REPORT SUMMARY

2020 State of Encrypted Attacks

The Zscaler™ global threat research team, ThreatLabZ, analyzed more than 6.6 billion sessions from the industry's largest inline security cloud to provide comprehensive visibility into how adversaries are abusing encryption to bypass traditional security controls.

SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) protocols are used in the majority of web traffic to protect it from "eavesdropping" by those seeking to view private transmissions and steal data. Many websites use encryption (HTTPS) as their primary security measure.

Many people assume that encrypted traffic means safe traffic. But that false sense of security creates risk because it means that the majority of organizations allow encrypted traffic to go uninspected, and attackers know this. The problem is that most security teams can't fully inspect SSL traffic, as their legacy tools lack the processing power to decrypt, inspect, and re-encrypt packets without bringing performance to a standstill.

Our new report brings to light how attackers are escalating their abuse of encryption standards to deliver successful attacks. What were once relatively lightweight payloads on misspelled websites have evolved into advanced malware and ransomware delivered through domain squatting, brand phishing, and homograph attacks.

Hackers prey on people's trust of popular brands like Apple and Netflix

Attackers have rapidly increased registration of malicious domains, which contributed to the 260 percent increase in SSL-encrypted threats over the last nine months.

Cybercriminals use "domain squatting" and "homograph attacks" to imitate popular, legitimate web pages with pixel-perfect replicas. Their ultimate goal is obvious: prey on the trust of big brands to deliver malware and steal login credentials (such as banking information) and other sensitive personal information. For example, links to registered domains along the lines of *gmali.com* and *app1e.com* could be clicked on by someone not paying close attention and these sites can look nearly indistinguishable from the legitimate ones. And, as these domains leverage SSL/TLS encryption by default, they could easily bypass traditional security controls.

Key highlights:

- **Explosive growth in volume:** 260% increase in SSL-based threats in the last nine months.
- **SSL-based attacks delivered through trusted cloud providers:** Cybercriminals continue to become more sophisticated in avoiding detection, taking advantage of the reputations of trusted cloud providers such as Dropbox, Google, Microsoft, and Amazon to deliver malware over encrypted channels.
- **Hidden ransomware on the rise:** More than 500% increase in ransomware delivered over encrypted web traffic between March and September.
- **Preventing encrypted threats requires SSL inspection at scale:** Security and data protection systems that can't inspect 100% of traffic put enterprises at risk.

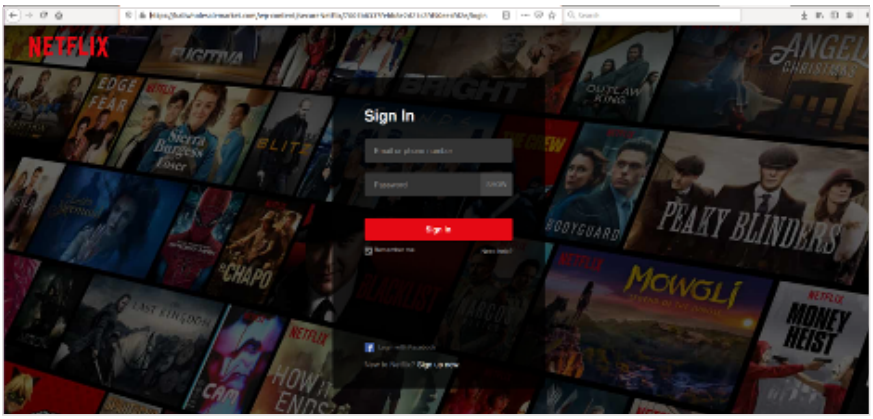

Figure 1: *Malicious site imitating the legitimate Netflix sign-in page.*

Attackers Abuse AWS, Google Drive, OneDrive, and Dropbox to deliver encrypted threats

Malicious content delivered with encryption from file-sharing services represented 30 percent of all malicious SSL traffic, almost doubling from March 2020.

Cloud-based file-sharing services are powerful tools for boosting employees' collaboration and productivity. These services securely share files and information, with the SSL-encrypted content generally bypassing security controls. While good for performance, bypassing security can open a backdoor into many enterprises.

Attacks can be initiated by creating file-sharing URLs to malicious content in services like Google Drive or Dropbox as part of an email phishing campaign. This approach removes the need to attach infected files to emails, which users have been trained to treat with suspicion. Because the content is hosted on a legitimate file-sharing site, it comes with a level of trust—and infected users can quickly spread the attack by sharing the link across the organization.

Encrypted ransomware attacks continue to rise

Five-hundred percent increase in the use of ransomware over encrypted channels since March 2020.

Ransomware, malware that encrypts a host's device or an organization's data or network, is used widely by cybercriminals. As the name suggests, the attacker's goal is to hold data hostage to extract payment. After successfully stealing and encrypting the organization's data, an attacker may threaten to leak the data if no payment is made. Ransomware attacks delivered over SSL-encrypted channels is the next evolution of this growing and highly destructive attack vector because it makes these attacks harder to detect.

Telecom companies and healthcare institutions have been hit the hardest because they tend to pay the ransoms due to the sensitive nature of their data. Ransomware families including FileCrypt/FileCoder variants, Sodinokibi, Maze, and Ryuk have been the most prevalent in our research.

Healthcare organizations bear the brunt of SSL-based attacks

While all industries were targeted, healthcare was the number-one impacted sector, receiving more than 25 percent of encrypted attacks.

Cybercriminals, showing no limits to their depravity, have increased their attacks on the healthcare sector during the pandemic using advanced threats over encrypted channels. Our research found that healthcare was targeted by 25.5 percent of SSL-encrypted threats. While costly, threats hidden in encryption can have even more dire consequences, particularly when they affect the delivery of healthcare.

What's needed to prevent encrypted threats

It's increasingly important to recognize that SSL traffic is not necessarily secure traffic. Just as the use of encryption has increased, so has its use among adversaries to hide their attacks. The need to inspect encrypted traffic is greater than ever.

- **Decrypt, detect, and prevent threats in all SSL traffic** with a proxy-based architecture and cloud-native performance.
- **Quarantine unknown attacks and stop patient-zero malware** with AI-driven quarantine that holds suspicious content for analysis, unlike firewall-based passthrough approaches.
- **Provide consistent security for all users and all locations** to ensure everyone has the same great security all the time, whether they are at home, at headquarters, or on the go.
- **Instantly reduce your attack surface** by starting from a position of zero trust, where lateral movement can't exist. Apps are invisible to attackers, and authorized users directly access needed resources, not the entire network.

Read the report for all the findings and an analysis of the growing threat inside SSL traffic.

Read the Report

About Zscaler

Zscaler accelerates digital transformation with its Zero Trust Exchange™, a SASE-based platform that provides fast, secure connections between users, devices, and applications over any network.

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