part of an organized crime syndicate. Today, though, these syndicates can be as small as a dozen individuals with net-working knowledge and extra time on their hands. Sometimes, rival businesses will even conduct DDoS attacks on each other to gain a competitive edge.

Ideological Disagreements: Attacks are often launched to target oppressive governing bodies or protestors in political situations. An attack of this kind is often conducted to support a particular political interest or belief system (e.g., a religion).

Commercial or Industrial Espionage: Attacks help to gather information or cause damage to particular industry sectors. For example, attacks on companies such as Sony, British Airways and Equifax caused consumers to lose faith in whole industries.

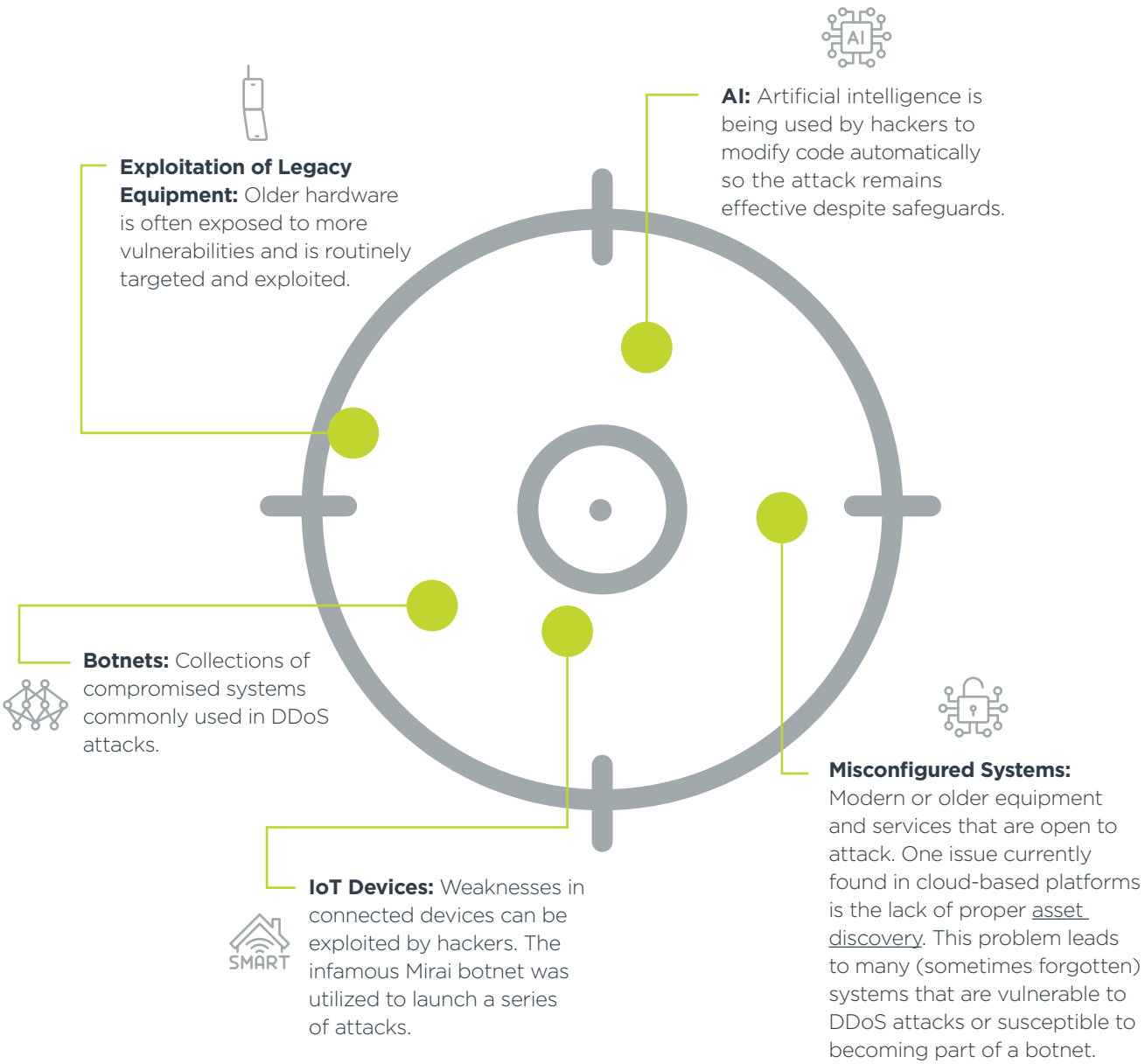
Tactical: In this case, the DDoS attack is always waged as part of a larger campaign. In some cases, the campaign includes a physical attack or another series of software-based attacks. Attacks are used to divert attention away from normal IT tasks to take advantage of a different target – the old bait-and-switch cyberattack.

Extortion: Other attacks are used to attain some personal or monetary gain through extorted means.

State-Sponsored: DDoS attacks are often waged to cause confusion to military troops and civilian populations alike.

Missile Launched:
Tools That Perform DDoS Attacks

Attackers use several devices to target organizations. These are some common tools for DDoS attacks:



Exploitation of Legacy Equipment: Older hardware is often exposed to more vulnerabilities and is routinely targeted and exploited.

AI: Artificial intelligence is being used by hackers to modify code automatically so the attack remains effective despite safeguards.

Botnets: Collections of compromised systems commonly used in DDoS attacks.

IoT Devices: Weaknesses in connected devices can be exploited by hackers. The infamous Mirai botnet was utilized to launch a series of attacks.

Misconfigured Systems: Modern or older equipment and services that are open to attack. One issue currently found in cloud-based platforms is the lack of proper asset discovery. This problem leads to many (sometimes forgotten) systems that are vulnerable to DDoS attacks or susceptible to becoming part of a botnet.

The Role of Recon:
How Attackers Gather Information Before a DDoS Attack

Attackers use various methods to glean useful information. Understanding these approaches will help you calculate how susceptible your organization is to an attack. Information gathering involves direct and indirect forms of reconnaissance.

Direct Recon

Direct recon utilizes tools and physical activity to gain information. Attackers can use tools such as Nmap to map the network, thereby provides attackers with a comprehensive picture of connected devices. Surprisingly, much of the initial information gathering takes place offline. Details obtained in real-world settings can be very valuable and attackers get them by:

- **Shoulder surfing:** Attackers skim info by looking over your shoulder. This also includes instruction on social engineering tactics.
- **Dumpster diving:** Attackers make use of scavenged documents taken from the trash. Sensitive information can easily be obtained by sifting through organizational and individual trash, particularly that of a high-profile person.
- **Organizational activity:** Attackers use building activity to gain physical recon. By monitoring who comes and goes and what time they routinely enter and exit, hackers can gain access to protected physical space and computing equipment.

Indirect Recon

Indirect recon is undertaken as an effort to understand the target. They identify things like:

- **Individuals susceptible to social engineering:** Attackers introduce malware or attack a specific network element.
- **Network configuration:** Attackers locate routers, firewalls and DNS servers to determine the traffic needed.
- **Digital assets:** Traditional computer networks and any cloud-based systems.
- **End points:** Can be vulnerable if configured poorly.
- **Monocultures:** Exploiting a monoculture can yield extensive damage with a smaller amount of effort.

A common name given to indirect recon is open-source intelligence (OSINT). Indirect reconnaissance tools do not leave the same traces as active tools.

Network Profiling

Attackers can use techniques like ping and port scan to uncover network vulnerabilities and utilize AI-driven scans to detect weaknesses they can exploit. This can vary by existing network conditions and is constantly evolving.

Tools for Cybersecurity Awareness

Whois

An information resource provided by ICANN concerning Domain Name Service (DNS) registrations. Although most Whois lookups give back redacted information, it is possible to obtain in-depth information from certain Whois sites.

Shodan

Often called "Google for hackers," this site contains an up-to-date searchable database of public-facing systems. A Shodan search can identify IoT, OT and traditional resources (e.g., web servers) that have default settings, patch levels and passwords.

Censys

A site similar to Shodan.

IVRE

A site similar to Shodan.

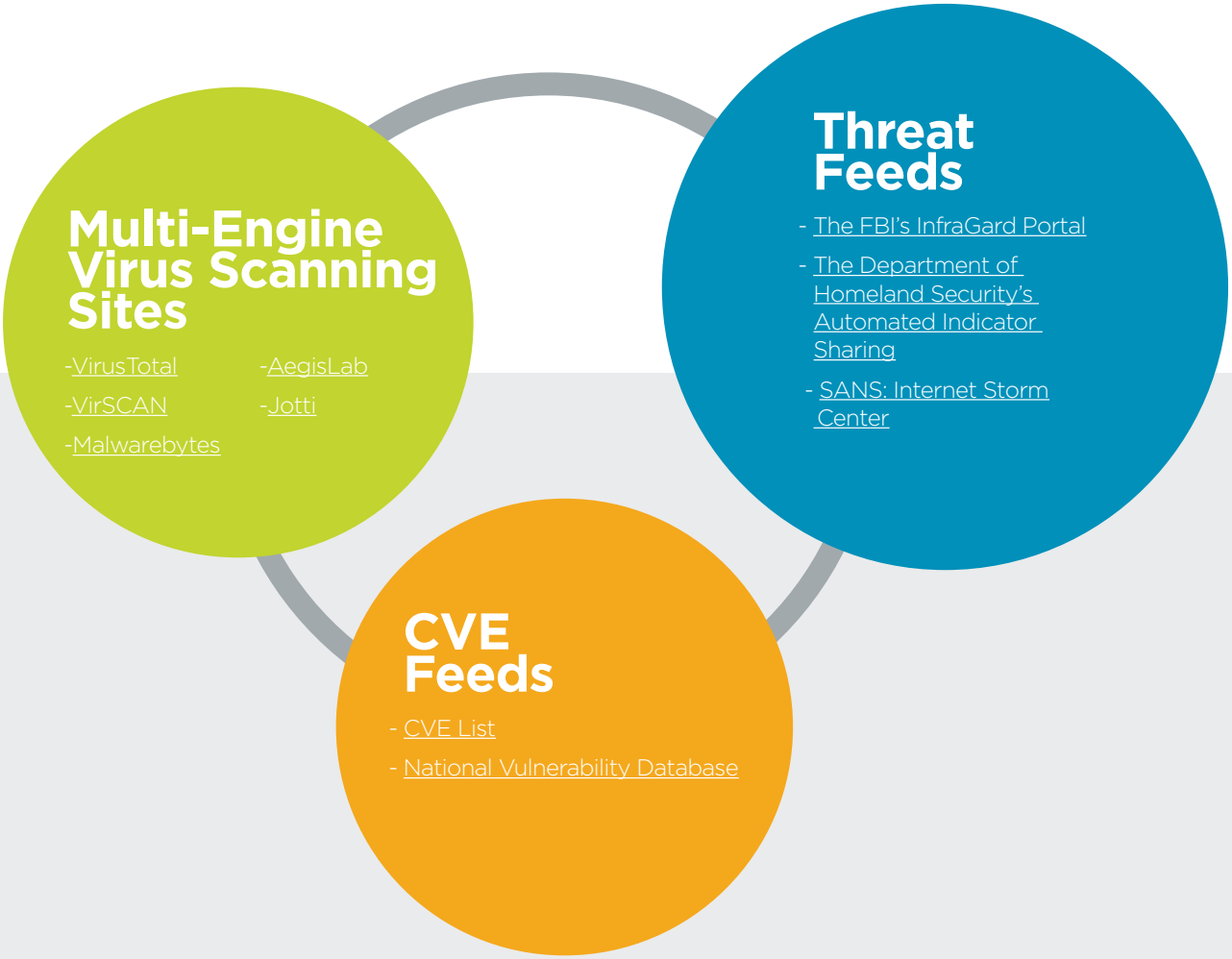
Maltego

A Java-based application that obtains OSINT information.

Modern Warfare:
The Role of AI in DDoS Attacks

There are multiple resources for IT pros to gain information about cyber threats.

3 RESOURCES FOR CYBER THREAT DETAILS



A Misguided Defense: Illegitimate Use of Legitimate Resources

Increasingly, attackers are using the same systems that defenders use. Sites such as VirusTotal are completely legitimate. It is used to amalgamate all antivirus vendor tools. Legitimate IT and security workers can use this site to see if certain files contain threat vectors (e.g., botnet code, etc.).

But, attackers will often use legitimate tools such as VirusTotal to actually create vectors that evade antivirus vendors. They upload the evil code that they've created to VirusTotal. If VirusTotal flags the malware, then they continue to make changes to the malware code they've created until VirusTotal no longer detects the attack.

Attackers will launch this code and attack victims. Because VirusTotal uploads are also usually available to the public, it is possible for anyone (including attackers and other companies) to view the files that have been uploaded. Such uploads can reveal information about networks and companies that have been attacked. Some companies may not want to provide even indirect information about attacks on their network.

Attackers also use the benefits of innovation to their advantage. It stands to reason that with more sophisticated technology come more advanced attacks.

How Attackers Use AI

- Identify systems
- Determine their state
- Exploit open communication of vulnerabilities
- Automate code changes to remain impervious to detection

Target Identified:
What Do DDoS Attackers Target the Most?

Certain systems are particularly vulnerable to DDoS attacks. Attackers will target the following devices in an attempt to gain control of your network.

- **End Points:** This includes equipment such as mobile devices, workstations and servers – anything that is connected to your network.
- **ISP/Cloud Providers:** Because these providers service many companies, they are often a target of DDoS attacks.
- **Operational Technology:** When the goal is to target infrastructure, OT often comes under attack.
- **Social Media:** Instagram and Facebook have both been the target of attacks affecting access for all platform users.

SECTORS MOST VULNERABLE TO DDoS ATTACKS:

HEALTH CARE

GOVERNMENT

INTERNET SERVICE PROVIDERS (ISPs)

CLOUD SERVICE PROVIDERS

DDoS Response and Mitigation

Preparation and quick response are of vital importance when facing a DDoS attack. Knowing what to look for and where to find information can help you mitigate damage.

Eyes on the Enemy:
Identifying DDoS Attacks

Look for these DDoS attack warning signs:

- Customers report slow or unavailable service
- Employees utilizing the same connection also experience issues with speed
- Multiple requests come in from a specific IP address over a short amount of time
- You receive a 503 service unavailable error when no maintenance is being performed
- Ping requests to technology resources time out due to Time to Live (TTL) timeouts
- Logs show an abnormally huge spike in traffic

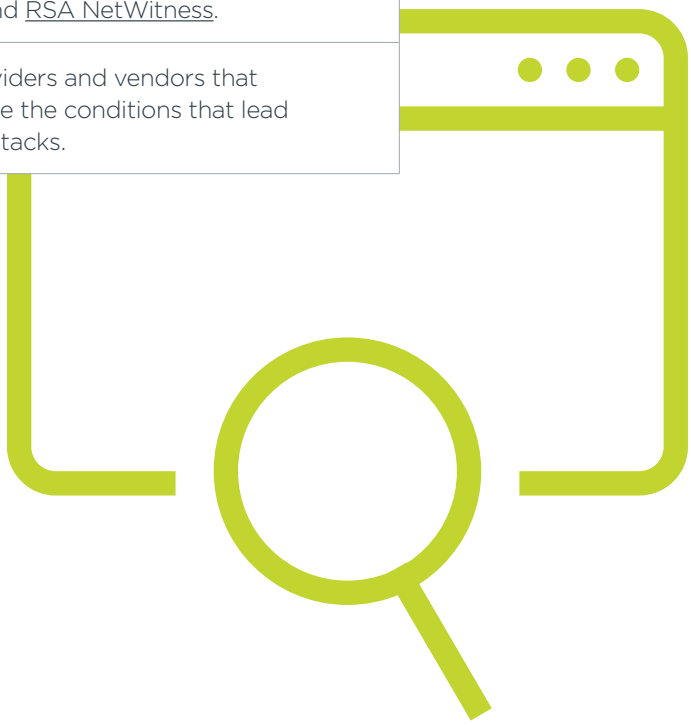
To find help with tracking and locating DDoS attacks in real time, use the following resources:

- Digital Attack Map
- Botnet Connection Dashboard
- Threatbutt Internet Hacking Attack Attribution Map
- Is It Down Right Now?

Tracking the Attack:
Traffic Monitoring Applications

Many traffic monitoring applications exist. Here are a few examples.

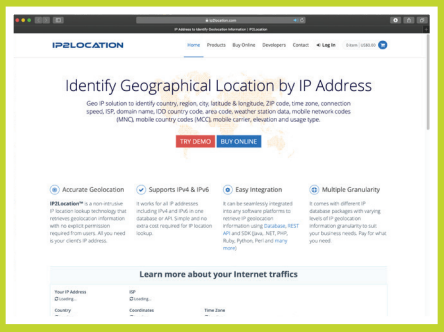
Tool	Description
ntop	Provides detailed network traffic and usage statistics.
Wireshark	The de facto standard packet capturing app.
Capinfos	Prints statistics from pcap files.
Snort	Open-source intrusion detection system (IDS).
Cisco IOS Netflow	Like Ntop – detailed network usage statistics.
Endpoint protection	Software can include products from Tanium, Symantec, Sophos and many others.
Spreadsheets	Don't laugh. Security analysts spend hours poring over spreadsheets created by IDS and security information and event management (SIEM) tools.
Security Information and Event Management (SIEM) software	Many SIEM products exist, including AlienVault, Splunk Enterprise Security and RSA NetWitness.
Third-Party Security Providers	Managed service providers and vendors that track and help manage the conditions that lead to successful DDoS attacks.



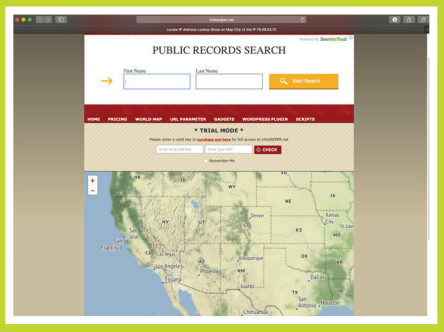
Tactically, IT professionals spend considerable time tracing spoofed traffic to its actual source. Here are some commonly used applications:

IP Tracker

IP2Location

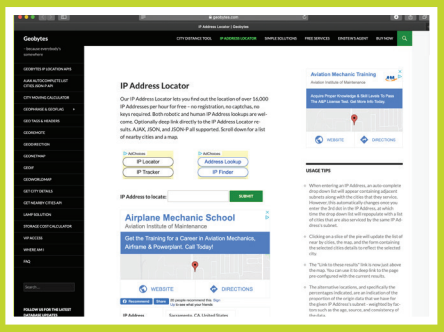


InfoSniper

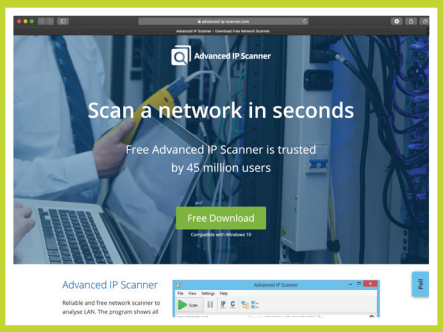


MaxMind Geo IP

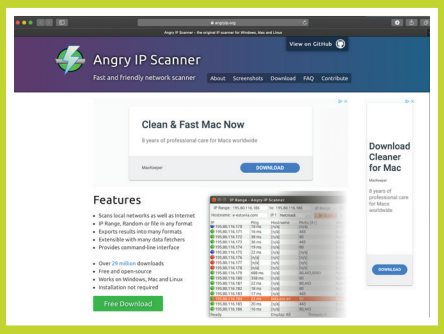
Geobytes IP Locator



Advanced IP Scanner



Angry IP Scanner



Prep the Defense:
DDoS Mitigation

When it comes to DDoS threats, a little prep work can go a long way. Try these tactics to practice preventative measures.

Network Reconfiguration

Examining how your network is configured can help reveal weaknesses before attackers can exploit the holes. Perform consistent audits internally and externally to help cover all your bases. Additionally, Border Gateway Protocol (BGP) can help reroute network traffic before it reaches its intended target.

Reconfiguration can be manual, where an IT pro manually changes network assets and configurations or automatic using AI or pre-determined orchestration tools.

Tabletop Exercises and Simulations

These are two options you can utilize for staff training on cybersecurity incidents:

- Tabletop exercises focus on non-technical aspects of incident response and can be practiced "at the table." These skills include things such as communication, teamwork and protocol knowledge.
- Simulations involve live drills of a mock cybersecurity incident so that IT pros and staff can practice their actual technical response skills.

Read more about how to run a war game.

Staff Training

All staff need to be trained to learn to recognize the warning signs of a possible attack. This should not only fall to IT departments or third-party providers. It is vital that all personnel understand who to report to and what information needs to be provided to help limit the damage of an incident.

Executive Buy-In

As with any coordinated organization-wide effort, you'll need executive buy-in. It's essential that leadership recognize the value of cybersecurity awareness and preparation and that they allocate the necessary resources and stress the importance to staff.

A Defense Strategy: DDoS Response

1. Detection:

Early detection is critical for defending against a DDoS attack. Look for warning signs, provided above, that you may be a target.

2. Diversion

The next step involves diverting traffic so that it doesn't affect your critical resources. This is done by sending the DDoS traffic into a scrubbing center or other resource that acts as a sinkhole. This process should be transparent so that employees and customers don't need to change their behavior to accommodate slowness.

3. Filtering

A transparent filtering process helps to drop the unwanted traffic. This is done by installing effective rules on network devices to eliminate the DDoS traffic.

4. Analysis

Understanding where the DDoS attack originated is important. This knowledge can help you develop protocols to proactively protect against future attacks. While it may be tempting to try and kill off the botnet, it is challenging, can create logistical and legal issues and is usually not recommended.

Weapons at the Ready:
Response Techniques and Services

As with any cyber threat, there are multiple services and tools available to IT pros to help mitigate possible damage.

- **Scrubbing Centers:** Essentially, scrubbing centers take traffic meant for a certain IP address and route it to a different location. The scrubbing center cleans the data, only allowing legitimate business traffic to pass on to the destination.
- **Scrubbers:** Similarly named, scrubbers provide DDoS mitigation services to organizations. Well-known providers include:
    - Akamai
    - Radware
    - Cloudflare

Examples of Layer 7 methods for managing DDoS attacks include:

- **Traffic filtering:** The use of scrubbing centers and services.
- **Layer 7 control:** Using CAPTCHAs and cookie challenges.

There are also several DDoS mitigation service vendors available to help manage an attack.

DDoS Mitigation Vendor	Services Offered
AWS Shield	Offers protection against layer 3 and layer 4 attacks. Available to all customers at no extra charge. Additional protection for Layer 7 attacks are available for a fee.
Neustar DDoS Protection	Solutions include cloud-based, on-premise and hybrid DDoS protection.
Cloudflare DDoS Protection	Layer 3, 4, and 7 services for free, as well as more sophisticated services for a fee.
Akamai	Highly respected service for help against volumetric attacks. Owns many sites around the world to help identify and filter traffic.
AppTrana	Focuses on Layer 7, as well as volumetric (Layer 3 and 4) traffic.
Alibaba DDoS	Specializes in mitigating volumetric attacks.

A Coordinated Defense:
Best Practices for DDoS Response

Use the steps in the following table to prepare for a DDoS attack.

DDoS Preparation Step	Description
1 Policy creation or alteration	If you don't have a defined security policy, then creating one is the first step. If your policy is older or hasn't considered modern DDoS methods and issues, it's time to make a few changes.
2 Identify vulnerable assets	Identify key endpoint and server assets, including the following: • Traditional installed services • Cloud services • Data centers • Infrastructure servers (e.g., DNS and dynamic host configuration protocol (DHCP). • Business-critical servers: web, customer relationship management (CRM), AI, machine learning, streaming, data collection and so forth. It may also be necessary to outline all business-critical applications running on your web servers.
3 Information backup	Have full copies of mission-critical information to allow your organization to reduce mean time to recovery and mean time to respond.
4 ISP backup	Larger organizations will want to have multiple ISPs ready in case one becomes flooded with traffic or can't provide an essential filtering service in time. Another option is obtaining a third-party scrubbing service that filters out DDoS traffic.
5 Server and endpoint backup	It is important to back up server resources, as well as workstations and other devices.
6 Risk analysis	A DDoS preparation scheme will always identify the risk involved when specific resources become compromised.
7 Identify and assign responsibility	The last thing an organization wants to do is assign responsibility for DDoS response during or after an actual attack. Assign responsibility before an attack happens.
8 Practice	Never assume that an untested set of procedures is adequate. In the same way an untested backup is no backup at all, an untested DDoS response plan is no plan at all.

A Coordinated Defense:
Best Practices for DDoS Response

When dealing with a DDoS attack, there are certain best practices that can help keep a situation under control. Observe these DDoS attack do's and don'ts.

Do: Overcommunicate with management.
Leadership needs to be informed and involved so that the necessary steps are taken to limit damage.

Do: Delegate tasks.
A DDoS attack means all hands on deck. Enlist other IT pros to report back and follow up with quick updates.

Do: Focus on root-cause analysis.
Uncovering the cause of the attack can be vital when attempting to slow the progression.

Do: Conduct mock exercises for DDoS attacks.
This may involve planned or surprise exercises to properly educate IT pros, staff and management on response activities.

Do: Work with ISPs, cloud providers and other service providers to determine the costs related to the DDoS attack.
Get a report from all providers. To move past the attack, you need to know exactly what you are dealing with and have documentation to illustrate it.

Don't: Overcommunicate with the public.
To limit damage to your brand's reputation and ensure you have the attack contained, only provide necessary information to the public.

Don't: Assume that it is someone else's responsibility to handle the attack.
These attacks must be dealt with quickly, and waiting to hand off responsibility can cost valuable time.

Don't: Try to solve the problem alone. DDoS attacks can escalate very quickly.
Enlisting others in your mitigation efforts will help curb the attack more quickly.

Don't: Make the assumption that IT pros, staff or management know what to do during a DDoS attack.
Without proper training, these attacks can be damaging, and many employees lack the practical skills to counter-act the hack.

Don't: Presume old reports are still valid.
Any reports older than six months or that involve data from before a company merger or major business change should not be considered sound data.

IT Pro Skills and Tools

As an IT pro, you can take steps to help ready yourself for a DDoS attack. Check out the following skills and tools that can help you successfully manage an incident.

Attack Basics:
The Skills You Need to Manage DDoS Attacks

Employers will want to know that you are armed with the skills necessary for combatting a DDoS attack. Adding these skills to your toolset will help illustrate your ability to thwart attacks.

Develop effective planning and management of products and applications.

Communicate clearly during a response.

Demonstrate ability to work with cloud and ISP providers to tackle difficult situations and troubleshoot problems.

Illustrate effectiveness in red teaming and blue teaming drills.

Proactively act as a threat hunter to identify potential threats and understand critical systems to business operations.

Incident Response Standards

Standards such as the U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 provide a helpful foundation for knowing how to respond to attacks of various types. The IT industry also uses the ISO/IEC 27035-1:2016 standard as a guideline for incident response procedures. As a general rule, organizations with a reputation for responding well to incidents tend to use such standards as helpful guidelines, rather than absolute rules to follow.

IT pros can also benefit from seeing demonstrations of attacks to learn how data behaves in particular situations. Take the time to view demonstrations of the following attacks:

RANSOMWARE

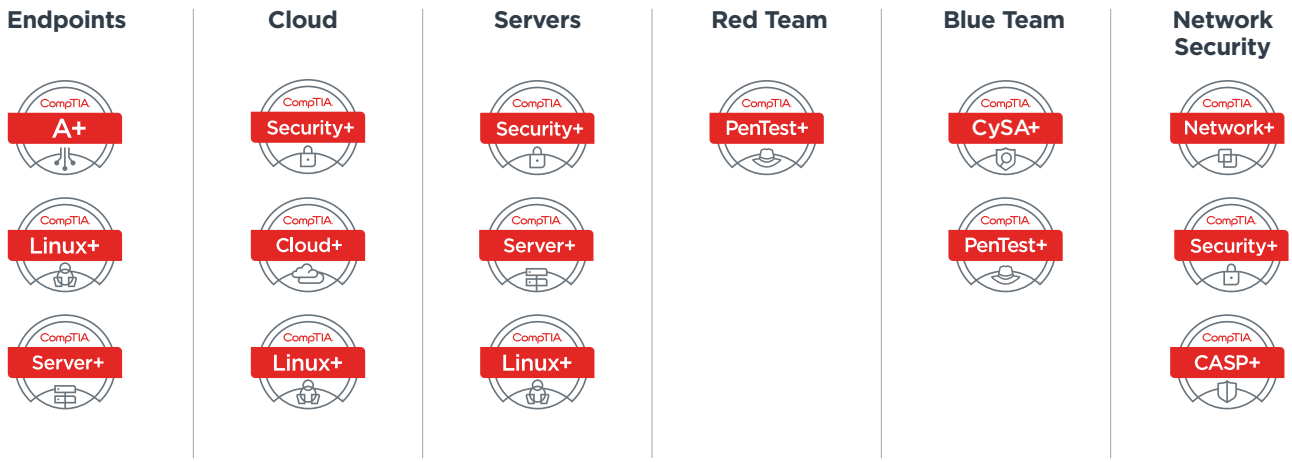
DDoS

BROWSER-BASED THREAT

DDoS Boot Camp:
DDoS Education Options for IT Pros

Ongoing education is essential for any IT pro. Technology advances every day, and IT pros that stagnate will eventually be deemed unnecessary as legacy systems die off and new platforms take their place. To remain relevant, it's important to continue educating yourself.

The standards and practices taught in the industry will also help you and your organization respond to DDoS attacks. One way to obtain the appropriate level of knowledge is to learn the standards and best practices covered by the IT certifications found in the CompTIA Cybersecurity Pathway.



Download the exam objectives for the above CompTIA exams to see what's covered and decide which one is right for you.

Terms to Know

TCP: Transmission control protocol

UDP: User Datagram Protocol

ACK: Acknowledgement packet

SYN: Synchronize packet

ICMP: Internet Control Message Protocol

HTTP: Hyper Text Transfer Protocol

DNS: Domain Name System

OSI/RM: Open Systems Interconnection/Reference Model

Incident response: Steps to take when managing a DDoS attack.

SYN Flood: Where an attacker manipulates the three-way TCP handshake to create a DDoS attack.

TCP handshake: A three-step process that occurs whenever two computers communicate with each other at the beginning of a TCP session. Also known as the TCP three-way handshake.