Zscaler Finds Over 87% of Cyberthreats Hide in Encrypted Traffic, Reinforcing Need For Zero Trust

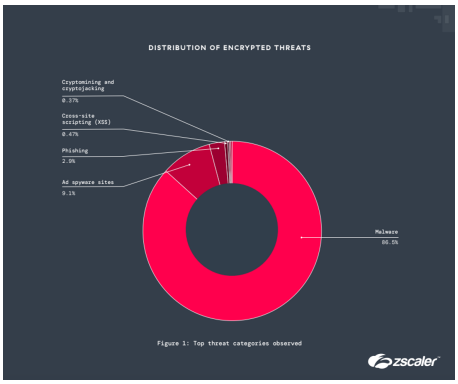
December 5, 2024

Latest Zscaler ThreatLabz Report Uncovers How Cybercriminals Use Encrypted Channels to Launch Crypto, Phishing and Other Sophisticated Attacks

Key Findings:

- Malware, phishing and cryptominers account for nearly 90% of all encrypted threats observed in ThreatLabz analysis
- Manufacturing was the target of 42% of encrypted attacks, making it the most- targeted industry
- The United States and India are the top targets of encrypted attacks

ThreatLabz Encrypted Attacks Report 2024



Distribution of Encrypted Attacks

SAN JOSE, Calif., Dec. 05, 2024 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today published its Zscaler ThreatLabz 2024 Encrypted Attacks Report, which explores the latest threats blocked by the Zscaler security cloud and provides critical insights into how encryption has become a conduit for more sophisticated threats, further compounded by the rise of artificial intelligence (AI). ThreatLabz found that over 87% of all threats were delivered over encrypted channels between October 2023 and September 2024—a 10% increase year-over-year. The report offers strategies and best practices to help organizations tackle these covert threats.

"The rise in encrypted attacks is a real concern as a significant share of threats are now delivered over HTTPS," said Deepen Desai, Chief Security Officer, Zscaler. "With threat actors focused on exploiting encrypted channels to deliver advanced threats and exfiltrate data, organizations must implement a zero trust architecture with TLS/SSL inspection at scale. This approach helps to ensure that threats are detected and blocked effectively, while safeguarding data without compromising performance."

Encrypted malware continues to dominate
Malware accounted for 86% of encrypted attacks, totaling 27.8 billion hits—a 19% year-over-year increase. Encrypted malware includes malicious web content, malware payloads, macro-based malware, etc. This growing prevalence of malware reflects a strategic shift by attackers adapting tactics to thrive within encrypted traffic, using encryption to conceal malicious payloads and content.

According to ThreatLabz researchers, the most active malware families were:

- AsyncRAT
- Choziosi Loader/ChromeLoader
- AMOS/Atomic Stealer
- Ducktail
- Agent Tesla
- Koi Loader

The report also details notable year-over-year increases in web-based attacks, including cryptomining/cryptojacking (123%), cross-site scripting (110%) and phishing (34%), among other encrypted threats—surges that could be potentially fueled by the growing use of generative AI technologies by threat actors.

Most targeted industry verticals
Manufacturing was the most-targeted industry, accounting for 42% of encrypted attacks—nearly three times more than the second-most targeted industry, technology and communications. Attacks on the manufacturing industry grew 44% year-over-year, likely driven by rapid industry 4.0 advancements and the extensive use of interconnected systems, which have expanded the attack surface and heightened manufacturers' vulnerability to cyber threats.

The top five most targeted industries were:

- Manufacturing
- Technology and communications
- Services
- Education
- Retail and wholesale

Countries that experience the most encrypted attacks
ThreatLabz found that the United States, India and France are the most frequently targeted nations by encrypted attacks. The U.S. and India are consistently the top two most frequently targeted, highlighting their significance as high-value targets for cybercriminals. The top five most targeted countries by encrypted attacks were:

- United States - 11B
- India - 5.4B
- France - 854M
- United Kingdom - 741M
- Australia - 672M

Stopping encrypted attacks with zero trust
Understanding how zero trust disrupts encrypted threats requires looking at a typical attack sequence. Advanced attacks often unfold in four stages:

1. First, attackers conduct reconnaissance to find a way into the targeted network.
2. Next, they breach the network, often via exploits, brute-force attacks or stolen credentials.
3. Once inside, they move laterally, escalate privileges and establish persistence.
4. Finally, they carry out their objectives, typically conducting data exfiltration to extract valuable information that can be leveraged for further extortion or attacks.

The Zscaler Zero Trust Exchange ™ platform provides security controls at each stage to mitigate risk and stop encrypted threats.

A key component of the Zscaler platform's approach is its full TLS/SSL inspection capabilities, based on an advanced proxy architecture. Zscaler advises inspecting 100% of traffic to protect users and organizations from threats concealed within encrypted channels.

Organizations can bolster their ability to protect their devices, apps and data from encrypted attacks by following these recommendations:

- Understand that any internet-facing service can be found and attacked or abused
- Inspect incoming encrypted traffic to detect and block threats
- Use a zero trust architecture to secure all connectivity holistically between users and applications, between devices like IoT and OT systems, between all locations and branch offices, between cloud workloads and more.
- Implement microsegmentation to reduce access, even for authenticated users.
- Leverage an AI-driven cloud sandbox to isolate and quarantine unknown attacks and stop patient-zero malware before it touches users.
- Reduce the number of entry points into an environment.
- Inspect outgoing northbound traffic along with incoming southbound traffic to disrupt C2 communications and protect sensitive data.

The ThreatLabz 2024 Encrypted Attacks Report provides additional insights and best practices to help organizations effectively prevent encrypted attacks. Download your copy here today.

Research Methodology
Analysis of 32.1 billion blocked threats from October 2023 to September 2024 in the Zscaler cloud shows that all blocked threats came via encrypted channels.

About ThreatLabz
ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

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:

Zscaler PR
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/cf6e16ce-f9d0-4b72-b7ea-1eabaad015e3