SANS Institute
InfoSec Reading Room

Stopping IoT-based Attacks on Enterprise Networks

The increased use of IoT devices on business networks presents an growing challenge to security, and printers are an especially overlooked device from a security perspective. This paper examines specific attack areas for IoT devices, particularly printers, including data, management, monitoring and reporting, and make recommendations for protecting against various attacks.

SANS

A SANS Whitepaper

Stopping IoT-based Attacks on Enterprise Networks

Written by **G. W. Ray Davidson, PhD**

June 2018

Sponsored by:

HP

Introduction

Networks have evolved from simply connecting laptops, desktops and networking equipment to supporting new devices such as wearables, sensors and even smart cars. Employers increasingly allow users to connect their own devices to the organization's network, and in some cases they even require workers to purchase their own devices to do so.

Even as the network becomes more complex and varied, security and IT professionals have recognized that widely used devices, such as printers, physical security systems, HVAC control systems and point-of-sale devices, represent vulnerable potential attack surfaces.

All of these many and varied endpoints require active management, both for normal operations and for security. The increased diversity of the network translates not only into an increase in workload and resources, but also into the development and implementation of new tools and techniques for endpoint management, monitoring and reporting.

The increasingly prevalent use of IoT devices on business networks presents an increasing challenge to security.

The increased diversity is clearly shown in the results of the annual SANS endpoint surveys.[1,2] Not surprisingly, newer technologies such as smart sensors and employee-owned mobile devices are less likely to be covered under an organization's security/IR program. But in the 2016 report, a common networked device—the printer—was the least likely to be covered under an organization's security management program, and the results did not change significantly in the 2017 report. Considering the ubiquity of printers, this can represent a large vulnerability for an organization and deserves attention.

This whitepaper will examine specific attack areas, including data, management, monitoring and reporting, and make recommendations for protecting against various attacks. Given the lack of awareness surrounding printer security, one of the largest deployments of such endpoints, we will pay special attention to ensuring that those devices don't become attack vectors.

Device Vulnerabilities

Vulnerabilities will continue to multiply with the addition of new device types. Understanding exactly what bad actors are after, however, can help prevent IoT attacks.

New Device Types Are New Targets

New types of devices on the network create new surfaces for adversaries to attack and new vulnerabilities to defend. Internet of Things (IoT) attacks are becoming more advanced, following the same development path we've seen previously, from website defacement and DDoS to attacks for financial gain and espionage. And printers continue to be part of the wide world of IoT devices.

The first major attack against IoT devices was Mirai, which worked as a botnet apparently designed with the goal of denial of service.[3] Then came reports of Hide and Seek, which uses P2P techniques to build a structure designed for data exfiltration, among other things.[4] IoT attacks have even entered popular culture—the main character in the TV series "Mr. Robot" uses a Raspberry Pi device to gain access to the HVAC system in a large data center in order to threaten the security of corporate backup files.

For more conventional IoT devices, exploitation of printers has been known and discussed for almost two decades. The Phenoelit Group published tools for printer

---

[1] Davidson, G. W. Ray, "Can We Say Next-Gen Yet? State of Endpoint Security," March 2016, www.sans.org/reading-room/whitepapers/analyst/next-gen-yet-state-endpoint-security-36827

[2] Davidson, G. W. Ray, "Next-Gen Endpoint Risks and Protections: A SANS Survey," March 2017, www.sans.org/reading-room/whitepapers/analyst/next-gen-endpoint-risks-protections-survey-37652

[3] Antonakakis, Manos; April, Tim; Bailey, Michael; Bernhard, Matt; Bursztein, Elie; Cochran, Jaime; Durumeric, Zakir; Halderman, J. Alex; Invernizzi, Luca; Kallitsis, Michalis; Kumar, Deepak; Lever, Chaz; Ma, Zane; Mason, Joshua, Menscher, Damian; Seaman, Chad; Sullivan, Nick; Thomas, Kurt; Zhou, Yi; "Understanding the Mirai Botnet," Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada; August 2017.

[4] "New Hide 'N Seek IoT Botnet using custom-built Peer-to-Peer communication spotted in the wild," Bitdefender Labs, Jan. 24, 2018, https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild

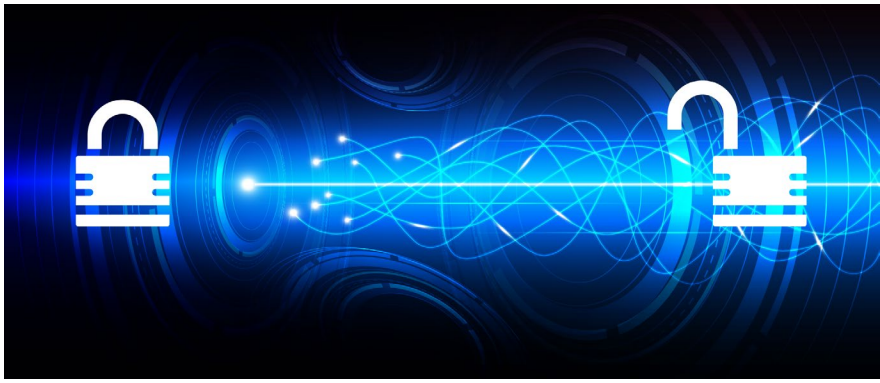
exploration and exploitation in the early 2000s.[5] Recently, Müller et al. published[6] a more general description of network printer exploitation and presented it at Black Hat 2017.[7]

IoT attacks will undoubtedly increase in 2018.[8] As users and security professionals, how should we understand the threat and prepare defenses and response plans? How can we prevent attacks? And when they occur, as they inevitably will, how can we best position ourselves to detect the attack and respond to minimize negative effects?

IoT Attack Surfaces Apply to Conventional Devices

Most of the new devices connecting to the network come under the heading of the IoT. Recognizing the increased network threat from these devices' diversity, the Open Web Application Security Project (OWASP) has created a subproject[9] to characterize risks and make recommendations for protection of networks that include IoT devices. The risks and recommendations also apply to conventional devices such as printers, and so they are included in the analysis presented here. The OWASP IoT project provides a comprehensive framework, and defines 15 different attack surfaces,[10] all of which should be considered and weighted based on the environment under consideration. For purposes of this analysis, we consider the most general and most common cases, as follows.

IoT Attacks Target Data



It's worth reiterating that the goal of any attack on a network is access to data. The ultimate target is usually data directly related to the business, such as financial information, R&D plans, customer data, personally identifiable information (PII) and protected health information (PHI). But device-related data can also be targeted as a means to reach the ultimate target. This approach targets the device itself, configuration data, or data about the users of the devices, such as login credentials.

Data exists on the network in two configurations: at rest and in transit. Data at rest includes data in files on storage media. This type of data can often be easily protected using encryption, provided that the decryption key is not readily available for exploitation. Data in transit includes the same data, which may normally be at rest but is in transit between storage locations, or on its way to an output device such as a printer, or perhaps an LED or LCD display. It also includes more ephemeral data, such as login or access credentials, or telemetry data from a sensor. Data in transit can be protected by encryption, but generally the means for decryption must exist at one end of the transit path, which presents an exploitable vulnerability.

---

[5] "PFT & Hijetter," www.phenoelit.org/hp

[6] Müller, J.; Mladenov, V.; Somorovsky, J.; and Schwenk, J., "SoK: Exploiting Network Printers," *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2017, pp. 213-230.

[7] "Exploiting Network Printers," www.youtube.com/watch?v=DwKzSO4yA_s

[8] "2018 forecast – CyberWire Special Edition," Jan. 26, 2018, www.thecyberwire.com/podcasts/cw-podcasts-special-2018-forecast.html

[9] The OWASP IoT Project, www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[10] IoT Attack Surface Areas, www.owasp.org/index.php/IoT_Attack_Surface_Areas

Prevention and Response to IoT attacks

Recognizing that IoT devices represent a new set of threats to the network, the Center for Internet Security has developed an Internet of Things Security Companion to the CIS Critical Security Controls.[11] As of this writing, it hasn't yet been updated to correspond to V7 of the Critical Security Controls, but the current version is still quite valuable for assessment and planning. (All the numbering below is consistent with V6.)

Inventory

The first step to preventing attacks on IoT devices is knowing that those devices are on the network in the first place. Control #1 – Inventory of Authorized and Unauthorized Devices is first for a reason. This control is especially important for IoT devices, because scanning the network for endpoints may pose a threat to non-PC devices, putting them into error states or causing them to shut down or reboot spontaneously.

As found in the SANS endpoint security surveys referenced earlier, many enterprises don't include IoT devices in their central device management processes, and even fewer include them in their security and incident management programs. As an example, only 60 to 70 percent of enterprises include printers in their device management solutions, and 40 to 50 percent of enterprises include them in their IR processes.

SANS surveys indicated that only 60 to 70 percent of enterprises include printers in their device management solutions, and 40 to 50 percent of enterprises include them in their IR processes.

The situation is complicated because some IoT devices use proprietary communications protocols with application-specific messaging and may require passive line or RF monitoring, or even manual audits. Thus, it may be very difficult to create and maintain an inventory of connected IoT devices via scanning; manual physical inventory may be necessary.

Architecture

Most authorities strongly recommend the use of segregation strategies such as VLANs to isolate IoT devices in general. Segregation is especially important for devices that cannot be updated regularly, such as laboratory research equipment, medical devices or critical manufacturing devices. For devices such as printers, which need to be accessed from standard user devices, it may be more appropriate to use firewalls or intrusion detection systems to control flow among different portions of the network. This guidance corresponds to Control #18 – Boundary Defense, referring not to the perimeter of the organization but to internal boundaries between and among internal networks.

Organizations should monitor for personal IoT-related traffic and take actions to deny that traffic when necessary.

Consistent implementation of this control may be complicated by the fact that employees often co-mingle IoT software on their corporate assets (laptops/phones) with their personal IoT devices (e.g., fitness trackers), or bring their personal IoT devices (e.g., smart TVs) directly into the network. This practice opens up command-and-control channels between the installed software and sites on the Internet used for data collection or management. Recent reports that fitness trackers worn by military personnel may have inadvertently revealed the location of military bases is a good, if extreme, example of the danger.

[11] "Internet of Things Security Companion to the CIS Critical Security Controls," www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-IoT-Security-Companion-201501015.pdf

Organizations should monitor for personal IoT-related traffic and take actions to deny that traffic when necessary.

Access Control

Many IoT devices require passwords to access system management functions. Some can be attached to a directory, such as Active Directory, to allow the use of domain administrator accounts and restrict the use of administrator privileges. If the use of a directory is not possible, strong passwords are essential, and account access must be audited.

This aspect of security can be especially challenging for IoT devices that are deployed in relatively public areas. Those devices also frequently require the use of shared accounts by the technicians who maintain them. In those cases, additional physical security, such as locks and manual auditing procedures, can serve as compensating controls.

All these suggestions fall under the guidance of several controls, including #5 – Controlled Use of Administrative Privileges, #14 – Controlled Access Based on Need to Know, #15 – Wireless Access Control and #16 – Account Monitoring and Control. If authentication to the IoT device is not required, which is occasionally the case, then the use of a compensating control such as physical access control should be considered mandatory.

Management

As noted in the 2016 and 2017 SANS endpoint surveys, a high percentage of IoT devices fall outside the existing central management processes of an organization, ranging from a low of 35 percent (for printers) to 80 percent or higher (for less common devices such as sensors, industrial control system and manufacturing-floor devices, HVAC, etc.). The ramifications of this situation go beyond the simple access management noted above.

Once an organization is aware of the presence of these devices on its network and has appropriately restricted their access to the network, it must actively manage them. Some devices will have no configuration options. But for a device with several instances on the network, it is advisable to determine a secure configuration, then store and maintain the configuration in a configuration management database (CMDB.) Then, when additional instances of the device are added to the network, they can be configured using that previously determined secure configuration. This procedure is covered in Control #3 – Secure Configurations for Hardware and Software.

In addition to maintaining a secure configuration for new deployments, devices should come under the organization's vulnerability assessment and patching program, as noted in Control #4 – Continuous Vulnerability Assessment and Remediation. When new threats or software configurations are available, however, testing in a production environment is often impractical and unadvisable. Collaborative or vendor laboratories are likely the best venues for testing. In addition, IoT software is often upgraded as a new flash image, rather than patched. This process may not be feasible over the network and require direct physical access. Whatever the case, digital signatures should be used and evaluated by the device prior to loading.

Monitoring

As noted above, IoT devices can add a substantial change in the attack surface and threat profile for an organization. Security teams needs to exercise their collective imagination to create potential threat models and defenses. These models will determine the monitoring strategy as well. Conventional devices can often accommodate the use of agents on the host; IoT devices are not likely to support that model. IoT devices may use unique protocols, so monitoring of normal network traffic may not provide necessary visibility into activity involving the devices. And direct query of the device may be problematic, since standard query methods may put the device into an error state or disable the device.

Defense

Control #8 – Malware Defense addresses the specific problem of malware infecting and then running on an IoT device. Most IoT devices have limited processing power, so both malware infection and implementation of malware protections can be seriously problematic. In addition, with the exception of devices running a more or less full Linux stack, there have not been significant examples of exploits targeting specific IoT targets. This will likely change, however, as individual IoT technologies achieve more widespread deployment. As this report is being written, for example, researchers have announced proof of concept to hack Amazon's Alexa to allow it to spy on users.[12]

While it may not be possible to implement onboard monitoring, observation of network traffic can provide a useful substitute. If malware infection is possible, a primary vector will likely be through subversion of patching or firmware updates. Organizations should pay serious attention to supply chain risk management to prevent this intrusion.

Reporting

Control #6 – Maintenance, Monitoring and Analysis of Audit Logs discusses the necessity of a reporting capability to facilitate monitoring. Ideally the monitoring and response capability are centralized and integrated within an organization, so normalization of the reporting artifacts is critical. If the device includes a reporting capability such as syslog or syslog-ng, this probably can be integrated into the organization's larger monitoring capability, though coding of logs may be necessary to make them useful. XML- or JSON-formatted logs can facilitate this integration. Some devices may require the use of out-of-band logging and reporting, but these should still be integrated into the central reporting infrastructure to facilitate response coordination.

[12] Researchers Hacked Amazon's Alexa to Spy on Users, Again," Threat Post, April 25, 2018, https://threatpost.com/researchers-hacked-amazons-alexa-to-spy-on-users-again/131401

Recommendations

The increasingly prevalent use of IoT devices, including printers, on business networks presents an increasing challenge to security. To address this increased challenge, organizations should do the following:

- Maintain an accurate inventory of IoT and other hardware devices on the network. You can't manage what you can't see.
- Control access to the potentially problematic devices through physical and/or logical isolation and account-related controls, utilizing directory protocols where possible.
- Actively manage the devices, preparing new devices with a standard configuration prior to adding them to the network, and incorporating them into the vulnerability assessment and patching process at deployment.
- Continuously monitor the devices, either via onboard host defenses and logging or by observing network traffic involving the devices.
- Integrate the reporting capability from these newer types of devices into the existing, preferably centralized, reporting and response capability of the organization.

IoT devices are here to stay. It's preferable to generalize existing processes to accommodate the newcomers, rather than creating "separate but equal" processes that will have to be merged later.

About the Author

G. W. Ray Davidson, PhD, is the former dean of academic affairs for the SANS Technology Institute. He continues to serve as a mentor, subject matter expert and technical reviewer for the SANS Institute and holds several GIAC certifications. Ray started his career as a research scientist and subsequently led global security projects for a major pharmaceutical company. He has taught at the college level and worked at a security startup. Ray currently works with clients to develop and implement network security monitoring and threat intelligence capabilities. He is also active in the leadership of the Michigan Cyber Civilian Corps.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: July 20th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced