# Zscaler Study Confirms IoT Devices are a Major Source of Security Compromise, Reinforces Need for Zero Trust Security

July 15, 2021

**Report Reveals a 700% Increase in IoT-Specific Malware and the ‘Chattiest’ IoT Devices**

**Key Findings**

- Technology, manufacturing, retail, and healthcare industries accounted for 98 percent of IoT malware attack victims
- Entertainment and home automation devices, including virtual assistants, pose the most risk
- Most IoT attacks originated in China, the United States, and India
- The top three nations victimized by IoT attacks were Ireland, the US, and China
- Gafgyt and Mirai malware families accounted for 97 percent of the IoT malware

SAN JOSE, Calif., July 15, 2021 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today released a new study examining the state of IoT devices left on corporate networks during a time when businesses were forced to move to a remote working environment. The new report, “IoT in the Enterprise: Empty Office Edition,” analyzed over 575 million device transactions and 300,000 IoT-specific malware attacks blocked by Zscaler over the course of two weeks in December 2020 – a 700% increase when compared to pre-pandemic findings. These attacks targeted 553 different device types, including printers, digital signage and smart TVs, all connected to and communicating with corporate IT networks while many employees were working remotely during the COVID-19 pandemic. The Zscaler™ ThreatLabz research team identified the most vulnerable IoT devices, most common attack origins and destinations, and the malware families responsible for the majority of malicious traffic to better help enterprises protect their valuable data.

“For more than a year, most corporate offices have stood mostly abandoned as employees continued to work remotely during the COVID-19 pandemic. However, our service teams noted that despite a lack of employees, enterprise networks were still buzzing with IoT activity,” said Deepen Desai, CISO of Zscaler. “The volume and variety of IoT devices connected to corporate networks is vast and includes everything from musical lamps to IP cameras. Our team saw 76 percent of these devices still communicating on unencrypted plain text channels, meaning that a majority of IoT transactions pose great risk to the business.”

**What Devices are Most at Risk?**
Out of over half a billion IoT device transactions, Zscaler identified 553 different devices from 212 manufacturers, 65 percent of which fell into three categories: set-top boxes (29 percent), smart TVs (20 percent), and smartwatches (15 percent). The home entertainment & automation category had the greatest variety of unique devices but they accounted for the least number of transactions when compared to manufacturing, enterprise, and healthcare devices.

Most traffic instead came from devices in manufacturing and retail industries – 59 percent of all transactions were from devices in this sector and included 3D printers, geolocation trackers, automotive multimedia systems, data collection terminals like barcode readers, and payment terminals. Enterprise devices were the second most common, accounting for 28 percent of transactions, and healthcare devices followed at nearly 8 percent of traffic.

ThreatLabz also discovered a number of unexpected devices connecting to the cloud, including smart refrigerators and musical lamps that were still sending traffic through corporate networks.

**Who’s Responsible?**
The ThreatLabz team also looked closely at activities specific to IoT malware tracked in the Zscaler cloud. Volume-wise, a total of 18,000 unique hosts and roughly 900 unique payload deliveries were observed in a 15-day timeframe. Malware families Gafgyt and Mirai were the two most common families encountered by ThreatLabz, accounting for 97 percent of the 900 unique payloads. These two families are known for hijacking devices to create botnets – large networks of private computers that can be controlled as a group to spread malware, overload infrastructure, or send spam.

**Who is Being Targeted?**
The top three nations targeted by IoT attacks were Ireland (48 percent), the United States (32 percent), and China (14 percent). The majority of compromised IoT devices, nearly 90 percent, were observed sending data back to servers in one of three countries: China (56 percent), the United States (19 percent), or India (14 percent).

**How can Organizations Protect Themselves?**
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. Rather than trying to eliminate shadow IT, IT teams should enact access policies that keep these devices from serving as open doors to the most sensitive business data and applications. These policies and strategies can be employed whether or not IT teams (or other employees) are on-premises. ThreatLabz recommends the following tips to mitigate the threat of IoT malware, both on managed and BYOD devices:

- **Gain visibility into all your network devices.** Deploy solutions able to review and analyze network logs to understand all devices communicating across your network and what they do.
- **Change all default passwords.** Password control may not always be possible, but a basic first step for deploying

corporate-owned IoT devices should be to update passwords and deploy two-factor authentication.

- **Update and patch regularly.** Many industries – particularly manufacturing and healthcare – rely on IoT devices for their day-to-day workflows. Make sure you stay apprised of any new vulnerabilities that are discovered, and that you keep device security up-to-date with the latest 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 Zscaler ThreatLabz**
The Zscaler ThreatLabz research team consists of security experts, researchers, and network engineers responsible for analyzing and eliminating threats across the Zscaler security cloud and investigating the global threat landscape. The team shares its research and cloud data with the industry at large to help promote a safer internet.

All data presented in this report is sourced directly from the Zscaler platform, which facilitates over 160 billion transactions daily. The data for this report was collected between December 15th and December 31, 2020, and only represents devices and attacks on corporate networks in physical office locations. ThreatLabz observed approximately 300,000 blocked transactions related to IoT malware, exploits, and command-and-control communications, including a total of 18,000 unique hosts and roughly 900 unique payload deliveries in this 15-day timeframe.

For more information, including access to the full report, please see "IoT in the Enterprise: Empty Office Edition."

**About Zscaler**
Zscaler (NASDAQ: ZS) accelerates digital transformation so 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 in-line cloud security platform.

**Media Contacts**
Natalia Wodecki
Global PR Director
press@zscaler.com