SSL-encrypted traffic on the rise

Up to 80% of internet traffic is SSL encrypted.

260% Increase in SSL threat volume
30% Of SSL threats start from cloud-based file-sharing services
500% Increase in ransomware over SSL

Cybercriminals are not making any ethical exceptions, even during the COVID pandemic, as they continue to indiscriminately target the healthcare industry with advanced threats over encrypted channels.

Cybercriminals capitalize on COVID-19
Healthcare industry takes the brunt of SSL-encrypted threats

Advanced threats blocked over TLS/SSL from top cloud storage services

Hackers abuse file-sharing services
Steady growth of attacks aimed at Google Drive, OneDrive, AWS, and Dropbox

Misspellings can be costly
Domain squatting and homograph attacks dominate SSL threat landscape

Corporate brands and functions most frequently phished

Microsoft: 36%
Tech Support: 17%
PayPal: 12%
Google: 10%
OneDrive: 10%

Zscaler’s global threat research team, ThreatLabZ, analyzed more than 6.6 billion sessions for its annual “State of Encrypted Attacks” report. Threats hidden in SSL-encrypted traffic are on the rise, and security teams must recognize that encrypted traffic does not mean safe traffic any more. As this attack vector grows, so does the need to inspect all SSL traffic.