KNOW YOUR IoT SECURITY RISK

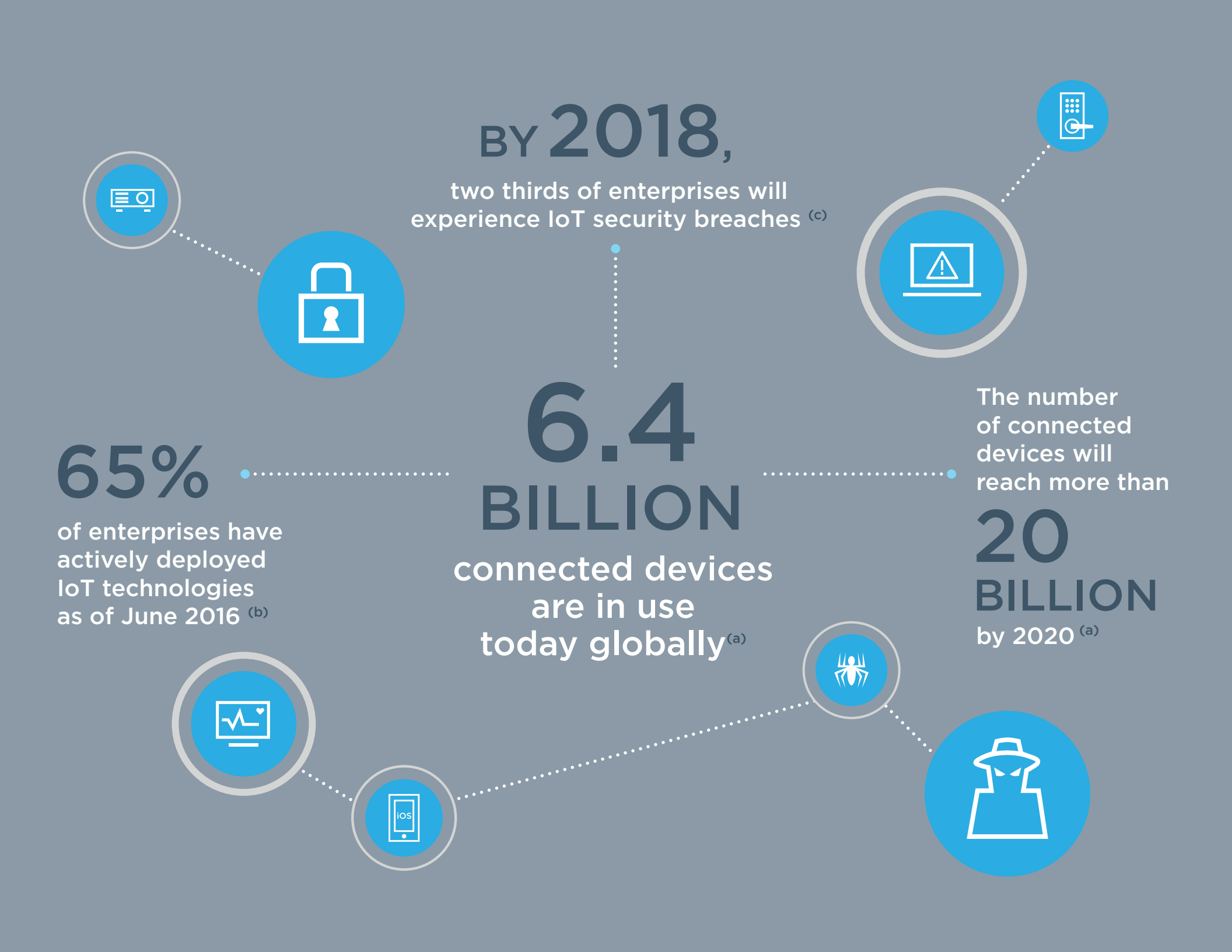
How Hackable is Your Smart Enterprise?

ForeScout IoT Enterprise Risk Report explores common IoT devices that make organizations vulnerable to dangerous – if not disastrous – attacks.

ForeScout®

“IoT is here to stay, but the proliferation and ubiquity of these devices in the enterprise is creating a much larger attack surface and easy entry points for hackers to gain access to the network. The solution starts with real-time, continuous visibility and control of devices the instant they connect -- you cannot secure what you cannot see.”

Michael DeCesare, ForeScout President & CEO


BY 2018,
two thirds of enterprises will experience IoT security breaches (c)
6.4
BILLION
connected devices are in use today globally(a)
65%
of enterprises have actively deployed IoT technologies as of June 2016 (b)
The number of connected devices will reach more than
20
BILLION
by 2020 (a)
iOS

RESEARCH OVERVIEW

ForeScout IoT Enterprise Risk Report

Industry attention has narrowed in on the threat of commonly known Internet of Things (IoT) devices and their potential safety implications to the home, but there is as much, if not more, to consider when exploring IoT threats in the enterprise.

Research into seven common enterprise IoT devices revealed that their core technologies, fundamental development methods and rapid production makes implementing proper security within the software, firmware and hardware a complex, overlooked and often neglected task.

Key Findings

The identified seven IoT devices can be **hacked in as little as three minutes, but can take days or weeks to remediate.**

Should any of these devices become infected, hackers can **plant backdoors to create and launch an automated IoT botnet DDoS attack.**

Cybercriminals can leverage **jamming or spoofing techniques** to hack smart enterprise security systems, enabling them to **control motion sensors, locks and surveillance equipment.**

With VoIP phones, **exploiting configuration settings to evade authentication** can open opportunities for **snooping and recording of calls.**

Via connected HVAC systems and energy meters, hackers can **force critical rooms (for example, server rooms) to overheat** critical infrastructure and ultimately **cause physical damage.**

Danger Rankings

DISASTROUS

Could cause irreversible damage, invade user privacy, gain access to private corporate information or destroy critical equipment.

IP-Connected Security Systems

IP-Connected Infrastructure: Climate Control & Energy Meters

DISRUPTIVE

Can disrupt corporate and operational processes.

Smart Video Conferencing Systems

Connected Printers

VoIP Phones

DAMAGING

Would allow snooping around a corporate network or extracting private credentials.

Smart Fridges

Smart Lightbulbs

Danger Scenarios

When successfully hacked, all of these devices are a gateway into the broader enterprise network. Breaking it down even further, IoT hacks can lead to:

Tampering with temperature controls and destroying critical equipment

Spying via video and microphone

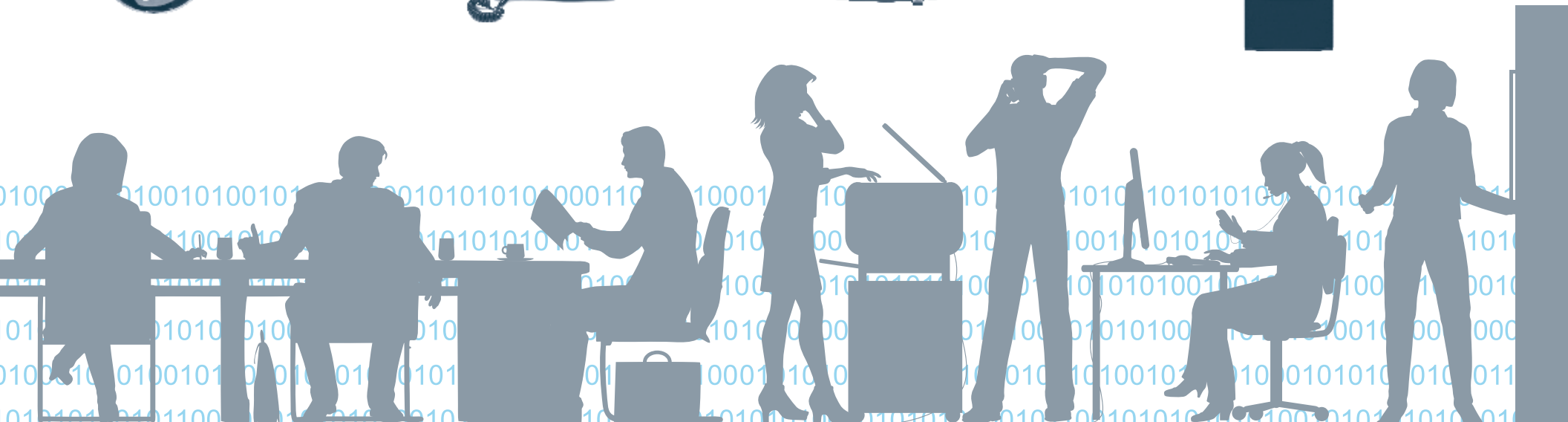
Extracting Wi-Fi credentials to carry out further attacks

Disabling to allow physical break-ins

Snooping on calls

Accessing private company and user information

Obtaining user credentials



EXPLORING SEVEN COMMON IoT DEVICES

Where Do The Vulnerabilities Lie?

DISASTROUS

IoT DEVICE RISKS

IP-Connected Security Systems

Use wireless communication to connect with other smart devices for easy entry and access, which can open the floodgates for crafty hackers.

Many use proprietary radio frequency technology that lacks authentication and encryption to communicate. They also have dependencies on some cloud services and are connected to the internet.

Most use radio signals that are easy to detect and fail to employ frequency hopping techniques, leaving them open to jamming and spoofing.

Attackers can form radio signals to send false triggers and access system controls.

Jamming or spoofing an enterprise security system could allow criminals to turn off motion sensors, remotely open locks, or redirect/switch off surveillance equipment.

Weak credentials can be used as ‘bouncing off’ points to attack other systems.

(See references page #1-3)

DISASTROUS

IoT DEVICE RISKS

IP-Connected Infrastructure: Climate Control & Energy Meters

HVAC systems provide an avenue for hackers to gain network access. Enterprises are also using smart electric meters to monitor wireless energy – creating additional risk.

HVAC systems are typically on the same network that internal systems are connected to, which hackers can easily access to intercept data, escalate privilege and carry out further attacks.

Smart energy meters can allow attackers to alter the reported energy levels of a company - potentially leading to fraudulent accounting and metering.

Attackers can force critical rooms (for example, server rooms) to overheat and cause physical damage.

IP-connected infrastructure uses wireless technology that is often accessible to anyone within range.

(See references page #4)

DISRUPTIVE

IoT DEVICE RISKS

Smart Video Conference Systems

Enable internet-based streaming, conference calling and screen-sharing, often only requiring the click of a button for users to share screens – and for hackers to commandeer it.

Vulnerable to exploits that allow remote attackers to control any of the apps on the system, take over social and communication apps, record audio and video.

Since they are wired Ethernet or Wi-Fi connected, hackers have access to sensitive places like boardrooms, C-Level offices and conference rooms that are not often accessible by outside visitors.

Attackers have full access to all software, memory and hardware, exposing the microphone, camera and stored credentials.

Similar to all software, most use common OSs, which have significant overflow vulnerabilities.

Buffer overflow allows the Smart TV to be accessible from behind a router or firewall, exposing it to intruders from anywhere on the Internet.

Smart TVs connect to the local network over IP and also serve as a pivot point for hackers to gain full network access.

Attackers can exploit other systems on the network entirely from a shell they've compromised on the TV.

(See references page #5-11)

DISRUPTIVE

IoT DEVICE RISKS

Connected Printers

Nearly all printers are networked over IP, making them accessible from virtually any computer on the network – and a welcome mat to hackers to infiltrate the enterprise.

Without physical access, hackers can comprise printers to siphon private documents printed through them.

This is almost undetectable without proper security and monitoring.

If printers are on a public network or attackers are on the same Wi-Fi network, they can send a specially crafted Simple Network Management Protocol (SNMP) packet to obtain the admin password, and gain full control of the printer.

By accessing specially crafted URLs that evade authentication, attackers can visit pages that expose the printer's credentials.

Many exploitable issues are are not resolvable without updates to firmware or an intrusion detection system.

(See references page #12-21)

DISRUPTIVE

IoT DEVICE RISKS

VoIP Phones

VoIP phones leverage the network for many sophisticated features that makes communication easy, not only for employees – but also malicious hackers.

Complex routing exposes phones to remote snooping and some can be activated as a speakerphone with no visible indication.

Hackers can exploit configuration settings to evade authentication and then update the phone, allowing them to listen to phone conversations or make calls.

Attackers only need to know the IP address of the phone to be able to access it.

(See references page #22-23)

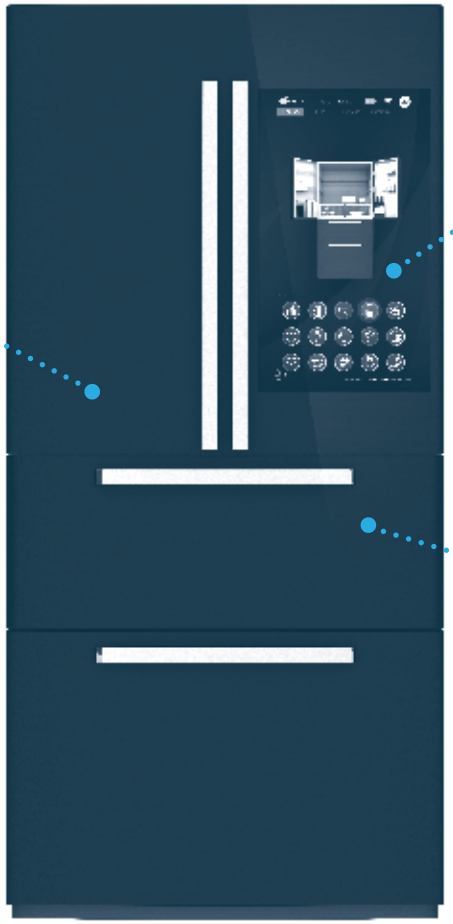
DAMAGING

IoT DEVICE RISKS

Smart Fridges

Wi-Fi-enabled refrigerators with LCD screens have access to widely used operational apps (such as scheduling applications, calendars and notification systems) and the credentials stored within.

Due to lax certificate checking, attackers on the same network could conduct a MITM (man-in-the-middle) attack to intercept communication and modify traffic between a client and server.



This can be done by injecting spoofed Address Resolution Protocol (ARP) requests or Domain Name System (DNS) responses, both of which are critical to IP networks today and provide no method of authentication or encryption.

This grants attackers access to any of the integrated enterprise applications, and the user credentials associated with that account.

(See references page #24)

DAMAGING

IoT DEVICE RISKS

Smart Lightbulbs

Smart lightbulbs operate on Wi-Fi and proprietary mesh networks – they can easily integrate into other connected systems that can be controlled by external devices and hackers.

Mesh network communication channels can be sniffed by attackers.

By sniffing the network, attackers only need to be within Wi-Fi range of the smart bulb with no original access to the network.

Hackers can extract password-protected Wi-Fi credentials without being on the network, allowing them to gain access to other systems and devices in the enterprise – from laptops to smartphones and even network-connected manufacturing systems.

Some bulbs have been shown to send Wi-Fi credentials in plain text, making extraction possible.

(See references page #25-27)

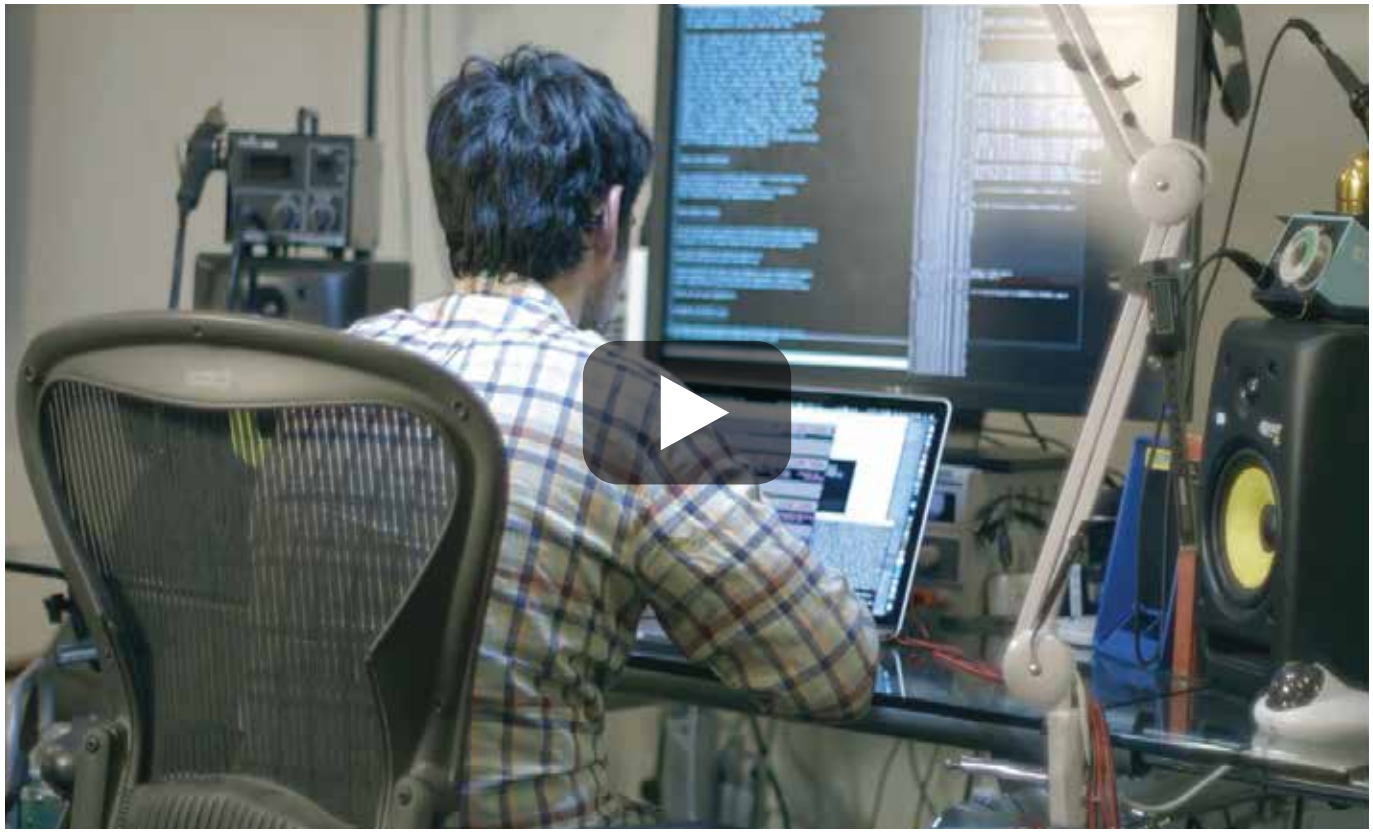
Anatomy of an IoT Attack

IoT threats could spread through networks and the internet.

IoT threats would work even more effectively by targeting the specialized wireless communication protocols that IoT devices share, such as Wi-Fi, Bluetooth, ZigBee.

If a threat were to successfully infect a device and infiltrate one network, it could spread to an entirely separate, segregated network - just by being within wireless range of another IoT device, despite no previous communication between the two.

Visualizing an IoT Attack



Research Methodology

Commissioned by ForeScout Technologies, the IoT Enterprise Risk Report employed the skills of Samy Kamkar, one of the world's leading ethical hackers, to investigate the security risks posed by IoT devices in enterprise environments. The report sought to uncover vulnerabilities in enterprise-grade technology, utilizing both physical testing situations, as well as drawing from peer-reviewed industry research.

Kamkar conducted extensive research (including reviewing datasheets, previous hacks, peer-reviewed/industry research, known CVEs and first-hand conversations with industry peers) to evaluate each device, looking into vulnerabilities of the following: inputs, outputs, physical ports, communication protocols, manufacturing techniques and software and/or firmware involved.

Summary

While IoT devices make it possible for organizations to run faster and more efficiently, they are too often used with little regard to their security risk. The rush to deliver new types of IoT technologies sacrifices security – almost 100 percent of the time. Once these devices are on the network, it's easy for malware to compromise them, or for a hacker to gain access through them and steal critical information.

It's a cybersecurity challenge and an opportunity to help CISOs fill the ensuing security gaps.

Businesses need an agentless approach to be able to manage their IoT devices – helping them to see the devices in real time. Enterprise IoT devices, some of which were examined in this analysis, are not designed with security agents, and IT departments often turn a blind eye when new devices are added to the corporate network to avoid the hassle of re-deploying their security protections.

In the age of IoT, visibility and control of devices on the network is a must have, not a nice to have.

Best Practices

IoT security starts with full visibility and control over devices as soon as they connect to the corporate network.

DISCOVER AND CLASSIFY
IoT devices the instant they connect to the network

CONTROL
network access based on device type, posture and behavior

ORCHESTRATE
integrate islands of security; leverage existing investments for better protection

About ForeScout

ForeScout Technologies is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network.

Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of January 2016, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions.

Learn more at ForeScout.com

© 2016. ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo, ControlFabric, CounterACT Edge, ActiveResponse and CounterACT are trademarks or registered trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners.

Glossary

IoT	Internet of Things
IP	Internet Protocol
VoIP	Voice Over Internet Protocol
OS	Operating System
SNMP	Simple Network Management Protocol
MITM	Man-in-the-Middle
ARP	Address Resolution Protocol
DNS	Domain Name System
OT	Operational Technology
IT	Information Technology
DDoS	Distributed Denial of Service

References

a) Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," Gartner. 10 November 2015.

b) 451 Research: Today 65% of Enterprises Already Using Internet of Things; Business Value found in Optimizing Operations and Reducing Risk," 451 Research. 29 June 2016.

c) Gens, F. "Webcast: IDC's global technology predictions for 2016," IDC. 4 November 2015.

1) Rose, A. and Ramsey, B. "Picking Bluetooth Low Energy Locks from a Quarter Mile Away," Merculite Security. 6 August 2016.

2) Jmaxxz, "Backdooring the Frontdoor." 7 August 2015.

3) Fernandes, E., Jung, J. and Prakash, A, "Security Analysis of Emerging Smart Home Applications," In Proceedings of 37th IEEE Symposium on Security and Privacy, May 2016.

4) "CVE-2016-4529," CVE. 5 May 2016.

5) "Vulnerability Summary for CVE-2014-7911," National Vulnerability Database. 15 December 2014.

6) "CVE-2014-6041," CVE. 1 September 2014.

7) Lee, S and Kim, S. "Hacking, Surveilling, and Deceiving Victims on Smart TVs," CIST. August 2013.

8) Grattafiori, A. "The Outer Limits: Hacking A Smart TV," iSEC Partners. 28 October 2013.

9) "CVE-2012-5958," CVE. 21 November 2012.

10) Russon, M. "It's official, your smart TV can be hijacked: Malware is holding viewers to ransom," International Business Times. 12 January 2016.

11) Metzger, M. "Millions of smart TVs and remote control apps vulnerable," SC Magazine. 9 December 2015.

12) "Samsung Printer SNMP Hardcoded Community String Authentication Bypass Vulnerability," Acunetix. 25 March 2015.

13) "CVE-2015-1056," CVE. 16 January 2015.

14) "CVE-2014-3111," CVE. 29 April 2014.

15) "CVE-2013-4613," CVE. 17 June 2013.

16) Costin, A. "Hacking printers: for fun and profit," Hack.Lu. 2010.

17) "CVE-2013-2507," CVE. 8 March 2013.

18) "CVE-2013-2670," CVE. 22 March 2013.

19) "CVE-2013-2671," CVE. 22 March 2013.

20) "CVE-2012-4964," CVE. 17 September 2012.

21) "CVE-2012-4964," CVE. 17 September 2012.

22) "Cisco Small Business SPA300 and SPA500 Series IP Phones Unauthenticated Remote Dial Vulnerability," Cisco. 15 March 2015.

23) "Polycom Configuration," Free Switch. 20 July 2014.

24) Venda, P. "Hacking DefCon 23's IoT Village Samsung fridge," Pen Test Partners. 18 August 2015.

25) Chapman, A. "Hacking into Internet Connected Light Bulbs," Context. 4 July 2014.

26) "LIFX Firmware release 1 February 2015," LIFX. 1 February 2015.

27) Wakefield, J., "Smart LED light bulbs leak Wi-Fi passwords", BBC, 8 July 2014.