Insight

The Printer Is an Endpoint: Proactively Addressing the Security Vulnerability

Tom Austin
Frank Dickson
Robert Ayoub
Robert Westervelt

IDC OPINION

Non-PC-connected devices are receiving increased attention from security practitioners as cybermiscreants are increasingly leveraging them as gateways into our networks or as instruments of attack. These devices, often included in the category of Internet of Things (IoT), require the same level of care, attention, and protection as other devices in our enterprise networks. Printers are IoT devices that are highly vulnerable to attack because of the requirements of keeping them open and accessible to the entire organization. Attackers seize on the lack of attention given to printer security relative to other devices and peripherals on enterprise networks. Thus printers should receive the same attention as any other network endpoint, with the following steps to be given immediate priority:

- **Inventory:** The organization should compile a complete inventory of all printers, brand, model, features, and configurations.
- **Harden:** Shut off unneeded services that the printer offers and manage passwords.
- **Maintain and patch:** Maintaining and patching printer endpoints create harder targets, pushing cybermiscreants to use their tools on organizations that have not maintained their systems.
- **Secure the connection:** Shore up the management protocols used for the printer.

IN THIS INSIGHT

This IDC Insight highlights the vulnerable nature of printers in our enterprise networks and provides steps to reduce the risk they pose to the business.

SITUATION OVERVIEW

Current Environment

The attention given to Internet-of-Things security grew significantly following a series of high-profile distributed denial-of-service (DDoS) attacks that focused a high volume of malicious traffic from thousands of compromised surveillance cameras, digital video recorders, and other connected devices to bring down popular websites. The volume of the traffic is historically significant. The attack methodology was noteworthy.

Attackers seized on poor security hygiene, using malware to exploit vulnerabilities that should have been patched or configuration errors that opened up weaknesses. The task for the cybermiscreant was an easy one. In many cases, those that deployed the devices failed to change default passwords. Attackers leveraged bots to quickly identify these devices on the internet and connected them, creating

a dangerous botnet. The reality is that the IPv4 space is not that big and even low-skilled cybercriminals can scan the entire space in short order and compromise devices with default passwords like username "root" and password "root." The ease and scale of a compromise is scary. As we look for other IoT devices that share some of the characteristics of those that have been used in the latest attacks, attention is drawn to consumer, small business, and enterprise printers.

Many IT professionals may think of IoT as only applying to certain verticals or device types. As a result, IT teams may simply mitigate risk by addressing access rights to secure such IoT devices. These recent DDoS attacks illustrated, however, that there are now many devices with universal access to the network that are not properly secured and maintained. Printers fall squarely into this category. Typically, all employees have access to a variety of devices. Software updates and access control on printers are often overlooked compared with traditional IT products. Printers may be the next vector for a large IoT attack but could pose new dangers to business operations because they reside inside the corporate network, offering the potential for data theft and DDoS on the internal portion of a network.

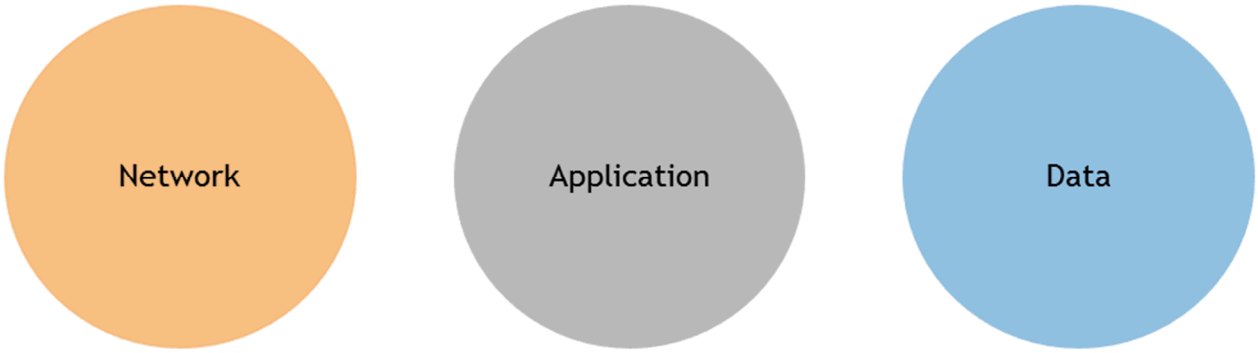
Your Printer Is an Endpoint!

Please consider this scenario. An unknown device is placed into an enterprise network, behind network perimeter defenses like firewalls, IPS, and other IT infrastructure, so that the device has unfettered access to all the corporate network resources. To maximize the device's functionality, a web server is embedded into the device. To make the device accessible, all the ports will be set as "open" by default and enable the connectivity with as much as a gigabit of Ethernet connectivity. The device will have a rich OS-like Linux to maximize functionality. The device will not be examined on an ongoing basis using the enterprise's vulnerability scanner as the embedded web server will likely light up the organization's SIEM tools like a Christmas tree with false positives. The vulnerability scanner will be configured to ignore the devices, leading to the conclusion, depending on the brand, that the device will not be updated, maintained, or patched over 5-year useful life or sometimes 10-year useful life of the device. Device protection will consist of a default password, and unvetted third parties will maintain the device. The device will be core to organizational productivity, so there will be one of these devices for every 10 employees. Some might call this a nightmare; some might call this a printer.

A very important point needs to be clarified. "Print security" is a mature security discipline, driven for the most part for the need for data security. As one may assume, compliance standards play a strong role in driving the print security discipline, especially the Big 4: Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST), and the ISO 27000 family of standards. These standards provide guidelines for managing sensitive and value company information, including topics such as encryption and access management. Figure 1 shows the classic disciplines of cybersecurity.

FIGURE 1

Classic Disciplines of Cybersecurity



Source: IDC, 2016

Printer security, as opposed to print security, is solely focused on physical devices associated with printing and is a network security discipline. Printer security views the printer as an endpoint, treating the printer with the same care as any other endpoint such as notebooks, servers, and mobile devices. Although they share a common vernacular and have some related areas of concern, print security and printer security are unique disciplines.

How Vulnerable Are Network Printers?

Management Lacking

Printers are a juicy target for cybermiscreants; several reasons drive this conclusion. First, printers often do not command much attention by security personnel; after all, they are "only printers." When we look at the issue from a historical context, printers and copiers were often not considered part of IT. The management was considered part of facilities function. When they became networked devices, as long as the devices were behind the enterprise firewall, they were largely considered "low risk." As our enterprise network security perimeters transitioned to a state of decreasing effectiveness, the multitude of issues that arose, such as increasingly sophisticated malware, dominated mind share and the vulnerability of print endpoints went under identified.

Larger Attack Surface

The second issue compounds the problem of a lack of attention in our post Stuxnet security reality. Combination printer/scanner/fax machines are increasingly sophisticated, and they have general-purpose computers installed inside to control all of the action. Windows and Linux systems are often built into many modern printers. Because these computer controllers get little hardening and patching attention, they are often vulnerable. In addition, functionality requires connectivity which results in many printers being shipped with a multitude of open ports to support usability. Here are some of the ports that may ship "open":

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 137 (WINS)
- UDP 161 (SNMP)

- UDP 162 (SNMP Traps)
- TCP 515 (LPR/LPD)
- TCP 631 (IPP)
- TCP 5000 (XML)
- TCP 5001 (IPDS)
- UDP 5353 (MDNS)
- TCP 8000 (HTTP)
- TCP 9000 (Telnet)
- TCP 9100 (Raw Print)
- TCP 9200 (IR Alerts)
- UDP 9200 (Discovery)
- UDP 9300 (NPAP)
- TCP 9400 (Lexmark Print Port)
- TCP 9500 (NPAP)
- TCP 9600 (IPDS)
- UDP 9700 (Plug-n-Print)
- TCP 10000 (Telnet)
- And many others

A lack of attention combined with powerful computing power and a potpourri of connective options means that attackers can access printers in several ways, such as a modem, wireless access point, or through a jump-off from spyware-infected desktops. After gaining access, they can use this power to hit other machines on your internal network or participate in a distributed denial of service. Most printers have unfettered access to an internal network. Thus an attacker who compromises a printer can scan all over for exploitable systems.

As with other endpoint devices requiring protection, printers are more than just a "gateway" for cybermiscreants but also a target. Printers often store sensitive documents in their print spool. Printers are often combined with a document scanner, too, and docs are often stored in the scanning archive for far longer than most people expect. The following list calls out many of the issues of concern for security professionals associated with printers:

- BIOS, operating system, and firmware
- Centralized printer management
- Network (wired and wireless) and peripheral connectivity
- Control panel
- Hard disk and removable storage media
- Capture
- Specialized and standard media input trays
- Output trays
- Remote, BYOD, and mobile printing

FUTURE OUTLOOK

Recommendations

If printer security has not been a focus for your organization, IDC has some recommendations of where to start.

It All Begins with Visibility

As with any endpoint requiring security, you should start with the basics, and step one is always visibility. The organization should compile a complete inventory of all printers, brand, model, features, and configurations. With printers, such a list can be problematic as individual initiative often places printers in unidentified places (shadow IT). Labs, executive offices, or field service offices will often place a printer on the network for their convenience, regardless of the implications that it has on security.

Ideally, your endpoint inventory of printers will be derived from a network access controller (NAC) or asset management tool, which has device discovery as core functionality. Truly comprehensive visibility of printers is extremely difficult without a NAC. Granted, some models of printer can provide for network autodiscovery when they are connected to the network, with the operative word being some. If your network environment is not fortunate enough to include a homogenous installed base of such printers, a NAC is the way to go.

Harden Your Printer Endpoints

Printers within the organization must be managed just as any other connected endpoint. Shut off any unneeded services that the printer offers, such as File Transfer Protocol (FTP). Most organizations do not need FTP access to their printers, and it can often cause more harm than good. For instance, some printers allow an attacker to make FTP requests and take jobs off of a print spool anonymously. Also, many FTP services on modern printers are subject to FTP bounce attacks. With a tool like Nmap (Network Mapper), an attacker can obscure the source of a port scan, convincing a compliant FTP server to allow proxy FTP connections. While such FTP bounce scans are old techniques, a remarkable number of brand-new print servers are susceptible to such attacks.

However, the single most important activity in hardening printer endpoints is password management; if an organization does nothing else, they should at least address this. The single most egregious mistake made by organizations is failing to change the default passwords. According to the 2016 Verizon Data Breach Investigations Report (DBIR), 63% of confirmed data breaches involved leveraging weak/default/stolen passwords. If printers are managed by facilities or third-party vendors, convenience is paramount (for them). When a device needs to be maintained, finding a password can be an issue. When there is one printer for every 10 employees, an organization with 10,000 employees can have 1,000 passwords to maintain. Security, thus, gives way to convenience (not the first or last time you will hear that). Password management though is not just a failing of non-technical staff. The second most egregious mistake made is having the user name and password freely accessible in unencrypted text, freely available to anyone with an http:// connection.

Maintain and Patch

The vast majority of breaches occur because of a lack of hygiene. According to the 2016 Verizon Data Breach Investigations Report (DBIR), the top 10 exploited vulnerabilities in 2015 accounted for 85% of successful exploit traffic. The important fact is that most exploited vulnerabilities are known and

publicly disclosed. Cybermiscreants will use what works and maximize the investment that they have made in their malware tools. Cybermiscreants are business people, looking for an ROI from their efforts.

Maintaining and patching printer endpoints will make you a harder target, pushing cybermiscreants to use their tools on organizations that have not maintained their systems. To borrow a metaphor, sometimes, it makes sense to not worry about outrunning the bear: worry about outrunning the guy (organization) next to you.

When it comes to patching, not all printers are created equal. Some manufacturers offer management tool sets that will allow you to monitor, manage, and patch some make and model of printers. Such tool sets are extremely valuable as, alluded to earlier, an enterprise's vulnerability scanner will likely have issues with printers because of the embedded web server. To prevent "noise" from being imported into the SIEM tools, vulnerability scanners are often configured to ignore printers. If you happen to have such printers with robust management tool sets, you are in luck. If not, you may have to manually patch each printer using "sneakernet" as cobbling together an automated solution may be difficult.

Secure the Connection

Shore up the management protocols used for the printer. Most modern printers support some sort of management via HTTP and/or HTTPS, and a few even support Telnet or Secure Shell (SSH). Carefully choose a management protocol that provides encryption, like HTTPS or SSH.

Last, make sure that your printer does not have wide-open access to the rest of your internal network. Segmenting our enterprise networks is a network security best practice, and your printers need to be included in the effort. Consider putting your printers on their own private VLAN. Filter access to that VLAN so that the printer can receive print jobs but not initiate connections to any other systems. If you have the budget and the time, you can even put a firewall in front of your printers to really limit access to and from them.

Conclusion

Printers have not received the attention that other cybersecurity threat vectors received. The vulnerability and the corresponding threat is real, very real. Organizations of all sizes must take steps to address the concern and address it quickly. Cybermiscreants are voracious copycats. Once a threat vector has been exploited for gain by one malicious actors, others follow quickly.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com