Zscaler ThreatLabZ Reveals Malicious Content Delivered Over SSL/TLS Has More Than Doubled in Six Months

August 2, 2017

Researchers Share Latest Findings from the Zscaler Cloud Showing Increasingly Sophisticated Malware Strains Using SSL to Encrypt Activity

SAN JOSE, CA--(Marketwired - Aug 2, 2017) - Zscaler, Inc., the leading cloud security company, today announced the findings of a study from Zscaler™ ThreatLabZ showing that malicious threats using SSL encryption are on the rise in 2017. According to the study, an average of 60 percent of the transactions in the Zscaler cloud, the largest security cloud, have been delivered over SSL/TLS. Researchers also found that the Zscaler cloud saw an average of 8.4 million* SSL/TLS-based security blocks per day this year.

"Hackers are increasingly using SSL to conceal device infections, shroud data exfiltration and hide botnet command and control communications. In fact, our study found that the amount of phishing attempts per day delivered over SSL/TLS has increased 400 percent from 2016," said Deepen Desai, senior director, security research and operations. "SSL inspection is a necessity in ensuring the security of network traffic in the enterprise. Zscaler sits between users and the internet, inspecting every byte of traffic, including encrypted traffic, so we can catch hidden threats before they get into the network."

ThreatLabZ researchers also identified new malicious payload distributions, based off unique payloads hitting the Zscaler Cloud Sandbox, leveraging SSL/TLS for command and control (C&C) activity. Banking Trojans comprised 60 percent of the payloads, including families like Dridex, Zbot, Vawtrak and Trickbot, while 25 percent were comprised of multiple ransomware families. Less popular payloads included Infostealer Trojan families and other miscellaneous families.

Additional findings include:

- The amount of malicious content being delivered over SSL/TLS has more than doubled in the last six months.
- The Zscaler cloud blocked an average of 12,000 phishing attempts per day delivered over SSL/TLS -- an increase of 400 percent from 2016.
- New, increasingly sophisticated malware strains use SSL to encrypt their C&C mechanisms.
- Zscaler saw an average of 300 hits per day for web exploits that included SSL as part of the infection chain.
- The most prevalent malware family leveraging SSL-based callbacks was Dridex/Emotet, which contributed 34 percent of the total unique, new payloads in 2017.
- New malicious payloads leveraging SSL/TLS for C&C activity:
  -- 60 percent were comprised of multiple Banking Trojan families (Zbot, Vawtrak, Trickbot, etc.)
  -- 25 percent were comprised of ransomware families
  -- 12 percent were comprised of Infostealer Trojan families (Fareit, Papras, etc.)
  -- 3 percent were from other miscellaneous families

*Number based on sample of Zscaler customers using the SSL inspection feature.
To access an infographic with all the findings, click here.

Additional resources:

- Zscaler SSL Inspection
- Webcast: Are Your Appliance-Based Security Solutions Ready for 2018-bit SSL Certificates?

About Zscaler
Zscaler 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 the world's largest cloud security platform, protecting thousands of enterprises and government agencies from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.

Media Contact:
Whitney Glockner Black
Director of Communications
650-260-4616
wblack@zscaler.com