IoT IN THE ENTERPRISE

Empty Office Edition 2021

The COVID-19 pandemic forced companies to abruptly shutter their offices, instructing employees to work from home. For all of 2020 and much of 2021, these buildings weren't the only thing abandoned. Countless IoT devices remained inside the walls and connected to the corporate network, still refreshing data, performing functions and awaiting commands.

The Zscaler ThreatLabz threat research team took a deeper look into this activity on both sanctioned and unsanctioned IoT devices to unveil eye-opening IoT malware trends from the Zscaler cloud.

WHEN EMPLOYEES WERE AWAY, THREAT ACTORS PLAYED

Despite much of the global workforce working from home, IoT malware on corporate networks increased.

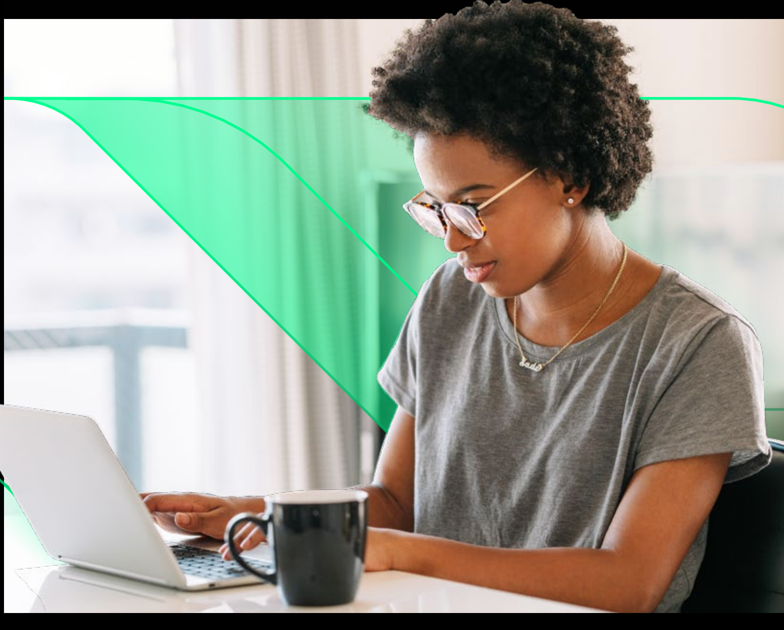
+700% year-over-year increase

833 IoT malware blocked every hour

RISKIEST DEVICES: ENTERTAINMENT & HOME AUTOMATION

Only 5% of traffic was from entertainment and home automation devices, including digital home assistants, set-top boxes, smart TVs, and smart watches. These introduced the most risk.

- Most device variety: 420 devices from 150 different manufacturers
- Almost no encryption: 98.66% of communications were in plaintext
- Traffic routed to suspicious destinations: 11% headed to China and Russia



MOST POPULAR MALWARE & DESTINATIONS

Malware payloads by family based on **900** unique deliveries:

Family	Share
Gafgyt	63.1%
Mirai	34.1%
Tsunami	1.9%
VPNFilter	0.9%
Hajime	0.1%

88.5% of compromised IoT devices routed data back to servers in:

56% China

19% United States

14% India

MOST IoT MALWARE ATTACKS

Top 3 Industries

40% Technology

28% Manufacturing

24% Retail & Wholesale

Top 3 Victimized Nations

Nation	Share
Ireland	48%
United States	32%
China	14%

4 FUNDAMENTALS FOR DEFENDING AGAINST IoT MALWARE

As smart devices continue to gain popularity, it's critical to enact access policies to keep them from acting as an open door to your network and use best practices, including:

- Track and manage network devices
- Change default passwords
- Stay on top of patching and updates
- Implement a zero trust architecture

Want to learn more?

Read the detailed results

zscaler.com

Research © 2021 ThreatLabZ, the research division of Zscaler Inc. All rights reserved. Zscaler™ is either (i) a registered trademark or service mark or (ii) a trademark or service mark of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.