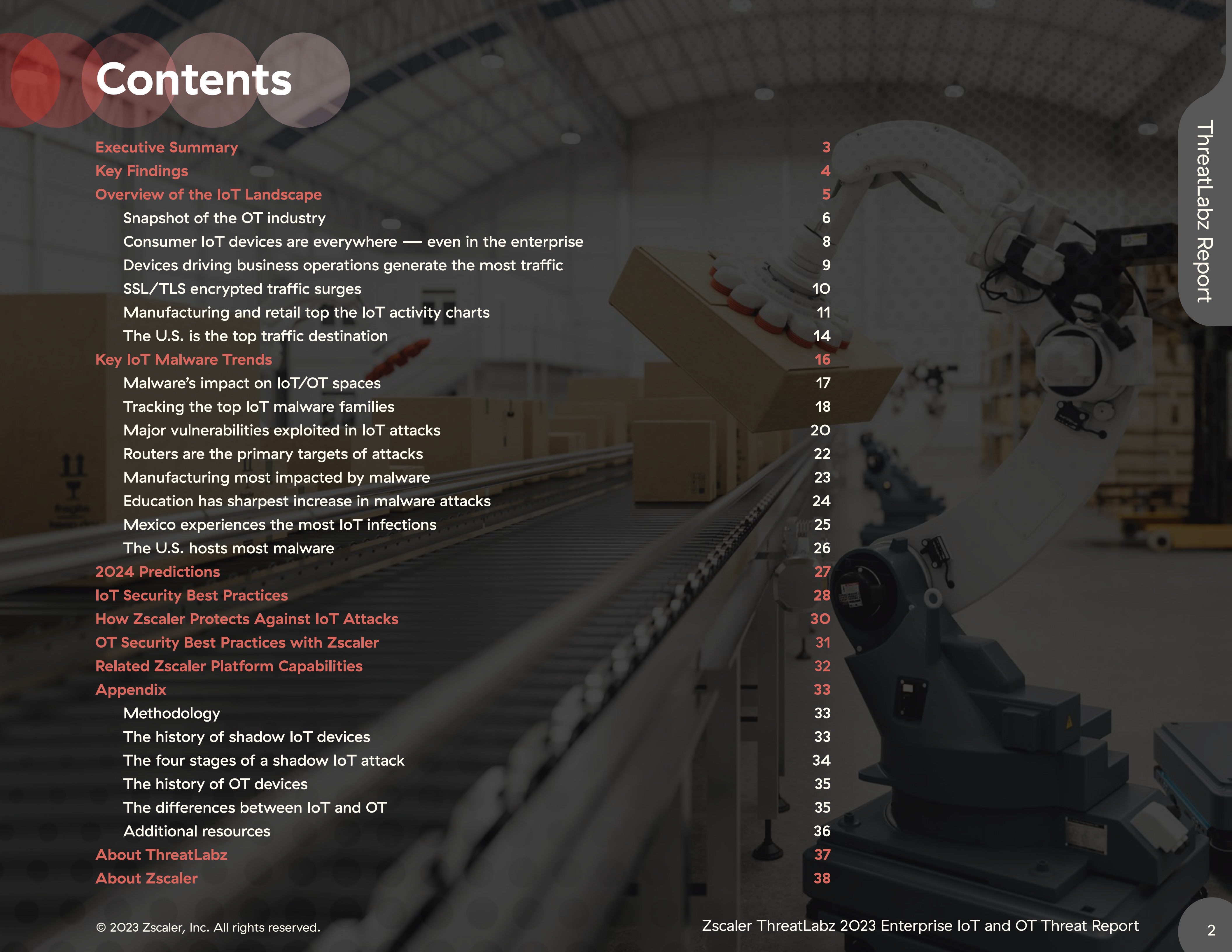
zscaler™

ThreatLabz Report

# Zscaler ThreatLabz 2023 Enterprise IoT and OT Threat Report



# Contents

# Executive Summary

**Welcome to the era of connectivity and convenience. Internet of Things (IoT) devices have undoubtedly transformed how we live, work, and manage Operational Technology (OT) environments. Overall, the global number of connected IoT devices is projected to surpass 29 billion by 2027, a sharp increase from 16.7 billion in 2023.[1]**

This proliferation of devices and smart technology also represents more opportunities to be exploited by cybercriminals — turning IoT connectivity into a potentially inconvenient or, even worse, devastating reality.

To help organizations better understand the current IoT landscape and how to protect their corporate networks, the Zscaler ThreatLabz research team analyzed device traffic and IoT malware data from the Zscaler Zero Trust Exchange, the world's largest inline security cloud.

Over the course of three months, the ThreatLabz team identified 3 trillion IoT device transactions from 850+ unique device types. The highest volume of IoT device traffic came from the manufacturing industry — a sign of the times as manufacturers adopt smart technology to meet modern requirements for speedy supply chain fulfillment and innovation.

An in-depth look at malware activity over a six-month period found approximately 300,000 blocked attacks from known IoT threat actors. This represents a 400% increase in IoT malware attacks compared to the previous year (January—June 2022). Zscaler researchers discovered that the Mirai and Gafgyt botnets continue to drive the rise in IoT malware attacks.

As more organizations and individuals rely on internet-connected devices, the responsibility of minimizing security risks and vulnerabilities is largely in their hands. Regulatory frameworks and guidelines for device manufacturers *are* in the works[2,3] but are still in the nascent stages.

The Zscaler ThreatLabz 2023 Enterprise IoT and OT Threat Report will give you valuable insights into the state of IoT threats and the best practices for protecting your organization.

The report also offers strategies to ensure the resilience of OT environments, spotlighting the convergence of IoT and OT driven by digital transformation in critical sectors such as manufacturing and utilities.

[1] Number of connected IoT devices growing 16% to 16.7 billion globally
[2] Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products
[3] The UK Product Security and Telecommunications Infrastructure (Product Security) regime - GOV.UK

# Key Findings

**IoT device traffic increased by 18%** compared to our last report, consistent with a steady adoption of IoT and connected devices.

**IoT malware attacks grew more than 400%** in the Zscaler cloud compared to the same period in 2022, highlighting the need to prioritize protection against malware.

**Botnet activity continues to dominate,** with the Mirai and Gafgyt malware families accounting for **66%** of attack payloads.

**Cybercriminals are targeting legacy vulnerabilities,** with **34** of the **39** most popular IoT exploits specifically directed at vulnerabilities that have existed for more than three years.

**Routers were the most targeted device,** as their always-connected, ubiquitous nature and function as a central control point for network traffic makes routers a prime target.

**Manufacturing was the top targeted industry** and bears the brunt of malware attacks, experiencing **54.5%** of all attacks and an average 6,000 attacks per week.

**Education experienced a substantial increase in malware attacks** since 2022 with a percentage jump of **961%**.

**Mexico and the United States were the most targeted countries,** accounting for **69.3%** of attacks, collectively.

# Overview of the IoT Landscape

The IoT landscape consists of billions of interconnected devices worldwide that help enhance efficiency, automation, and convenience for home, work, and play. Such massive connectivity also gives rise to an increasingly complex threat landscape. Understanding the intricacies of this landscape is critical to safeguarding networks against IoT threats.

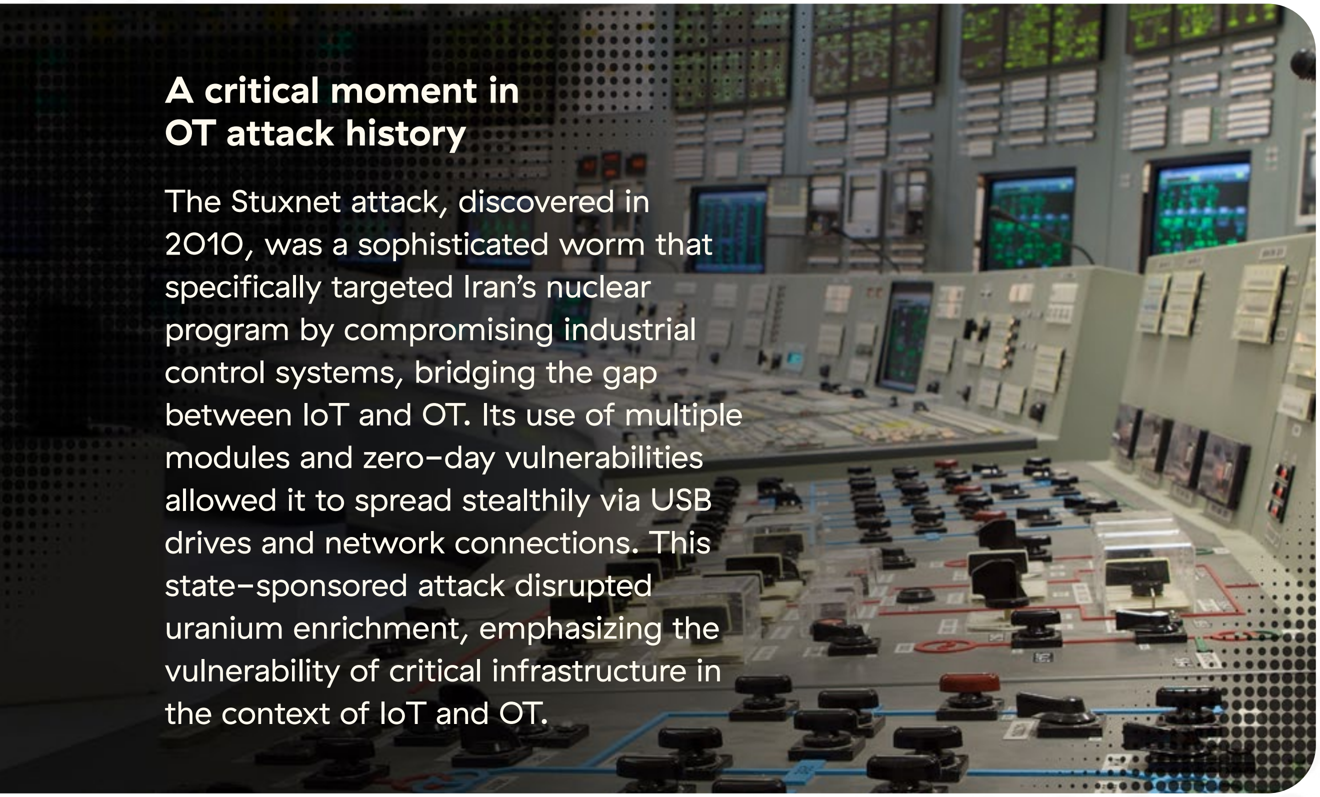
This section aims to shed light on the IoT devices and traffic passing through the world's largest inline security cloud.

The following highlights will be explored in the sub-sections to follow:

- **Consumer devices are "smart" and most common,** but business process-oriented IoT generated the most transactions.
- **Manufacturing and retail devices accounted for 50%+ of transactions,** highlighting their widespread adoption and business-critical function in these sectors.
- **Nearly two-thirds (62.1%) of total IoT transactions happened over SSL/TLS,** indicating that more organizations are taking care to encrypt IoT traffic.
- **Enterprise, home automation, and entertainment devices** are generating the highest counts of plaintext transactions.
- **Russia and China** are attracting the most entertainment and home automation device traffic.

## Snapshot of the OT industry

Operational Technology (OT) systems, which are the backbone of critical processes in sectors like manufacturing, energy production, and utilities, now integrate with IoT devices. Because the OT landscape is characterized by legacy systems that were designed and implemented at a time when cybersecurity was secondary, the IoT/OT landscape is highly susceptible to “cyber-physical” attacks. Moreover, the need for remote access by employees and third-party vendors to OT and IIoT (Industrial Internet of Things) systems via VPN can substantially increase the attack surface of these systems — particularly as VPN vulnerabilities have become a primary attack vector for cybercriminal organizations.



### A critical moment in OT attack history

The Stuxnet attack, discovered in 2010, was a sophisticated worm that specifically targeted Iran’s nuclear program by compromising industrial control systems, bridging the gap between IoT and OT. Its use of multiple modules and zero-day vulnerabilities allowed it to spread stealthily via USB drives and network connections. This state-sponsored attack disrupted uranium enrichment, emphasizing the vulnerability of critical infrastructure in the context of IoT and OT.

## Top 5 IoT Devices

IoT device traffic increased by 18% compared to two years prior, consistent with a steady adoption of IoT and connected devices. Network-connected IoT devices are everywhere in the modern enterprise, and as these top devices show, they may or may not always be sanctioned by the IT department.

### Set-Top Box

Set-top boxes, which connect televisions to the internet and other applications, account for the most IoT traffic worldwide.

### Smart TV

Smart TVs make up the majority of entertainment and home devices, and are more likely to route to Russia and China.

### Smart Watch

A compromised smart watch could expose sensitive corporate data, putting it at risk of malicious use.

### Data Terminal

Data collection terminals account for 62.1% of all IoT traffic in the manufacturing sector. They capture information from various sources for tracking purposes.

### Media Player

Media players enable the playback of various multimedia content and if not secured properly, they can serve as entry points for cyberattacks.

## Consumer IoT devices are everywhere — even in the enterprise

When ThreatLabz researchers reviewed IoT devices sending traffic to the Zscaler cloud, consumer devices topped the list. This is a stark reminder that these often unsanctioned, “shadow” IoT devices always permeate our networks.

Three specific consumer device categories accounted for almost half of all IoT devices. The category with the highest number of individual devices was by far TV set-top boxes (like Apple TV, Roku, Fire TV, etc.), which enable analog television sets to receive digital broadcasts (23.9%) followed by smart watches (13.8%) and smart TVs (13.3%).

It’s noteworthy that business-critical devices like digital signage media players (9.3%) and data collection terminals (8.5%) rounded out the top five.

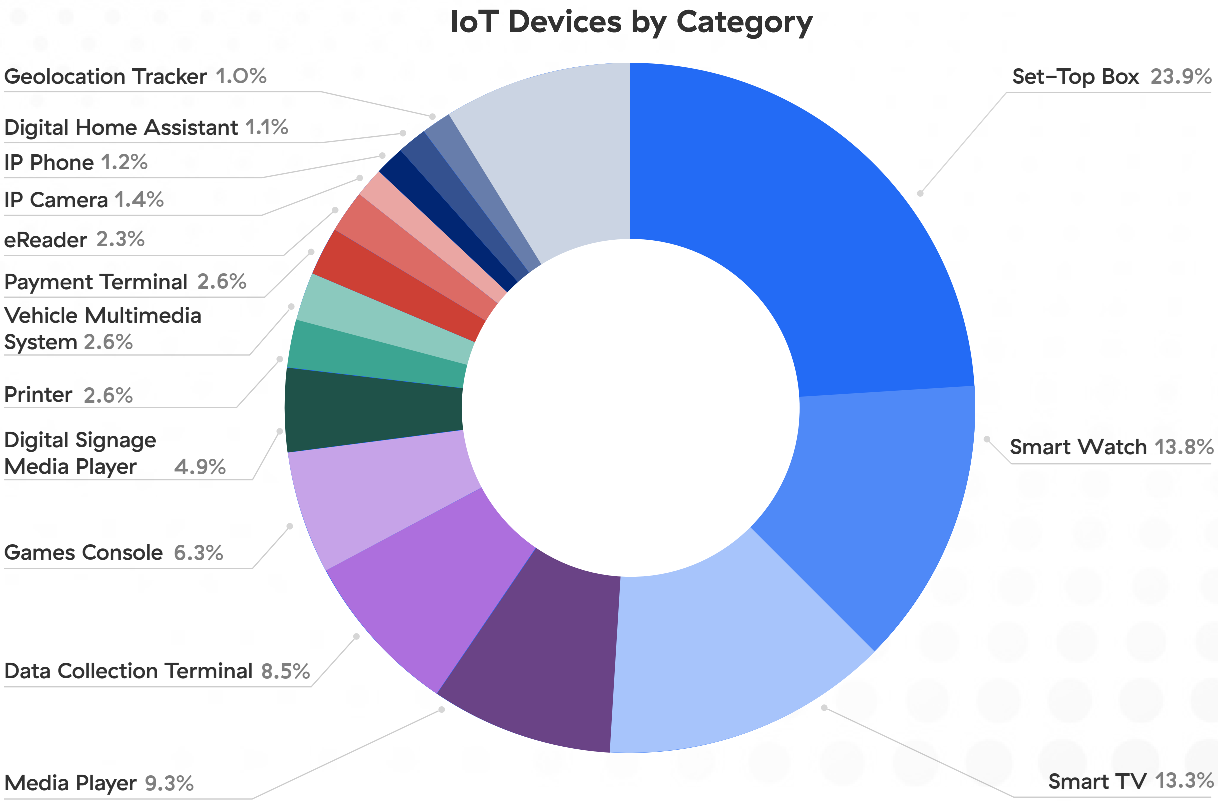


*Figure 1: Breakdown of the top IoT device categories sending traffic to the Zscaler cloud*

## Devices driving business operations generate the most IoT traffic

IoT devices that businesses rely on for operations generated the largest amount of outbound data transactions. The majority of IoT transactions came from data collection terminals (51.9%), which are wireless barcode readers used in manufacturing, engineering, logistics, and warehousing applications. These were followed by printers at 25.2% and digital signage media players at 10.6%.

### Volume of IoT Transactions by Device Category

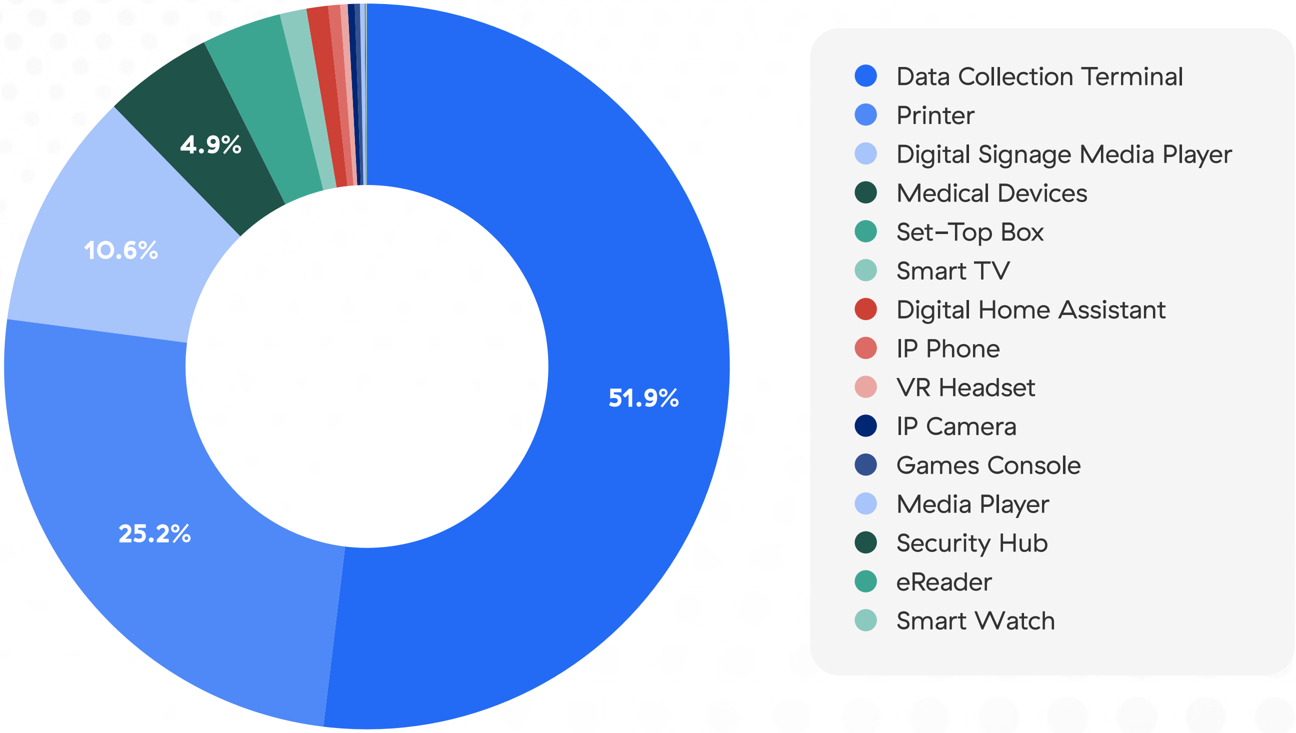


*Figure 2: Breakdown of the IoT devices generating the most traffic*

## SSL/TLS encrypted traffic surges

And for some good news: 62.1% of all IoT transactions employed SSL/TLS channels, which encrypt traffic for protection. In contrast, we observed that 37.9% of transactions occurred over unencrypted, plaintext channels. These findings are markedly different from our 2020 report results, wherein only 17% of transactions used SSL/TLS.

*(Disclaimer) – Our analysis focused on the usage of HTTP versus HTTPS.

What's more, all observed devices employed SSL/TLS to some extent, but the percentage of communications that were actually encrypted varied widely by device type. Enterprise and home entertainment devices predominantly used plaintext communications. Healthcare, manufacturing, and retail devices primarily used encrypted communications.

While the prevalence of SSL/TLS is a positive sign for sectors where data privacy and integrity are paramount, it's good to note that encrypted channels can be (and often are) exploited by threat actors — enabling them to evade detection, move laterally within networks, and steal data without raising alarms. In fact, more than 85% of attacks were encrypted in 2022, according to the ThreatLabz State of Encrypted Attacks Report.

This reality makes it paramount for organizations to have visibility into and inspect all encrypted traffic in accordance with zero trust principles.

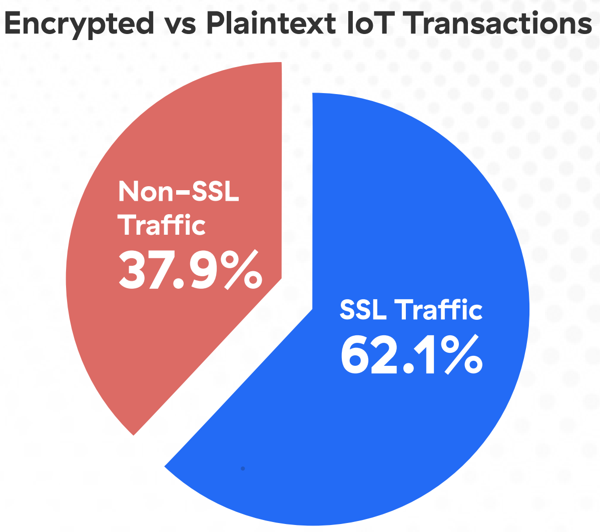


*Figure 3: Comparison of SSL/TLS vs. non-SSL transactions*

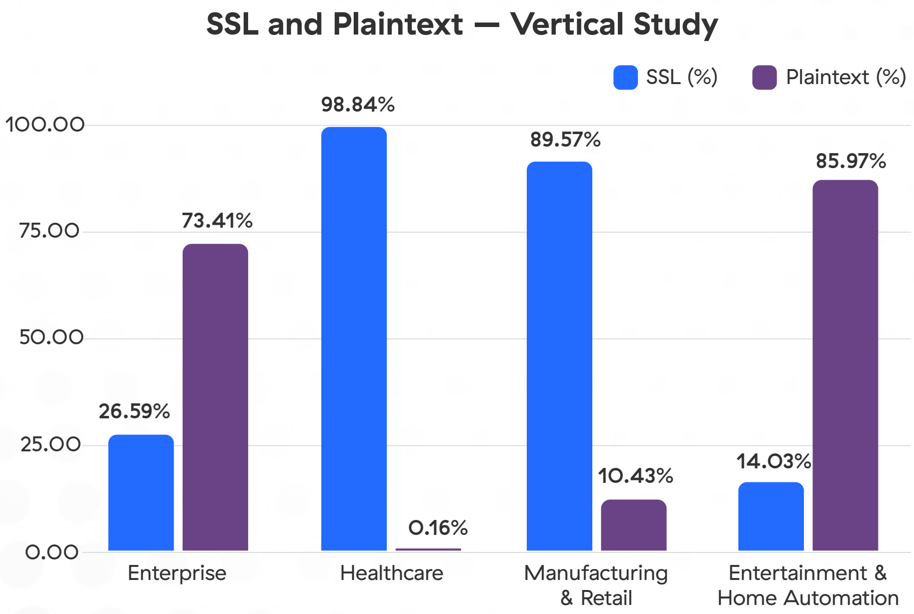


*Figure 4: SSL/TLS vs. plaintext transactions for the top traffic-generating verticals*

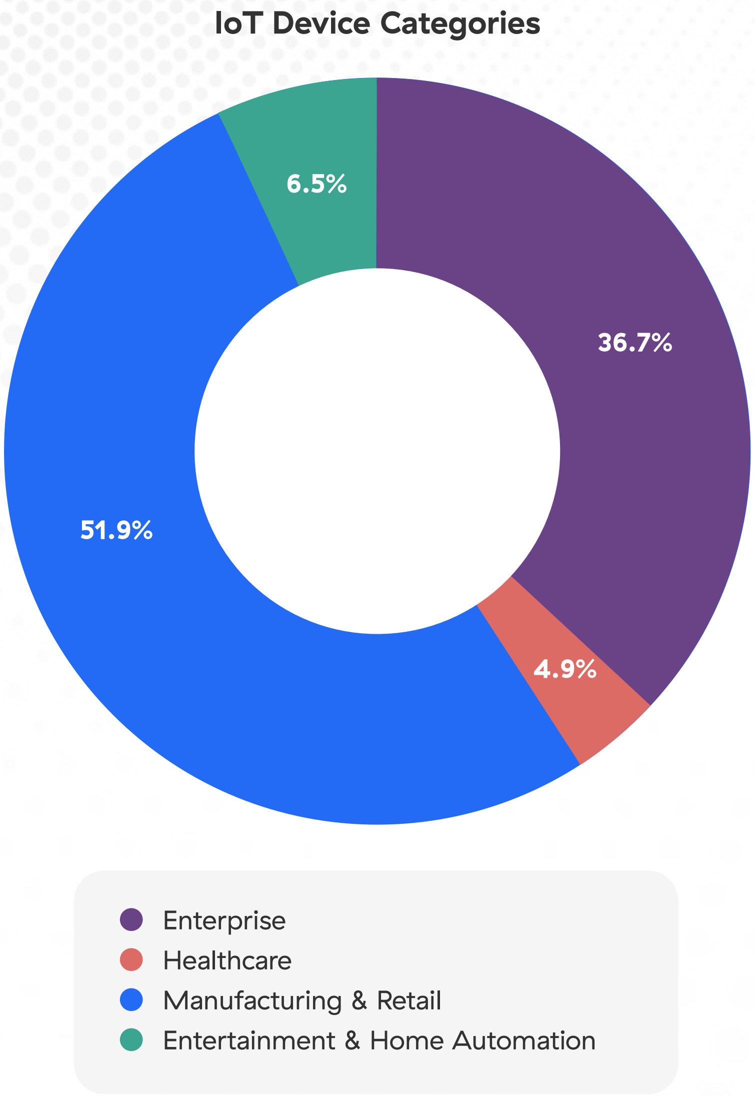


*Figure 5: Vertical IoT device categories generating the most transactions*

## Manufacturing and retail top the IoT activity charts

Breaking traffic into different device categories, nearly 90% of traffic is from manufacturing, retail, and enterprise devices.

- **Manufacturing and retail devices** accounted for 51.9% of transactions, including 3D printers, geolocation trackers, industrial control devices, automotive multimedia systems, data collection terminals, and payment terminals.
- **Enterprise devices** accounted for 36.7% of transactions and comprised digital signage media players, digital video recorders, IP cameras and phones, printers, and networking devices.
- **Healthcare devices** accounted for 4.9% of transactions and included a number of medical devices that come primarily from three manufacturers: GE Healthcare, Abbott Laboratories, and Hologic.
- **Entertainment and home automation devices** accounted for 6.5% of transactions generated from a wide variety of devices such as digital home assistants, media players, set-top boxes, smart glasses, smart home devices, smart TVs, and smart watches.

**Manufacturing leads the way for unique devices**

We observed that the manufacturing and services verticals comprise the highest number of unique IoT devices by count, as shown in the chart below. Moreover, the manufacturing sector's substantial lead in unique IoT devices, nearly tripling the count of other sectors, underscores its dedication to automation and digitization, positioning it as a frontrunner in leveraging IoT for enhanced production efficiency, product quality, and innovation within Industry 4.0[1].

## Unique Devices — Customer Verticals

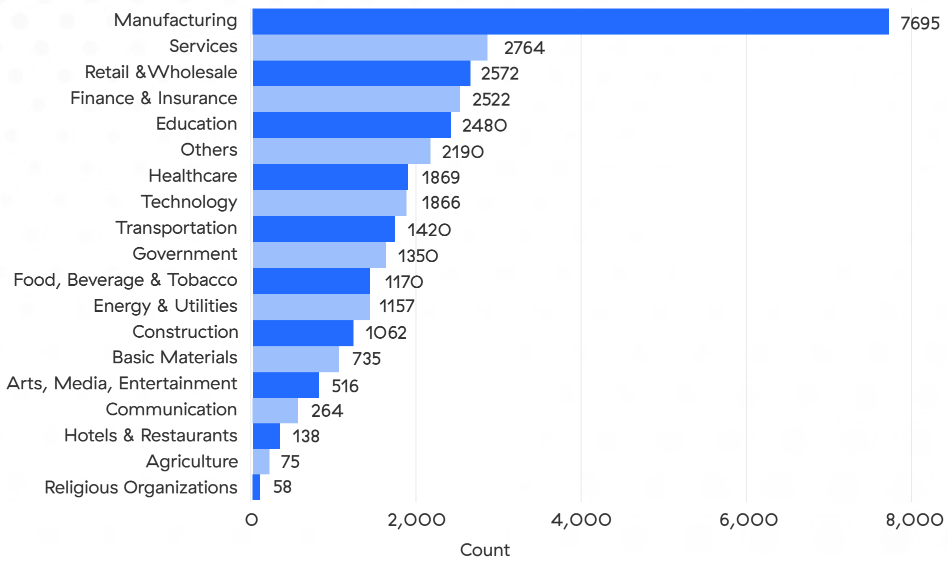
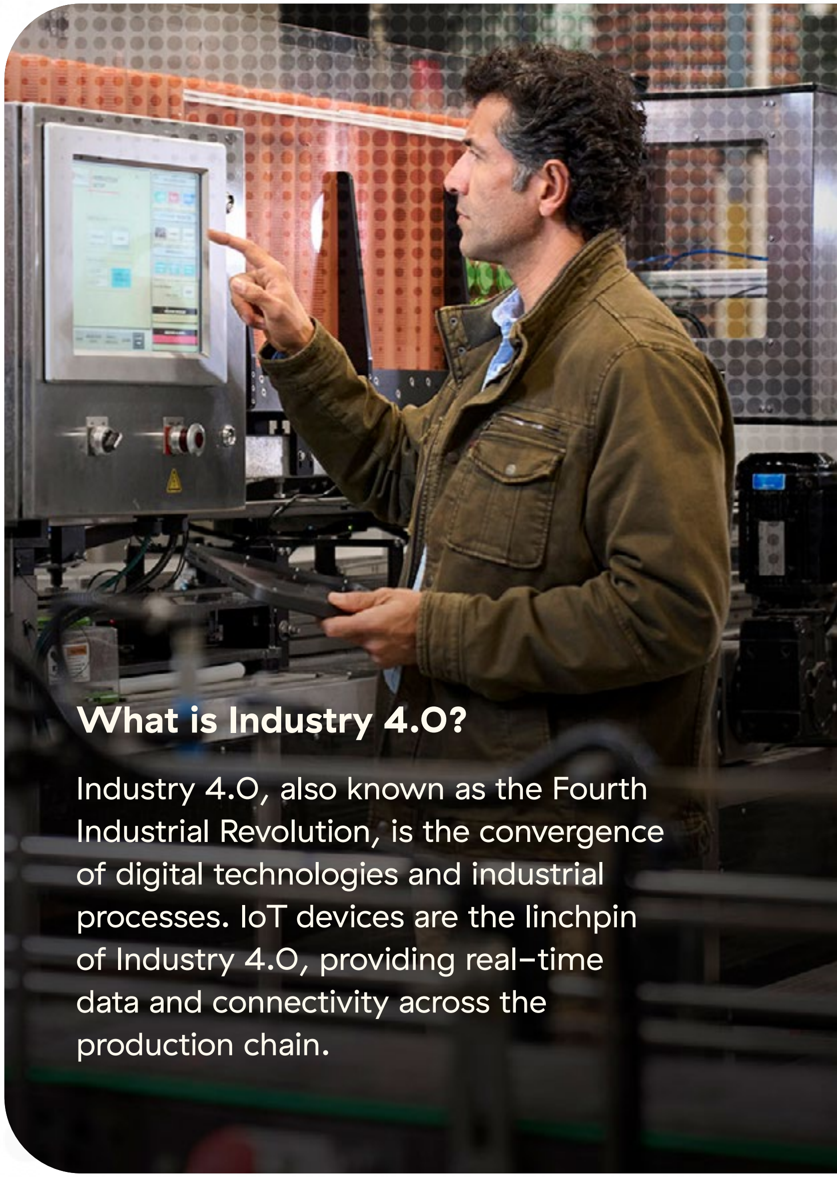


*Figure 6: Unique device count by vertical*



### What is Industry 4.0?

Industry 4.0, also known as the Fourth Industrial Revolution, is the convergence of digital technologies and industrial processes. IoT devices are the linchpin of Industry 4.0, providing real-time data and connectivity across the production chain.

[1] sap.com/products/scm/industry-4-0/what-is-industry-4-0.html

### Retailers generate the most IoT traffic

Our traffic analysis revealed that retail and wholesale customers contribute the highest volume of traffic, followed by manufacturing customers.

## Traffic by Customer Verticals

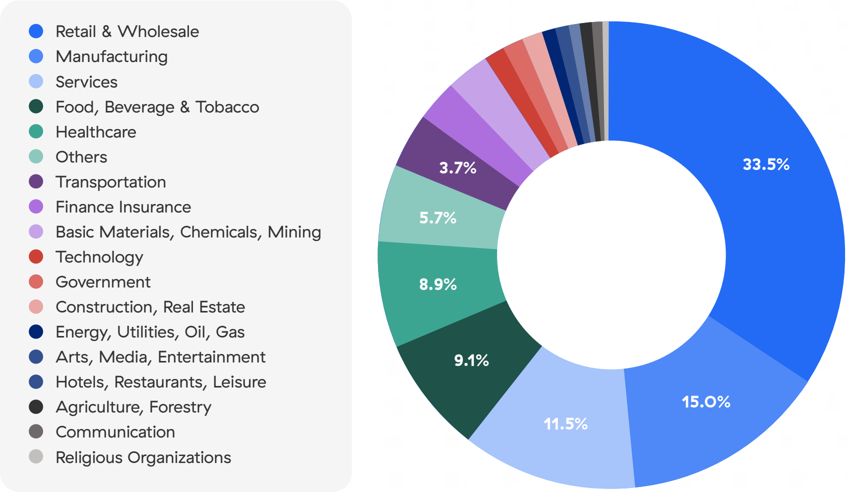


*Figure 7: Traffic analysis by vertical*

## The U.S. is the top traffic destination

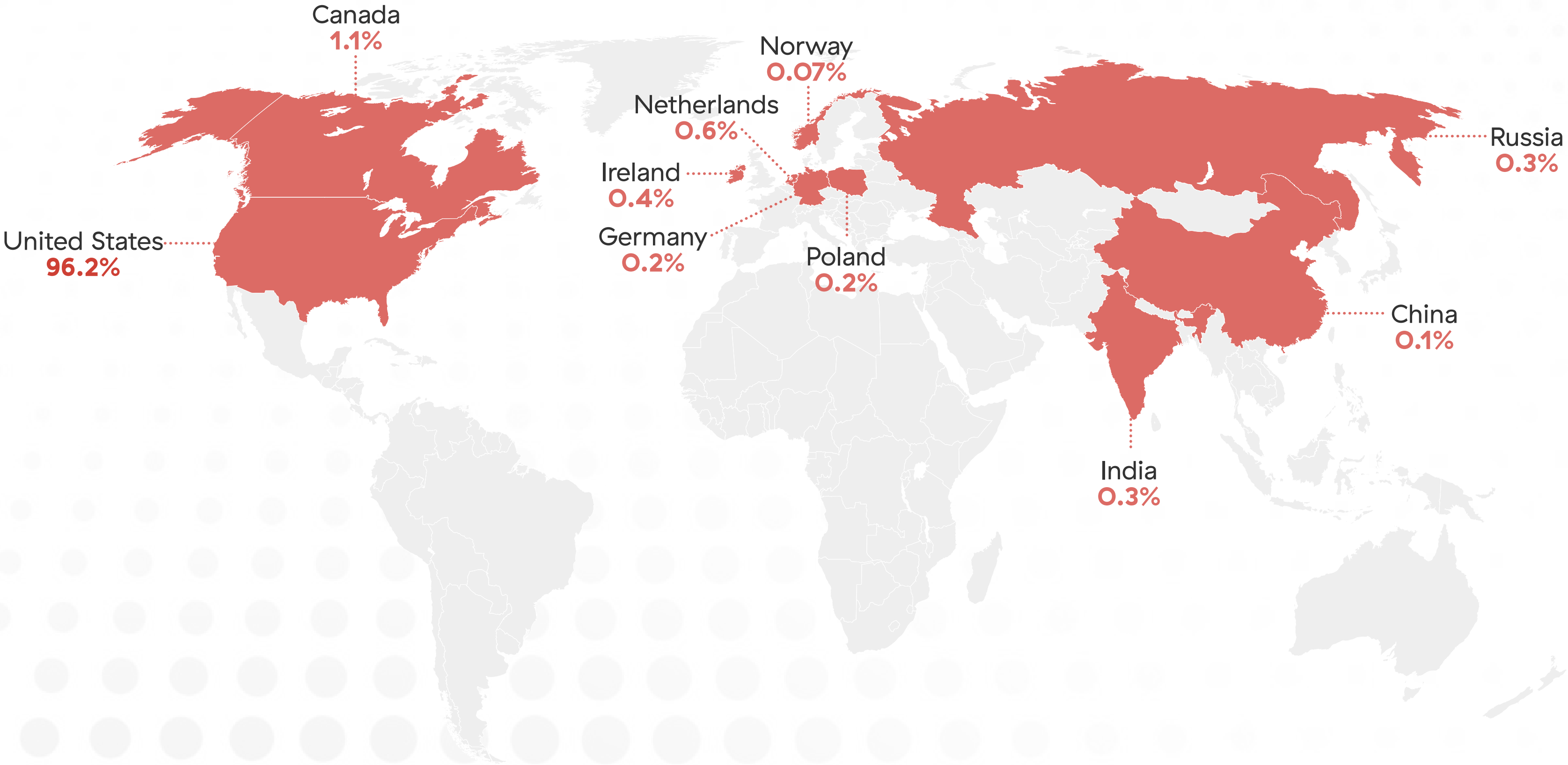
ThreatLabz researchers looked at the countries that IoT devices were routing data to — referred to as “destinations.” Most of this communication is legitimate, with the IoT devices doing what they are designed to do, which is send and receive data.

The United States was by far the top destination, receiving 96.2% of traffic, followed by Canada and Netherlands. The top ten destination countries are displayed below.

The top ten destinations (where the device traffic was being sent) by the highest number of unique IoT devices were:

- United States
- Canada
- Netherlands
- Ireland
- Russia
- India
- Poland
- Germany
- China
- Norway

*Figure 8: A global map showing the top 10 destinations for IoT data*



**Entertainment and home automation devices frequently route to China and Russia**
Devices from entertainment and home categories like smart TVs, game consoles, set-top boxes, and IP cameras are the primary contributors to traffic headed to China and Russia. While much of this is legitimate non-malicious traffic, these are destinations that ThreatLabz considers to be suspicious due to their potential for government spying and other data vulnerabilities.

On the other hand, devices designed for the enterprise, like data collection terminals, had less than 4% of their traffic going back and forth to suspicious destinations.

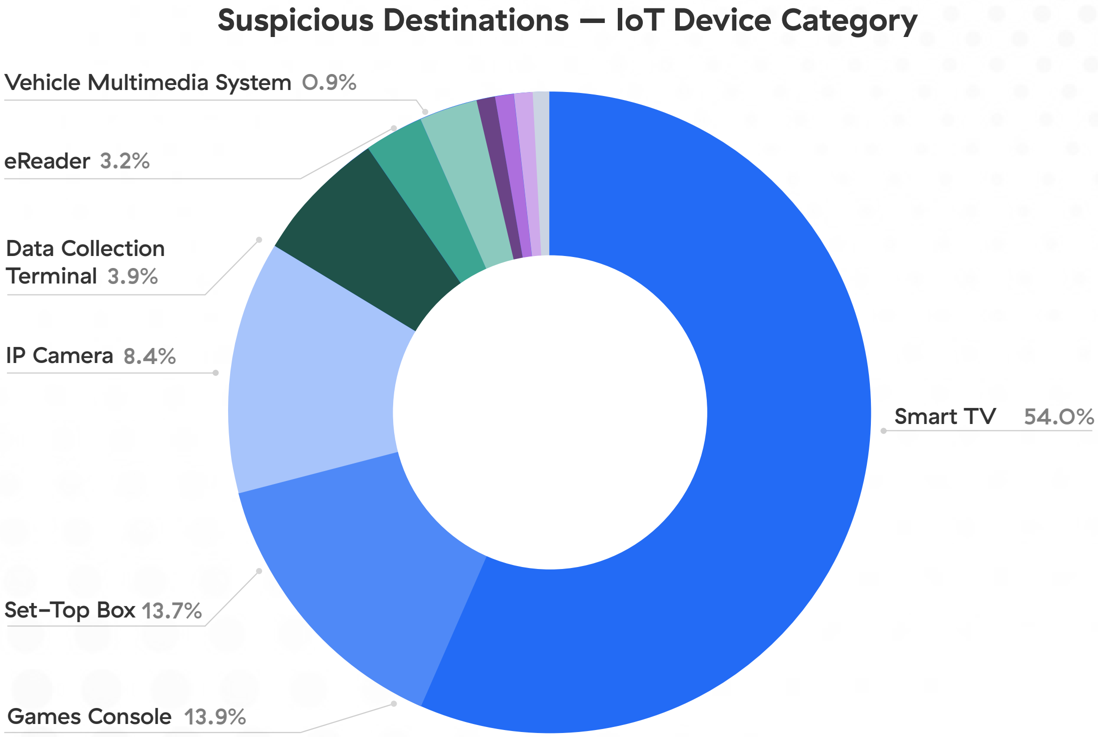


*Figure 9: Breakdown of IoT devices that were sending traffic to China and Russia*

# Key IoT Malware Trends

The threat of IoT malware looms large for organizations, individuals, and governmental entities. Overall, we saw a notable increase in malware attacks compared to 2022, with a five-fold growth in the number of blocked transactions, representing over 350 unique attack payloads. The Mirai and Gafgyt malware families continue to drive the majority of attacks, highlighting the continued IoT botnet risk.

This significant year-over-year growth in IoT malware is further proof of the relentlessness of cybercriminal organizations to adapt to evolving conditions and continue to escalate the scale of IoT malware attacks against enterprises.

The following highlights will be explored in the sub-sections to follow:

- **400% growth in IoT malware attacks,** with 5x the number of blocked IoT transactions compared to 2022.
- **350+ unique malware attack payloads,** highlighting the diversity of the IoT malware landscape and the breadth of vulnerabilities exploited.
- **66% of blocked payloads come from the Mirai and Gafgyt malware families,** showcasing the prevalence of the IoT botnet risk.
- **Nearly 75% of exploited CWEs are command injection vulnerabilities.** These are unauthorized executable input commands, often used to download and execute stager scripts or malicious binaries.
- **With only 5 of the 39 most popular IoT exploits being disclosed in the past three years,** it's evident that attackers are exploiting legacy vulnerabilities.

## Malware’s impact on IoT/OT spaces

Malware trends that specifically target Internet of Things (IoT) devices have emerged as a significant threat to operational technology (OT) systems. The interconnectedness of IoT and OT allows malware to travel from corporate networks into critical OT systems, not only disrupting important processes but endangering the safety and lives of human beings who get caught in a “cyber-physical” attack. Moreover, the VPNs that remote contractors use to connect to OT systems have themselves become key attack vectors and another entry point for malware into the network.

## Tracking the top IoT malware families

Mirai and Gafgyt continue to drive the majority of IoT malware attacks. From a blocked transaction perspective — including payloads, payload URLs, and command and control (C2) communications — Mirai alone caused 91% of blocks. When it comes to blocked payloads, overall, Mirai and Gafgyt caused 46% and 20% of blocks, respectively. These findings correspond with the reported rise in IoT botnet-driven distributed denial-of-service (DDoS) attacks, which, in the first half of 2023, led to an estimated global financial loss of $2.5 billion[1].

The IoT malware landscape is broad, however. Here is an analysis of the top IoT malware families driving attacks:

### Mirai

Mirai is a botnet that uses brute-force techniques to attack IoT devices through various protocols. Mirai also exploits vulnerabilities in IoT devices to infect other IoT devices. These targeted vulnerabilities mostly exist in management frameworks, and by exploiting them, cybercriminals achieve remote code execution. Infected devices are often turned into bots as part of a larger botnet army. Mirai has been one of the most prolific IoT malware families for years, waging what was the largest DDoS attack in history back in 2016.[2]

### Gafgyt

Gafgyt is a malware that infects Linux systems to launch DDoS attacks. This malware has spawned numerous variants since its 2015 source code leak, and has since infected millions of devices, with the majority being IoT devices, particularly cameras and DVRs. These botnets have been responsible for DDoS attacks of up to 400 Gbps in intensity.[3]

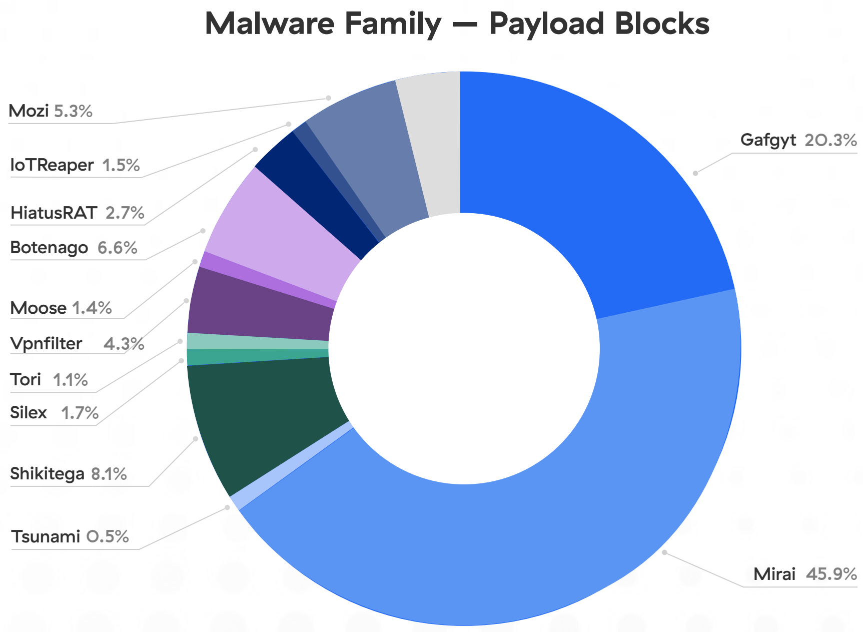


*Figure 10: Top IoT malware families observed in the Zscaler cloud, January—June 2023*

[1] www.nokia.com/networks/security-portfolio/threat-intelligence-report/
[2] info.zscaler.com/resources-industry-reports-the-state-of-encrypted-attacks-2022
[3] minim.com/blog/smart-home-cybersecurity-news-roundup-what-is-gafgyt-malware-october-2019-edition

## 8 prolific IoT malware families

### BotenaGo

This malware, written in Golang and discovered in 2021, employs 30 exploit functions and poses a significant threat to routers and IoT devices. This is because it creates backdoors for remote control via port 19412.[1]

### HiatusRAT

This malware gives the attacker remote access to the compromised machine after infection. The threat actor can track activity on router ports relevant to file transfers and email conversations, thanks to the packet capture program.[2]

### IoTReaper

This malware botnet infects other IoT devices to create a global botnet. Its ability to spread from device to device means it can spread quickly once it gains access to a network and begins executing commands from a C2 server.[3]

### Moose

This malware family mainly targets Linux-based consumer routers. The compromised devices serve two purposes: intercepting unencrypted network traffic and providing proxy services to the operator of the botnet.[4]

### Mozi

This botnet, discovered in 2019, primarily infects vulnerable IoT devices by exploiting weak or default usernames and passwords. Once a device is compromised, it becomes part of the Mozi botnet, which can be controlled by malicious actors.[5]

### Shikitega

This malware is known for targeting endpoints and IoT devices that are running Linux-operating systems. Shikitega is delivered through a multi-stage infection process, with each module responsible for specific tasks.[6]

### Silex

This malware exploits weak or default credentials to quickly spread and wipe firmware as a means to “brick” them — essentially turning devices into useless, non-functional pieces of equipment.[7]

### VPNFilter

This malware affects routers and storage devices by using backdoor accounts and exploits of several known vendors. It operates in multiple stages that include initial infection, C2 communications, and the third stage, in which the payloads are deployed.[8]

[1] cybersecurity.att.com/blogs/labs-research/att-alien-labs-finds-new-golang-malwarebotenago-targeting-millions-of-routers-and-iot-devices-with-more-than-30-exploits
[2] blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/
[3] wirelesswatchdogs.com/blog/why-iotroop-/-reaper-remains-a-persistent-threat
[4] welivesecurity.com/2016/11/02/linuxmoose-still-breathing/
[5] microsoft.com/en-us/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/
[6] cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux
[7] trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/-silex-malware-bricks-IoT-devices-with-weak-passwords
[8] trendmicro.com/en_in/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html

## Major vulnerabilities exploited in IoT attacks

Among the binaries (executable files) classified as malicious, we observed that 31% of them contained at least one exploit. In total, 39 different vulnerabilities are being exploited by different payloads.

Command injection was the most commonly leveraged Common Weakness Enumeration (CWE) category, accounting for nearly 75% of the vulnerabilities. Command injections involve injecting executable commands in a crafted HTTP request, often used to download and execute a stager script or the malicious binaries themselves.

Only 5 out of 39 exploits discovered during our research had been disclosed in the last three years, highlighting the prevalence of — and risk from — legacy vulnerabilities. The oldest vulnerability observed dates back to 2013.

Approximately 62% of the vulnerabilities discovered were specific to routers.

The following is the list of all the exploited vulnerabilities, along with their CWE.

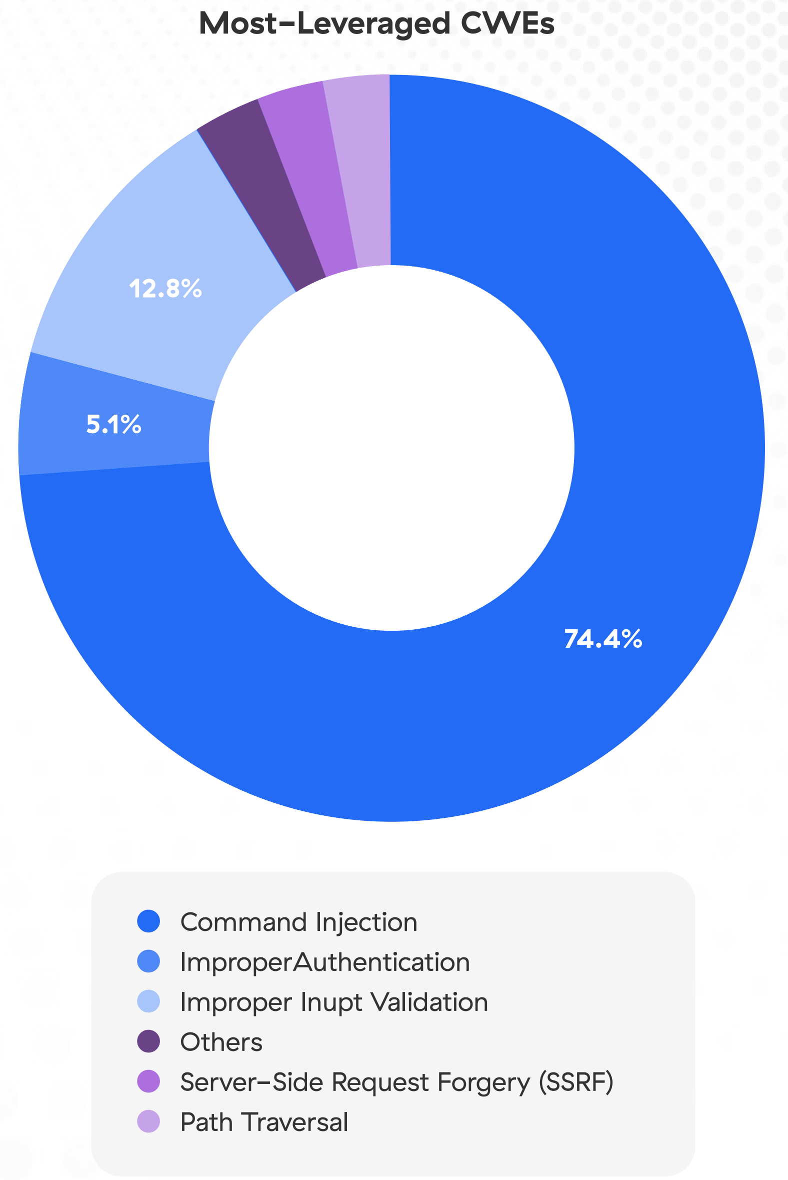


*Figure 11: Distribution of Common Weakness Entries (CWEs) by exploited vulnerability*

| CVE | Vulnerability Name | CWE |
|---|---|---|
| CVE-2021-20090 | Arcadyan Buffalo Firmware Path Traversal Vulnerability | Path Traversal |
| – | AVTECH Unauthenticated Command Injection | Command Injection |
| CVE-2021-38647 | Azure OMIGOD remote code execution vulnerability | Improper Authentication |
| – | CCTV/DVR “language/Swedish” Remote Command Execution | Command Injection |
| CVE-2018-20057 | D-Link “formSysCmd” Authenticated Remote Command Execution via ‘sysCmd’ parameter | Command Injection |
| CVE-2016-11021 | D-Link DCS-930L Devices OS Command Injection Vulnerability | Command Injection |
| CVE-2020-9377 | D-Link DIR-610 Devices Remote Command Execution | Command Injection |
| CVE-2016-20017 | D-Link DSL-2750B OS Command Injection | Command Injection |
| CVE-2013-7471 | D-Link UPnP “soap.cgi” Unauthenticated Remote Command Execution | Command Injection |
| CVE-2018-10561 | Dasan GPON Routers “GponForm/diag_Form” Authentication Bypass and Command Injection vulnerabilities via ‘dest_host’ parameter | Improper Authentication |
| – | Eir WAN Side Remote Command Injection | Command Injection |
| – | EnGenius EnShare IoT Gigabit Cloud Service 1.4.11 – Remote Code Execution | Command Injection |
| CVE-2015-2051 | HNAP SoapAction-Header Command Execution D-Link -Command Injection | Command Injection |
| CVE-2017-17215 | Huawei HG532 “DeviceUpgrade_1” Authenticated Remote Command Execution | Improper Input Validation |
| CVE-2016-20016 | JAWS Webserver unauthenticated shell command execution MV POWER DVR | Command Injection |
| – | Linksys “tmUnblock.cgi” Unauthenticated Remote Command Execution | Command Injection |
| CVE-2013-3307 | Linksys X3000 1.0.03 build 001 – Multiple Vulnerabilities | Command Injection |
| CVE-2021-33544 | Multiple camera devices by UDP Technology, Geutebrück and other vendors | Command Injection |
| – | NetGain ping Command Injection | Command Injection |
| CVE-2016-6277 | Netgear cgi-bin Command Injection | Command Injection |
| CVE-2017-6334 | Netgear DGN2200 Devices OS Command Injection Vulnerability | Command Injection |
| CVE-2017-6077 | Netgear DGN2200 Remote Code Execution Vulnerability” with the CWE as “Command Injection” | Others |
| – | Netgear setup.cgi unauthenticated RCE | Command Injection |
| – | NUUOS OS Command Injection | Command Injection |
| CVE-2021-35395 | Realtek Jungle SDK Unauthenticated Command Injection vulnerabilities in “formSysCmd” and “formWsc” pages | Others |
| CVE-2014-8361 | Realtek SDK – miniigd UPnP SOAP “wanipcn.xml”/”picsdesc.xml” Unauthenticated Command Execution | Improper Input Validation |
| CVE-2014-3206 | Seagate BlackArmor NAS “localJob.php” Unauthenticated Remote Command Execution | Improper Input Validation |
| CVE-2018-20062 | ThinkPHP “noneCms” Remote Code Execution Vulnerability | Improper Input Validation |
| – | VACRON NVR “board.cgi” Remote Command Execution via ‘cmd’ parameter | Command Injection |
| – | ZTE ZXV10 H108L manager_dev_ping_t.gch RCE | Command Injection |
| CVE-2017-18368 | Zyxel “ViewLog.asp” router Unauthenticated Remote Command Execution via ‘remote_host’ parameter | Command Injection |
| CVE-2017-6884 | Zyxel, EMG2926 < V1.00(AAQT.4)b8 – OS Command Injection | Command Injection |
| CVE-2018-10562 | Dasan GPON Routers Command Injection Vulnerability | Command Injection |
| SonicWall SSL-VPN 8.0.0.0 – ‘shellshock/visualdoor’ Remote Code Execution | SonicWall SSL-VPN software version 8.0.0.0 | Command Injection |
| CVE-2020-25506 | D-Link “system_mgr.cgi” Unauthenticated Remote Command Execution | Command Injection |
| CVE-2021-22986 | F5 BIG-IP and BIG-IQ Centralized Management iControl REST Remote Code Execution Vulnerability | Server-Side Request Forgery (SSRF) |
| – | UPnP SOAP TelnetD Command Execution D-Link | Improper Input Validation |
| CVE-2020-8515 | DrayTek Vigor2960 “mainfunction.cgi” Unauthenticated Remote Command Execution via ‘keyPath’ parameter | Command Injection |
| CVE-2020-10987 | Tenda “setUsbUnload” Unauthenticated Remote Command Execution via ‘deviceName’ parameter | Command Injection |

## Routers are the primary targets of attacks

**66.7% of all attacks target routers.**

Routers are appealing IoT malware targets due to their central position in networks, continuous internet connectivity, widespread use of default credentials, and susceptible to firmware vulnerabilities. This last factor — firmware vulnerabilities — is a commonplace concern, as evidenced by top router manufacturers Netgear and ASUS making headlines this year for highly critical security vulnerabilities[1,2].

Despite these warnings, critical router vulnerabilities remain largely unpatched[3], ripe for novel malware to exploit and launch DDoS attacks[4].

### Top Attacked Devices Based on Payload

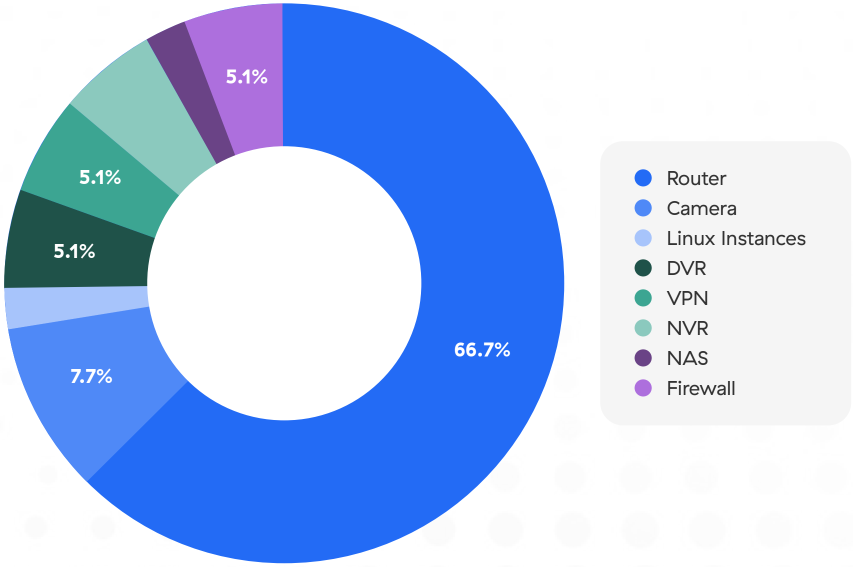


*Figure 12: Top attacked devices based on payloads*

1. bleepingcomputer.com/news/security/asus-urges-customers-to-patch-critical-router-vulnerabilities
2. thehackernews.com/2023/05/netgear-routers-flaws-expose-users-to.html
4. venturebeat.com/security/report-majority-of-critical-router-vulnerabilities-remain-unpatched/
5. zdnet.com/article/chaos-iot-malware-taps-go-language-to-harvest-windows-linux-for-ddos-attacks

## Manufacturing most impacted by malware

On an average week, the manufacturing sector receives more than triple the number of attacks as any other sector.

Manufacturing customers take the brunt of IoT malware attacks (54.5%). The food, beverage, and tobacco and education sectors come in far behind, experiencing 16.5% and 14.1% of attacks, respectively.

With a low tolerance for operational disruptions, manufacturing is high stakes for malware attacks. Attacks on manufacturing customers can have ripple effects that impact other sectors like:

- supply chain and logistics
- defense and national security
- finance
- retail
- technology
- construction and real estate

### Affected Customer Verticals

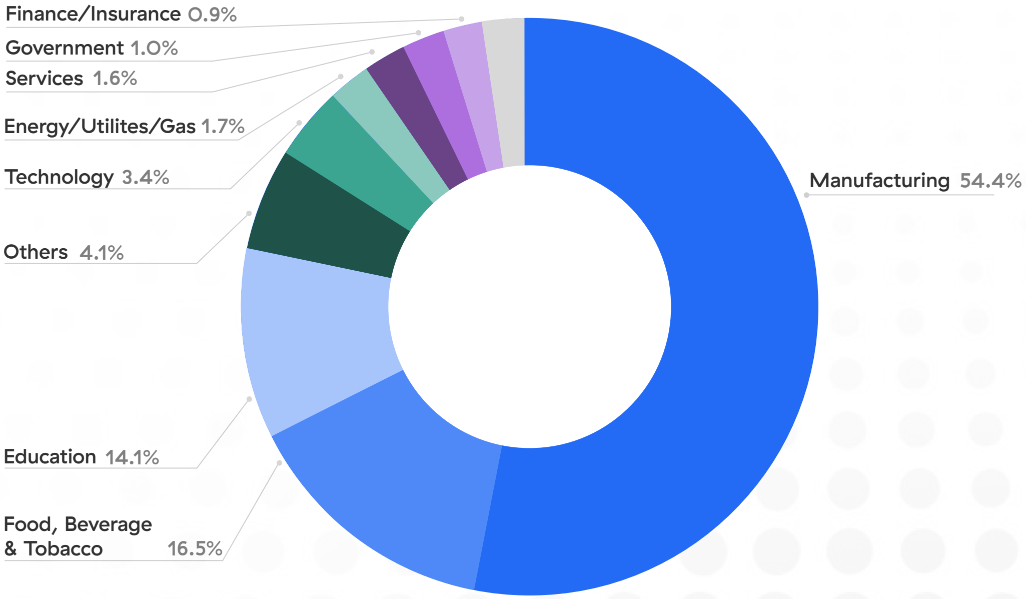


*Figure 13: Breakdown of verticals targeted by IoT malware attacks*

## Education has the sharpest increase in malware attacks

IoT malware attacks in education increased an astounding 961%. Educational institutions are considered 'soft targets' because of the wealth of personal data stored on their networks, leaving both students and educational institutions vulnerable. The transition to remote learning has considerably widened the attack surface for hackers. The proliferation of unsecured IoT devices within school networks has provided attackers with easier access points. Moreover, the limited investment in robust cybersecurity measures by schools further simplifies attacks.[1]

The following year-over-year comparison of IoT malware attacks showcases the industries with the greatest percentage changes.

| Vertical | 2022 | 2023 | % change |
|---|---:|---:|---|
| Education | 152 | 1613 | 961.1842105 |
| Arts, Media, Entertainment | 132 | 797 | 503.7878788 |
| Basic Materials, Chemicals, Mining | 14 | 83 | 492.8571429 |
| Technology | 2678 | 8403 | 213.7789395 |
| Finance, Insurance | 701 | 2180 | 210.9843081 |
| Services | 2033 | 3079 | 51.45105755 |
| Food, Beverage & Tobacco | 305 | 367 | 20.32786885 |

[1] blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/

## Mexico experiences the most IoT infections

With 46.1% of IoT malware infections, Mexico stands as the most infected country. Three of the top four most infected countries (Mexico, Brazil, and Colombia) are all Latin American nations. While adoption is generally slower than in regions like Asia and Europe, the number of IoT connections in Latin America is anticipated to reach 1.3 billion by 2025, compared to roughly 800 million today.[1]

### Top Infected Countries

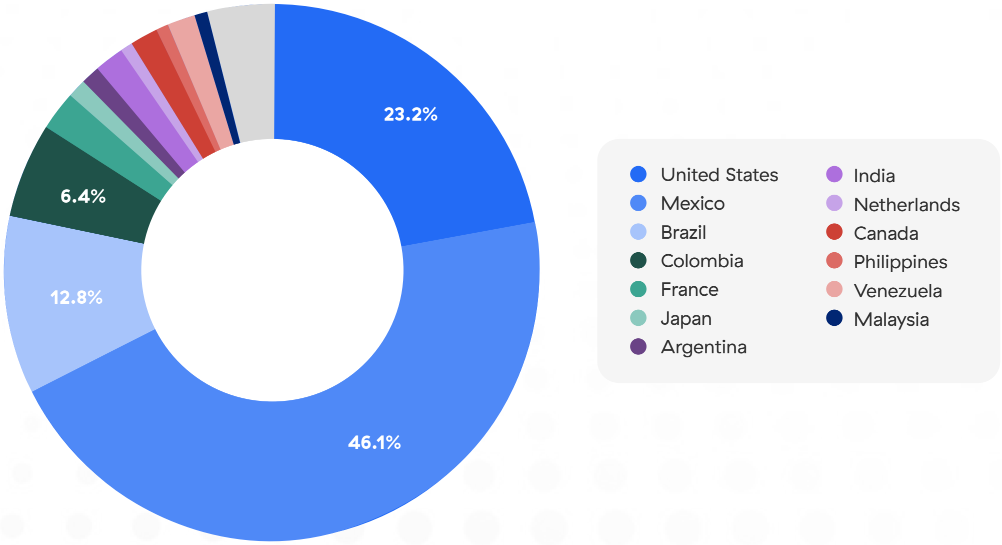


*Figure 14: Countries that experience the most IoT infections*

[1] gsma.com/latinamerica/wp-content/uploads/2018/11/IoTGuide-ENG.pdf

The United States is a heavy hitter when it comes to attracting and distributing malware, likely because of the country's robust digital infrastructure.

## The U.S. is top target for IoT malware

Findings show that the United States is a top target for IoT malware authors with 96% of all IoT malware distributed from compromised IoT devices in the United States.

### Top Malware Targets

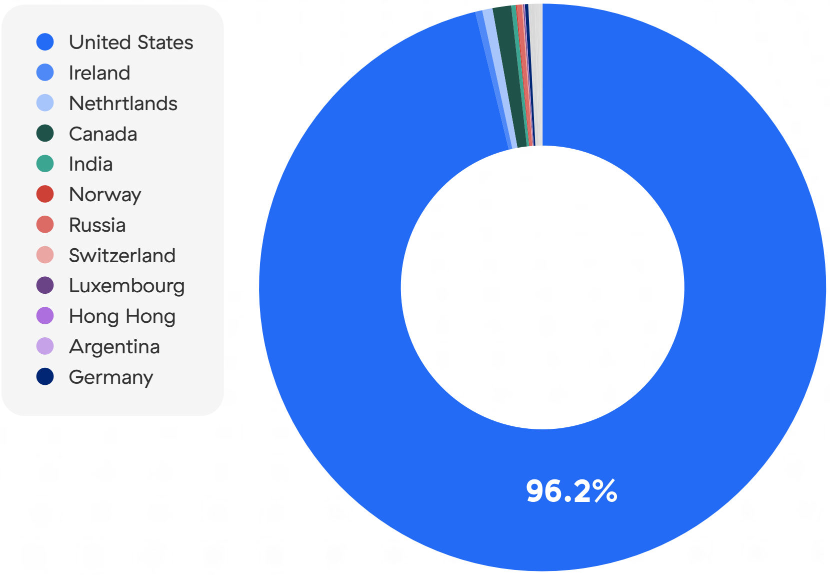


*Figure 15: Top IoT malware hosting countries*

# 2024 Predictions

**Vulnerable IoT devices will increase as a primary threat vector,** exposing enterprises to breaches and new security risks. The lack of standardized security measures by device IoT developers and manufacturers leads to vulnerabilities that attackers can easily exploit. Coupled with the widespread adoption and use of these devices, IoT is low-hanging fruit for easy yet significant financial gain for attackers. This will continue to lead to an uptick in IoT-related attacks in 2024 and beyond.

**Manufacturing will continue to be a prime target for IoT attacks.** Experiencing the lion's share of attacks (54.5%), manufacturing saw an average of 6,000 attacks per week. This heightened exploit activity is closely tied to its Industry 4.0 transformation, marked by rapid IoT adoption to drive day-to-day efficiencies. This growth is apparent in the research: data collection terminals — such as wireless barcode scanners used in logistics, warehousing, and — alone account for 62.1% of all IoT traffic. Given this expanded attack surface, manufacturing organizations must work to gain comprehensive visibility into the IoT devices (and vulnerabilities) active in their environments and prevent unrestricted access to the corporate network. In addition, operational technology (OT) systems must adapt to accommodate this influx of data and connectivity — which has dissolved the traditional OT "air gap" of many organizations — while simultaneously facing heightened security challenges to protect critical industrial processes.

**IoT and IoMT devices commonly used in healthcare environments will increasingly pose risks for the public.** Many Internet of Medical Things (IoMT) devices and the information they handle can impact people's health, personal safety, and security. The healthcare industry processes some of the highest data volumes and protects some of the most sensitive user data including PII, health records, and payment processing information. Furthermore, healthcare is rife with legacy devices that run outdated software, decades-old protocols, and unsupported operating systems, all of which serve as an open door for attacks.

**AI capabilities will also empower threat actors, helping to identify targets and vulnerabilities in connected devices.** While enterprises will increasingly leverage AI-powered technology for proactive threat mitigation, on the flip side, threat actors will use AI-based tools to automate attacks and evade traditional security measures, leading to more targeted IoT attacks.

**5G will exponentially grow the number of potential IoT and OT targets for threat actors to compromise.** As 5G adoption grows, so will IoT and operational technology (OT) attack surfaces. Higher data speeds and lower latency will continue to drive the proliferation of connected devices.

**Expect industry standards around user security and privacy concerns to impact IoT device manufacturers' security development practices** as IoT threats continue to escalate in the years to come. Additionally, more regulatory checks and mandates will be introduced to standardize IoT security measures, holding manufacturers accountable for the security of their products. Will these policy changes occur soon enough? It is important that organizations take steps to protect themselves until regulatory agencies and device manufacturers can catch up with the evolving threat landscape.

# IoT Security Best Practices

With the surge in IoT device adoption, implementing proactive IoT cybersecurity measures is crucial for organizations. For many, this requires modernizing their security strategy.

Traditional security approaches were designed for a different era. Legacy strategies and tools can't adapt to the intricacies and array of IoT devices, leaving attack surfaces exposed and vulnerabilities wide open. Many legacy systems cannot effectively monitor and manage connected devices, leading to blind spots that threat actors can exploit. Moreover, inspecting encrypted IoT traffic with traditional network-based security tools is too resource-intensive, becomes untenable, and in some cases may be impossible due to the inability to push certificates to these devices.

How can you overcome these challenges and get ahead of today's IoT threats? Embrace a multi-layered security approach to ensure a resilient IoT ecosystem. Operate with a "trust no one and no device, inspect and verify every connection" mindset. Aim to identify vulnerabilities before they become a problem. Be prepared to disrupt attacks at any stage if threat actors exploit connected devices.

These guiding principles, along with the following best practices compiled by our experts, can help protect your organization from future IoT attacks and build a culture of resilience to evolving threats.

## 1 Maintain comprehensive visibility into IoT devices.

Securing IoT devices begins with knowing what devices are connected to your network and what those devices are doing. Gain visibility into all IoT devices, including unmanaged devices, by utilizing solutions that analyze network logs to monitor communications and activity. Continuous visibility and awareness of what is connected to the network at all times is critical, no matter where devices are located.

## 2 Protect admin credentials and enable MFA.

Multi-factor authentication (MFA) requires users to enter a secondary mode of verification in addition to their password. This extra layer of security can thwart attackers from gaining access to user accounts if they have obtained credentials, preventing lateral threat movement from compromised user devices.

## 3 Stay on top of patching.

Unpatched devices are more vulnerable to attacks. Keep authorized IoT devices secure by enabling automatic updates and patching them quickly to address any new vulnerabilities that arise. When patching isn't possible, a zero trust architecture significantly reduces the risk posed by unpatched devices.

## 4 Enforce an IoT security framework.

Ensure IoT devices do not have unrestricted access to the network and are limited to the sites and servers they need. This can be achieved using a zero trust architecture. Ensuring all users follow the same security procedures will also go a long way in preventing initial compromise.

## 5 Train employees on IoT device security.

Educate employees about the risks of connecting unauthorized devices to the network. Encourage them to report any new devices they connect and conduct security awareness training to help employees identify and avoid attacks on user devices.

## 6 Inspect encrypted traffic.

Attacks commonly use encrypted channels, which often are not inspected, making it easy for even moderately sophisticated attackers to bypass security controls. Organizations must inspect all encrypted traffic to prevent attackers from compromising systems.

## 7 Implement a zero trust security architecture.

Eliminate implicit trust. Enforce segmentation with least–privileged access to ensure users and devices can access only what they need. Any unsanctioned shadow IoT devices that need internet access should go through traffic inspection and, ideally, be blocked from corporate data via a proxy.

## 8 Follow Zscaler ThreatLabz research feeds.

Get regular insights on the latest cyberthreats and developments, including published indicators of compromise (IOCs) and MITRE ATT&CK mappings. This information can be used to train your team, improve your security posture, and help prevent IoT attacks.

**Follow ThreatLabz on X @ThreatLabz and our security research blog.**

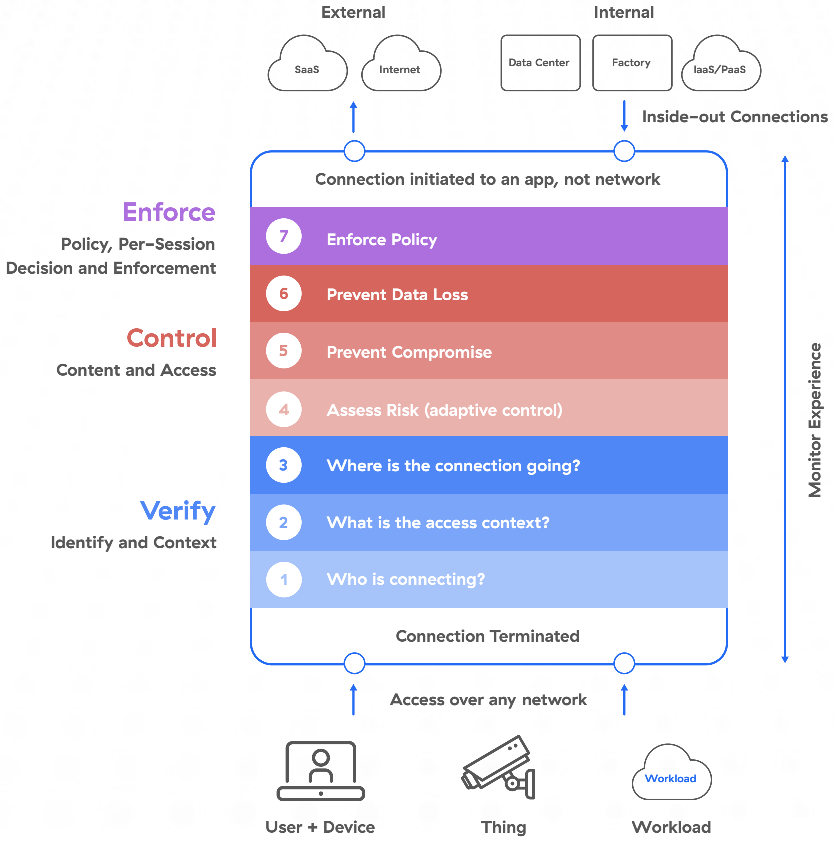
# How Zscaler Protects Against IoT Attacks

The ever-growing Internet of Things and uptick in IoT malware is a clear sign of things to come. Extending zero trust security to IoT devices is a business imperative. The reality is that a majority of IoT devices lack security controls and do not need access to sensitive corporate data or applications. The best approach is to assume that no devices can be trusted and to restrict unfettered access to the network.

The Zscaler Zero Trust Exchange™ is grounded on this exact premise — no device, user, or workload is inherently trustworthy. The holistic zero trust platform verifies identity and context, applies controls, and enforces policy before brokering a secure connection between a device and an application over any network.

With the Zero Trust Exchange, organizations gain powerful defenses against IoT attacks.

**Eliminate blind spots:** Get complete visibility of all IoT devices, servers, and unmanaged user devices across your business. AI/ML capabilities automatically classify and identify device types based on activity and behavior, without the need to install or manage sensors. Always-on monitoring provides real-time insight into your IoT device landscape.



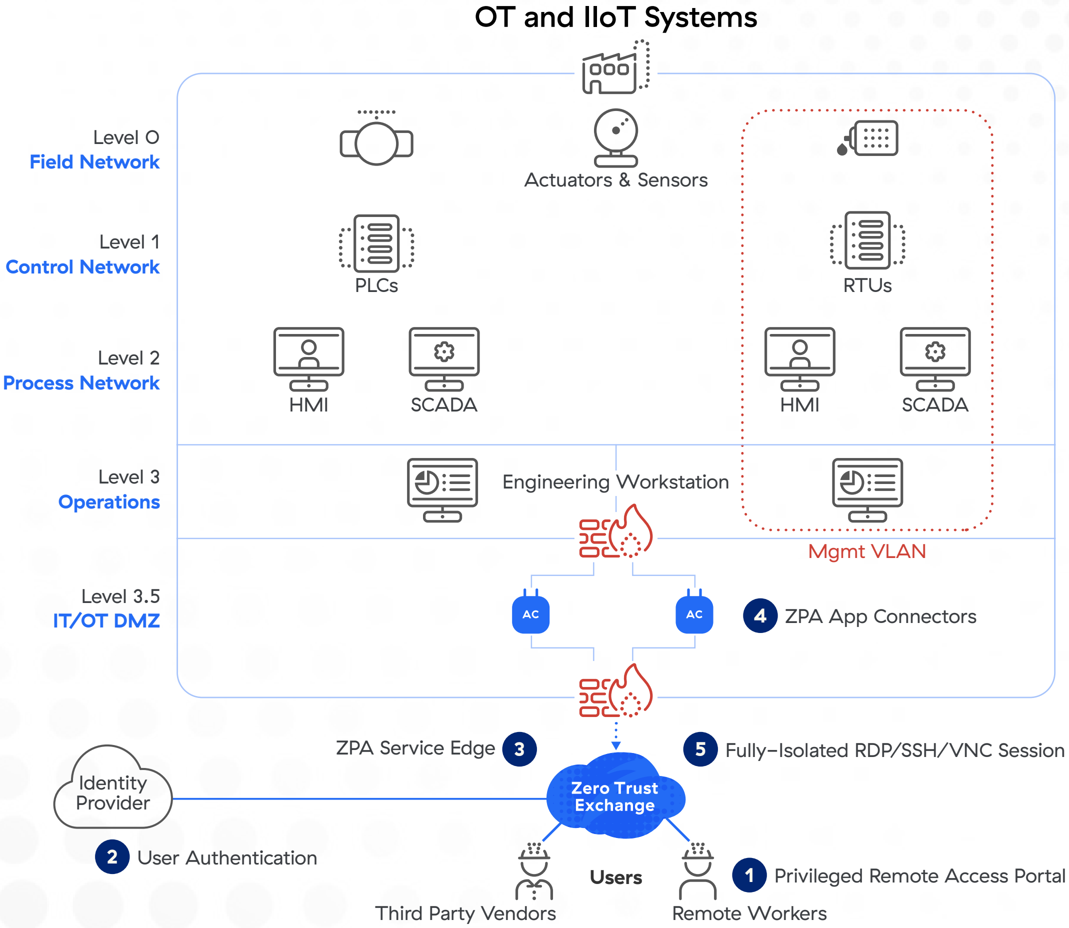
**Prevent compromise:** Ensure safe internet access for cloud-based controllers and software updates and block communication with known malicious command-and-control sites. Eliminate exposed ports for remote management by establishing inside-out connections to the Zero Trust Exchange, which allows admins and vendors to securely access IoT/OT devices over a browser session.

**Protect corporate data:** Prevent accidental or malicious lateral movement of threats from infected IoT devices. The Zscaler Zero Trust Exchange segments user and application traffic, protecting critical applications from lateral intrusion from unknown, untrusted IoT devices.

# OT Security Best Practices with Zscaler

Historically, OT environments have been "air gapped" or physically isolated from the outside world. As they become more digitized and connected to the internet, particularly with the need for remote maintenance by third-party technicians, they become more susceptible to malware, ransomware, and supply chain attacks. These risks can lead to operational disruptions and put workers at risk. It is no longer sufficient to protect OT assets from compromise with traditional perimeter security measures such as firewalls and VPNs, which expand the OT attack surface and are only as secure as their latest patch.

- Implement a zero trust security architecture. Zero trust is key to preventing unplanned downtime and ensuring maximum productivity in industrial systems. Zero trust can minimize your attack surface, eliminate lateral movement, and accelerate OT/IoT convergence.
- Leverage Zscaler Privileged Remote Access. This cloud-based solution provides remote workers and third-party vendors with clientless remote desktop access to sensitive RDP, SSH, and VNC production systems without having to install a client on unmanaged devices or log into jump hosts and VPNs. Securely store device and system passwords in the Privileged Credentials Vault.
- Leverage Zscaler Internet Access™ to detect botnet and command-and-control activity and Zscaler Advanced Cloud Sandbox to prevent entry of malware in file/firmware updates.



# Related Zscaler Platform Capabilities

**Zscaler IoT Device Visibility** provides a holistic view of all IoT devices, servers, and unmanaged user devices across your organization.

**Zscaler Private Access™** safeguards applications by limiting lateral movement with least-privileged access, user-to-app segmentation, and full inline inspection of private app traffic.

**Zscaler Privilege Remote Access** enables fast, direct, and secure access tooperational technology (OT) and industrial Internet of Things (IIoT) assets.

**Zero Trust Branch Connectivity** securely connects devices and users to applications without the complexity of overlay networks.

**Zscaler Internet Access™** helps identify and stop malicious activity by routing and inspecting all internet traffic through the Zscaler Zero Trust Exchange™.

**Advanced Threat Protection** blocks all known command-and-control (C2) domains.

**Advanced Firewall** extends C2 protection to all ports and protocols, including emerging C2 destinations.

**Browser Isolation** creates a safe gap between users and malicious web categories, rendering content as a stream of picture-perfect images to eliminate data leakage and the delivery of active threats.

**Zscaler Sandbox** prevents unknown malware delivered in second stage payloads.

**Zscaler Deception™** detects and contains attackers attempting to move laterally or escalate privileges by luring them with decoy servers, applications, directories, and user accounts.

# Appendix

## Methodology

The research methodology for this report includes analysis of device logs from a multitude of sources and industry verticals.

The report uses data derived from customer deployments that connect to the Zscaler global security cloud, which processes over 9 billion threats and policy violations per day, with over 250,000 daily security updates.

The team focused their research on understanding the distinct attributes and activity of IoT devices via device fingerprinting (DFP) and analyzing the IoT malware threat landscape.

Device fingerprinting data from March—May 2023 included:

- A complete inventory of devices, including device types and manufacturers
- The volume and source of IoT device transactions
- The industries and geographies contributing to IoT traffic

IoT malware threat data from January—June 2023 included:

- The most active malware families
- The industries and geographies most targeted by IoT attacks
- The top attacked devices based on payloads

## The history of shadow IoT devices

Shadow IoT devices, a persistent cybersecurity concern, have their roots in the rapid proliferation of Internet of Things (IoT) technology during the early 21st century. Their history can be traced to the convergence of multiple factors:

- Increasing ubiquity of and affordability of IoT devices
- Bring Your Own Device (BYOD) trend
- Lack of stringent device management protocols within organizations

As IoT devices become more accessible, employees and individuals began introducing these devices into corporate and network environments without the explicit approval or oversight of IT departments. These unauthorized devices, typically unmanaged and unpatched, act as potential security loopholes, creating entry points for malicious actors and network vulnerabilities.

The issue of shadow IoT devices gained significant traction in the mid-2010s when organizations recognized the extent of the threat. The absence of visibility and control over these devices led to a series of cybersecurity incidents, ranging from data breaches to network disruptions. In response, the cybersecurity community developed advanced solutions to detect and manage shadow IoT devices, including network access control (NAC) systems and robust endpoint security solutions.

Furthermore, awareness campaigns and comprehensive employee training initiatives were initiated to educate individuals about the intricate security risks associated with the unauthorized connection of IoT devices to corporate networks. The relentless evolution of IoT technology, coupled with the ever-expanding threat landscape, continues to challenge organizations, rendering mitigation of shadow IoT device risks a pivotal component of a contemporary cybersecurity strategy.

## The four stages of a shadow IoT attack

In the following scenario, we will walk through how an attacker might gain unauthorized access and control through a personal smart printer brought into a corporate office without notifying the IT department.

### Stage 1

An employee introduces a personal smart printer into the corporate office environment without notifying the IT department, rendering it a shadow IoT device. An attacker identifies this device within the corporate network. They may use network scanning tools or known vulnerabilities to discover it.

### Stage 2

Once the printer is identified, the attacker recognizes the opportunity to infiltrate the corporate network and attempts to take control of the device. They may use default factory-set credentials or exploit vulnerabilities in the smart printer's firmware or unpatched software.

### Stage 3

After successfully compromising the smart printer, they establish a foothold within the corporate network. Subsequently, the attacker scans the network for other vulnerable devices or security weaknesses. Identifying an underprotected file server, they employ the compromised printer to launch attacks, potentially planting malware or unauthorized access tools on the server, using the printer as a pivot point to move laterally and access sensitive data.

### Stage 4

The primary objective of the attacker is data theft. Through the compromised file server, they exfiltrate sensitive documents containing confidential information, financial data, or personally identifiable information (PII) related to employees or clients. Additionally, the attacker may choose to maintain persistence by using the compromised smart printer as an ongoing entry point into the network, facilitating continuous monitoring of network traffic and enabling future unauthorized access.

In this scenario, the shadow IoT device, a smart printer, becomes a vector for the attacker to gain access to the corporate network, exploit connected devices, and steal sensitive information.

## The history of OT devices

The beginnings of operational technology (OT) devices can be traced back to the early 20th century when industries sought more efficient ways to manage their processes. During this era, simple mechanical controls, such as levers and gears, were employed to automate specific tasks. These early innovations laid the foundation for what would later become the world of OT.

The 1950s and 1960s marked a pivotal era for OT with the advent of the Supervisory Control and Data Acquisition (SCADA) systems. These systems introduced the concept of remotely monitoring and controlling industrial processes. SCADA systems played a vital role in industries like manufacturing, utilities, and transportation, enabling greater efficiency and safety.

As digital technology advanced, the 1980s and 1990s witnessed the widespread adoption of Programmable Logic Controllers (PLCs). PLCs monitor automated or human input in industrial processes and make output adjustments accordingly. They became the cornerstone of control systems, offering reliability, and efficiency in managing processes.

The late 20th century saw the integration of more advanced computing capabilities into OT devices. These digital advancements allowed for better control and monitoring, but they also brought new challenges. With the increased connectivity of OT devices to networks, the issue of cybersecurity became a critical concern as the digital world began to intersect with the industrial one.

The 21st century has been marked by the convergence of Information Technology (IT) and OT. This complex landscape will continue to grow in efficiency (and complexity) as IoT and advanced analytics processes are integrated.

## The differences between IoT and OT

The Internet of Things (IoT) and Operational Technology (OT) have emerged as two integral pillars that drive the digital transformation of industries. While IoT and OT share the common goal of enhancing operational efficiency, they differ significantly in their scope, function, and technical requirements.

**Core differences**

IoT is primarily concerned with connecting a vast array of everyday objects, devices, and sensors to the internet. It is about gathering data from various sources for analysis and decision-making, often associated with consumer and business applications. OT, on the other hand, focuses on managing and controlling critical industrial processes and infrastructure. It encompasses supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and other technologies for essential managing physical processes. When it comes to function, IoT devices are more inclined towards data collection, transmission, and the remote control of various devices. They are often found in smart homes, wearable devices, and smart cities. OT systems are mission-critical and are designed to monitor, control, and automate industrial processes. They are commonly used in manufacturing, energy production, and utilities.

**Technical details**

Security requirements differ significantly between IoT and OT. IoT devices often rely on lightweight security protocols due to limited resources, while OT systems require robust security measures to safeguard against critical infrastructure threats. IoT devices may use standard internet protocols like HTTP, MQTT, or CoAP for communication. OT systems, on the other hand, often use specialized industrial protocols like ModBus, DNP3, and Profibus.

**Bridging the gap**

The convergence of IoT and OT is an exciting development. However, it also introduces a set of unique challenges. As IoT devices are increasingly integrated into industrial environments, the lines between these two domains blur.

## Additional resources

### IoT in the Enterprise: Empty Office Edition

by the Zscaler ThreatLabz team

This report highlights the security risks posed by IoT devices in abandoned corporate offices during the COVID-19 pandemic. Despite employees working from home, IoT malware on corporate networks increased by 700% year-over-year. Our analysis found that entertainment and home automation devices were the riskiest, with most IoT communications occurring on unencrypted channels. The Gafgyt and Mirai malware families were prevalent in IoT attacks, with the technology, manufacturing, retail, and healthcare industries as the primary targets. Most attacks originated in China, the United States, and India.

### Shining a Light on Shadow IoT to Protect Your Organization

by Deepen Desai

This article discusses the rise of shadow IoT devices in organizations and the security challenges they pose. It emphasizes the importance of gaining visibility into these devices, implementing a zero trust approach, and advocating for global policies to enhance IoT security.

# About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

# About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.

Learn more at zscaler.com or follow us on Twitter @zscaler.

zscaler™ | Experience your world, secured.™

**About Zscaler**

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com.