DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

March 2021

Abstract

As information systems become more sophisticated, so do the methods used by the attackers. Criminal and nation state actors have long recognized the value of denial-of-service attacks which can cause serious business interruptions for any organization connected to the internet. Denial-of-Service attacks have increased in magnitude as more devices come online and organizations increase remote access for their staff. This paper covers the motivations behind DDoS attacks, provides several historical examples and details several strategic and tactical recommendations IT and information security professionals can implement in their organizations to limit impacts from these disruptive attacks.

Table of Contents

Executive Summary

As information systems become more sophisticated, so do the tactics, techniques and procedures (TTPs) used by attackers. While the financially motivated perversion of DDoS attacks has been a tactic used since the late 1990's, the use of Ransom denial-of-service attacks has been largely adopted by cyber criminals since 2015. Ransome denial-of-service attacks, or RDoS, are usually initiated through extortion letters sent via email to recipients of varying positions within organizations. The letter conveys threats to bombard the victim's network with unsolicited traffic within a certain number of days and advises of a relatively small attack to demonstrate capabilities for legitimacy. If victims do not pay the ransom, normally in the form of Bitcoin, the fee to stop the attack will increase with each day that passes without having received payment. In cases where the threat actor receives no communications from the victim, they will often execute follow-on RDoS attacks ranging weeks to months later from the initial attack.

Denial-of-Service attacks have increased in magnitude as more devices come online through Internet of Things (IoT) devices and organizations reinforce remote connectivity systems to supplement pre-existing infrastructure. Threat actors sought to capitalize on the current threat landscape in 2020 as telework increases in response to the novel coronavirus and efforts to encourage social distancing. Regardless of size, organizations often fail to exercise asset and inventory management best practices conducive to a thorough understanding of their attack surface. In addition, IoT devices often utilize default passwords and do not have sound security postures, making them vulnerable to compromise and exploitation. Infection of IoT devices often goes unnoticed by users, and an attacker could easily compromise hundreds of thousands of these devices to conduct a large-scale attack.

Impacts to the Threat Landscape

Defending the health sector from threats is an ongoing challenge as adversaries appear to have endless attack methodologies available. Of the large breadth of malicious methods, distributed denial-of-service (DDoS) and ransom denial-of-service (RDoS) attacks have been frequently used by threat actors. In 2020, for instance, Digital Shadows researchers observed several attacks against the healthcare industry, most notably a March 2020 DDoS attack against the US Health and Human Services Department operated by an unknown threat actor at a critical moment amid the coronavirus outbreak. According to research conducted by Digital Shadows, three main trends that can be expected to persist throughout 2021 include leveraging IoT devices, offering DDoS service solutions, and DDoS extortion. The persistent creation of malicious tools and the propensity to sell them on criminal markets to accommodate threat actor demand ensures that the playbooks of threat actors involved in DDoS activity will continue to expand in tandem with attempts to mitigate the threat of such attacks.

With a significantly large portion of organization staff having migrated to remote work in 2020, cyber criminals sought to exploit the growth of internet use and home working during the Covid-19 pandemic according to research conducted by NETSCOUT. The cybersecurity company's ATLAS Security Engineering and Response Team (ASERT) revealed it observed over 10 million attacks of this nature in 2020, which is around 1.6 million higher than the previous year. Details revealed that attack frequency increased 20% throughout 2020, but with the exclusion of the pre-pandemic months including January through most of March, attack frequency grew by 22% year-on-year. Analysis of the information disclosed that healthcare and other essential sectors choosing to shift to a more digital workforce in response to the pandemic were heavily targeted by cyber criminals.

Motivations

Following a year riddled with attacks targeting organizations to disrupt and render enterprise operability useless, there has been a sizeable return in DDoS and RDoS activity. Adversaries have been observed targeting corporate networks with the intention to cause disruption and spread disinformation to undermine responses to the pandemic involving vaccine research, distribution, and treatment administration. Other motivations include the pursuit of financial gain as the rise in Bitcoin-to-USD prices, more than likely, encourage attackers of varying sizes to return or re-prioritize RDoS and DDoS extortion schemes. Oftentimes, this comes in the form of threat actor groups with sophisticated tools designed to disrupt or take down enterprise networks. These efforts are exacerbated by individuals acting as hacktivists or pranksters lacking the skills and time to invest in creating their own tools leveraging malicious services offered on the dark web to achieve similar objectives.

Observed Activity

Propensity to Change Objectives

With the ability to quickly change which sectors to target, based on newly discovered risks and vulnerabilities to exploit or motives influencing operations, cyber criminals have a host of different threat landscapes to attack. One historical example includes the targeting of banks in the finance sector in September 2012 and continued for nearly nine months in which a series of DDoS attacks was launched by Iranian nation-state backed threat actors. The cyberattacks hit nearly 50 US financial institutions in over 200 DDoS attacks, according to the US Department of Homeland Security (DHS). A Middle Eastern hacking group known as the Izz ad-Din al-Qassam Cyber Fighters claimed to be at the center of the attacks while US intelligence officials pointed at Iranian government-linked hacker groups.

Regardless of the origins of the executed disruptive attacks, numerous financial institutions including Bank of America, the New York Stock Exchange (NYSE), J.P. Morgan Chase, and others were specifically identified as targets. However, there was an abrupt stop of the attacks and those closely investigating the matter assessed it was due in large part to the Iranian presidential election. According to the analyses of data collected by Google, the attackers potentially shifted operations to focus domestically on gathering intelligence about groups and individuals supporting specific candidates. The influx of detected and disrupted email-based phishing campaigns aimed at compromising accounts of numerous Iranian users represents the agility of malicious operations influenced by the climate of current or emerging global events. Since then, these threat actors have fortified their arsenal and have established a high degree of surveillance and control. This has enabled them to quickly pivot between targets and re-prioritize objectives when exploiting vulnerabilities specific to any sector threat landscape.

Ransomware Gang DDoS Adoption

In an effort to encourage contact with the attacker, ransomware gangs have been observed adopting DDoS attack methods to increase the likelihood of receiving payment. As ransomware remains one of the biggest global cyber threats to healthcare, it is paramount that security personnel remain vigilant and aware of the tactics, techniques, and procedures operators will use to make a profit. Security researchers in October 2020, reported that ransomware gangs were beginning to utilize DDoS attacks against a victims' network or website as a supplemental tool to force them to pay a ransom. At the time, the two operations using this new tactic were SunCrypt and RagnarLocker. Increases to the current threat landscape provided ransomware gangs with new attack surfaces to attempt to exploit and implement crippling tactics to strongarm organizations to pay ransom demands.

With cyber criminals hoping to make the largest profit in the quickest amount of time, healthcare providers are likely targets. Recently joining the trend of using DDoS attacks to extort payment from victims is the Avaddon ransomware gang. Avaddon ransomware began operations in June 2020 after initiating spam campaigns that globally targeted users. The ransomware gang tried their hand in double extortion tactics when they sent a threatening ransom note to an undisclosed victim organization advising the organization had 240 hours to cooperate. Failure to do so would result in the exposure of its database, including personal data of customers and employees, as well as financial documents. According to the ransom note, the victim's website was under DDoS attack, which would not stop until Avaddon was contacted.

Third-Party Targeting

CloudFare Magic Transit

A new type of DDoS attack was previously identified by Cloudfare whose waves mimicked that of an acoustic beat. The acoustic beat-inspired attacks delivered a sustained wave-shaped DDoS pattern for at least eight hours. Codenamed "Beat," after a term coined in the acoustics world to signify the interference of two different wave frequencies, the attack launched a flood of packets whose rate was determined by an equation representing the two waves. The cybercriminal behind the attack that targeted a Magic Transit customer may have utilized the method they did in an attempt to overcome Cloudflare's DDoS protection systems.

Magic Transit protects entire IP subnets from DDoS attacks, while also accelerating network traffic as it uses Cloudflare's global network to mitigate attacks employing both BGP and GRE for routing and encapsulation. By using the unidirectional TCP state tracking machine, flowtrackd, the company was able to detect the attack as a flood of ACK packets that did not belong to any existing TCP connection and automatically dropped them. In total, the adversary's attack persisted for over 19 hours with an amplitude of 7 Mpps, a wavelength of 4 hours and a peak of 42 Mpps. During the two days in which the attack took place, Cloudflare systems automatically detected and mitigated over 700 DDoS attacks targeting the customer.

MobileIron Enterprise MDM

Mobile Device Management (MDM) systems are used inside enterprises to manage employees' mobile devices, by allowing system administrators to deploy certificates, applications, access-control lists, and wipe stolen devices remotely. One MDM in particular, MobileIron, was targeted by several threat actors after a security researcher informed the vendor about bugs which were patched in July 2020. Two of the three vulnerabilities, CVE-2020-15505 and CVE-2020-15506 were considered critical and had a 9.8 CVSSv3 score. The other vulnerability, CVE-2020-15507 received a rating of high and held a 7.5 CVSSv3 score. Exploitation of these CVEs would introduce security issues including remote code execution, authentication bypass, and arbitrary file reading respectively.

In September 2020, a detailed write-up about the vulnerabilities was released in which other researchers created proof-of-concept exploits that later became publicly available via GitHub. Some vendors did not take advantage of the grace period provided to patch vulnerable systems, leaving them exposed to the potential for exploitation by threat actors. This led to subsequent attacks in which the first wave took place at the beginning of October 2020, according to detections by RiskIQ researchers. One attack in particular, reported by security firm Black Arrow, involved a threat actor attempting to hack into MobileIron MDM systems and install the Kaiten DDoS malware. Other nefarious instances involved the exploitation of CVE-2020-15505 which the US National Security Agency (NSA) listed as one of the top 25 vulnerabilities exploited by Chinese state-sponsored hackers during that time. According to the NSA, Chinese threat actors were using the MobileIron vulnerability, in conjunction with others, to gain an initial foothold on internet-connected systems to pivot to internal networks. At the height of the vulnerabilities' disclosure, more than 20,000 organizations, including several Fortune 500 companies, used its MDM solutions according to MobileIron making it one of the most dangerous security flaws disclosed last year.

Takedown Campaigns

International task forces involving multiple law enforcement agencies, working in collaboration with private sector companies, have partnered to secure the successful dismantling of the botnets used by cyber criminals to launch malware and DDoS attacks. Two such recent examples are mentioned below.

Emotet

On January 27, 2021, after the two-year planning of a global law enforcement operation, the world's most prolific and dangerous malware botnet was taken down. Those involved included Europol, the FBI, the UK's National Crime Agency and others which resulted in investigators taking over infrastructure controlling Emotet. Machines that were infected by Emotet were directed to infrastructure controlled by law enforcement which put an end to cyber criminals exploiting compromised systems and the propagation of malware. At the height of its operations, Emotet was the cause of millions of dollars in damages experienced by state, local, tribal, and territorial governments.

Emotet first emerged as a banking trojan in 2014 and later evolved into one of the most powerful forms of malware used by cyber criminals. Emotet compromised Windows computer systems using backdoors via automated phishing emails that distributed malware-laden Word documents. Successful exploitation involved altering subjects of emails and documents to lure victims into opening them which led to the installation of the malware. Regular themes included invoices, shipping notices and information about the novel coronavirus pandemic. The investigation of Emotet also disclosed a database of stolen email addresses, usernames, and passwords which Europol worked with Computer Emergency Response Teams (CERTs) to aid those infected with Emotet.

Trickbot

On October 12, 2020, the collaborative efforts of Microsoft's Defender team, FS-ISAC, ESET, Lumen's Black Lotus Labs, NTT, and Broadcom's cyber-security division Symantec led to the takedown of the TrickBot botnet. Prior to the execution of the takedown, each participant conducted investigations into TrickBot's backend infrastructure of servers and malware modules. Microsoft, ESET, Symantec, and partners analyzed the content providing insight into the malware's inner workings including all the servers the botnet used to control infected computers and serve additional modules. Microsoft later took to legal proceedings as they provided the information, requesting control over TrickBot servers.

With the court's approval, Microsoft and partners were able to disable the IP addresses, render the content on command and control (C2) servers inaccessible, suspend all services to the botnet operators, and prevent residual efforts to purchase or lease additional servers. Around the time of TrickBot's takedown, operators had infected more than one million computers in which some of the compromised systems included IoT devices. On October 13, 2020, multiple sources reported that the TrickBot botnet survived the attempted takedown as operators quickly spun up new infrastructure. The perseverance displayed by TrickBot operators and the ability to quickly revive operations further solidifies the importance of exercising best security practices and remaining vigilant to secure critical infrastructure.

Risk and Impact

The increasing frequency, intensity, and scale of DDoS attacks poses a significant threat to the entire healthcare industry with a reach spanning across every healthcare subsector. All healthcare entities, Health-ISAC members included, face a multitude of potential risks caused by potentially crippling DDoS attacks. Below are a few prominent areas within the healthcare industry that are essential to the availability and support of patient-centered care. Each subsection serves to provide an overview of the negative impacts caused by the disruptive activity of DDoS attacks.

Healthcare Operations

Critical operations rely on the integrity and infallibility of services. Without these services, basic utilities would disrupt the intake, processing, and outgoing care of patients, suppliers, and employees. The disruption of essential healthcare operations by DDoS attacks can cause:

- **Loss of Life**: Disruption of essential care and supplies being delivered to vulnerable patients via a DDoS attack can potentially cause the worst outcome of a disruption of healthcare operations; loss of patient life. Patients being admitted to hospitals in critical condition and in need of immediate access to care or the safety and integrity of surgical procedures are matters highly considered to be at risk when considering potential impacts to HDO services.

- **Disruptions to Telemedicine:** With increases to telehealth in 2020 due to Covid-19 social distancing efforts, patients and clinicians are heavily relying on the support and protection of infrastructure that allows this method of long-distance communication. Disruptions to this remote service could be devastating to some populations that have benefited tremendously due to its quality, access, and more personalized delivery.

Patient-Centered Care & Reputation

The practice of patient-centered care is compartmentalized into different process functions to administer medical attention that is meaningful and valuable to both patients and their families. The process functions include assessment, diagnosis, planning, implementation, and evaluation. In all, the aforementioned process functions are critical to the quality of patient care and significantly impacts the reputation of healthcare providers in which adverse effects can lead to the following:

- **Reduced Efficiency:** The technological advances of today's time has increased the efficiencies of medical professionals all around the world as tasks have become more streamlined and automated. Digital medical systems including electronic medical records (EMRs), picture archiving and communication systems (PACs), remote patient monitoring systems, as well as infusion and insulin pumps are commonly used tools in healthcare environments. In the event of a sustained DDoS attack, the risks associated with losing access to systems is damaging from both an operational and financial standpoint.

  When systems become unavailable, employees are forced to implement manual processes to fulfill duties including checking patients' vital signs, administering dosages, or access to properly functioning imaging equipment are a few of the many areas that would be noticeably impacted. The time it would generally take an employee to complete daily tasks will increase, effecting staff's ability to administer care to others. In addition to the loss of these systems, organizations will have to address the financial impacts that come with the total cost of ownership (TCO) and recovery after downtime.

- **Loss of Credibility:** Healthcare entities, staff, and patients alike, all want to be certain that medical assistance is not only efficient, but consistently available to readily provide access to care. Failure to maintain medical equipment uptime is detrimental to the capability of providing care and ultimately effects the organization's reputation both internally and externally. Both prospective employees and patients, respectively, will refrain from seeking employment or medical assistance from organizations whose reputation has been soured from the inability to exhibit resilience against negative outside forces. Ultimately, organizations may be seen as unfit to provide the best care possible and experience a loss in human capital.

Critical Infrastructure

The systems and networks that make up the infrastructure for organizations provides the foundation that critical operations require. Disruptions to critical infrastructure can have dire consequences that span across the organization and can impact:

- **Access to Corporate Resources:** Due to the massive increase in the remote workforce, demands to ensure business continuity by providing remote users with access to essential corporate applications and services is at an all-time high. Now more than ever, a relatively minor DDoS attack could bring down a remote employee access / Virtual Private Network (VPN) gateway, preventing access to tools and systems necessary to employee job functions. Threat actors are aware organizations are more exposed while employees are working remotely especially as a result of the ongoing pandemic in 2020 and 2021. As a result, it is important that IT departments leverage tools necessary to maintaining load balancing best practices to avoid VPN gateways from being overwhelmed and unable to provide required access for remote workers.

Mitigation Strategies

Organizations are encouraged to formulate denial-of-service response plans that are predicated on resilience, incorporating key elements including system checklists, response teams, and efficient communication and escalation procedures. It is equally important to remain vigilant in securing network infrastructure and practicing basic network security for the purpose of establishing a standard that is recognized throughout the organization. In addition, organizations should consider force multiplying mitigation efforts by leveraging strategic relationships with entities such as ISACs, law enforcement initiatives, and governmental departments dedicated to the implementation of defense in depth controls.

The following network defense and operational / technical mitigation techniques were borrowed from a Financial Services ISAC publication, and provides a wealth of information relevant to the climate of today's threat landscape and the impacts of DDoS attacks. Each section details information regarding current network defense, strategic DDoS mitigation, and operational and technical DDoS mitigation techniques.

Current Network Defense Techniques

- Blackhole routing – Blackhole routing is a technique used as far upstream as possible by diverting and discarding malicious network traffic destined for a targeted organization.

- Sinkhole routing – Sinkhole routing is a means of diverting traffic to an unused area of the network. This can provide opportunity for monitoring and investigative analysis.

- Unicast Reverse Path Forwarding (uRPF) – This security feature works by enabling a router to verify the "reachability" of the source address in packets being forwarded. If the source IP address is not valid, the packet is discarded.

- Geographic Dispersion (Global Resources Anycast) – A newer solution for mitigating DDoS attacks dilutes attack effects by distributing the footprint of DDoS attacks so that the target(s) are not individually saturated by the volume of attack traffic. This solution uses a routing concept known as Anycast, which allows traffic from a source to be routed to various nodes (representing the same destination address) via the nearest hop/node in a group of potential transit points.

- Reputation-Based Blocking – Reputation-based blocking limits the impact of untrustworthy URLs by providing URL analysis incorporating world-wide threat telemetry, intelligence, and analytic modeling and a decision component which focuses on the reputation of a URL.

- Host-based Intrusion Detection System (IDS) – Intrusion Detection Systems are network devices that monitor, detect, and alert on malicious activities using signature or statistical anomaly based detection techniques.

- Intrusion Prevention System (IPS) – Intrusion Prevention Systems are network devices that monitor, detect, and prevent malicious activity using signature or statistical anomaly-based detection techniques. Signature based intrusion prevention systems rely on vendor threat signature updates which fail to keep up with the latest DDoS threats.

- ACLs and Firewall Rules – ACLs provide day zero or reactive mitigation for DDoS attacks, as well as a first-level mitigation for application-level attacks. An ACL is an ordered set of rules that filter traffic. Firewalls, routers, and even switches support ACLs.

- DNS – DNS-related information can be correlated with other forms of telemetry (NetFlow, packet capture, application logs) to further investigate potential malicious behavior in the network. For example, there may be a baseline level of DNS queries from certain sources and a spike or change can indicate potential malicious behavior in the network.

Strategic DDoS Mitigation Techniques

Organizations are advised to employ a top-down approach that incorporates DDoS as a critical attack vector as part of their strategic risk management program. Some key areas listed below will enable organizations to effectively and efficiently manage threats faced by DDoS attacks.

- Security Management Framework – Organization should implement a holistic threat management framework which includes DDoS specific controls to manage and protect against DDoS threats including a DDoS risk assessment and incident response plan.

- Build and Maintain a Cyber Resilience Infrastructure – Develop the ability to withstand disruptions to IT capabilities supporting critical business operations. Improve overall operational resilience to DDoS attacks, focusing on:
    - DNS caching solutions which allow for resolution of network addresses in the face of DNS failures and outages.
    - Surge-support/ high-capacity, cloud-based DDoS protection services allow you to quickly reroute or quarantine DDoS traffic.
    - Load-balanced/scalable front end web servers can help handle an initial onslaught of queries targeted at those environments.
    - Risk-sensing anti-DDoS appliances that support quick identification and diversion of web-based queries that may be part of DDoS attacks.
    - Modular and micro-segmented network infrastructure provides agility and limits impact to systems.

- Traffic Profiling – Develop a thorough understanding of your normal traffic patterns and usage. Develop a plan for triaging traffic and know in advance what traffic needs to be retained and what can be dropped during an attack.

- Third Party/Service Level Agreements – Organizations should ensure that technical, operational, and strategic provisions related to DDoS mitigation and recovery, such as Request for Technical Assistance (RTA) are implemented in service level agreements, third party vendors understand and are bound to them, and testing of the processes is conducted periodically.

- Staff Training – Organizations should ensure that staff responsible for mitigating DDoS attacks regularly receives technical and operational training on latest attack vectors, anti-DDoS technology, disaster recovery/incident response, and DDoS detection/escalation methods.

- Information/Intelligence Sharing – Organizations should participate in information and intelligence sharing initiatives between private organizations as well as the public sector. Early warning of potential attacks and lessons learned from post-incidents will help reduce the potential impact of DDoS threats.

- Develop Security Vendor Relationships – Organizations should develop and maintain relationships with security vendors (Anti-Virus, DDoS Mitigation, and Upstream Providers) that can effectively help with the detection and mitigation phase and provide information about the latest DDoS trends and malware research.

- Joint Cybersecurity Exercises – Organizations should participate in joint cybersecurity exercises and initiatives with DDoS mitigation vendors, Department of Homeland Security (DHS), Department and Human Services (DHS), and Health Information Sharing and Analysis Center (Health-ISAC) which will provide knowledge sharing and best practice capabilities against DDoS threats.

Operational and Technical DDoS Mitigation Techniques

Organizations need to employ a combination of operational and technical controls to successfully prevent, detect, and react against DDoS attacks.

Prevent

Preventive controls are countermeasure that organizations can implement that will protect against DDoS attacks. Below are operational and technical controls that organizations should implement.

Operational

The following operational controls should be considered to assist in preventing DDoS attacks.

- Asset Inventory – Organizations should maintain an asset inventory which will help identify critical assets that need to be prioritized for protection against DDoS attacks. Identify your critical assets and applications that are external facing. Know where applications are hosted, what controls are in place, and how they connect to the Internet and the internal network end-to-end.

- Business Continuity – Organizations should ensure DDoS is included as part of their business continuity plan and testing. DDoS should be included in tabletop exercises, simulations, technical recovery testing, tests of third party facilities/services, and complete full-scale tests. Mobile applications should be included in this testing. For resiliency purposes, know if you are sharing a network connection for both customer and employee use. If employees are sharing the same bandwidth or network equipment (including VLANs), then the operational team could be impacted or locked out from defending the network.

- Capacity Management – Planning for additional capacity will ensure critical infrastructure which includes applications, servers, systems, network devices, and bandwidth is/are capable of withstanding DDoS attacks. Consider the effectiveness and ramifications of over-provisioning bandwidth. Expanding bandwidth will move the fault line downstream to firewalls, routers and, ultimately, your web applications. These may or may not be able to handle increased loads.

- Change/Configuration Management – Change/configuration management programs will ensure changes are consistent, recorded, and controlled in accordance with information security policies.

- Risk Assessments/Penetration Testing – DDoS should be included in application and network penetration testing programs which will help identify problems such as traffic bottle necks and ensure that critical infrastructure can withstand traffic load and stress against it. Risk assessments will help prioritize DDoS mitigation efforts.

- Secure Application Design – Implement and follow secure software development lifecycle processes and best practices to ensure that applications are securely developed and, where critical, deployed to be continuously available.

- Secure Network Design – Implement and follow secure system/network development lifecycle processes and best practices. Ensure networks are segregated, single points of failure are treated with redundancy, and load balancing is implemented.

Technical

The following technical controls should be employed to prevent against DDoS attacks.

- Deploy Anti-DDoS Devices/Services – Deploy and manage vendor provided solutions which provide resiliency against DDoS attacks. Ensure DDoS mitigation functions are enabled and tested on all devices. Ensure thresholds are set appropriately based on intelligence about current attack methodologies.

- Layered Filtering – Employ egress/ingress filtering to prevent spoofing at multiple levels of the infrastructure which includes: routers, application/network firewalls, servers, and systems.

- Protocol and Port Filtering – Critically reexamine all protocols and ports that are incoming to your organization. If possible deny all UDP connections and allow only critical TCP ports.

- Connection Whitelisting – Consider building a connection whitelist as part of your business continuity plan so that in a DDoS or other contingency scenario you can block all traffic except that critically required for the functioning of your organization.

- Security Patch Management – Regular and timely management of security patches will protect the infrastructure against security vulnerabilities and infection of devices from malware based bots.

- Deploy Anti-Virus Software – Deploy anti-virus software and update virus signatures on a regular basis in the environment.

- System Hardening – Follow and apply best practice configurations to protect against DDoS attacks.

Detect

Detective controls will help identify and provide early warning indicators against DDoS threats. Below are detective operational and technical controls that organizations should consider implementing.

Operational

The following operational controls should be employed to detect DDoS attacks.

- Countermeasures – Review your countermeasures in the context of reported incidents and attempt to determine whether your countermeasures would have mitigated the identified attack against your environment.

- Develop Security Vendor Relationships – Organizations should develop relationships with security vendors that can effectively help with the detection phase and provide information about the latest DDoS trends and malware research.

- Information Sharing/Monitoring – Ensure threat awareness of ongoing DDoS threat activities through participation in information sharing and open source intelligence/monitoring.

- Baseline Activity – Know your baselines for log-ins, transactions, connections, and users, mindful of traditionally high volume transaction days. Increases or dips may be leading indicators. Provide analytics and tactics information to operational team and senior management.

Technical
The following technical controls should be employed to provide early detection of DDoS attacks.

- Deploy Intrusion Detection Systems – Deploying intrusion detection systems will provide another layer of detective controls and provide early warning indications in the event of DDoS attacks. Ensure DDoS related signatures for relevant attack types are deployed and functioning.

- Centralized Monitoring/Logging –DDoS alerting, logging, and reporting systems should be deployed which will provide consistent and responsive event analysis and correlation. Ensure your Managed Security Services provider (MSSP) is engaged and aware if there are active DDoS attacks that could be redirected to your organization. Revalidate reporting and escalation thresholds with the MSSP. Ensure there is a complete audit trail of activity for forensic analysis, including accurate timestamps, signatures, source/destination addresses, etc.

- Deploy Honeypot systems – Honeypot systems should be deployed which will provide the capability to identify and track botnet/malware activity.

- Deploy Sinkholes – Sinkholes should be deployed which provide the capability to reroute malicious attack traffic to a destination for analysis and intelligence purposes which can further assist in attribution. Ensure the sinkhole(s) are off network from primary connections to ensure the sinkhole itself does not contribute to the DDoS.

React
Reactive security controls may be deployed in the event of a DDoS attack.

Operational
The following operational controls can assist in responding to DDoS attacks.

- Collaboration and Communication Protocols – Large scale attacks affecting the institution may require enterprise level response and organizations should implement a hierarchical structure for large scale events. Establish multiple bridge lines to facilitate communications among and between the different technical teams, management reporting, and response coordination. Integrating your DDoS response plan into your corporate incident response and crisis management program will ensure all appropriate parties, such as Enterprise Risk and Fraud, are engaged.

- Channel and Press Communications – Organizations should engage channel leads and public relations teams to develop call center and press messaging and materials. Prepare for this by developing an incident notification and communications strategy for both internal communications, including one for senior management, and external communications, including key service providers, customers, and the media.

- DDoS Response Annex to the Incident Response Plan – Organizations should develop specific processes for DDoS response under the corporate incident response plan. Ensure roles and responsibilities are clearly defined to minimize the decision makers and the approval process for managing the response effort. Organizations should obtain pre- approvals for invoking the mitigation service so as not to delay invocation once the attack starts.

- Establish Service Provider relationship – Organizations should establish and maintain relationships with upstream ISPs and DDoS mitigation providers. In the event of a sustained DDoS attack, service providers can be beneficial in helping prevent system/service downtime. Work with your ISPs and your DDoS mitigation provider to establish a protocol to share information during an attack. Great ISP information sharing will help to reduce the need to coordinate or mediate the sharing of bad IP addresses among ISPs.

- Limit non-critical activities – Consider halting non-critical scanning activity as well as non-essential applications, maintaining only those critical to the survival of your customer-facing applications. This approach will help to eliminate uncertainty and reduce “noise” during the attack.

- Social Media Monitoring – Monitor Twitter and other media sources to identify customers continuing to report outages. This can be especially helpful after the attack has stopped to identify legitimate customers being erroneously blocked.

- Information Sharing – Consider working with other HDOs that are experiencing or have experienced a DDoS attack by sharing actionable attack information directly with those organizations and through the Health-ISAC. You are obligated to inform your primary regulator of any DDOS attacks.

Technical
The following technical controls may assist in mitigating DDoS attacks.

Primary technical tools used to mitigate DDoS attacks are:

- Loading scripts onto load balancers to filter malicious traffic
- Web Application Firewalls
- Third party BGP-based scrubbing
- Third party DNS-based scrubbing
- Network blocks based on Layer 3 or 4 characteristics
- Upstream Filtering
- Connection rate limiting
- Blackhole and sinkhole routing
- Packet/Session Time-to-Live (TTL) Restrictions
- Protocol/Port Filtering

Correct
Corrective security controls are countermeasures that organizations can implement to limit the extent of the damage caused by DDoS attacks and prevent similar attacks from recurring.

Operational
The following operational controls should be employed to prevent against DDoS attacks.

- Attribution – Organizations should engage their law enforcement partners and work with them during DDoS botnet takedown missions which will increase understanding of adversary TTPS and aid in prevention of future attacks.

- Lessons learned – Organizations should prepare a detailed post-incident report and discuss lessons learned and update incident response plans as necessary.

Conclusion

With the proliferation of IoT devices, advancements in technology, demand for access to sophisticated systems, and historical trends, DDoS attacks will expectedly grow in volume and frequency. Cyber criminals are expected to continue to seek and exploit vulnerabilities within these systems in an attempt to weaponize them for DDoS and RDoS campaigns. Plans to implement 5G capabilities coupled with recent and ongoing shifts to digitization by organizations has provided new grounds for intrusion by threat actors.

It is imperative organizations remain vigilant in securing critical infrastructure by monitoring pre-existing and new technologies, ensuring new policies are being followed, and adhering to security best practices for managing enterprise networks and remote workforces.

References

CISA: Security Tip (ST04-015)
SANS Institute: Information Security Reading Room – Preparing to Withstand a DDoS Attack
Security Magazine: How DDoS Activity Has Evolved this Year
InfoSecurity Magazine: DDoS Attacks Surge in 2020 Due to #COVID19
Acoustic Beat-Inspired DDoS Attack
Another Ransomware Now Using DDoS Attacks, Forcing Payment
MobileIron MDM System Targeting
Taking Down Emotet
Operation Ababil
Krebs on Security: Iranian Elections Bring Lull in Bank Attacks
Microsoft and Others Orchestrate Takedown of Trickbot Botnet
Trickbot Legal Documents
TrickBot Botnet Survives Takedown Attempt
NCBI Resources: Nursing Process
Security Magazine: Protecting VPNs from DDoS Attacks in the Age of Remote Work
The Business Journals: Are Remote Workers Protected Against Hackers?

Feedback and suggestions on this document are encouraged and welcome.
Please email contact@h-isac.org