Are you concerned about printer security?

You should be.

Lindsey Hearst
Print Security Advisor, Channel Lead
April 29, 2019 dy, 2018

NSA Presentation at RSA 2018

- 93% of 2017 incidents were preventable with best practices
- In 2018, NSA stated 90% of cyber incidents are due to human error

United Kingdom National Audit Office

- 80% of cyber attacks are preventable with basic cyber hygiene

GOOD CYBER HYGIENE

Security by Obscurity

If no one notices the printer is vulnerable, then it isn't vulnerable.


VS.
SERIES

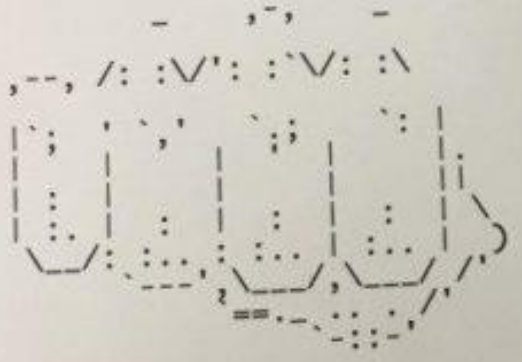
--- WHAT IS GOING ON ---

PewDiePie, the currently most subscribed to channel on YouTube, is at stake of losing his position as the number one position by an Indian company called T-Series, that simply uploads videos of Bollywood trailers and songs.

--- WHAT TO DO ---

1. Unsubscribe from T-Series
2. Subscribe to PewDiePie

3. Share awarness to this issue #SavePewDiePie
4. Tell everyone you know. Seriously.
5. BROFIST!



--- EXTRA POINTS ---

1. Subscribe to Dolan Dark

2. Subscribe to grandayy

3. Hit that dab like Wiz Khalifa
4. Delete TikTok

5. Smile, the world is a great place.
6. Nevermind it's 2018 and we're all gonna die

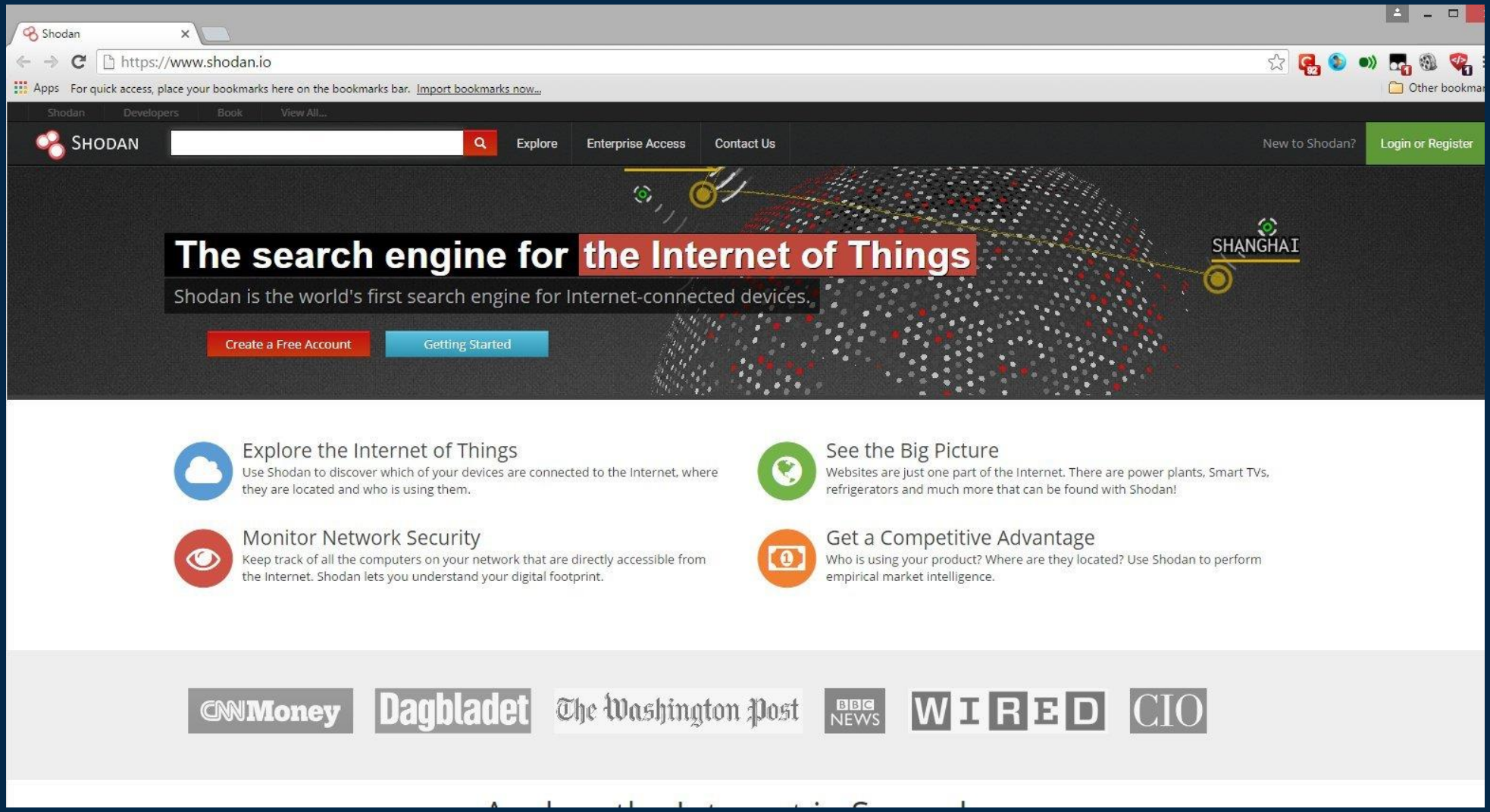
The risk is real

It’s easy for hackers to break into unsecured printers

“I probe around for a multifunction printer and see that it is configured with default passwords. Great, I am in…”

“We've compromised a number of companies using printers as our
initial foothold. We move laterally from the printer, find Active Directory, query it with an account from the printer and bingo, we hit GOLD…”

Peter Kim
Industry-leading penetration
Tester, Hacker, Author


Shodan
https://www.shodan.io
Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Shodan Developers Book View All...
SHODAN
Explore
Enterprise Access
Contact Us
New to Shodan?
Login or Register
The search engine for the Internet of Things
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
SHANGHAI
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.
CNNMoney
Dagbladet
The Washington Post
BBC NEWS
WIRED
CIO

Common imaging and printing vulnerability points

BIOS and firmware
Compromised firmware can open a device and network to attack

Management
Undetected security gaps put data at risk

Network
Jobs can be intercepted as they travel to/from a device

Control panel
Users can exploit device settings and functions

Ports and protocols
Unsecured ports (USB or network) or protocols (FTP or Telnet) put device at risk

Storage media
Printers store sensitive information that can be at risk

Capture
Unsecured MFPs can be used to send scans anywhere

Input tray
Special media can be tampered with or stolen

Output tray
Abandoned documents can fall into the wrong hands

Mobile printing
On-the-go employees may expose data

The world's most secure printing*

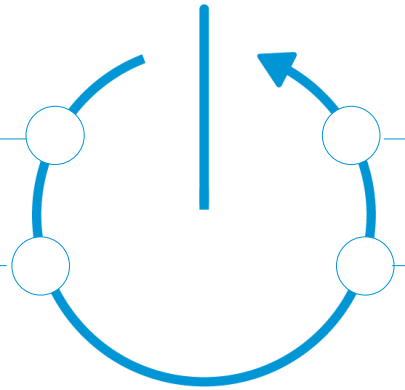
Real-time threat detection, automated monitoring, and built-in software validation

1. Check BIOS/boot code

Prevents the execution of malicious code during bootup by allowing only HP-signed, genuine code to be loaded

2. Check firmware

Allows only authentic, good firmware—digitally signed by HP—to be loaded



3. Check printer settings

After a reboot, HP JetAdvantage Security Manager checks and fixes any affected security settings

4. Continuous monitoring

Protects operations and stops attacks while device is running

Inspects outgoing network connections to stop suspicious requests (Enterprise only)

HP Labs

HP Sure Start

During startup, the integrity of the boot code or BIOS is validated

Whitelisting

When loading firmware, only authentic, good code—digitally signed by HP—is loaded

Run-time intrusion detection

During run-time, HP printers detect and prevent unexpected changes to memory

HP Labs

HP Connection Inspector

When connecting to the network, HP Enterprise printers put a stop to suspicious requests

Self-healing HP Enterprise and Managed printers can automatically repair themselves from attack in real time

HP JetAdvantage Security Manager

automatically assesses and remediates device security settings

Common imaging and printing vulnerability points

BIOS and firmware
Compromised firmware can open a device and network to attack

Management
Undetected security gaps put data at risk

Network
Jobs can be intercepted as they travel to/from a device

Control panel
Users can exploit device settings and functions

Ports and protocols
Unsecured ports (USB or network) or protocols (FTP or Telnet) put device at risk

Storage media
Printers store sensitive information that can be at risk

Capture
Unsecured MFPs can be used to send scans anywhere

Input tray
Special media can be tampered with or stolen

Output tray
Abandoned documents can fall into the wrong hands

Mobile printing
On-the-go employees may expose data

TOTAL CVE Entries: 109284

CVE-2018-17310	On the RICOH MP C1803 JPN printer, HTML Injection and Stored XSS vulnerabilities have been discovered in the area of adding addresses via the entryNameIn parameter to /web/entry /en/address/adrsSetUserWizard.cgi.
CVE-2018-17309	On the RICOH MP C406Z printer, HTML Injection and Stored XSS vulnerabilities have been discovered in the area of adding addresses via the entryNameIn parameter to /web/entry /en/address/adrsSetUserWizard.cgi.
CVE-2018-17002	On the RICOH MP 2001 printer, HTML Injection and Stored XSS vulnerabilities have been discovered in the area of adding addresses via the entryNameIn parameter to /web/entry /en/address/adrsSetUserWizard.cgi.
CVE-2018-17001	On the RICOH SP 4510SF printer, HTML Injection and Stored XSS vulnerabilities have been discovered in the area of adding addresses via the entryNameIn parameter to /web/entry /en/address/adrsSetUserWizard.cgi.
CVE-2018-15748	On Dell 2335dn printers with Printer Firmware Version 2.70.05.02, Engine Firmware Version 1.10.65, and Network Firmware Version V4.02.15(2335dn MFP) 11-22-2010, the admin interface allows an authenticated attacker to retrieve the configured SMTP or LDAP password by viewing the HTML source code of the Email Settings webpage. In some cases, authentication can be achieved with the blank default password for the admin account. NOTE: the vendor indicates that this is an "End Of Support Life" product.
CVE-2018-14903	EPSON WF-2750 printers with firmware JP02I2 do not properly validate files before running updates, which allows remote attackers to cause a printer malfunction or send malicious data to the printer.
CVE-2018-14900	On EPSON WF-2750 printers with firmware JP02I2, there is no filtering of print jobs. Remote attackers can send print jobs directly to the printer via TCP port 9100.
CVE-2018-14899	On the EPSON WF-2750 printer with firmware JP02I2, the Web interface AirPrint Setup page is vulnerable to HTML Injection that can redirect users to malicious sites.
CVE-2018-10326	PrinterOn Enterprise 4.1.3 suffers from multiple authenticated stored XSS vulnerabilities via the (1) department field in the printer configuration, (2) description field in the print server configuration, and (3) username field for authentication to print as guest.
CVE-2018-1000537	Marlin Firmware Marlin version 1.1.x and earlier contains a Buffer Overflow vulnerability in cardreader.cpp (Depending on branch/version) that can result in Arbitrary code execution. This attack appear to be exploitable via Crafted G-Code instruction/file is sent to the printer.
CVE-2017-7998	Multiple cross-site scripting (XSS) vulnerabilities in Gespage before 7.4.9 allow remote attackers to inject arbitrary web script or HTML via the (1) printer name when adding a printer in the admin panel or (2) username parameter to webapp/users/user_reg.jsp.
CVE-2017-2788	A buffer overflows exists in the psnotifyd application of the Pharos PopUp printer client version 9.0. A specially crafted packet can be sent to the victim's computer and can lead to a heap based buffer overflow resulting in potential remote code execution. This client is always listening, has root privileges, and requires no user interaction to exploit.
CVE-2017-2787	A buffer overflows exists in the psnotifyd application of the Pharos PopUp printer client version 9.0. A specially crafted packet can be sent to the victim's computer and can lead to a heap based buffer overflow resulting in potential remote code execution. This client is always listening, has root privileges, and requires no user interaction to exploit.
CVE-2017-2786	A denial of service vulnerability exists in the psnotifyd application of the Pharos PopUp printer client version 9.0. A specially crafted packet can be sent to the victim's computer and can lead to an out of bounds read causing a crash and a denial of service.
CVE-2017-2785	An exploitable buffer overflow exists in the psnotifyd application of the Pharos PopUp printer client version 9.0. A specially crafted packet can be sent to the victim's computer and can lead to a heap based buffer overflow resulting in remote code execution. This client is always listening, has root privileges, and requires no user interaction to exploit.
CVE-2017-15400	Insufficient restriction of IPP filters in CUPS in Google Chrome OS prior to 62.0.3202.74 allowed a remote attacker to execute a command with the same privileges as the cups daemon via a crafted PPD file, aka a printer zeroconfig CRLF issue.

Firmware Vulnerability Assessment

Summary | Devices | Bulletins

Status	Description	Devices	Percent
OK	FW has no known security bulletins, supported, and no more than 1 revision out of date	0	0%
Out-of-date	FW has no known security bulletins, supported, but is more than 1 revision out of date	0	0%
Reactive Support	FW has no known security bulletins; only FW fixes addressing prioritized security risks	12	3%
Bulletin	FW has a known security bulletin	107	28%
	Reactive Support: 19		
	Non-Reactive Support: 88		
No Firmware	No Firmware Update	0	0%
No data	No/manual data collection	0	0%
Not evaluated	Insufficient information was available to evaluate	258	68%
	Because model not yet evaluated: 0		
	Because model not recognized: 215		
	Because firmware version missing: 0		

Hospital

Status	Description	Devices	Percent
OK	FW has no known security bulletins, supported, and no more than 1 revision out of date	12	0%
Out-of-date	FW has no known security bulletins, supported, but is more than 1 revision out of date	12	0%
End of Support	No longer publishing regularly scheduled firmware updates	208	8%
Bulletin	FW has a known security bulletin	822	33%
	End of Support: 242		
	Upgradeable: 580		
No Firmware	No Firmware Update	0	0%
No data	No/manual data collection	0	0%
Not evaluated	Insufficient information was available to evaluate	1410	57%
	Because model not yet evaluated: 0		
	Because model not recognized: 3		
	Because firmware version missing: 3		
	Because firmware version mismatch: 0		
	Because firmware version not recognized: 1404		

University

Status	Description	Devices	Percent
OK	FW has no known security bulletins, supported, and no more than 1 revision out of date	0	0%
Out-of-date	FW has no known security bulletins, supported, but is more than 1 revision out of date	1	0%
End of Support	No longer publishing regularly scheduled firmware updates	58	15%
Bulletin	FW has a known security bulletin	144	38%
	End of Support 48		
	Upgradeable 96		
No Firmware	No Firmware Update	0	0%
No data	No/manual data collection	0	0%
Not evaluated	Insufficient information was available to evaluate	181	47%
	Because model not yet evaluated 0		
	Because model not recognized 92		
	Because firmware version missing 2		
	Because firmware version mismatch 0		
	Because firmware version not recognized 87		

Common imaging and printing vulnerability points

BIOS and firmware
Compromised firmware can open a device and network to attack

Storage media
Printers store sensitive information that can be at risk

Management
Undetected security gaps put data at risk

Capture
Unsecured MFPs can be used to send scans anywhere

Network
Jobs can be intercepted as they travel to/from a device

Input tray
Special media can be tampered with or stolen

Control panel
Users can exploit device settings and functions

Output tray
Abandoned documents can fall into the wrong hands

Ports and protocols
Unsecured ports (USB or network) or protocols (FTP or Telnet) put device at risk

Mobile printing
On-the-go employees may expose data

Types of policy settings

250+ security settings in HP enterprise MFPs

File system access protocols

Device control

Direct connect ports

Control panel lock

Fax speed dial lock

File erase mode

Authentication services

LDAP Server Authentication

802.1x Authentication

FTP Firmware Update

Network Services

Remote Firmware upgrade

Novell remote configuration

Telnet

Job storage authentication

Authentication

Job creation authentication

Send to e-mail authentication

Send to folder authentication

Service Location Protocol (SLP)

Bonjour

Web Services Discovery (WS-Discovery)

Device discovery

Link-Local Multicast Name Resolution Protocol

PJL password

SNMPv1/v2

SNMPv3

Device PIN presence

Credentials

Admin (EWS) password

File system password

Fax PIN

Bootloader password presence

Public username

Credential type

Email

Allow return email address change

Secondary email authentication

Restrict Addresses

Maximum attachment size

TCP/IP Printing (P9100)

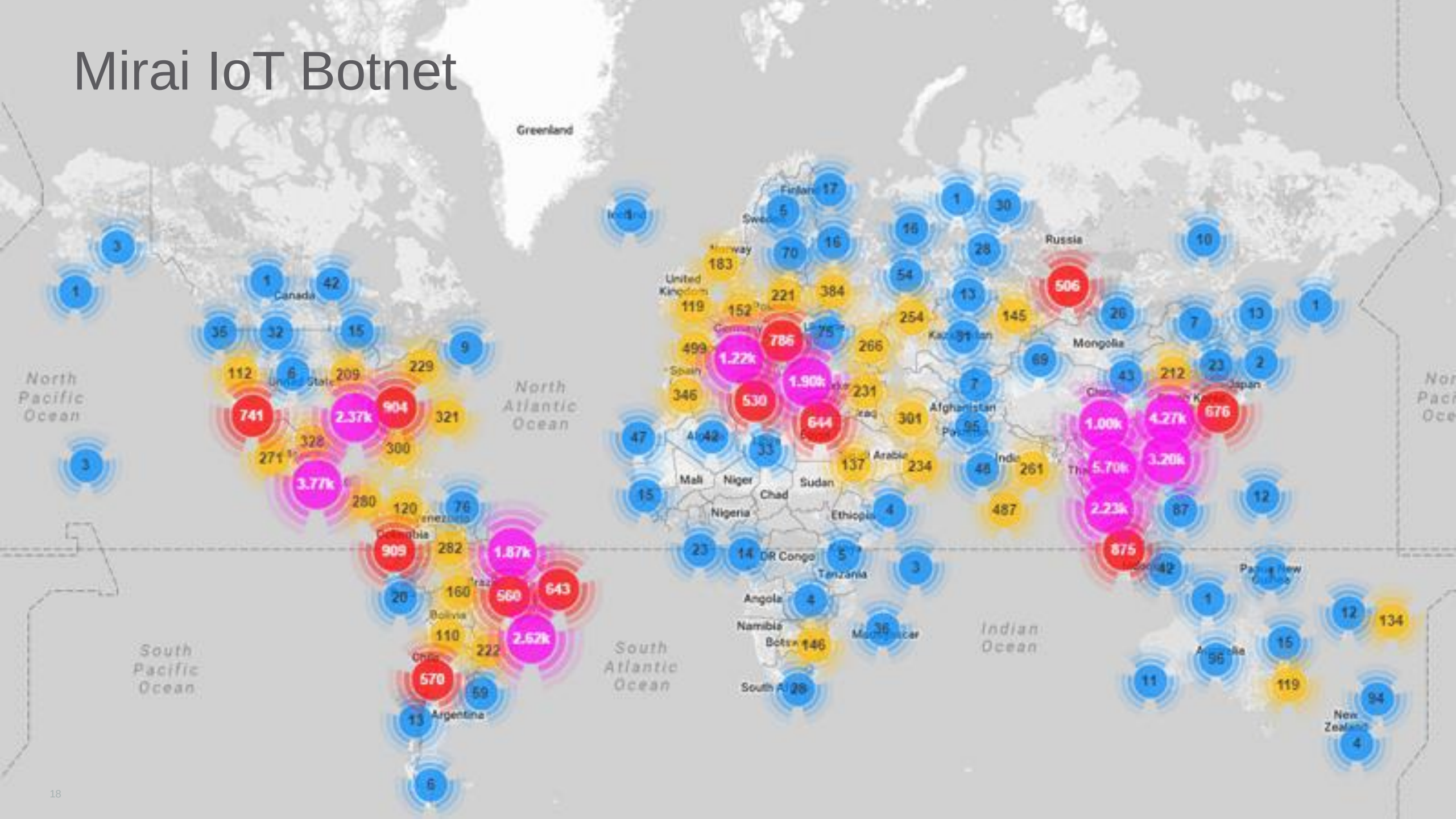
Printing

File Transfer Protocol

Internet Printing Protocol

Novell (IPX/SPX)

Mirai IoT Botnet



You may have the security tools and technologies, but are you …

- Encrypting in-transit data?
- Protecting hard drives?
- **Keeping firmware updated**?
- Erasing hard disks on decommissioned devices?

- **Able to implement best practices with limited IT resources with little print security expertise?**

- **Complying with industry and government regulations?**

- Configuring interfaces and credentials?
- **Managing admin passwords?**
- Managing with existing network security tools?

THANK YOU

Contact information

Disclaimers and trademarks

Disclaimers

$11.7M average annualized cost of cybercrime: Ponemon Study sponsored by HPE, "2017 Cost of Cyber Crime," 2017. accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

163 ZB by 2025: IDC forecasts that by 2025 the global datasphere will grow to 163 zettabytes (IDC, Data Age 2025, 2017), https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.

95% of new electronic designs will include IoT: By 2020, IoT technology will be in 95% of electronics for new product designs. Gartner, Smarter with Gartner, Gartner Top Strategic Predictions for 2018 and Beyond, October 3, 2017.

7.9B records exposed: 2017 saw more than 5,200 breaches that exposed nearly 7.9 billion records. 2017 Year End Data Breach QuickView Report by Risk Based Security / Cyber Risk Analytics, January 2018.

29K vulnerable printers: Washington Times, "Hackers target US Universities sending anti-Semitic flyers to printers," 2016, antisemitismwatch.com/tag/the-washington-times.

43% of companies ignore printers in their endpoint security practices. Only 16% of companies think printers are a high security risk: Spiceworks survey of 309 IT decision-makers in North America, EMEA, and APAC, on behalf of HP, November 2016.

61% of organizations reported at least a single print-related data breach in the past year: Quocirca, "Managed Print Services Landscape, 2016," quocirca.com/content/managed-print-services-landscape-2016, July 2016.

94% of financial firms say copier/printer security is important or very important: InfoTrends, "Designing Hardware & Solutions," Brendan Morse, October 2016.

HP Access Control must be purchased separately. To learn more, please visit hp.com/go/hpac.

HP FutureSmart feature availability: Some features enabled by future HP FutureSmart upgrades may not be available on older devices if, for example, physical product characteristics limit the functionality of the new feature.

HP JetAdvantage Insights is a web-based application that requires Internet access. Supported browsers include recent versions of Microsoft® Internet Explorer®, Google Chrome™, Mozilla® Firefox®, and Safari®. Learn more about HP JetAdvantage Insights at hp.com/go/JetAdvantageInsights.

HP JetAdvantage Private Print is available at no charge and requires that the printer be connected to the Internet with web services enabled. It is supported on devices with touchscreens. Not available in all countries. Learn more at hp.com/go/JetAdvantagePrivatePrint.

HP JetAdvantage Secure Print works with any network-connected printer or MFP. On-device authentication is available for many HP LaserJet, PageWide, and OfficeJet Pro devices. Some devices may require a firmware upgrade. Internet connection required for cloud storage and retrieval of print jobs. Print-job release from a mobile device requires a network connection and QR code. For more information, see hp.com/go/JetAdvantageSecurePrint.

HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

hp.com/go/documentmanagement.

HP Web Jetadmin is available for download at no additional charge at hp.com/go/webjetadmin.

"IDC MarketScape: U.S. Smart Multifunction Peripheral 2018 Vendor Assessment," Keith Kmetz, Max Pepper, February 2018. (Link to the report: http://www8.hp.com/us/en/business-services/managed-print-services/analysts-corner-idc.html)

"IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment," Robert Palmer, Allison Correia, October 2017. (Link to the report: http://idcdocserv.com/US41988517e_HP)

Limited multivendor setting support for HP Print Governance and Compliance Service: 13 Top Priority Security Settings as determined by Security Experts (EWS password, SNMP V1/V2, SNMP V3, AppleTalk, etc.).

Most comprehensive device, data and document security: Includes device, data and document security capabilities by leading managed print service providers. Based on HP review of 2017 publicly available information on security services, security and management software and device embedded security features of their competitive in-class printers. For more information visit: hp.com/go/MPS securityclaims or hp.com/go/mps.

Only HP offers a governance and compliance service: Based on HP internal research on competitor offerings of governance and compliances services. As of August 2016, only HP offers a service specifically for print devices.

Percent of end-point breaches has more than doubled in the last 6 years: Verizon, 2016 Data Breach Investigations Report, 2016. verizonenterprise.com/verizon-insights-lab/dbir/2016

Pro embedded security features: Select HP LaserJet Pro, OfficeJet Pro, and PageWide Pro devices include embedded features that can detect and stop an attack. For more information, please visit hp.com/go/PrintersThatProtect.

Quocirca, Print2025, Louella Fernandes, January 2018. (Link to the report: http://www8.hp.com/us/en/business-services/managed-print-services/analysts-corner-quocirca.html)

Remediation SLA: HP will endeavor to remotely provide 97% compliance remediation ("Remediation SLA") for all qualifying devices that are viewable and remain in reporting status on the DCA. Any device that has security policies set to "detect presence only" and/or deemed to be a Non-Reporting Device at any time 30 days prior to Remediation SLA measurement, shall not be included in the measurement for the Remediation SLA.

The world's most secure printers: HP's most advanced embedded security features are available on HP Enterprise-class and Managed devices with FutureSmart firmware 4.5 or above and is based on HP review of 2017 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/printersecurityclaims.

Trademarks

Android and **Google Chrome** are trademarks of Google Inc.

Microsoft is a U.S. registered trademark of the Microsoft group of companies.