Information Security Blog › How-To › How to Stop Cyberattacks on Your IoT Infrastructure

HOW-TO SEPTEMBER 21, 2018

How to Stop Cyberattacks on Your IoT Infrastructure

PRAMOD BORKAR - TECHNICAL MARKETING

SHARE

In part one of our internet of things (IoT) blog series, we provided background on the tremendous growth of IoT and their innovative use cases—from alarm systems, to power grid monitoring, to devices that are combating honeybee colony collapse disorder.

We also looked at the 600% increase in IoT attacks that occurred between 2016 – 2017. And we examined that while many organizations have deployed IoT devices, typically they aren't properly monitored or controlled with the same diligence and policies as other network systems.

Are IoT devices like security cameras, printers, and thermostats creating cybersecurity risks?

Your security operations center (SOC) most likely can tell when a user makes a VPN connection and authenticates with a database server. But do they know when someone makes a connection to a non-computer asset? Can you tell who has accessed your lighting controls, your security cameras, or your fire control system? Do you even know about all of the devices connected to your network? What about network-connected printers?

If your organization is like most, many of these IoT systems aren't even on your radar, often because there isn't the necessary monitoring solution for such internet connected devices.

"Research *published by academics has resurfaced several serious vulnerabilities in popular internet-connected printers, which if exploited could allow an attacker to remotely steal sensitive documents from print jobs.*

"Worse, the researchers say, is that an attacker could use one of the age-old bugs to read the printer's network credentials, such as for email sharing, or other corporate accounts if the printer is used for other functions, like scanning and faxing."

Subscribe

Email address SUBMIT

TRENDING HOW-TO ARTICLES

1 On-the-Job Cryptocurrency Mining: Protecting your organization from energy theft

TRENDING INFORMATION SECURITY ARTICLES

1 The Complete Guide to CSIRT Organization: How to Build an Incident Response Team

2 Insider Threats: How to Stop the Most Common and Damaging Security Risk You Face

3 2018 State of the SOC Report

4 5 Best Practices for Your Incident Response Plan

5 How Criminals Can Build a "Web Dossier" from Your Browser

We all know that letting a hacker take over a critical asset in a hospital, power grid, or military facility could have disastrous results. But what's the big deal if a hacker takes over a security camera or thermostat? What's the risk if someone is tinkering with your environmental controls or watching your parking lot? And how does a hacker even access one of these devices?

Unpatched IoT Devices

Many IoT devices are unpatched, connecting to corporate networks through standard internet service providers. A security-conscious organization would likely cordon off these devices through isolated routers, making sure that there are no pathways from the devices to protected network assets.

But hackers can use readily available tools to easily locate publicly connected devices with documented security vulnerabilities. Once they find a target, they can attempt a factory reset and get root access to the device through published lists from a Common Vulnerabilities and Exposure (CVE) site. If successful, they can now control the device, such as watching a video feed.

If a compromised camera is in an organization's lobby, the attacker can view employees and visitors coming and going, and potentially see what's being typed on a receptionist's computer. Moreover, they can initiate a DDoS attack on many device types, rendering them unavailable or unresponsive for an extended period of time.

Lateral moves

Determined attackers can learn, for example, the IP address and model number of the router to which the compromised IoT device is attached. Once that is known, they can determine if the router has vulnerabilities.

For example, some routers have well known code-execution vulnerabilities, and the targeted organization might have failed to apply patches in a timely manner. An attacker could use a tool to crack the router's hashed data to obtain the router's credentials, then install and execute code that enables them to scour the network for valuable data. If the original attack vector was a lobby camera, the attacker might already know credentials of at least one network user (possibly obtained by viewing a computer screen or from analyzing user keystrokes).

Given this IoT attack landscape, remember that your organization is exposed to the same compliance regulations such as GDPR (and penalties), regardless of whether a breach is caused by a network-connected device or a user.

Analyzing IoT device behavior

To know what's happening with your IoT devices, you have to understand their baseline behavior. To do this, you need:

- **Visibility into the communication patterns of your network devices.** Most communication between machines and network zones is unknown today.
- **An understanding of each connected device**, including its trusted and normal operating behaviors. For example, has one or more of your devices experienced a password spray or brute force attack?
- **Knowledge of asset ownership**—who is responsible for a given device? Who originally connected it, and who was the last person to update its configuration? Typically, we find a lack of responsibility for system level behaviors of IoT devices.
- **Correlation of IP addresses to device or user names**. You need to be able to identify risky devices and the users who have interacted with them.
- **An understanding of network activity in the absence of users**. Data about firewalls,

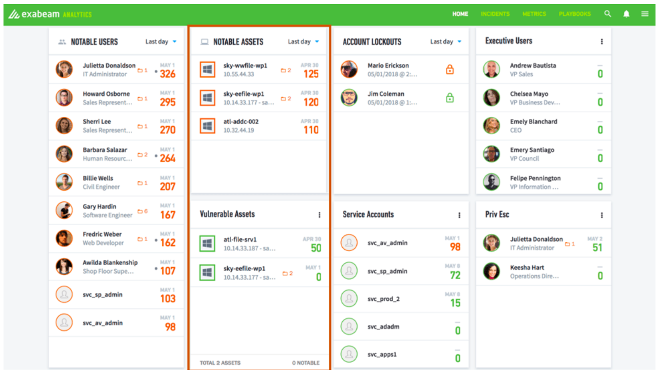
network packets, and net flow are required to get a complete picture of network behavior.

Users – Exabeam Advanced Analytics (AA) has solved these problems from the perspective of *users*. It analyzes each network user's behavior patterns over consecutive sessions, scoring users based on how far they deviate from normal patterns. When a score exceeds a predetermined trigger point, AA notifies your SOC, so they can investigate potential breaches. In addition, your analysts can examine any user, behavior pattern, and time frame to investigate, for example, any unusual events that have occurred.

Devices – Adding to Advanced Analytics, Exabeam Entity Analytics provides the same set of features for your network connected devices (IoT). Entity Analytics monitors any connected devices and notifies you when its behavior patterns fall outside a normal range.

Following an IoT attack chain

Continually monitoring the behavior of each of your IoT entities, such a system can notify you when it detects abnormal behaviors (Fig. 1).



NOTABLE USERS Last day

Julietta Donaldson, IT Administrator, 1, MAY 1, 326
Howard Osborne, Sales Represent..., 1, MAY 1, 295
Sherri Lee, Sales Represent..., 1, MAY 1, 270
Barbara Salazar, Human Resourc..., 2, MAY 1, 264
Billie Wells, Civil Engineer, 1, MAY 1, 207
Gary Hardin, Software Engineer, 6, MAY 1, 167
Fredric Weber, Web Developer, 1, MAY 1, 162
Awilda Blankenship, Shop Floor Supe..., MAY 1, 107
svc_sp_admin, MAY 1, 103
svc_av_admin, MAY 1, 98

NOTABLE ASSETS Last day

sky-wwfile-wp1, 10.55.44.33, 2, APR 30, 125
sky-eefile-wp1, 10.14.33.177 - sa..., 2, APR 30, 120
atl-addc-002, 10.32.44.19, APR 30, 110

Vulnerable Assets

atl-file-srv1, 10.14.33.187 - sa..., APR 30, 50
sky-eefile-wp1, 10.14.33.177 - sa..., 2, MAY 1, 0

TOTAL 2 ASSETS 0 NOTABLE

ACCOUNT LOCKOUTS Last day

Mario Erickson, 05/01/2018 @ 2:...
Jim Coleman, 05/01/2018 @ 1:...

Executive Users

Andrew Bautista, VP Sales, —, 0
Chelsea Mayo, VP Business Dev..., —, 0
Emely Blanchard, CEO, —, 0
Emery Santiago, VP Council, —, 0
Felipe Pennington, VP Information ..., —, 0

Service Accounts

svc_av_admin, MAY 1, 98
svc_sp_admin, MAY 8, 72
svc_prod_2, MAY 8, 15
svc_adadm, —, 0
svc_apps1, —, 0

Priv Esc

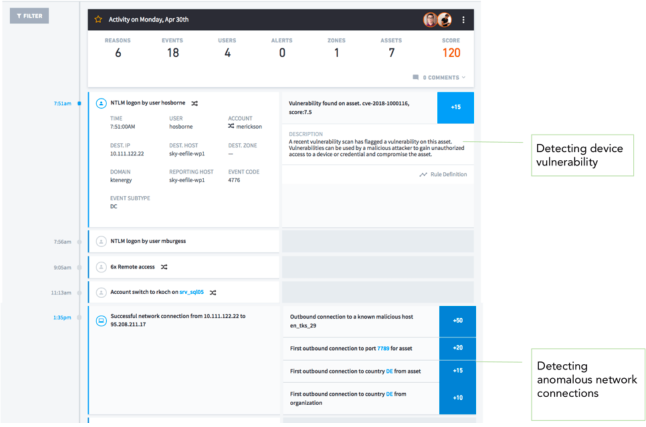
Julietta Donaldson, IT Administrator, 1, MAY 2, 51
Keesha Hart, Operations Dire..., —, 0

Figure 1 – Exabeam Advanced Analytics dashboard showing notable assets that have high-risk scores

Prebuilt incident timelines answer critical questions and provide you with all of the information you need for a rapid investigation:

- What happened, and in what order?
- Was it normal or abnormal for that particular asset?
- What happened before and after the security incident?
- Was there lateral movement to other users or devices?

In examining the timeline for a device (Fig. 2), you can easily see the progression of events that caused an escalated score.



Activity on Monday, Apr 30th

REASONS	EVENTS	USERS	ALERTS	ZONES	ASSETS	SCORE
6	18	4	0	1	7	120

7:51am NTLM logon by user hosborne

TIME	USER	ACCOUNT
7:51:00AM	hosborne	merickson
DEST. IP	DEST. HOST	DEST. ZONE
10.111.122.22	sky-eefile-wp1	—
DOMAIN	REPORTING HOST	EVENT CODE
ktenergy	sky-eefile-wp1	4776
EVENT SUBTYPE		
DC		

Vulnerability found on asset. cve-2018-1000116, score:7.5 +15

DESCRIPTION
A recent vulnerability scan has flagged a vulnerability on this asset. Vulnerabilities can be used by a malicious attacker to gain unauthorized access to a device or credential and compromise the asset.

7:56am NTLM logon by user mburgess

9:05am 6x Remote access

11:13am Account switch to rkoch on srv_sql05

1:35pm Successful network connection from 10.111.122.22 to 95.208.211.17

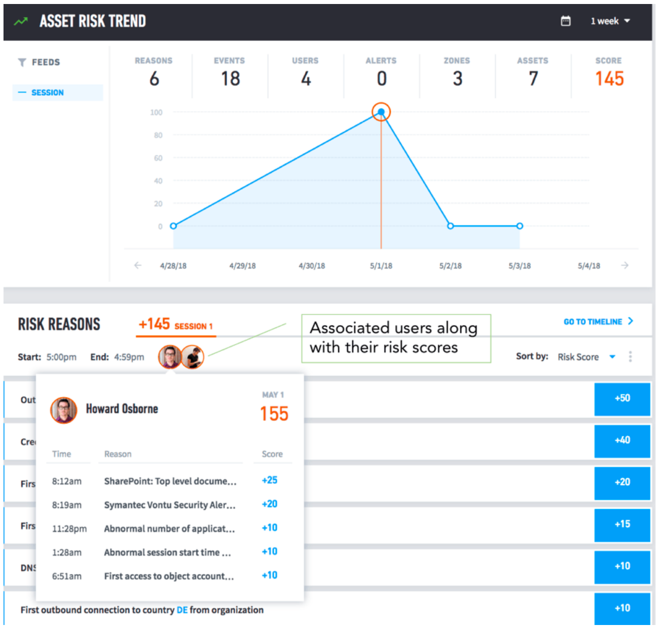
Outbound connection to a known malicious host en_tks_29 +50
First outbound connection to port 7789 for asset +20
First outbound connection to country DE from asset +15
First outbound connection to country DE from organization +10

Detecting device vulnerability

Detecting anomalous network connections

Figure 2 – Event timeline stitches together user and asset behavior. In this example, the risks are due to device vulnerability and anomalous network connections.

The left column shows the time stamp for each event. The right column highlights abnormal events and indicates the number of risk points each event adds to its risk score. User and entity behaviors are integrated into a “single pane of glass” view. This allows even junior-level analysts to instantly pivot from viewing an entity, to viewing the users associated with it and the impacts (Fig. 3).



Start: 5:00pm End: 4:59pm

Associated users along with their risk scores

Howard Osborne — MAY 1 — 155

Time	Reason	Score
8:12am	SharePoint: Top level docume...	+25
8:19am	Symantec Vontu Security Aler...	+20
11:28pm	Abnormal number of applicat...	+10
1:28am	Abnormal session start time ...	+10
6:51am	First access to object account...	+10

Out	+50
Cre	+40
Firs	+20
Firs	+15
DNS	+10
First outbound connection to country DE from organization	+10

Figure 3 – The ability to pivot between devices and users helps investigators to pinpoint anomalous behavior quicker.

We’ve provided some examples of how IoT hardware interacts with users and other entities on your network. You’ve seen a few of the problems they can cause, as well as the kinds of information you’ll need to successfully track and manage the growing pool of IoT devices.

Remember, most complex threats involve both users and assets. Exabeam Entity Analytics enables you to easily pivot and follow the progression of a security incident—no matter where it reaches your network.

- See Cybersecurity Strategies for the Growing Risks of the Internet of Things (IoT)
- Information Security Blog: Introducing Behavioral Analysis for Devices – Exabeam Entity Analytics
- Exabeam Entity Analytics Product Overview

# IOT

PRAMOD BORKAR
TECHNICAL MARKETING

More like this

If you'd like to see more content like this, visit the Exabeam Blog

Explore more

INFORMATION SECURITY

Operation Aurora – 2010's Major Breach by Chinese Hackers

JANUARY 8, 2019 — TIM MATTHEWS

Exabeam's Cybersecurity History Review: Read about Operation Aurora and the series of cyberattacks in 2010 conducted by the Elderwood Group based in Beijing, China, with ties to the People's Liberation Army.

INFORMATION SECURITY

Exabeam's Top Cybersecurity Blog Posts of 2018

JANUARY 2, 2019 — MARITZA MARIE DUBEC

2018 was a memorable year for cybersecurity. Millions of people were impacted as we saw more companies hit by megabreaches—from a major hotel chain to a social media platform used by billions. Here are our top 10 blog posts that had the biggest readership and were the most noteworthy.

UEBA

User Behavior Analytics (UBA/UEBA): The Key to Uncovering Insider and Unknown Security Threats

JANUARY 2, 2019 — ORION CASSETTO

Learn about UBA technology, and its extension UEBA (User Entity Behavior Analytics), how it works, and which threats it uncovers that no other tool can see.

Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information.

REQUEST A DEMO

PRODUCT

Exabeam Advanced Analytics
Exabeam Cloud Connectors
Exabeam Data Lake
Exabeam Entity Analytics
Exabeam Incident Responder
Exabeam Spectrum
Exabeam Threat Hunter

ANALYST CORNER

PARTNERS

SUPPORT

SOLUTIONS

Compliance
Threat Detection
Cloud Security
IoT Monitoring
SOC Automation

ABOUT

CAREERS

MEDIA KIT

LEARN

Library
Newsroom
Glossary
SIEM Cost Comparison

BLOG

Information Security
SIEM
UEBA
Security Operations Center
DLP
Incident Response

SIEM GUIDE

What is SIEM?
SIEM Architecture
Events and Logs
UEBA
SIEM Use Cases
SIEM Analytics
The SOC, SecOps and SIEM
Incident Response and Automation
SIEM Buyer's Guide

CONTACT

2 Waters Park Dr., Suite 200
San Mateo, CA 94403

1.844.EXABEAM

info@exabeam.com

Terms & Privacy Policy — Sitemap