HC3: Analyst Note

May 30, 2024 TLP:CLEAR Report: 202405301200

Healthcare Sector DDoS Guide

Executive Summary

A Distributed-Denial-of-Service (DDoS) attack is a type of cyber attack in which an attacker uses multiple systems, often referred to as a botnet, to send a high volume of traffic or requests to a targeted network or system, overwhelming it and making it unavailable to legitimate users. With the number of attacks increasing every year, they can come at any time, impact any part of a website's operations or resources, and lead to massive amounts of service interruptions and huge financial losses. In the health and public health (HPH) sector, they have the potential to deny healthcare organizations and providers access to vital resources that can have detrimental impact on the ability to provide care. Disruptions due to a cyber attack may interrupt business continuity by keeping patients or healthcare personnel from accessing critical healthcare assets such as electronic health records, software based medical equipment, and websites to coordinate critical tasks. As such, this comprehensive DDoS guide is intended for target healthcare audiences to understand what DDoS attacks are; what causes them; types of DDoS attacks with timely, relevant examples; and mitigations and defenses against a potential attack.

Report

Not to be confused with Denial-of-Service (DoS) attacks, which usually attacks from a single system, a DDoS attack originates from multple sources and sends a larger volume of traffic into the system at once, making it difficult for network administrators to quickly detect and eliminate the threat. DDoS attacks have continually grown in size and sophistication, but 2023 accelerated this trend at an unforeseen pace. Last year alone, cybercriminal groups, geopolitically motivated hacktivists, and malicious actors utilized the relatively inexpensive cost of launching DDoS attacks, the scale of massive botnets built from everyday digital and Internet of Things (IoT) devices, and protocol-level zero-day vulnerabilities to launch record-breaking attacks on businesses, government institutions, and, most disturbingly, on critical but vulnerable public infrastructure, including hospitals.

In most cases, the assumed goals are to cause damage, productivity loss, and financial losses and to gain public attention, which is why these threat actors select an increasingly broad range of victims who are known to have insufficient IT security. It is important to remember that DDoS attacks are targeted attacks for which the threat actors consciously select their targets. Threat actors utilize DDoS attacks due to the cost effectiveness and relatively low resources and technical skills needed to deploy this type of attack as a hacker does not have to install any code on a victim's server. Moreover, DDoS attacks are getting more sophisticated and complex while getting easier and cheaper to perpetrate as cyber criminals take advantage of the sheer number of insecure internet-connected devices.

Profile of a DDoS Attacker

DDoS attackers are often groups of attackers 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. While any type of cyber threat actor (i.e., advanced persistent threats, cybercriminal groups, individuals, etc.) could orchestrate DDoS attacks, one of the biggest shifts in the DDoS threat landscape is the rise of hacktivist groups and the emergence of political motivation, rather than financial motivation, as the main driver for DDoS attacks.

Often considered a form of crowd-funded cyber terrorism, these groups present themselves as quasi-military organizations to solicit donations in cryptocurrency on social media channels to perpetrate DDoS

attacks on unsuspecting victims. As a result, the profile of targeted victims has expanded to include government institutions, civilian infrastructure, and non-profit organizations. For the HPH sector, this had also led to an increase in DDoS attacks against hospitals and healthcare institutions.

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

Motivations Behind DDoS Attacks

While DDoS attacks vary greatly in nature when it comes to tactics and methods, DDoS attackers also may have a multitude of motives, including the following:

- Financial Motives: 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 networking knowledge and extra time on their hands. Sometimes, rival businesses will even conduct DDoS attacks on each other to gain a competitive edge.
- Ideological Motives: Attacks are often launched to target oppressive governing bodies or protestors in political situations. A DDoS attack of this kind is often conducted to support a particular political interest or belief system, such as a religion.
- State-Sponsored Motives: DDoS attacks are often waged to cause confusion for military troops or civilian populations when political unrest or dissension becomes apparent. This was the case in 2008 when Russia conducted DDoS attacks against the Republic of Georgia prior to their invasion.
- Tactical Motives: In this case, the DDoS attack is waged as part of a larger campaign. In some cases, the campaign includes a physical attack or another series of software-based attacks. For example, militaries have been known to combine DDoS attacks with physical ones. Tactical attacks are used to divert attention away from normal IT tasks to take advantage of a different target – the old bait-and-switch cyberattack.
- Business/Economical Motives: DDoS attacks of this variety help to gather information or cause damage to industry sectors. For example, attacks on companies such as Sony, British Airways and Equifax caused consumers to lose faith in entire industries.
- Extortion Motives: Other attacks are used to attain some personal or monetary gain through extorted means.

Duration of DDoS Attacks

DDoS attacks vary greatly in length and sophistication. A DDoS attack can take place over a long period of time or be quite brief.

- Long-Term Attack: An attack waged over a period of hours or days is considered a long-term attack. For example, one attack on a company caused disruption for three days before finally being mitigated.
- Burst Attack: Waged over a very short period, these DDoS attacks only last a minute or even a few seconds.

Despite being very quick, burst attacks can be extremely damaging. With the advent of internet of things (IoT) 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. A burst DDoS attack is often advantageous for the attacker because it is more difficult to trace.

DDoS Attack Classification

In general, DDoS attacks can be segregated by which layer of the Open Systems Interconnection (OSI) model they attack. They are most common at the Network (layer 3), Transport (Layer 4), Presentation (Layer 6) and Application (Layer 7) Layers.

#	Layer	Application	Description	Vector Example
7	Application	Data	Network process to application	HTTP floods, DNS query floods
6	Presentation	Data	Data representation and encryption	SSL abuse
5	Session	Data	Interhost communication	N/A
4	Transport	Segments	End-to-end connections and reliability	SYN floods
3	Network	Packets	Path determination and logical addressing	UDP reflection attacks
2	Datalinks	Frames	Physical addressing	N/A
1	Physical	Bits	Medica, signal, and binary transmission	N/A

While thinking about mitigation techniques against these attacks, it is useful to group them as Infrastructure layer (Layers 3 and 4) and Application Layer (Layer 6 and 7) attacks.

Infrastructure Layer Attacks

Attacks at Layer 3 and 4, are typically categorized as Infrastructure layer attacks. These are also the most common type of DDoS attack and include vectors like synchronized (SYN) floods and other reflection attacks like User Datagram Packet (UDP) floods. These attacks are usually large in volume and aim to overload the capacity of the network or the application servers. But fortunately, these are also the type of attacks that have clear signatures and are easier to detect.

Application Layer Attacks

Attacks at Layer 6 and 7, are often categorized as Application layer attacks. While these attacks are less common, they also tend to be more sophisticated. These attacks are typically small in volume compared to the Infrastructure layer attacks but tend to focus on particular expensive parts of the application thereby making it unavailable for real users. For instance, a flood of HTTP requests to a login page, or an expensive search API, or even Wordpress XML-RPC floods (also known as Wordpress pingback attacks).

Categories of DDoS Attack Tools

A number of tools exist that can be adapted to launch DoS/DDoS attacks, or are explicitly designed for that purpose. The former category are often “stressors” — tools with the stated purpose of helping security researchers and network engineers perform stress tests against their own networks, but which can also be used to perform genuine attacks. Some are specialized and only focus on a particular layer of the OSI model, while others are designed to allow for multiple attack vectors. Categories of attack tools include:

Category	Description
Low and slow attack tools	As the name implies, these types of attack tools use a low volume of data and operate very slowly. Designed to send small amounts of data across multiple connections in

	order to keep ports on a targeted server open as long as possible, these tools continue to take up the server's resources until it is unable to maintain additional connections. Uniquely, low and slow attacks may at times be effective even when not using a distributed system such as a botnet and are commonly used by a single machine.
Application layer (L7) attack tools	These tools target layer 7 of the OSI model, where Internet-based requests such as HTTP occur. Using an HTTP flood attack to overwhelm a target with HTTP GET and POST requests, a malicious actor can launch attack traffic that is difficult to distinguish from normal requests made by actual visitors.
Protocol and transport layer (L3/L4) attack tools	Going further down the protocol stack, these tools utilize protocols like UDP to send large volumes of traffic to a targeted server, such as during a UDP flood. While often ineffective individually, these attacks are typically found in the form of DDoS attacks where the benefit of additional attacking machines increases the effect.

Commonly Used DoS/DdoS Attack Tools

Attack Tool	Description
Low Orbit Ion Cannon (LOIC)	The LOIC is an open-source stress testing application. It allows for both TCP and UDP protocol layer attacks to be carried out using a user-friendly WYSIWYG interface. Due to the popularity of the original tool, derivatives have been created that allow attacks to be launched using a web browser.
High Orbit Ion Cannon (HOIC)	This attack tool was created to replace the LOIC by expanding its capabilities and adding customizations. Using the HTTP protocol, the HOIC is able to launch targeted attacks that are difficult to mitigate. The software is designed to have a minimum of 50 people working together in a coordinated attack effort.
Slowloris	Slowloris is an application designed to instigate a low and slow attack on a targeted server. It needs a relatively limited amount of resources in order to create a damaging effect.
R.U.D.Y (R-U-Dead Yet)	R.U.D.Y. is another low and slow attack tool designed to allow the user to easily launch attacks using a simple point-and-click interface. By opening multiple HTTP POST requests and then keeping those connections open as long as possible, the attack aims to slowly overwhelm the targeted server.

Types of DDoS Attacks

There are several different types of DDoS attacks, as illustrated by multiple cybersecurity organizations. One simplified version from SentinelOne is below:

Type of DdoS Attack	Description
Network-layer attack	This type of attack involves overwhelming the targeted network or system with traffic from multiple sources, such as by flooding it with packets.
Application-layer attack	This type of attack involves exploiting vulnerabilities in an application or service, such as a web server, to cause it to crash or become unresponsive.
Protocol attack	This type of attack involves exploiting vulnerabilities in network protocols, such as TCP or UDP, to cause the targeted system to crash or become unresponsive.
Amplification attack	This type of attack involves using a reflection technique, such as DNS amplification, to amplify the volume of traffic sent to the targeted system.

Hybrid attack	This type of attack combines multiple attack vectors, such as network-layer and application-layer attacks, to create a more complex and effective attack.

A more detailed version can be gleaned from The Center for Internet Security, Inc. (CIS)' Multi-State Information Sharing and Analysis Center (MS-ISAC), which further categorizes DDoS attacks into two categories: Standard and Reflection, as seen in the table below with detailed descriptions and recommendations from their website.

A standard DDoS attack occurs when cyber threat actors direct substantial network traffic to a target server or network. One of the ways a threat actor accomplishes this is by using a botnet to send the network traffic. A botnet is a large number of previously compromised devices (also known as "bots" or "zombies") that can be controlled over the internet from a single location and directed to carry out desired actions. When a threat actor uses a botnet to perform a DDoS attack, they send instructions to zombie machines connected to that botnet, thereby magnifying the scale of their attack. By leveraging a botnet, attackers enable a DDoS attack to originate from multiple networks and even multiple countries.

A reflection DDoS attack occurs when attackers spoof their IP address to pose as the intended victim and then send requests to public-facing servers. The responses to these requests are sent to the intended victim from legitimate servers.

Category	Type of DdoS Attack	Variations
Standard	SYN Flood	Slowloris Attacks ESSYN/XSYN Flood PSH Flood
Standard	UDP Flood	
Standard	SMBLoris	
Standard	ICMP Flood	Smurf Attack
Standard	HTTP GET Flood	HTTP POST Flood
Reflective	NTP Reflection Attack with Amplification	
Reflective	DNS Reflection Attack with Amplification	
Reflective	CLDAP Reflection Attack with Amplification	TCP LDAP Reflection Attack with Amplification Variant
Reflective	WordPress Pingback Reflection Attack with Amplification	
Reflective	SSDP Reflection Attack with Amplification	
Reflective	Microsoft SQL Reflection Attack with Amplification	
Reflective	Memcached DDoS Attacks (Amplification)	

Best Practices to Prevent a DDoS Attack

- **Use infrastructure upgrades and redundancy:** Having a robust and scalable infrastructure can help withstand a sudden influx of traffic. Implementing redundancy, such as having multiple servers in different locations, can ensure continued service even if one server is targeted.
- **Perform regular security audits and patch management:** Regularly check for system vulnerabilities and keep all your software, including operating systems, applications, and any security tools, updated. Install patches and fixes as soon as they become available.
- **Have an incident response plan:** Have a clear and well-practiced response plan in place. This ensures you know what to do if an attack happens, which can significantly reduce the potential

damage.

- Monitor traffic: Monitoring your network traffic can help you identify patterns indicative of a DoS or DDoS attack. Using tools that can alert you to unusual traffic patterns can help you respond quickly when an attack happens.
- Use a DDoS mitigation service: These services specialize in detecting and mitigating DDoS attacks, providing an extra layer of security. They can help absorb the traffic associated with these attacks and prevent them from reaching your network.
- Use a SIEM solution: A (security information and event management) SIEM solution provides real-time analysis of network traffic and system logs, swiftly identifying abnormal patterns indicative of DDoS attacks. This proactive approach empowers you to mitigate threats before they escalate, enhancing your cybersecurity posture.

Steps for DDoS Attack Response

Typical steps for responding to a DDoS attack include:

- Detection: Early detection is critical for defending against a DDoS attack. Look for warning signs, provided above, that you may be a target. DDoS detection may involve investigating the content of packets to detect Layer 7 and protocol-based attacks or utilizing rate-based measures to detect volumetric attacks. Rate-based detection is usually discussed first when it comes to DDoS attacks, but most effective DDoS attacks are not blocked using rate-based detection.
- 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.
- Diversion and Redirection: This step involves diverting traffic so that it doesn't affect your critical resources. You can redirect DDoS traffic by sending it into a scrubbing center or other resource that acts as a sinkhole. It is typically recommended that you transparently communicate what is taking place so that employees and customers don't need to change their behavior to accommodate slowness.
- Forwarding and 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 can create logistical problems and may result in legal ramifications. Generally, it is not recommended.
- Alternate Delivery: It is possible to use alternate resources that can almost instantaneously offer new content or open new networking connections in the event of an attack.

Tools for Understanding How DDoS Attacks Work

DDoS attacks take on many forms and are always evolving to include various attack strategies. It is essential that IT administrators equip themselves with the knowledge of how attacks work. There are three models that can help provide insight into the inner workings of DDoS attacks:

- Lockheed Martin Cyber Kill Chain: Used to help provide a framework for attack strategies, 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 provides a knowledge base of known adversarial tactics and techniques 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.
- Diamond Model of Intrusion Analysis: The Diamond model helps organizations weigh the capabilities

of an adversary and the capabilities of the victim, as discussed in a CompTIA blog about the three major cybersecurity models. Even though the Diamond model was created to model actual intrusions, it is also useful for identifying DDoS attacks.

Additional DDoS Resources:

- Understanding Denial-of-Service Attacks (Cybersecurity and Infrastructure Security Agency)
- Advanced DDoS Mitigation Techniques (National Institute of Standards and Technology)
- Distributed-Denial-of-Service (DDoS) Attacks (Health-ISAC)

DDoS Terminology

As DDoS attacks are highly technical, below are some common verbiage used when describing an attack:

Term	Definition
Advanced Persistent Threat (APT)	A stealthy threat actor, typically a state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.
Amplification attack	Type of DDoS attack that involves using a reflection technique, such as DNS amplification, to amplify the volume of traffic sent to the targeted system.
Application-layer attack	Type of DDoS attack that involves exploiting vulnerabilities in an application or service, such as a web server, to cause it to crash or become unresponsive.
Botnet	A network of computers infected and remotely controlled through a virus or malware program, that is used to make the requests to servers in a DdoS attack.
Burst attack	A DDoS attack lasting only a minute or even a few seconds.
Cybercriminal group	Individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company or personal data for generating profit.
Denial-of-Service Attack	An attack on a website that sends an overload of traffic (requests) to a web server.
Distributed-Denial-of-Service Attack	An attack that uses multiple compromised computer systems to increase the number of requests that can be made to a server at one time, making server overloads easier to accomplish and more difficult to prevent.
Gigabytes-per-second and Terabytes-per-second	A measurement of how much data is sent to servers in a DDoS attack, typically denotated as GB/s or TB/s.
Hacktivist	Often considered a form of crowd-funded cyber terrorism, these groups present themselves as quasi-military organizations to solicit donations in cryptocurrency on social media channels to perpetrate DDoS attacks on unsuspecting victims.
High Orbit Ion Cannon (HOIC)	An attack tool created to replace the Low Orbit Ion Cannon (LOIC) by expanding its capabilities and adding customizations.
Hybrid attack	Type of DDoS attack that combines multiple attack vectors, such as network-layer and application-layer attacks, to create a more complex and effective attack.
Internet of Things (IoT)	Describes the network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.
Layer 1 Attack	The channel transfers raw binary data between machines. It uses Bluetooth, USB, IrDA as well as hubs, sockets, and patch panels. Example attack: Layer 1 can be affected by physical destruction or any other network disruption. Man made failures lead to complete unusable hardware. DoS or DDoS attacks are impossible on this level.
Layer 2 Attack	The data link layer is responsible for the data exchange between the nodes within the local network. The data is arranged into frames and transmitted to the physical layer. Another function of this link layer is setting unique identifiers to network adapters – MAC addresses. Example attack: the most common is MAC flooding. Network switches are overloaded with data packets to disable all connection ports.

HC3: Analyst Note

May 30, 2024 TLP:CLEAR Report: 202405301200

Term	Definition
Layer 3 Attack	On this layer, routers and switches of different networks start interacting. Routing is based on the conversion of MAC addresses into network addresses. The main goal of this layer is to build the best way to transfer data between devices. Example attack: ICMP flood that overloads the target network with ICMP messages. It's aimed at reducing bandwidth and limiting the number of requests which can be processed via ICMP protocol.
Layer 4 Attack	It uses UDP and TCP protocols, as well as processes and transports data packets between communication nodes. Layer 4 controls the information flow and detects errors. If they are detected, it re-sends the data. Example attack: exceeding thresholds for channel width and number of available connections. The most common types of DDoS attacks are Smurf and SYN flood.
Layer 5 Attack	Layer 5 is responsible for interaction between applications, as well as establishing and terminating connections, and synchronizing OS tasks. Example attack: an attacker exploits software vulnerabilities via Telnet, so the administrator loses access to the server.
Layer 6 Attack	The layer encodes and decodes data and adapts it for humans or machines in an understandable way. This includes video, audio, images, and text data. There's the SSL protocol between Layer 6 and Layer 7. It provides the client with a secure connection to the server and mutual authentication. Example attack: SSL garbage flood. Hackers generate incorrect SSL requests to attack the victim's server. This slows down resources because it takes a long time to verify encrypted SSL packets.
Layer 7 Attack	The application layer works entirely for the user and presents data to the user in an understandable form. Example attack: malware that creates a large number of requests (HTTP flood) to connect, enter logins, place an order, download videos, etc. At the same time, legitimate users can't access the site because it's overloaded with junk requests.
Long-term attack	A DDoS attack waged over a period of hours or days.
Low Orbit Ion Cannon (LOIC)	An open-source stress testing application that allows for both TCP and UDP protocol layer attacks to be carried out using a user-friendly WYSIWYG interface
Memcached	A distributed memory caching system popularly used in DDoS attacks.
Mirai	Malware created to target Linux-based IoT devices, including home security cameras and routers. Mirai and its many variants are currently among the most-used malware to create DdoS botnets.
Network-layer attack	Type of DDoS attack that involves overwhelming the targeted network or system with traffic from multiple sources, such as by flooding it with packets.
OSI Model	The Open Systems Interconnection (OSI) model is a conceptual framework that divides network communications functions into seven layers. Sending data over a network is complex because various hardware and software technologies must work cohesively across geographical and political boundaries. The OSI data model provides a universal language for computer networking, so diverse technologies can communicate using standard protocols or rules of communication.
Protocol attack	Type of DDoS attack that involves exploiting vulnerabilities in network protocols, such as TCP or UDP, to cause the targeted system to crash or become unresponsive.
Reflective DDoS Attack	Occurs when attackers spoof their IP address to pose as the intended victim and then send requests to public-facing servers.
R.U.D.Y (R-U-Dead Yet)	A low and slow attack tool designed to allow the user to easily launch attacks using a simple point-and-click interface
Saturation	A term used for the amount of volume sent to a server during a DDoS attack. Supersaturation occurs when all of a system's resources are filled with requests from the DDoS attack, completely shutting down the system, while sub-saturation refers to small DDoS attacks that can negatively impact system performance and resources but are not nearly large enough to shut down a server completely. Sub-saturating attacks are increasingly common, often go undetected, and are commonly used as a "smokescreen" for larger attacks.
SIEM solution	Security information and event management (SIEM) solutions provide real-time analysis of network traffic and system logs, swiftly identifying abnormal patterns indicative of DDoS attacks.
Slowloris	An application designed to instigate a low and slow attack on a targeted server. It needs a relatively limited amount of resources in order to create a damaging effect.
Standard DDoS Attack	Occurs when cyber threat actors direct substantial network traffic to a target server or network.

HC3: Analyst Note

May 30, 2024 TLP:CLEAR Report: 202405301200

Relevant HHS Reports

HC3: Analyst Note – Internet of Things (IoT) Security (August 4, 2022)

HC3: Analyst Note – KillNet's Targeting of the Health and Public Health Sector (December 2022-March 2023) (April 5, 2023)

HC3: Analyst Note – Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector (January 30, 2023)

HC3: Threat Briefing – APT and Cybercriminal Targeting of HCS (June 9, 2020)

HC3: Threat Briefing – Iranian Threat Actors & Healthcare (November 3, 2022)

HC3: Threat Briefing – North Korean and Chinese Cyber Crime Threats to the HPH (September 21, 2023)

HC3: Threat Briefing – Types of Cyber Threat Actors That Threaten Healthcare (June 8, 2023)

References

Cook, Sam. "20+ DDoS attack trends and statistics in 2024: The rising threat." Comparitech. January 8, 2024. https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

"DDoS Attack Classification: A Complete Guide to DDoS Attack Types." DDoS-Guard. January 25, 2023. https://ddos-guard.net/en/blog/classification-of-ddos-attacks

"Distributed Denial of Service (DDoS): An Easy Guide 101." SentinelOne. Accessed April 15, 2024. https://www.sentinelone.com/cybersecurity-101/what-is-a-distributed-denial-of-service-ddos/

"Distributed Denial of Service (DDoS): MS-ISAC Guide to DDoS Attacks." Multi-State Information Sharing & Analysis Center. May 2023. https://learn.cisecurity.org/ms-isac-guide-to-ddos-attacks?_gl=1*16bhq4*_ga*MTE2OTYxMDg1NS4xNzEwMTY1MDIw*_ga_N70Z2MKMD7*MTcxMzE5ODk3My4yLjAuMTcxMzE5ODk3OC41NS4wLjA.*_ga_3FW1B1JC98*MTcxMzE5ODk3My4yLjAuMTcxMzE5ODk3OC4wLjAuMA.

"DoS and DDoS Attacks." ManageEngine. Accessed April 15, 2024. https://www.manageengine.com/log-management/cyber-security-attacks/what-is-denial-of-service-attack.html

Dummer, Sven and Sandeep Rath. "A Retrospective on DDoS Trends in 2023 and Actionable Strategies for 2024." Akamai. January 9, 2024. https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023

Gasic, Dalibor. "Top Cyber Attacks in 2022." Purplesec. January 12, 2022. https://purplesec.us/security-insights/top-cyber-attacks-2022/

"How to DDoS – DoS and DDoS attack tools." Cloudfare. Accessed April 15, 2024. https://www.cloudflare.com/learning/ddos/ddos-attack-tools/how-to-ddos/

"What is a DDoS Attack?" Amazon. Accessed April 15, 2024. https://aws.amazon.com/shield/ddos-attack-protection/

"What is a DDoS Attack and How Does It Work?" CompTIA. Accessed April 15, 2024. https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works

"What Is the Difference Between Dos and DDoS Attacks?" Radware. Accessed April 15, 2024. https://www.radware.com/cyberpedia/ddos-attacks/dos-vs-ddos-attack-what-is-the-difference/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback