Based Threats on the Rise in 2017

As the use of SSL/TLS encryption increases, so has the use of SSL to deliver malicious content.

In 2017, an average of 60% of traffic in the Zscaler cloud has been SSL/TLS encrypted.

Malicious content being delivered over SSL/TLS has more than doubled in the last six months.

60%

Malicious content delivered over SSL/TLS

The Zscaler cloud blocks an average of 8.4 million* requests in SSL/TLS-based traffic daily, 600,000 of those contain advanced threats.

The Zscaler cloud has blocked an average of 12,000 phishing attempts per day delivered over SSL/TLS, a 400% increase over 2016.

The most prevalent malware family leveraging SSL-based callbacks was Dridex/Emotet, which contributed 34% of the total unique, new payloads in 2017.

– Deepen Desai, Senior Director, Security Research

New Malicious payloads leveraging SSL/TLS for C&C activity

Banking Trojans (Zbot, Vawtrak, Tickbot, etc) 60%
Ransomware families 25%
Infostealer Trojan families 12%
Other 03%

Zscaler protects thousands of organizations with 100% cloud-based security that inspects all traffic, including SSL-encrypted traffic, without adding latency. zscaler.com

*Number based on a sample of Zscaler customers using the SSL inspection feature. Research is based on traffic observed in the Zscaler cloud between January 1 and June 30, 2017. Research © 2017 ThreatlabZ, the research division of Zscaler, Inc. All rights reserved. Zscaler™ is a trademark or registered trademark of Zscaler, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners.