Ransomware Surges as Attempts Spike 146% Amid Aggressive Extortion Tactics

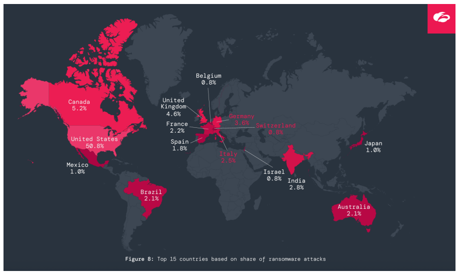
July 29, 2025

Zscaler's Annual ThreatLabz Report Reveals Key Ransomware Groups Stole 238 TB of Data in One Year

Key Findings:

- **Ransomware attacks blocked by the Zscaler cloud rose 146%**, the sharpest spike observed in the past three years.
- **Public extortion cases jumped by 70%** based on data leak site analysis.
- **Data exfiltration volumes increased 92%**.
- **Manufacturing, Technology, and Healthcare were the top targeted industries**, and the Oil & Gas sector experienced a 935% increase in attacks.

Ransomware report countries



Top 15 countries based on share of ransomware attacks

SAN JOSE, Calif., July 29, 2025 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today published its annual Zscaler ThreatLabz 2025 Ransomware Report. The report examines the latest trends shaping the ransomware threat landscape, revealing how attacks are adapting and escalating. It highlights the most targeted sectors and regions, profiles the most active ransomware families, analyzes shifting attack methodologies, and provides actionable recommendations to help organizations strengthen their defenses. ThreatLabz's findings underscore the critical importance of organizations adopting a comprehensive Zero Trust Everywhere strategy. This approach is essential to prevent ransomware and other malicious threats from lateral movement and compromising sensitive user data, applications, and information.

"Ransomware tactics continue to evolve, with the growing shift toward extortion over encryption as a clear example," said Deepen Desai, EVP Cybersecurity, Zscaler. "GenAI is also increasingly becoming part of the ransomware threat actor's playbook, enabling more targeted and efficient attacks. As threats advance, security measures must keep pace. The Zscaler Zero Trust Exchange™ platform empowers organizations to shrink their attack surface, identify and block initial compromise threats, prevent lateral movement, and stop data exfiltration to shut down extortion events before they happen."

Data Demand Fuels Steady Attack Growth

Ransomware attacks are intensifying at an alarming rate, with attempted attacks blocked in the Zscaler cloud up 146% year-over-year. This escalation reflects a strategic shift: ransomware groups are increasingly prioritizing extortion over encryption. Accordingly, the report details a 92% increase in the total volume of exfiltrated data by 10 major ransomware groups in the past year, rising from 123 TB to 238 TB. This emphasis on data theft—and the threat of exposure—allows attackers to exert greater pressure on victims, amplifying the impact of ransomware on organizations globally.

Industries Under Siege

Cybercriminals continue to focus on the high-stakes environments of the Manufacturing (1,063 attacks), Technology (922), and Healthcare (672) sectors, making them the most frequently hit by ransomware over the past year. These industries are particularly vulnerable due to the potential for operational disruption, the sensitivity of stolen data, and the associated risks of reputational damage and regulatory fallout.

The Oil & Gas sector has seen a staggering increase in ransomware attacks, spiking over 900% year-over-year. This surge is likely a result of increased automation of systems that control critical infrastructure, including drilling rigs and pipelines, expanding the sector's attack surface, coupled with outdated security practices.

United States Is the Target of Half of All Ransomware Attacks

Leak site data highlights a distinct geographic disparity, with victims in the United States accounting for 50% of ransomware attacks, significantly outpacing Canada (5%) and the United Kingdom (4%). Ransomware attacks in the U.S. more than doubled to 3,671, exceeding the combined total number of attacks reported across all other countries in the top 15 most-targeted countries. This concentration demonstrates how threat actors continue to strategically target digitally concentrated, high-value economies.

Ransomware Groups Driving the Surge

Several highly active groups continued to dominate the ransomware ecosystem, with RansomHub leading the pack, claiming the highest number of publicly named victims at 833. Akira and Clop have both moved up in the ransomware attack rankings since last year. Akira, associated with 520 victims, has steadily expanded its reach through numerous affiliates and initial access brokers. Clop, known for its focus on supply chain attacks, is close behind with 488 victims, employing an effective strategy of exploiting vulnerabilities in commonly used third-party software.

Zscaler ThreatLabz identified 34 newly active ransomware families over the past year, bringing the total number tracked to 425 since their research began, and has a public GitHub repository that now hosts 1,018 ransomware notes, with 73 added in the last year.

How Zscaler Stops Ransomware with Zero Trust + AI

Ransomware flourishes in environments with fragmented security, limited visibility, implicit trust, and outdated legacy architectures that amplify risk rather than reduce it. The Zscaler Zero Trust Exchange mitigates these risks by replacing traditional, network-centric models with a cloud-native, AI-driven zero trust architecture, and stops ransomware at every stage of the attack life cycle by:

- **Minimizing the attack surface**

- **Preventing initial compromise**
- **Eliminating lateral movement**
- **Blocking data exfiltration**

Additional AI-powered ransomware protections from Zscaler include:

- Breach prediction
- Phishing and C2 detection
- Inline sandboxing
- Zero Trust Browser
- Segmentation
- Dynamic, risk-based policy
- Data discovery and classification
- Data loss prevention (DLP) controls

Download the Report
Get the full ThreatLabz 2025 Ransomware Report to explore how Zscaler ThreatLabz plays an active role in protecting enterprises worldwide. **Download today.**

Research Methodology
The research methodology for this report is a comprehensive process that uses multiple data sources to identify and track ransomware trends. The ThreatLabz team collected data between April 2024 and April 2025 from sources including the Zscaler global security cloud, and the team's own analysis of ransomware samples and attack data.

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 160 data centers globally, the SASE-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/b92c9822-3941-45ec-8aa1-87defcd57281