ThreatLabz 2024_Encrypted Attacks Report

Table_of Contents

Executive Summary_

Encryption is a cornerstone of cybersecurity, safeguarding sensitive data and ensuring privacy in our increasingly interconnected world. Unfortunately, it can also create blind spots that bad actors can abuse to launch and hide malicious activities. This is evident in the steady increase in encrypted attacks the Zscaler ThreatLabz team has observed in recent years, as cybercriminals take advantage of encryption to obfuscate malware and other malicious payloads, execute phishing scams, exfiltrate data, and more.

To shed light on these stealthy cyberthreats, ThreatLabz continuously analyzes encrypted data from the Zscaler Zero Trust Exchange™, which processes more than 500 billion transactions and 500 trillion signals every day.

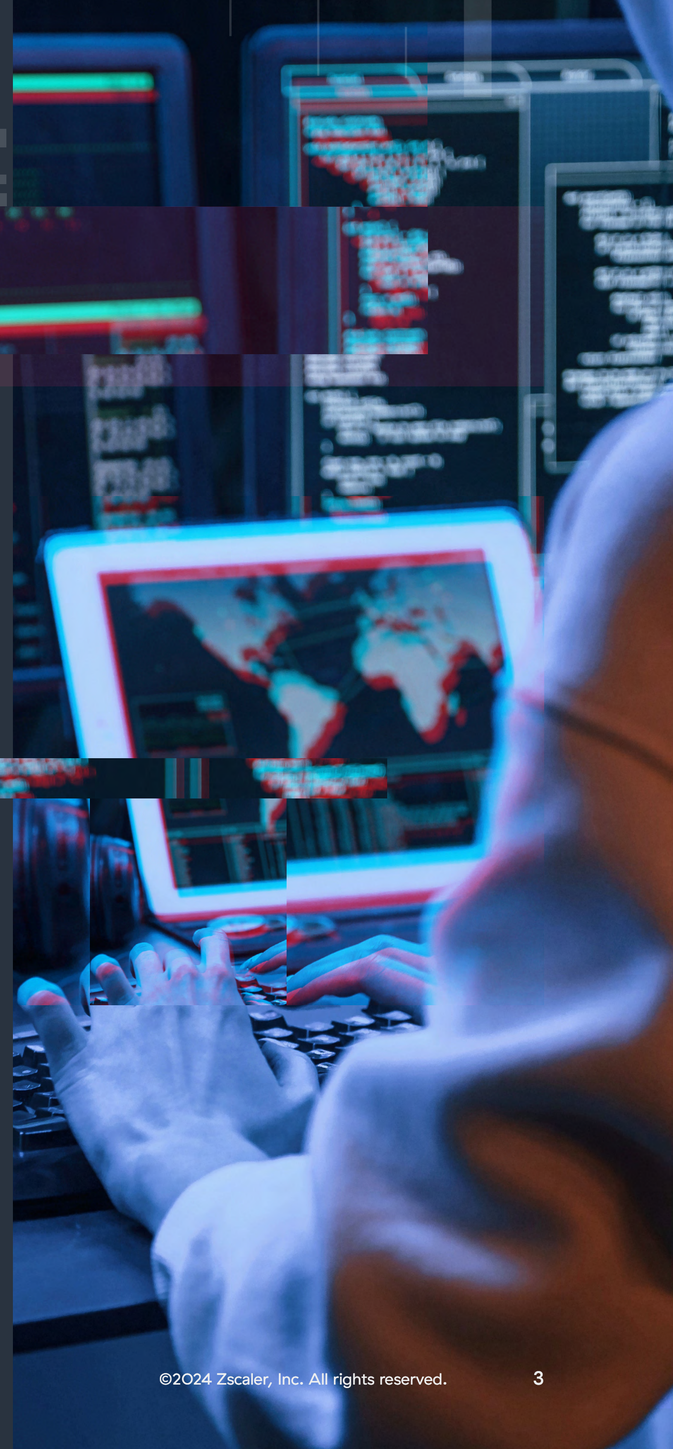
The Zscaler ThreatLabz 2024 Encrypted Attacks Report explores the latest data and provides critical insights into how encryption has become a conduit for more sophisticated threats, further compounded by the rise of artificial intelligence (AI).

Between October 2023 and September 2024, the Zscaler cloud blocked 32.1 billion attacks embedded in TLS/SSL–encrypted traffic. ThreatLabz found that this amounts to 87.2% of all threats, reflecting a consistent uptick in cybercriminals' use of encryption to sidestep security measures.

In 2024, malware remained a leading encrypted threat, accounting for 86.5% of blocked encrypted attacks, or 27.8 billion incidents, followed by ad spyware sites (2.9 billion) and phishing (921 million). These findings signal a broader shift toward the convergence of AI and encryption, reflective of AI's pervasive hand in today's cyberthreat landscape. The 34.1% growth in encrypted phishing since last year points to the use of generative AI by attackers to make their campaigns more deceptive and difficult to detect.

The escalation in encrypted threats spans all industries, though some are bearing a heavier load. Manufacturing remains the top–targeted industry in ThreatLabz analysis, with the retail & wholesale and education verticals seeing the highest increases in encrypted attacks compared to last year.

Given these rising risks, how can organizations stay protected? The key is comprehensive TLS/SSL traffic inspection to keep encrypted threats out of the enterprise. The challenge, however, lies in the sheer computational resources required to inspect encrypted traffic at scale, especially with traditional, hardware–based security tools. In addition to exploring the latest trends in encrypted threats, the ThreatLabz 2024 Encrypted Attacks Report offers achievable strategies and best practices to help organizations address this challenge and tackle these covert threats head–on.



Key_ Findings

Threats over HTTPS grew by 10.3% year-over-year in the Zscaler cloud, reflecting a steady rise in the volume and complexity of attacks using encrypted channels.

A substantial 87.2% of total threats are now delivered over encrypted channels, highlighting the critical need for full inspection of all internet and SaaS traffic.

Advanced persistent threat (APT) groups are increasingly abusing cloud services, like GitHub and Dropbox, and social platforms like LinkedIn and X, to deliver malware and steal data over encrypted channels.

Encrypted malware emerged as the leading threat, comprising 86.5% of observed attacks, with AsyncRAT being the most prevalent family, followed by ChromeLoader, and Atomic Stealer. Encrypted malware includes malicious web content, malware payloads, macro-based malware, etc.

Web-based cryptomining and cryptojacking increased a notable 122.9% year-over-year, driven primarily by CoinIMP, Kryptex, and XMRig, highlighting a concerning trend as unauthorized mining escalates alongside rising cryptocurrency values.

Phishing attacks over encrypted channels increased by 34.1%, fueled by the growing use of generative AI tools and the growing availability of phishing-as-a-service kits that include TLS certificates in their offerings.

Encrypted botnets have decreased in volume by 59.3% as command-and-control (C2) activity has become stealthier, pointing to a shift toward more covert, less noisy approaches within encrypted channels.

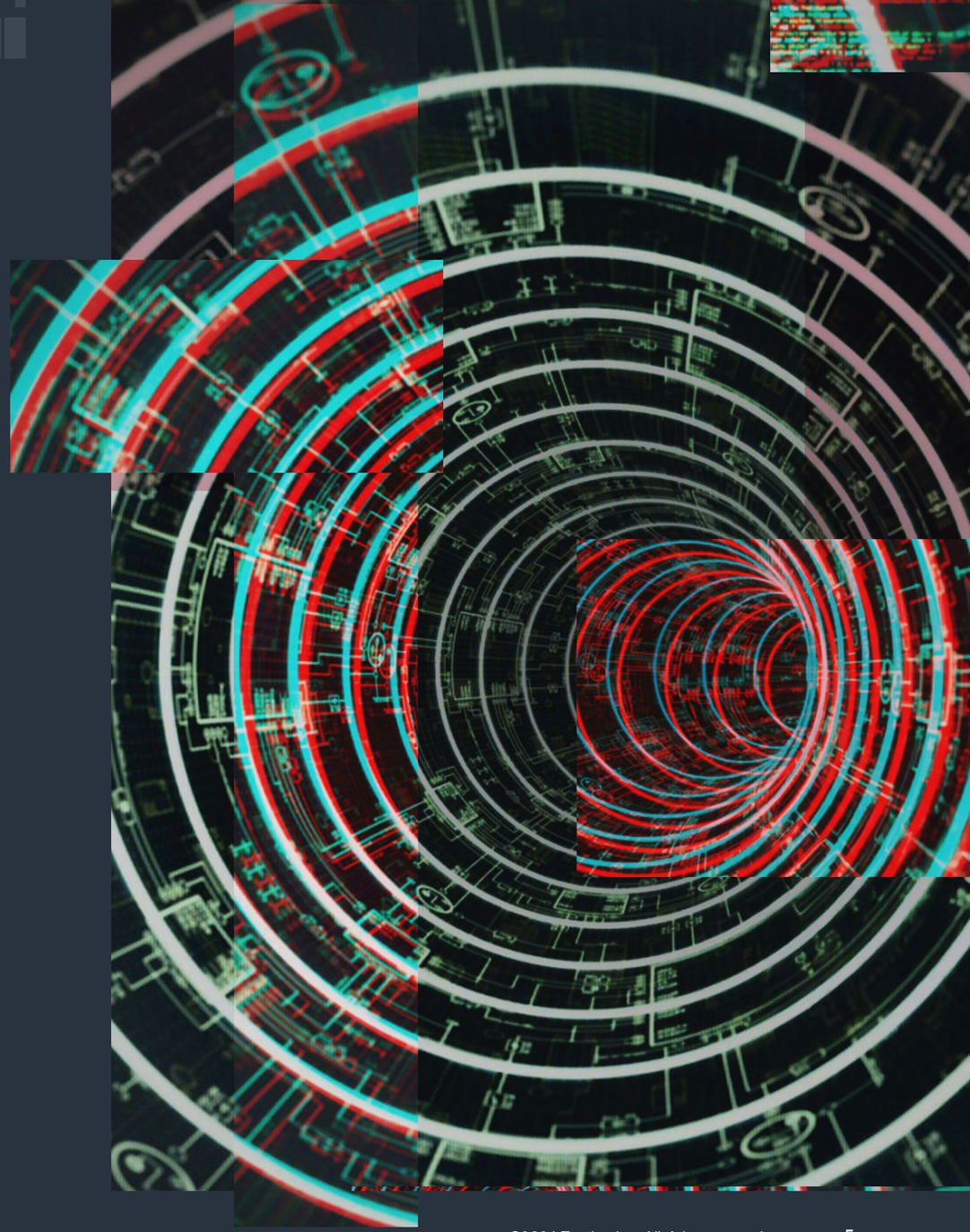
Manufacturing was the target of 42.3% of encrypted attacks, making it the top targeted industry as attackers focus on the sector's extensive use of interconnected systems and vital role in global supply chains.

The retail & wholesale and education sectors saw 232.3% and 28.7% year-over-year surges in encrypted attacks, respectively, with attackers capitalizing on these industries' high volumes of sensitive data.

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

Encrypted attacks over newly registered domains (NRDs) rose by 414.9% year-over-year, accounting for a smaller share of encrypted attacks compared to other threat categories, but indicating a growing trend of rotating throwaway domains in encrypted traffic, further complicating detection and tracking efforts.

Encrypted Threat_Landscape



Our annual look at the Google Transparency Report[1] shows just how much encryption has become the norm. As of this September, 99% of Chrome traffic is encrypted with HTTPS, with Mac and Windows close behind. Encryption's broad adoption boosts privacy protection, yet it also opens the door to more hidden threats.

For the fifth consecutive year, Zscaler has seen an increase in encrypted attacks, with 87.2% of all blocked attacks now utilizing encrypted channels.

Among these threats, **malware** continues to dominate, accounting for 86.5% of all encrypted threats observed in ThreatLabz analysis, up from 78.1% last year. The growing prevalence of malware reflects a strategic shift among attackers who have adapted their malware tactics to thrive in encrypted traffic. **Ad spyware sites** are the second-most common encrypted threat, while encrypted **phishing** has spiked by 34.1% over the past year, taking advantage of encryption to appear more legitimate and evade detection.

Cryptomining/cryptojacking and **cross-site scripting (XSS)** represent some of the fastest-growing encrypted threats, with 122.9% and 110.2% increases year-over-year, respectively. Attackers are leveraging encryption to hide cryptomining scripts and XSS payloads in legitimate traffic, effectively blurring the lines between benign and malicious activity. Cryptojacking, in particular, has surged as attackers abuse encrypted channels to harness processing power for profit—undetected.

Defending against the wide spectrum of encrypted threats, from malware and phishing to botnets and browser exploits, requires a strategic and resilient approach. Each threat type presents unique risks that can compromise data security and system integrity if not properly addressed. The following sections offer in-depth analysis of the top encrypted threat categories identified by ThreatLabz in the Zscaler cloud, with insights to help organizations navigate the complexities of today's encrypted threat landscape.

[1] https://transparencyreport.google.com/?hl=en_GB

Top Threat_ Categories

The threat landscape is in constant flux, with shifts in the popularity of encrypted attack types as cybercriminals adapt their methods over time. Understanding which threats are currently most prevalent is essential for organizations to ensure effective defenses.

The breakdown of the top threat categories is as follows:

1. Malware
2. Ad spyware sites
3. Phishing
4. Ad spyware
5. Cross-site scripting
6. Cryptomining and cryptojacking
7. Botnet attacks
8. Browser exploit
9. Webspam
10. Newly registered domains

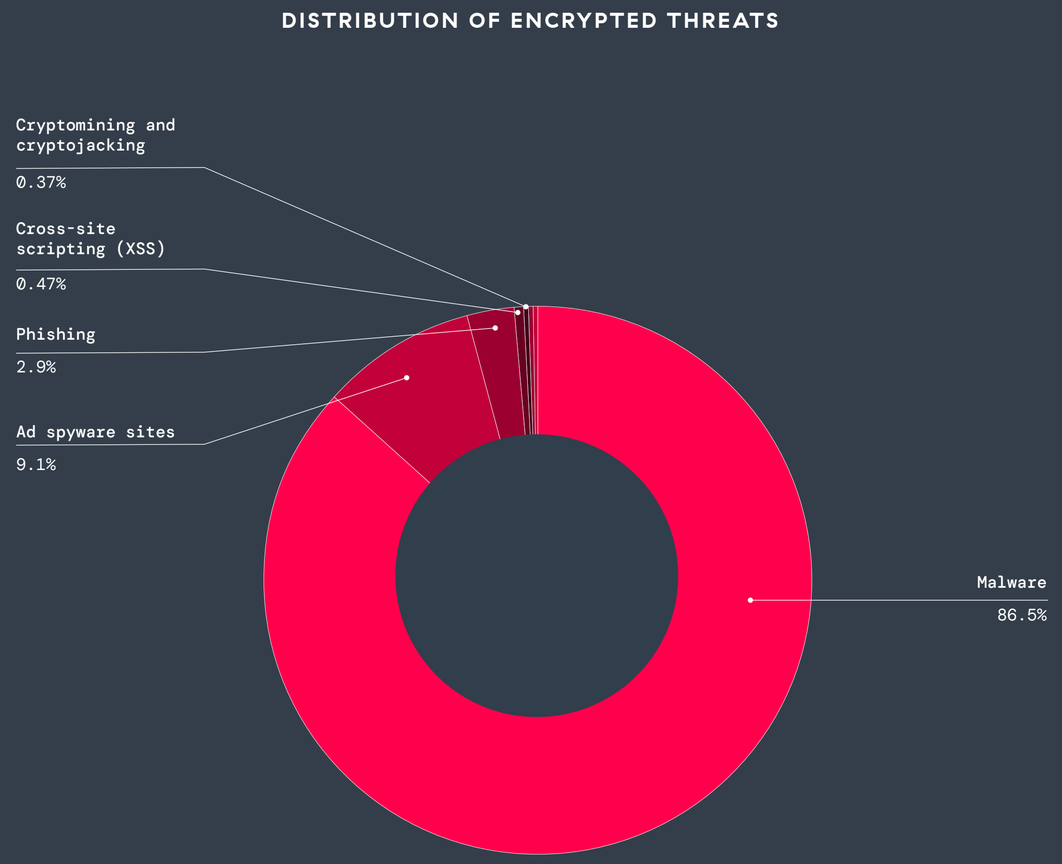


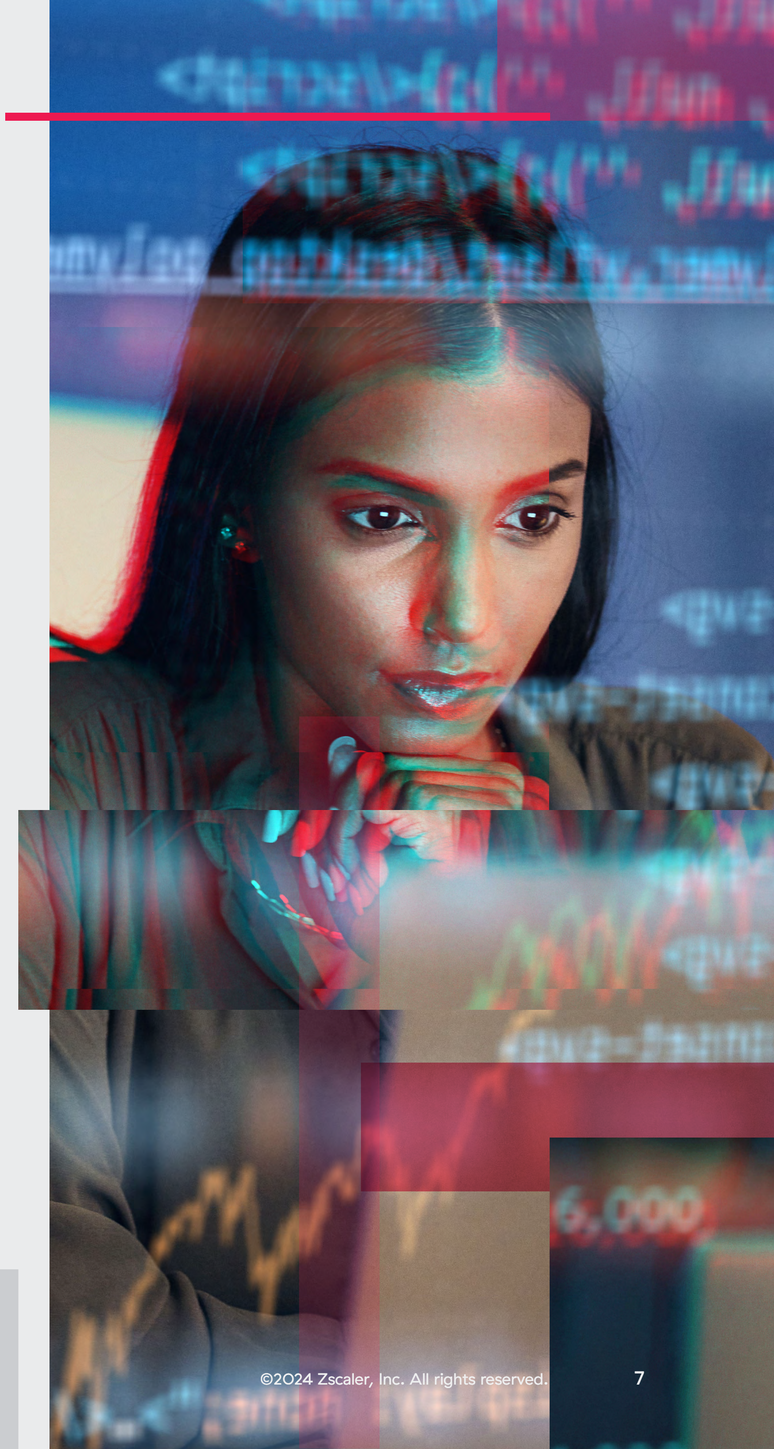
Figure 1: Top threat categories observed

Threat category comparison: 2023 vs. 2024

Threat category	Hits (2023)	Hits (2024)	Percentage change
Malware	23.3 B	27.8 B	19.2%
Ad spyware sites	5.4 B	2.9 B	-46.2%
Phishing	686.6 M	921 M	34.1%
Cross-site scripting (XSS)	72.6 M	152.5 M	110.2%
Cryptomining and cryptojacking	54 M	120.4 M	122.9%
Ad spyware	92.6 M	67.5 M	-27.1%
Browser exploit	15.8 M	21.4 M	35%
Botnet	48.7 M	19.8 M	-59.3%
Webspam	5 M	2.1 M	-59%
Newly registered domains	37,092	190,973	414.9%

Tracking how different threat categories compare year-over-year helps organizations maintain a proactive rather than reactive stance against cyberthreats, enabling important initiatives.

- Understand threat evolution
- Resource allocation and prioritization
- Adaptation of defense mechanisms
- Spotting and analyzing attack trends
- Strategic planning and threat intelligence



Malware: 86.5% of attacks

Malware accounted for 86.5% of encrypted attacks, totaling 27.8 billion hits—a 19.2% increase from the previous year's 23.3 billion hits. This surge highlights the pervasive threat of malware in encrypted traffic, as attackers use encryption to conceal malicious payloads and content.

According to ThreatLabz researchers, these were the most active malware families from October 2023 to September 2024:

1. AsyncRAT

A remote administration trojan used for remotely controlling computers. AsyncRAT utilizes a secure channel for C2 and can monitor, control, and steal sensitive information from the victim's machine.

2. Choziosi Loader/ChromeLoader

A persistent browser hijacker that uses PowerShell to add a malicious extension to the target's Chrome browser. This extension modifies browser settings to display malicious advertisements, such as fake giveaways, surveys, adult games, and dating sites, and also leaks the user's search queries.

3. AMOS/Atomic Stealer

An infostealer targeting macOS, designed to steal credentials, sensitive system information, cryptocurrency wallets, and browser cookies.

4. Ducktail

A trojan that infects browsers and steals user information. Ducktail has been observed targeting Facebook users, TikTok Business accounts, and Google Ads accounts. For C2 communication, the malware leverages Telegram bot clients.

5. Agent Tesla

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

6. Koi Loader

A dropper used to download malicious payloads to the victim's machine. It is typically delivered through drive-by downloads from compromised websites or as attachments in phishing emails..

Ad spyware sites: 9.1% of attacks

Ad spyware sites accounted for 9.1% of total encrypted attacks, with 2.9 billion hits—a 46.2% decrease from the previous year's 5.4 billion hits. Despite the decline, ad spyware sites pose a concerning threat, often leveraging encryption to host ads carrying spyware and other harmful software.

The top ad spyware sites include:

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

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

Phishing: 2.9% of attacks

Phishing accounted for 2.9% of total encrypted attacks, with 921 million hits—a 34.1% increase from the previous year's 686.6 million hits.

The most popular phishing themes were:

1. Tech support scams
2. Microsoft
3. Facebook
4. Telegram
5. Netflix
6. Google
7. DHL
8. Adobe
9. WhatsApp
10. Amazon

Real examples of phishing

Three common phishing methods are tech support scams, cryptocurrency scams, and brand imitation phishing. Here are some real–world examples:

Tech support scams

In these scams, scammers pose as tech support from trusted companies, using fake alerts or calls to claim device issues. Victims are urged to provide remote access or pay for fake services. ThreatLabz observed tech support phishing campaigns being served over HTTPS. Figures 2 and 3 show some such phishing pages.

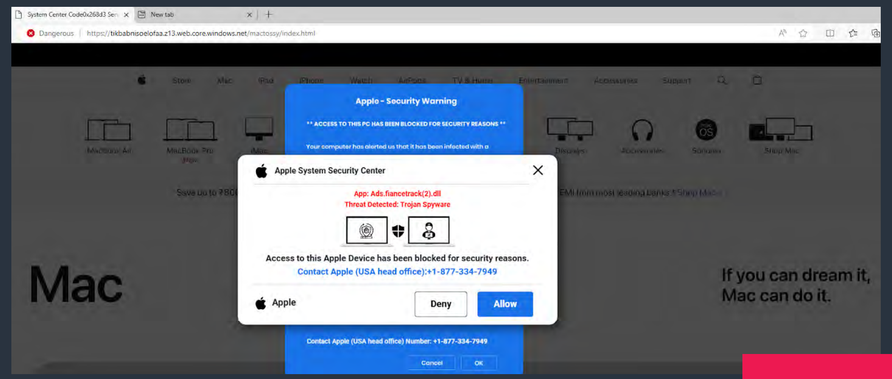


Figure 2: A phishing scam imitating Apple

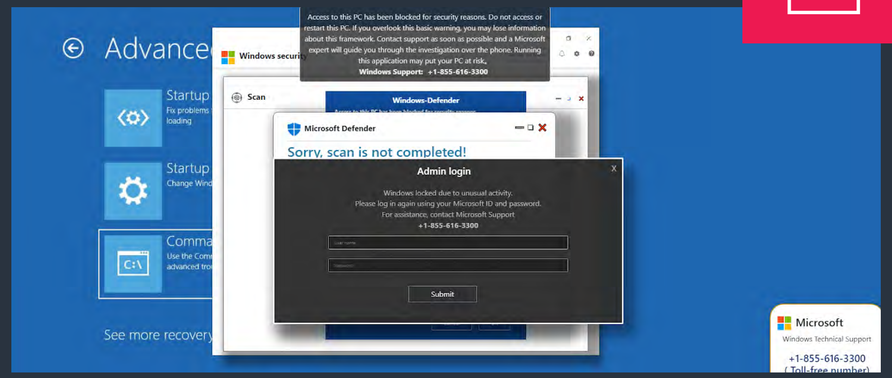


Figure 3: A phishing scam imitating Microsoft

Cryptocurrency scams

Cryptocurrency scams lure victims with promises of fast profits through fake investment schemes or giveaways. Often using phishing emails or fake crypto sites, scammers trick victims into transferring funds or revealing private credentials.

ThreatLabz observed several cryptocurrency scams that claim to multiply cryptocurrencies within 24 hours. Additionally, we found instances of fake trading platforms.

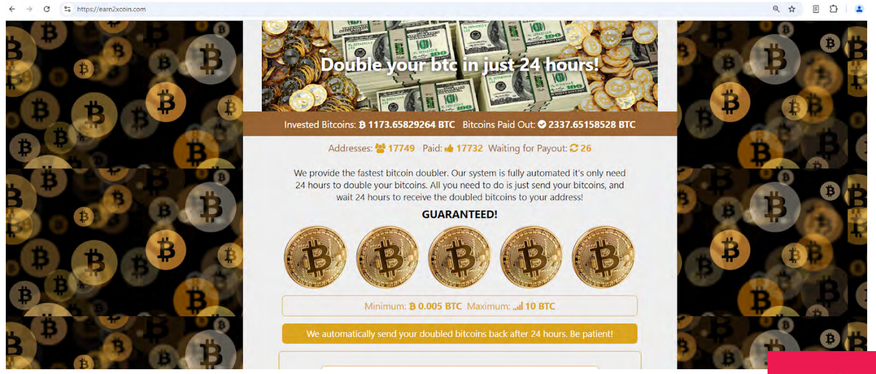


Figure 4: Bitcoin multiplier scam

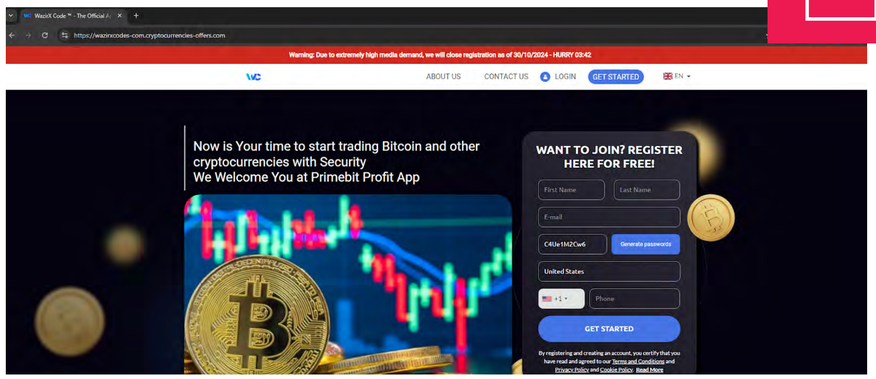


Figure 5: Fake trading platform

Brand imitation

In **brand imitation phishing**, scammers impersonate trusted brands via fake emails or websites to steal credentials or payment information. They rely on brand familiarity to deceive victims into divulging sensitive information.

Amazon

Figures 6 and 7 show an example of a phishing page served over HTTPS imitating Amazon.

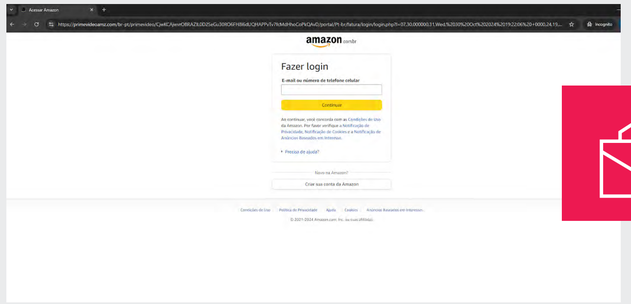


Figure 6: Fake Amazon login page

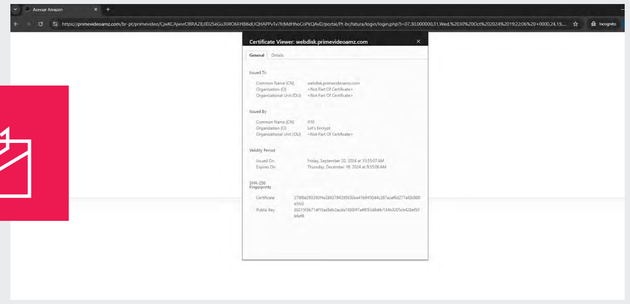


Figure 7: Fake Amazon login page

Telegram

Figures 8 and 9 show an example of a phishing page served over HTTPS imitating Telegram.

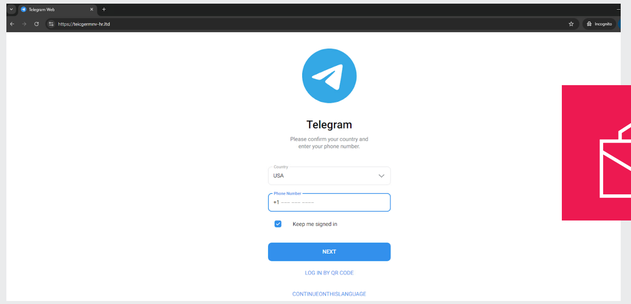


Figure 8: Fake Telegram login page

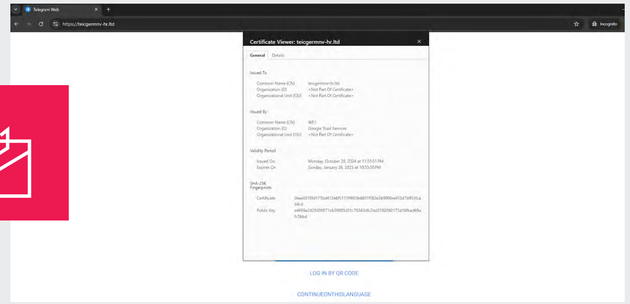


Figure 9: Fake Telegram login page

Ad spyware: 0.21% of attacks

Ad spyware accounted for 0.21% of total encrypted attacks, with 67.5 million hits—a 27.1% from the previous year's 92.6 million hits.

The top ad spyware threats include:

- **PremierOpinion:** PremierOpinion monitors and collects browsing and purchasing behavior to produce market reports and analyses. Classified as adware or potentially unwanted software, it displays surveys on shopping sites and may install without user consent, often slowing down browsers like Internet Explorer, Google Chrome, and Mozilla Firefox. It is frequently bundled with other free software, leading to unintentional installation. It collects internet usage, demographic data, hardware, software, configuration details, and application usage. Some personal information may be used to understand household demographics and combined with data from consumer data brokers.
- **SearchProtect:** SearchProtect is a potentially unwanted application that alters homepage and default search engine settings on browsers like Internet Explorer, Google Chrome, and Mozilla Firefox, redirecting users to search.conduit.com. It also blocks users from making further changes to these settings. SearchProtect tracks browsing activity, including visited web pages, user language, IP address, geographic location, and search queries. This adware can lead to malware infections and privacy concerns. It shares similarities with other browser hijackers such as Sweet-page.com, Aartemis.com, Nationzoom.com, and Do-search.com. Users often install this adware inadvertently while downloading free software through "download clients" that bundle promoted browser plugins.
- **WhenUClick:** WhenUClick is adware that installs alongside free software, generating intrusive pop-up ads, redirecting browsers, and collecting browsing data without consent. Running in the background, it slows down systems and compromises privacy, often embedding itself deeply to resist removal. By tracking user behavior, it displays targeted ads to generate revenue.
- **Popads:** Popads is an ad network focused on pop-under ads, known for high payouts and detailed targeting options. While popular with advertisers, it has also drawn misuse from threat actors embedding ads in harmful content, like phishing redirects and malware.
- **MobiGame:** MobiGame, also known as Mobiplayer or Desktop Games, is malware that masquerades as an Android emulator for Windows. It cannot be uninstalled through the Windows Control Panel and does not appear in the Start menu, leaving only an icon on the desktop labeled "Play Store." MobiGame uses deceptive marketing tactics, often posing as an essential update for a popular game like Minecraft. It frequently bundles with other malware, adware, browser hijackers, spyware, and potentially unwanted programs, leading to various problems and jeopardizing user data.

- **YandexBot:** YandexBot is a web crawler operated by Yandex. It scans websites to gather information and updates for Yandex's search index. YandexBot accesses and processes website content, metadata, and links, enabling the indexing of pages, images, videos, and other resources.

- **Toptools:** Toptools is a potentially unwanted program often installed with free software. It alters browser settings to redirect users, increase pop-up ads, and push sponsored content. It tracks browsing data for targeted ads, slowing down systems and compromising privacy.

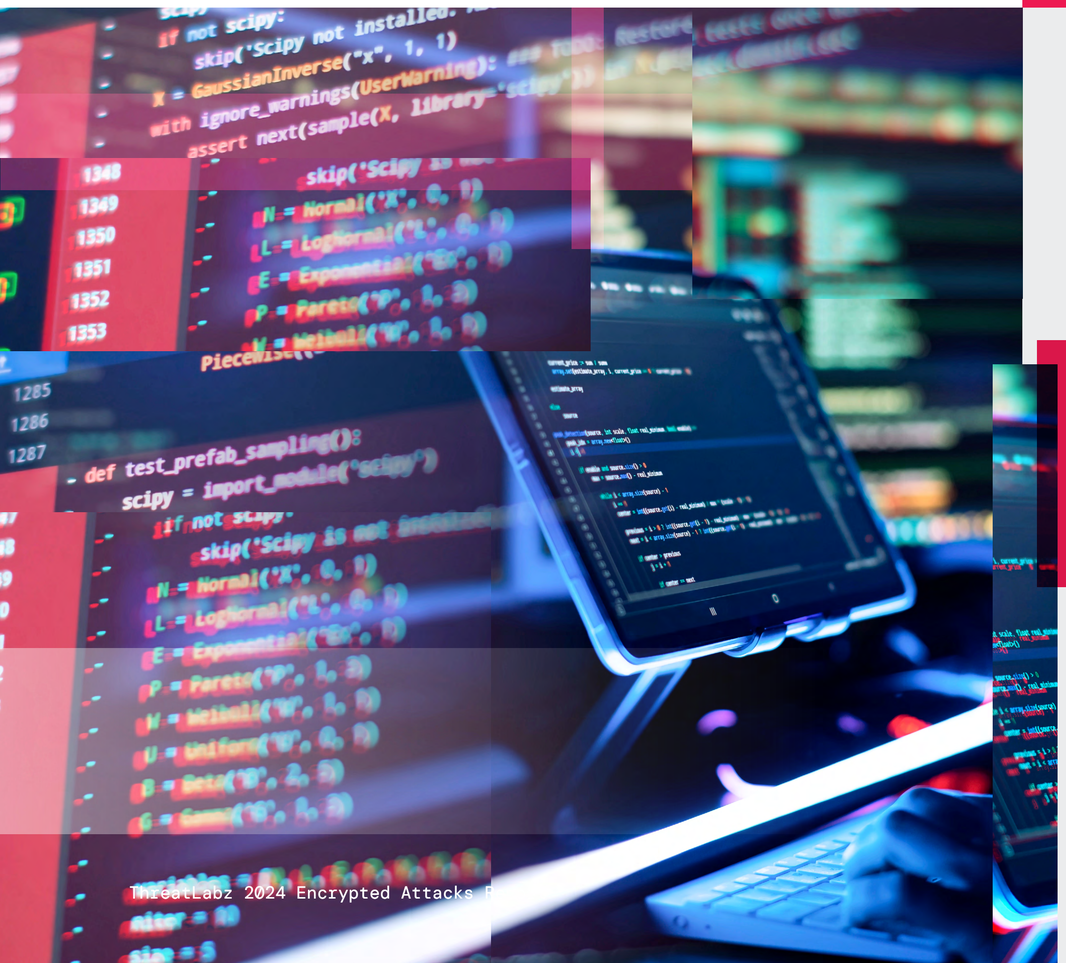
- **Neoreklami:** Neoreklami is adware that overwhelms users with intrusive ads, including pop-ups and banners, potentially leading to untrustworthy websites and raising the risk of scams or malware infections. It can expose sensitive information, slow system performance, and increase resource consumption. Neoreklami often gathers and transmits users' personal information to third parties without consent and is frequently bundled with other unwanted apps, such as browser hijackers and toolbars, further compromising the user experience.

- **MyTransitGuide:** MyTransitGuide is a browser hijacker that claims to offer public transport information but actually modifies homepage and default search engine settings on browsers like Internet Explorer and Mozilla Firefox, redirecting them to ask.com. It often infiltrates systems through bundling with other software downloaded from sites like download.com, softonic.com, or soft32.com. These downloads may include high-risk adware or malware.

- **FLPlayer:** FLPlayer claims to enable Android devices to play Flash-based live video streaming content. In reality, FLPlayer displays various third-party advertisements, including banners and pop-ups, and is classified as adware. It tracks online activity and shares this data with third parties, leading to targeted ads

Cross-site scripting (XSS): 0.47% of attacks

XSS accounted for 0.47% of total encrypted attacks, with 152.5 million hits—a 110.2% increase from the previous year's 72.6 million hits.



GenAI's role in the encrypted XSS attack surge

In 2024, we observed a dramatic increase in XSS attacks, with incidents more than doubling compared to the previous year. This surge is likely fueled by the adoption of GenAI technologies to automate and tailor malicious scripts for XSS attacks, making them more effective and difficult to detect.

- **Automated script generation for XSS attacks:** GenAI tools can generate custom malicious scripts to exploit vulnerabilities in web applications with ease. This can involve creating obfuscated JavaScript payloads designed to evade traditional security filters using AI to detect and adapt to a target site's unique defenses. Attackers can leverage GenAI to create highly personalized XSS payloads that appear legitimate or target specific input fields, increasing the success rate while reducing detection rates.

- **Enhanced evasion and mutation techniques:** GenAI enables attackers to craft adaptive XSS scripts that morph during execution to evade detection. By automating the generation of scripts that alter themselves in real time, attackers can circumvent static detection models. These adaptable scripts are particularly effective over encrypted channels, where they bypass initial detection layers and only become active once inside a target environment.

Cryptomining and cryptojacking: 0.37% of attacks

Cryptomining accounted for 120.4 million hits, representing 0.37% of total encrypted attacks—a 122.9% increase from the previous year's 54 million hits.

The increase in cryptomining and cryptojacking attacks may be linked to the rising value of various cryptocurrencies. For instance, bitcoin saw a significant jump in 2024, increasing from approximately $34,000 to $75,000. Additionally, CleanSpark, a bitcoin mining company operating multiple data centers, reported[2] a 32% increase in bitcoin mined compared to the previous month. This spike in profitability likely drives cybercriminals to target systems for unauthorized mining, intensifying cryptojacking activity.

The top cryptomining threats were:

1. CoinIMP
2. Kryptex
3. XMRig
4. DeepMiner
5. JSECoin
6. Webmine
7. CryptoLoot
8. CookieMiner
9. ElectrumStealer
10. MoneroMiner

[2] https://investors.cleanspark.com/news/news-details/2024/CleanSpark-Releases-October-2024-Bitcoin-Mining-Update/default.aspx

[3] https://www.fortinet.com/blog/threat-research/the-growing-trend-of-coin-miner-javascript-infection

ThreatLabz recently detected the following cryptocurrency-related threats in the Zscaler cloud:

1. CoinIMP

CoinIMP is a JavaScript-based coin miner that uses a victim's CPU and GPU to mine cryptocurrency without their knowledge. The infection begins when a user visits a website embedded with CoinIMP JavaScript. Once executed, the script starts the mining activity and evades detection by antivirus and ad blockers. CoinIMP is a fork of CoinHive and has been used in past campaigns.

2. Kryptex

Kryptex (a.k.a. TeamRedMiner) is a commercial GPU miner optimized for AMD GPUs and Xilinx FPGAs. It utilizes the maximum potential of AMD GPUs for mining and can operate as a silent miner running in the background unnoticed by the end user. Kryptex is the GUI version of TeamRedMiner. The network traffic of the miner is SSL encrypted.

3. XMRig

XMRig (a.k.a. Monero Miner or CryptoNight) is open source software for mining cryptocurrencies like Monero or bitcoin. This cryptojacking malware consumes significant CPU resources, causing slow performance and overheating. It spreads through malicious advertisements and bundling with other cyberattacks, commonly distributed as fake updates for software like Adobe Flash Player, Java, and cracked software. XMRig does not target specific industries but opportunistically steals computational resources. Its network communication is TLS/SSL-encrypted, and it connects to a mining pool, with its Dynamic DNS visible in network traffic flow.

4. DeepMiner

DeepMiner allows threat actors to customize phishing content based on geographical location and make it disappear if the page has been visited before, avoiding detection. This technique hides malicious URLs and has been adopted to conceal cryptocurrency mining JavaScript on compromised websites, causing visitors' computers to start cryptomining. Similar to CoinHive, DeepMiner provides website owners with a JavaScript code to embed on their sites. For example, threat actors previously compromised Milk New Zealand's website to mine Monero using DeepMiner[3].

5. JSECoin

JSECoin is a service that mines cryptocurrency via web browsers by injecting JavaScript into targeted websites. While some legitimate websites use this feature and notify users, rogue sites do not, mining Monero without user consent. This unauthorized mining consumes large amounts of processing power, causing performance issues and hindering other running processes. Although JSECoin has been shut down and is no longer available, its previous misuse highlights the potential for similar abuses by other services.

6. Webmine

Webmine, similar to JSECoin, is a service used for mining cryptocurrency via web browsers by injecting JavaScript into targeted websites. While some legitimate websites use this feature and notify users, rogue websites do not provide any notification. These sites mine Monero using visitors' processing power, often consuming large amounts and causing performance issues. The mining activity is conducted without regard for the user's system efficiency. Webmine's network communication is TLS/SSL-encrypted.

7. CryptoLoot

CryptoLoot is a JavaScript-based cryptomining tool, similar to CoinHive and DeepMiner, used for cryptojacking to maximize returns from web traffic. It was delivered via the CookieScript.info service, where a cookie consent JavaScript file contained a copy of CryptoLoot, an in-browser Monero miner.

8. CookieMiner

CookieMiner, derived from Darthminer, integrates an Empyre-based Mac backdoor and XMRig miner to bypass authentication by stealing login credentials, text messages, and web cookies. This allows attackers to withdraw funds and manipulate cryptocurrency prices for profit. CookieMiner can steal browser cookies, saved usernames, passwords, credit card details, iPhone text messages, and crypto wallet data while maintaining control of the victim's machine and mining. It configures the victim's machine to mine cryptocurrency and maintain persistence through commands. Some required IOCs for simulation and traffic generation are unavailable on VirusTotal, complicating the recovery of transactions conducted by CookieMiner.

GenAI's role in the cryptomining attack surge

In 2024, we observed a dramatic rise in cryptomining and cryptojacking attacks, with these threats surging by over 100% compared to the previous year. Besides the skyrocketing value of different cryptocurrencies, this surge is also likely driven by the adoption of GenAI technologies that streamline the creation of advanced cryptomining scripts.

- **Optimized cryptomining scripts:** GenAI can help attackers develop efficient cryptomining scripts that run unobtrusively, optimizing them to use minimal resources to avoid detection by monitoring tools. These scripts can even adjust based on the host's CPU and memory load, making them less likely to trigger suspicion and able to run long-term persistence, especially in environments where traffic is encrypted.
- **Exploitation of vulnerabilities in encrypted channels:** GenAI models trained on vast datasets may be able to identify subtle vulnerabilities in encrypted communication protocols. This enables attackers to deploy cryptomining payloads that slip through encrypted channels, particularly by masking them within standard traffic patterns, making them harder to spot without deeper inspection tools.

Botnet: 0.06% of attacks

Botnet attacks accounted for 19.8 million hits, representing 0.06% of total encrypted attacks—a 59.3% decrease from the previous year's 48.6 million hits.

The top botnet threats include:

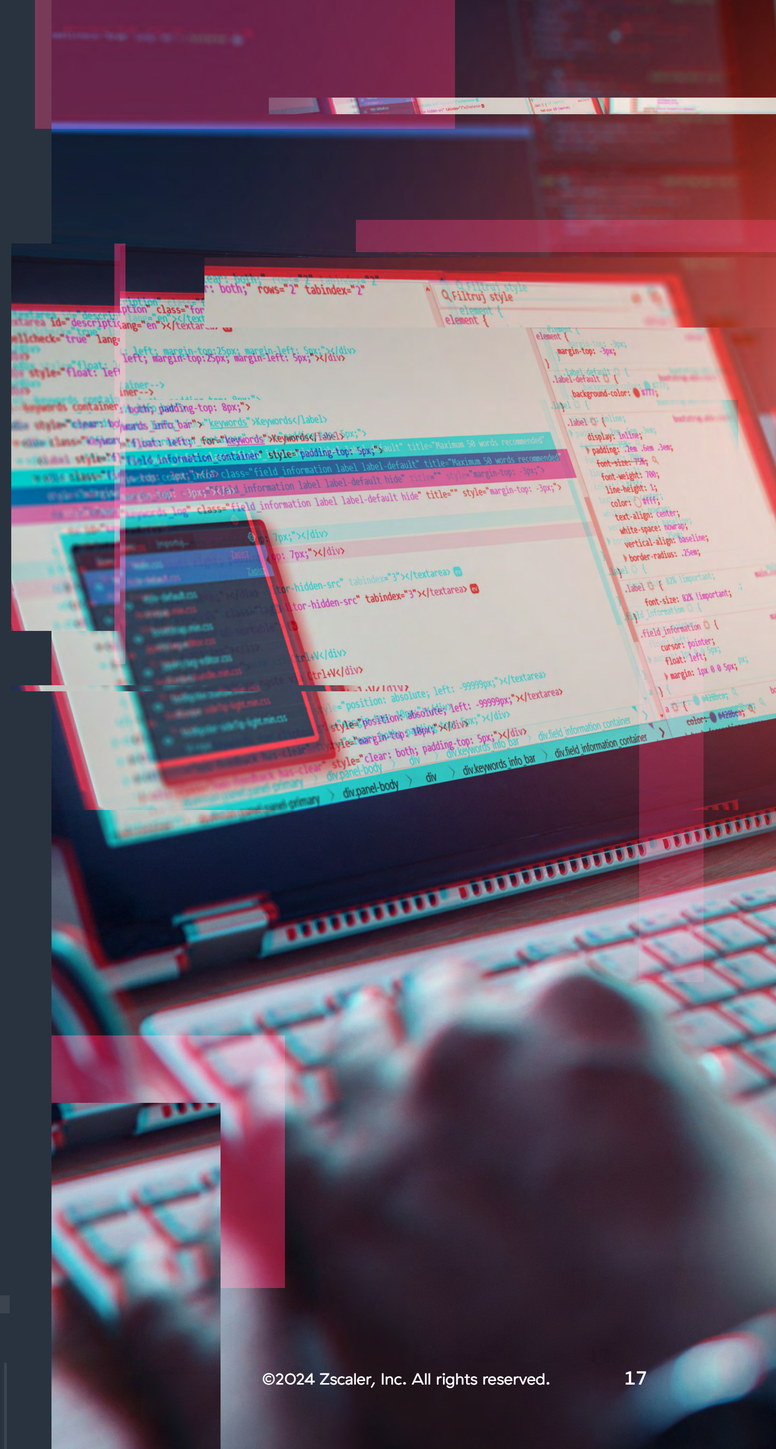
- CobaltStrike
- Ducktail
- Azorult
- Wacapew
- Meterpreter
- Mythic
- GoRat
- NJRat
- IcedID
- Lumma Stealer

A shift to stealth in C2 operations

ThreatLabz research indicates that C2 activity over encrypted channels is evolving to become significantly stealthier. Our analysis reveals a nearly 60% reduction in the volume of detectable C2 communications, despite a concurrent 19.2% increase in malware instances. This shift reflects an evolution in botnet tactics: while initial infection and persistence phases are steadily increasing (indicating that more systems are being compromised and maintained), post-infection activities, such as data exfiltration and lateral movement, are becoming less conspicuous.

This trend suggests that while the overall number of infections may remain constant (or even increase), attackers are employing more refined and discreet strategies. This mirrors the behavior observed in the Dark Angels ransomware group during their historic US$75 million payout, as detailed in the **ThreatLabz 2024 Ransomware Report**.

Our findings are further supported by a 2024 threat report from Spamhaus[4] indicating that botnet C2 activity has decreased between January and June 2024, reinforcing the trend toward quieter, more sophisticated C2 operations within botnet networks.



[4] https://info.spamhaus.com/hubfs/Botnet%20Reports/Jan-Jun%202024%20Botnet%20Threat%20Update.pdf

Countries that Experience the Most Encrypted Attacks

Understanding the top targeted countries is crucial for developing region-specific cybersecurity strategies. Our findings indicate that the US, India, and France are the most frequently targeted nations. The US and India consistently rank at the top, highlighting their significance as high-value targets for cybercriminals.

The top 10 countries most targeted by encrypted attacks between October 2023 and September 2024 were:

1. United States
2. India
3. France
4. United Kingdom
5. Australia
6. Canada
7. Germany
8. Lithuania
9. Poland
10. South Africa

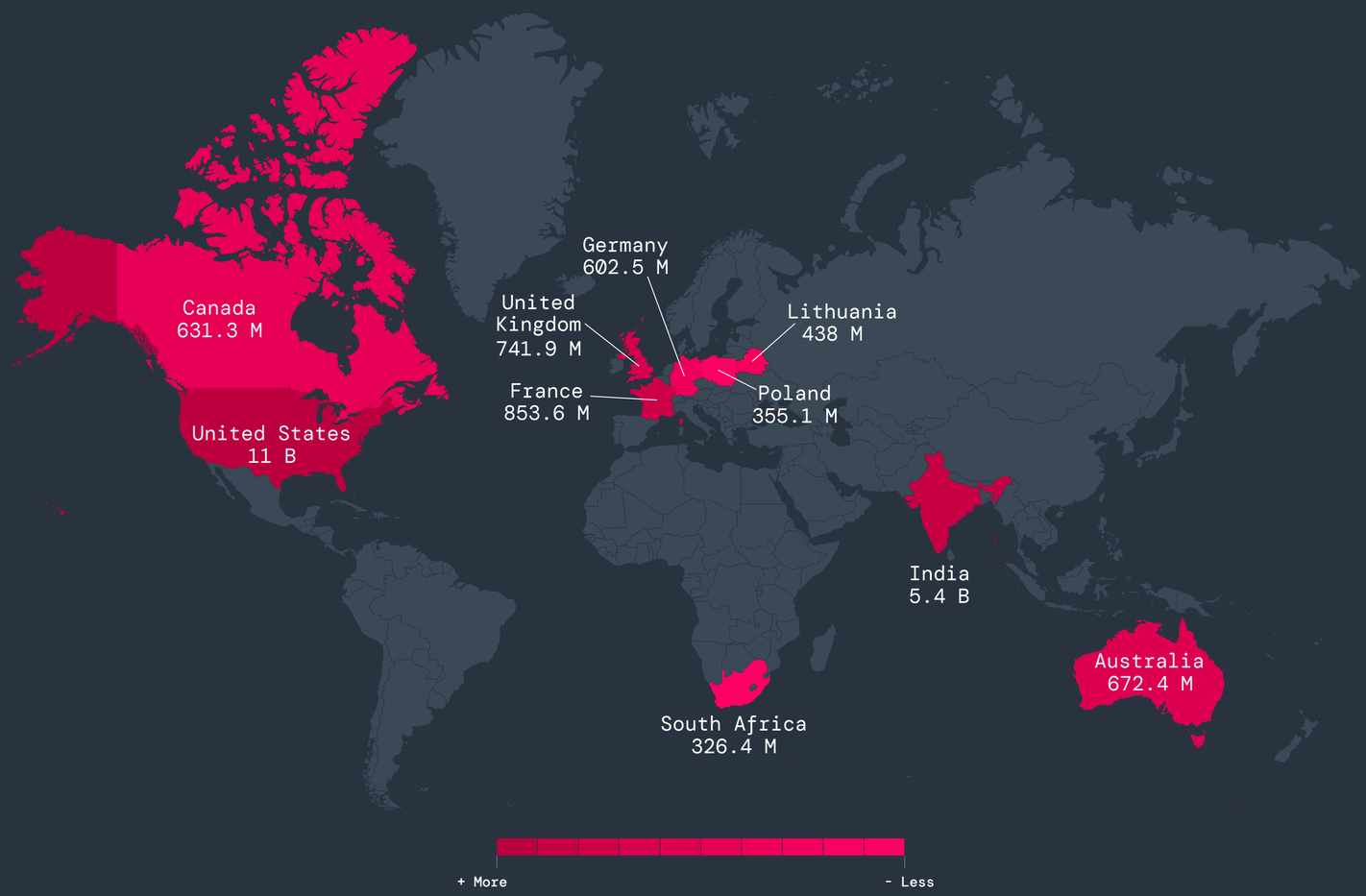


Figure 10: A map of the countries that experience the most encrypted attacks

Encrypted Attacks by World Regions

Our research reveals broad threat trends worldwide, but significant regional differences highlight how local cybercriminal activities shape threat dynamics uniquely in each area. Globally, malware, ad spyware sites, and phishing remain the primary threats; however, their impact varies considerably across regions.

NORTH AMERICA

In line with worldwide patterns, North America experienced a rise in encrypted malware (52.9%) and phishing (11%) alongside a drop in botnet activity (–3.7%), but uniquely saw a decrease in cryptomining/cryptojacking activity.

Threat category	Hits (2023)	Hits (2024)	Percentage change
Malware	6.1 B	9.4 B	52.9%
Ad spyware sites	551.4 M	8.1 B	223.7%
Phishing	331.4 M	367.9 M	11%
XSS	11.7 M	39.1 M	233.1%
Ad spyware	81.5 M	28.6 M	-64.9%
Cryptomining and cryptojacking	26.7 M	11.9 M	-55.3%
Browser exploit	3 M	6.6 M	117.2%
Botnet	6.2 M	6 M	-3.7%
Webspam	2.1 M	980,775	-52.9%
Newly registered domains	13,371	90,594	577.5%

EUROPE

Europe saw significant surges in XSS (272.4%) and cryptomining/cryptojacking (123.5%), but experienced a slight decline in encrypted phishing attacks, which stands out given the global rise in phishing.

Threat category	Hits (2023)	Hits (2024)	Percentage change
Malware	5.6 B	4.5 B	-19.8%
Ad spyware sites	528.5 M	267.5 M	-49.4%
Phishing	208.6 M	197.2 M	-5.5%
Cryptomining and cryptojacking	31.9 M	71.3 M	123.5%
XSS	13.2 M	49.2 M	272.4%
Ad spyware	21.9 M	11.1 M	-49.6%
Botnet	14.7 M	4.6 M	-68.8%
Browser exploit	641,724	2.2 M	238.9%
Webspam	852,339	226,725	-73.4%
Newly registered domains	5,750	25,180	337.9%

ASIA PACIFIC AND JAPAN (APJ)

The APJ region aligned with overall upward trends in encrypted malware (26.3%), phishing (65.1%), and XSS (88.1%), but also experienced fewer cryptomining/cryptojacking attacks year–over–year.

Threat category	Hits (2023)	Hits (2024)	Percentage change
Malware	6.9 B	8.7 M	26.3%
Ad spyware sites	153.1 M	256.5 M	67.5%
Phishing	91.9 M	151.6 M	65.1%
XSS	19.7 M	37.1 M	88.1%
Cryptomining and cryptojacking	39.9 M	17.2 M	-57%
Browser exploit	4.6 M	10.5 M	-131.6%
Ad spyware	27.8 M	9.7 M	-64.93%
Botnet	10.9 M	6.1 M	-44.5%
Webspam	4.1 M	442,947	-68.2%
Newly registered domains	10,798	38,972	260.9%

AFRICA

Phishing activity saw an increase of 304.1%, while botnet activity significantly declined by 95.3%.

Threat category	Hits (2023)	Hits (2024)	Percentage change
Malware	2.5 B	409.5 M	-83.1%
Phishing	11.2 M	45.3 M	304.1%
Ad spyware sites	42.5 M	24.9 M	-41.4%
Ad spyware	12.1 M	2.1 M	-82.8%
Cryptomining and cryptojacking	6.1 M	779,492	-87.3%
Botnet	12.9 M	610,129	-95.3%
XSS	188,467	266,433	41.4%
Browser exploit	20,748	112,814	443.7%
Webspam	300,896	56,754	-81.1%
Newly registered domains	875	17,027	1845.9%

MIDDLE EAST

In line with worldwide patterns, the Middle East experienced a 112.9% increase in phishing.

Threat category	Hits (2023)	Hits (2024)	Percentage change
Malware	441.8 M	227.2 M	48.6%
Phishing	9.4 M	20.1 M	112.9%
Ad spyware sites	21.8 M	20.1 M	-7.9%
Cryptomining and cryptojacking	2.8 M	2 M	-29.1%
XSS	347,188	1.7 M	403.7%
Botnet	600,456	730,728	21.7%
Ad spyware	826,030	601,653	-27.2%
Browser exploit	65,103	429,855	560.3%
Webspam	234,477	149,873	-36.1%
Newly registered domains	707	584	-17.4%

LATIN AMERICA

The Latin region experienced an increase in malware, phishing, and cryptomining—matching worldwide trends.

Threat category	Hits (2023)	Hits (2024)	Percentage change
Malware	511.5 M	717.4 M	40.3%
Ad spyware sites	53.8 M	50.3 M	-6.4%
Phishing	23 M	41.3 M	79.4%
Cryptomining and cryptojacking	5.3 M	12.4 M	132.6%
Ad spyware	8.9 M	8.5 M	-4.9%
XSS	890,272	4.5 M	406.8%
Botnet	168,524	768,589	356.1%
Browser exploit	215,597	147,458	-31.6%
Webspam	268,335	52,437	-80.5%
Newly registered domains	1,494	8,227	450.7%

Top Targeted Industries

Identifying the most impacted by encrypted attacks allows organizations to adapt their security strategies to effectively address industry-specific threats.

Manufacturing remains the most targeted industry by a significant margin, facing nearly three times the attacks of the the next most targeted sectors, technology and communications. Attacks on manufacturing have increased 43.9% compared to last year, driven by rapid digitization through Industry 4.0 advancements, which are transforming manufacturing into a digital-first domain. This shift increases the attack surface, making manufacturers more vulnerable to a growing array of cyberthreats.

For deeper analysis of how technology and manufacturing are increasingly intertwined, explore the most recent ThreatLabz report on internet of things (IoT) and operational technology (OT) trends.

The top five most affected industries were:

1. Manufacturing
2. Technology and communication
3. Services
4. Education
5. Retail and wholesale

Industry	Hits (2023)	Hits (2024)	Percentage change
Manufacturing	9.4 B	13.5 B	43.9%
Technology and communication	7 B	4.4 B	-37.1%
Services	4 B	3.8 B	-5.3%
Education	2 B	2.6 B	28.7%
Retail and wholesale	709.1 M	2.4 B	232.3%
Finance and insurance	1.8 B	1.7 B	-4.1%
Healthcare	2.6 B	1.4 B	-39.2%
Government	1.6 B	1.4 B	-13.7%
Others	942.5 M	896.4 M	-4.9%

Comparing_TLS/SSL Certificates

TLS/SSL certificates are essential for verifying the identity of a website owner and enabling secure, encrypted connections between users and that site. However, not all certificates offers the same level of trust. Certificate types vary, with each requiring different degrees of identity verification, providing progressively stronger assurances to users.

Certificate distribution	2023	2024	Percentage change
Domain Validation (DV)	303.4 M	327.8 M	8%
Extended Validation (EV)	11.6 M	4.9 M	-57.8%
Organization Validation (OV)	242.6 M	175.7 M	-27.6%

CERTIFICATE VALIDATION TYPE DISTRIBUTION

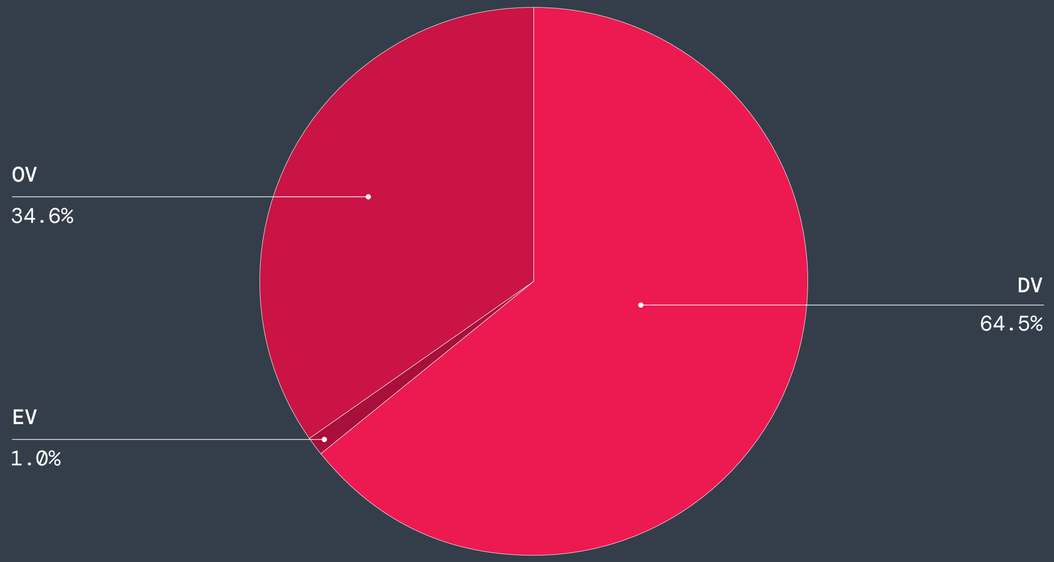


Figure 11: The distribution of TLS/SSL traffic by certificate

Domain Validation (DV) remains the most common type of certificate at 64.5%. To obtain one, applicants only need to prove control over the domain, typically by matching the registrant's email domain with the WHOIS record. These certificates are easy to acquire and offer the lowest level of trust.

Obtaining an **Extended Validation (EV)** certificate is both costly and time-consuming, which explains why only 1% of certificates fall into this category.

Distribution of ASNs in TLS/SSL Phishing Destinations

Examining the Autonomous System Numbers (ASNs) associated with phishing destinations and presenting the top destinations, provides a clearer picture of the network infrastructure utilized in phishing attacks. This information is vital for identifying attribution and threat detection.

Hetzner Online, a German-based hosting and data center company, leads the pack by a margin at 16.6%. Cloudflare and Amazon come in at 15.6% and 15.1%, respectively.

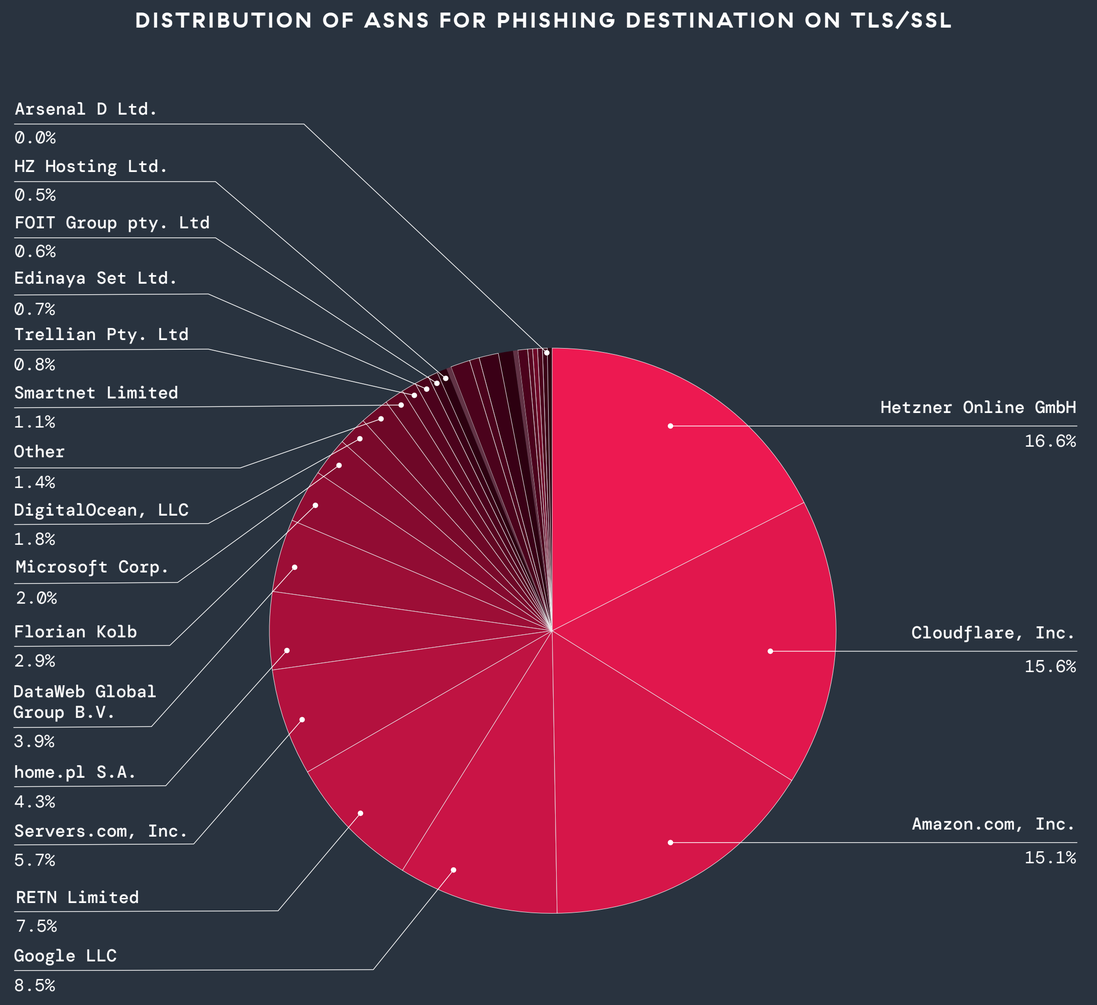


Figure 12: Where most TLS/SSL traffic is going during phishing

Encrypted Attack_Trends

Evolving AiTM phishing techniques

As phishing tactics evolve, adversary-in-the-middle (AiTM) techniques are growing more sophisticated, enabling attackers to mimic trusted sites with striking accuracy. The following example demonstrates how AiTM methods use advanced tools and TLS/SSL encryption to create nearly undetectable phishing campaigns.

In this scenario, the phishing page serves a TLS certificate issued by Let's Encrypt, which lacks any organization-specific details. This certificate was automatically retrieved and renewed through CertMagic, a tool used by the AiTM reverse proxy service Evilginx to secure phishing domains. By default, Evilginx relies on Let's Encrypt, allowing attackers to set up a valid-looking TLS certificate quickly and easily.

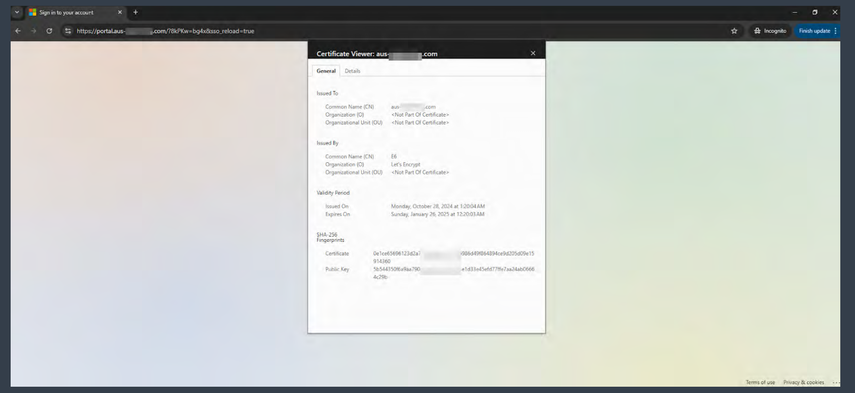


Figure 13: A seemingly valid TLS certificate

The phishing page is able to check Microsoft servers to validate usernames. When a user enters a valid username, the phishing page proxies the connection directly to Microsoft's legitimate server.

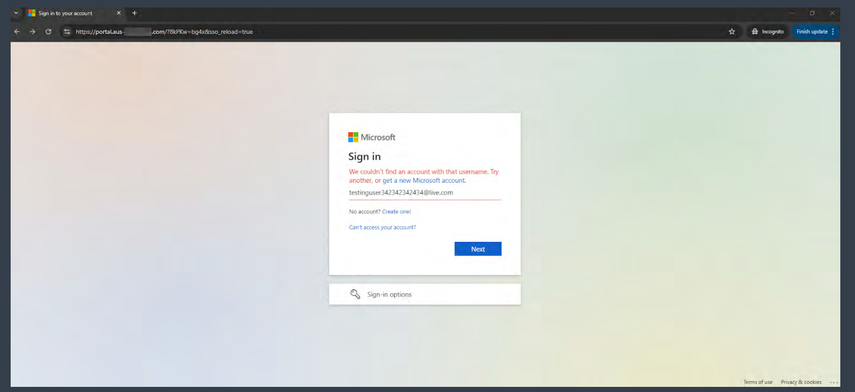


Figure 14: A proxied Microsoft login page

A side-by-side comparison of the phishing page and genuine Microsoft login page reveals identical code, with the phishing page only differing in its modified URL—a hallmark of AiTM attacks.

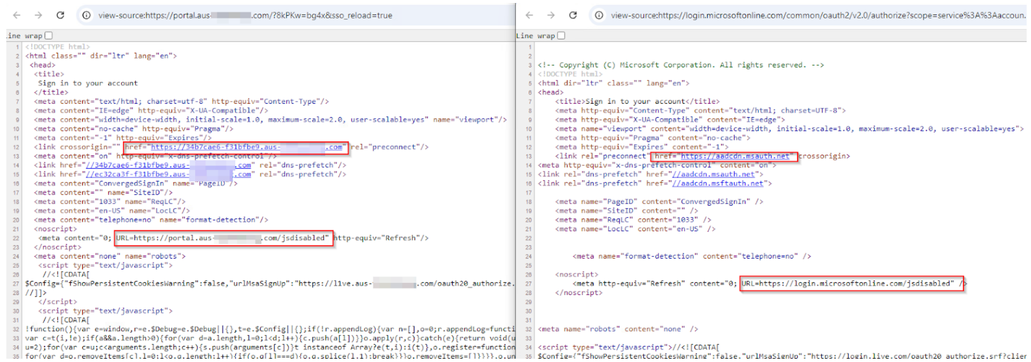


Figure 15: Phishing page code vs. Microsoft page code

Additionally, attackers use WebSockets TLS/SSL (WSS) keepalive connections to maintain persistent communication. These keepalive signals function as a "heartbeat," ensuring the AiTM proxy remains connected to both the victim and the legitimate service without interruption. This tactic allows attackers to intercept and forward credentials or session tokens in real time, making it exceptionally challenging to detect and mitigate these threats.

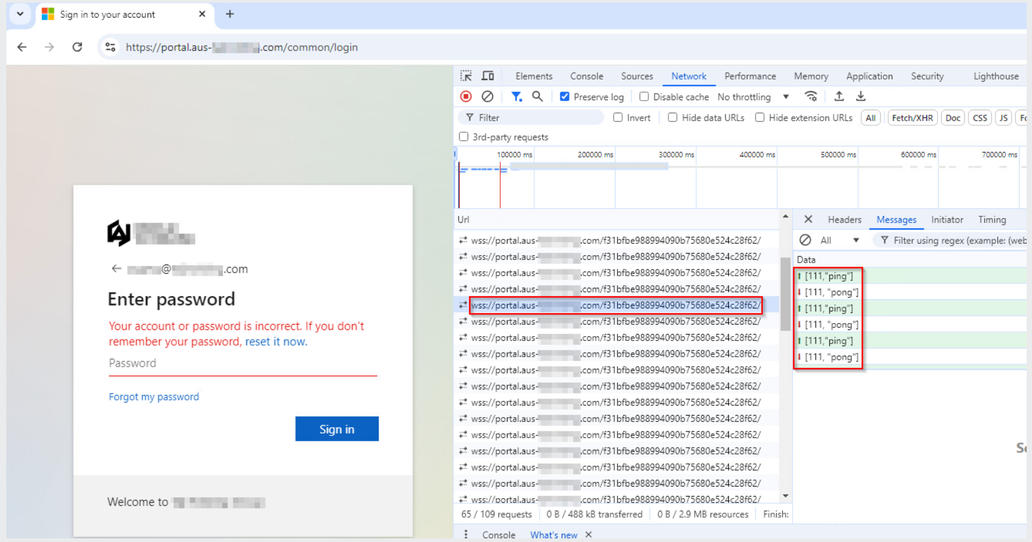


Figure 16: "Ping-pong" traffic via WSS

Data exfiltration via HTTPS

Data exfiltration has become a significant trend in encrypted attacks, with attackers leveraging encryption channels to siphon off sensitive data from targeted systems.

Here are three examples of how attackers are using various malware strains to covertly exfiltrate data, using HTTPS encryption to bypass detection.

VIPKeylogger

- **Capabilities:** A variant of SnakeKeyLogger, VIPKeylogger is a credential stealer that targets web browsers, email clients, and more. It captures keystrokes, clipboard content, credit card data, and screenshots, posing a serious risk to user privacy and security.
- **Delivery method:** Typically delivered via phishing and spear-phishing malspam campaigns, VIPKeylogger often arrives as a malicious Office document attached to an email. Once executed, the document downloads and installs the keylogger on the victim's device.
- **Exfiltration tactics:** VIPKeylogger can exfiltrate stolen data through multiple encrypted methods, including sending it to an email address using SMTP, uploading it to an FTP server, or sending it to a Telegrambot over HTTPS post requests.

LummaC2

- **Capabilities:** An information stealer written in C++, LummaC2 can steal data from a wide range of sources, including cryptocurrency wallets, Steam accounts, KeePass, Telegram, FileZilla, and browser extensions. The list of crypto wallet extension and browsers to target are sent by the C2 server.
- **Delivery method:** As a malware-as-a-service (MaaS) tool, LummaC2 is deployed using various loaders like HijackLoader, Emmental, and PrivateLoader, often through deceptive methods such as fake CAPTCHA pages and ClickFix tactics.These tactics enhance its distribution and lure victims into installation.
- **Exfiltration tactics:** LummaC2 gets its target list from the C2 server, compiles the stolen data into a zip archive, and sends it back to the server via an HTTPS POST request. This reliance on HTTPS for exfiltration ensures that the data remains encrypted during transmission, making it more difficult for traditional network security tools to intercept.

Blank Grabber

- **Capabilities:** An open source information stealer written in Python, Blank Grabber can steal passwords, cookies, Discord tokens, and cryptocurrency wallets, and can even capture webcam images from the victim's system.
- **Delivery method:** Blank Grabber is commonly distributed through GitHub repositories that appear to offer gaming-related themes, such as game cheats and boosters, as well as through malicious packages on the PyPi platform.
- **Exfiltration tactics:** Blank Grabber can exfiltrate stolen data in two ways: Discord webhooks or Telegram bots, both of which use HTTPS for transmission. By embedding the stolen data within encrypted HTTPS traffic, Blank Grabber ensures that it bypasses conventional security measures.

Rise in cloud service abuse

In recent years, there has been a significant rise in the abuse of cloud services by advanced persistent threat (APT) groups. These threat actors abuse cloud platforms to conduct their malicious activities while evading traditional security measures.

APT groups abuse cloud services for several reasons. By blending in with legitimate traffic, they can take advantage of TLS/SSL encryption enabled by default, which helps them evade network security controls. This approach requires low investment and maintenance while making it difficult to track their command–and–control (C2) infrastructure. Consequently, it increases the shelf life of their campaigns, allowing them to operate undetected for longer periods.

Threat researchers can gain valuable extra intelligence when investigating APT groups using cloud services. Researchers can also gather information on the campaign timeline and volume, the nature of the targets, and access to private tools and samples used by the attackers. This intelligence is crucial in understanding and mitigating the threats posed by these groups.

Mitigations and countermeasures

To combat the rise in cloud service abuse by APT groups, organizations should implement several mitigations and countermeasures:

- **Monitor for anomalous network activity related to cloud services:** Continuous monitoring can help detect unusual patterns that may indicate malicious activity.
- **Allow traffic only for allowlisted cloud services:** Restricting access to only approved cloud services can reduce the attack surface.
- **Conduct APT social engineering attack simulations:** Regular security awareness training that includes simulations of APT social engineering attacks can help employees recognize and respond to potential threats.

KEY OBSERVATIONS IN CLOUD SERVICE ABUSE

By monitoring and analyzing the patterns of behavior exhibited by APT groups when abusing cloud services, the research community can enhance its ability to detect, mitigate, and defend against these threats. Key observations include:

Russian threat actors like to reuse the same cloud service platforms over and over in their campaigns.

Russia–linked APT groups are meticulous in their operations, frequently adding new cloud service APIs to their arsenal and reusing cloud hosting services for abuse.

Iran–linked APT groups overwhelmingly use OneHub, a cloud storage service, to distribute malware.

APT groups such as MuddyWater have consistently used OneHub to distribute Remote Monitoring and Management (RMM) tools for over two years.

North Korean threat actors consistently abuse cloud services, indicating a preference in their attack methods.

APT groups like APT37 continue to abuse the same set of services to deliver ROKRAT, demonstrating a persistent approach in their campaigns.

Threat actors reuse cloud service account names and emails across multiple campaigns.

APT groups are known for reusing cloud hosting accounts across multiple campaigns and email addresses across cloud hosting services, often to launch spear phishing campaigns.

MOST COMMON TACTICS USED IN CLOUD SERVICE ABUSE

Key tactics for abusing cloud services include:

- **Dead drop resolvers:** Attackers use cloud storage or repositories as "dead drops" to store IP addresses or domains for C2 communication, allowing them to change C2 locations without directly interacting with the malware.
- **Cloud services API abuse:** Cybercriminals abuse cloud service APIs to bypass security controls, using legitimate cloud infrastructure for malicious activities like data exfiltration and spreading malware.
- **Webhooks abuse:** Attackers misuse webhooks to hide their original location (i.e., IP address) when delivering malware or stealing data by leveraging the automated messaging between apps.
- **Payload hosting:** Threat actors host malware payloads on trusted cloud services, making it easier to bypass detection by security tools that might overlook files stored on reputable platforms.

SOCIAL MEDIA ABUSE BY APT GROUPS

APT groups are increasingly using social media as a cover tool, transforming it into a multifunctional asset in their attack campaigns. From launching advanced social engineering tactics to utilizing platforms as dead drop resolvers, these actors are hiding critical C2 data in the fabric of everyday digital interactions. This abuse of social platforms presents a significant challenge for security teams, as it allows attackers to mask their activities under the guise of legitimate content while bypassing traditional security.

The most commonly abused social media platforms are:

LinkedIn
- Fake recruiter profiles
- Fake organizations

X (formerly Twitter)
- Fake profiles impersonating security researchers or blockchain experts

TOP APT GROUPS ABUSING CLOUD SERVICES

Many of the most active and sophisticated APT groups, particularly those linked to Russia, North Korea, and Iran, have adopted cloud-based tactics to conceal their operations and enhance their reach.

Other APT groups that have increasingly leveraged cloud service abuse include:

- **APT28**, a.k.a. Fancy Bear, a Russian state-backed group known for targeting government, military, and media entities worldwide, often focusing on cyber-espionage and information warfare.
- **APT29**, a.k.a. Cozy Bear, another Russian-backed group, leverages cloud storage for C2 and data exfiltration in espionage campaigns against government and private sector targets.
- **APT35**, a.k.a Charming Kitten, an Iran-linked group, leverages cloud storage services (e.g., Google Drive, Dropbox) for file storage and C2 in espionage operations.
- **APT37**, a.k.a. ScarCruft or Temp.Reaper, linked to North Korea, is known for targeting South Korean entities, as well as organizations in Japan, Vietnam, and the Middle East. The group often leverages cloud services for C2 and data exfiltration.

TOP SERVICES ABUSED FOR C2 COMMUNICATION

The following services are the most abused for C2 communication, indicating that APT groups overwhelmingly prefer these platforms to disguise their C2 communications:


Github


Telegram


Dropbox


Webhook.site

TOP SERVICES ABUSED FOR PAYLOAD DELIVERY

The following services are the most abused for payload delivery, showing that attackers commonly use these platforms to host and distribute malware, taking advantage of their trusted reputation to evade detection:


OneDrive


Dropbox

TOP 10 CLOUD SERVICES ABUSED

Overall, Dropbox, OneDrive, and Telegram are the three most abused legitimate cloud services globally. The top 10 are:

1. Dropbox
2. OneDrive
3. Telegram
4. GitHub
5. Google Drive
6. Discord
7. OneHub
8. Mockbin
9. Slack
10. Webhook

ThreatLabz Research_Highlights

BlindEagle strikes Colombian insurance sector using BlotchyQuasar malware

Summary:
In June 2024, ThreatLabz detected new activity from BlindEagle (also known as AguilaCiega, APT-C-36, APT-Q-98), an APT actor targeting the Colombian insurance sector. BlindEagle used phishing emails impersonating the Colombian tax authority (DIAN) to deliver a variant of QuasarRAT known as BlotchyQuasar. The campaign aimed to steal banking and payment-related data, using advanced obfuscation techniques and a combination of compromised government accounts, dynamic DNS, and VPN services to hide its infrastructure. The attackers employed BlotchyQuasar's capabilities to monitor interactions with various financial services and log sensitive information from victim systems.

Delivery:
BlindEagle initiated attacks via phishing emails that spoofed DIAN, warning victims of unpaid taxes to create urgency. The email included a URL or PDF attachment with a link to a Google Drive folder containing a ZIP archive. This password-protected archive, hosted by a compromised Colombian government Gmail account, contained the BlotchyQuasar malware. The phishing emails were traced back to infrastructure leveraging the Powerhouse Management VPN service to hide the origin.

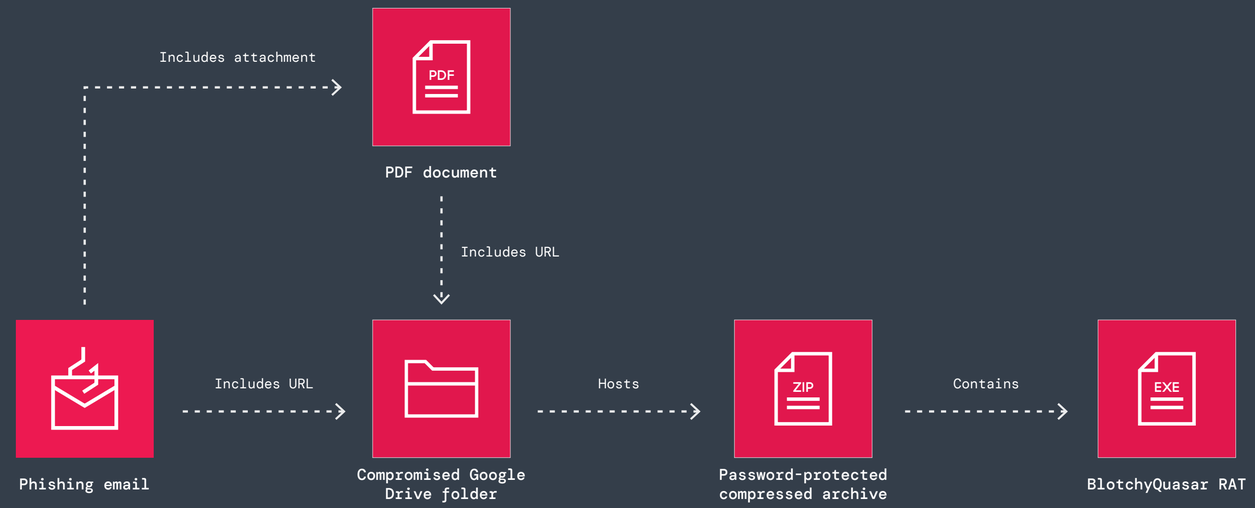


Figure 17: A high-level overview of a BlindEagle attack chain, where the initial phishing email includes a download URL for a password-protected compressed archive, and the final payload is a packed BlotchyQuasar sample

Network:
BlotchyQuasar retrieved its C2 domains from encrypted Pastebin posts. These domains resolved to dynamic DNS services and IP addresses linked to Colombian internet providers and compromised routers. BlindEagle's infrastructure primarily used VPN services, including Powerhouse Management and other Colombian ISPs, to protect their C2 infrastructure and obtain new IP addresses that closely match those of intended victims. Additional malicious domains associated with QuasarRAT and other malware were uncovered during the investigation, all of which are available in this blog post.

HijackLoader’s modular evolution showcases new capabilities and advanced evasion tactics

Summary:

HijackLoader, first observed in 2023, is a modular malware loader that can deliver a range of malware families such as Amadey, Lumma Stealer, Racoon Stealer V2, and Remcos RAT. In 2024, new evasion techniques were added to enhance its stealth capabilities. HijackLoader uses modules to bypass security measures, evade detection, and inject code into target systems. One of its unique features is using a decrypted PNG image to load subsequent attack stages. A Python script provided by ThreatLabz researchers can help decrypt and analyze the HijackLoader modules.

Delivery:

HijackLoader uses a modular architecture and delivers the next stage payloads through a PNG image that is either embedded or downloaded from the web. The malware families it distributes include Amadey (most prominent), Lumma Stealer, Racoon Stealer v2, and Remcos RAT.

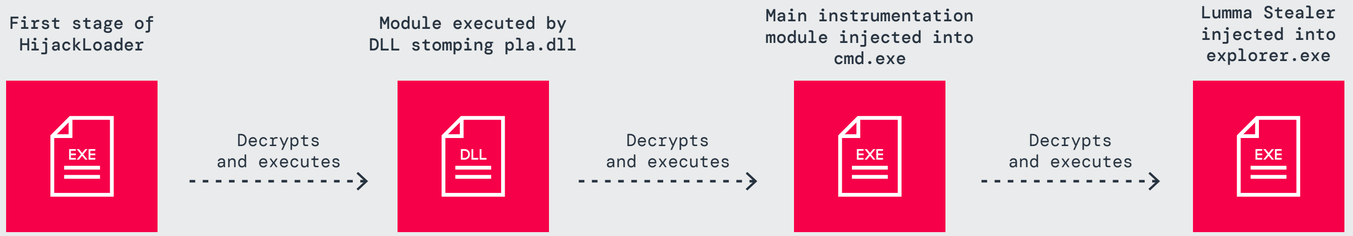
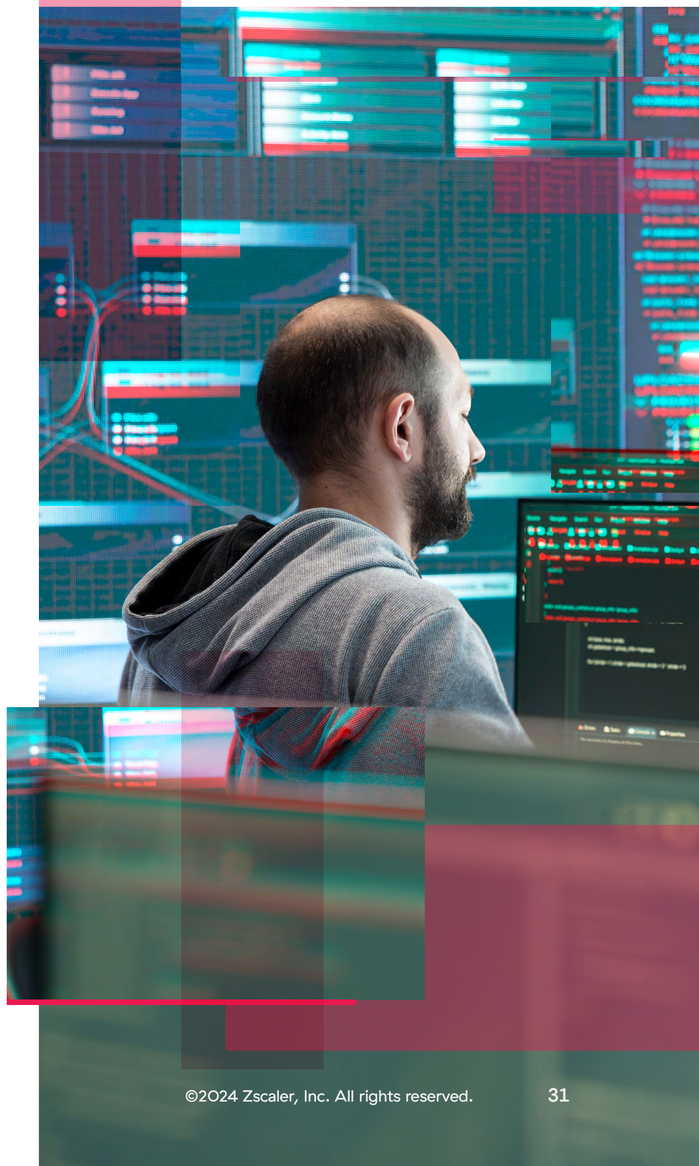


Figure 18: Attack chain showing how HijackLoader delivers Lumma Stealer

Network:

HijackLoader’s primary mechanism for reaching its targets is through its ability to decrypt and process PNG images, which hold encrypted modules. These modules include features like bypassing Windows Defender, UAC bypass, and user mode API hook evasion via the Heaven’s Gate technique. The loader also uses network resources to download the required PNG image, relying on APIs like WinHTTP for connectivity. Attackers also use WinHTTP APIs to check for an internet connection, without which the loader will not decrypt the modules.



APT29 (Cozy Bear) targets European diplomats with WINELOADER

Summary:

ThreatLabz uncovered a sophisticated cyberattack targeting European diplomats with a fake invitation to a wine-tasting event, leading to the installation of a backdoor called WINELOADER. The attack utilized a compromised website to host malicious payloads and was executed with advanced evasion tactics. APT29 leveraged a modular malware framework, indicating a possible nation-state actor focusing on geopolitical relations between India and Europe.

Delivery:

The infection began with a PDF file masquerading as an official wine-tasting event invitation from the Ambassador of India. Clicking the link in the PDF redirected users to a compromised website, downloading a ZIP archive containing malicious files. The infection chain relied on a sideloading technique using a legitimate Microsoft executable to deploy the WINELOADER malware, which downloaded additional modules from a C2 server.

Network:

The threat actors used compromised infrastructure to host both the initial payload and the C2 servers. The C2 communication employed advanced obfuscation and encryption techniques to evade detection, making the attack difficult to trace. The C2 servers were designed to respond only to specific requests, further enhancing evasion tactics and complicating analysis.

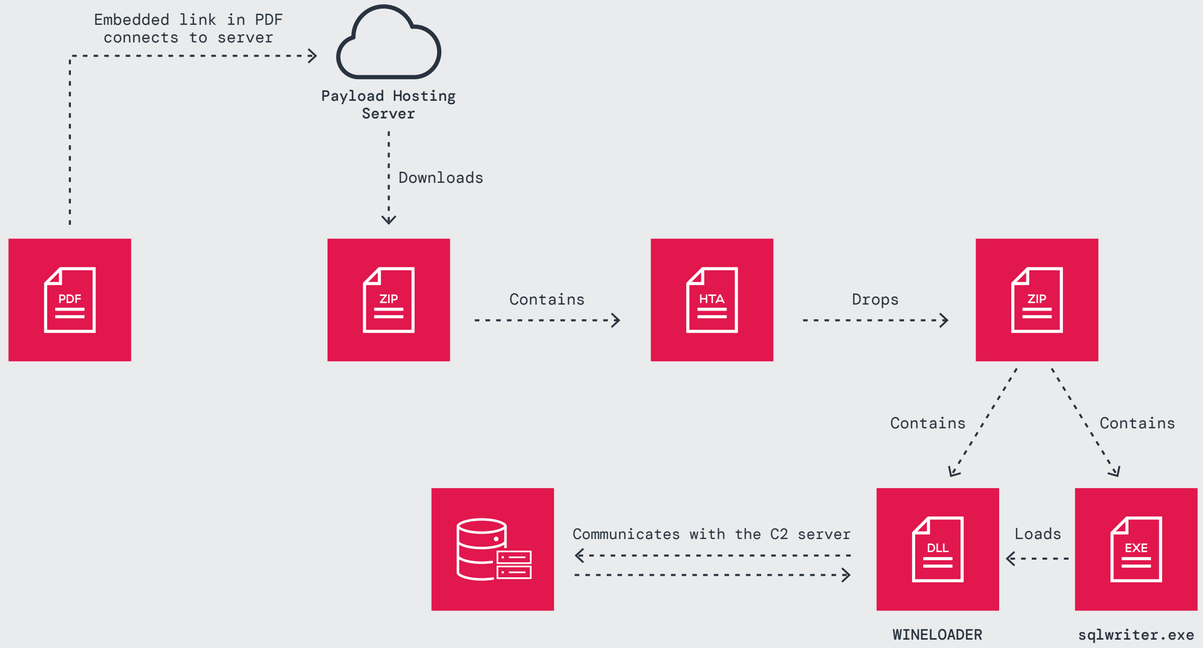


Figure 19: Multi-stage attack chain of WINELOADER

Analyzing the resurgence of Zloader

Summary:

Zloader, also known as Terdot, DELoader, or Silent Night, is a modular trojan that emerged in 2016 from the leaked Zeus source code, originally targeting German banks. Following a period of inactivity due to a takedown in April 2022, Zloader resurfaced in late 2023 with significant enhancements, including advanced obfuscation techniques, RSA encryption for network communications, and support for 64-bit Windows operating systems. The latest versions showcase a shift from banking fraud to ransomware tactics, reflecting the evolving threat landscape. Zloader continues to employ anti-analysis strategies, such as junk code, dynamic API import hashing, and more recently, execution restriction to the originally infected machine, which prevents the malware from being analyzed on different systems, making it more challenging for security researchers to analyze.

Delivery:

Upon infection, Zloader now checks a unique Windows registry key to prevent execution on any machine other than the one it first infected. The registry key is created using a hardcoded seed and acts as a verification checkpoint during the malware's operation. If the malware is moved to a new system, the registry check fails, causing the malware to terminate. Additionally, Zloader performs further checks, including verifying the machine's specific location path and configuration. This multilayered approach ensures that Zloader can only run within the precise environment of its initial infection, complicating reverse engineering.

Network:

The new iteration of Zloader incorporates sophisticated network communications frameworks that utilizes a combination of 1,024-bit RSA and RC4, alongside Zeus's visual encryption algorithm, for securing data exchange with its C2 servers. By employing updated obfuscation techniques and a refined domain generation algorithm (DGA) for backup C2 communications when primary servers are unavailable, Zloader can maintain operational effectiveness while evading detection. The malware's network structure is designed to obfuscate its activities, complicating efforts to trace its communications and infrastructure. ThreatLabz identified various botnet IDs linked to Zloader, indicating ongoing activity and potential for future ransomware campaigns as the threat group continues to evolve.

DodgeBox/MoonWalk

Summary:

In a recent pair of research articles, ThreatLabz examined the latest tools used by APT41, a China-based nation-state threat actor. These tools, DodgeBox and MoonWalk, represent highly sophisticated malware loaders and backdoors designed to evade detection and maintain long-term persistence on compromised systems. Both tools are part of an ongoing trend of nation-state actors leveraging modular and evasive tactics in their operations.

DodgeBox is a malware loader used to execute malicious payloads in-memory, evading detection by antivirus (AV) and endpoint detection and response (EDR) systems. It achieves this by using DLL hollowing, DLL unhooking, stack spoofing, and other stealthy techniques. ThreatLabz observed APT41 loading the MoonWalk backdoor, another APT41 tool that expands on DodgeBox's stealth capabilities.

MoonWalk is a modular malware backdoor designed for communication with an attacker-controlled C2 server. It can leverage Google Drive for C2 communication, blending malicious activity with legitimate network traffic. Like DodgeBox, MoonWalk uses advanced evasion techniques, including the abuse of Windows Fibers, a lesser-known Windows feature that further helps evade AV/EDR solutions by complicating the control flow. Together, these tools exemplify APT41's sophisticated tactics, showcasing a high level of skill and adaptability.

Delivery:

From Mandiant's reporting[5], the attack chain begins with APT41 compromising web servers of a targeted organization. APT41 then deploys a variety of malware on the web server and performs lateral movement to infect other hosts within the organization. There, DodgeBox is deployed to load the MoonWalk backdoor in-memory.

Once loaded, MoonWalk immediately unloads the DodgeBox DLL from memory to reduce its footprint and hide its origins. It then decrypts its configuration and loads embedded plugins. MoonWalk includes at least two embedded plugins—one for C2 communication and another for utility functions like public-key cryptography and compression. In total, MoonWalk has been observed to use at least 15 different plugins. Such a modular architecture allows MoonWalk to be customized and updated by attackers to fit different attack scenarios.

Lastly, MoonWalk begins communicating with its C2. In the sample analyzed by ThreatLabz, MoonWalk was configured to communicate using Google Drive as a channel.

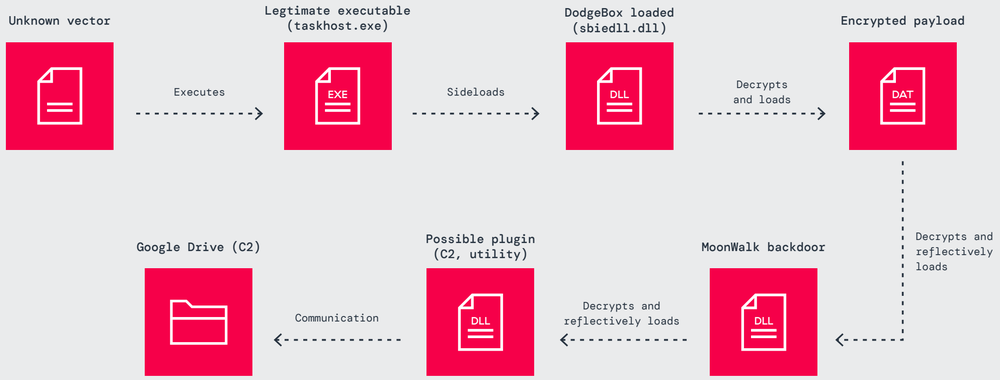


Figure 20: Attack chain used to deploy the DodgeBox loader and MoonWalk backdoor

Network:

MoonWalk utilizes a custom C2 protocol that leverages Google Drive to blend in with legitimate traffic. This is effective in evading detection as enterprise environments are less likely to flag traffic directed at trusted cloud services. The C2 protocol includes several layers of encryption to secure communication between the infected system and the attacker's infrastructure.

The protocol starts with a cryptographic handshake, where MoonWalk generates AES secrets and leverages public key cryptography to exchange these secrets with the C2 server. Once the keys have been exchanged, MoonWalk communicates by uploading and downloading encrypted files to and from an attacker-controlled Google Drive account. These files can contain heartbeat messages, which MoonWalk regularly sends to the server, as well as system information, commands to execute, and their results. This is a critical component of encrypted attacks, as the use of strong encryption methods makes it difficult for security measures and analysts to intercept and analyze the data being transmitted.

[5] https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust

2025_ Predictions

1. Artificial intelligence and automation will power an upswell of encrypted threats.

These advancements will empower threat actors to execute highly sophisticated, elusive strategies—ranging from realistic, AI-generated spear-phishing emails to malicious content and novel threats that abuse TLS/SSL channels, bypassing conventional security with ease. Generative AI in particular will allow attackers to scale their efforts, launching convincing, localized attacks through encrypted channels, making detection even more challenging.

2. Threat actors will archive encrypted communications for future post-quantum decryption.

More and more threat actors will attempt to archive encrypted communications with the intent to decrypt them once post-quantum cryptography becomes viable. With milestones in quantum computing, such as NIST's August 2024 release of the first finalized post-quantum encryption standards, the focus on post-quantum cryptography is intensifying. Although cryptanalytically relevant quantum computers are not expected until the 2030s, threat actors will prepare for a future where quantum computing can break today's encryption. In response, organizations should prioritize adoption of post-quantum encryption standards to defend against future decryption threats and ensure long-term data security.

3. Abuse of legitimate cloud services will be a key factor in encrypted attack growth.

As organizations increasingly rely on trusted cloud services, threat actors will abuse these platforms to facilitate encrypted attacks, hosting malicious content and exfiltrating sensitive data over secure channels. Leveraging widely used cloud platforms and their wildcard certificates, attackers will conceal their activities within legitimate traffic, adding significant complexity to defense efforts. This trend highlights the need for advanced monitoring and inspection of encrypted traffic across cloud environments.

4. APTs will increasingly abuse encrypted channels to conceal their activities.

Nation-state-backed APT groups, in particular, will use their substantial resources and expertise to abuse weaknesses in encrypted protocols to infiltrate target networks, posing heightened risks to entities such as government agencies and critical infrastructure.

5. Encrypted C2 activity will become even stealthier.

As organizations deploy AI-driven defense systems to swiftly detect volume-based anomalies, volumetric C2 traffic will decline and attackers will increasingly turn to encrypted, low-profile methods. Minimizing the volume and signature of C2 communications within encrypted channels will allow attackers to evade detection by security systems that rely on this volume-based anomaly detection, setting a new standard for sophisticated threat tactics and challenging traditional detection approaches.

How the Zscaler Zero Trust Exchange Stops Encrypted Threats

Enterprises need to go beyond traditional security to defend against encrypted threats—and to do this effectively, a zero trust architecture is essential: every user, device, application, and workload must be verified through multiple layers of identity, context, security, and policy checks before access is granted.

Understanding how zero trust disrupts encrypted threats requires looking at a typical attack sequence. Advanced attacks often unfold in four stages:

1. First, attackers conduct reconnaissance to **find a way in**.
2. Next, they **breach the network**, often via exploits, brute-force attacks, or stolen credentials.
3. Once inside, they **move laterally**, escalate privileges, and establish persistence.
4. Finally, they carry out their objectives, typically conducting **data exfiltration** to extract valuable information which can be leveraged for further extortion or attacks.

The **Zscaler Zero Trust Exchange™** platform provides security controls at each stage to mitigate risk and stop encrypted threats.

A key component of the Zscaler platform's approach is its full TLS/SSL inspection capabilities, based on an advanced proxy architecture. Zscaler advises inspecting 100% of traffic to protect your users and organization from threats concealed within encrypted channels. With full inspection, you reap the benefits of the Zero Trust Exchange—without it, encrypted threats can slip by undetected, hiding in plain sight.

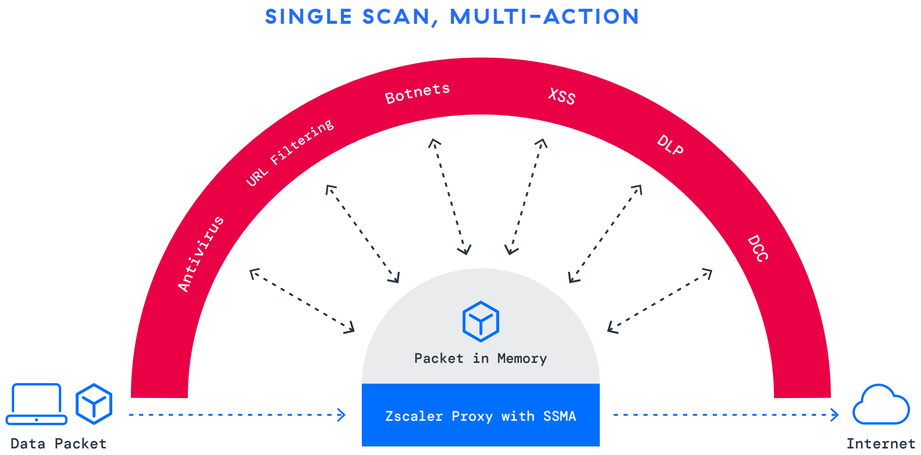


Figure 21: Inspect all traffic at scale, including TLS/SSL, with our unique Single Scan, Multi-Action™ engine. Apply layered, inline, AI-powered security controls and stop threats without disrupting user productivity.

Minimize the attack surface

Encrypted traffic flows between users and applications, often under an assumption of implicit trust—meaning anyone who can access the network should be able to connect to any application within. However, when encrypted connections—via VPNs, exposed workloads, or other methods—are unchecked, they expand the attack surface by allowing threat actors to hide within encrypted channels.

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 abused. Zscaler eliminates this attack surface by ensuring that applications and services remain invisible to the internet. This approach stops encrypted threats from reaching applications, providing a proactive defense that doesn't rely on shared network access.

Prevent initial compromise

Zscaler places internet–facing applications behind the Zero Trust Exchange. Our global security cloud comprises 160 data centers that collectively act as a proxy, providing a single entry and exit point for all traffic while ensuring comprehensive traffic visibility and control. **Zscaler Internet Access™** (ZIA) performs full TLS/SSL inspection to verify every connection and stop hidden threats without sacrificing performance. ZIA's inspection capabilities leverage AI–powered analysis and inline detection to quickly identify and block sophisticated threats within encrypted traffic. This approach eliminates the need for traditional, resource–intensive physical appliances, allowing organizations to handle encrypted traffic growth easily and continuously.

Eliminate lateral movement

Once attackers gain a foothold, they often seek to move laterally. Zscaler stops lateral movement through advanced segmentation and AI–powered, context–aware policies. **Zscaler Private Access™** (ZPA) limits users' access to only specific applications based on identity, context, and policies. This approach replaces complex rule–based network segmentation with simple, identity–based access control. Additionally, Zscaler uses **deception technology** to lure attackers with strategically placed decoys that alert on unauthorized lateral movement attempts and malicious activities in encrypted channels.

Block C2 callback

Malware often attempts to reach C2 servers. This contact allows attackers to take over machines, issue additional commands, download additional malware, or steal data. ZIA disrupts these communications by inspecting both outgoing (northbound) and incoming (southbound) encrypted traffic, blocking any unauthorized C2 connections. The platform's built–in **data loss prevention tools** detect and halt malicious outbound traffic, protecting sensitive data from exfiltration and preventing encrypted C2 callbacks from compromising the network.

THE ZERO TRUST EXCHANGE ADVANTAGE

The Zscaler platform operates on the "cloud effect," harnessing threat intelligence from more than 500 trillion daily signals and over 500 billion daily transactions to refine and strengthen protections across its entire customer base—meaning that any threat detected on the global network enhances protections for all Zscaler customers.

Wipro secures encrypted traffic with Zscaler

By replacing traditional firewalls and VPNs with Zscaler, **Wipro** strengthened its defenses with inline TLS/SSL inspection of all internet and SaaS traffic to detect and block encrypted threats.

8.2M **Encrypted threats blocked** (in one quarter)

8.1B **Policy violations prevented** (in one quarter)

30% **Boost in workforce productivity**

Best_Practices for Preventing Encrypted Threats

Organizations can bolster their ability to protect their devices, apps, and data from encrypted attacks by following these recommendations:

- **Understand that any internet-facing service can be found and attacked or abused.** This includes firewalls, whether in the data center, cloud, or branch .
- **Inspect incoming encrypted traffic to detect and block threats.** An online proxy based architecture is ideal because it enables decrypting, detecting and preventing threats in all encrypted traffic at scale. If your organization uses a secure web gateway, ensure it is configured to decrypt and inspect encrypted traffic.
- **Use a zero trust architecture to secure all connectivity holistically** between users and applications, between devices like IoT and OT systems. This empowers enterprises to inspect all traffic, all the time—improving security while simplifying operations.
- **Implement microsegmentation to reduce access, even for authenticated users.** By creating one-to-one segments that are brokered and authenticated by zero trust architecture, users are connected directly to requested application without ever exposing the network.
- **Leverage an AI-driven cloud sandbox to isolate and quarantine unknown attack** and stops patient-zero malware before 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 C2 communications and protect your sensitive data.

Report_ Methodology

Analysis of 32.1 billion blocked threats from October 2023 to September 2024 in the Zscaler cloud shows that all blocked threats came via encrypted channels.

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**.

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 160 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.**