2020 State of Encrypted Attacks

No SSL Inspection, No Threat Protection
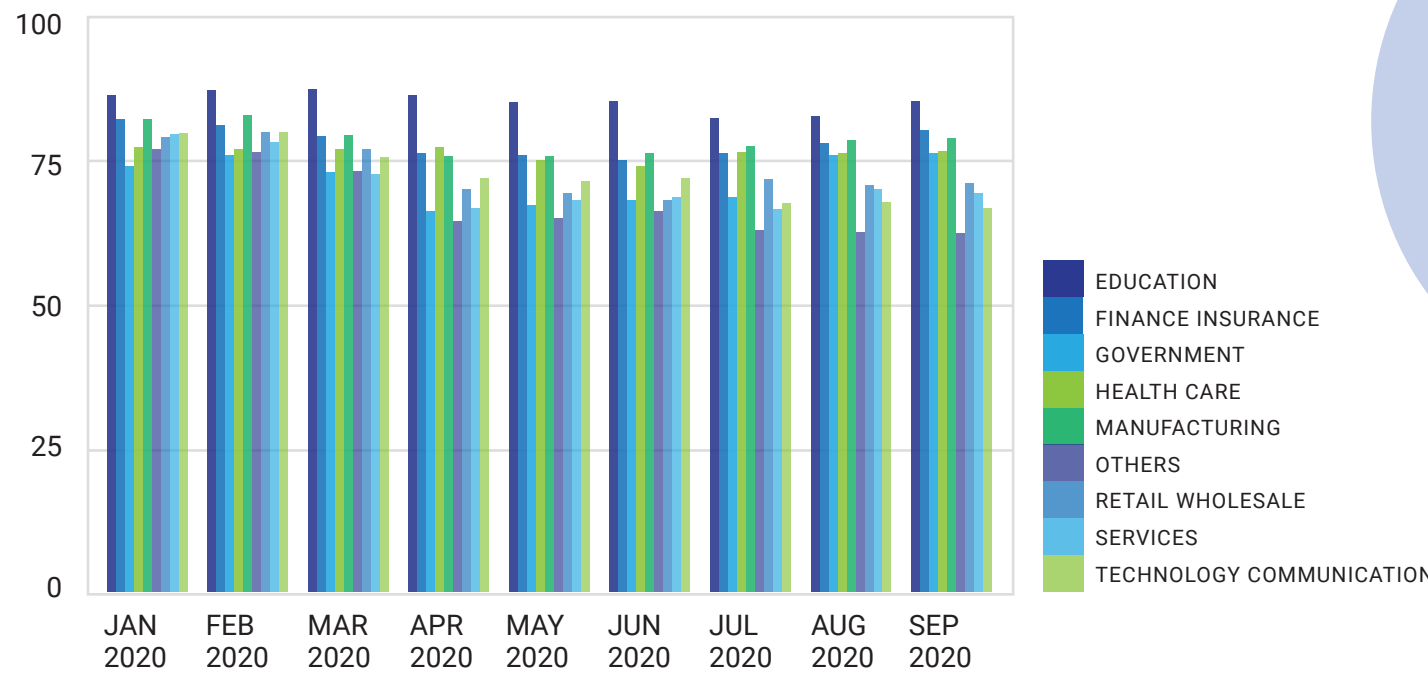
Zscaler's ThreatLabZ team analyzed threats delivered over encrypted internet traffic in 2020.

Read the Report

SSL-encrypted traffic on the rise
Up to 80% of internet traffic is SSL encrypted

Percentage of encrypted traffic across industry verticals

Legend:
- EDUCATION
- FINANCE INSURANCE
- GOVERNMENT
- HEALTH CARE
- MANUFACTURING
- OTHERS
- RETAIL WHOLESALE
- SERVICES
- TECHNOLOGY COMMUNICATION

Months: JAN 2020, FEB 2020, MAR 2020, APR 2020, MAY 2020, JUN 2020, JUL 2020, AUG 2020, SEP 2020

SSL

260%
Increase in SSL threat volume

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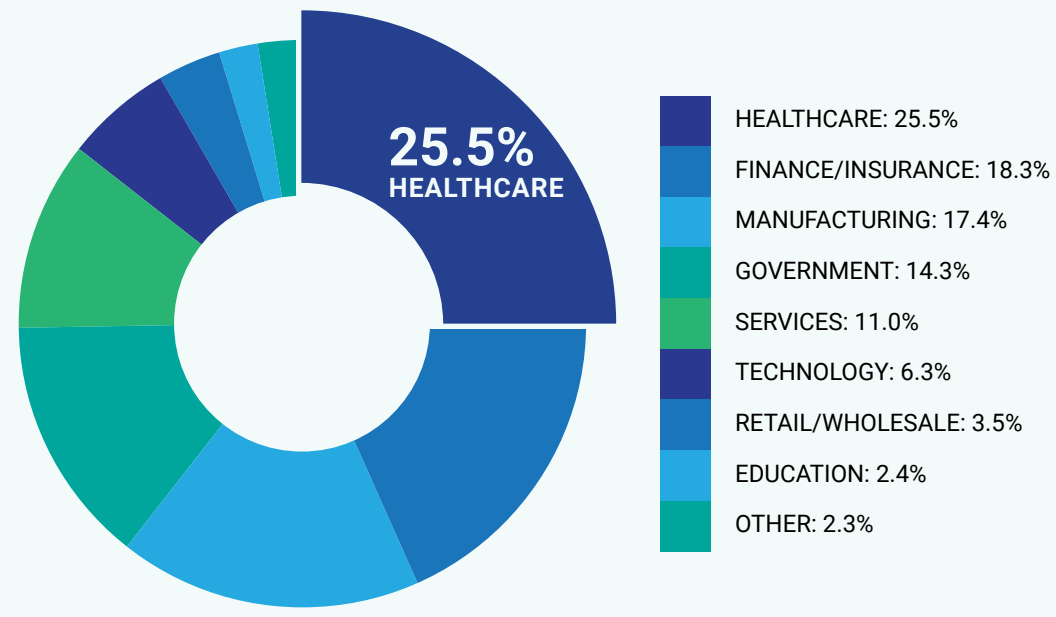
500%
Increase in ransomware over SSL

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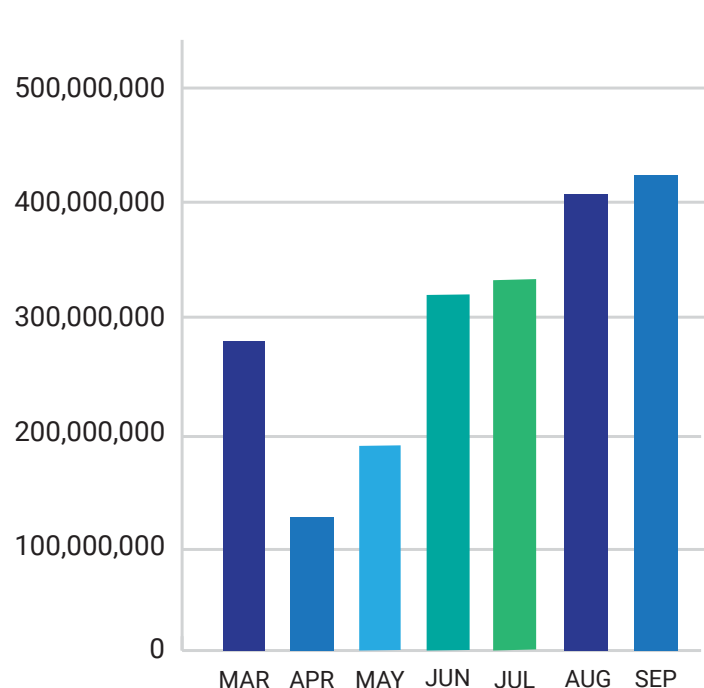
Cybercriminals capitalize on COVID-19
Healthcare industry takes the brunt of SSL-encrypted threats

Malware blocked over encrypted channels by industry

25.5% HEALTHCARE

- HEALTHCARE: 25.5%
- FINANCE/INSURANCE: 18.3%
- MANUFACTURING: 17.4%
- GOVERNMENT: 14.3%
- SERVICES: 11.0%
- TECHNOLOGY: 6.3%
- RETAIL/WHOLESALE: 3.5%
- EDUCATION: 2.4%
- OTHER: 2.3%

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

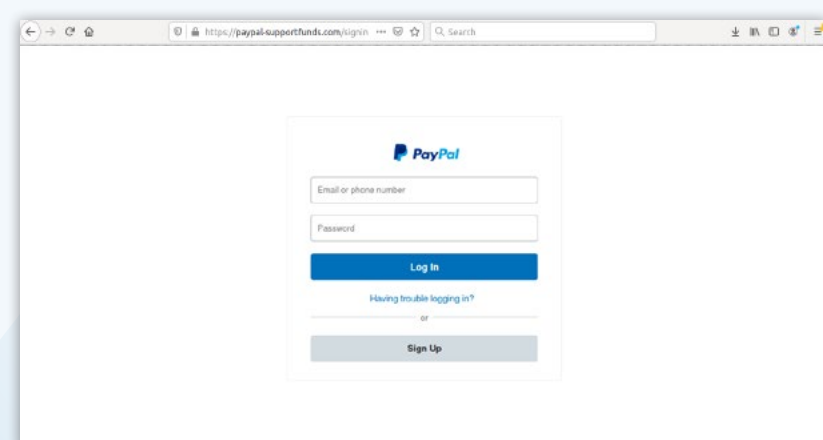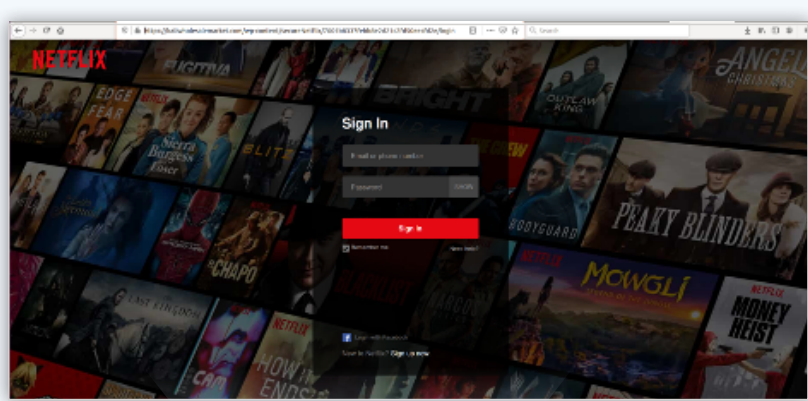Months: MAR, APR, MAY, JUN, JUL, AUG, SEP

Hackers abuse file-sharing services
Steady growth of attacks aimed at Google Drive, OneDrive, AWS, and Dropbox
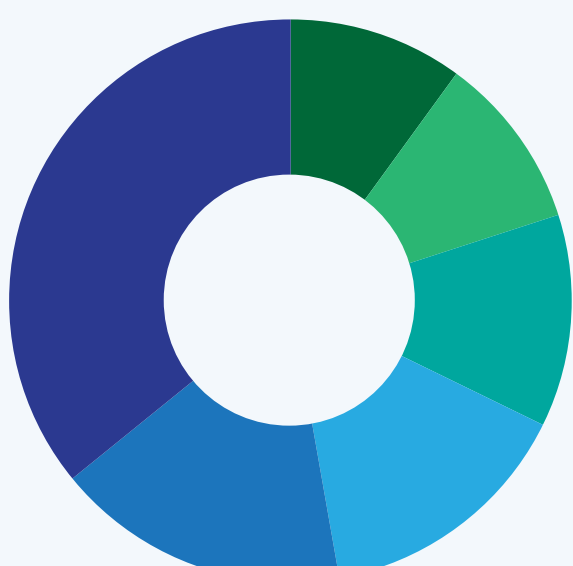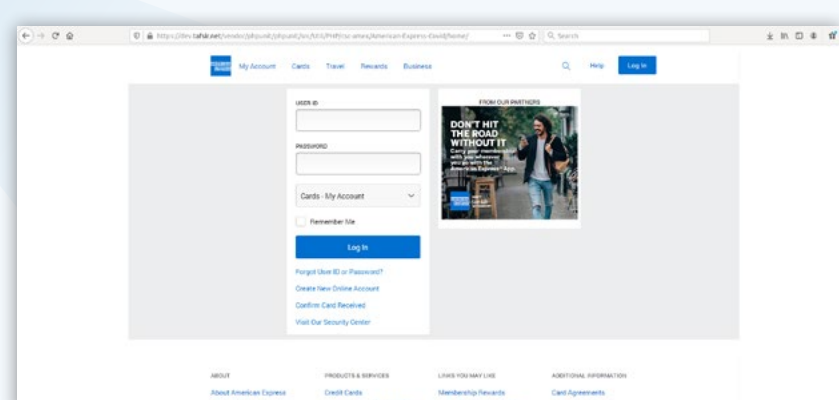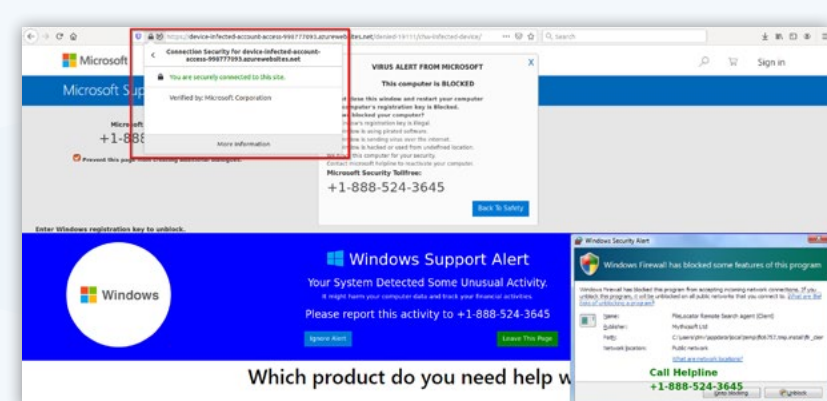
Misspellings can be costly
Domain squatting and homograph attacks dominate SSL threat landscape

These images are malicious replicas of legitimate webpages. Cybercriminals use popular brands to lure the unsuspecting user with a fake website to steal login credentials, PII, and financial information, and execute malware.

Corporate brands and functions most frequently phished

- Microsoft: 36%
- Tech Support: 17%
- PayPal: 15%
- Webmail: 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.

Read the Report

zscaler

zscaler.com