

# IoT and OT Threat Trends in the Enterprise

Highlights from our 2023 ThreatLabz study of internet of things (IoT) and operational technology (OT) threat trends observed in the world's largest inline security cloud.

IoT and OT growth isn't slowing down. Neither is **malware**.



**400%** increase in IoT malware attacks over the same period in 2022<sup>1</sup>

**350+** unique malware attack payloads

## The 5 hardest-hitting malware families

Mirai  
**46%**

Gafgyt  
**20%**

These notorious malware families, known for turning IoT devices into bots, constituted the bulk of attack payloads, underscoring the ongoing threat of IoT botnets in IoT and OT environments.

Shikitega  
**8.1%**  
Part of a rising trend in Linux-based threats

BotenaGo  
**6.6%**  
Written in Golang, employs 30+ exploit functions

Mozi  
**5.3%**  
Exploits weak or default usernames and passwords

Have you forgotten about vulnerabilities of the past? Attackers haven't.

**34 of the 39** most popular IoT exploits targeted **3+ year old vulnerabilities**.



## Hardest-hit industries, devices, and nations



**55%**  
6,000 attacks per week

### Manufacturing sees lion's share of attacks

Over half of IoT malware attacks targeted manufacturing, followed by the food, beverage, and tobacco and education sectors. These attacks can disrupt critical OT processes that are integral to many industrial manufacturing domains.

**67%**

### Routers are the most-targeted device

More than two-thirds of IoT malware attacks took aim at routers, followed by IP cameras and DVRs.



### Mexico and the United States are top attack destinations

**46%**    **23%**

<sup>1</sup> Research compared January–June 2023 data over the same 2022 period.

## Best practices to defend against IoT and OT threats

The number of IoT and OT devices connecting to enterprise networks is only going up — expanding your attack surface. To safeguard your organization against threats like malware, you need to:

- Maintain comprehensive visibility into IoT devices
- Protect admin credentials and enable MFA
- Enforce an IoT/OT security framework
- Implement a zero trust security architecture

For more best practices and findings, download the Zscaler ThreatLabz 2023 Enterprise IoT/OT Threat Report.

[Get the Report](#)

