2021 REPORT

IoT in the Enterprise: Empty Office Edition

What happens when employees abandon their smart devices at work?

zscaler™

Throughout 2020 and well into 2021, the COVID-19 pandemic left many corporate offices eerily quiet and devoid of employees. But despite the lack of people, these buildings were still buzzing with activity under the surface. The buildings themselves weren't the only things left abandoned: smart watches, digital signage, networked printers, and many other IoT devices were still connected to the network—refreshing data, performing functions, awaiting commands.

Threat actors took notice, and many attempted to take advantage. In the midst of the enormous global shift to work-from-anywhere. That translates to a staggering 833 IoT malware blocked every hour.

The ever-growing breadth of IoT devices that makes its way onto corporate networks includes everything from smart watches and IP cameras to automobiles and musical furniture. Seventy-six percent of the transactions occur on unencrypted plain text channels, though all devices use SSL for at least a subset of their communications. Organizations must employ zero trust policies and architectures to protect their networks from being exploited via these devices. This report from the Zscaler ThreatLabz threat research team is an eye-opening deep dive into both sanctioned and unsanctioned IoT devices and IoT malware trends based on two weeks of data from the Zscaler cloud.

We'll walk through the data from two studies: an IoT device fingerprinting study that identifies IoT devices and traffic, and an IoT malware study based on data from the Zscaler cloud. Because IoT devices—especially unsanctioned devices—do not have agents, all of the data in this report represents devices and attacks on corporate networks in physical office locations. This data for this report was collected between December 15 and December 31, 2020, when most non-essential business office locations were shut down.

700% increase in IoT-specific malware year over year.

Key findings

→ IoT malware on corporate networks has increased by 700 percent since our 2019 study, despite much of the global workforce working from home

→ Entertainment and home automation devices posed the most risk due to their variety, low percentage of encrypted communication, and connections to suspicious destinations

→ Gafgyt and Mirai—malware families popularly used in botnets—accounted for 97 percent of the IoT malware payloads blocked by the Zscaler cloud

→ Technology, manufacturing, retail & wholesale, and healthcare industries accounted for 98 percent of IoT attack victims

→ Most attacks originated in China, the United States, and India

→ Most targets for IoT attacks were in Ireland, the United States, and China

IoT Device Fingerprinting

Most common devices

Looking at over a half a billion IoT device transactions, ThreatLabz identified 553 different device types from 212 manufacturers and sorted them into 21 categories. The three most common categories—accounting for almost 65 percent of total devices—were set-top boxes (29 percent), smart TVs (20 percent), and smart watches (15 percent).

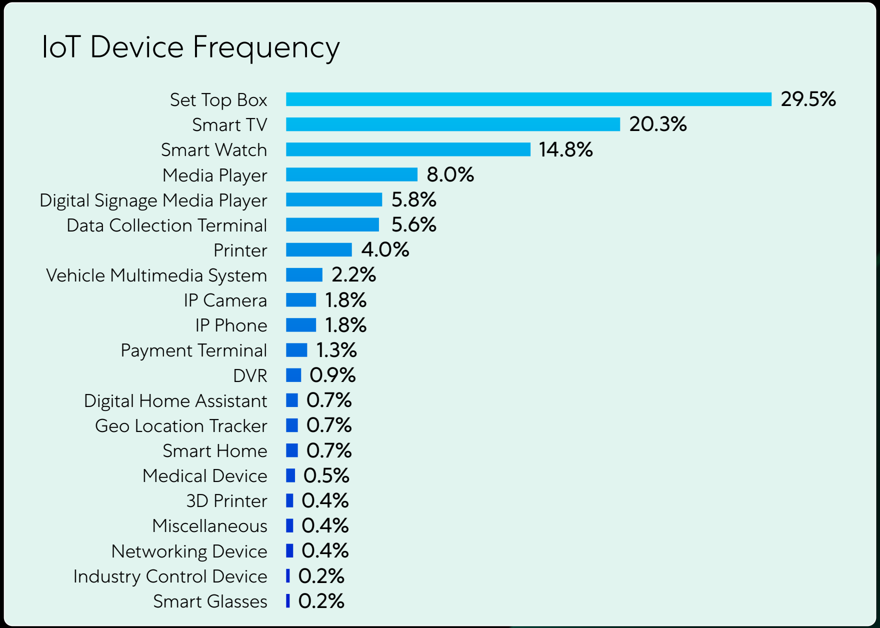
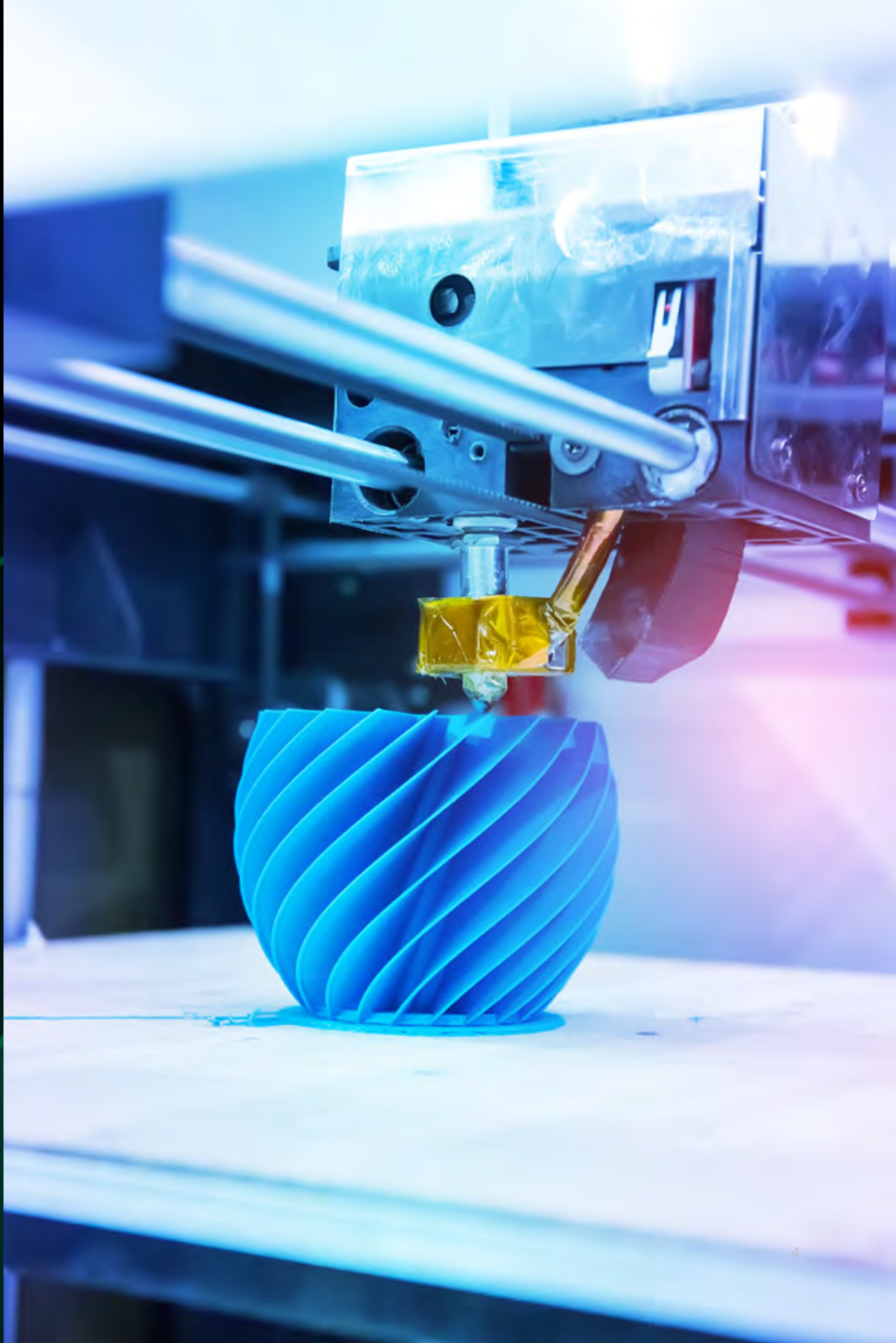


Figure 1: IoT device frequency



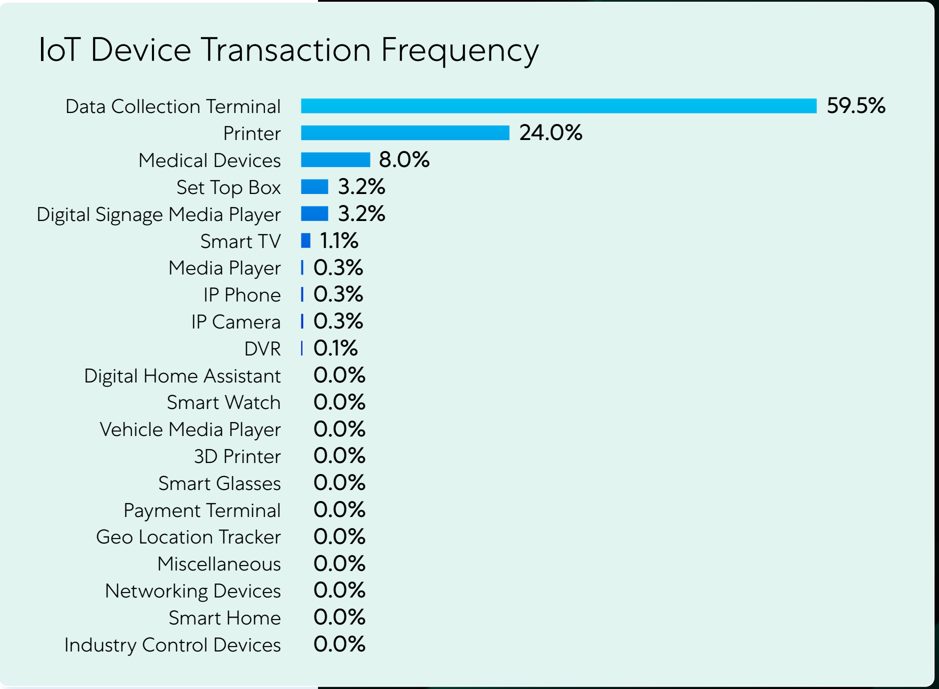
Internet of musical furniture?

The “Internet of Things” continues to expand to new categories, some of which may be completely off the radar of IT teams. ThreatLabz discovered a number of unexpected devices connecting to the cloud, including:

- **Smart refrigerators:** A smart refrigerator from Samsung has the ability to stream music, videos, and content from the owner’s phone to a screen on the refrigerator door.
- **Musical lamp:** Ikea and Sonos have created a combination table lamp and smart media player device named Symfonisk.
- **Automobiles:** Tesla and Honda automobile media players each were seen connecting to corporate networks.
- **Wi-Fi memory cards:** Wi-Fi memory cards from Eye Fi, generally used in cameras for storing and sharing photos, were sending traffic through the Zscaler cloud.

Chattiest devices

IoT device transactions accounted for 0.038 percent of the total transactions on the Zscaler cloud during the two-week period. Some devices accounted for many more transactions than others, with data collection terminals and printers accounting for over 80 percent of the total IoT traffic by themselves, as shown in Figure 2.



Base: 575,091,158 IoT device transactions
Figure 2: IoT device transactions

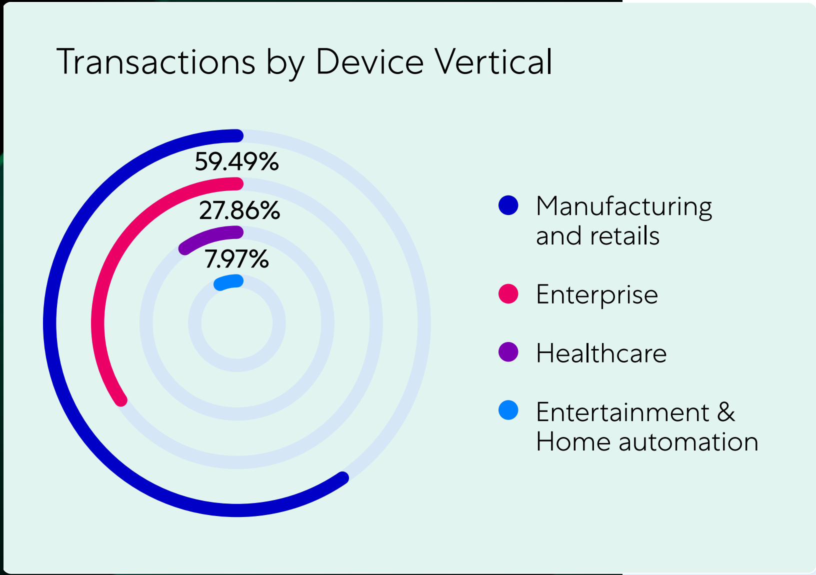


Figure 3: IoT devices by type

Traffic by device – vertical classification

IoT devices were further grouped into four categories based on the industries that produced them:

- **Manufacturing/retail devices** accounted for 59 percent of transactions and included 57 different device types from 20 manufacturers, and included 3D printers, geolocation trackers, industrial control devices, automotive multimedia systems, data collection terminals, and payment terminals.
- **Enterprise devices** accounted for 28 percent of transactions and comprised digital signage media players, digital video recorders, IP cameras and phones, printers, and networking devices.
- **Healthcare devices** accounted for eight percent of transactions and included a number of medical devices that come primarily from three manufacturers: GE Healthcare, Abbott Laboratories, and HOLOGIC.
- **Entertainment & home automation devices** accounted for five percent 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. While these accounted for the lowest percentage of transactions, they had the most variety and included a number of consumer devices—a total of 420 devices from 150 different manufacturers.

IoT devices communicate in plain text most of the time

ThreatLabz observed that 76 percent of total transactions from IoT devices occurred over plain-text channels, with only 24 percent of transactions occurring over secure encrypted channels. While this ratio seems unacceptably low, it is almost a 3x improvement from our 2019 study, in which only 8.5 percent of IoT communications were encrypted. Nonetheless, the security risk persists: plaintext communications are much easier for attackers to spy on or, worse, to intercept and modify, allowing them to exploit the IoT devices for malicious purposes.

All 553 devices observed in the study used SSL in some capacity, but the percentage of communications that were actually encrypted varied widely by device type. Enterprise and home entertainment devices communicated almost entirely in plain text, whereas healthcare devices communicated via SSL roughly half the time.

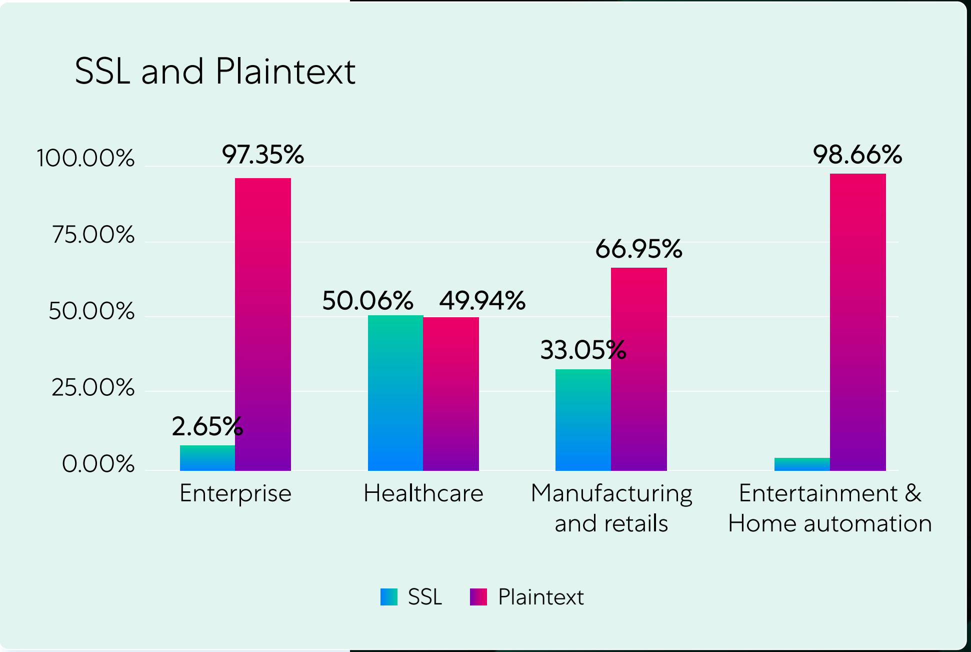


Figure 4: Percentage of encrypted communications by device type

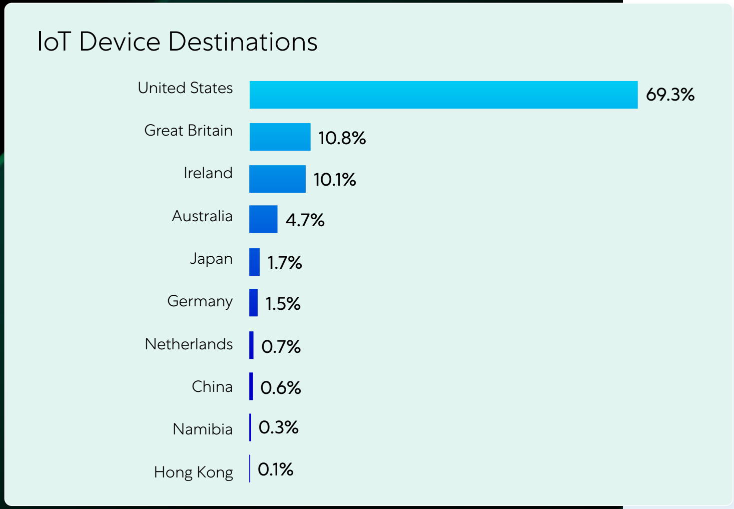


Figure 5: Top IoT communication destinations

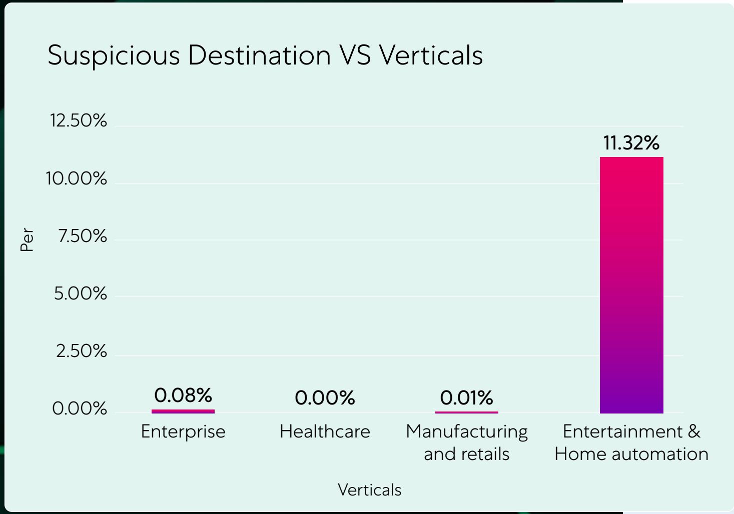


Figure 6: Percentage of suspicious traffic by device type

What countries are IoT devices talking to?

ThreatLabz 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 69 percent of traffic, followed by Great Britain (11 percent) and Ireland (10 percent). The top ten destination countries are displayed below.

Entertainment and home automation devices are much more likely to route to China and Russia

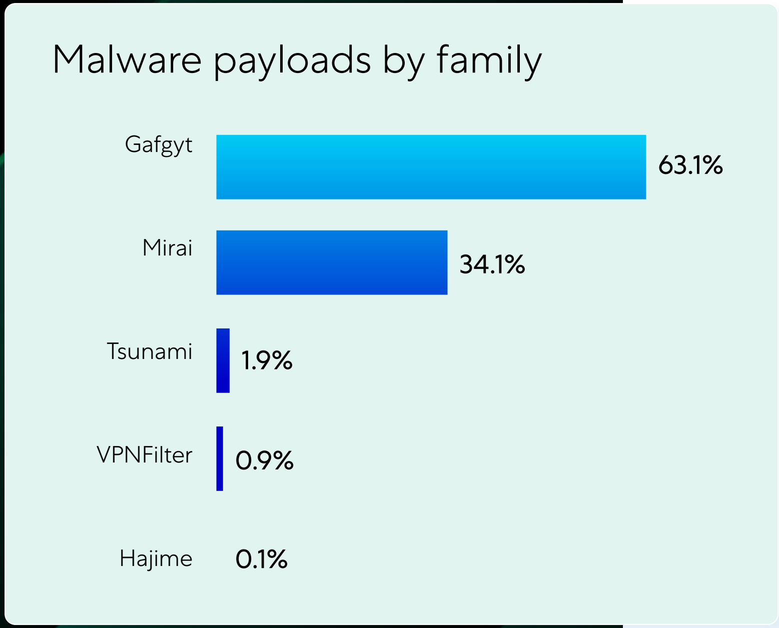
Eleven percent of traffic from entertainment and home automation devices was headed to China and Russia. While much of this is legitimate, non-malicious traffic, these are destinations that ThreatLabz considers to be suspicious due to their potential for government spying and other data vulnerabilities. Almost all (99.9 percent) of this suspicious traffic came from smart TVs and set-top boxes.

Conversely, devices designed for enterprise, healthcare, and manufacturing and retail use cases collectively had less than .1 percent of their traffic going back and forth to suspicious destinations.

IoT malware study

During the same two-week time period as our IoT fingerprinting study, ThreatLabz also took a look at activities specific to IoT malware in the Zscaler cloud.

ThreatLabz observed approximately 300,000 blocked transactions related to IoT malware, exploits, and command-and-control communications, which represents nearly a 700 percent increase from the previous year. In malware transaction volume, we observed a total of 18,000 unique hosts and roughly 900 unique payload deliveries in a 15-day timeframe.



Base: 900 payloads
Figure 7: Unique malware payloads by family

Top IoT threats

Malware families Gafgyt and Mirai were by far the top two most prolific IoT malware families in our study. In fact, 97 percent of the 900 unique payload deliveries that we observed belonged to these two families. Other active families included Tsunami, VPNFilter, and Hajime.

While Gafgyt had the most unique payloads, Mirai malware payloads were utilized more frequently in IoT attacks during our study. Looking at transaction volumes, 76 percent of blocked attacks were from the Mirai malware family, 5 percent from Gafgyt, and 15 percent from others.

IoT Botnets
IoT device exploits can provide attackers with access both to the device and to connected networks, which enables all sorts of malicious activity. Mirai and Gafgyt are particularly known for using devices to create botnets—networks of devices under an attacker's control that allow for large-scale coordinated attacks. Botnets have been used for distributed denial-of-service (DDoS) attacks, financial breaches, cryptocurrency mining, and targeted intrusions, just to name a few. The Mirai botnet is known for waging what was the largest DDoS attack in history back in 2016, causing widespread internet outages. ThreatLabz evaluated attempted botnet callbacks as part of this malware study, and found that attackers were targeting not only IoT devices, but also a number of popular routers and other networking devices to carry out these attacks:

Top Botnet Callback Devices	
CCTVs and DVRs from over 70 vendors	MVPower DVRs
Multiple devices using the Realtek SDK with the miniigd daemon	Linksys Devices
Huawei HG532	Netgear R7000/R6400 devices
ZyXEL Router	DGN1000 Netgear routers
Dasan GPON routers	D-Link devices
Eir D1000 routers	Vacron NVR devices
D-Link devices	

Most targeted industries

Technology companies saw the highest rate of attack from IoT malware, comprising 40 percent of infections. The next-most targeted industries were manufacturing (28 percent) and retail & wholesale (24 percent).

Countries waging the most malware attacks

In our study, 88.5 percent of compromised IoT devices were found to be routing data back to servers in one of three countries: China (56 percent), the United States (19 percent), or India (14 percent). These are known as "malware destination" countries, and in each case they either delivered the malware directly or connected to it post-infection. Some attackers will set up command and control servers within the country that they're targeting, so the server location may not necessarily indicate the actual location of the attacker.

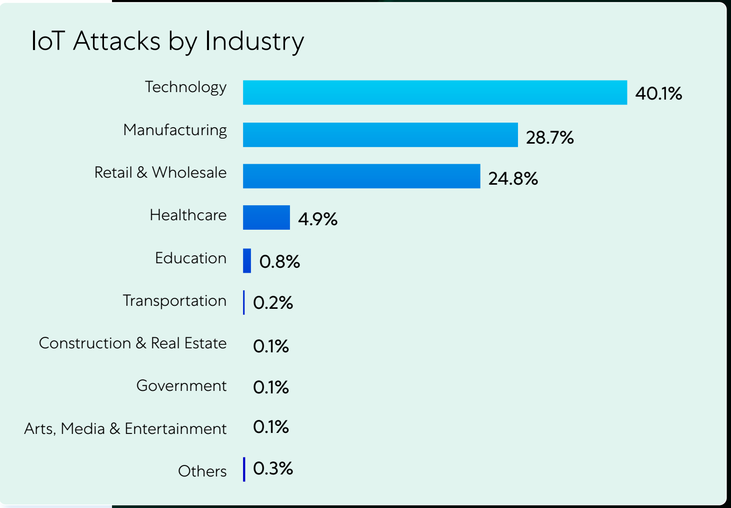


Figure 8: IoT attacks by industry

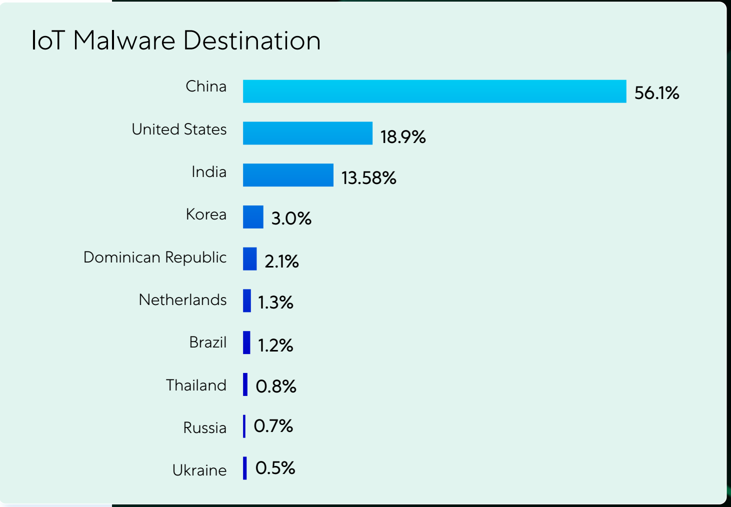


Figure 9: Top IoT malware destinations

Top ASNs of threat actors

Taking a more granular look into malware destinations, below are the top autonomous system numbers (ASNs) and IP addresses that ThreatLabz observed connecting to IoT malware:

ASN	IP	AS Name
16276	158.69.0.77	OVH, FR
398468	193.42.137.107	VMSNETWORKS, US
213035	193.239.147.144	SERVERION-AS Serverion B.V., NL
36352	107.173.125.167	AS-COLOCROSSING, US
202448	86.105.252.203	MVPS https://www.mvps.net, CY
46606	162.241.126.53	UNIFIEDLAYER-AS-1, US
53667	198.251.81.249	PONYNET, US
212953	46.102.106.25	MRS-BILISIM, TR
35913	45.15.143.175	DEDIPATH-LLC, US
213371	37.49.230.52	SQUITTER-NETWORKS, NL
35913	45.15.143.140	DEDIPATH-LLC, US
42864	45.95.169.218	GIGANET-HU GigaNet Internet Service Provider Co, HU
63916	103.42.214.181	IPTELECOM-AS-AP IPTELECOM Global, HK
134520	103.42.214.181	GIGSGIGSCLOUD-AS-AP GigsGigs Network Services, HK
3462	111.248.163.38	HINET Data Communication Business Group, TW
36352	107.173.181.189	AS-COLOCROSSING, US
36352	192.227.147.157	AS-COLOCROSSING, US
212369	45.155.125.116	TRDESERVER, TR
206898	185.172.110.205	BLADESERVERS, AU
213035	193.239.147.245	SERVERION-AS Serverion B.V., NL

Figure 10: Top ASNs of threat actors

Top IoT malware targets

ThreatLabz also evaluated "source countries"—the targets of malware—based on the client IP address. The top three nations victimized by IoT attacks were Ireland (48 percent), the United States (32 percent), and China (14 percent).

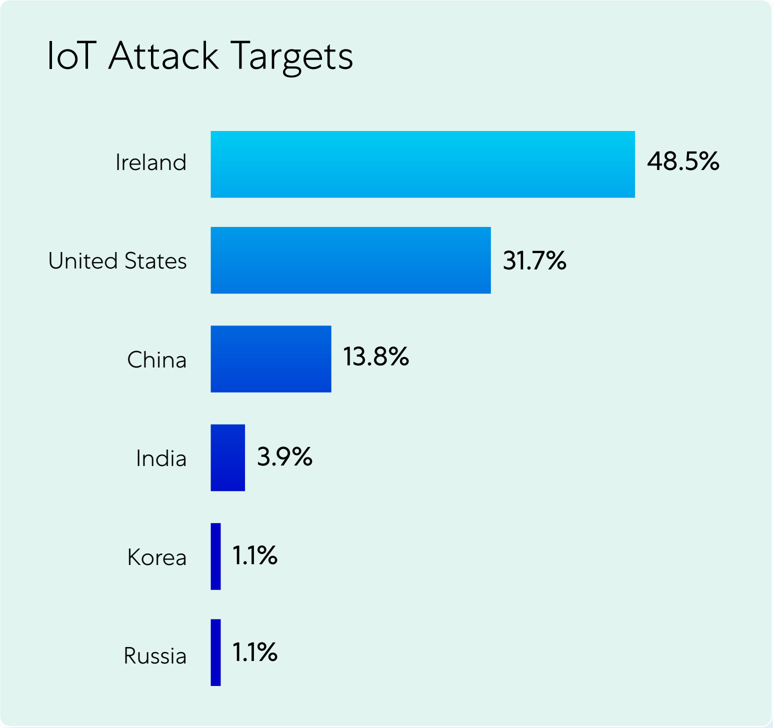


Figure 12: Top IoT malware source countries

Fundamentals for defending against IoT malware

As the list of "smart" devices out in the world grows on a daily basis, it's almost impossible to keep them from entering your organization, so it's critical to enact access policies that keep these devices from serving as an open door to your sensitive data and applications.

The following best practices will help to ensure that you can mitigate the threat of IoT malware, both with sanctioned and unsanctioned devices:

→ **Track and manage your network devices.** Many IoT devices are unmanaged, so you cannot rely on data from endpoint agents alone to gain visibility into what devices are in use on your premises. Deploy a solution that looks at network logs to understand what devices are currently communicating across your network and what they do. Implement architectures that allow you to inspect both encrypted and unencrypted network traffic for device communications that you may not otherwise be aware of. Then deploy safeguards.

→ **Change default passwords.** It's a tale as old as IT, but one of the easiest and most common ways for attackers to exploit devices is to use their default passwords. Password control may not be possible for unsanctioned IoT devices, but is a basic first step for deploying corporate-owned IoT devices, and should be part of your security training for any devices that employees bring to work.

→ **Stay on top of patching and updates.** Many industries—particularly manufacturing and healthcare—rely on IoT devices for their day-to-day workflows. For these sanctioned devices, make sure you stay apprised of any new vulnerabilities that are discovered, and that you keep your device security up-to-date with patches.

→ **Implement a zero trust security architecture.** Enforce strict policies for your corporate assets so that users and devices can access only what they need, and only after authentication. Restrict communication to relevant IPs, ASNs, and ports needed for external access. Unsanctioned IoT devices that require internet access should go through traffic inspection and be blocked from all corporate data, ideally through a proxy. The only way to stop shadow IoT devices from posing a threat to corporate networks is to eliminate implicit-trust policies and tightly control access to sensitive data using dynamic identity-based authentication—also known as zero trust.

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 Zero Trust Exchange™ 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**.