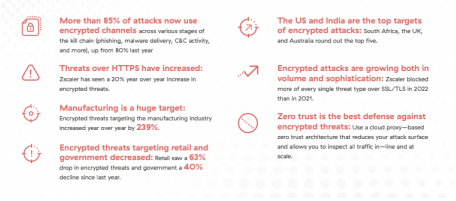
Zscaler Study Finds More Than 85% of Attacks Now Use Encrypted Channels, with Malware Topping Attacks in 2022

December 14, 2022

Annual State of Encrypted Attacks Report Finds Security Threats are Growing in Volume 20% Year over Year, Stressing the Need for Zero Trust Architecture

- More than 85% of attacks now use encrypted channels across various stages of the kill chain, up 20% from last year.
- Nearly 90% of all cyberthreats that affect users and organizations come from malware that downloads a malicious payload via a link shared in an email or infected websites.
- The U.S. and India are top targets for encrypted attacks. South Africa, the UK and Australia round out the top five.
- Encrypted threats targeting the manufacturing and education industry increased by 239% and 134%, respectively; conversely, retail saw a 63% and government a 40% decline

The State of Encrypted Attacks 2022 Report



Highlights of the 2022 State of Encrypted Attacks Report

SAN JOSE, Calif., Dec. 14, 2022 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced the release of its annual State of Encrypted Attacks Report, which details the analysis of more than 24 billion threats from October 2021 through September 2022 to track trends of HTTPS-based attacks. The research leveraged insights from more than 300 trillion daily signals and 270 billion daily transactions in the Zscaler Zero Trust Exchange™ — the world's largest security cloud.

The report uncovered that malware continues to pose the greatest threat to individuals and businesses across nine key industries, with manufacturing, education and healthcare being the most commonly targeted. Encrypted attacks remain a significant problem for countries around the globe, with the U.S., India and Japan seeing the biggest increases in attacks over the last 12 months. In addition, South Africa has seen a notable increase in TLS/SSL attacks compared to 2021.

"As organizations mature their cyber defenses, adversaries are becoming more sophisticated, particularly in their use of evasive tactics," said Deepen Desai, CISO and VP of Security Research and Operations at Zscaler. "Potential threats continue to hide in encrypted traffic, empowered by as-a-service models that dramatically reduce the technical barriers to doing so. It is critical for organizations to adopt a cloud-native zero trust architecture that allows consistent inspection of all internet bound traffic and effectively mitigate these attacks."

Malware is king among cybercriminals
While cybercriminals hide a variety of attack tactics in encrypted traffic, malware continues to be the most prevalent. Malicious scripts and payloads used throughout the attack sequence make up nearly 90% of the encrypted attack tactics blocked in 2022. This category includes ransomware, which remains a top concern for CISOs as ransomware attacks have increased 80% year over year.

As defenses become more complex, attackers have also continued to evolve their techniques, creating new malware variants that are harder to spot and able to bypass reputation-based technologies. The most prevalent malware families the Zscaler ThreatLabz team observed abusing encrypted channels include ChromeLoader, Gamaredon, AdLoad, SolarMarker, and Manuscrypt.

Usual suspects make way for a newcomer
The five countries most targeted by encrypted attacks include the U.S., India, South Africa, the UK and Australia. South Africa is a relative newcomer to the list, soaring to the top in 2022 after bumping France from its 2021 top-five ranking. Japan (613%), the U.S. (155%) and India (87%) also saw a significant uptick in targets year over year.

Manufacturing and education continue to produce the biggest risk
Not all industries are targeted by encrypted attacks at the same rate, with businesses deploying legacy security solutions often falling victim more often than others. This year, the manufacturing industry saw a 239% increase in these types of attacks, displacing technology as the most targeted type of business in 2022. Manufacturing remains an attractive target for cybercriminals because of significant transformation occurring across the industry in recent years, including the adoption of new safety measures to manage COVID-19, and infrastructure and applications to counteract supply chain issues. However, adopting new applications, products and services have increased the attack surface for manufacturing businesses, leaving many open to new vulnerabilities that must be addressed in the future.

The next closest industry to see the largest jump in attacks was education, with a 132% increase year over year. Education remains a notable target for the second year in a row, with a 50% increase in attacks from 2020 to 2021. Industries like education and manufacturing benefit most from zero trust architecture, which enables inspection of all internet bound traffic to identify suspicious activity and mitigate the growing risk of encrypted attacks.

On a positive note, in 2022, attacks against government organizations and retail decreased by 40% and 63%, respectively. Retail endured a major spike in encrypted attacks in 2021 as attackers took advantage of pandemic-driven e-commerce trends, but these have normalized in the past year. Law enforcement agencies across the world have actively pursued cybercriminals targeting these critical industries, making them less attractive targets for hacking groups looking for easy money.

Zscaler secures organizations against encrypted attacks at scale

Zscaler blocked 24 billion threats in 2022 — a 20% increase from the 20.7 billion blocked in 2021, which was a 314% increase from 2020. This shows that cybercriminals are continuing to evolve their tactics to avoid detection and slip past information security teams. Today, most attacks leverage SSL or TLS encryption, which is resource intensive to inspect at scale, and best done using a cloud native proxy architecture. While legacy firewalls support packet filtering and stateful inspection, their resource limitations make them poorly suited for this task. This creates a critical need for organizations to implement cloud native architectures that support full inspection of encrypted traffic in alignment with zero trust principles.

Businesses looking to minimize the risk of encrypted attacks should consider these recommendations as part of their adoption strategy:

- Use a cloud native, proxy-based architecture to decrypt, detect and prevent threats in all encrypted traffic at scale.
- Leverage an AI-driven sandbox to quarantine unknown attacks and stop patient zero malware.
- Inspect all traffic, all the time, whether a user is at home, at headquarters or on the go, to ensure everyone is consistently protected against encrypted threats.
- Terminate every connection to allow an inline proxy architecture to inspect all traffic, including encrypted traffic, in real-time — before it reaches its destination — to prevent ransomware, malware and more
- Protect data using granular context-based policies, verifying access requests and rights based on context.
- Eliminate the attack surface by connecting users directly to the apps and resources they need, never to networks.

To download the full report, see the 2022 State of Encrypted Attacks Report.

Methodology
Analysis of 24 billion blocked threats from October 2021 to September 2022 in the Zscaler cloud shows that all blocked threats came via encrypted channels, SSL and TLS.

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 Contact:
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at:
https://www.globenewswire.com/NewsRoom/AttachmentNg/ca90e676-bbd4-45de-9cd9-42c48b4cff3a