



From Compromise to Breach: How Infostealers Power Account Takeover

Prepared by:
Marisa Atkinson, Senior Analyst II, Hunt

What we will talk about

- Infostealer Logs
- Why should organizations care?
- Infostealer Log Ecosystem
- Account Takeovers: Autofills
- Account Takeovers: Browser Cookies
- Antidetect Browsers and Stealer Logs

Stealer Logs

- What are infostealers?
 - Malware that harvests information from infected devices
 - Host info, credentials, cookies, autofill, credit cards, files, crypto wallets, etc.
- What are infostealer “logs”?

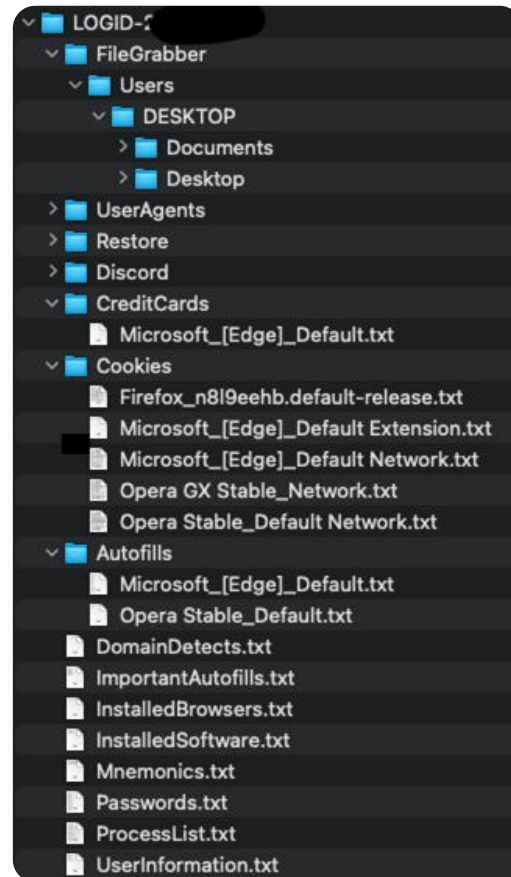
```
UserInformation.txt
Build ID: GAds
IP: 20
FileLocation: C:\Users\Administrator\Downloads\Adobe Photoshop 24.2.0.315.exe
UserName: DESKTOP
MachineName: DESKTOP-VROQLKN
Country: JM
Zip Code: KGN5
Location: Kingston, Kingston
HWID: AB2914C683AEBFA83D96244014BE04F0
Current Language: English (United States)
ScreenSize: {Width=1366, Height=768}
TimeZone: (UTC-06:00) Central Time (US & Canada)
Operation System: Windows 10 Pro x64
Log date: 9/4/2024 16:28:27

Available KeyboardLayouts:
English (United States)
English (Jamaica)

Hardwares:
Name: Total of RAM, 8056.59 Mb or 8447942656 bytes
Name: Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 2 Cores
Name: Intel(R) HD Graphics 520, 1073741824 bytes

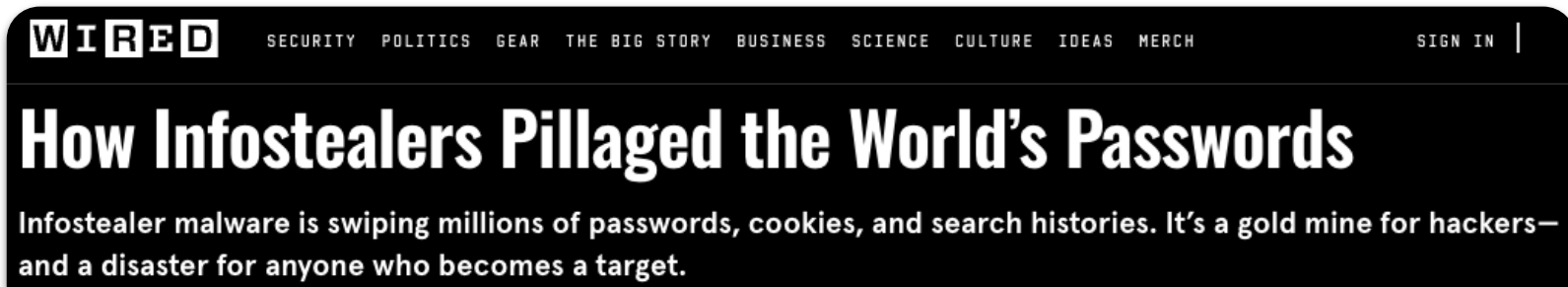
Anti-Viruses:
Windows Defender
```

```
Passwords.txt
URL: https://www.roblox.com/NewLogin
Username: xrjy*****
Password: xrjy*****
Application: Microsoft_[Edge]_Default
=====
URL: https://signup.live.com/signup
Username: sha*****@*****.com
Password: SHAj*****
Application: Microsoft_[Edge]_Default
=====
URL: https://quickq.io/login
Username: sha*****@*****.com
Password: SHAj*****
Application: Microsoft_[Edge]_Default
=====
URL: https://dog.lucky13systems.com/login
Username: kia***@*****.com
Password: IAMsh*****
Application: Microsoft_[Edge]_Default
=====
URL: https://ttec.taleo.net/careersection/iam/accessmanagement/
Username: kia****
Password: Bads*****
Application: Microsoft_[Edge]_Default
=====
URL: https://marketplaceqa.nexrepapps.com/login
Username: kia***@*****.com
Password: IAMsh*****
Application: Microsoft_[Edge]_Default
=====
```



Why should organizations care?

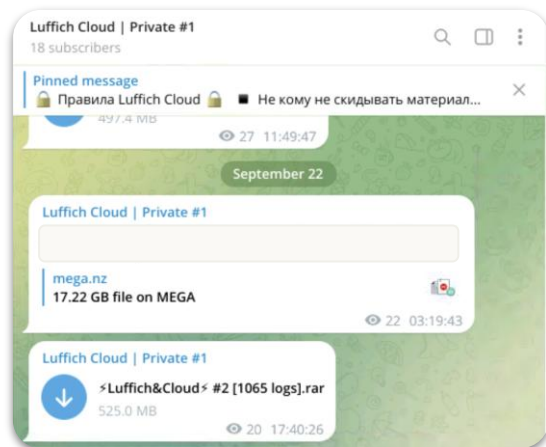
- Recent headline grabbing breaches have been result of initial access via infostealer infections on corporate or personal devices
 - VPNs, RDP/VNC, webmail, third party business critical apps, etc.
- Ease of use and effectiveness has resulted in higher supply and demand



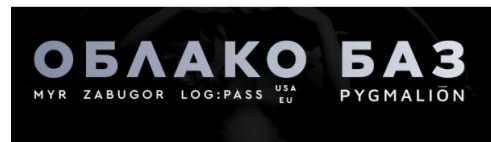
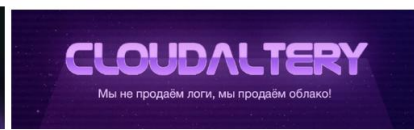
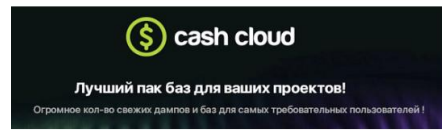
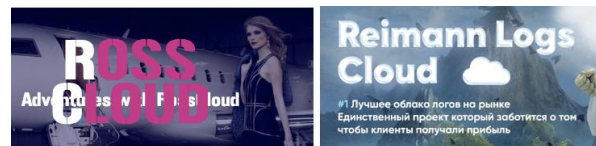
The image shows a screenshot of a Wired article header. At the top left is the 'WIRED' logo. To its right is a navigation menu with the following items: SECURITY, POLITICS, GEAR, THE BIG STORY, BUSINESS, SCIENCE, CULTURE, IDEAS, and MERCH. On the far right of the navigation bar is a 'SIGN IN' link. Below the navigation bar is the article title 'How Infostealers Pillaged the World's Passwords' in a large, bold, white font. Underneath the title is a short introductory paragraph: 'Infostealer malware is swiping millions of passwords, cookies, and search histories. It's a gold mine for hackers—and a disaster for anyone who becomes a target.'

Log Exploitation

- Log Reselling
 - Cloud Log Subscriptions
 - Marketplace Platforms
 - Telegram Bots
- Cryptocurrency Wallet Draining
- Account Takeover

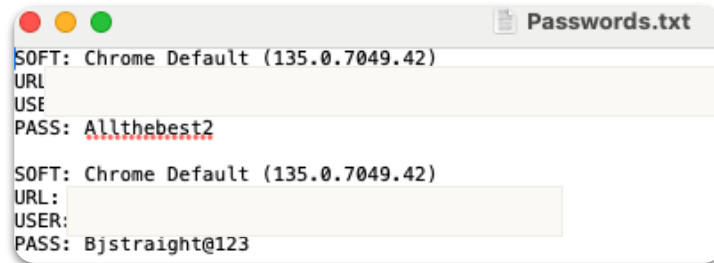
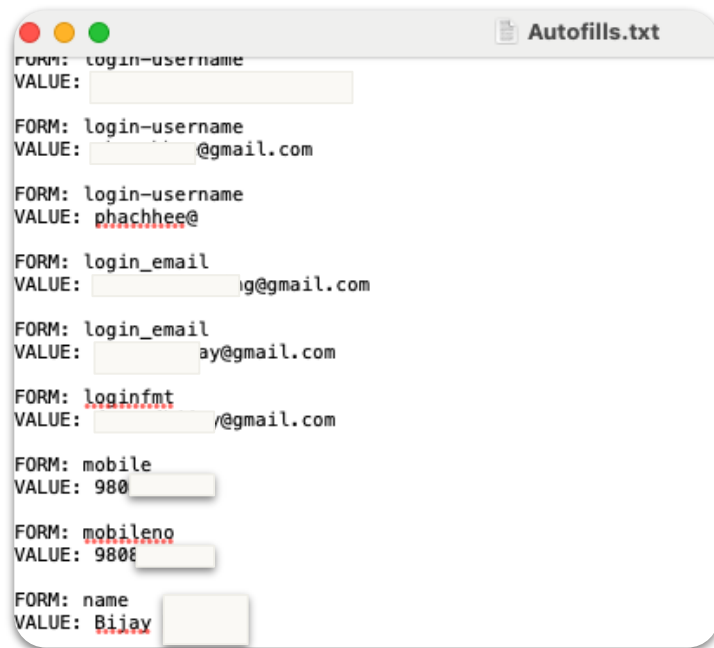
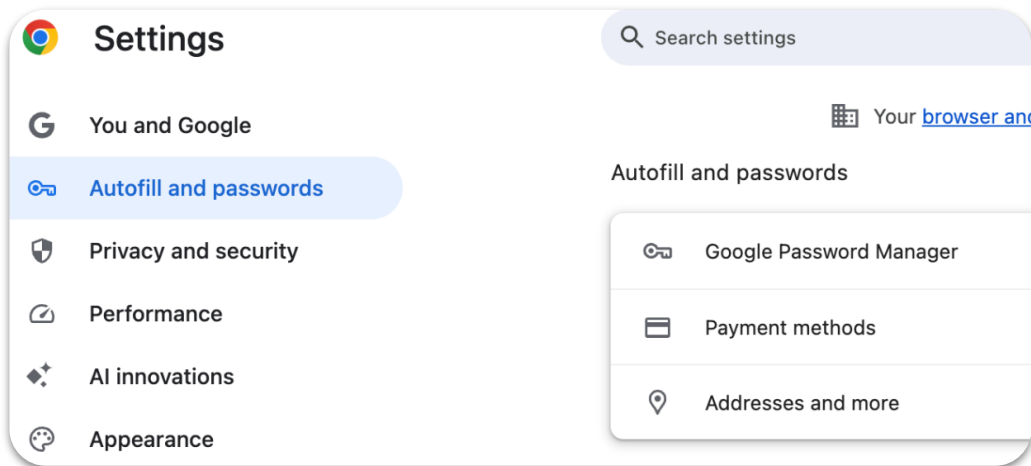


Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
AZORult	Uttar Pradesh ISP: Squaredel	accounts.google.com account.protonvpn.com accounts.google.com 192.168.1.1 accounts.google.com pngtree.com twitter.com	-	!	archive.zip	2021.03.09	0.11Mb	nn###an [Diamond]	\$ 10.00	Buy
AZORult	England ISP: Digital Energy Technology Ltd	steamcommunity.com accounts.google.com secure.account.oup.com tlauncher.org login.microsoftonline.com roblox.com discord.com diennas.tamo.it klase.eduka.it emapamokos.it Show more...	-	!	archive.zip	2021.03.09	0.16Mb	nn###an [Diamond]	\$ 10.00	Buy
AZORult	California ISP: Leaseweb USA	web4.cc.ntu.edu.tw softconf.com shopee.tw web4.cc.ntu.edu.tw connect.ubisoft.com ceiba.ntu.edu.tw ethics.moe.edu.tw my.taishinbank.com.tw tsmc.taleo.net wireless.ntu.edu.tw Show more...	-	!	archive.zip	2021.03.09	0.02Mb	nn###an [Diamond]	\$ 10.00	Buy



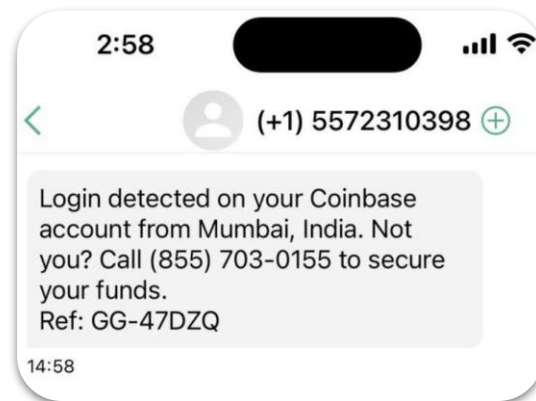
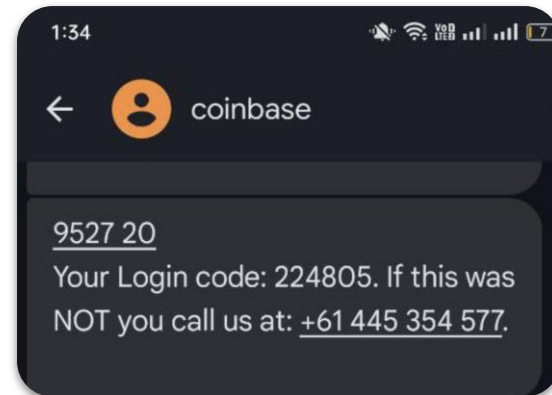
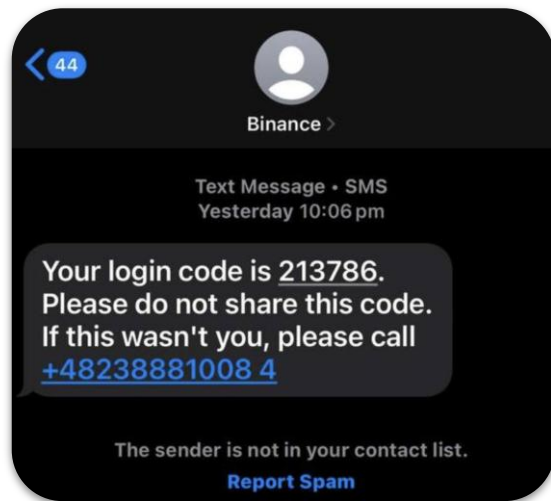
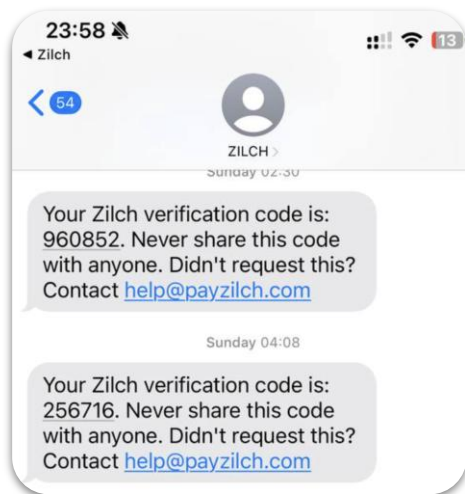
Account Takeover

- Stolen Username + Password Combinations
- Browser Cookies + Hijacking



OTP Bypassing

- Social Engineering to obtain One-Time Passcodes



OTP: Bypassing

The image shows a composite screenshot illustrating a bypass of One-Time Password (OTP) verification. On the left, a Yahoo! Fantasy Sports page is visible with a modal overlay for verification. The modal prompts the user to "Enter verification code" and states "You'll get a text on +1 ****-1614". A "Next" button is highlighted in purple. Below the button, it says "Resend code in 0:37" and "Try signing in another way".

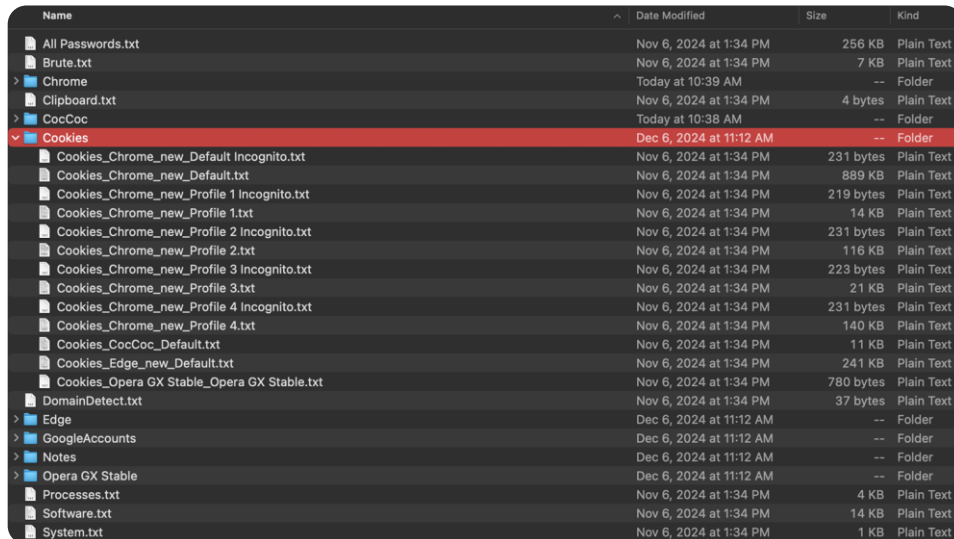
On the right, a dark-themed interface titled "Bot Logs" displays a list of events for a user named "SamratExe@maximum.run:-5". The events include:

- Call completed @ 03:38:49
- Send OTP now
- Target pressed 1
- Human detected @ 03:38:11
- Call answered @ 03:38:04
- Call ringing @ 03:38:00
- Call started @ 03:37:57
- Carrier: AT&T type mobile
- Service: Yahoo
- Initiated call to [redacted] from +17622620098

At the bottom of the bot log interface, there are buttons for "CH: 1", "CH: 2", "CH: 3" (which is highlighted in green), and "VIP". A "Clear Logs" button is also present.

Account Takeover: Browser Cookies

- Strings of data stored locally that allow browsers to operate with persistence
- Highly valuable to threat actors

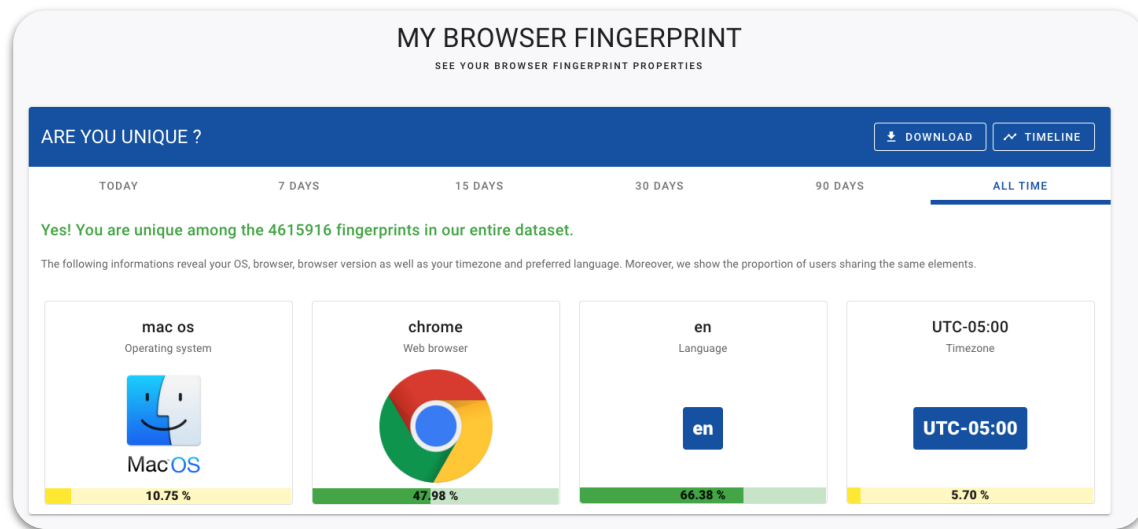


Name	Date Modified	Size	Kind
All Passwords.txt	Nov 6, 2024 at 1:34 PM	256 KB	Plain Text
Brute.txt	Nov 6, 2024 at 1:34 PM	7 KB	Plain Text
Chrome	Today at 10:39 AM	--	Folder
Clipboard.txt	Nov 6, 2024 at 1:34 PM	4 bytes	Plain Text
CocCoc	Today at 10:38 AM	--	Folder
Cookies	Dec 6, 2024 at 11:12 AM	--	Folder
Cookies_Chrome_new_Default Incognito.txt	Nov 6, 2024 at 1:34 PM	231 bytes	Plain Text
Cookies_Chrome_new_Default.txt	Nov 6, 2024 at 1:34 PM	889 KB	Plain Text
Cookies_Chrome_new_Profile 1 Incognito.txt	Nov 6, 2024 at 1:34 PM	219 bytes	Plain Text
Cookies_Chrome_new_Profile 1.txt	Nov 6, 2024 at 1:34 PM	14 KB	Plain Text
Cookies_Chrome_new_Profile 2 Incognito.txt	Nov 6, 2024 at 1:34 PM	231 bytes	Plain Text
Cookies_Chrome_new_Profile 2.txt	Nov 6, 2024 at 1:34 PM	116 KB	Plain Text
Cookies_Chrome_new_Profile 3 Incognito.txt	Nov 6, 2024 at 1:34 PM	223 bytes	Plain Text
Cookies_Chrome_new_Profile 3.txt	Nov 6, 2024 at 1:34 PM	21 KB	Plain Text
Cookies_Chrome_new_Profile 4 Incognito.txt	Nov 6, 2024 at 1:34 PM	231 bytes	Plain Text
Cookies_Chrome_new_Profile 4.txt	Nov 6, 2024 at 1:34 PM	140 KB	Plain Text
Cookies_CocCoc_Default.txt	Nov 6, 2024 at 1:34 PM	11 KB	Plain Text
Cookies_Edge_new_Default.txt	Nov 6, 2024 at 1:34 PM	241 KB	Plain Text
Cookies_Opera GX Stable_Opera GX Stable.txt	Nov 6, 2024 at 1:34 PM	780 bytes	Plain Text
DomainDetect.txt	Nov 6, 2024 at 1:34 PM	37 bytes	Plain Text
Edge	Dec 6, 2024 at 11:12 AM	--	Folder
GoogleAccounts	Dec 6, 2024 at 11:12 AM	--	Folder
Notes	Dec 6, 2024 at 11:12 AM	--	Folder
Opera GX Stable	Dec 6, 2024 at 11:12 AM	--	Folder
Processes.txt	Nov 6, 2024 at 1:34 PM	4 KB	Plain Text
Software.txt	Nov 6, 2024 at 1:34 PM	14 KB	Plain Text
System.txt	Nov 6, 2024 at 1:34 PM	1 KB	Plain Text

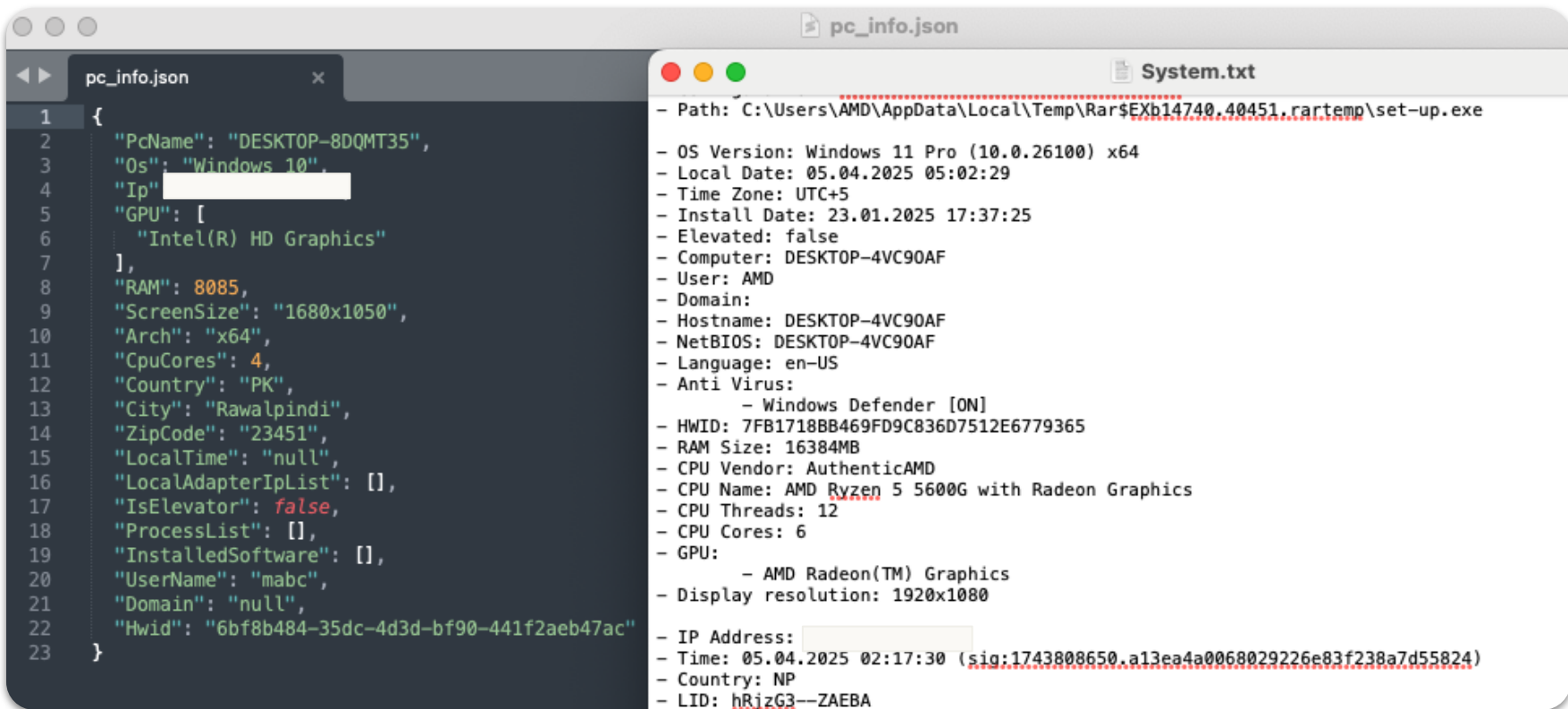
```
3501 nk.com.vn TRUE / FALSE 176404448 _ga GA1.1.2053379062.1729484447
3502 inhplus.com TRUE / FALSE 1738642819 _gcl_aw GCL.1738866819.Cj0KQCI Aoae5BhCNARIsADVLZeqtr7088Xp_FghYXJ10Z~2coj5SH
3503 uviet.vn FALSE / TRUE 0 twk_idm_key RvqZ1eHjYxnly49ka6E-j
3504 bbanK.com.vn FALSE / FALSE 0 ASP.NET_SessionId g35gnelrjwrxs3c1k5vncbdt
3505 bbanK.com.vn FALSE / FALSE 0 _RequestVerificationToken
G1vwPwoUeMqHZNb030XjhuLGEFUk653pEJwhcVX62mzp9Xshu-uKQVVAIMrEweYkngfGyS3EKcZvpvLMQKmZKQmQ8szVil98fMT01
3506 bbanK.com.vn FALSE / FALSE 0 LANG_CODE VI
3507 nk.com.vn TRUE / FALSE 1764044788 _ga_R3XMN343KH GS1.1.1729484447.1.1.1729484788.60.0.0
3508 huviet.vn TRUE / TRUE 1745833223 twk_uuid_5ed61e689e5f6944228fb557 %7B%2uuid%22%3A%21.1vxHjdekfgTUAEU4ziazZtr
V0LENIz:in8mENUx6izNuTJmkTh1E8YgcLPsscaR3RJETO0%22%2C%22version%22%3A%2C%22domain%22%3A%22maychviet.vn%22%2C%22ts%22%3A173
3509 bbanK.com.vn FALSE / FALSE 0 f5avr0932598578aaaaaaaaaaaaaaaa_cspm
GKLJIKLLMBAMDHFIAPOHFPEIEBNDAGDKAFJDAJBAAOKFPMDJPGENJKNPCPFCDHCKNDNAKNKBCJADBEFAMLHGEEHFLQMADEF0IJOBD0CFOIACENHHEIDA
3510 bbanK.com.vn FALSE / TRUE 0 f5avraaaaaaaaaaaaaaaa_session_
INNPECKLEPJINOFBFKKAPJCBLDHJADHBIBJNEIMBNDHBE CNBAJDEDEEAPDRGICPFDDJII CCGGKJINBCJAINKMFNNLHCBHBDGDHCKOKGPCIJHFCIEMDPNPFDDMH
3511 .media.net TRUE / TRUE 1760435358 data-b 4cb8f0b1-59cb-4e2c-a4c6-7d207d30b981~1
3512 .media.net TRUE / TRUE 1760409574 data-ap setstatuscode~3
3513 .media.net TRUE / TRUE 1757986475 data-bs 4dcde1d6-b34c-4ed0-befa-6bac824fc52f~1
3514 .media.net TRUE / TRUE 1732852728 data-c k-bzWt64N_c2WucdGJ0z7ZlRK2bqm-LZv-XINwKQ~3
3515 .media.net TRUE / TRUE 1757987506 data-bt 4cb8f0b1-59cb-4e2c-a4c6-7d207d30b981~1
3516 .media.net TRUE / TRUE 1758073750 data-bai 362d7fe3994d4fbf2ndcae00lzmg7kqp~1
3517 www.mbbanK.com.vn FALSE / FALSE 0 alias_current
```

Browser Fingerprinting

- Data collected by a website about a user's browser and operating system.
- Fingerprints may use the following data points:
 - Operating system
 - System Language
 - Keyboard layout
 - System fonts
 - User agents
 - WebGL
 - Browser extensions
 - CPU
 - HTTP headers
 - Screen resolutions
 - Cookie history
 - Timezone



Browser Fingerprinting continued



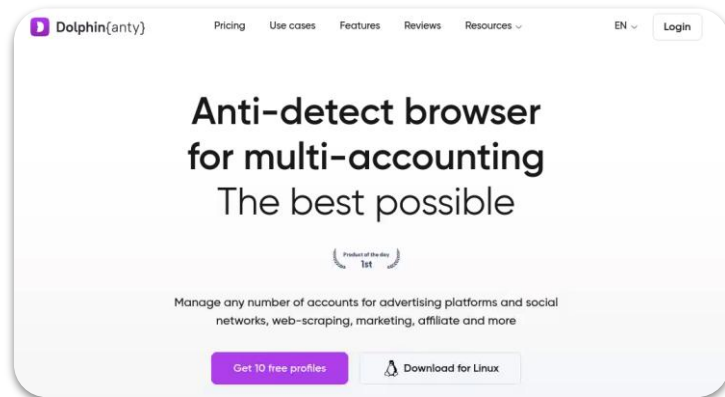
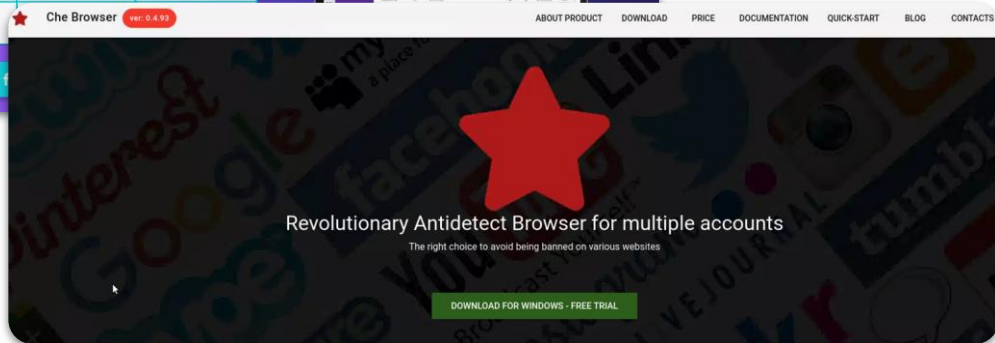
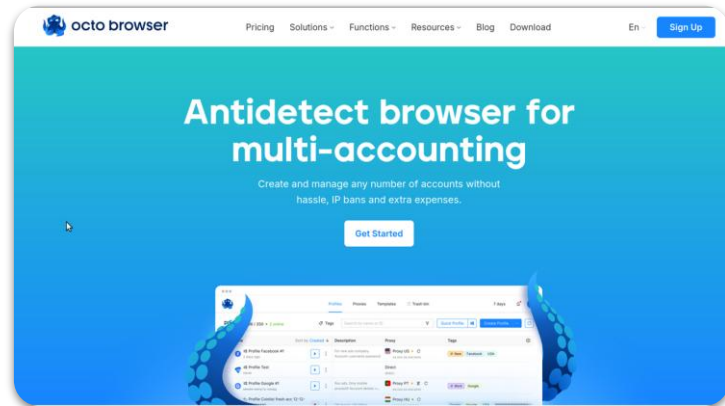
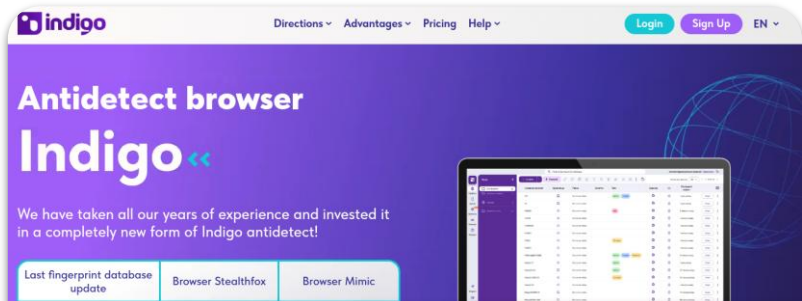
The screenshot shows a browser window with two tabs. The left tab, titled 'pc_info.json', displays a JSON object with various system and user information. The right tab, titled 'System.txt', displays a list of system details, including path, OS version, local date, time zone, install date, elevated status, computer name, user, domain, hostname, NetBIOS name, language, anti-virus status, HWID, RAM size, CPU vendor and name, CPU threads and cores, GPU information, display resolution, IP address, time, country, and LID.

```
1 {
2   "PcName": "DESKTOP-8DQMT35",
3   "Os": "Windows 10",
4   "Ip": " ",
5   "GPU": [
6     "Intel(R) HD Graphics"
7   ],
8   "RAM": 8085,
9   "ScreenSize": "1680x1050",
10  "Arch": "x64",
11  "CpuCores": 4,
12  "Country": "PK",
13  "City": "Rawalpindi",
14  "ZipCode": "23451",
15  "LocalTime": "null",
16  "LocalAdapterIpList": [],
17  "IsElevator": false,
18  "ProcessList": [],
19  "InstalledSoftware": [],
20  "UserName": "mabc",
21  "Domain": "null",
22  "Hwid": "6bf8b484-35dc-4d3d-bf90-441f2aeb47ac"
23 }
```

```
- Path: C:\Users\AMD\AppData\Local\Temp\Rar$EXb14740.40451.rar\temp\set-up.exe
- OS Version: Windows 11 Pro (10.0.26100) x64
- Local Date: 05.04.2025 05:02:29
- Time Zone: UTC+5
- Install Date: 23.01.2025 17:37:25
- Elevated: false
- Computer: DESKTOP-4VC90AF
- User: AMD
- Domain:
- Hostname: DESKTOP-4VC90AF
- NetBIOS: DESKTOP-4VC90AF
- Language: en-US
- Anti Virus:
  - Windows Defender [ON]
- HWID: 7FB1718BB469FD9C836D7512E6779365
- RAM Size: 16384MB
- CPU Vendor: AuthenticAMD
- CPU Name: AMD Ryzen 5 5600G with Radeon Graphics
- CPU Threads: 12
- CPU Cores: 6
- GPU:
  - AMD Radeon(TM) Graphics
- Display resolution: 1920x1080
- IP Address: " "
- Time: 05.04.2025 02:17:30 (sig:1743808650.a13ea4a0068029226e83f238a7d55824)
- Country: NP
- LID: hRizG3--ZAEB4
```

Anti-Detect Browsers

- Software designed to change and modify browser fingerprints



Anti-Detect Browsers

General Advanced ↓ Mass import

None **F** FB **G** Google **T** TikTok **₿** Crypto **👤** OnlyFans

Start pages ⓘ

+ ADD

Proxy ⓘ

No proxy 📄 New proxy 📁 Saved proxies 🔥 Get free proxy

Cookie ⓘ

Paste your cookies or drag and drop your file here

[📄 UPLOAD FILE COOKIES](#)

File format .txt или .json

+ UPLOAD LOCAL STORAGE

UserAgent Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36

Proxy No proxy

WebGL Info Google Inc. (Intel Open Source Technology Center)
ANGLE (Intel Open Source Technology Center, Mesa DRI Intel(R) HD Graphics 2000 (SNB GT1), OpenGL 3.3 (Core Profile) Mesa 21.0.3)

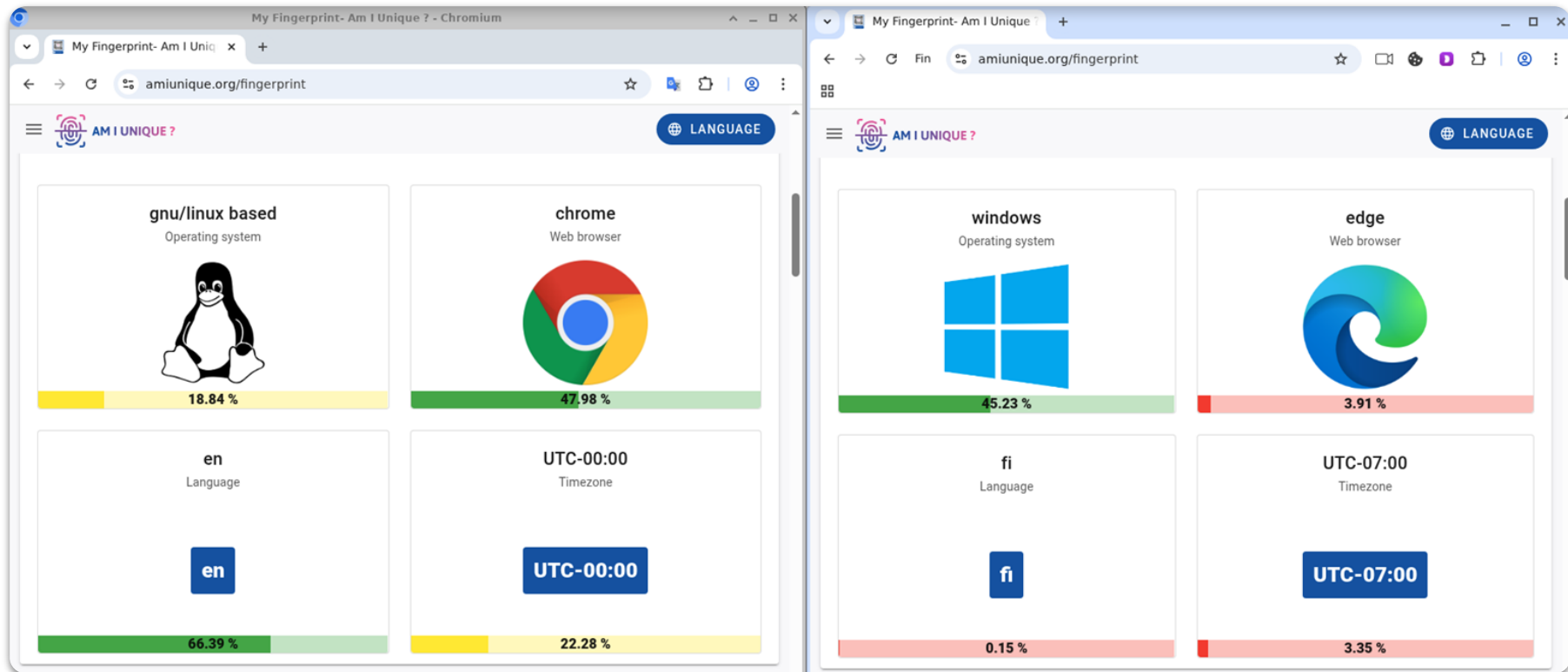
Cpu 4 cores

Memory 8 GB

Screen Real

[ADVANCED CONFIGURATION](#)

Anti-Detect Browsers



Antidetect Browsers

The screenshot displays a web browser window with the following details:

- Browser Title:** Dolphin(antv)
- Address Bar:** Profile 37 usaa.com/my/usaa
- Navigation Menu:** Home, Insurance, Banking, Retirement, Investing, Advice, Perks, Search, Chat, Log Off
- Greeting:** Good Afternoon, Carmen
- Banking Summary Table:**

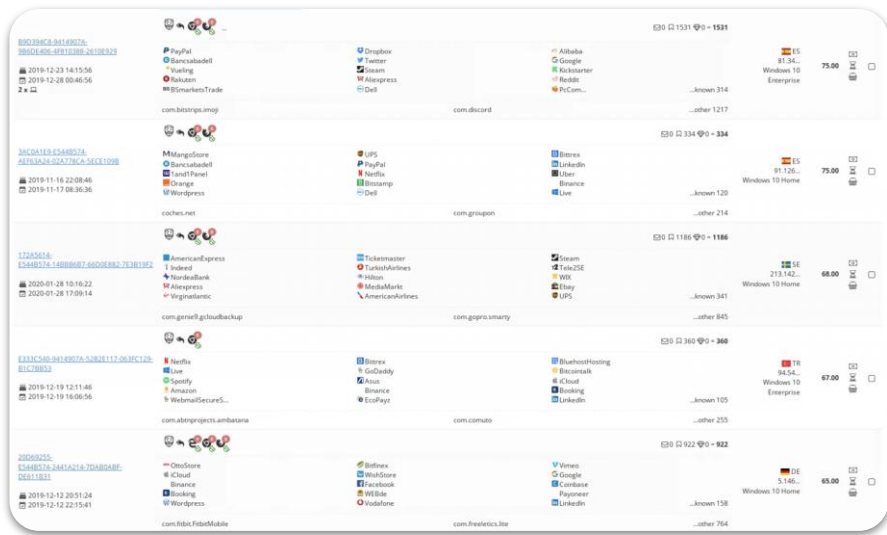
Account Name	Account ID	Balance
USAA CLASSIC CHECKING	*7694	\$22,933.09
PERFORMANCE FIRST SAVINGS	*0431	\$73,668.98
Signature Visa	*7426	-\$238.89
American Express Card	*1771	-\$492.94
YOUTH SPENDING	*9087	\$369.14

Assets: \$96,971.21
Liabilities: -\$731.83
Total: \$96,239.38

- Reward Balance:** \$125.63 Cash Back Reward. Includes a link to "Go To Rewards Center".
- USAA PERKS:** Save Up To 25% On Hotels. Text: "Book with USAA Perks* and save up to 25% on hotels worldwide."

Case Study: Genesis Market

- Underground market popular for offering Browser fingerprints with bot purchases
- Offered a browser plugin for injecting fingerprints
- Shutdown in 2023



Home

Welcome to **Genesis Store** - professional place that helps you to increase anonymity in World Wide Web.

There are few simple steps to do it:

1. **Login** to Genesis Store on any OS (Windows, Mac OS, Linux...) from **Chromium-based browser*** (SRWare Iron, Iridium, Chromium, Sleipnir ...)
2. Find, choose and **buy** the bot you like:
 - bot only with logs 📄
 - bot only with fingerprints 🖨
 - bot with both logs and fingerprints 📄 + 🖨
3. If bot has at least 1 fingerprint, you can install **free** plugin **Genesis Security** in any Chromium-based browser*
4. **Activate** your plugin using a unique key from Profile
5. **Download** your bot in the plugin. You will receive a fingerprints and cookies
6. **Install** preferable fingerprint and cookies in the plugin settings
7. **Congrats!** Now you are a complete copy of your bot! Use all the accesses to the fullest! 🤖

P.S. Do not forget to use **clean socks** 🧦

* Most relevant and stable Chrome-like Browser at the moment **SRWare Iron**
Use **old versions** of the browser: 69, 70, 71, 72.
<http://download1.srware.net/old/iron/win/installer/>
Starting from version 73 cookies may be imported **not correctly**.

The plugin may be installed **automatically** or **manually** by dragging and dropping into the More Tools -> Extensions of your browser.

Please **do not use Chrome browser**. In new versions it is **impossible** to install a plug-in from a third-party developer.

Links to download different Chromium-based browsers:

- Iridium browser
<https://iridiumbrowser.de/>
- SRWare Iron
<https://www.srware.net/>
- Chromiumium (ungoogled)
<https://ungoogled-software.github.io/ungoogled-chromium-binaries/>

Navigator

<input checked="" type="checkbox"/>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36	userAgent
<input checked="" type="checkbox"/>	5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36	appVersion
<input checked="" type="checkbox"/>	Mozilla	appName
<input checked="" type="checkbox"/>	Netscape	appName
<input checked="" type="checkbox"/>	en-US	language
<input checked="" type="checkbox"/>	en-US	languages
<input checked="" type="checkbox"/>	2	deviceMemory
<input checked="" type="checkbox"/>	true	cookieEnabled
<input checked="" type="checkbox"/>	1	doNotTrack
<input checked="" type="checkbox"/>	1	hardwareConcurrency
<input checked="" type="checkbox"/>	0	maxTouchPoints
<input checked="" type="checkbox"/>	Win64	platform
<input checked="" type="checkbox"/>	Gecko	product
<input checked="" type="checkbox"/>	20030107	productSub
<input checked="" type="checkbox"/>	Google Inc.	vendor
<input checked="" type="checkbox"/>		vendorSub
<input checked="" type="checkbox"/>	false	javaEnabled
<input checked="" type="checkbox"/>	true	onLine

[show more](#)

Screen

<input checked="" type="checkbox"/>	1600	width
<input checked="" type="checkbox"/>	900	height

[show more](#)

Window

<input checked="" type="checkbox"/>	1584	outerWidth
<input checked="" type="checkbox"/>	857	outerHeight
<input checked="" type="checkbox"/>	1568	innerWidth
<input checked="" type="checkbox"/>	808	innerHeight
<input checked="" type="checkbox"/>	2	devicePixelRatio

[show more](#)

Audio FP Detection

Use original info from FP
 Generate new data

Canvas FP Detection

Use original info from FP
 Generate new data

Fonts FP Detection

Use original info from FP
 Generate new data

ClientRects FP Detection

Extra FP Detection Technologies

Battery info

77	level %	true	charging
----	---------	------	----------

Step 3. Review, edit FP details manually (using helpers) and finally create it

User-Agent Helper

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36

Language Helper

en-US - English (United States)

Timezone Helper

(UTC -10:00) Pacific/Honolulu

Headers

<input checked="" type="checkbox"/>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36	User-Agent
<input checked="" type="checkbox"/>	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b2	Accept
<input checked="" type="checkbox"/>	gzip, deflate	Accept-Encoding
<input checked="" type="checkbox"/>	en-US;q=0.9,en-L	Accept-Language
<input checked="" type="checkbox"/>	1	DNT (Do Not Track)

WebRTC Leak IP Detection

IPs v4/v6

Geolocation

timeout

Navigator Plugins & Mimetypes

<input checked="" type="checkbox"/>	internal-not-yet-present	Mimetypes: 2	Shockwave Flash
<input checked="" type="checkbox"/>	npitunes.dll	Mimetypes: 1	iTunes Application Detector
<input checked="" type="checkbox"/>	Flash.ocx	Mimetypes: 2	Shockwave Flash

WebGL Leak Info FP Detection

<input checked="" type="checkbox"/>	WebKit	VENDOR	<input checked="" type="checkbox"/>	Google Inc.	UNMASKED VENDOR
<input checked="" type="checkbox"/>	WebKit WebGL	RENDERER	<input checked="" type="checkbox"/>	ANGLE (AMD Radeon R6 Direct3D11	UNMASKED RENDERER
<input checked="" type="checkbox"/>	WebGL 1.0 (OpenGL ES 2.0 Chromium)	VERSION	<input checked="" type="checkbox"/>	WebGL GLSL ES 1.0 (OpenGL ES GLSL	SHADING LANGUAGE

[Create config free \(0.00 \\$\)](#)