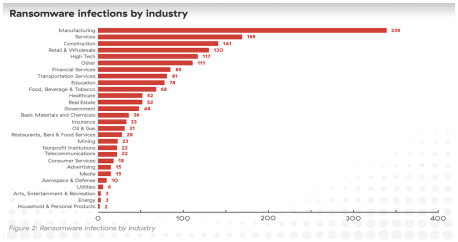
Zscaler ThreatLabz 2022 Ransomware Report Reveals Record Number of Attacks and Nearly 120% Growth in Double Extortion Ransomware

June 2, 2022

Manufacturers are the Most Targeted for the Second Year in a Row; Healthcare Sees the Biggest Jump in Ransomware Attacks with Nearly a 650% Increase

Zscaler 2022 Ransomware Report



Ransomware infections by industry

Key Findings:

- Ransomware attacks have increased by 80% year-over-year with ransomware-as-a-service being used by eight of the top 11 ransomware families.
- Nearly one in five ransomware attacks target manufacturing businesses, making this industry the most targeted for the second year in a row.
- Healthcare (650% increase) and Restaurant and Food Service (450%) industries saw the biggest growth of ransomware attacks when compared to 2021.
- Ransomware families are rebranding to evade law enforcement and continue to infect businesses.
- Supply chain ransomware attacks are multiplying damages and allowing attackers to bypass traditional security controls.
- The Russia-Ukraine war is threatening an increase in ransomware combined with other attack techniques, such as the pairing of PartyTicket ransomware and HermeticWiper malware.

SAN JOSE, Calif., June 02, 2022 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today released the findings of its annual ThreatLabz Ransomware Report, which revealed an 80 percent increase in ransomware attacks year-over-year. In 2022, the most prevalent ransomware trends include double-extortion, supply chain attacks, ransomware-as-a-service, ransomware rebranding, and geo-political incited ransomware attacks. The report analyzes over a year's worth of data from the largest security cloud in the world, which processes more than 200 billion daily transactions and 150 million daily blocked attacks across the Zscaler Zero Trust Exchange™. The report details which industries are being targeted the most by cybercriminals, explains the damage caused by double-extortion and supply chain attacks, and catalogs the most active ransomware groups operating today.

"Modern ransomware attacks require a single successful asset compromise to gain initial entry, move laterally, and breach the entire environment, making legacy VPN and flat networks extremely vulnerable," said Deepen Desai, CISO of Zscaler. "Attackers are finding success exploiting weaknesses across businesses' supply chains as well as critical vulnerabilities like Log4Shell, PrintNightmare, and others. And with ransomware-as-a-service available on the darkweb, more and more criminals are turning to ransomware, realizing that the odds of receiving a big payday are high."

The tactics and scope of ransomware attacks have been steadily evolving, but the end goal continues to be a disruption of the target organization and theft of sensitive information for the purposes of ransom. The size of the ransom often depends on the number of systems infected and the value of the data stolen: the higher the stakes, the higher the payment. In 2019, many ransomware groups updated their tactics to include data exfiltration, commonly referred to as a 'double extortion' ransomware. A year later, select groups added another attack layer with distributed denial of service (DDoS) tactics that bombard the victim's website or network, creating more business disruption, thus pressuring the victim to negotiate.

This year, the most dangerous ransomware trend involves supply chain attacks that target a supplier's business and use established connections and shared files, networks, or solutions for second-stage attacks on that supplier's customers. ThreatLabz also noted nearly a 120 percent increase in double-extortion ransomware victims based on data published on threat actors' data leak sites.

For the second year in a row, manufacturing companies were the most targeted with nearly one in five ransomware attacks directed at manufacturers. However, attacks on other sectors are rapidly growing. The growth rate of attacks on healthcare companies was particularly striking, with double-extortion attacks growing by nearly 650 percent when compared to 2021. This was followed by the restaurants and food services industry, which saw over a 450 percent spike in ransomware.

As governments across the world have started to take ransomware seriously, many threat groups have disbanded and reformed under new names. For example, DarkSide rebranded as BlackMatter, DoppelPaymer rebranded as Grief, and Rook rebranded as Pandora. However, their threat has not diminished even as their tactics have changed. Instead, many are now offering their tools for sale on the dark web, increasing their scale through a ransomware-as-a-service business model.

Earlier this year, the United States issued a statement warning of the potential for malicious cyber conduct against the United States as a response to economic sanctions against Russia. The statement urged immediate action to harden cyber defenses among both public and private sector organizations. Additional nations that are standing with Ukraine delivered similar warnings. To date, ThreatLabz has identified multiple attacks, such as the use of PartyTicket ransomware and the HermeticWiper malware against Ukraine, and attacks from the Conti threat group against multiple government entities. ThreatLabz is continuing to monitor for geopolitical attacks.

Desai added, "to minimize the chances of being breached and the damage that a successful ransomware attack can cause, organizations must use defense-in-depth strategies that include reducing the attack surface, adopting zero trust architecture that can enforce least-privilege access control, and continuously monitoring and inspecting data across all environments."

Organizations trying to mitigate ongoing risks from ransomware and double- or triple-extortion attacks should consider the following seven key prevention measures that can increase long-term network inviolability.

How the Zscaler Zero Trust Exchange Can Prevent Ransomware Attacks
The Zscaler Zero Trust Exchange incorporates ransomware prevention controls into a holistic zero trust architecture that disrupts every stage of attacks and minimizes damages. The following best practices and advanced capabilities can significantly reduce the risk of a ransomware attack.

- **Preventing compromise with consistent security policies:** With full SSL inspection at scale, browser isolation, inline sandboxing, and policy-driven access control to prevent access to malicious websites.
- **Eliminating lateral movement by removing applications from the internet and implementing a zero trust network access (ZTNA) architecture:** By connecting users directly to apps, not the network, to limit the blast radius of an attack.
- **Shutting down compromised users and insider threats:** By combining inline application inspection and integrated deception capabilities to detect and trick, and stop would-be attackers.
- **Stopping data loss:** By keeping software and training up-to-date, as well as deploying inline data loss prevention and inspecting data both in motion and at rest will prevent theft by threat actors.

For more details on how to protect against ransomware and threats, and how to develop a ransomware response plan, read the 2022 ThreatLabz State of Ransomware Report.

Methodology
The ThreatLabz team evaluated data from the Zscaler Zero Trust Exchange, which secures over 200 billion transactions and blocks 150 million threats daily across the globe. ThreatLabz analyzed a year's worth of global ransomware data from the Zscaler cloud, along with intelligence from external sources, from February 2021 through March 2022 to identify key trends, industries, and geographies at risk, and emerging tactics.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange 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 inline cloud security platform.

Media Contacts
Natalia Wodecki
Global PR Director
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/5314be11-c032-49f1-a03a-2ed7fad90ad0