



July 27, 2017

Evelyn L. Remaley
Deputy Associate Administrator
National Telecommunications and Information Administration
1401 Constitution Avenue NW., Room 4725
Washington, DC 20230

**Re: Promoting Stakeholder Action Against Botnets and Other Automated Threats
[Docket No. 170602536-7536-01]**

Symantec Corporation (Symantec) appreciates the opportunity to provide a response to the Request for Comments (RFC) issued by the National Telecommunications and Information Administration (NTIA) on June 13, 2017.¹ The RFC sought comments on promoting stakeholder action against botnets and other automated threats. In particular, the RFC sought input on how to mitigate the impact of botnet attacks and how best to secure devices to prevent infections in the first place. As the largest cybersecurity company in the world, Symantec has significant expertise defending against botnet infections, working with law enforcement to take them down, and understanding the threat landscape that allows them to thrive. Symantec believes that the Department of Commerce can play a critical role in bringing together private sector entities and government, all of whom have a stake in responding to botnet attacks and protecting devices against botnet malware infections.

The Botnet Threat

The uses for malicious bots are only limited by the imagination of the criminal bot master. One common use for botnets is for Distributed Denial-of-Service (DDoS) attacks, which occur when multiple infected systems are used to overwhelm a victim and render it unable to respond to legitimate requests. DDoS attacks are also used to provide cover for other, more sophisticated attacks. Organized crime groups have been known to launch DDoS attacks against banks to divert the attention and resources of the bank's security team while the main attack is launched, which can include draining customer accounts or stealing debit or credit card information. Despite increased efforts by law enforcement to take down botnets, Symantec observed an increase of 6.7 million bots from 2015 (91.9 million) to 2016 (98.6 million).² This increase is at least in part due to the rapid increase in the number of new devices connected to the Internet – the Internet of Things (“IoT”).

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

² Symantec, *Internet Security Threat Report*, 41, (April 2017) (“Symantec”).

No recent threat has challenged our collective defenses or is more representative of today's evolving threat landscape than botnets incorporating IoT devices. Infected IoT devices offer a powerful new weapon for cybercriminals looking to amplify their power. These IoT devices are an increasingly attractive target for botnets for three reasons:

1. **Security is not the priority.** For the device manufacturer, being "first to market" with a product is valued more than being the most "secure to market". This can lead to development practices that ignore security considerations, such as default or hard-coded passwords and open ports, which users do not, or cannot change.
2. **No ability to receive security updates.** IoT devices often do not have built-in mechanisms to receive automatic firmware updates, which leads to known vulnerabilities being unpatched.
3. **Out of sight, out of mind.** Consumers often forget about their device once it is installed. This means that their owners are unaware when devices are being used for malicious purposes.

Perhaps the best example of the destructive power of IoT botnets came in late 2016, when the Mirai botnet, which is made up of IoT devices, was used in a number of high-profile DDoS attacks. It remains difficult to state conclusively how many Mirai-infected devices were out there, but some estimates showed as many as 493,000 Mirai-infected devices.³

In an effort to understand the evolving security threat to IoT, Symantec established an IoT honeypot to observe attacks. The honeypot appeared as an open router and attempts to connect to the system were logged and analyzed. Between January and December 2016, the number of unique IP addresses targeting the honeypot almost doubled. At times of peak activity, when Mirai was expanding rapidly, attacks on the honeypot were taking place every two minutes. The attack on Domain Name Service (DNS) company Dyn showed just how powerful a DDoS attack using IoT devices could be, when it disrupted many of the world's most popular websites and applications. This raised the sobering question of what could happen if attackers decided to target industrial control systems or critical national infrastructure. (See Figure 1)

Attacks using IoT devices also greatly lower the barrier of entry for cyber criminals, as there is little or no security on many of them. Unlike a desktop computer, or laptop, which often have security software installed and receive automatic security updates, IoT devices are often only protected by a user name and password. Analysis of the passwords used by IoT malware to attempt to log into devices revealed that user names and passwords are often never changed from their factory default settings.

³ <http://www.pcworld.com/article/3132571/hacker-create-more-iot-botnets-with-mirai-source-code.html>

I. Consensus Driven IoT Security Standards

Symantec encourages the Department not to “reinvent the wheel.” Instead, it should build on the NIST Cybersecurity Framework (Framework) by promoting adoption by device manufacturers. In addition, the Department should begin a multistakeholder process to develop industry standards around the secure development of IoT devices, drawing on the considerable experience of the private sector, government, and academia. Further, cybersecurity standards are most effective when they are developed and harmonized globally. This will avoid burdening multinational manufacturers with multiple, often conflicting, requirements.

Leverage NIST Cybersecurity Framework. Many best practices employed in traditional IT security can also be applied to securing IoT. Broader adoption of the Framework, including by IoT device manufacturers and other stakeholders, will improve security across the board and make it more difficult for attackers to be successful. The Framework was designed to be flexible and allow companies of all sizes and different industries to help make risk-based cybersecurity decisions. Adapting the Framework’s approach to the IoT space is a natural progression, considering the wide variety of platforms, uses, and industries involved in the IoT market.

Symantec also sees utility in developing specific applications of the Framework to address particular problems, such as DDoS attacks. As part of the Coalition for Cybersecurity Policy and Law, we helped create a DDoS threat profile under the Cybersecurity Framework (attached). This profile could be a starting point to help NTIA and NIST promote adoption of the Framework in ways that will help minimize the impact of DDoS attacks.

Secure by Design. Most IoT devices are “closed” and cannot have security added after the device leaves the factory. In such cases, they need to have security build into the device, starting at the design phase. There is a strong need for consensus-based standards with respect to the development of secure IoT devices. Today, connected device manufacturers do not necessarily consider security as a top priority or even a secondary priority. Development and promotion of consensus-based voluntary standards that take into account the wide variety of devices – from the smallest sensor to a connected car – would help guide manufacturers to implement better security practices based on risk. Improving some the basic security of IoT devices will diminish the potential power of IoT-fueled botnets by making them more difficult to infect and control.

One very basic security standard that manufacturers should implement is to stop manufacturing devices with hardcoded passwords, which can never be changed. And if a device is shipped with default passwords, manufacturers should require consumers to change those passwords. Most users are unaware of the dangers of default credentials and are unlikely to attempt to change them without being forced to do so. Best practices dictate that users should have a unique user name and password combination for all of their IoT devices. However, unless device manufacturers prompt users to select a unique password most will not

do so – and these default passwords will continue to be a security weak point. In addition, the passwords that the manufacturers set as their default are often easily guessed. For example, according to Symantec’s IoT honeypot, 37% of malicious login attempts used the password “admin.” The Mirai botnet spread so quickly by continuously scanning for IoT devices using well-known factory default passwords.⁴ Analysis of the IoT honeypot data also allowed us to determine the countries from which attacks were initiated, but does not necessarily mean the attackers were based in those countries. Nearly 27% of the attacks came from China and nearly 18% from the United States (See Figure2). This data reinforces our view that botnets are a global phenomenon, with nodes located in multiple countries. Any potential policies on botnets should be treated with a global view in mind.

Market-driven Security. The Department should work with stakeholders to assess how the market does – and does not – encourage secure practices, and to develop initiatives to use market forces to drive secure development. The Presidential *Commission on Enhancing National Cybersecurity* report in late 2016 addressed this issue, proposing the development of the equivalent of a cybersecurity “nutritional label” which would describe the security level of a device. Other groups have proposed similar solutions, including labels that convey privacy and cybersecurity related information, related risks for use of particular product or service, and guidance about how to secure the device properly. An easy to understand and properly placed label could enhance consumer decision-making power, and thus allow manufacturers to differentiate themselves in the marketplace as being more “secure.”⁵ The European Commission is considering something similar with their “Trusted IoT Label” initiative.⁶ Lastly, proposals that attempt to use legal liability or the nascent cybersecurity insurance market to shape standards adoption are other ways to drive a market for IoT security.

But the market might not address all circumstances, particularly in critical infrastructure. Where the market fails to drive security, the Department should look at other alternatives to shape the market, including security baselines, changes in liability, and other market forces. Securing the IoT space is too critical to our economy and national security to leave to chance.

II. Public-Private Partnerships Critical to Addressing IoT Security

Much of the cybercrime we see today is facilitated by malicious botnets. They allow cybercriminals to increase their distribution power exponentially and provide a potent tool for any number of crimes. Because cybercrime and botnets are a borderless problem, any effort to thwart them requires cooperation and coordination – between the government and the private sector, between governments across the globe, and within the private sector itself. The government can play a critical role in facilitating collaborative action against botnets and other cybercrime threats.

⁴ Symantec 66

⁵ <https://www.nist.gov/cybercommission>

⁶ http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm

Facilitating Information Sharing. One important role the government can play is to enhance and improve the quality of information sharing with the private sector. While we have made great strides in threat information sharing over the last several years, there is more work to be done. Specifically, threat information sharing needs to be more targeted to the specific needs of the stakeholder. To that end, the government can also play an important role by convening working groups that target specific threats in addition to the broader initiatives.

The private sector is also banding together to counter cybercrime and, industry partnerships have proven highly effective in fighting cybercrime. The Cyber Threat Alliance (CTA) is an excellent example of the private sector working together to improve the overall safety and security of the Internet. In 2014, Symantec, Fortinet, Intel Security, and Palo Alto Networks formed the CTA to work together to share threat information, including mobile threats. Since that time, Cisco and Checkpoint have joined the CTA as founding members. The goal of the CTA is to better distribute detailed information about advanced attacks and thereby raise the situational awareness of CTA members and improve overall protection for our customers. By raising the industry's collective intelligence through these new data exchanges, CTA members have delivered greater security for individual customers and organizations.⁷

Law Enforcement Action. Public-private partnerships can lead to concrete law enforcement results. Symantec has been a global leader in partnering with law enforcement to take down many of the largest botnets and most prolific cybercriminals.⁸ One recent example came in December 2016, when Symantec concluded a decade-long research campaign that helped unearth an international cybercriminal gang dubbed “Bayrob.” The group is responsible for stealing up to \$35 million from victims through auto auction scams, credit card fraud and computer intrusions. Over time, Symantec’s research team gained deep technical insight into Bayrob’s operations and its malicious activities, including its recruitment of money mules. These investigations and countermeasures were crucial in assisting the Federal Bureau of Investigation (FBI) and authorities in Romania in building their case to arrest three of Bayrob’s key actors and extradite them to the U.S. They are currently in federal custody awaiting trial. The government should continue to leverage private sector resources to help fight cybercrime and bring cybercriminals to justice.

Botnets nearly always involve infected machines physically located in multiple countries, often with their command-and-control structures located in countries outside the reach of U.S. law enforcement. This poses a difficult challenge for our law enforcement agencies. Even if countries are willing to help U.S. law enforcement take down these command-and-control structures, they often lack the resources and expertise to be an effective partner. Significant capability gaps exist between countries ability to investigate and prosecute cybercrimes. The Government should encourage cyber-capacity building efforts globally and facilitate international collaboration to prosecute cybercriminals.

⁷ <https://cyberthreatalliance.org>

⁸ Testimony <https://www.judiciary.senate.gov/imo/media/doc/07-15-14McGuireTestimony.pdf>

Dual-Use Export Controls on Cybersecurity. We encourage the Department to remain vigilant against new export laws and regulations that are not properly considered or vetted, no matter how well intended they may be. One example is the draft rule that came from the Wassenaar Arrangement, of which the United States is a signatory. If implemented as written, the proposed rule would have imposed strict controls on the export of almost all cybersecurity products and services. Most common forms of updates and patches even for features and functionality would be restricted under language in the draft rule, making critical and required cyber hygiene activities almost impossible. The definitions and controls in the draft rule as written were so vague that it would have curtailed threat information sharing and restricted access to cybersecurity products that offer protections against attacks. The European Union is exploring even more restrictive export controls on cybersecurity. These proposals would most certainly slow security research by restricting the ability of industry cybersecurity and academic researchers from sharing time critical technology and software with other researchers around the world, damage U.S. and worldwide security companies, and severely impair our ability to protect our customers around the world. The end result of these ill-defined and restrictive export controls will be a worldwide cyber eco-system at much greater risk.

III. Raising Awareness of Consumers

The Department should also make efforts to promote current industry efforts to educate consumers on good security practices. Raising consumer awareness around cybersecurity has long been a pillar of the U.S. Government's cybersecurity strategy and the Department should support these efforts. Several examples exist today, including the work being done by the National Cyber Security Alliance (NCSA) and the STOP.THINK.CONNECT. global campaign to raise awareness of online threats.⁹ While consumer education will never be a panacea, awareness-raising efforts like STOP.THINK.CONNECT can provide consumers with the tools to recognize malicious emails, a trend that is growing more acute, with an increase of nearly 50% from 2015 to 2016.¹⁰ The Department should also encourage the private sector to provide employees cybersecurity training that focuses on the secure use of devices.

Leveraging Private Sector Technology. Even as cybercriminals evolve, the private sector is keeping pace by innovating and deploying new security technology. For instance, a number of excellent training tools exist that can help companies educate employees on detecting malicious emails before they inadvertently infect devices linked to their companies network.¹¹ Providing cybersecurity training to employees and raising their overall cybersecurity I.Q. will help stem the spread of botnets and other infections. In addition to raising awareness and practicing good cyber hygiene, consumers can help protect themselves and their connected devices by leveraging new security technology. For instance, deploying a secure Wi-Fi router can help protect connected devices on your home network by stopping cyber-attacks at the

⁹ STOP. THINK. CONNECT. <https://www.stopthinkconnect.org>.

¹⁰ Symantec, 23

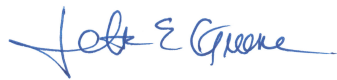
¹¹ <https://www.symantec.com/content/dam/symantec/docs/data-sheets/phishing-readiness-en.pdf>

network level, before they are infected and become part of a botnet such as Mirai.¹² The Department should encourage and promote the development and deployment of state-of-the-art security technology.

IV. Conclusion

Symantec thanks NTIA for the opportunity to provide input to this very important effort. We look forward to working with NTIA as the process moves forward and we are pleased to provide additional information or answer any questions you may have.

Sincerely,

A handwritten signature in blue ink that reads "Jeff E. Greene". The signature is written in a cursive style with a long horizontal stroke at the end.

Jeff Greene
Senior Director, Global Government Affairs
& Cybersecurity Policy
Symantec Corporation

¹² <https://www.cnet.com/products/norton-core/preview/>

Attachment

Figure 1

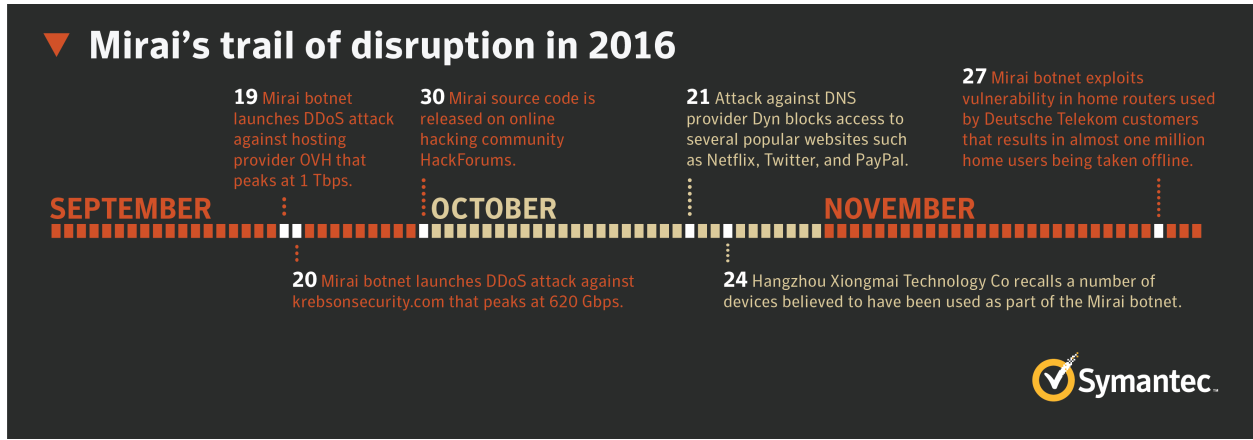
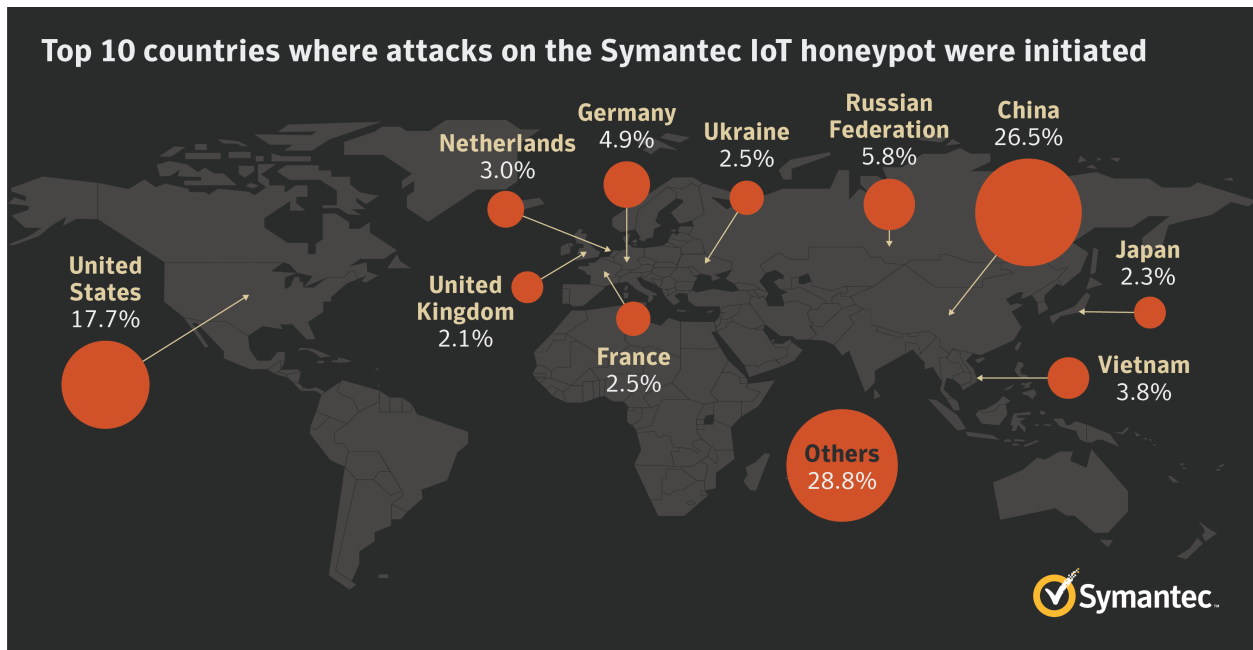


Figure 2



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

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
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

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
		ID.AM-3: Map organizational communication and data flows	P2	<p>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</p> <p>Maintain network maps showing data flows</p> <p>Create an operational process document detailing communication workflows</p>
		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

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
	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

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
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)	P1	PR.IP-1: Create and maintain a baseline configuration of information technology/industrial control systems 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

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
		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, SSDP and SIP
		DE.AE-2: Analyze detected events to understand attack targets and methods	P1	Determine source and destination traffic characteristics when anomalous traffic is

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
				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 into all 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.

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
		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

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
		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

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
				with the operational security community.
	Mitigation (RS.MI)	RS.MI-2: Mitigate incidents	P1	<p>Mitigate DDoS attacks using any or all of the following:</p> <ul style="list-style-type: none"> - 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 <p>Critical resources should be protected by always on mitigation capabilities</p> <ul style="list-style-type: none"> - Contract or coordinate with upstream bandwidth provider for defense against high-magnitude attacks. <p>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</p> <p>Identify and maintain key security metrics around mitigation and escalation effectiveness.</p>

<i>Function</i>	<i>Category</i>	<i>Sub-Category</i>	<i>Priority</i>	<i>Framework Comment</i>
Recover (RC)	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.
	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