INFOGRAPHIC

THE STATE OF

Encrypted Attacks

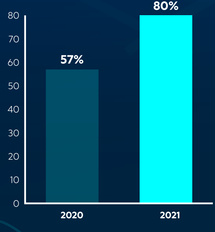
Just because data is encrypted doesn't mean it's safe.

A recent ThreatLabz study found that encrypted malware has increased dramatically year-over-year:

Zscaler blocked **314%** as many attacks over encrypted channels in 2021 vs 2020

More than **80%** of attacks now happen over encrypted channels, up from 57%

Percentage of Attacks on Encrypted Channels

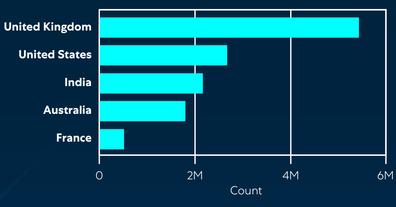


2,344%
increase on attacks against the tech industry

841%
increase on attacks against retail and wholesale

Attacks hit over **200** countries and territories, targeting tech hubs in particular

The five most-targeted countries of encrypted attacks



Most common encrypted attacks

- Malware
- Phishing
- Cryptomining
- Adspyware
- Botnets
- Browser Exploits

Stop encrypted threats with zero trust

Prevent compromise
Protect users, servers, workloads, and IoT/OT by minimizing the attack surface and inspecting all traffic.

Prevent lateral movement
Stop attackers from moving on your network to find high value targets.

Prevent data theft
Inspect all internet-bound data to prevent data loss to the internet and exploitation of unmanaged devices.

A cloud proxy-based zero trust architecture allows you to inspect all traffic at speed and at scale. Learn more stats about encrypted threats and how to defend against them: **Download the report.**

Read the report →

zscaler™