Zscaler ThreatLabz Finds Most Cyberattacks Hide In Encrypted Traffic

December 14, 2023

86% of Cyberattacks Are Delivered Over Encrypted Channels, with Manufacturing Being The Most Targeted Industry

Key findings:

- Threats over HTTPS grew by 24% year-over-year in the Zscaler cloud, representing nearly 30 billion threats blocked
- Encrypted malware and malicious content is a top threat, comprising 78% of observed attacks
- Manufacturing was the most targeted industry, experiencing 32% of encrypted attacks, with over 2.1 billion AI/ML-related transactions processed
- Browser exploits and ad spyware sites have increased by 297% and 290% year-over-year

SAN JOSE, Calif., Dec. 14, 2023 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, announced today the release of its annual Zscaler™ ThreatLabz 2023 State of Encrypted Attacks Report. This year's report focused on the increase in threats over HTTPS, which grew by 24% from 2022, underscoring the sophisticated nature of cybercriminal tactics that target encrypted channels. For the second year in a row, manufacturing was the industry most commonly targeted, with education and government organizations seeing the highest year-over-year increase in attacks. Additionally, malware, which includes malicious web content and malware payloads, continued to dominate over other types of encrypted attacks, with ad spyware sites and cross-site scripting accounting for 78% of all blocked attacks. This year's research analyzed nearly 30 billion blocked threats from October 2022 to September 2023 by the Zscaler Zero Trust Exchange™ platform, the world's largest security cloud platform.

In total, 86% of all cyber threats, including malware, ransomware, and phishing attacks, are delivered over encrypted channels.

"With nearly 95% of web traffic flowing over HTTPS and 86% of the advanced threats delivered over encrypted channels, any HTTPS traffic that does not undergo inline inspection represents a significant blind spot that cybercriminals continue to exploit when targeting global organizations," said Deepen Desai, Chief Security Officer, Zscaler. "To defend against encrypted attacks, organizations should replace vulnerable appliances, like VPNs and firewalls, with a Zero Trust Network Access (ZTNA) solution. This allows IT teams to inspect TLS traffic at scale while blocking threats and preventing sensitive data leakage."

Malware is the top encrypted threat
Malware keeps its top spot as the champion of encrypted threats, driving 23 billion encrypted hits between October 2022 and September 2023 and comprising 78% of all attempted cyberattacks.

Encrypted malware includes malicious web content, malware payloads, macro-based malware, and more. The most prevalent malware family in 2023 was ChromeLoader, followed by MedusaLocker and Redline Stealer.

Manufacturing keeps its spot as the most targeted industry
Manufacturers saw the largest amount of AI/ML transactions compared to any other industry, processing over 2.1 billion AI/ML-related transactions. It remains the most targeted industry, accounting for 31.6% of encrypted attacks tracked by Zscaler. As smart factories and the Internet of Things (IoT) become more prevalent in manufacturing, the attack surface is expanding and exposing the sector to more security risks and creating additional entry points that cybercriminals can exploit to disrupt production and supply chains.

Additionally, the use of popular generative AI applications, like ChatGPT, on connected devices in manufacturing heightens the risk of sensitive data leakage over encrypted channels.

Education and Government see a huge surge in attacks
The Education and Government sectors experienced a 276% and 185% year-over-year surge in encrypted attacks, respectively. The Education industry has also seen a significantly expanded attack surface in recent years, with the shift to enable more remote and connected learning. Meanwhile, the Government sector remains an attractive target, particularly for nation-state-backed threat actors, as reflected in the growth of encrypted threats.

Stopping encrypted attacks with the Zscaler Zero Trust Exchange
To defend against the evolving encrypted threat landscape, enterprises must rethink traditional approaches to security and networking and adopt more comprehensive, zero trust architectures. Enterprises must implement a zero trust architecture that inspects all encrypted traffic and leverages AI/ML models to block or isolate malicious traffic. This creates a single, operationally simple way to apply policy across all traffic, without impacting performance or creating a compliance nightmare.

The Zscaler Zero Trust Exchange platform offers a more holistic approach to zero trust security, providing security controls that comprehensively reduce business risk at each stage of an attack. Additionally, it enables HTTPS inspection at scale using a multilayered approach that has inline threat inspection, sandboxing, and data loss prevention, along with a wide array of AI-driven defense capabilities. The Zscaler platform also uses cloud effect to automatically update within seconds and ensure customers have rapid protection against the latest threats and vulnerabilities, continuously improving their security posture.

ThreatLabz recommendations to prevent encrypted attacks

- Use a cloud native, proxy-based architecture to decrypt, detect, and prevent threats in all encrypted traffic at scale.
- Inspect all traffic, all the time, use SSL inspection to detect malware payloads, phishing and C2 activity that use SSL/TLS

communication.
- Leverage an AI-driven sandbox to quarantine unknown attacks and stop patient zero malware that may be delivered over TLS.
- Evaluate the organization's attack surface to quantify risk and secure the exposed attack surface.
- Use zero trust architecture to secure all connectivity holistically.
- Use user-app segmentation to enforce least privilege access, even for authenticated users.

To download your full copy of the report, please visit *Zscaler ThreatLabz 2023 State of Encrypted Attacks Report*.

Methodology
Analysis of 29.8 billion blocked threats inside encrypted channels, SSL and TLS, from October 2022 to September 2023 in the Zscaler cloud.

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