Zscaler Releases Semi-Annual Cloud Security Insights Report

February 27, 2019

Leader in Cloud Security Reveals 400% Increase in Phishing Attacks in 2018

SAN JOSE, Calif.--(BUSINESS WIRE)--Feb. 27, 2019-- Zscaler, Inc., the leader in cloud security, announced today the release of its semi-annual 2019 Cloud Security Insights Threat Report – An Analysis of SSL/TLS-based Threats, which examines encrypted traffic across the Zscaler™ cloud from July through December 2018. The report, compiled by the Zscaler™ ThreatLabZ research team, delves into a variety of attacks executed over SSL and blocked by Zscaler, including phishing attacks, botnets, browser exploitation, and malicious content.

As the use of SSL grows to the point where it's the standard protocol, cybercriminals are increasingly using encryption to conceal and launch attacks. This has become possible because SSL certificates, which used to be difficult to obtain, are now readily available at no charge.

"With the ever-increasing concerns over data privacy, there has been a massive trend toward Internet properties having encryption by default. This is a great thing for privacy, but it presents a challenge to IT security. Decrypting, inspecting, and re-encrypting traffic is nontrivial, causing significant performance degradation on traditional security appliances, and most organizations are not equipped to inspect encrypted traffic at scale," said Amit Sinha, Executive Vice President of Engineering and Cloud Operations, Chief Technology Officer, Zscaler. "With a high percentage of threats now delivered with SSL encryption, and over 80 percent of Internet traffic now encrypted, enterprises are blind to over half of malware sent to their employees. The Zscaler™ cloud platform enables "man-in-the-middle" SSL inspection at scale, so it can inspect SSL traffic without latency and capacity limitations and provide customers with protection against the growing number of threats attempting to hide behind encryption."

During the study period, Zscaler blocked **1.7 billion threats** hidden in SSL traffic, which translates to an average of 283 million advanced threats blocked per month.

Key Research Highlights:

- **Phishing:** On average, the Zscaler™ cloud platform blocked 2.7 million phishing attacks over encrypted channels per month in 2018. This represents an increase of more than 400 percent when compared to SSL-based phishing attacks blocked in 2017.
- **Malicious Content:** An average of 32 million botnet callback attempts were blocked by the Zscaler™ cloud platform every month in 2018.
- **Browser Exploitation:** The Zscaler™ cloud platform blocked an average of 240,000 browser exploitation attempts per month in 2018.
- **Newly Registered Domains:** Nearly 32 percent of newly registered domains that were blocked by the Zscaler™ cloud platform were using SSL encryption.

"One of the most notable SSL threat trends that we saw in 2018 was the increase in JavaScript skimmer-based attacks. These attacks start with the e-commerce sites being compromised and injected with malicious, obfuscated JavaScript, which, in turn, tries to tap into purchase transactions," said Deepen Desai, Vice President of Security Research, Zscaler. "With the increase in JavaScript skimmer-based attacks, criminals can conduct their nefarious activity within the confines of the SSL environment, leaving most e-commerce sites unaware of the activity."

As the world's largest security platform built for the cloud , Zscaler processes, on average, more that 60 billion transactions per day. With nearly 80 percent of that traffic encrypted, the Zscaler™ cloud blocks an average of 9.5 million SSL-based advanced threats every day.

About Zscaler

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100 percent cloud-delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant distributed cloud security platform, protecting thousands of customers from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.

Zscaler™, Zscaler Internet Access™, and Zscaler Private Access™, ZIA™ and ZPA™ are either (i) registered trademarks or service marks o trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

View source version on businesswire.com: https://www.businesswire.com/news/home/20190227005219/en/

Source: Zscaler, Inc.

Danielle Ostrovsky
Zscaler PR Manager
410-302-9459