Response to Request for Public Comment:

Promoting Stakeholder Action Against Botnets and Other Automated Threats

[RIN 0660-XC03]
[Docket No. 170602536-7536-01]

National Telecommunications and Information Administration (NTIA)

Department of Commerce

Attention:
Evelyn L. Remaley
Deputy Associate Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave. NW
Washington, DC 20230

Katherine Gronberg
Vice President, Government Affairs

Timothy Jones | CISSP, CISM, CCSK, FSCA
Manager of Systems Engineering - Public Sector
ForeScout Technologies, Inc.
408.213.3191
info@forescout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134

ForeScout® Technologies, Inc.

Response to the National Telecommunications and Information Administration's (NTIA) Request for Public Comment entitled:

Promoting Stakeholder Action Against Botnets and Other Automated Threats

July 28, 2017

Introduction

ForeScout Technologies is pleased to provide comments in response to the NTIA's solicitation for stakeholder input regarding botnets and other automated threats. ForeScout is also pleased to participate in the NTIA's Multi-stakeholder Process on Internet of Things (IoT) Security Upgradability and Patching as well as to have participated in the workshop held by the National Cybersecurity Center of Excellence (NCCoE) on July 11 and 12, 2017, entitled, "Enhancing Resilience of the Internet and Communications Ecosystem."

Section 2(d) of the Executive Order (EO) entitled, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," dated May 11, 2017, directs the Secretaries of Commerce and Homeland Security to conduct a process to "identify and promote action by appropriate stakeholders to improve the resilience of the Internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." The Internet Engineering Task Force (IETF) defines a malicious or potentially malicious bot as "a program that is installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a remote administrator, or 'bot master.'" IETF further defines a "bot network" ("botnet") as "a concerted network of bots capable of acting on instructions generated remotely." Botnets can be programmed to perform a variety of functions, including malicious functions such as to enable identity theft, spam, email address harvesting, distributed denial-of-service (DDoS) attacks, hosting of illegal content, and so on.[1]

Significant attention has been focused on one particular type of malicious activity that is enabled by botnets, namely DDoS attacks, because of the occurrence of two large-scale attacks in late 2016.[2] The first of these attacks occurred in September 2016, and targeted the cybersecurity blog KrebsOnSecurity. This attack was approximately 665 Gigabits of traffic per second (Gbps) in size, which was many orders of magnitude larger than what is needed to knock most sites offline, and orders of magnitude larger than previous DDoS attacks we have seen.[3] The second noteworthy DDoS attack occurred in October

[1] Internet Engineering Task Force (IETF), "Recommendations for the Remediation of Bots in ISP Networks," March 2012, p.4.

[2] A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems. (Source: Search Security/Tech Target).

[3] KrebsOnSecurity, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

2016, and targeted the U.S.-based domain name provider, Dyn. The size of this attack was almost double the size of the Krebs attack, measuring at an unprecedented 1.2 Terabytes of traffic per second (Tbps).

The Dyn attack caused an inconvenient interruption of service for music services, social media platforms and single sign-on capabilities, but it did not cause any overt significant economic or physical disruption or destruction. However, the Dyn attack is just a preview of the damage that can be wrought through a DDoS attack. Government officials and other experts are rightfully concerned about this shocking growth in DDoS attacks because they know that load balancing and traffic rerouting—the traditional responses to such attacks—won't work as well, or may not work at all, against attacks of this magnitude and larger. Malware that can exploit known and unknown vulnerabilities, either on IoT or Windows-based devices, is proliferating faster than we can get tools into people's hands to prevent its spread. Large-scale attacks that are far more disruptive than the ones we have seen are not only likely, they are highly probable, in a very short time frame.

Device Explosion Means Willing Recruits

One of the main reasons why these recent DDoS attacks were significantly larger than those seen in the past is because bot masters now have the ability to conscript vulnerable IoT devices into their botnets. They can remotely command these IoT devices to direct packet traffic to a chosen target, flooding the target domain and knocking it offline. The number of IoT devices on global networks has increased exponentially each year for the past several years. (See Figure 1). Internet of Things (IoT) devices are proliferating because they are cheap, easy to get and offer benefits such as lifestyle improvements, efficiencies and cost savings.

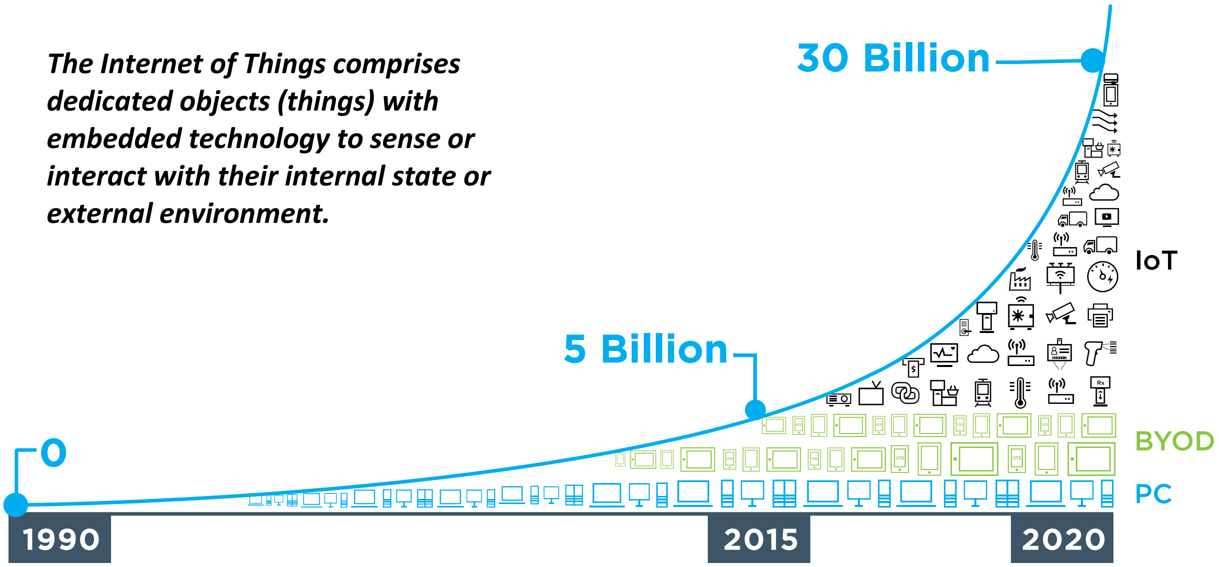
The Internet of Things comprises dedicated objects (things) with embedded technology to sense or interact with their internal state or external environment.

Figure 1. *The explosive growth of connected devices on global networks* (Source: ABI Research, 2017)

Until now, consumers largely have connected devices such as thermostats, baby monitors, appliances, and wearables to their home networks with little or no consideration for security. Businesses, in pursuit of tantalizing efficiencies, convenience, cost savings and safety enhancements, have been connecting devices to their enterprise networks just as enthusiastically as consumers, if not more so. More traditional office-environment-type businesses have been connecting communications systems and buildings systems such as Nest thermostats, video monitors and Voice over Internet Protocol (VoIP) phones. Hospitals have been connecting medical devices such as pharmaceutical dispensing cabinets, infusion pumps and X-ray machines so rapidly that the "Internet of Medical Things" (IoMT) has become its own sub-category of IoT. Industrial organizations are no less enthusiastic, layering connected technology directly into their control and production environments or into peripheral, supporting systems (e.g., programmable logic controllers, valves, thermostats, and scanners). These devices also have their own IoT subcategory: the "Industrial Internet of Things" (IIoT). We group IoMT and IIoT devices under the umbrella of "operational technology," or OT.

The sheer number of vulnerable devices that can now be recruited across global networks represents the potential for DDoS attacks of unprecedented size. ForeScout has encountered enterprises that employ vast amounts of networked devices throughout their business and operational environments—in one example every single overhead light was networked. Consequently, today, it is impossible to ponder the question of how to mitigate massive DDoS attacks without also contemplating how to reduce the massive amounts of insecure IoT devices currently on global networks. The two issues are inseparable and it is in the latter area—the insecurity of IoT devices—that ForeScout's expertise lies.

Securing IoT Devices Is a Shared Responsibility

The explosion in the number of IoT devices on global networks is not, by itself, the root of the DDoS problem. It is the growth of the number of devices coupled with the near-total lack of attention the security of these devices has received until now. This holds true for almost all of the stakeholder levels in the "security ecosystem," throughout the IoT device lifecycle: IoT device manufacturer, application provider, network provider, and end user.

Security at the design level has been almost wholly ignored, primarily because razor-thin profit margins and pressure to take these products quickly to market dis-incentivize manufacturers from "building in" security features. Another reason why security has been ignored is due to the physical limitations of most IoT devices. IoT devices are quite different from traditional information technology devices such as laptops, desktops and servers. They differ mainly in the sense that they have minimal hardware, nonstandard operating systems and very limited processing capabilities. Whereas it is relatively easy to embed or enable a security feature such as password protection onto an IoT device, other types of security functionality (for example, running encryption software and/or virtual private network capabilities) requires more power and processing than most of these devices have. To consider running an authentication tool (such as a digital certificate) or even a tool that would allow you to scan a device for malware, the device needs to allow a software agent to be installed, which most IoT devices do not and cannot have installed.[4]

[4] An "agent" is a small piece of software that resides on a device. Agents can have various functions and, among other things, can allow a device to be scanned for malware and vulnerabilities. Such agents usually connect back to a server, which has a list of new malware to check for (and remediate) or new patches that must be installed on the device's operating system (OS) or firmware.

Consumers by and large do not consider the security of the devices they connect to their home networks. Some enterprises do consider the security of these IoT or OT endpoints, but most do not. This stands in stark contrast to the awareness both consumers and businesses have developed over the last decade or more of the consequences of connecting a laptop to their network that is not running basic security tools such as an antivirus program and firewall and has not been recently updated.

What are the things that can be done right now to mitigate the problem?

1. Global network infrastructure providers must continue to work together to share information and also to invest in network-level defenses such as port blocking, traffic flow routing, and notification policies, as well as anti-spoofing and other attribution methodologies.
2. Internet Service Providers (ISPs) and enterprises (particularly those that provide critical services and functions to our society and economy such as financial institutions and healthcare providers) must continue to develop and invest in DDoS mitigation services (like load balancing and dynamic provisioning)—especially promising are those that leverage the cloud.
3. Enterprises, particularly those with IoT- and OT-heavy environments, must make securing IoT devices part of their risk mitigation strategies, using tried-and-true tools alongside some newer ones. (ForeScout's expertise—providing enterprises with the ability to automatically and agentlessly detect, profile, and enforce policy-based controls on IP-enabled devices on their networks—is targeted in this area).
4. Consumers must be provided with the know-how and tools (not yet widely available to them) to be able to secure IoT devices on their home networks. On the education front, *Consumer Reports* will soon begin evaluating devices for their security level so consumers can make informed decisions. On the tools front, several home IoT security products debuted at the Consumer Electronics Show in 2017, including Norton Core.
5. Device developers and manufacturers must build more security features into the IoT devices they produce, particularly features such as password protection that are fairly cheaply and easily implemented. This necessary shift will be driven by consumer and enterprise awareness, enterprise and government buying decisions, litigation and legal precedent, and (to some degree) regulatory action.[5]

ForeScout believes the combination of the above steps will significantly reduce the number of vulnerable IoT devices that can be recruited into large-scale DDoS attacks globally. Each of the stakeholder groups identified above will be compelled to act through a variety of means, including increased awareness, market incentives (such as tax or contracting preferences, competitive advantage, legal precedent and insurance imperatives), coordinated industry action, or even government action (such as the issuance of guidelines, labeling mechanisms, regulations or even through the government's sheer buying power).

[5] Particularly for IoT devices utilized in regulated industries such as healthcare, there is a growing list of enforcement actions that has already had an impact on how manufacturers approach device security.

Thus Far, an Over-Emphasis on Security by Design

A few models have been advanced that would certainly assist in the creation of safer ecosystems for IoT. However, in general, these tend to focus too much on things that depend on manufacturers *doing* something, compelled either by incentives or requirements.

Shortly after the October 2016 Dyn botnet attack, the Department of Homeland Security (DHS) issued *Strategic Principles for Securing the Internet of Things*.[6] The document's recommendations were helpful, especially Principal 3, "Build on recognized principles," which referenced the National Institute of Standards and Technology (NIST) Framework. But the strategic principles were too focused on the condition of individual devices. The first and second principles are: "Incorporate Security at the Design Phase" and "Promote Security Updates and Vulnerability Management." By and large, the principles did not address stakeholders beyond the manufacturers and missed the opportunity to present IoT as part of a larger ecosystem that includes users of IoT. After all, an IoT device doesn't become dangerous until it is connected to a network.

One exception, "Connect carefully and deliberately," seemed to head in the right direction. Users should connect carefully. However, the recommendation to "not connect things when you don't have to" isn't very practical moving forward. The idea that IoT devices connect sporadically undermines one of the key benefits of IoT. How many of us want security cameras that only transmit "some of the time" or an insulin pump that monitors "occasionally?" Two of the largest U.S. government cybersecurity programs, the Continuous Diagnostics and Mitigation Program (run by DHS and serving U.S. civilian agencies) and Comply to Connect (for the Defense Department) are premised on allowing devices to connect, but only when they meet certain conditions and behave according to certain rules. These programs are rooted in the concept: let a device on and monitor it relentlessly (in NIST vernacular, Information Security Continuous Monitoring, or ISCM).

Security by design is an important part of the discussion, to be sure, but it is by no means the only thing we should be focusing on in our quest to reduce the number of unsecured IoT devices on global networks. Firstly, even when manufacturers can be incentivized or coerced into producing better software and hardware, there will still be vulnerabilities—just like there are in the Windows machines that fell victim to WannaCry. Patching for IoT devices, while a terrific idea, is unlikely to be any better than the patching methodologies we use for computers and other traditional networking equipment. It could in fact be much worse since, at least for the foreseeable future, as we cannot rely on IoT manufacturers to issue and distribute patches and updates. Realistically, we can't even expect manufacturers to be anywhere near as good as mainstream software companies at this. Further, how is any such regime going to be regulated and enforced? Will the consumer be willing to pay for more secure devices? Finally, we note that any patching/upgradability mechanism or requirement will need to involve a third-party vetting process in order to address the problem of deliberately implanted vulnerabilities ("backdoors").

[6] https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

We Can't Afford To Wait for Manufacturers to Fix Devices

ForeScout believes that it is important to examine what can be done about botnets at the supply chain level and at the time of device design and manufacture. But, no matter what, IoT security is going to need to be managed to a great extent by the enterprise itself. We are encouraged to see that the policy discussion is shifting more toward the steps enterprises and consumers can take to control how IoT devices are behaving on their networks. (See bullet number 3 above.) Evidence of this shift is provided in the Food and Drug Administration's December 2016 release of its *Postmarket Management of Cybersecurity in Medical Devices* guidelines, which address how IoT devices should be treated once deployed in hospital environments.[7] Also, the Health Care Industry Cybersecurity Task Force released its report in June 2017, which recommends that health delivery organizations utilize compensating controls to secure medical devices on their networks.[8]

Enterprises need a way to secure IoT on their networks not *only* to avoid the conscription of these devices into botnets, but to prevent them from being used as possible entry points for attackers to move laterally within the organization's networks to higher-value assets (HVAs) such as customer data, intellectual property or data that is sensitive from a physical security standpoint. Failure to secure these devices also opens the door to disruption of operations across the organization, potentially leading to partial or full system downtime—or even outright failure. To understand what these compensating controls entail, enterprises need look no further than the NIST Framework and the Center for Internet Security (CIS) (formerly SANS) controls.

Secure IoT on Networks with Compensating Controls

Until security measures in other parts of the device ecosystem are reliably and broadly implemented, compensating controls are the way that the issue of unsecured IoT devices on global networks can be addressed. In this context, compensating controls refer to security mechanisms that can be put in place (in this case, in the enterprise's network architecture) that serve to mitigate or eliminate the risk associated with vulnerable IoT devices because security mechanisms in other parts of the device ecosystem are too difficult or impractical to implement, or because they fail outright. Compensating controls can be a major factor in preventing botnets and other automated threats from targeting IoT.

Detection

A basic tenet of cybersecurity is *"you can't protect what you can't see."* Hardware and software asset management are the top two security controls in both the NIST cybersecurity framework and the CIS Top 20 Controls.[9] Put simply, "hardware asset management" and "software asset management" mean you should know what devices are on your networks as well as what software those devices are running. It can be difficult enough for companies and government agencies to have an accurate and current picture of devices running traditional operating systems in their enterprises. However, "domain awareness" is vastly more difficult with respect to IoT devices because typically those devices cannot be

[7] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[8] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

[9] NIST Framework https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf and SANS Critical Security Controls: https://www.sans.org/media/critical-security-controls/Poster_Fall_2014_CSCs_WEB.PDF

"seen" by traditional cybersecurity tools because they do not support an agent. These agent-based tools only see that "something is there" and cannot tell what it is, what it's running or how it's behaving. From a security standpoint, the endpoint is invisible. Another reason why devices often go undetected on networks is that they can be missed by point-in-time scans. IoT devices are transient by their nature, and large numbers of devices can come and go from the network in the time span (often 72 hours) between network sweeps. These IoT devices also go undetected because they do not respond to ping sweeps (or modified ping sweeps) which many security tools leverage for discovery.

The failure to even know when IoT devices are present on a network represents a huge gap in many enterprises' security and provides ample recruiting opportunities for botnets. ForeScout's customers have reported seeing up to 60 percent more devices in an environment than network administrators originally guessed were there. That delta represents completely unmanaged and unprotected assets to which the enterprise is totally blind, hence the moniker "Shadow IT." Shadow IT makes up an ever-increasing percentage of most enterprises' threat surface. And the distribution of self-propagating, botnet-creating malware on the dark web, most notably Mirai, makes it easy for even the most inexperienced hacker to build enormous botnets because the malware can easily spread amongst this undetected IOT.[10]

The importance of detection (or "visibility") derives from *NIST 800-53 Control* ***AC-3 Access Enforcement*** and uses the defined logical access to information and system resources in accordance with applicable access control policies established by the organization. A flexible and granular policy engine combined with a range of control options is needed to establish this control. This includes the ability to configure the enforcement of access to provide the right action for each situation automatically, without the need for human intervention.

Federal agencies are already beginning to address the problem of Shadow IoT on their networks through two large-scale programs, the Continuous Diagnostics and Mitigation Program (CDM) for civilian agencies and Comply to Connect (C2C) for the Department of Defense (DoD). What is groundbreaking about these programs is that they will give the agencies *continuous* domain awareness—knowledge of a device's presence on the network the instant it connects to the network, versus a periodic scan—and they will allow agencies to discover and account for devices, including non-traditional IoT and operational technology (OT) devices.

[10] The Continuous Diagnostics and Mitigation (CDM) program discovered 44% more devices than federal agencies estimated when the project was originally scoped. This problem of "Shadow IoT," fortunately, is being addressed as civilian agencies deploy Phase 1 security tools in CDM. (Source: https://fedtechmagazine.com/article/2017/07/why-shadow-it-now-gets-second-chance-cios)

Authentication

Once a device is detected on a network, it is critical to determine that it is authorized to be there—in a word, *authentication*. Authenticating an IoT device on a network (usually with some kind of whitelisting construct) is not the same as determining its fitness to be allowed on, i.e., its security status. ForeScout observes that, frequently, enterprises conflate authentication as security, and we see this bleeding into policy discussions such as the one about botnets. Most authentication solutions currently sold are focused on Windows-based endpoints and depend on a specific protocol like 802.1X or a digital certificate, which IoT devices do not support. The default for authenticating IoT devices often then becomes relying on the device's MAC address, which can be faked or "spoofed" and is not best practice.

The importance of authentication comes from *NIST 800-53 Control* ***AC-14 Permitted Actions without Identification or Authentication***. When a device attempts to connect to the network, a check must be performed to verify the device's admissibility. Because MAC address admission and bypass authentication are imperfect authentication methods, it is absolutely critical to track the device's active sessions to better understand its expected behavior, as proof of admissibility.

Scanning for Vulnerabilities and Indicators of Compromise

The purpose of scanning is to determine the security state (hygiene) of an endpoint (such as whether it's running an outdated operating system or other applications, whether it has been infected by malware and whether it is configured properly). Knowing these things about a device gets you closer to understanding the security threat posed by a particular device. However, many existing vulnerability and detection scanning tools depend on an agent to be able to know a device's hygiene status. An alternative to scanning individual devices, which typically requires an agent and can in some circumstances cause resets that cause systems to fail, is to monitor the networking infrastructure to determine characteristics of devices that are looking to connect. As a device communicates to the networking infrastructure, it reveals a lot of useful data about potential critical vulnerabilities or indicators of compromise (IOCs). This data can be seen passively originating from the device.

NIST 800-53 Control ***RA-5 Vulnerability Scanning*** is a critical component to understanding residual risk. Ideally, devices that are trying to connect are evaluated for vulnerabilities against a baseline "healthy" device, where the definition of "baseline" is updated continuously and automatically (without human intervention). This is critical to speeding up the detection and remediation of rapidly proliferating endpoints in a risk-based model.

Scanning for Indicators of Compromise (IOCs), the aim of which is to identify factors such as specific malware signatures (code) that point to hacker activity, is aligned with *NIST 800-53 Control* ***SI-4 Information System Monitoring***.

Behavioral Profiling

Making a determination as to whether a device is "secure" doesn't only have to do with what is running on the device (such as an unpatched program or malicious code). You also need to monitor a device's behavior. Is it communicating out of an inappropriate port? Is it trying to scan other parts of your network? Is it beaconing to an unfamiliar IP address? Unexpected behaviors such as unusual communications or attempted surveillance actions are indicators of compromise and call for some kind of remediation (see below).

One idea that has been offered to assist enterprises in profiling device behavior in order to create security policies is some kind of information-sharing construct in which manufacturers make information available about how devices are supposed to behave. One such idea is the Manufacturer Usage Descriptions (MUD) framework advanced by Cisco in collaboration with the Internet Engineering Task Force (IETF), which proposes that manufacturers post information about expected device behavior to a MUD server and users, in turn, access such information using a MUD Controller. ForeScout enthusiastically encourages the development of an information-sharing construct for device characteristics and behaviors. To be truly effective in combating botnets, however, such a construct must be universally accepted. To be universally accepted, it has to have reasonably low barriers to participation. It should not require either device producers or users to procure new networking equipment and it should place as few requirements as possible on the manufacturer. We must also carefully consider important questions such as how to ensure device information is securely transmitted, how manufacturer and/or device end of life will be addressed, and how to incentivize manufacturers to participate (or, if their participation is required, how to enforce any requirements).

> Behavior profiling—determining what is "normal behavior for devices"—aligns with *NIST 800-53 Control* ***IR-5 Incident Monitoring*** and ***SC-7 Boundary Protection.*** Expectations about device behavior will vary widely amongst devices and will change continuously. Thus the process of using this information to enforce policies on devices will require real-time information gathering, analytics and notification.

ForeScout notes that there are a variety of existing ways to reliably profile device behavior, which helps in classifying and setting security policies for devices. ForeScout relies on data points like 802.1X and Dynamic Host Configuration Protocol (DHCP) requests, as well as observed Hypertext Transfer Protocol (HTTP) traffic, banners, Media Access Control (MAC) classification data and Lightweight Directory Access Protocol (LDAP) data.[11] It's also possible to classify a device based on other factors such as session monitoring and its appropriate level of power consumption, i.e. power over Ethernet (PoE) data.

[11] Fingerbank.org, is a platform we frequently reference. It collects information, including a device's MAC address, its DHCP fingerprint and its User-Agent, to help profile devices.

Segmentation

NIST 800-53 Control ***AC-5 Separation of Duties*** defines information system access authorizations, which provides control over what parts of the network devices are authorized to access. *NIST 800-53 Control* ***SC-3 Security Function Isolation*** recommends the isolation of security functions from non-security functions by means of an isolation boundary consisting of physical or logical paths.

Subdividing a network into “lanes” (i.e., subnetworks, or “subnets”) offers the ability to segment or “wall off” endpoints from other parts of your networks. It is one way to remediate a badly behaving device, e.g., the one trying to scan your network won’t be able to reach out of its subnet, or the one looking to connect to its command and control server (critical for most botnets) will be unable to do so. If an enterprise has strong detection and device classification capabilities, then it should aim to automatically segment devices immediately upon connecting to the network (automatically, meaning without a human needing to make a decision). This is especially critical for health delivery organizations. Segmentation is not so much a remediation tool, but rather good basic network hygiene. There’s no reason to comingle different types of assets on a network. They can be monitored and controlled more easily, and en masse, when they are grouped into appropriate segments, whether this occurs at the switch level or at the wireless access point.

Mitigation

We have observed that, too often, discussions omit options for how to remediate the problems found on devices, probably because this is not a “one-size-fits-all” consideration. Response, or mitigation, needs to be aligned to the risk. What to do about discovered anomalies is a policy exercise on the part of the enterprise—one that, above all, needs to be carefully considered in advance so policies can be implemented rapidly. With a multitude of response options—taking devices offline, dropping them into their own Virtual Local Area Network (VLAN), applying an access control list (ACL) to the interface the device connects to, remediating found problems in place (patching, rebooting, replacing), etc.—policies need to keep pace with the enterprise’s changing needs, especially when it comes to scaling for growth and balancing business/operational needs with security.

NIST 800-53 Control ***CA-2 Security Assessments*** provides a framework for assessment planning, but the response or mitigation needs to be aligned to the risk.

Sharing Contextual Information

The ability to have an enterprise’s cybersecurity tools work together to achieve instantaneous and automated mitigation exists today. It is often called “integration.” ForeScout calls it “orchestration.” Put simply, by providing the ability to share contextual insights and automate workflows and security processes between third-party security products, orchestration makes participating products smarter and greatly improves system-wide security effectiveness. Today, silos exist because cybersecurity vendors—often competitors—are neither required nor incentivized to create products that interoperate, thus requiring humans to connect the various outputs and totally defeating the concept of automation. The beauty of integration/orchestration is that it allows an enterprise to leverage information gleaned from across its network, including from and on its IoT devices. For example, if your firewall detects an intrusion at the network perimeter, you may want to have a way of scanning your device ecosystem for that particular code/malware. The role of orchestration in filling gaps, automating remediation and quarantining critical environments where a lot of IoT devices are connected cannot be overemphasized.

Orchestration aligns with several of the *NIST 800-53 Controls*, especially, Detect, Respond and Recover:

- ***DE.AE-1***: A baseline of network operations and expected data flows for users and systems is established and managed
- ***DE.DP-4***: Event detection information is communicated to appropriate parties
- ***RS.CO-3***: Information is shared consistent with response plans
- ***RC.IM-2***: Recovery strategies are updated

Compensating Controls: Other Considerations

Scalability/Automation. With the rapid growth in the number of IoT devices in nearly all enterprises, solutions must be able to scale indefinitely to support up to hundreds of thousands of devices. Tools must be chosen for their ability to function in an automated manner to reduce the amount of human involvement. Automation refers to a state in which enterprises allow their security tools to respond to threats automatically, without human intervention, according to previously established policies. Automation is key to monitoring and managing a large number of diverse devices and mitigating potential threats. Automation greatly reduces the reliance on the human facilitation of patching or removing malware, which can be time-consuming and prone to human error. Automation is essential when it comes to solving the IoT security problem.

Diverse IoT Environments. There is overwhelming diversity in the types of devices that different enterprises will employ in their environments. Each device ecosystem will encounter unique challenges in deploying compensating controls. For example, in more industrial-type organizations, older operating systems as well as controllers on the networks often don't support many newer security tools. In hospitals, where devices are managed under guidelines from both the manufacturer and the FDA, compensating controls should be deployed with these considerations in mind. The key is to understand that, even for what might be considered a "sensitive environment," some solutions exist (certainly for detection and segmentation) that require fewer network changes, are less disruptive, and are easier to deploy than others.

Information Security Continuous Monitoring. Enterprises need look no further than the tried-and-true NIST Cybersecurity Framework and SANS controls to get a handle on their device-related problems. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal information Systems and Organizations, defines continuous monitoring as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."[12] Two United States government programs, CDM and C2C, referenced earlier in this document, aim to implement ISCM across the entire government. Their requirements have become the de facto standard for how the USG secures IoT endpoints. And while the federal government has by no means "solved" the IoT security problem, it has taken an aggressive, enterprise-wide approach to it.

Conclusion

The attacks of 2016 are merely a preview of the damage that can be wrought through a large-scale DDoS attack. For practical purposes, we are just seeing the tip of the iceberg when it comes to these types of attacks. Why? Because hundreds of millions of vulnerable and corrupted devices are already connected to the Internet with no easy way to "fix" them. If we as a community fixate on fixing them, these types of attacks will continue to go unaddressed. We all wish manufacturers were more mindful of security and took care to embed even basic security in the devices they produce, both to protect the information they transmit and to prevent them from being recruited into DDoS attacks. But we can't afford to wait for market incentives or regulation to impose a solution that may not fully address the problem. As we wait, cybercriminals of all kinds—from solo hacktivists to criminal syndicates to foreign intelligence agencies—are successfully devising new viruses and attack methods to exploit newly introduced devices and software. Worse yet, billions of new IoT devices will come online in the next few years and without the actions described herein, practically all of these will be unsecured, providing an infinite potential for cyber-exploits.

We must encourage and promote the "security culture" everywhere, but we must also take action in the here and now to reduce the number of vulnerable devices worldwide that are fodder for DDoS attacks. We must focus on the stakeholder groups where this culture has the best chance of taking root. There is a lot that most end-users—everyone from business enterprises and government agencies to consumers—can do that they currently are not doing. The business case for tools that can secure IoT is very clear to our customers, for whom securing IoT is primarily about securing their high-value data and, increasingly, preserving their operations (which depend on healthy, functioning IoT). We must continue to equip them and consumers alike with the knowledge and tools to implement best practices to ensure IoT devices can continue to deliver – safely – their significant benefits. These best practices are not new: the frameworks we rely on for traditional IT environments absolutely apply to IoT. We must defang the myth that IoT is "unsecurable," and we cannot be distracted from the distant promise of "security by design."

About ForeScout

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of March 31, 2017 more than 2,400 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate multivendor response. Learn how at www.forescout.com.

[12] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf