Zscaler ThreatLabz 2023 State of Encrypted Attacks Report

Encrypted Threat Check 2023

Did you know...

the vast majority (86%) of cyberthreats hide in 'safe' encrypted traffic?

Explore key insights from our Zscaler ThreatLabz 2023 State of Encrypted Attacks Report, which analyzed more than 29 billion blocked threats in the world's largest inline security cloud.

95% of web traffic is secured with HTTPS[1]. It's also where most malware, ransomware, and phishing attacks hide.

24.3%
growth in encrypted attacks, year over year

276.4% and **185%**
increase in attacks targeting education and government, respectively

1. Google Transparency Report.
2. Research collected September 2022–October 2023

The face of encrypted malware

78.1% of encrypted threats are driven by malware. These malware families represent the most common encrypted threats for 2023. Malware comes in many different forms, like malicious web content, infected websites, and email attachments, to name a few.

ChromeLoader
Persistent browser hijacker that modifies browser settings to show malicious advertisements and leak users' search queries.

Redline Stealer
Information stealer that leverages custom file-grabbers to pilfer a victim's sensitive data from web browsers, applications, emailing and messaging apps, and cryptocurrency wallets.

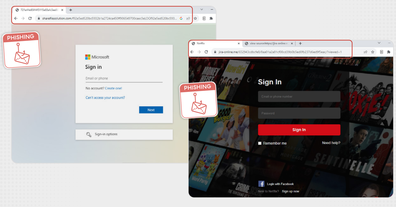
MedusaLocker
Ransomware strain delivered over email or software vulnerability that encrypts a victim's files and demands a ransom in exchange.

Nemucod
Trojan downloader that delivers malware by sending victims an email containing a zip file, which appears to come from a legitimate sender.

Phishing attacks grew by 13.7%

Phishing attacks targeting enterprise user credentials are on the rise. Many of the most common phishing attacks are linked to popular applications belonging to Microsoft, Adobe, Google, Facebook, Amazon, Netflix, and more.

Microsoft · OneDrive · SharePoint · Adobe · amazon · NETFLIX · facebook · Google · DHL · ebay



The hardest-hit industries and key trends

Manufacturing bears the brunt of encrypted attacks

31.6% of encrypted attacks targeted manufacturers, with an overall **25%** YoY growth in threats.

Education (276%) and government (185%) see sharp rise in attacks

As these sectors embrace connectivity and cloud transformation, their attack surface — and attractiveness to threat actors exploiting encryption — grows.

Browser exploits (297%) and ad spyware sites (290%) show massive growth

More attackers are using encrypted channels to exploit web browser vulnerabilities and distribute spyware.

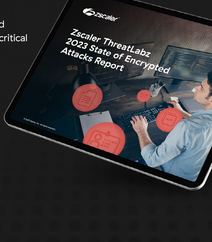
The U.S. and India are top targets for encrypted attacks

The U.S. **(53.3%)** and India **(27.7%)** also showed significant overall growth in encrypted attacks.

Best practices to secure your encrypted traffic

The volume and sophistication of attacks over encrypted SSL/TLS traffic will only grow — making it even more critical for enterprises to scan 100% of their encrypted traffic. To safeguard against these threats, enterprises should:

- Discover the internet-connected attack surface
- Implement an inline zero trust architecture
- Inspect 100% of encrypted SSL/TLS traffic
- Use microsegmentation to reduce application access



For full findings and best practices, download the Zscaler ThreatLabz 2023 State of Encrypted Attacks Report.

Get the Report

zscaler | Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com