Zscaler's 2021 Encrypted Attacks Report Reveals 314 Percent Spike in HTTPS Threats

October 28, 2021

Massive Increase in Cyber Attacks Targeting Technology and Retail Industries Confirms Immediate Need for Zero Trust Security

Key findings

- Threats over HTTPS have increased more than 314 percent year-over-year, exceeding 250% growth for the second straight year.
- Attacks on tech companies increased by 2,300 percent year-over-year; attacks on retail and wholesale companies increased by 800 percent.
- Healthcare and government attacks saw a decrease in attacks year-over-year.
- The UK, U.S., India, Australia, and France are the top five targets of encrypted attacks.
- Malware is up 212 percent, and phishing is up 90 percent, whereas cryptomining attacks are down 20 percent.

SAN JOSE, Oct. 28, 2021 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced the release of its annual State of Encrypted Attacks Report, which tracked and analyzed over **20 billion threats** blocked over HTTPS, a protocol originally designed for secure communication over networks. This year's study found an increase of more than 314 percent year-over-year across geographical areas that include APAC, Europe, and North America, underscoring the need for a zero trust security model and greater traffic inspection than most companies can achieve with legacy firewall-based security models.

Zscaler's Zero Trust Exchange analyzes more than **190 billion daily transactions**, extracting over **300 trillion signals** which provides unmatched visibility to enterprise data at scale. ThreatlabZ research team leveraged these large data sets to provide unique insights into security risks posed by encrypted channels across key industries. Seven of the industries in the study experienced higher attack rates from threats in SSL and TLS traffic, while last year's most-targeted industry, healthcare, saw a decrease of 27 percent since January 2021. Conversely, the technology industry was plagued by threats at a rate much higher than other types of businesses, accounting for 50 percent of attacks.

In today's enterprise, more than 80 percent of internet-bound traffic is encrypted, which means that enterprises face the unique challenge of enforcing consistent security for all of their remote users. Cybercriminals are increasingly sophisticated in their tactics, and they're using encrypted channels at various stages of malware and ransomware attacks.

"Most enterprise IT and security teams recognize this reality but often struggle to implement SSL/TLS inspection policies due to a lack of compute resources and/or privacy concerns," said Deepen Desai, CISO and VP Security Research and Operations at Zscaler. "As a result, encrypted channels create a significant blind spot in their security postures. Zscaler's new report on the state of encrypted attacks demonstrates that the most effective way to prevent encrypted attacks is with a scalable, cloud-based proxy architecture to inspect all encrypted traffic, which is essential to a holistic zero trust security strategy."

Cybercrime at an all-time high
Between January 2021 and September 2021, Zscaler blocked more than 20 billion threats over HTTPS, increasing more than 314 percent from the previous year. Cybercriminals are getting increasingly savvy with their attacks and have benefited from affiliated networks and malware-as-a-service tools available on the dark web.

While cybercriminals can use various attack types to hide in encrypted traffic, malicious content represented a staggering 91 percent of attacks, a 212 percent increase over last year. In contrast, cryptomining malware is down 20 percent, reflecting a broader shift in the attack trends, with ransomware becoming a more lucrative option.

Tech industry under siege
The report found that attacks on tech, retail, and wholesale companies saw a significant increase in threats. Attacks on technology companies increased by a staggering 2,300 percent, and retail and wholesale saw attacks increase by over 800 percent. As more retailers offer digital shopping options during the 2021 holiday shopping season, cybercriminals are expected to be targeting more ecommerce solutions and digital payment platforms with malware and ransomware attacks. This has been exacerbated by the sudden need to support remote workers with remote connectivity to teleconferencing, SaaS-based apps, and public cloud workloads.

Tech companies are also an attractive target due to their role in the supply chain. A successful supply-chain attack like Kaseya and SolarWinds can give attackers access to a trove of user information. Additionally, as the world begins its return to normal, and as businesses and public events are opening up around the globe, many employees are still working in relatively insecure environments. Getting access to critical point-of-sale systems is extremely attractive to cybercriminals as it opens the door to huge profits.

Critical services see a decline
After being a top target in 2020, attacks on healthcare organizations decreased by 27 percent in 2021. Similarly, attacks on government organizations decreased by 10 percent. Ransomware attacks that targeted critical services, including the Colonial Pipeline attack and the ransomware attack on the Health Services Executive of Ireland, have caught the attention of the highest levels of law enforcement, including the White House, which recently signed an Executive Order to improve the nation's cybersecurity.

"After being the two most frequently targeted sectors in 2020, healthcare and government organizations had an immense sense of urgency to revamp their security postures with modern architectures, which are largely based on zero trust. There was also increased government scrutiny and a law

enforcement crackdown on cybercriminal groups in response to high-profile attacks against critical services such as Colonial Pipeline," said Desai. "As a result of these two factors, we have seen a decrease in attacks on healthcare and government organizations this year."

More countries targeted
Zscaler ThreatLabz observed attacks in over 200 countries and territories worldwide, including small countries that are not common targets such as islands across the Caribbean. In addition, an increase in work-from-anywhere has led to employees branching out from the usual giant tech hubs like, the San Francisco Bay Area, New York, London, Paris, Sydney.

The five most-targeted countries of encrypted attacks include the U.K. (5,446,549,767), U.S. (2,674,879,625), India (2,169,135,553), Australia (1,806,003,182), and France (519,251,819).

As a whole, Europe led the way with 7,234,747,361 attacks, with APAC (4,924,732,36) and North America (2,778,360,051) rounding out the top three.

Protect your business
As organizations shift to support new, digitally enabled working models, it's increasingly important to ensure that their assets and traffic to those assets are secure. To lower the threat from encrypted attacks, Zscaler ThreatLabz recommends a zero trust security strategy that allows organizations to:

- **Prevent Compromise:** Provide consistent security for all users and all locations to ensure everyone has the same level of security all the time, whether they are at home, at headquarters, or abroad. Use a cloud-native, proxy-based architecture to inspect all traffic for every user and decrypt, detect, and prevent threats that may be hiding in HTTPS traffic.
- **Prevent Lateral Movement:** Use zero trust architecture with deception to reduce your attack surface and prevent lateral movement by cybercriminals. This type of architecture makes applications invisible to attackers while allowing authorized users to directly access needed resources and not the entire network.
- **Prevent Data Loss:** Quarantine unknown attacks or compromised apps in an AI-driven sandbox to stop patient-zero malware and ransomware. Unlike with firewall-based passthrough approaches, this design holds all suspicious content for analysis, ensuring that breach attempts are stopped before they are able to access sensitive systems and steal business-critical information.

To download the full report, see the 2021 State of Encrypted Attacks.

Methodology
The ThreatLabz team evaluated data from the Zscaler security cloud, which monitors over 190 billion transactions daily across the globe. Zscaler blocked over 20.7 billion threats transmitted via encrypted channels over a nine-month window from January 2021 through September 2021.

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 SASE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

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