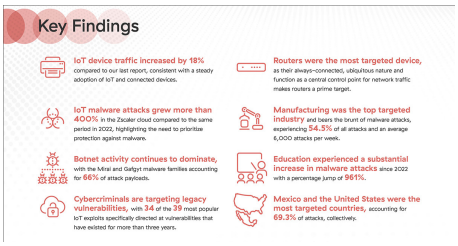
Zscaler ThreatLabz Finds a 400% Increase in IoT and OT Malware Attacks Year-over-Year, Underscoring Need for Better Zero Trust Security to Protect Critical Infrastructures

October 24, 2023

Zscaler ThreatLabz 2023 Enterprise IoT and OT Threat Report Uncovers Manufacturing and Education Sectors Targeted the Most, with Education Realizing a Nearly 1000% Increase in IoT Malware Attacks

Zscaler 2023 IoT Report



Zscaler 2023 IoT Report Key Findings

Key findings:

- **The manufacturing industry, which relies heavily on both IoT and OT, was the top targeted sector, bearing** the brunt of blocked IoT malware attacks, accounting for 54.5% of all attacks and averaging 6,000 weekly attacks across all monitored devices
- **Education experienced a substantial increase in IoT malware attacks**, with a percentage jump of 961%
- **Mexico and the United States were the most targeted countries**, collectively accounting for 69.3% of attacks
- **IoT botnet activity, a growing concern in the realm of OT, continues to dominate**, with the Mirai and Gafgyt malware families accounting for 66% of attack payloads

SAN JOSE, Calif., Oct. 24, 2023 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ:ZS), the leader in cloud security, announced today the release of the Zscaler™ ThreatLabz 2023 Enterprise IoT and OT Threat Report. This year's report provides an in-depth look at malware activity over a six-month period, analyzing approximately 300,000 blocked attacks on IoT devices secured by the Zscaler Zero Trust Exchange™ platform. The high number of attacks on IoT devices represents a 400% increase in malware compared to the previous year. The increasing frequency of malware attacks targeting IoT devices is a significant concern for OT security, as the mobility of malware can facilitate movement across different networks, potentially endangering critical OT infrastructure.

ThreatLabz focused on understanding IoT device activity and attributes via device fingerprinting and analyzing the IoT malware threat landscape. As more industries, organizations and individuals continue to rely on internet-connected devices, the threat from malware and legacy vulnerabilities increases. By adopting a zero trust architecture, organizations can gain visibility into IoT device traffic and minimize IoT security risks.

"Weak enforcement of security standards for IoT device manufacturers coupled with the proliferation of shadow IoT devices at the enterprise level poses a significant threat to global organizations. Often, threat actors target 'unmanaged and unpatched' devices to gain an initial foothold into the environment," said Deepen Desai, Global CISO and Head of Security Research, Zscaler. "To address these challenges, I encourage organizations to enforce zero trust principles when securing IoT and OT devices - never trust, always verify, and assume breach. Organizations can eliminate lateral movement risk by utilizing continuous discovery and monitoring processes to segment these devices."

Consistent growth in attacks
With the steady adoption of IoT and personal connected devices, the report found an increase of over 400% in IoT malware attacks year-over-year. The growth in cyber threats demonstrates cyber criminals persistence and ability to adapt to evolving conditions in launching IoT malware attacks.

Additionally, research indicates that cybercriminals are targeting legacy vulnerabilities, with 34 of the 39 most popular IoT exploits specifically directed at vulnerabilities that have existed for over three years. The Mirai and Gafgyt malware families continue to account for 66% of attack payloads, creating botnets from infected IoT devices that are then used to launch denial-of-service (DDoS) attacks against lucrative businesses. Botnet-driven distributed DDoS attacks are responsible for billions of dollars in financial losses across industries around the globe. In addition, DDoS attacks pose a risk to OT by potentially disrupting critical industrial processes and even endangering human lives.

Manufacturing top targeted industry - Education being taught a lesson
Manufacturing and retail accounted for nearly 52% of IoT device traffic, with 3D printers, geolocation trackers, industrial control devices, automotive multimedia systems, data collection terminals, and payment terminals sending the majority of signals over digital networks. However, the quantity of device traffic has created opportunities for cybercriminals, and the manufacturing sector now sees an average of 6,000 IoT malware attacks every week. Moreover, these substantial IoT malware attacks can disrupt critical OT processes, which are integral in many industrial manufacturing plants like automotive, heavy manufacturing, and plastic & rubber. This creates long-term challenges for security teams at manufacturing businesses but also demonstrates that industrial IoT holds a substantial lead in adopting unique IoT devices (nearly three times more than other sectors). This increase is critical as manufacturing organizations continue adopting IoT tools for automation and digitization of legacy infrastructure.

Education is another sector that suffered from outsized attention from cybercriminals in 2023, with the propagation of unsecured as well as shadow IoT devices within school networks providing attackers with easier access points. The wealth of personal data stored on their networks has made educational institutions particularly attractive targets, leaving students and administrations vulnerable. In fact, the report found IoT malware attacks in the education sector increased by nearly 1000%.

The United States and Mexico are the most targeted
Findings show that the United States is a top target for IoT malware authors with 96% of all IoT malware distributed from compromised IoT devices in the United States.

In 2023, Mexico experienced the most infections, with 46% of all IoT malware infections. In fact, three of the top four most infected countries (Mexico, Brazil, and Colombia) are all Latin American countries.

Safeguarding against IoT/OT attacks with the Zscaler Zero Trust Exchange™
The Zscaler Zero Trust Exchange platform is a holistic approach to zero trust security, verifying identity and context, applying access controls, and enforcing policies before brokering a secure connection between a device and an application from anywhere, and on any network.

Zscaler protects enterprise networks using the Zero Trust Platform by leveraging Zscaler Internet Access™ (ZIA™), whose identity-driven access and risk-based, comprehensive security protects the exchange of telemetry between IoT devices and corporate networks.

Zscaler protects the security of enterprise networks with the Zero Trust Exchange platform, which utilizes Zscaler Privileged Remote Access to provide remote workers and third-party vendors with clientless remote desktop access to sensitive RDP, SSH, and VNC production systems without having to install a client on unmanaged devices or log into jump hosts and VPNs. This means remote employees or third-parties can access and service OT devices without compromising the security of the network or the critical infrastructure it powers.

To download your full copy of the report, please visit *Zscaler ThreatLabz 2023 Enterprise IoT and OT Threat Report*.

Methodology
The research methodology for this report includes analysis of device logs from a multitude of sources and industry verticals between January and June 2023.

The report uses data derived from customer deployments that connect to the Zscaler global security cloud, which processes over 500 trillion daily signals and blocks 9 billion threats and policy violations per day, with over 250,000 daily security updates.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

Media Contact:
Nick Gonzalez
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/ebe5bd1a-92fd-491a-a005-c3eab5088ac8