July 27, 2017

VIA EMAIL: counter_botnet_RFC@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Comment of Arbor Networks

Arbor Networks ("Arbor") submits this comment in response to the Request for Comments ("RFC") issued by the National Telecommunications and Information Administration ("NTIA") on June 13, 2017.[1] The RFC sought input regarding the steps that can be taken to improve industry's ability to defend against attacks using botnets and the role the federal government should play in addressing the increasing threat posed by botnets. Arbor appreciates the opportunity to participate in this critically important conversation. Arbor supports the development of voluntary industry-developed standards to protect against distributed denial of service ("DDoS") and other attacks launched using botnets, and believes that the Department of Commerce ("the Department") should facilitate this effort by bringing together interested industry and government representatives to develop these standards. Appendix A, attached, contains Arbor's views on current best practices for DDoS attack mitigation and end-point security.

Arbor provides network security and DDoS solutions to more than 1,200 customers in 107 countries, including 90% of tier 1 internet service providers ("ISPs") and three of the five largest online retailers.[2] The tools that Arbor provides to its customers give them a detailed view of their own networks along with information about global internet traffic and emerging threats. Arbor supports the Department's efforts to convene industry representatives with the aim of identifying best practices to protect against attacks launched using botnets. Arbor believes that the development of best practices and standards will encourage more companies, including startups and smaller companies, to implement stronger cybersecurity protections against such attacks.

As one of the top providers of DDoS protection products, Arbor has a unique insight into the growing threat to the online economy from DDoS attacks launched using botnets. In just the last year, Arbor has seen a marked increase in the frequency, scale, and complexity of DDoS attacks.[3] According to survey data, the percentage of companies experiencing between 11 and 50 DDoS attacks per month has increased from 22% to 36% between 2015 and 2016.[4] The percentage of companies experiencing more than 50 DDoS attacks per month has also grown from 8% to 21% during the same period.[5] As you can see from the chart below, the size of reported DDoS attacks

[1] 82 Fed. Reg. 27042 (June 13, 2017) (Docket No. 170602536-7536-01).

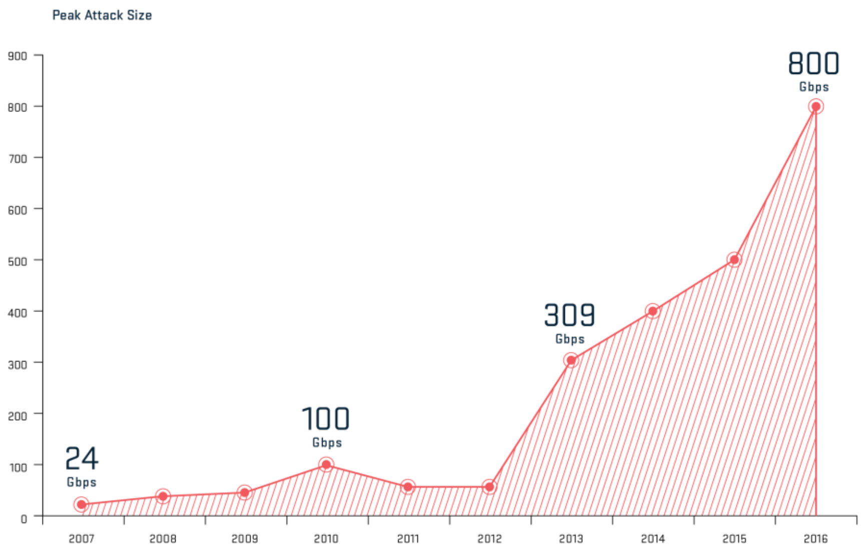
[2] Information about the types of customers to whom Arbor provides products and services is available on its website at https://www.arbornetworks.com.

[3] Arbor Networks, *Worldwide Infrastructure Security Report* 21 (2017).

[4] *Id.* at 46.

[5] *Id.*

has also increased significantly with the largest reported attack reaching 800 Gbps, which represents a 60% increase over the prior year.[6]



Source: Arbor Networks, Inc.

These attacks have also increased in their complexity, with 67% of service providers reporting multi-vector attacks on their networks.[7] This number represents an 11% increase over the last year.[8] As you can see from the list below, the targets of these attacks are at a varied array of organizations. Arbor believes that the increasing threat presented by DDoS attacks is the result of significant growth in the Internet of Things ("IoT") market combined with decreasing barriers to launching a DDoS attack.

[6] *Id.* at 10.
[7] *Id.* at 11.
[8] *Id.*

Attack Target Customer Verticals

69%	End-User/Subscriber
48%	Government
41%	Financial Services
40%	Hosting
36%	eCommerce
35%	Gaming
31%	Education
13%	Law Enforcement
10%	Healthcare
10%	Energy/Utilities
9%	Gambling
7%	Manufacturing
7%	Other

Source: Arbor Networks, Inc.

The threat presented by botnets is growing more urgent and more complex as the number of IoT devices increases. Mitigating this threat will require the participation and cooperation of private and public entities across a number of industry sectors. Arbor believes that the Department is well positioned to bring these entities together to identify a voluntary and flexible set of standards that companies can follow to improve their ability to defend against botnets. Arbor recognizes that the National Institute of Standards and Technology ("NIST") and NTIA have already begun work with respect to both the disclosure of vulnerabilities and updating or upgrading IoT devices and with NIST's July 11 and 12 workshop on Enhancing Resilience of the Internet and Communications Ecosystem.[9]

I. The Department should encourage adoption of the DDoS Threat Profile under the NIST Cybersecurity Framework.

The Department's work to promote the adoption of NIST's Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") has been instrumental in improving cyber readiness. The Framework reflects voluntary, industry-led standards, guidelines, and best practices that help companies make risk-informed decisions about the security measures they integrate into their devices. Arbor was pleased to work with AT&T and Cisco, along with

[9] *See* NTIA, *Multistakeholder Process: Cybersecurity Vulnerabilities*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities; NTIA, *Multistakeholder Process: Internet of Things (IoT) Security Upgradability and Patching*, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

other members of the Coalition for Cybersecurity Policy and Law, to create a "threat profile" for DDoS under the Framework. This profile offers organizations the ability to prioritize and measure their readiness for a DDoS attack utilizing the existing framework core. See Appendix B for the latest version of the DDoS Profile.

II. The Department should facilitate establishing greater action to alert and help users when their devices may be part of a botnet.

One of the reasons that botnet operators have increasingly targeted IoT devices is that the users of these devices frequently have less interaction with the device itself. Such devices may have limited user interfaces, may be difficult to access, and there may be few, if any, indications to a user that a device is part of a botnet. As a result, users typically do not realize that their devices have been compromised and do not take steps to remove malware or otherwise secure the device. Providing users with notice that their devices may be part of a botnet may help them take steps to protect and secure their own devices. However, it is important that such notice be provided in a context in which users will understand the notice and include sufficient information for users to take appropriate action. Providing this context and level of detail is particularly challenging given the diversity of the IoT market, which makes the multistakeholder process particularly appropriate to identify workable solutions to these challenges.

The Department can facilitate this effort by identifying the companies most likely to obtain evidence that users' devices are part of a botnet and bringing them together to discuss best practices for notifying users. In light of the substantial variation in the information available to different types of companies and their differing relationships with their customers, such notice should remain voluntary. However, the creation of reasonable guidelines for providing such notice could encourage more companies to notify users of devices that may be compromised, enabling those users to take appropriate action.

III. Conclusion

Arbor thanks the NTIA for the opportunity to provide this comment. We look forward to engaging with the NTIA throughout this process and participating in discussions about measures that should be taken to protect against and dismantle botnets.

Sincerely,

Arabella Hallawell
Arbor Networks

Appendix A

In this appendix, Arbor sets out its views regarding best practices for DDoS attack prevention, detection, and mitigation strategies and measures that end users and companies should consider. We believe that broad adoption of the best practices set out below, along with increased industry and government collaboration, will help mitigate the impact of DDoS attacks and slow the growth of the botnets used to launch these attacks.

Network operators of all types should work with peers and relevant organizations such as Internet Engineering Task Force ("IETF"), North American Network Operators Group ("NANOG"), industry vertical information sharing and analysis centers ("ISACs"), the Messaging, Malware, and Mobile Anti-Abuse Working Group ("M^{3}AAWG"), and others to share information and coordinate strategies for dealing with the threat of botnets.

In addition, we believe that most end users are unaware of the nature, capabilities, and potential threats posed by IoT devices. Broad and sustained education programs targeting the end-user community can raise awareness and facilitate best practice adoption.

I. Identify: Threat Intelligence

Defensive capabilities should be designed and configured based on observed trends in DDoS activity from direct and indirect network traffic analysis. Arbor Networks' Annual Report, released in Jan 2017, shows massive increases in the size and volume of large DDoS attacks. Further, the report illustrates the proliferation of complex, multi-vector attacks and the continued increase in average attack size.

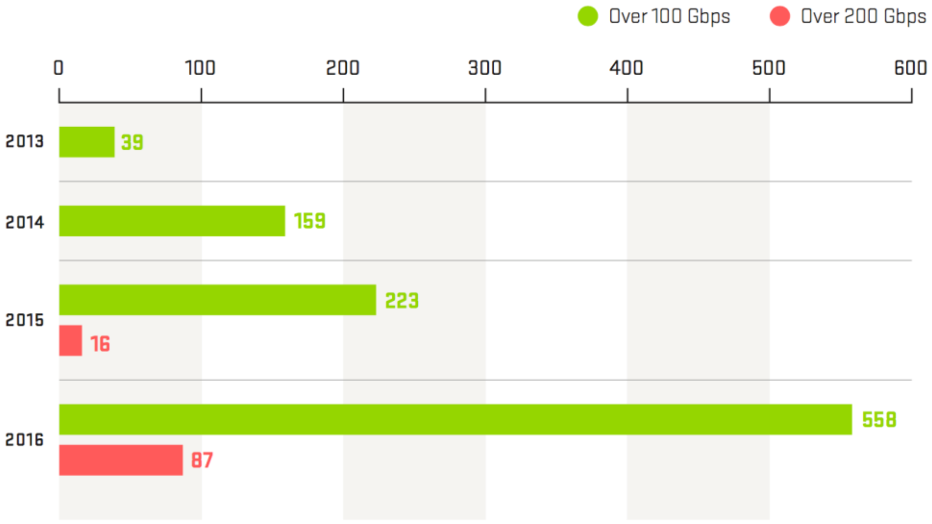
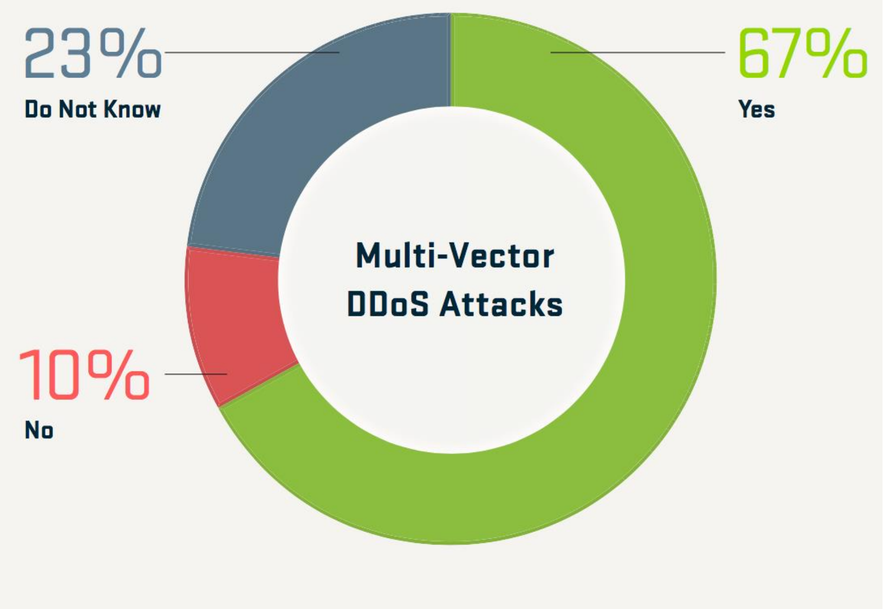


Figure AT2 *Growth in Large Attacks Year Over Year*

The proportion of ISPs seeing complex, multi-vector attacks on their network has also increased from just under a third in 2014, to just over a half in 2015, to just over two thirds in 2016.



Companies should use the threat intelligence that is available to them through both threat reports and real attack data to guide their DDoS defense strategy. Companies should identify data and guidance appropriate to their industry, country, region, and vertical.

II. Protect

Botnets can amplify the amount of traffic they can generate during DDoS attacks by using techniques such as reflection amplification. Reflection amplification involves an attacking device sending UDP queries to a service such as NTP, DNS, Chargen, etc. to illicit a large response packet. If the attacking device spoofs the source address of generated queries to be that of the victim, then the "amplified" traffic is delivered to the target of the attack by servers owned by innocent third parties. This mechanism can be used to maximize the traffic generated by a given botnet while obfuscating the original source IP addresses of the traffic and has been behind some of the largest DDoS attacks seen on the internet in recent years. BCP 38 and BCP 84 can be used to filter spoofed traffic at ISP boundaries, but unfortunately these capabilities have not been globally adopted.

Companies should be encouraged to use best-practice, layered DDoS defenses for critical infrastructure and services. DDoS is a well understood threat, and the correct defenses and appropriate ISP cooperation can successfully protect critical infrastructure from this threat.

A. Multi-Layer Approach.

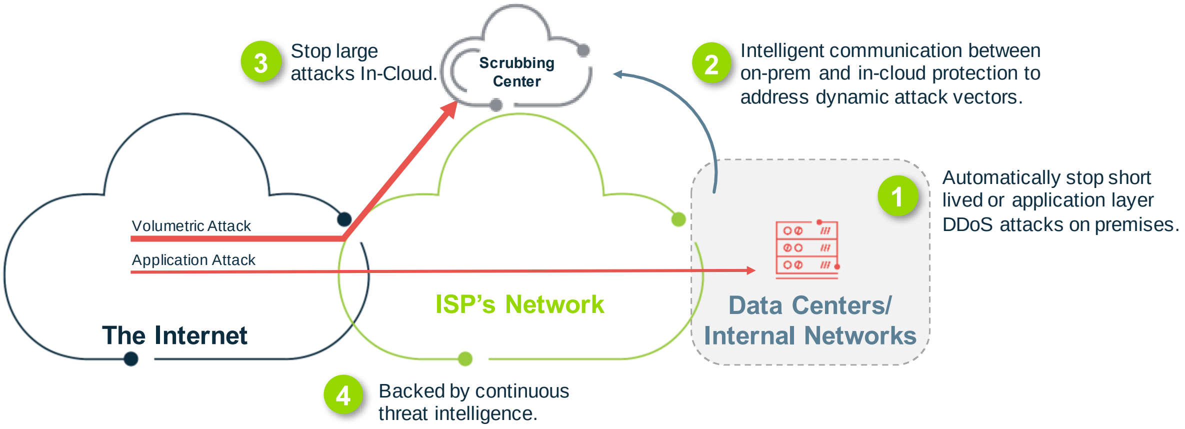
Industry best practice for DDoS protection is a multi-layer, or hybrid, approach that takes into account the different types and targets of DDoS attacks. High-volume flood attacks that target internet connectivity must be mitigated in the ISP network or cloud, away from the intended target before they overwhelm local network connectivity. Application-layer and state-exhaustion attacks need to be detected and mitigated on premise, close to where the applications or services reside, so attack traffic is mitigated quickly before there is a (lasting) service impact. While it is generally possible to perform application-layer attack mitigation in ISP network or cloud infrastructure, detection can be more of a problem due to the limited visibility network operators have of traffic at layer-7. There are solutions to this problem, without using a layered-protection approach, but these have two shortcomings:

It can be necessary to permanently forward traffic through a scrubbing center for application-layer inspection.

There can be a lack of full control and reporting when using cloud-based mitigation, which is especially important when organizations launch new applications or modify existing ones.

A multi-layer DDoS protection approach, with intelligent communication between layers, helps companies protect against complex DDoS attacks.

Layered, Automated, DDoS Attack Protection



3
Stop large attacks In-Cloud.
Scrubbing Center
2
Intelligent communication between on-prem and in-cloud protection to address dynamic attack vectors.
1
Automatically stop short lived or application layer DDoS attacks on premises.
Volumetric Attack
Application Attack
The Internet
ISP's Network
Data Centers/ Internal Networks
4
Backed by continuous threat intelligence.

B. Endpoint Prevention

Companies should consider appropriate controls to prevent botnet attacks. Basic network, service, and appliance hygiene – if used – could prevent a significant proportion of infections. For example, companies should:

- Secure access by changing default usernames/passwords.
- Update and patch operating systems and applications.
- Engage in outbound filtering of IoT and other host devices, allowing only devices that need internet access to have internet access.
- Not give administrator privileges to end users.
- Not allow creation of local accounts (only domain accounts) whenever possible.
- Require the use of mobile device management software or similar company-managed security enforcements on all mobile devices.
- Block access to all non-approved email systems (e.g., Hotmail, Yahoo)
- Block access to all non-approved offsite file sharing (e.g., Dropbox, Google drive)
- Implement network segmentation and quarantine capabilities.
- Engage in network monitoring of packets and/or flows to understand what is normal and what is a change from normal.

Companies should also make security a key part of the evaluation criteria for all infrastructure and applications procured, including by taking embedded operating systems, IoT, etc. into account. Commercial pressure forcing reasonable and appropriate security measures may encourage or produce increased security controls and measures that will complement regulations and/or standards regarding securing IoT devices, SaaS, Cloud, etc.

III. Detect

Companies should consider whether to use embedded router / switch capabilities to rapidly identify attacks and attack patterns using built-in telemetry technologies that give broad visibility of network activity. To date, Netflow (or one of its variants) provides a much-adopted and used technology for export telemetry.

IV. Respond: DDoS Attack Mitigation

A. Blocking Attack Traffic.

Many mechanisms exist to block DDoS account traffic. Companies should consider these approaches and apply the security control appropriate to their environment. Companies can consider the use of an embedded router / switch capabilities to block attack traffic. Access Control Lists ("ACLs") can be configured to drop well-known illegitimate traffic, such as traffic to / from bogon addresses, and traffic matching known attack signatures (at layer 3.4), e.g., NTP reflection amplification traffic. Companies using this mechanism should understand that filters must be configured on routers / switches, which can be a barrier to their use during an attack due to the operational overhead and risk (if appropriate filters are not already in place).

A Source- or Destination-based remote triggered blackhole can also be used to drop all traffic from / to a given prefix. The advantage of this mechanism is that it can be easily used during an attack if the appropriate routing configuration is in place. However, it can be considered a blunt instrument, as all traffic from / to a prefix is discarded.

Border Gateway Protocol ("BGP") Flowspec (RFC5575) can also be used. This combines the specificity of the ACL with the ease of use of BGP blackhole, as layer 3/4 filters can be announced over multi-protocol BGP so that matching traffic (on routers that install the route) can be dropped, rate-limited, redirected etc. BGP FlowSpec has some limitations and concerns regarding stability and functionality of major FlowSpec implementations, but has the major advantage of using BGP as the "transport" protocol. Companies with concerns on this approach should track FlowSpec adoption and consider using it.

Currently, no automated inter-provider coordination for blocking malicious traffic has been broadly adopted. Where this is in place, it exists as an agreement between specific organizations and their operational security staff. Partially this is due to the absence of a standardized and widely adopted way to exchange DDoS data and, more generally, botnet intelligence between organizations. The DDoS Open Threat Signaling Working Group (DOTS WG) in the Internet Engineering Task Force (IETF) addresses this gap, developing the technology to exchange DDoS-related information; however, standardization and adoption is still a few years away. The DOTS WG also has a set of draft standards for a communication technology allowing multiple defensive solutions to work together to deal with a DDoS attack.

B. Governance and Collaboration.

Collaboration across all sectors is essential to identifying and remediating infected host computers or devices. Industry vertical Information Sharing and Analysis Centers such as the FS-ISAC have proven very effective at sharing threat intelligence and best practices for defense and mitigation of attacks.

DDoS peering could be an effective and efficient method for mitigation by leveraging more distributed resources and stopping attack traffic closer to the source. Network operators would notify each other of attack traffic to be mitigated that is either originating from or traversing their networks. Much like transit peering, the volume of mitigated traffic would be measured and accounted for reconciliation at regular intervals so that imbalances could then be restituted by financial agreements.

Cybersecurity Framework DDoS Profile

Executive Summary

The Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) version 1.0, developed by the National Institute of Standards and Technology (NIST), with extensive private sector input, provides a risk-based and flexible approach to managing cybersecurity risk that incorporates industry standards and best practices. The Cybersecurity Framework is by design crafted to allow individual organizations to determine their own unique risks, tolerances, threats and vulnerabilities, so that they may prioritize their resources to maximize effectiveness.

The Framework is general in nature to allow for broad applicability to a variety of industries, organizations, risk tolerances and regulatory environments. A Framework Profile is the application of Framework components to a specific situation. A Profile may be customized to suit specific implementation scenarios by applying the Framework Category and Sub-Categories appropriate to the situation. Profiles should be constructed to take into account the organization's:

- Business/mission objectives
- Regulatory requirements
- Operating environment

Organizations can use Profiles to define a desired state for their Cybersecurity posture based on their business objectives, and use it to measure progress towards achieving this state. It provides organizations with the ability to analyze cost, effort and risk for a particular objective. Profiles may also be used by industry sectors to document best practices for protection against specific threats.

The below Cybersecurity Framework Profile focuses on Distributed Denial of Service (DDoS). DDoS attacks are increasing in complexity, size, and frequency, and the range of targets and methods (e.g., from using individual PCs to using connected Internet of Things (IoT) devices) has also broadened. This threat profile emphasizes how the Cybersecurity Framework can address DDoS attacks, which NIST has acknowledged is a growing risk.

To develop the threat profile, we have reviewed all the Cybersecurity Framework Categories and Subcategories and determined those most important to combat the DDoS threat. The Categories and Sub-Categories were then labeled into different priorities as follows:

P1 – Minimum actions required to protect network and services against DDoS attacks

P2 – Highly recommended actions to protect network and services against DDoS attacks

P3 – Recommended actions to protect network and services against DDoS attacks.

The DDoS threat mitigation profile represents a Target Profile focused on the desired state of organizational cybersecurity to mitigate DDoS attacks. It may be used to assist in identifying opportunities for improving DDoS threat mitigation and aiding in cybersecurity prioritization by comparing current state with this desired Target state.

In the development of this profile we did not identify the need for any additions or changes at the Category or Subcategory level. Instead, the comments provided as part of the profile give the necessary guidance to refine the understanding of the Subcategory as it applies to DDoS threat mitigation.

Overview of the DDoS Threat

A DDoS attack attempts to overwhelm a network, service or application with traffic from multiple sources. There are many methods for carrying out DDoS attacks. These can include

- Low bandwidth connection oriented attacks designed to initiate and keep many connections open on the victim exhausting its available resources.
- High bandwidth volumetric attacks that exhaust available network or resource bandwidth.
- Protocol oriented attacks that take advantages of stateful network protocols such as TCP.
- Application layer attacks designed to overwhelm some aspect of an application or service.

Although each of these methods can be highly effective, in recent years, there has been considerable attention given to volumetric attacks as the result of several high-profile incidents.

One prominent example of a volumetric DDoS attack vector is reflection amplification. This is a type of DDoS attack in which the attacker fakes the attack target's IP address and launches queries from this address to open services on the Internet to solicit a response. The services used in this methodology are typically selected such that the size of the response to the initial query is many times (x100s) larger than the query itself. The response is returned to the real owner of the faked IP. This attack vector allows attackers to generate huge volumes of attack traffic, while making it difficult for the target to determine the original sources of the attack traffic. Reflection amplification has been responsible for some of the largest DDoS attacks seen on the Internet through the last decade.

Attackers can build out their attack capability in many ways, such as the use of malware to infect Internet connected computers, deploying servers within hosting environments, exploiting program flaws or other vulnerabilities, and by exploiting the use of inadequate access controls on Internet connected devices to create botnets.

Botnets are created when an attacker infects or acquires a network of hosts, then controls these devices to remotely launch an attack at a given target. Increasingly, botnets are incorporating Internet of Things (IoT) devices, which continue to proliferate at a remarkable rate. Botnets allow for a wide variety of attack methods aimed at evading or overwhelming defenses.

DDoS is often referred to as a 'weaponized' threat as technical skills are no longer needed to launch an attack and services to conduct DDoS have proliferated and become easily obtainable for relatively low cost.

Availability is a core information security pillar but the operational responsibility and discipline for assessing and mitigating availability-based threats such as DDoS often falls to network operations or application owners in addition to Risk and Information Security teams. Because of this divided responsibility, fissures in both risk assessment and operational procedures for addressing these threats may occur. The goal of this profile is to ensure the strategic and operational discipline needed to protect and respond to DDoS threats is comprehensively addressed by applying the appropriate recommendations and best practices outlined in the Cybersecurity Framework.

DDoS Threat Mitigation Profile

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
Identify (ID)	**Asset Management (ID.AM)**	**ID.AM-1:** Inventory physical devices and systems within the organization	**P2**	Catalog critical Internet facing services by location and capacity Catalog ISP connectivity by ISP, bandwidth usage, bandwidth available
		ID.AM-2: Inventory software platforms and applications within the organization	**P1**	Determine critical Internet facing services by type of application/service, IP address and hostname

Function	Category	Sub-Category	Priority	Framework Comment
		ID.AM-3: Map organizational communication and data flows	**P2**	Identify key stakeholders in the organization critical to availability of Internet facing services including application owners, security personnel, network operations personnel, executive leadership, legal/risk personnel and ISP or Cloud based DDoS mitigation service providers Maintain network maps showing data flows Create an operational process document detailing communication workflows
		ID.AM-4: Catalogue external information systems	**P3**	Identify applications and services that are run in cloud, SaaS, hosting or other external environments
		ID.AM-5: Resources are prioritized based on their classification, criticality, and business value	**P2**	Determine what Internet facing services will result in the most business impact if they were to become unavailable
	Business Environment (IDE.BE)	**ID.BE-4:** Establish dependencies and critical functions for delivery of critical services	**P2**	Catalog external dependencies for services and applications including DNS, NTP, cloud/hosting provider, partner network connections and Internet availability
		ID.BE-5: Establish resilience requirements to support delivery of critical services	**P3**	Ensure geographical redundancy and high availability of equipment providing services, network infrastructure and Internet connections

Function	Category	Sub-Category	Priority	Framework Comment
	Risk Assessment (ID.RA)	**ID.RA-1:** Identify and document asset vulnerabilities	P2	Determine network and application bottlenecks including throughput, connection rate and total connections supported
		ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources	P3	Monitor vulnerabilities lists (CVE, NVD and similar) to check if critical Internet facing services have vulnerabilities that could be used as a condition for Denial of Service.
		ID.RA-3: Identify and document internal and external threats	P3	Continuously gather industry information around DDoS trends, peak attack sizes, frequency, targeted verticals, motivations and attack characteristics
		ID.RA-4: Identify potential business impacts and likelihoods	P2	Create a risk profile that quantifies potential cost of recovery operations per DDoS incident, revenue loss, customer churn, brand damage and impact to business operations
	Governance (ID.GV)	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	P1	Put processes in place to ensure all regulatory requirements are met. Train all personnel responsible for DDoS incident response on the relevant legal and regulatory requirements surrounding the data that they may handle. Document regulatory and data privacy policies of DDoS service providers and partners

Function	Category	Sub-Category	Priority	Framework Comment
Protect (PR)	**Awareness and Training (PR.AT)**	**PR.AT-2:** Privileged users understand roles & responsibilities	P1	Security Operations personnel have been trained on DDoS defense processes, products and services Equip security operations personnel with an operational run book defining what process to follow and who to contact should an incident take place
	Information Protection Processes and Procedures (PR.IP)	**PR.IP-1:** Create and maintain a baseline configuration of information technology/industrial control systems	P1	Create a baseline DDoS protection architecture consisting of best current practices for the network, network based protection capabilities and non-stateful Intelligent DDoS Mitigation capability Implement anti-spoofing and black/white list filtering at network edge Maintain DDoS protection configuration that provides general protection for all services and always on protection for all business-critical assets
		PR.IP-7: Continuously improve protection processes	P2	Conduct a minimum of 2 annual tests of DDoS protection capabilities Perform after-action reviews following all DDoS incidents and DDoS protection tests adjusting DDoS defenses accordingly

Function	Category	Sub-Category	Priority	Framework Comment
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	P3	The organization's Business Continuity and Disaster Recovery plans should have components to address the potential effects of a DDoS attack
		PR.IP-10: Response and recovery plans are tested	P3	The DDoS components of the Business Continuity and Disaster Recovery plans should be tested.
		PR.IP-12: A vulnerability management plan is developed and implemented	P3	Vulnerabilities that can be leveraged for DDoS events should be documented and remediated.
	Protective Technologies (PR.PT)	**PR.PT-4:** Protect communications and control networks	P1	Perform filtering of traffic to control plane network and/or control plane traffic policing
Detect (DE)	**Anomalies and Events (DE.AE)**	**DE.AE-1:** Establish and manage a baseline of network operations and expected data flows for users and systems	P1	Continuously measure traffic to hosts, resources or groups of resources to determine expected traffic over time. Determine traffic baselines for IP protocols such as TCP, UDP, ICMP, GRE and critical applications such as HTTP, DNS, NTP, SSDPand SIP
		DE.AE-2: Analyze detected events to understand attack targets and methods	P1	Determine source and destination traffic characteristics when anomalous traffic is

Function	Category	Sub-Category	Priority	Framework Comment
				detected that is indicative of DDoS
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	P2	Aggregate data for detected DDoS events from multiple network sources contributing to the attack.
		DE.AE-4: Impact of events is determined	P2	Total traffic rates for DDoS events can be measured across all contributing network sources Performance and availability of services can be measured before, during and after events
		DE.AE-5: Incident alert thresholds are established	P1	Configure notifications to security monitoring personnel and appropriate stakeholders when traffic exceeds measured or configured thresholds
	Security Continuous Monitoring (DE.CM)	**DE.CM-1:** Monitor network to detect potential cybersecurity events	P1	Continuously measure traffic intoall network ingress points and between transit points on the internal network for traffic anomalies To the extent possible and/or practical from a business perspective, continually measure outbound traffic for detection of traffic anomalies that could represent sources contributing to outbound or cross-bound DDoS attacks.

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
		DE.CM-8: Vulnerability scans are performed	P1	Scan Internet facing services to identify vulnerabilities that can be exploited for participation in DDoS events.
	Detection Processes (DE.DP)	**DE.DP-3:** Test detection processes	P2	Conduct regular testing of DDoS defense capabilities including occasional unannounced tests performed with no prior warning to assess the DDoS defense strategies and processes Conduct DDoS simulation wargames as part of security staff onboarding and periodically for the security response team
		DE.DP-5: Continuously improve detection processes	P2	Perform after-action review on any defense testing or DDoS events after all operations are successfully restored to identify and improve DDoS detection capabilities Identify and maintain key security metrics around detection, identification and escalation effectiveness.
Respond (RS)	**Response Planning (RS.RP)**	**RS.RP-1:** Execute response plan during or after an event	P1	Follow DDoS response run book during any detected DDoS events
	Communications (RS.CO)	**RS.CO-1:** Ensure personnel know their roles and order of operations when a response is needed	P1	Define personnel responsible for detection, mitigation, coordination and communication during DDoS incidents

Function	Category	Sub-Category	Priority	Framework Comment
🟥		**RS.CO-4:** Coordinate with stakeholders consistently with response plans	P1	Document operational run book that includes roles, responsibilities and escalation process for all parties responsible for DDoS incident response including internal personnel and external consultants or services
		RS.CO-5: Engage in voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness	P3	Share and receive DDoS attack trends with consultants, service companies and/or threat intel companies to keep abreast of attack scale, frequency, motivations and evolving attack vectors
	Analysis (RS.AN)	**RS.AN-1:** Investigate notifications from detection systems	P1	Add DDoS alert notifications to monitoring and response systems including security and network operations management systems.
		RS.AN-2: Understand the impact of the incident	P2	Compare DDoS traffic rates, connection rates and total connections against documented system and network limits Identify actual and potential impact to business services, customers, employees and other stakeholders.
		RS.AN-3: Forensics are performed	P3	Save raw anomaly details in available form (logs, packet captures, flow telemetry data) to investigate parties involved in the incident and, where appropriate, to share incident details

Function	Category	Sub-Category	Priority	Framework Comment
				with the operational security community.
	Mitigation (RS.MI)	**RS.MI-2:** Mitigate incidents	P1	Mitigate DDoS attacks using any or all of the following: - Network capabilities such as ACLs, anti-spoofing, remote triggered blackhole and/or flow spec - Using intelligent DDoS mitigation systems on premise - Contracting a DDoS mitigation service Critical resources should be protected by always on mitigation capabilities - Contract or coordinate with upstream bandwidth provider for defense against high-magnitude attacks. Implement a notification system to detect when on premise bandwidth is reaching saturation then alert and/or automate movement of traffic to an upstream DDoS mitigation service Identify and maintain key security metrics around mitigation and escalation effectiveness.

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
	Improvements (RS.IM)	**RS.IM-1:** Incorporate lessons learned into response plans	P2	Adjust mitigation processes, capacity, technology and partnerships based on DDoS attack trends, DDoS response testing and results of DDoS after-action reviews Maintain key security metrics around the DDoS program to demonstrate program improvement and effectiveness.
Recover (RC)	**Recovery Planning (RC.RP)**	**RC.RP-1:** Execute recovery plan during or after an event	P2	Establish an internal and external communication plan as part of the DDoS run book that is used every time there is a DDoS incident
	Communications (RC.CO)	**RC.CO-1:** Manage public relations	P2	Ensure impacted applications are restored and availability communicated to relevant stakeholders Manage external communications based on visibility and impact of the DDoS attack on customers, partners or public