INTERNET OF THINGS DEVICES AS INTELLIGENCE ASSETS: CHALLENGES AND OPPORTUNITIES

KEY ISSUES:

Unprecedented volume of connected devices brings new security risks, making it difficult to harvest threat intelligence

Internet of Things (IoT) devices are entering the workplace at an astonishing rate, posing new risks to the enterprise. As businesses look for ways to mitigate this risk, security-as-usual isn't sufficient due to massive amounts of data, unexpected formats and the nature of the devices.

Definition

The Internet of Things (IoT) is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.[1] *The term has come to mean the network of physical objects embedded with electronics, software, sensors and network connectivity, allowing them to exchange data.*

Growth

The number of things connected to the Internet is expected to grow rapidly, reaching 50 billion things by 2020. [2]

Weakness of current approaches to security

Most security today is based on a set of expectations: devices will have a reasonable level of security built in; devices will be discoverable; they will create log files with indicators of compromise; log data can be correlated and aggregated into threat intelligence; and security teams can use threat intelligence to do on-the-fly policy changes and updates to increase security.

With IoT, none of these are a given.

- IoT devices have limited process, storage and power capabilities, making them poorly suited to agent-based security solutions.
- They are difficult to discover due to myriad device-to-device and device-to-server protocols.
- Log information is not in any standard format, nor is it easily stored on the device itself. [3]
- Indicators of compromise are challenging to harvest from log files and aggregate into traditional threat intelligence.
- It is problematic to use threat intelligence to effect on-the-fly policy changes.
- Updates are limited.

Complicating the issue is the fact that IoT devices don't just deal with information: they have the ability to change state, which alters the way CISOs have to deal with them. [4]

Types of security risks:

- Attacks based on "thingbots" (e.g. DDoS) are probably the most common and dangerous. [5] In January 2014, researchers found that more than 100,000 refrigerators and other appliances had been hacked to send out 750,000 malicious spam emails. [6]
- Industrial espionage via personal devices as an attack vector: monitors, sensors, smart phones/watches.
- Data breaches, where attackers spy on communications between peers in an IoT network and collect information on the services they implement.
- Weakening perimeters – because IoT devices are not designed with security in mind, they result in an overall weaker perimeter that must be defended. [7]

CHALLENGES AND OPPORTUNITIES:

As IoT changes the workplace, use threat intelligence as a strategic weapon

IoT challenges security professionals to deal with a multitude of unfamiliar raw devices and communication protocols. The inherent lack of security in many devices, such as those running embedded operating systems, makes them vulnerable to new exploits. Because of this, they require fine-grained access control and traffic and data security. Furthermore, the devices' demand for ubiquitous connectivity across public and private networks increases the overall enterprise threat surface. [8]

The opportunity: IoT devices produce a massive amount of raw information that could be collected, processed, analyzed and integrated with external threat feeds to improve the situational awareness picture. A recent study estimates that by 2020 the IoT will generate 44 zettabytes (44 trillion gigabytes) annually. The majority of this data is stored, aggregated and distributed through third parties, rather than residing on the devices themselves. [9]

If IoT information were integrated into threat intelligence platforms, security teams could build richer baselines and make better decisions regarding risk management and business continuity.

The problem is, how do you get this information from the devices? Because the raw data comes in a variety of formats, it must be interpreted, indicators of risk detected, and that information integrated into threat intelligence platforms. Due to the variety of formats, and multiple variations of those formats, making sense of the data is not easy.

A similar problem is how to use aggregate threat intelligence to communicate back to the IoT devices, improving their security. IoT-enabled applications need to be able to consume the communicated intelligence, and dynamically change their behavior based on that intelligence.[10] Devices that are built with device-based agents and network-based gateway nodes, and those that permit automated, encrypted firmware updates, can help in this regard.

Important trends:

- IoT threat intelligence toolkits enable developers to build real-time threat intelligence services and agents into IoT devices. [11]
- New threat intelligence platforms aggregate and integrate massive amounts of threat and risk information, implementing "collective threat intelligence" for IoT. [12]
- Information Sharing and Analysis Centers (ISACS) have been formed for many sectors (notably financial services, industrial control systems and defense), enabling a community of trusted partners to share their own threat intelligence data with other organizations. [13]
- Specifications such as the Structured Threat Information eXpression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII) aim to create a common format for threat information, enabling security teams to aggregate and analyze a wide variety of threat intelligence from multiple sources. [14]
- Many security vendors are enhancing their portfolios with basic support for embedded systems and machine-to-machine communication, including support for protocols, application security and requirements specific to IoT. [15]

THE PATH FORWARD:

Look at IoT as a catalyst for accelerated integration of threat intelligence

Technology: Comprehensive situational awareness has long been recognized as the ideal – and only – starting point for enterprise security: understand what's normal, so you can spot the abnormal. Expanded cyber threat intelligence, incorporating threat intelligence from both internal and external sources of risk, can bring this knowledge. It is also helpful to utilize an expanded set of threat intelligence sources as you build situational awareness. Explore the possibility of using readily available tools, like Shodan, to discover your externally visible IoT devices, give yourself insight into what your adversaries can readily discover, and target devices for increased controls.[16]

People: Make sure you are staffed and empowered to ensure optimal security of IoT devices. This may involve enabling the IT staff with additional resources to confirm that mechanisms are in place to patch devices, manage them from a central network, create device guidelines, etc. [17]

Processes : Don't overthink IoT security planning: because there is no standard guide to securing IoT, expect to start small and learn as you go. Tackle an immediate problem related to IoT, and then expand on your experience to start building out common architectural foundations, responsibilities and deployment scenarios. [18]

IoT can be a force multiplier for threat intelligence

Threat intelligence has become one of the hot topics in security today, but the advent of huge numbers of new devices, each capable of both generating and consuming threat intelligence, brings the discussion to new heights. Security teams will need to evaluate their existing IT-centric security approaches in light of an IoT-centric strategy, mining an increasingly larger stream of data from both internal and external sources. New formats for data integration should be investigated, as well as new tools and platforms to aggregate and manage huge data flows.

Prepare for expanded cooperation and information sharing among peers, and the industry as a whole. Take advantage of the opportunities afforded by IoT to expand and enhance threat intelligence systems, and better prepare for a world with billions of Internet-connected things.

1 "Internet of Things Global Standards Initiative". ITU. Retrieved 20 Nov 2015 from http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

2 Evans, Dave. "The Internet of Things: How the Next Evolution of the Internet is Changing Everything." Cisco Internet Business Solutions Group. April 2011. Retrieved from http://www.iotsworldcongress.com/documents/4643185/3e968a44-2d12-4b73-9691-17ec508ff67b

3 Schneider, Stan. Understanding the Protocols Behind the Internet of Things. Electronic Design. Oct 2013. http://electronicdesign.com/iot/understanding-protocols-behind-internet-things

4 Perkins, Earl. "What Securing the internet of Things Means for CISOs." Gartner Group. 11 April 2014. Retrieved from http://media.techtarget.com/facebook/downloads/what_securing_the_internet-F5DG554923.pdf?ASRC=SS_PMC&Offer=PROPLUS

5 John, Sian. "Securing the Internet of Things – Where's the Risk?" 2 January 2014. Symantec. Retrieved from http://www.symantec.com/connect/blogs/securing-internet-things-wheres-risk?sf21585364=1

6 "Internet of Things: How Much are We Exposed to Cyberthreats?" Infosec Institute. 25 January 2015. Retrieved from http://resources.infosecinstitute.com/internet-things-much-exposed-cyber-threats/

7 Ibid.

8 Oltsik, Jon. "The Internet of Things: a CISO and Network Security Perspective." ESG Group. October 2014. Retrieved from https://www.cisco.com/web/strategy/docs/energy/network-security-perspective.pdf

9 The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. EMC. April 2014. Retrieved from http://www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm

10 Ibid.

11 Quinnell, Richard. Collective Threat Intelligence for the IoT. Embedded. 26 May 2015. Retrieved from http://www.embedded.com/electronics-blogs/embedded-view/4439549/Collective-threat-intelligence-for-the-IoT

12 Threat Intelligence Platforms: The Next Must-Have for Harried Security Operations Teams. Dark Reading. June 2015. Retrieved from http://www.darkreading.com/threat-intelligence-platforms-the-next-must-have-for-harried-security-operations-teams/d/d-id/1320671

13 "Eight Essential Elements for Effective Threat Intelligence Management" IT-Harvest. May 2015. Retrieved from http://www.bitpipe.com/detail/RES/1440608169_518.html

14 OASIS Cyber Threat Intelligence (CTI) TC https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

15 Perkins, op cit.

16 Ernst and Young, op. cit.

17 "What to Consider Before Bringing IoT Devices and Wearables to the Workplace" Trend Micro. 15 April 2015. Retrieved from http://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/internet-of-things/

18 Perkins, op. cit.

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

12.15 | F1