WHEN EMPLOYEES WERE AWAY, THREAT ACTORS PLAYED

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

**833**
IoT malware blocked every hour

+700%
year over year increase

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:

<table>
<thead>
<tr>
<th>Malware</th>
<th>Payloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gafgyt</td>
<td>63.1%</td>
</tr>
<tr>
<td>Mirai</td>
<td>34.3%</td>
</tr>
<tr>
<td>Tsunami</td>
<td>1.9%</td>
</tr>
<tr>
<td>VpnFilter</td>
<td>0.9%</td>
</tr>
<tr>
<td>Hajime</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

83.5% of compromised IoT devices routed data back to servers in:

- China: 56%
- United States: 19%
- India: 14%

MOST IoT MALWARE ATTACKS

Malware payloads by family, based on 900 unique deliveries:

- Technology: 40%
- Manufacturing: 28%
- Retail & Wholesale: 24%

Top 3 Industries

- Ireland: 48%
- United States: 32%
- China: 14%

Top 3 Victimized Nations

4 FUNDAMENTALS FOR DEFENDING AGAINST IoT MALWARE

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

IoT IN THE ENTERPRISE

Empty Office Edition 2021

The COVID-19 pandemic forced enterprises to abruptly shut down 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.

Want to learn more?

zscaler.com