Zscaler’s Annual Ransomware Report Uncovers Record-Breaking Ransom Payment of US$75 Million, Reinforcing the Need for Zero Trust

July 30, 2024

Key Findings:

- ThreatLabz tracked an **18% increase in ransomware attacks** year-over-year
- **Manufacturing, healthcare, and technology sectors** were the top targets of ransomware attacks
- **The United States remains the top target of ransomware, experiencing nearly 50% of overall attacks,** followed by the United Kingdom, Germany, Canada, and France
- **ThreatLabz identified 19 new ransomware families during the analysis period,** bringing the total number to 391 since tracking started

ThreatLabz 2024 Ransomware Report

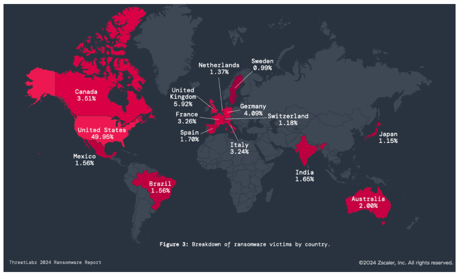

Figure 3: Breakdown of ransomware victims by country

SAN JOSE, Calif., July 30, 2024 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today published its Zscaler ThreatLabz 2024 Ransomware Report, which analyzed the ransomware threat landscape from April 2023 through April 2024. The annual report details the latest ransomware attack trends and targets, ransomware families, and effective defense strategies. Findings in the report uncovered an 18% overall increase in ransomware attacks year-over-year, as well as a record-breaking ransom payment of US$75 million – nearly double the highest publicly known ransomware payout – to the Dark Angels ransomware group. ThreatLabz believes Dark Angels’ success will drive other ransomware groups to use similar tactics, reinforcing the need for organizations to prioritize protection against rising and ever-more costly ransomware attacks.

“Ransomware defense remains a top priority for CISOs in 2024. The increasing use of ransomware-as-a-service models, along with numerous zero-day attacks on legacy systems, a rise in vishing attacks and the emergence of AI-powered attacks, has led to record breaking ransom payments,” said Deepen Desai, Chief Security Officer at Zscaler. “Organizations must prioritize Zero Trust architecture to strengthen their security posture against ransomware attacks. This is where an AI-powered Zero Trust platform like Zscaler helps organizations fast-track their segmentation journeys, reducing the blast radius as well as shutting down unknown vectors for future AI-driven attacks.”

Top industries impacted by ransomware
Ransomware attacks pose significant risks to businesses of all sizes and industries. The manufacturing industry was by far the most targeted according to the report, facing more than twice as many attacks as any other industry.

Industries face unique ransomware challenges based on how they operate, handle data, and their technology infrastructure. Despite the variables, ransomware extortion attacks have consistently surged, with the number of victim companies listed on data leak sites increasing by nearly 58% since last year’s ransomware report.

Most targeted industries in ransomware attacks

- Manufacturing
- Healthcare
- Technology
- Education
- Financial Services

United States remains top target
The United States once again faced a higher volume of ransomware attacks than any other country, accounting for nearly half of all incidents globally.

Most targeted countries for ransomware attacks:

- United States (49.95%)
- United Kingdom (5.92%)
- Germany (4.09%)
- Canada (3.51%)
- France (3.26%)

When comparing year-over-year change in ransomware attacks, the US, Italy and Mexico saw the highest increase in ransomware attacks, with staggering rises of 93%, 78% and 58%, respectively.

Most active ransomware families
While ransomware and other cyberthreats continue to evolve in complexity and sophistication, staying informed about the most prevalent and

dangerous ransomware families is crucial for maintaining an effective security posture.

ThreatLabz identified the most active ransomware families:

- LockBit (22%)
- BlackCat (aka ALPHV) (9%)
- 8Base (8%)

Top five ransomware families to watch in 2024-2025:

1. Dark Angels
2. LockBit
3. BlackCat
4. Akira
5. Black Basta

Zscaler helps enterprises stop ransomware with zero trust security
From initial reconnaissance and compromise to lateral movement, data theft and payload execution, Zscaler helps organizations stop ransomware at every stage of the attack cycle:

- **Minimize the attack surface**: Zscaler effectively minimizes the attack surface by hiding users, applications and devices behind a cloud proxy, where they are not visible or discoverable from the internet.
- **Prevent initial compromise**: The Zscaler Zero Trust Exchange employs extensive TLS/SSL inspection, browser isolation, advanced inline sandboxing and policy-driven access controls to prevent users from accessing malicious websites as well as detect unknown threats before they reach your network.
- **Eliminate lateral movement**: Leverage user-to-app or app-to-app segmentation so that users connect directly to applications (and apps to other apps), not the network, eliminating the risk of lateral movement.
- **Stop data loss**: Inline data loss prevention measures, combined with full TLS/SSL inspection, effectively thwart data theft attempts. Zscaler ensures that data is secured both in transit and at rest.

For a deeper dive into best practices for protecting your organization and the full findings, download the Zscaler ThreatLabz 2024 Ransomware Report.

Methodology
The research methodology for this report is a comprehensive process that uses multiple data sources to identify and track ransomware trends. The report team collected data from a variety of sources between April 2023 and April 2024.

To identify and understand ransomware activity, Zscaler utilizes its global security cloud processing over 500 trillion daily signals, blocking 9 billion threats daily, and delivering 250,000+ security updates. The ThreatLabz Threat Intelligence team tracks ransomware families at scale through reverse engineering and automating malware analysis to develop effective response strategies. ThreatLabz also works closely with international law enforcement agencies and has played a significant role in recent actions, including Operation Duck Hunt and Operation Endgame.

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
press@zscaler.com

A photo accompanying this announcement is available at
https://www.globenewswire.com/NewsRoom/AttachmentNg/33c744e3-5699-4d2c-a097-5be7fc622f1e