7 IOT EXPLOITS IN THE ENTERPRISE

The Internet-of-Things (IoT) evolved rapidly from an emerging niche concept to a virtually unavoidable buzzword. In a matter of just a few short years, it seems that almost anything you can think of is somehow connected to the Internet. IoT and industrial Internet-of-Things (IIoT) are streamlining manufacturing and logistics, and enabling better productivity and security across nearly every facet of our lives today—but the benefits of IoT also come with a healthy dose of security concerns.

It's easy to underestimate or dismiss the risk or attacks against IoT devices. "IoT" is such an overused term, and security issues are so pervasive that it's easy to become jaded or just tune it all out. The conversation about IoT attacks often revolves around doomsday scenarios that seem highly implausible outside of a James Bond movie. The reality, however, is that IoT attacks are happening all the time—possibly on your network—and most companies are not prepared to defend against them because traditional security products can't provide the visibility necessary to detect IoT threats.

As the volume of connected, IP-based devices grows exponentially, so does the associated threat landscape. There were an estimated 8 billion connected "things" by the end of 2017, and Gartner predicts that number will surpass 20 billion by 2020.[1]

SECURING THE ENTERPRISE OF "THINGS"

IoT devices are often inherently insecure, and frequently unmanaged—making them perfect targets for hackers and cyber criminals. In just the past year or two, there has been a dramatic rise in IoT attacks, including Satori, Hajime, Brickerbot, Reeper, and the Mirai botnet. There are also a concerning number of airborne exploits designed to take advantage of vulnerable wireless devices, such as Broadpwn, KRACK, Devil's Ivy, and Blueborne.

The attacks against IoT devices are affecting enterprises. A survey by IDC determined that 46 percent of organizations have experienced a breach or security incident associated with IoT security (or the lack thereof)—and 70 percent of those companies reported that the IoT security incident was more costly than a traditional breach.

The issue of IoT will multiply exponentially over the next few years as IoT adoption continues to skyrocket. A recent study by Symantec found a 600 percent increase in IoT attacks from 2016 to 2017—and that pace is not likely to slow down anytime soon. Gartner predicts that by 2020 only 10 percent of the devices connected to your network will be manageable by traditional methods, and that 25 percent of the enterprise attacks identified will be IoT-related.

Connected devices are already exposing companies to unique and innovative attack vectors. Hackers were reportedly able to capture the database of high-roller customers from a casino using a connected, IP-based thermometer placed in an aquarium in the casino lobby.

Such attacks are becoming common place. Armis is in a unique position to be seeing these attacks first hard. To illustrate the reality of the how IoT devices – truly unmanaged devices –d are being targeted, let's look at a few real-world examples.

1. COMPROMISED TABLET

These are actual attacks against IoT devices or infrastructure on actual businesses. For each case study, we will walk through how the attack happened and how it was discovered by Armis. We will also point out why traditional network and endpoint security tools are unable to protect against these attacks.

Next to smartphones, tablets are one of the most prevalent connected devices out there. They are small, light, portable, and versatile. Many businesses rely on tablets for everything from providing an interface for a kiosk in the lobby, to conducting point-of-sale transactions, to managing inventory and logistics, to the physician in the emergency room.

Companies also use tablets in conference rooms to manage the audio and video systems. One Armis customer had approximately 200 conference rooms—and each one was equipped with a tablet for that purpose. There's a good chance you have something similar in your offices.

Armis found that one of the conference room tablets was streaming audio and video to an unknown location. The stream was enabled 24x7—allowing the attacker to eavesdrop on any conversations or presentations conducted in that conference room. Obviously, that is a serious security problem.

How Armis Discovered the Problem

Armis monitors traffic on the wireless LAN controller—including traffic on the guest network, which is sometimes ignored by traditional security products. This comprehensive visibility enables Armis to discover and classify all devices on the network—and establish a baseline of the associated traffic types and volume for each device.

The Armis risk analysis engine identified anomalous traffic from a device on the guest network. Both the volume of traffic and the time of day the traffic was being generated were bizarre, compared to normal activity. Armis identified that the suspicious traffic was video and issued an alert to the customer. The customer examined the tablet in question and determined that it was streaming video traffic to an unknown location.

Why Traditional Security Tools Didn't Detect the Issue

The customer had a variety of other security tools and lines of defense, but none of them are designed to detect an attack like this.

A firewall is designed to protect the perimeter—to keep unknown traffic or unauthorized users outside of your network from getting inside. It generally does a great job in that role, but it is not

designed to detect anomalous devices or activity. To a firewall, the video data streaming from the tablet appears to be normal traffic.

NAC (network access control) is designed to inventory devices and to ensure that each device is on the correct network segment. The NAC system in this case had identified the tablet and placed it in the Guest network. At that point, the job of the NAC was done. The NAC is not designed to monitor traffic or detect anomalous activity.

The IPS (intrusion prevention system) is also not equipped to detect an attack like this. IPS will detect and block attacks inside the network, but the video traffic in and of itself is not suspicious. What makes the video traffic suspicious is the broader context, and the comparison against other similar devices on the network—a level of visibility that exceeds the capabilities of IPS.

> The lack of security by design in the IoT devices is another huge problem. Many devices that enterprises have begun connecting to the Internet have little by way of security protections and, worse, are not equipped even to receive OS updates, security patches and over the air fixes.[2]
>
> Gartner, March 2018

2. COMPROMISED SMART TV

Many conference rooms and boardrooms today are equipped with some sort of smart TV—a television or monitor that is connected to the network and provides additional features and capabilities beyond simply displaying a video feed. The fact that the device is on the network—and typically has a connection to the public internet—also exposes the conference or boardroom to increased risk.

A post from Security Boulevard emphasized the risk from connected devices—particularly smart TVs. It describes how IoT devices often have inherently weak security protocols, and the challenges of visibility when dealing with the volume of connected devices on the network. It explains, “Enterprises, even more so than singular households, need a resilient and reliable solution that protects their IoT devices from these types of threats while complementing their existing security infrastructure.”

In one customer’s board room, Armis discovered a smart TV that had been compromised and was attempting to infect any other connected device that came near it. Malware had been surreptitiously installed on the smart TV by a vendor as part of the remote control app, and was sending out a beacon to any device in range to connect so it could install the malware and spread throughout the network and beyond.

How Armis Discovered the Problem

When Armis starts working with a customer, the first thing we do is inventory and identify all devices in the environment. We also begin monitoring all connections in the airspace of the customer—including all Bluetooth wireless communications.

Our risk analysis engine identified unusual activity around the smart TV in the boardroom. When we examined the traffic more closely, we determined that the TV was sending out a beacon and connecting to any device it could over its open Wi-Fi hotspot or via Bluetooth.

Why Traditional Security Tools Didn’t Detect the Issue

There were other network security solutions in place before Armis came in, but none of them were capable of identifying this threat.

The smart TV in the boardroom had been whitelisted in the NAC (network access control) system, to ensure it would allow the device to connect to the network. Once a device is accepted and assigned on the network, the NAC’s job is done. It does not monitor behavior or external wireless connections.

The firewall, IPS (intrusion prevention system), and UEBA (user and entity behavior analytics) can’t see external wireless connections from devices. The smart TV was not sending data out through the gateway or traffic across the network, so these security solutions wouldn’t notice the suspicious activity.

3. COMPROMISED SECURITY CAMERA & ROUTERS

Security cameras are not a new concept, but in recent years there's been an explosion of internet-connected cameras. IP-based security cameras come in all shapes and sizes and are a simple and cost-effective means of setting up monitoring virtually anywhere—with the added bonus that you can typically store the video stream in the cloud and access the security camera feed over the internet.

Therein lies the issue, though. Anything you can access over the internet can also be accessed by hackers and cybercriminals over the internet as well. There are stories circulating about attackers tapping into webcams or security cameras and spying on people over the internet, but the camera itself can also be compromised for other purposes.

Armis discovered a situation at one customer where the security cameras had been hijacked and harnessed as part of a botnet—actively trying to infect other cameras and routers on the network. The idea of infected video cameras brings the Mirai botnet to mind—a scenario where vulnerable IP cameras were used to attack other devices and propagate the threat. In this case, though, the cameras were attacking the very network they were installed on.

How Armis Discovered the Problem

With every customer, Armis starts out the same way—by discovering and classifying all devices on the network. We monitored the network traffic and identified cameras that were trying to connect to other cameras and routers over ports 23 and 80—which are reserved for administrative access on the IP-based cameras.

Armis determined that the behavior was anomalous and that it was indicative of methods typically used to spread botnets. We then automatically triggered the switches on the network to block the devices and prevent any further malicious communication.

Why Traditional Security Tools Didn't Detect the Issue

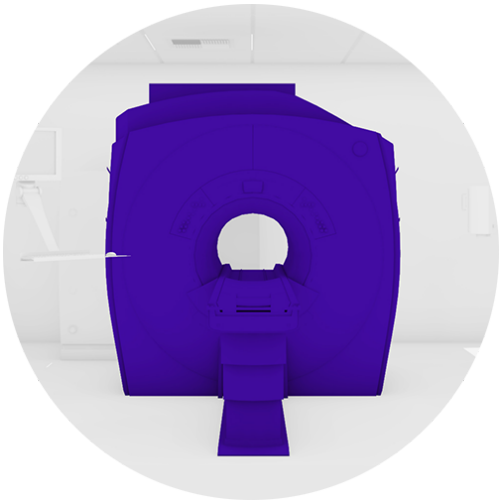
The customer had other traditional security tools in place, but none of them were capable of identifying this threat. Neither the NAC (network access control) or nor the firewall are designed to detect or block this type of activity.

The IPS (intrusion prevention system) also failed to discover this malicious behavior. In theory, an IPS solution that is installed in the right location, configured properly, and updated with the right signatures to recognize the behavior could identify this attack. A UEBA (user and entity behavior analytics) has similar potential to detect this threat under the right conditions. The UEBA is only as good as the data you feed it, though, so it's also very likely that a UEBA would miss this attack.

4. INFECTED HEALTHCARE DEVICE

One of the industries leading the way in innovative connected devices and adoption of IoT technologies is healthcare. Healthcare environments have a high ratio of IoT devices to computers, in some cases as high as 10-to-1, making them particularly susceptible to attacks.

The FDA recently approved a firmware patch for vulnerabilities affecting devices for over 350,000 patients. There have also been stories of hackers compromising X-Ray, MRI and other medical machines such as Orangeworm, and reports of a Russian company selling zero day exploits that can be used to hack into health information management software used in many facilities for patient scheduling and documentation.



An Armis customer in the healthcare industry had an MRI machine that was infected with the WannaCry ransomware that crippled systems around the world in 2017. It's an unfortunate reality that many of the more sophisticated medical devices run on older versions of Windows that are no longer officially supported by Microsoft. The MRI machine in question was running Windows XP—which hasn't been updated by Microsoft since April of 2014, and contains the EternalBlue vulnerability at the heart of the WannaCry attack.

The MRI machine was connected to an internal, protected hospital network, but the vendor of the MRI machines required the hospital to open up additional ports over the public internet for remote vendor support. The underlying Windows XP OS had not been patched or updated for EternalBlue because applying the patch would void the warranty.

How Armis Discovered the Problem

The process is the same when Armis starts working with any customer—we discover all of the devices connected to the network and monitor behavior and traffic from each device. Part of our process is to establish a baseline of normal—not just for each specific device, but also based on the type of device and how it compares with similar devices on the network. We noticed that the MRI machine was behaving anomalously for that type of device—sending and receiving SMB traffic, which shouldn't happen.

Why Traditional Security Tools Didn't Detect the Issue

The existing NAC (network access control), firewall, and IPS (intrusion prevention system) did not detect the issue. NAC simply recognizes and assigns the device to a network segment. Traffic was able to pass through the firewall using the ports the vendor required to be open. IPS is not equipped to identify a threat unless its been updated with the appropriate signatures.

It is possible that a UEBA (user and entity behavior analytics) solution could have detected this threat. If the customer had a UEBA installed and configured in a way that would allow it to see this low level traffic. The MRI machine does not produce any log files, so detection of this threat relies solely on traffic analysis.

5. UNAUTHORIZED NETWORK BRIDGE

Many of the printers in use today are also equipped to communicate over Wi-Fi or Bluetooth to make it more convenient for people to print from any device without having to be physically connected to the network. Some provide their own Wi-Fi hotspot—enabling users to connect directly to the printer itself rather than connecting across a broader network.

As with most technologies—the things that make them simple and convenient for users are double-edged swords that also expose them to risk and make it easier for attackers to exploit them as well.

A recent Armis customer had 145 printers on the network with open Wi-Fi hotspots—potentially allowing any device within range to connect to the network. With another customer, we discovered also printer on the network with an open Wi-Fi hotspot. Here is what we found.

How Armis Discovered the Problem

Armis began by discovering all devices on the network and monitoring network activity—including wireless activity in the customer's airspace. This comprehensive discovery and monitoring enables Armis to discover rogue devices, hotspots, and other unauthorized devices or networks in the customer environment.

We alerted the customer, so they could change the settings on the printer and shut down the open Wi-Fi hotspot. There were no devices connected to the hotspot, but—if there had been—Armis would have discovered those as well and provided the information to the customer to remediate the situation.

Why Traditional Security Tools Didn't Detect the Issue

None of the standard, traditional network security tools used by the customer are equipped to detect an open Wi-Fi hotspot. NAC (network access control) controls access to the network, but it does not monitor for open hotspots or external connections to printers on the network.

The firewall is designed to protect the network perimeter. IPS (intrusion prevention systems) monitor traffic to identify known attack behavior based on the signatures it has available. UEBA (user and entity behavior analytics) analyzes the behavior of users and devices to detect anomalies. None of these security solutions is designed to monitor for or detect open Wi-Fi hotspots or unauthorized connections to those hotspots.

6. PROTECTION OF GAS DISTRIBUTION FACILITIES

Manufacturing and utilities are two industries that benefit significantly from industrial IoT—or IIoT. The ability to use connected sensors, valves, and other controls makes it possible to monitor temperature, humidity, pressure, and other factors in real-time and make adjustments remotely to make sure production and efficiency are optimal.

While this brings new efficiencies and productivity, using IP-based devices in manufacturing and industrial environments also creates a very attractive target for hackers with the potential for catastrophic—or even deadly—consequences. The environments these IoT devices run in were not designed with security in mind, and IoT devices themselves are typically difficult to patch or update, exposing them to significant risk.

Armis was able to help a gas distribution facility detect a compromised device in its environment and identify 600 devices vulnerable to BlueBorne attack.

How Armis Discovered the Problem

The first thing Armis did when it began working with this customer is to perform comprehensive asset discovery across the entire environment. Armis discovered all 2,500 of the remote control and telemetry devices installed at various facilities by the client—and found the compromised device and vulnerable devices in the process.

Fortunately, there were no active connections or attacks detected by Armis. With Armis in place, the environment is continuously monitored—including the wireless airspace—to ensure that any future attacks or suspicious activity will be discovered. The customer can break the kill chain by blocking any device that becomes compromised or blocking any unauthorized network bridge.

Why Traditional Security Tools Didn't Detect the Issue

Traditional security tools are not capable of adequately protecting IoT devices. NAC (network access control) does not discover compromised IoT devices and has no ability to detect vulnerabilities like BlueBorne. A firewall is designed to prevent unauthorized access at the network perimeter. It doesn't monitor internal devices or traffic and has no way to detect BlueBorne vulnerabilities. Solutions like IPS (intrusion prevention systems) and UEBA (user and entity behavior analytics) might identify an active threat with the right signatures or configuration, but they are also not designed to detect IoT vulnerabilities inside the network.

7. ROGUE NETWORK STEALING CREDENTIALS

In office environments and public spaces, there are often multiple wireless access points to connect to. Some devices are designed to connect automatically with the best available network. In situations where users choose the wireless network, many people will just connect to whichever network looks the strongest.

Attackers have learned to exploit these behaviors with spoofed wireless access points—creating a rogue and masquerading networks that dupes people and devices into connecting to it instead; offering an opportunity for the attacker to access sensitive data or capture user credentials.

Armis often finds rogue networks at customers—a Wi-Fi Pineapple device—with corporate devices attached to it, possibly exposing or compromising sensitive data. This is one such story.

How Armis Discovered the Problem

Armis discovered and classified all devices in the customer environment and the traffic volumes associated with each device. Armis also gleaned Wi-Fi traffic volume data from the wireless LAN controller (WLC), including traffic on the Guest network and in the airspace—which is typically invisible to or ignored by other security solutions.

The Armis risk analysis engine identified anomalous traffic volume and timing on the Guest network and traced it to a rogue network created by the Wi-Fi Pineapple.

Why Traditional Security Tools Didn't Detect the Issue

The customer followed standard network security best practices and had other security tools in place, but none of those products has the features and capabilities necessary to detect a threat such as this.

NAC (network access control) is designed to inventory devices and ensure each device is assigned to the appropriate network. NAC does not monitor traffic volumes for anomalies, nor can NAC discover rogue access points in the enterprise airspace.

The firewall protects the network perimeter, but it has no ability to identify or block a rogue Wi-Fi access point or Wi-Fi network inside the network. IPS (intrusion prevention systems) and UEBA (user and entity behavior analytics) solutions can detect known threats or possibly identify suspicious activity if configured properly, but neither is designed to detect rogue wireless networks or monitor traffic and activity that might occur on a rogue network.

THE NEW SECURITY LANDSCAPE

IoT is more than a buzzword. These new, unmanaged devices are the new attack landscape, as we have seen. This is not simply from news headlines, but based on the findings, we see every day at Armis. Devices you can't install a traditional security agent on. And patching or updating their operating systems can be extremely challenging for a variety of reasons. Taken together, this presents a near perfect storm of risk — devices that are accessible, vulnerable, and unprotected. Enterprises are just now confronting the reality of how to protect themselves from these new airborne threats. Armis is purpose built for this new world, focused on discovering and analyzing these devices in order to protect organizations.

---

[1] Gartner Press Release, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016," February 7, 2017. https://www.gartner.com/newsroom/id/3598917

[2] "Gartner Expects 2018 IoT Security Spending to Reach $1.5 Billion," Dark Reading, March 21, 2018 https://www.darkreading.com/endpoint/gartner-expects-2018-iot-security-spending-to-reach-$15-billion-/d/d-id/1331334

About Armis

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

arims.com

EXPLOIT SUMMARIES

1. Compromised Tablet

Unauthorized Video Streaming

- Every conference room had a tablet to control the video system on the guest network.
- The tablet in one conference room was streaming video and audio
- This represented a leakage of sensitive conversations.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Gleaned WiFi traffic • Discovered and classified all devices and associated traffic volumes • Risk analysis engine identified anomalous traffic with the device	• Inventories devices and controls entry to the network. • Does not monitor traffic volumes • Not designed to detect anomalous devices. Video traffic seemed “normal”	• Designed to protect the perimeter. • Not designed to detect anomalous devices. • Data streaming from tablet seemed “normal” to firewall	• IPS looks for attacks, not for “normal” traffic such as video. • UEBA is not designed to detect anomalous devices. Video streaming from tablet seemed “normal” to UEBA

2. Compromised Smart TV

Smart Device Attempting to Infect Other Devices

- Boardroom was equipped with a Smart TV that had malware on it.
- Malware on the Smart TV was trying to infect nearby devices via Bluetooth

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Monitors Bluetooth & network traffic • Correlated traffic and activity to devices and locations. • Large amounts of WiFi & Bluetooth traffic detected. • TVs were beaconing to infect nearby devices	• The Smart TV was whitelisted on the NAC, so it let the TV onto the network. • Post-admission, NAC does not monitor behavior or external wireless connections	• The Smart TV was not sending out anything through the gateway. • The FW cannot see external wireless connections from devices	• The Smart TV was not sending out anything over the network. • The IPS cannot see external wireless connections from devices

3. Compromised Security Camera (& Routers)

Botnet Attack

- Security cameras on the network were compromised, part of a botnet, trying to propagate.

Armis	NAC	Firewall	IPS/UEBA
			
• Discovered and classified all devices • Monitored traffic • Risk Analysis Engine saw cameras trying to connect to other cameras & routers via ports 23 and 80 • Triggered switches to quarantine the devices	• Inventories devices and controls entry to the network. • Does not monitor traffic over time. • Not designed to detect anomalous behavior.	• Not designed to monitor internal network traffic. • Firewalls have difficult time detecting botnet propagation or C&C because it is disguised as peer-to-peer	• IPS could have discovered cameras if IPS was in the right location and had a behavior signature • UEBA might have discovered the behavior anomaly, if it had the right data

4. Infected Healthcare Device

Connected Smart Healthcare Device Attempting to Infect Other Devices

- MRI machine had an external internet connection for vendor remote support.
- Running Windows XP, unpatched since it would void the warranty.
- Infected with WannaCry and trying to infect other Windows systems via SMB.

Armis	NAC	Firewall	IPS/UEBA
			
• Discovered devices • Correlated traffic with each device • Risk analysis engine saw anomalous SMBv1 traffic. • Trigger sent to NAC to quarantine MRI machine	• Inventories devices and controls entry to the network. • Does not detect attacks.	• Designed to protect the perimeter. • Not designed to monitor internal network traffic	• UEBA could potentially detect the WannaCry if it was installed in a way that allowed it to see this low level traffic.

5. Unauthorized Bridge Network

Printer Allowed Anyone to Connect

- A printer that is connected to the wired network has an open hotspot on it, providing access to unauthorized parties.

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Monitored the airspace • Discovered printer with open hot spot, provided an alert • If there were any actual connections to the printers, Armis would discover those, too	• Inventories devices and controls entry to the network • Does not monitor open hotspots or external connections to printers	• Designed to protect the perimeter • Does not monitor open hotspots or connections to those hotspots	• IPS looks for attack behavior, not for dormant open hotspots • UEBA would not see the hotspot or the external connections

6. Protection of Gas Distribution Facilities

IIoT Devices at Gas Distribution Facilities Needed to be Protected

- WiFi-based remote control and telemetry systems
- Desire to protect systems from local attack

Armis	NAC	Firewall	IPS/UEBA
✓	✗	✗	✗
• Discovered and Discovered 2500 remote control and telemetry devices • Risk analysis engine saw one compromised device • Risk analysis engine saw 600 devices that were vulnerable to BlueBorne attack	• Does not discover compromised IoT devices • Does not detect BlueBorne vulnerabilities	• Designed to protect the perimeter • Not designed to monitor internal devices • Does not detect BlueBorne vulnerabilities	• Not designed to detect IoT vulnerabilities inside the network.

7. Rogue Network Stealing Credentials

Theft of Network Credentials

- A corporate device is connecting to a pineapple that is collecting its Active Directory credentials or hashes

Armis	NAC	Firewall	IPS/UEBA
			
• Detects when a corporate device connects to an external network • Detects when credentials or hashes move over unencrypted wireless traffic	• Detects and controls entry to the corp network only • Would not “see” the external network, nor the connections to it	• Designed to protect the perimeter • Would not “see” the external network, nor the connections to it	• Neither IPS nor UEBA would “see” the external network and the connections to it

About Armis

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

20190527.1