



# State of Encrypted Attacks 2022

# Contents

Introduction	3
Key findings	4
The Encrypted Threat Landscape	5
Top threat categories	7
Malware	7
Ad Spyware	8
Phishing	9
Cryptomining and cryptojacking	10
XSS	11
Botnet Callback Attempts	12
Mobile and IoT attacks	13
Top targeted geographies	14
Top industries	15
Comparing SSL Certificates	16
Predictions	17
What's needed to prevent encrypted threats	18
How the Zscaler Zero Trust Exchange stops encrypted threats	19
Malware case studies	21
Gamaredon	21
Lyceum	23
QuasarRAT	24
Qakbot	25
Phishing case studies	26
Mobile/IoT case studies	31
About ThreatLabz	33
About Zscaler	34

# Introduction

## Is encrypted traffic safe? Not always.

HTTPS protects data from prying eyes as it's transferred from a web server to a browser. In the early days of the Internet, HTTPS was used only when sensitive data was being transferred. Since then, the industry has recognized the benefits of using HTTPS to protect all data. Encrypted traffic can be anything: a username and password, a credit card number—even malware.

As HTTPS has become the standard for transmitting data over the Internet, users and organizations have come to expect it. Most have been trained to look for the little lock in their browser bar. To be successful, attackers too must use HTTPS to avoid raising suspicions. Just as HTTPS protects sensitive user data from prying eyes, it can now inadvertently also protect malicious code. Not only is encrypted traffic less likely to be inspected by security teams, but encrypted files are much harder to fingerprint, allowing malware to slip by undetected.

Indeed, a lot is slipping by. Between October 2021 and September 2022, Zscaler blocked 24 billion threats over HTTPS. This represents a 20% increase from the 20.7 billion threats blocked in 2021, which itself was a 314% increase from the year prior.

Cybercriminals continue to evolve their tactics to avoid detection and take advantage of computing trends, such as hybrid work. However, the availability of malware— and ransomware as a service eliminates the entry barrier for new cybercriminals. They no longer have to know how to write their own code or need to set up the operational infrastructure to launch and maintain a ransomware campaign. Everything they need is available on the dark web as a service.

Organizations must inspect all traffic, on premises and off, to reduce the risk of an encrypted threat making its way into the enterprise. Unfortunately, such inspection is incredibly resource intensive. Inspecting traffic at scale with legacy hardware—based security tools is nearly impossible. It can take, for example, five to seven times the number of next—generation firewalls to effectively inspect encrypted traffic without diminishing performance. As a result, many organizations allow at least some of their encrypted traffic to pass through uninspected, exposing themselves to significant risk.

# Key Findings

The Zscaler Zero Trust Exchange houses the largest security data set in the world, collected from more than 300 trillion signals and 260 billion daily transactions. The Zscaler ThreatLabz threat research team analyzed threats in encrypted traffic from October 2021 to September 2022. The following analysis sheds critical insights into the encrypted attack landscape. Key findings include:



**More than 85% of attacks now use encrypted channels** across various stages of the kill chain (phishing, malware delivery, C&C activity, and more), up from 80% last year



**Threats over HTTPS have increased:** Zscaler has seen a 20% year over year increase in encrypted threats.



**Manufacturing is a huge target:** Encrypted threats targeting the manufacturing industry increased year over year by **239%**.



**Encrypted threats targeting retail and government decreased:** Retail saw a **63%** drop in encrypted threats and government a **40%** decline since last year.



**The US and India are the top targets of encrypted attacks:** South Africa, the UK, and Australia round out the top five.



**Encrypted attacks are growing both in volume and sophistication:** Zscaler blocked more of every single threat type over SSL/TLS in 2022 than in 2021.



**Zero trust is the best defense against encrypted threats:** Use a cloud proxy—based zero trust architecture that reduces your attack surface and allows you to inspect all traffic in—line and at scale.

# The Encrypted Threat Landscape

Modern encryption, including Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) is used globally to protect the majority of internet traffic. [According to Google](#), 95% of the traffic it generates is encrypted. As the rates of encryption for legitimate traffic increase, they do for malicious traffic as well.

For the third consecutive year, the number of encrypted threats blocked by Zscaler increased both in overall volume and as a percentage of overall attacks. This is a testament to the continuously growing adoption of new tactics by threat actors.

Zscaler blocked 24 billion threats during a nine month period in 2022, a 20% increase over 2021. More than 85% of all attacks blocked over that period of time utilized encrypted channels.

There are various types of attacks that criminals can hide in encrypted traffic. Malware is still by far the most commonly observed threat category, though it's down from 90.8% to 89.8% of attacks as other categories grow. Malware includes [ransomware, a top concern for CISOs around the world](#) (and for good reason). Ransomware attacks alone increased 80% year over year.



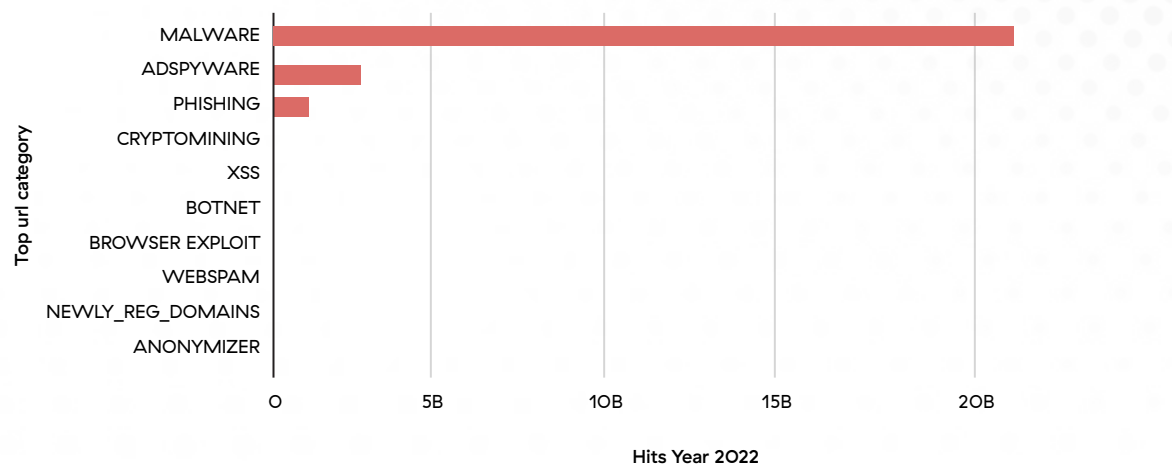
Encrypted attacks are growing both in volume and sophistication. Zscaler blocked more of every single threat type over SSL/TLS in 2022 than in 2021. Some of the relatively less common categories, like webspam and browser exploits, which each only account for less than .1% of all attacks, are growing the fastest. Webspam grew 1,642%.

Phishing via encrypted channels grew 89% year over year. Our recent [State of Phishing report](#) showed that phishing overall only increased 29%, which indicates that the use of encrypted channels in phishing attacks is growing substantially. This is likely due to the prevalence of phishing kits and increased adoption of the phishing as a service model that both lower the technical barriers to these attacks.

Despite the drop in the price of cryptocurrency in 2022, and declining profits for miners, cryptojacking remains the fourth most popular threat and experienced significant growth, 144% year over year, after previously experiencing a year over year decrease in 2021.

Methodology: Analysis of 24 billion blocked threats via SSL and TLS channels from October 2021 to September 2022 in the Zscaler cloud.

### Encrypted attacks by type



Delta 2022 vs 2021:	
WEBSHAM	1641.65%
BROWSER EXPLOIT	188.63%
CRYPTOMINING	144.44%
PHISHING	89.07%
XSS	81.27%
MALWARE	13.98%
AD SPYWARE	6.47%
BOTNET	3.49%

# Top threat categories

## Malware: 89.9% of attacks

Malware was the top category of attacks in 2022. Malware is typically delivered by users downloading a malicious payload from a link via email and websites. While most organizations have some form of protection against malware, attackers are evolving their techniques, creating new malware variants that are able to bypass reputation-based detection technologies.

As a result, organizations that don't inspect encrypted traffic are unable to detect malware until after it has infected their systems. Below are the most prevalent malware families observed in 2022.

While cybercriminals hide a variety of attack tactics in encrypted traffic, malware continues to be the most prevalent. Malicious scripts and payloads used throughout the attack sequence make up nearly 90% of the encrypted attack tactics blocked in 2022.

**ChromeLoader** 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.

**Gamaredon**, also identified as Primitive Bear, Shuckworm, and Actinium, is a custom Russian APT known to target Ukrainian government agencies and critical infrastructure. The multiplatform malware gains a foothold, opens up a backdoor, fingerprints systems for later attack, and steals critical information.

**AdLoad** targets macOS and evades built-in macOS security tools and third-party antivirus programs. A form of adware, AdLoad contacts obscure URLs and downloads unwanted software without the user's knowledge.

**SolarMarker** is known for its infostealing and backdoor capabilities. The malware is mainly delivered via SEO poisoning, an attack method in which threat actors create malicious websites packed with keywords and use search engine optimization techniques to make them show up prominently in search results.

**Manuscript** is a remote access tool (RAT) used to target cryptocurrency exchanges and related entities. Manuscript is capable of running arbitrary commands, performing system reconnaissance, and exfiltrating data.

## Ad Spyware: 6.3% of attacks

Encrypted ad spyware continues to be a menace for users. Ad spyware experienced just a slight decline, from 6.8% in 2021 to 6.3% of all encrypted attacks in 2022. Attackers disseminate ad spyware by bundling it with other software. Users blindly accept the software terms and conditions, and the ad spyware is installed on the system, unbeknownst to the user until they are bombarded with multiplying pop up ads. The top ad spyware families in 2022 include:

**Popads** is a legitimate advertising network used by website publishers to generate revenue. However, some adware redirects to Popads.net and displays fraudulent advertisements on the end user's computer.

**Searchprotect** changes the user's web browser to a different home page and search engine and prevents the user from changing them back. Opening a new browser tab triggers an endless stream of advertisement pop-ups with no "close" option.

**PremierOpinion** displays surveys on shopping websites. It monitors and transmits the user's activity, including internet browsing activity, demographics, and application usage. PremierOpinion impacts browser and CPU performance.

**MindSpark** modifies default browser settings and alters search settings. It can also impact browser performance and block competing software. MindSpark may also change the user's homepage and barrage the user with pop up ads.



## Phishing: 3% of attacks

Encrypted phishing attacks nearly doubled this year, from 1.8% in 2021 to 3% in 2022. Phishing uses social engineering to convince the recipient in an email or text message to share sensitive information or to click on a link containing hidden malware. The email or text message often purports to be from a trusted brand, and any brand is fair game.

However, cybercriminals tend to leverage popular brands and topics in an attempt to catch users of that brand or to appeal to current public interests, as in the case of COVID—19. As many users continue to work from home at least part time and the COVID—19 pandemic remains top of mind, we weren't surprised to find 2022's top phishing topics similar to 2021.

### Top encrypted phishing themes in 2022:



# Cryptomining and cryptojacking: .5% of attacks

Cryptomining software is designed to do just that: mine cryptocurrencies. Similarly, cryptojacking is used by cybercriminals to hijack a target system's computational power to mine cryptocurrency on the attacker's behalf. Cryptojacking impacts enterprise networks in various ways. Unwanted and unidentified mining activity inside networks causes increased wear and tear on corporate hardware, as the mining increases CPU cycles. Mining activity also hogs corporate network bandwidth and causes performance issues.

Cryptojacking made a comeback in 2022, growing more than 144% last year after experiencing a decrease in the year prior. It's likely that cybercriminals recognized the opportunity to exploit the computational power of users as they shifted into a hybrid work mode, working part of the time at home and the other part in the office.

## Top cryptojackers in 2022 include:

**Xmrig** is an open source cryptojacker that can be integrated with other malware. Xmrig itself does not steal sensitive information or encrypt data. Its sole purpose is to mine cryptocurrencies, so its impact is primarily the consumption of resources and the effects of this usage.

**ThetaToken** is a blockchain powered by a decentralized network where users share resources and video content. Through the platform, users stream videos by offering their bandwidth and additional computing resources in exchange for rewards, which are called Theta Tokens.

**ElectrumStealer** is a Trojanized version of a popular Bitcoin wallet service called Electrum. ElectrumStealer exfiltrates passwords and other coin—related data to a server the cybercriminal controls on the Electrum network. ElectrumStealer targets macOS.

**Webmine**, like Coinhive, is embedded in websites. The JavaScript miner enables website publishers to leverage their visitors' CPU power to earn Monero.

**CoinIMP** is a JavaScript miner that is embedded in websites. CoinIMP pitches itself as a way for users to pay website publishers for their content with their CPU resources. The web miner isn't blocked by antivirus or adblocker software. If it does get blocked, the creators react and work hard to unblock it.

## XSS: .2% of attacks

Cross-site scripting (XSS) made a small increase from .1% of encrypted attacks in 2021 to .2% of encrypted attacks in 2022. In a XSS attack, cybercriminals inject malicious code into legitimate websites.



# Botnet Callback Attempts: .2% of attacks

## Top malware families by CnC activity blocked over HTTPS

A botnet is a network of computers that have been infected with malicious software and is remotely controlled by a cybercriminal to carry out attacks. Botnet callback activity originating from infected systems comprised .2% of all encrypted attacks for the second year after previously skyrocketing in 2021, up 132% from 2020.

**SmokeLoader** is a Trojan that cybercriminals primarily use to drop other malware on infected systems. However, SmokeLoader can also be extended via plugins that provide information stealing capabilities. The Trojan is distributed by exploit kits and email campaigns and by being offered as a legitimate application.

**Gumblar** is a Trojan that injects malicious JavaScript code into a website pages or a user's web browser. Gumblar redirects a user's Google searches and then installs rogue security software via a PDF vulnerability.

**RecordBreakerStealer** is a revived version of Raccoon Stealer. It is sold as a Malware-as-a-Service (MaaS). As an infostealer, RecordBreakerStealer is designed to exfiltrate data and content from the infected system. The malware's simplicity and support service have made it popular amongst cyber criminals.

**Cobalt Strike** is commercial penetration testing software that is marketed to ethical hackers. However, the software is also used by cybercriminals. The software provides a variety of capabilities that cybercriminals leverage to carry out various attacks, from ransomware operations to espionage focused advanced persistent threats (APTs).

**QuasarRAT** is a fully functional and open source Remote Access Trojan (RAT) that primarily targets Microsoft Windows OS. QuasarRAT has been publicly accessible on GitHub since at least 2014. QuasarRat features a variety of techniques and capabilities, including a built-in keylogger, and the ability to obtain passwords and retrieve files from compromised machines.

**Occamy** is also a RAT used by cybercriminals to gain access to a target system. Once on the infected system, the cybercriminal can use Occamy to disable security programs, steal data, enroll the host in a botnet, drop additional malware on the system, and more. Occamy is often spread through fake email spam campaigns as well as software cracks or keygens downloaded from the internet.

## Mobile and IoT attacks

Attackers leverage mobile and IoT devices for a variety of malicious actions, ranging from hyper-targeted, such as hiding malware on smartphones to bypass MFA, to incredibly broad, such as botnet attacks that leverage IoT devices, to wage large-scale distributed denial of service (DDoS) attacks, scraping, cryptojacking, and spam attacks.

Attackers frequently gain access to mobile devices through SMiShing, a form of phishing that utilizes SMS messages, malicious mobile websites, and fraudulent apps hiding in app stores. In a recent three-month period, ThreatLabz [reported more than 50 malicious apps that generated an excess of 500k downloads](#), embedding such malware families as Joker, Harly, Coper, and Adfraud.

### Top mobile malware families include:

**Multiverze**, a ransomware that targets AndroidOS. Multiverze encrypts the information on the user's device or prevents it from operating correctly. The user is presented with a ransom note that states the requirements for decrypting the data or returning to regular operations.

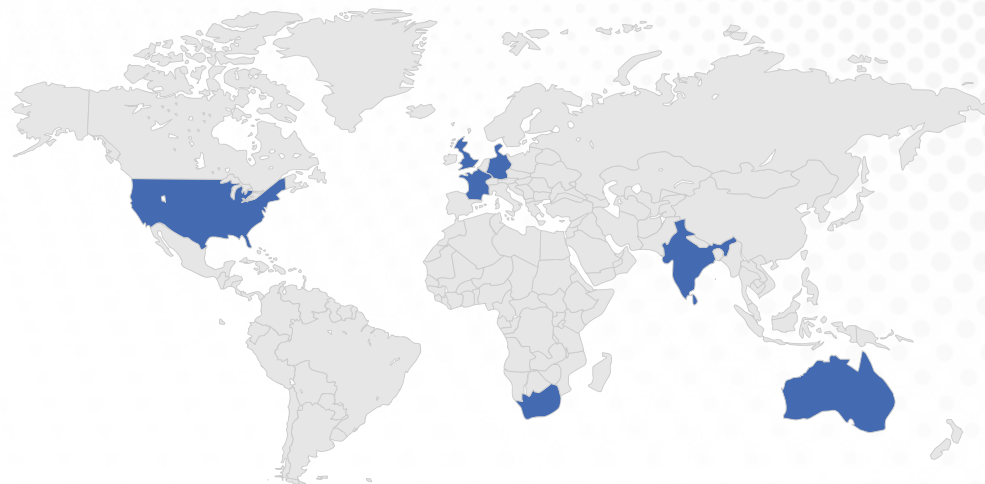
**Mirai**, a botnet that uses brute-force techniques to attack Internet of Things (IoT) devices through various protocols. Mirai also exploits vulnerabilities in IoT devices to infect other IoT devices. These vulnerabilities are mostly in management frameworks and, by exploiting them, cybercriminals achieve remote code execution. Infected devices are often turned into bots as part of a larger botnet army. Mirai has been one of the most prolific IoT malware families for years, waging what was the largest DDoS attack in history back in 2016. In 2021, [76% of the attacks that Zscaler blocked on IoT devices were from the Mirai family](#).



# Top targeted geographies

The five countries most targeted by encrypted attacks include the US, India, South Africa, the UK, and Australia. South Africa is a newcomer, having soared to the top of the chart in 2022 and bumping France from the top five, where it previously ranked fifth in 2021. South Africa had 3,112% more hits via TLS and SSL this year compared to last, becoming the third highest-attacked country in 2022.

Cybercriminals also shifted their focus to Japan, the US, and India, which increased 613%, 155%, and 87% respectively, year over year.



Growth in attacks by Country, 2022 vs 2021			
South Africa	3112.33%	Canada	87.49%
Japan	613.1%	India	86.59%
Russian Federation	544.95%	Spain	84.46%
Germany	352.37%	Malaysia	56.66%
United Arab Emirates	316.81%	United Kingdom	40.43%
Singapore	185.73%	Brazil	32.21%
Switzerland	162.75%	Australia	-21.78%
United States	154.73%	Philippines	-24.32
France	146.22%		
Netherlands	106.90%		
Italy	103.13%		

# Top industries

More than doubling in encrypted attacks, manufacturing displaced technology as the most targeted industry in 2022. Attackers appear to favor manufacturing, as the industry is a particular target for ad spyware when compared to other industries. It is also one of the two most phished industries via encrypted channels—the other being health care—leading other sectors substantially. Manufacturing has undergone significant transformation in the last several years in attempting to manage COVID-19 restrictions and supply chain bottlenecks. This has led to adoption of new applications, products, and services that increase the industry’s attack surface and expose new vulnerabilities.

The education and healthcare industries also experienced notable increases in encrypted attacks in 2022. Education saw a 132% year over year increase in attacks that follow a 50% increase last year. Healthcare saw a 34% increase in 2022 after a 27% increase in 2020.

Meanwhile, attacks against technology vendors via TLS and SSL decreased 6% year over year, after previously accounting for roughly 50% percent of total hits in 2021. Other industries that experienced a decrease in attacks over encrypted channels include retail, which fell 63 percent; government, which decreased by 40 percent; and finance and insurance, which declined by 5%.

Retail saw an 842% spike in encrypted attacks last year, likely a result of attackers taking advantage of infrastructure changes during the pandemic. Attacks against retail this year are still highly elevated from 2020 attack numbers, but normalized a bit from the massive 2021 spike.

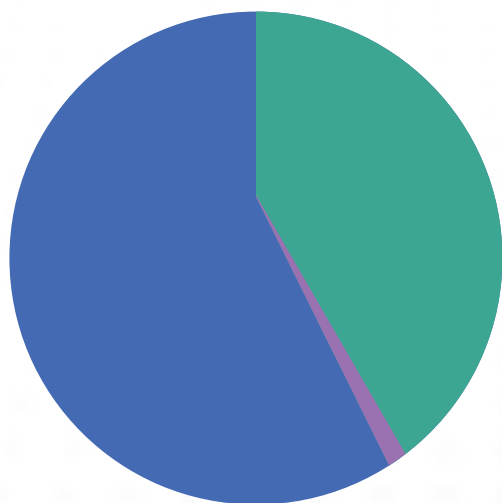
Attacks against government organizations decreased for the second year in a row, dropping by 10% in 2021 and 40% in 2022. Law enforcement has been cracking down on impactful cyberattacks against government and other critical industries, making them less attractive targets for criminals looking for easy money.

Industry Vertical	2022 vs. 2021
Education	133.77%
Finance/Insurance	-5.20%
Government	-39.60%
Healthcare	33.92%
Manufacturing	239.10%
Others	312.76%
Retail/Wholesale	-63.45%
Service	108.27%
Technology/Communication	-6.24%

# Comparing SSL Certificates

While all SSL and TLS certificates verify identity and allow for encrypted connections, there are different types of certificates that represent different levels of information being verified.

## Type of Certificate abused



OV 56.0% ■ DV 42.8% ■ EV 1.3% ■

**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, used by only 21% of the Fortune 500 companies as of 2021. 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.

Zscaler ThreatLabz found that almost 99% of malicious SSL traffic from October 2021 to October 2022 used either OV or DV certificates. EV certificates represented only 1.3% of traffic. It is notable that a majority of malicious traffic used certificates that required higher levels of verification, indicating the popularity of attackers compromising legitimate websites of trusted organizations in order to carry out attacks.



# Predictions

- 1. Growth in the as—a—service cybercriminal marketplace will continue to drive more attacks over encrypted channels.** Criminals can now simply pay for powerful malware and attack resources, allowing them to wage sophisticated attacks regardless of their own technical prowess. As the as—a—service model gains further popularity, more and more attacks will include evasive tactics, including encryption.
- 2. Organizations using legacy infrastructure will struggle with provisioning decisions.** It takes 10 times the amount of computation to inspect encrypted channels than it does to inspect unencrypted ones. This growth in encrypted traffic makes capacity planning for organizations relying on hardware a bit of a nightmare. They risk wasting money on firewalls that are way bigger than they need, or they risk running out of resources and potentially choosing not to inspect traffic that they really should.
- 3. Encrypted attacks will increase in 2023.** Encrypted attacks will continue to be the preferred method of delivering cyberthreats as adversaries predictably sync tactics and techniques with mainstream practices. With the majority of all traffic already being encrypted today, you can still expect to see an increase in the volume of encrypted threats over the next several years as novice threat actors bridge skill gaps to catch up with the crowd. To prepare for this reality, your security plan should include a permanent strategy for protecting against threats hidden within encrypted traffic.
- 4. Encrypted data exfiltration for extortion will surge.** As more ransomware adversaries adopt multi—extortion tactics to make victims pay, you can expect to see rising incidents of sensitive data theft. To bypass firewalls and other legacy security technology, adversaries encrypt data troves before transferring them out of the target’s environment.
- 5. Security standards for encrypted traffic will be under review.** Expect more attention around updating regulatory framework requirements to include security standards for analyzing encrypted traffic. Additional discussion that brings this topic to center stage is also anticipated.
- 6. Attacks will be harder to catch.** During this last year we saw the threat group Lapsu\$ appear in headlines, using a unique range of scrappy tactics to compromise organizations and exfiltrate valuable data with a rapid smash and grab approach. This should be a wake—up call for defenders and security leaders that time has run out on the previous luxury of building strategies around tidy linear attack chains with numerous events to detect, known indicators, and predictable adversarial techniques. The time is now to prepare for this new wave of potential threats that will surely come in 2023 and the years to follow. It is critical that your defenses focus on each stage of the attack cycle as if it is the only opportunity you will have to detect and stop an attack.

# What's needed to prevent encrypted threats

The data speaks for itself. Encrypted traffic carries malware and other threats. We've seen this trend increase over the last couple years, and we have every reason to believe that cybercriminals will continue to leverage encrypted traffic as a threat vector. The only way to stop encrypted threats is to inspect traffic. All of it.

Inspecting encrypted traffic hasn't always been practical. Fully inspecting traffic with legacy tools is costly and impacts performance. In addition, some regulations require different policies for distinct data types, making inspection an arduous task. Today, however, we have tried-and-true strategies that enable organizations to inspect all encrypted traffic without impacting performance or creating a compliance nightmare. We recommend that you:

- Use a cloud-native, proxy-based architecture to decrypt, detect, and prevent threats in all encrypted traffic at scale.
- Leverage an AI-driven sandbox to quarantine unknown attacks and stop patient-zero malware.
- Inspect all traffic, all the time, regardless of whether a user is at home, at headquarters, or on the go, to ensure that everyone is consistently protected against encrypted threats.

Start from a position of zero trust, which reduces the attack surface by preventing lateral movement. Zero trust renders apps invisible to attackers and, rather than access the entire network, authorized users only access the resources they need.

The solution requires the scalability and performance that can only be delivered by a cloud native, proxy-based architecture such as the Zscaler Zero Trust Exchange™. It is only cloud-based security platforms that meet the demands of decryption and inspection by elastically scaling computing resources. The Zscaler Zero Trust Exchange provides consistent policy enforcement across multiple locations.

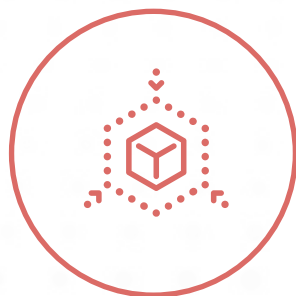
A multilayered, defense-in-depth strategy that reduces the attack surface and fully supports HTTPS inspection to surface hidden threats is essential to ensure that enterprises are protected.

# How the Zscaler Zero Trust Exchange stops encrypted threats

Trust no one. That is the guiding principle behind a zero trust strategy and architecture. Security controls are implemented based on the idea that anyone can have malicious intentions. The goal, therefore, is to reduce the scope of an attack by limiting visibility and access to network resources.

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

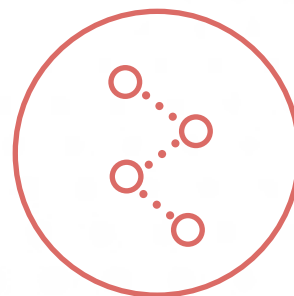
the network, often through an exploit, a brute-force attack on an exposed asset, or stolen credentials. Once inside, the cybercriminal moves laterally through the network, escalating privileges and establishing a network foothold. Finally, attackers carry out their objectives, usually data exfiltration. The Zscaler Zero Trust Exchange provides security controls at each stage of an attack to holistically reduce risk.



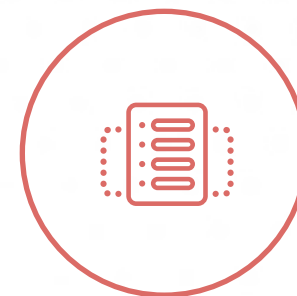
**Minimize the attack surface**



**Prevent compromise**



**Stop lateral movement**



**Stop data loss**

**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 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.

# Malware case studies

## Gamaredon

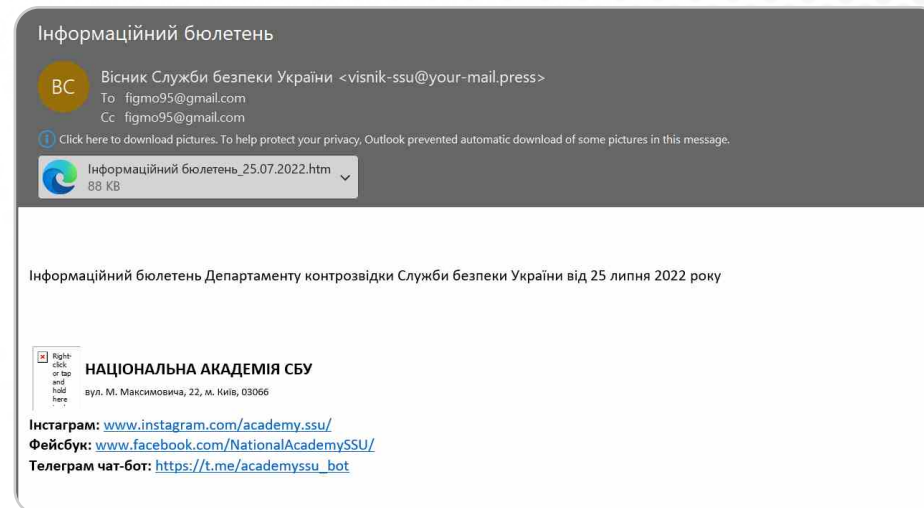
### Summary

Gamaredon APT has been active since 2013 and is known for targeting the Ukraine government, thereby increasing the tension between Russia and Ukraine. This threat group is known for creating custom malware with embedded advanced capabilities that allow them to exfiltrate victims' data to attacker—controlled servers. The malware uses the following techniques to evade security tools:

- It tries to bypass sandbox detection by delaying the execution of the malware using Windows APIs such as SleepEx, NTDelayExecution, until the sandbox analysis has ceased. It lures the victim with decoy documents.

### Delivery Mechanism

Attackers distribute Gamaredon in the wild using various strategies, such as a phishing email embedded with malicious Microsoft Office attachments or an ISO file with embedded LNK files that use PowerShell scripts to download malicious binaries.



## Persistence

For persistence, both of the following mechanisms are used by the malware:

- It checks if Microsoft Office is installed. The sample has attempted to see if Microsoft Office is installed before executing some action.
- It runs programs periodically or at specific time to perform any other action using scheduled task windows services such as schtasks.exe

```
C:\Windows\SysWOW64\schtasks.exe schtasks /create /tn Adobe.exe_del /tr 'taskkill /f /im Adobe.exe' /sc daily /st 10:05
```

## Network

In recent campaigns, we have noticed that Gamaerdon domains are registered by TIMEWEB—RU and are using the domain .RU. The IP address is present in the binary. It uses a TLS handshake instead of Secure Sockets Layer (SSL). We can see the following snapshot of the TCP traffic.

```

└─ 2351 337.128952 149.154.70.99      192.168.1.36  TCP      54 443 → 49752 [RST, ACK] Seq=1 Ack=251 Win=
<
Source Address: 149.154.70.99
Destination Address: 192.168.1.36
v Transmission Control Protocol, Src Port: 443, Dst Port: 49752, Seq: 1, Ack: 251, Len: 0
  Source Port: 443
  Destination Port: 49752
  [Stream index: 57]
  [Conversation completeness: Complete, WITH_DATA (47)]
  [TCP Segment Len: 0]
  Sequence Number: 1      (relative sequence number)
  Sequence Number (raw): 18228121
  [Next Sequence Number: 1      (relative sequence number)]
  Acknowledgment Number: 251      (relative ack number)
  Acknowledgment number (raw): 3579972486

```

# Lyceum

## Summary

Active since 2017, Lyceum Group is a state—sponsored Iranian APT group known for targeting Middle Eastern organizations in the energy and telecommunication sectors. Lyceum Group has been utilizing a newly developed and customized .NET—based DNS backdoor malware, which is a customized version of the open source tool DIG.net. DIG.net is an open source DNS resolver that can be used to query the DNS server and then parse the response.

## Delivery Mechanism

The main mechanism for delivering the payload is a Microsoft Office attachment embedded with a malicious macro. In a recent campaign we analyzed, the macro—enabled Microsoft Word document had a template that showcased news reports related to military affairs in Iran. The threat actor leveraged the AutoClose() function. Upon closing, the document function was executed and then it dropped the DNS backdoor onto the system.

## Persistence

The malware uses the STARTUP folder order to maintain persistence and executes whenever the system restarts. It generates a unique BotID, depending on the current Microsoft Windows username. It converts the username into its MD5 equivalent using the CreateMD5() function and parses the first eight bytes of the MD5 as the BotID for the identification of the user and system infected by the malware.

## Network

The malware leverages a DNS attack technique called DNS hijacking in which an attacker—controlled DNS server manipulates the response and resolution of DNS queries. The malware uses the DNS protocol for command and control (C2) communication, thereby evading detection. It comprises functionalities like Upload/Download Files and execution of system commands on the infected machine by abusing DNS records, including TXT records for incoming commands and address records for data exfiltration. The malware sets up an attacker—controlled DNS server by acquiring the IP address of the domain name, which in turn triggers a DNS request to the domain to resolve the IP address. Now this IP is associated as the custom attacker—controlled DNS server for all further DNS queries initiated by the malware.

# QuasarRAT

## Summary

QuasarRAT has been active since at least 2015. It is a legitimate, publicly available RAT for Microsoft Windows. Attackers 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 the operations perform on the client side managed by the server.

## Delivery vector

QuasarRAT delivers the RAT to the victim machine via spam emails, by backdooring or masquerading as cracked software, and other lures.

## Persistence

- QuasarRAT uses the following methods to achieve persistence in the target machine:
- It uses Mutex creation: QSR\_MUTEX\_[O-9A-Za-z]{18,}.
- It ensures that the malicious content is not running inside a security company's virtual machine by checking the public IP address of the machine.
- It drops files to the AppData directory.
- It uses scheduled task windows services to add and modify task schedules. For example:

```
'C:\Windows\SysWOW64\schtasks.exe' /create /
tn RtkAudioService64 /tr 'C:\Users\user\btpanui\
SystemPropertiesPerformance.exe' /sc minute /mo 1 /F
```

## Network

Quasar—encrypted communications uses 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. The distinctive first four bytes of the payload can be used to identify Quasar 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.

```
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 ia.I:q..
00000010 08 be 36 12 7a 4a 36 c2 8a 9b c1 67 b1 af bf 08 ...6.z]6. ...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.in.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 <N...|.k .@y.r.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> .
```



# Qakbot

## Summary

Active since 2008, Qakbot, also known as QBot, QuackBot, and Pinkslipbot, is a Trojan designed to steal passwords. This pervasive threat spreads using an email—driven botnet that inserts replies in active email threads. Qakbot threat actors are also known to target bank customers and use the access they gain through compromised credentials to spy on financial operations in order to gain valuable intelligence, and continue to evolve adopting new delivery vectors to evade detection.

## Delivery vector

Qakbot delivers the payload, such as XLM 4.0, via malicious Microsoft Office attachments and uses enticing file names with common formats like:Calculation-1517599969-Jan-24.xlsb,ClaimDetails-1312905553-Mar-14.xlsb,Compensation-1172258432-Feb-16.xlsb etc.

## Persistence

- Qakbot establishes persistence in the system by:
- Mutex creation
- Creating an autostart registry key
- Copying itself to the system's STARTUP or AppData directory
- Creating Scheduled Task services
- Injecting itself into legitimate Microsoft Windows processes such as explorer.exe

## Network

Qakbot uses WebInject to modify communications between the target machine and banking websites and steals the victim's credentials. Qakbot uses HTTPS or SSL and TLS traffic with no associated domains.

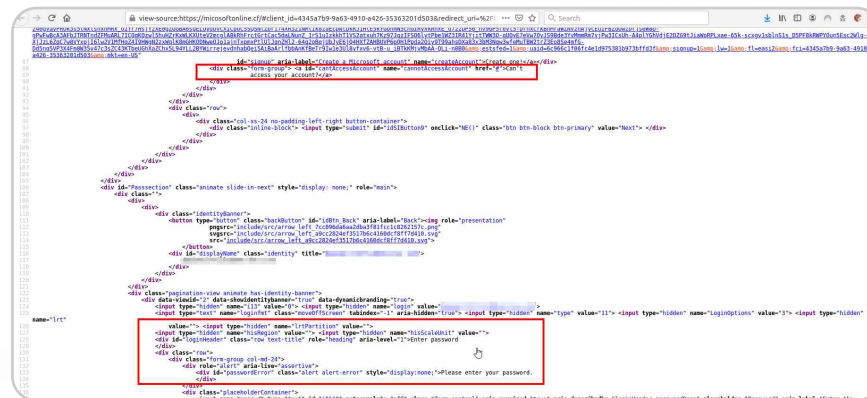
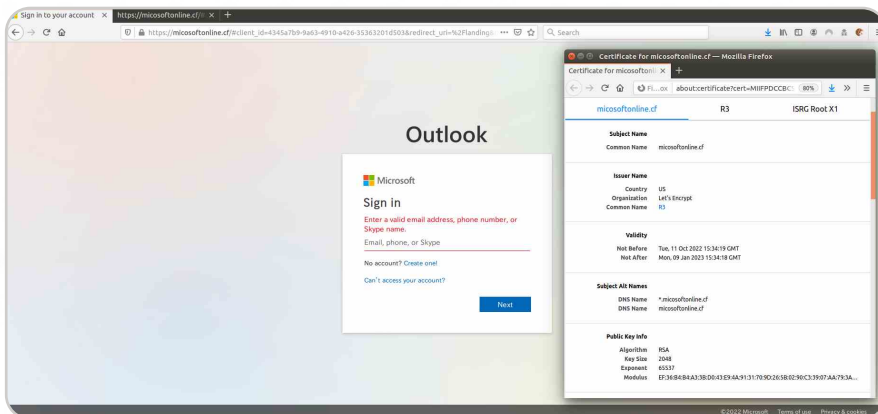
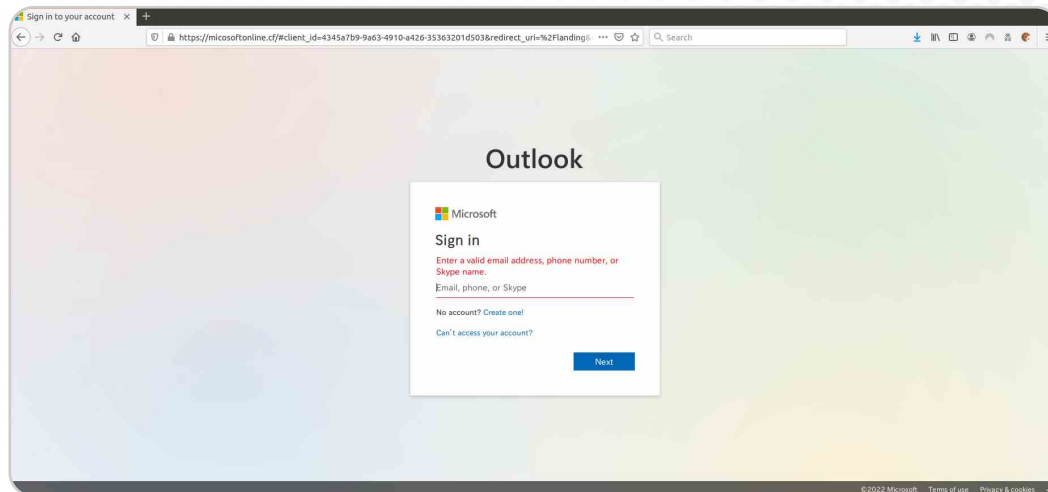
No.	Time	Source	Destination	Protocol	Length	Info
126	16.723997	184.28.221.40	192.168.1.50	TLSv1...	344	New Session Ticket, Change Cipher
529	16.753333	184.28.221.40	192.168.1.50	TLSv1...	344	New Session Ticket, Change Cipher
30	16.461933	184.28.221.40	192.168.1.50	TLSv1...	1514	Server Hello
33	16.462227	184.28.221.40	192.168.1.50	TLSv1...	1514	Server Hello
379	16.734415	184.28.221.40	192.168.1.50	TLSv1...	1514	Server Hello
6010	303.293228	20.190.154.17	192.168.1.50	TLSv1...	4150	Server Hello
6011	303.293246	20.190.154.17	192.168.1.50	TLSv1...	4150	Server Hello
2860	21.892464	20.54.89.106	192.168.1.50	TLSv1...	2491	Server Hello, Certificate, Server

# Phishing case studies

## Microsoft Phishing:

Zscaler ThreatLabz observed domain squatting for a phishing website over HTTPS, as seen below.

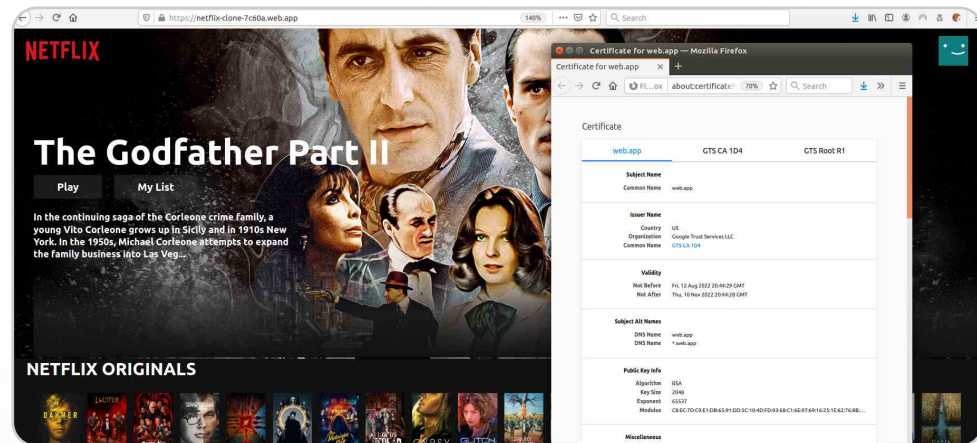
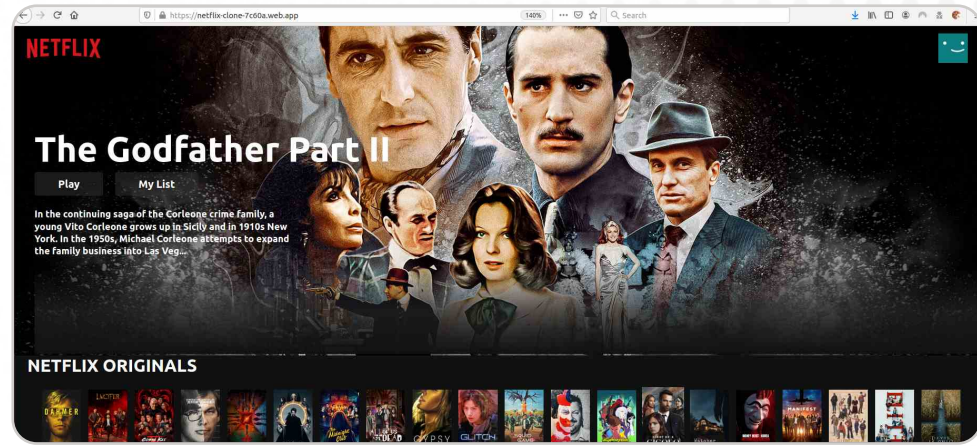
Phishing URL : [https://microsoftonline\[.\]cf/](https://microsoftonline[.]cf/)



## Netflix Phishing:

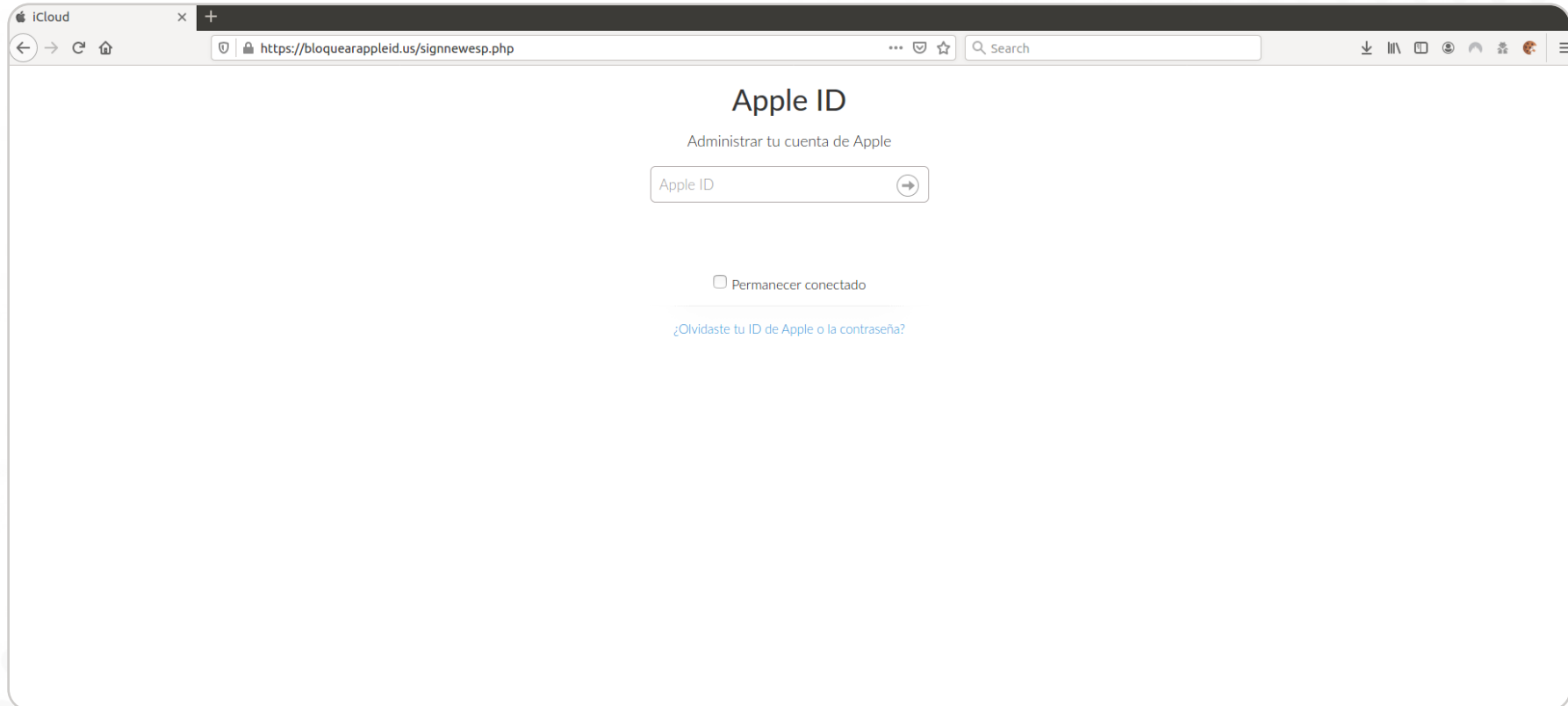
We also observed an instance of phishing that leveraged Netflix over HTTPS, which abused web hosting services like web[.]app and Google Trust certificates.

Phishing URL : [https://netflix-clone-7c60a.web\[.\]app/](https://netflix-clone-7c60a.web[.]app/)



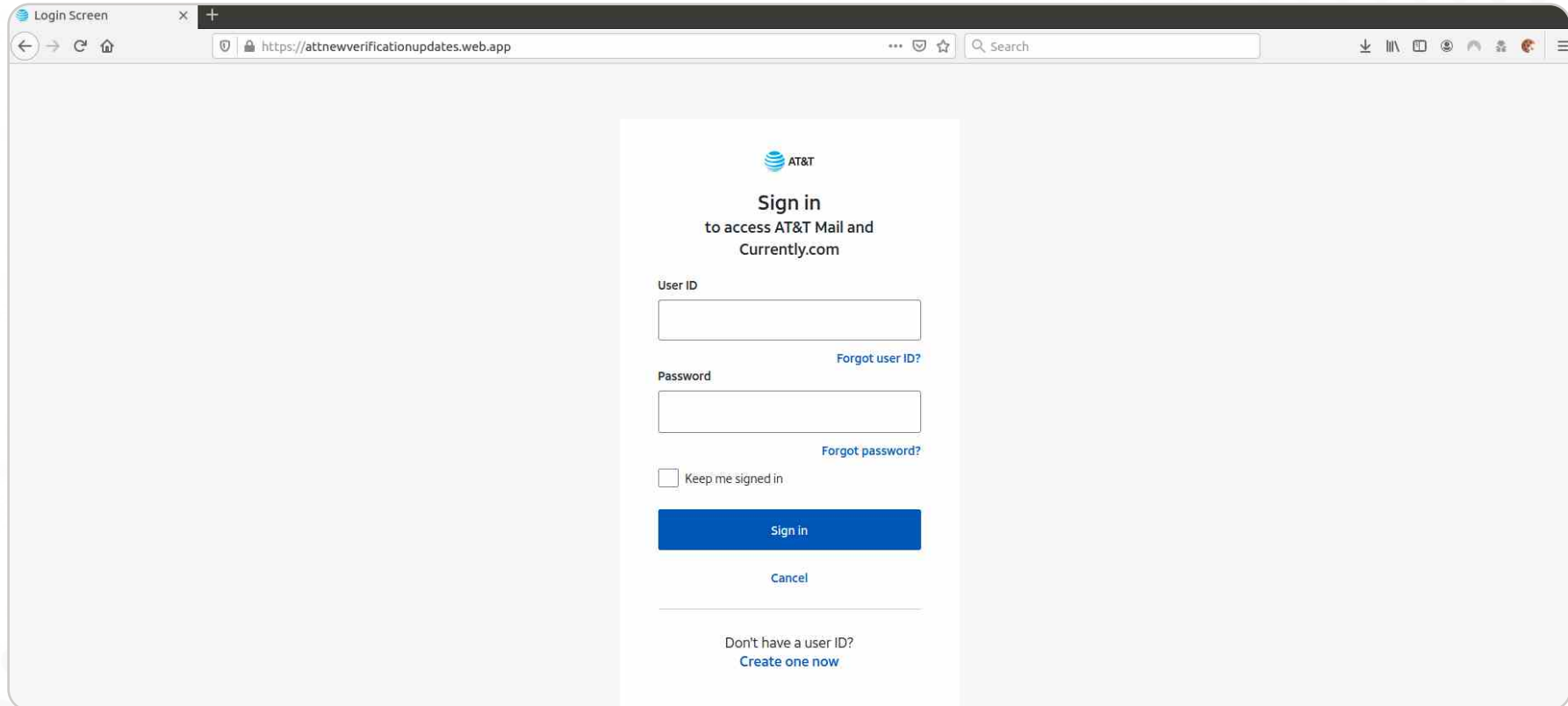
# Apple Login

Phishing URL : [https://bloquearappleid\[.\]us/signnewesp.php](https://bloquearappleid[.]us/signnewesp.php)



# ATT Phishing:

Phishing URL : [https://attnewverificationupdates\[.\]web\[.\]app/](https://attnewverificationupdates[.]web[.]app/)



The screenshot shows a web browser window with the address bar displaying `https://attnewverificationupdates.web.app`. The page content is a login form with the AT&T logo at the top. The text reads: "Sign in to access AT&T Mail and Currently.com". Below this, there are two input fields: "User ID" and "Password". To the right of the "User ID" field is a link "Forgot user ID?". To the right of the "Password" field is a link "Forgot password?". Below the input fields is a checkbox labeled "Keep me signed in". At the bottom of the form are two buttons: "Sign in" (a blue button) and "Cancel". At the very bottom of the page, there is a link "Don't have a user ID? Create one now".

# USPS Phishing:

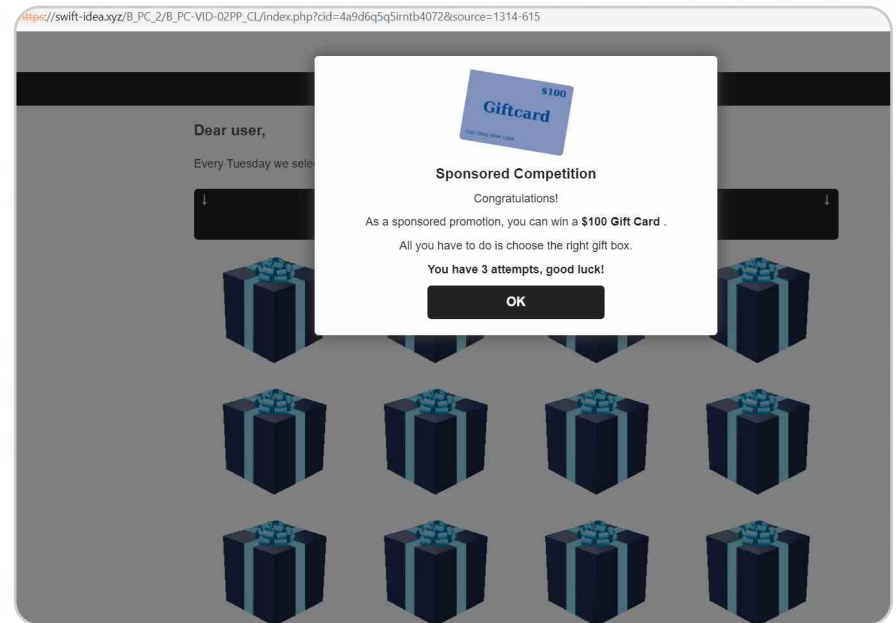
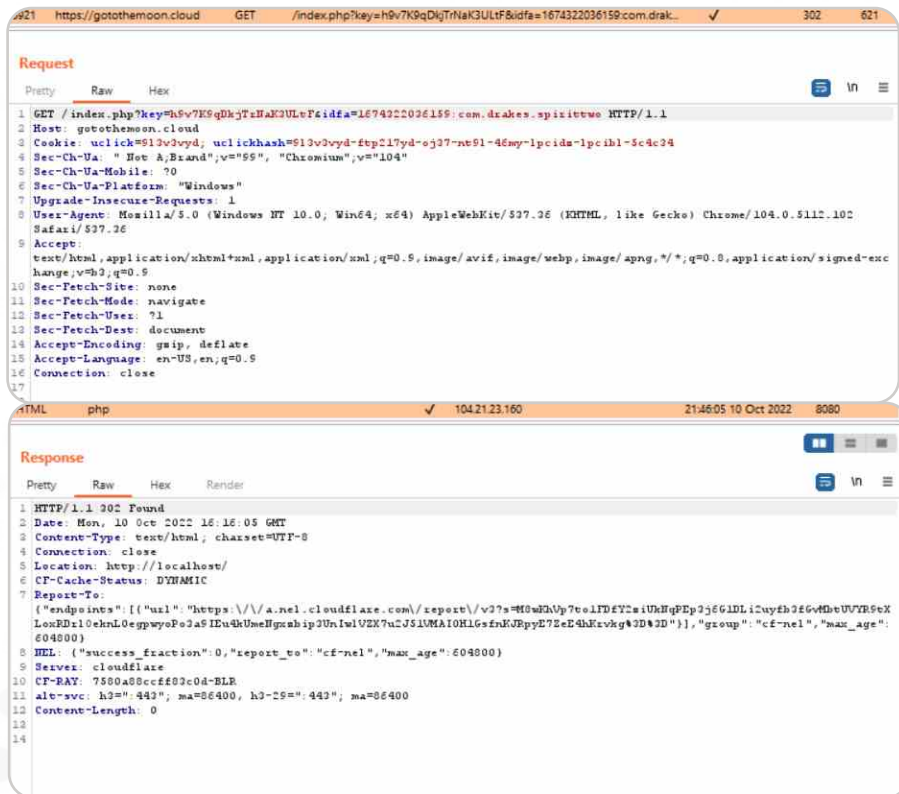
Phishing URL : <https://faqs.usps-cloud.com/?a=sec>

The screenshot shows a browser window with the URL <https://faqs.usps-cloud.com/?a=sec>. The page header includes the USPS.COM logo and navigation links: Quick Tools, Mail & Ship, Track & Manage, Postal Store, Business, International, and Help. The main content area is titled "USPS Tracking" and includes a "Track Another Package" link. A tracking number "US9514901185421" is displayed. The status section shows a red warning: "We have issues with your shipping address" and explains that USPS allows redelivery. Below this is a "Payment Method" section with a red warning: "This Redelivery request cost 3.00 USD." and input fields for Card Number, Expiry Date (MM/YY), and Security code. A "Continue" button is at the bottom of the form. At the very bottom of the page, there is a footer: "Can't find what you're looking for? Go to our FAQs section to find answers to your tracking questions."

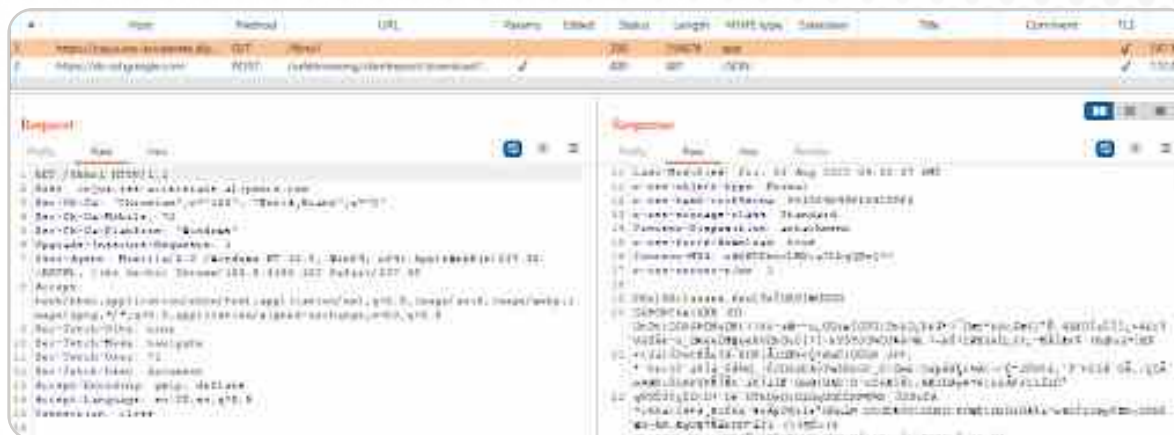
# Mobile/IoT case studies

**GriftHorse:** GriftHorse is known for subscribing victims to a premium SMS that charges their phone bill, causing a financial loss. GriftHorse started as a trick malware hiding payload in native JS to bypass static review.

The Trojan communicates with C&C servers over a secure channel for post—infection activities. GriftHorse highly depends on Facebook deferred deep linking, Appsflyer, and GitHub for cloaking and C2 communication, which all are also happening over SSL.



**Joker:** For years, Joker has been a persistent malware targeting the Android platform. It subscribes users to premium services using WAP or direct carrier billing. Apart from different in—app cloaking techniques, Joker C2 servers communicate over SSL. A new variant of Joker seems to be moving away from the SDK—based approach to a more controlled, SSL server side approach with SSL pinning on the client side to avoid detection.



**MaliBot:** MaliBot is a new strain of banking malware that mainly targets online banking customers in Spain and Italy. Its ability to steal credentials and cookies, and bypass multifactor authentication (MFA) codes make it powerful malware. MaliBot is focused on stealing financial information, credentials, crypto wallets, and personally identifiable information (PII). It also targets financial institutions. It is capable of remotely controlling infected devices using a VNC server implementation. We have observed multiple C2 activities over a secure channel from this banking malware.

**Hydra:** Hydra is another prevalent and fully capable banking malware. Its capabilities include screencast, which allows the attacker to visualize infected device activities, remote app installation, and more. These capabilities make this malware one of the most serious threats to mobile devices. Hydra also leverages Let's Encrypt SSL certificates for C&C activities. Some recent Hydra malware samples have been found to use Github for their C2 activities as well.

**Medusa:** Medusa is also a well—known strain of Android banking Trojan. It collects personal information, uses overlay, and steals credentials based on commands from the attackers. Medusa C2 servers also leverage secure 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](https://research.zscaler.com).

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



| 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](http://www.zscaler.com).

© 2022 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](http://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.