Zscaler 2023 Ransomware Report Shows a Nearly 40% Increase in Global Ransomware Attacks

June 28, 2023

Annual ThreatLabz Ransomware Report Tracks Trends and Impacts of Ransomware Attacks Including Encryption-less Extortion and Growth of Ransomware-as-a-Service

Key Findings:

- Ransomware impact is felt most acutely in the United States, which was the target for nearly half of ransomware campaigns over the last 12 months.
- Organizations in the arts, entertainment, and recreation industry experienced the largest surge in ransomware attacks, with a growth rate over 430%.
- The manufacturing sector remains the most targeted industry vertical, accounting for nearly 15% of total ransomware attacks. It is followed by the services sector, which experienced approximately 12% of the total quantity of ransomware attacks last year.
- 25 new ransomware families were identified as using double extortion or encryption-less extortion attacks this year.

SAN JOSE, Calif., June 28, 2023 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced the release of the 2023 ThreatLabz Ransomware Report. This year's report tracks the ongoing increase in complex ransomware attacks and spotlights recent ransomware trends, including the targeting of public entities and organizations with cyber insurance, growth of ransomware-as-a-service (RaaS), and encryption-less extortion. Since April 2022, ThreatLabz has identified thefts of several terabytes of data as part of several successful ransomware attacks, which were then used to extort ransoms.

"Ransomware-as-a-Service has contributed to a steady rise in sophisticated ransomware attacks," said Deepen Desai, Global CISO and Head of Security Research, Zscaler. "Ransomware authors are increasingly staying under the radar by launching encryption-less attacks which involve large volumes of data exfiltration. Organizations must move away from using legacy point products and instead migrate to a fully integrated zero trust platform that minimizes their attack surface, prevents compromise, reduces the blast radius in the event of a successful attack, and prevents data exfiltration."

The evolution of ransomware is characterized by the inverse relationship between attack sophistication and barrier of entry for new cybercriminal groups. The barrier of entry has decreased, while cyberattacks have grown in sophistication, due to the prevalence of RaaS, a model where threat actors sell their services on the dark web for 70-80% of ransomware profits. This business model has continued to increase in popularity over the last few years as evidenced by the frequency of ransomware attacks, which increased by nearly 40% over the last year. One of the most noteworthy trends that aligned with this growth in 2023 has been the growth of encryption-less extortion, a style of cyberattack that prioritizes data exfiltration over disruptive encryption methods.

Top Countries Targeted by Ransomware
The United States was the most targeted country by double-extortion ransomware attacks, with 40% of all victims calling this region home. The following three countries combined, Canada, United Kingdom, and Germany, had less than half of the attacks that targeted U.S. entities. The most prevalent ransomware families that Zscaler ThreatLabz has been tracking include BlackBasta, BlackCat, Clop, Karakurt, and LockBit, all of which pose a significant threat of financial losses, data breaches, and operational disruption to individuals and organizations of all sizes.

Over the last year, the most-targeted market sector globally was manufacturing, where intellectual property and critical infrastructure are attractive targets for ransomware groups. All ransomware groups tracked by Zscaler victimized businesses in this industry, which included companies engaged in goods production for sectors including automotive, electronics, and textiles - just to name a few. Zscaler research noted that the BlackBasta ransomware family was particularly interested in manufacturing organizations, targeting these types of businesses more than 26% of the time.

Growing Trends in Ransomware
In 2021, ThreatLabz observed 19 ransomware families that adopted double or multi-extortion approaches to their cyberattacks. This has since grown to 44 ransomware families observed. The reason these types of attacks are popular is because after they encrypt the stolen data, attackers threaten to leak the data online to further increase the pressure on victims to pay. The increasing popularity of Encryptionless Extortion attacks, which skips over the process of encryption, employs the same tactic of threatening to leak victims' data online if they don't pay. This tactic results in faster and larger profits for ransomware gangs by eliminating software development cycles and decryption support. These attacks are also harder to detect and receive less attention from the authorities because they do not lock key files and systems or cause the downtime associated with recovery. Therefore, Encryptionless Extortion attacks tend to not disrupt their victims' business operations - which subsequently results in lower reporting rates. Originally, the Encryptionless Extortion trend started with ransomware groups like Babuk and SnapMC. Over the last year, researchers saw a number of new families adopt the tactic, including Karakurt, Donut, RansomHouse, and BianLian.

Protecting Against Ransomware Attacks with the Zscaler Zero Trust Exchange

Guarding against ransomware attacks requires a comprehensive approach that tackles every stage of the threat, minimizing potential harm. The Zscaler Zero Trust Exchange offers an all-encompassing zero trust framework integrated with cutting-edge ransomware protection measures. By adopting the following guidelines, you can effectively reduce the risk of falling victim to a ransomware attack.

1. **Prevent Initial Compromise**: Employ consistent security policies that ensure uncompromising security. By implementing extensive SSL inspection capabilities, browser isolation, inline sandboxing, and policy-driven access control, you can thwart

access to malicious websites, block channels of initial compromise and detect unknown threats from reaching your users.

2. **Stop Compromised Users and Insider Threats**: Combining inline application inspection and Identity Threat Detection & Response (ITDR) with integrated deception capabilities empowers you to detect, deceive, and effectively stop potential attackers, whether they are external threats or insiders with malicious intent.

3. **Minimize External Attack Surface & Eliminate Lateral Movement**: Prevent attackers from maneuvering within your network by disconnecting applications from the internet and embracing a zero trust network access (ZTNA) architecture. Directly connecting users to applications, and applications to applications, rather than the network itself, significantly restricts the potential reach of an attack.

4. **Prevent Data Loss**: Implement inline data loss prevention measures with full TLS inspection and thoroughly inspect data both while in transit and at rest, to effectively stop data theft attempts. Stay one step ahead of threat actors by regularly updating software and providing comprehensive security training.

By leveraging the power of the Zscaler Zero Trust Exchange and adopting these best practices, organizations can proactively protect their users, workloads, IoT/OT devices and B2B connectivity, so that valuable data is safe from the ever-evolving threat landscape of ransomware attacks.

To download your full copy of the report, please visit 2023 ThreatLabz Ransomware Report.

Methodology
The ThreatLabz team evaluated data from the Zscaler security cloud, which monitors over 500 trillion daily signals and blocks 8 billion threats a day with over 250K security updates made daily. ThreatLabz analyzed a year's worth of global phishing data from the Zscaler cloud from April 2022 to April 2023 to identify key trends, industries and geographies at risk, and emerging tactics. This year, the ThreatLabz team also supplemented its own analysis of ransomware samples and attack data with external intelligence sources.

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 Contacts
Natalia Wodecki
Sr. Director, Global Integrated Communications & PR
press@zscaler.com