FLASHPOINT

From Compromise to Breach: How Infostealers Power Account Takeover

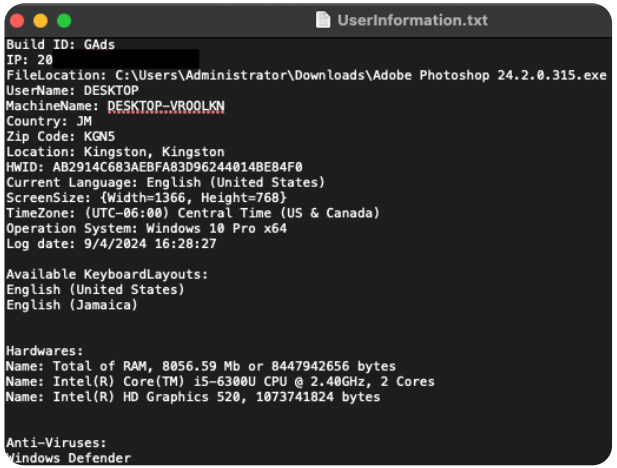
Prepared by:
Marisa Atkinson, Senior Analyst II, Hunt

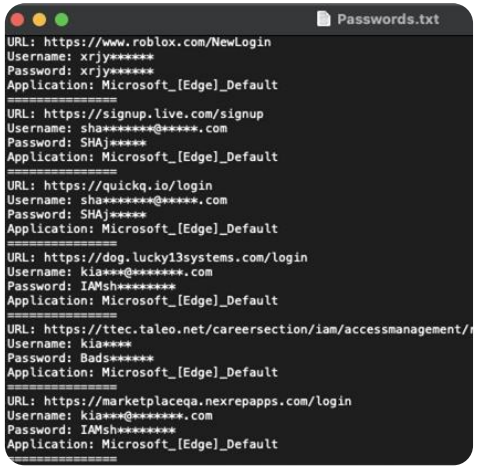
What we will talk about

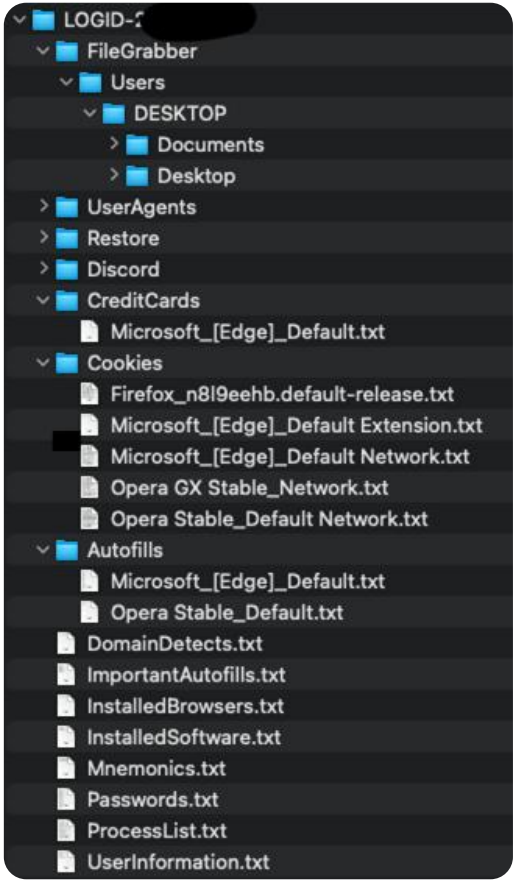
- Infostealer Logs
- Why should organizations care?
- Infostealer Log Ecosystem
- Account Takeovers: Autofills
- Account Takeovers: Browser Cookies
- Antidetect Browsers and Stealer Logs

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”?







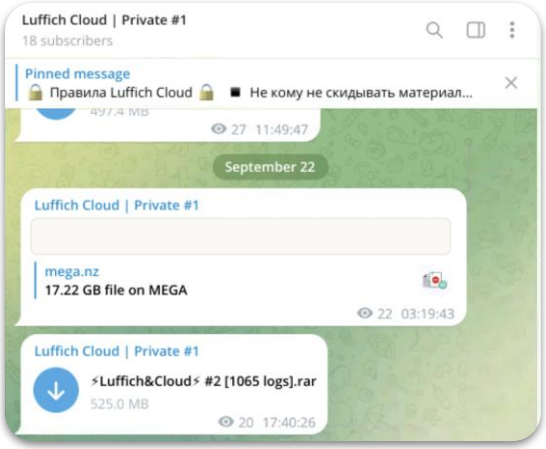
Why should organizations care?

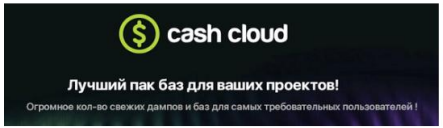
- Recent headline grabbing breaches have been result of initial access via infostealer infections on corporate or personal devices
  - VPNs, RDP/VNC, webmail, third party business critical apps, etc.

- Ease of use and effectiveness has resulted in higher supply and demand

Log Exploitation

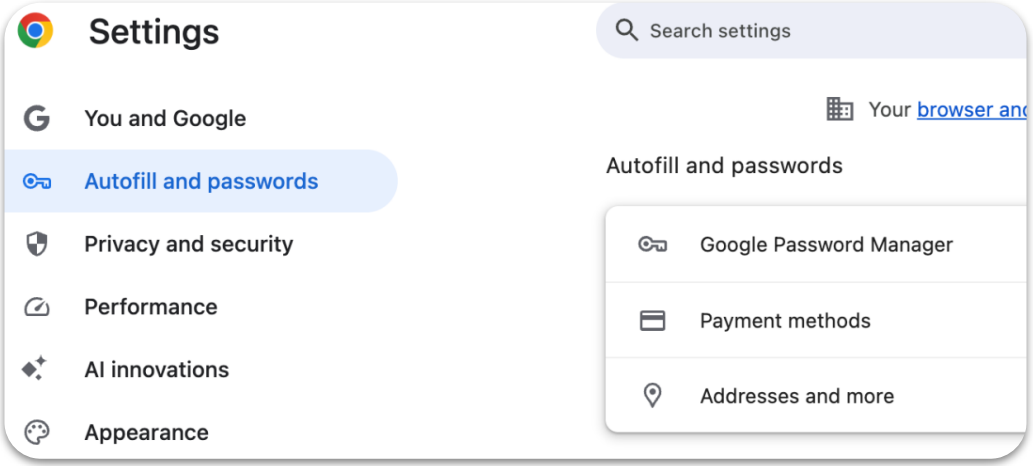
- Log Reselling
  - Cloud Log Subscriptions
  - Marketplace Platforms
  - Telegram Bots
- Cryptocurrency Wallet Draining
- Account Takeover

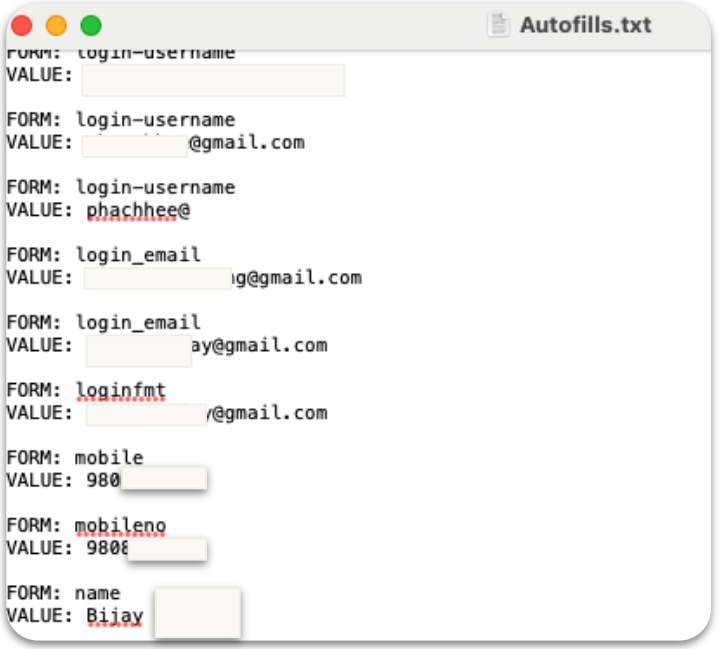


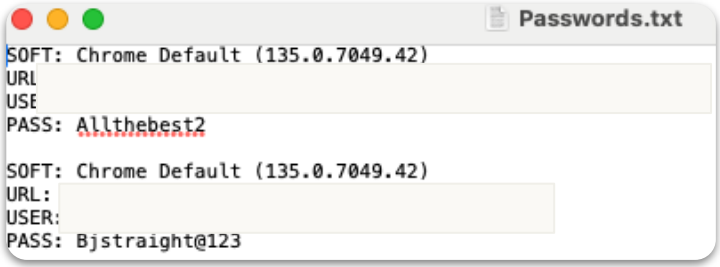


Account Takeover

- Stolen Username + Password Combinations
- Browser Cookies + Hijacking

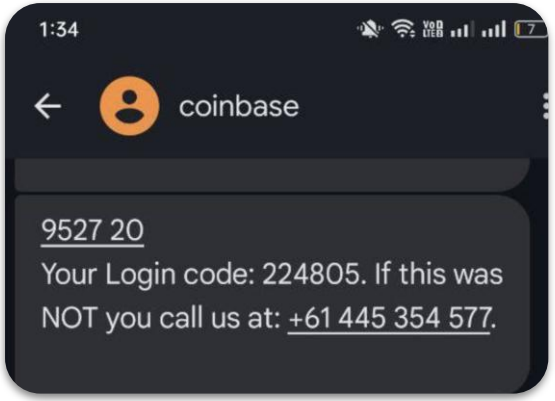


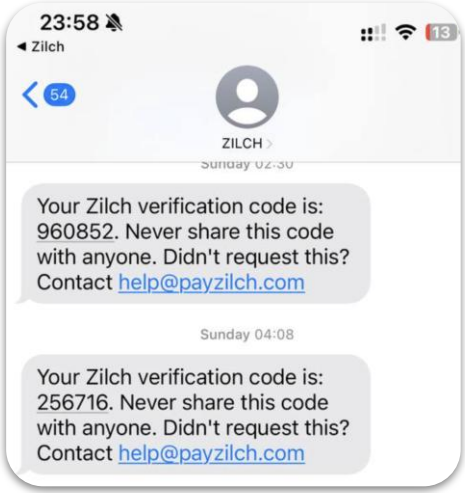


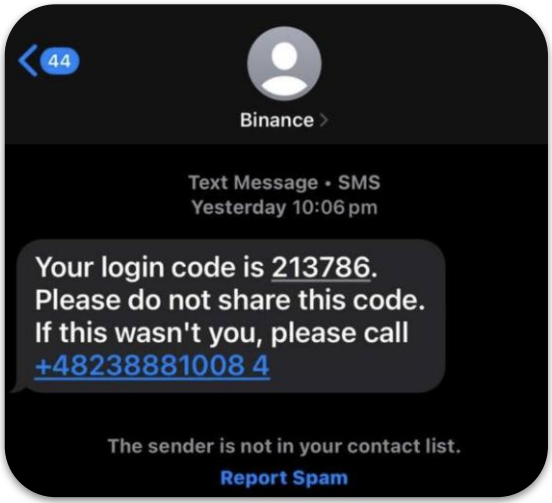


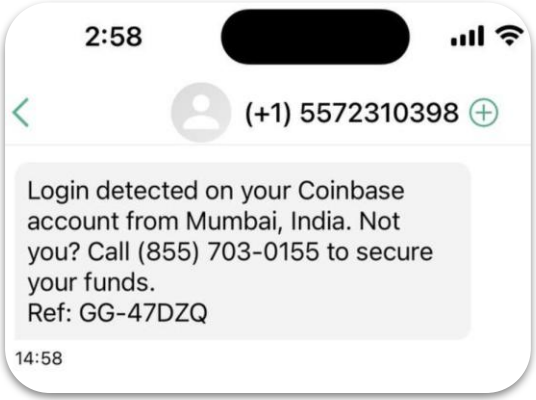
OTP Bypassing

- Social Engineering to obtain One-Time Passcodes

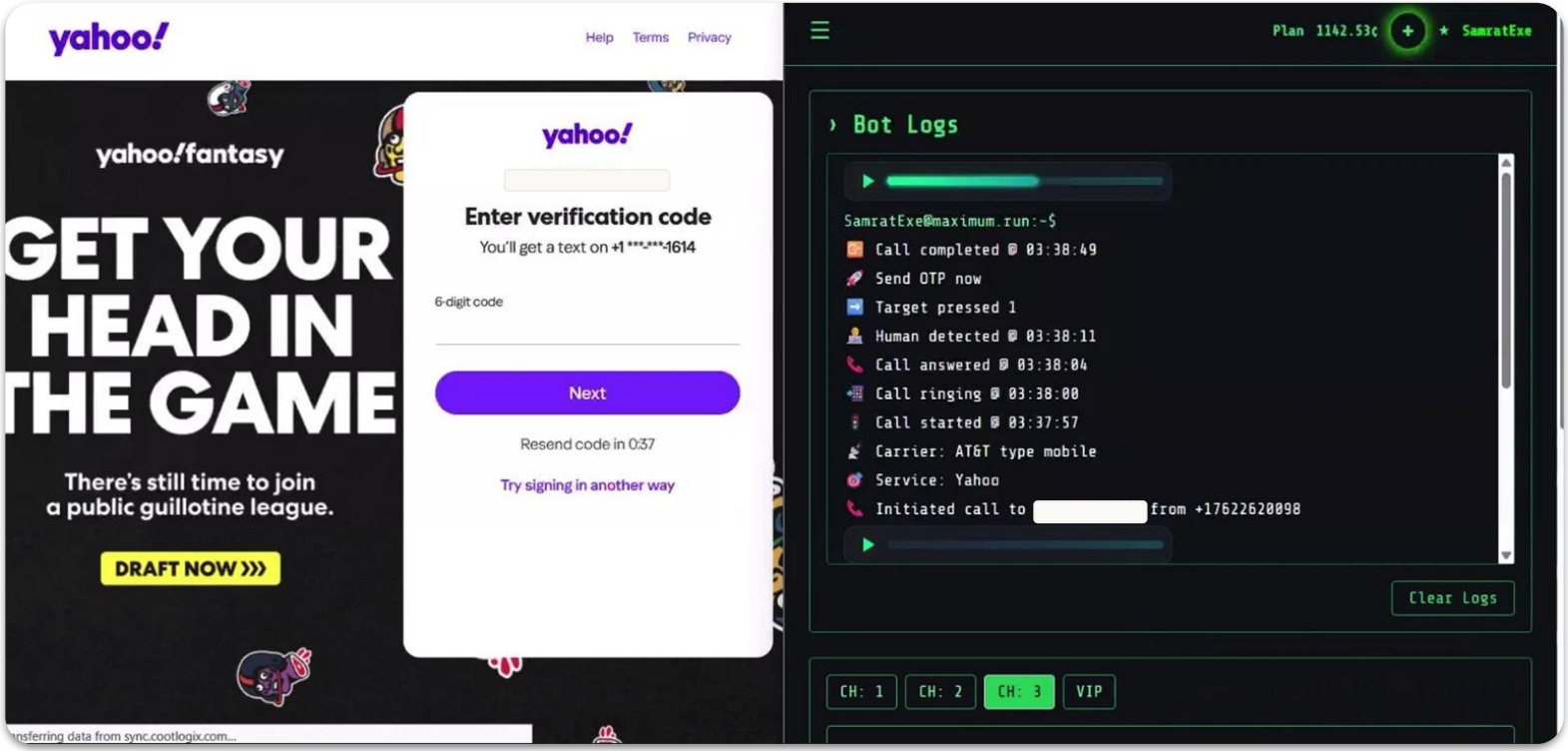






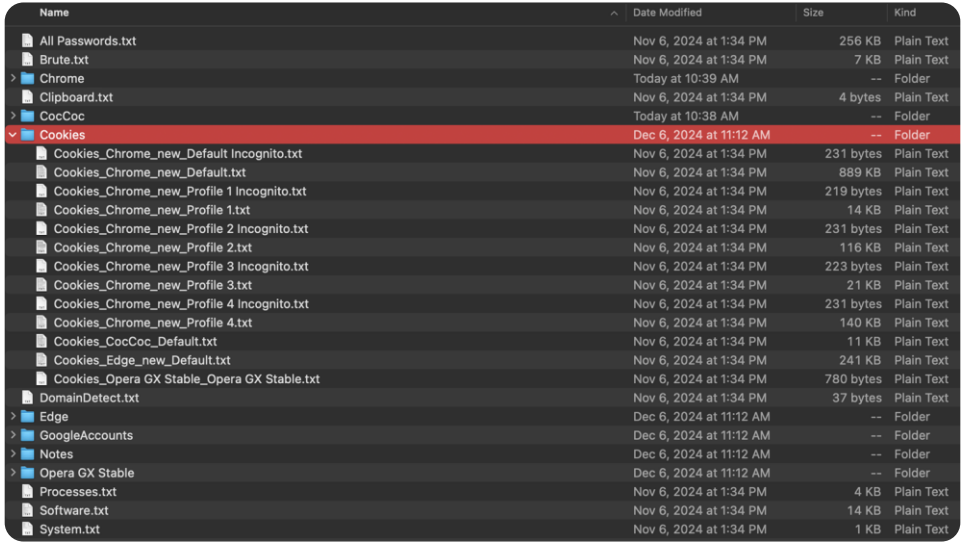


OTP: Bypassing



Account Takeover: Browser Cookies

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

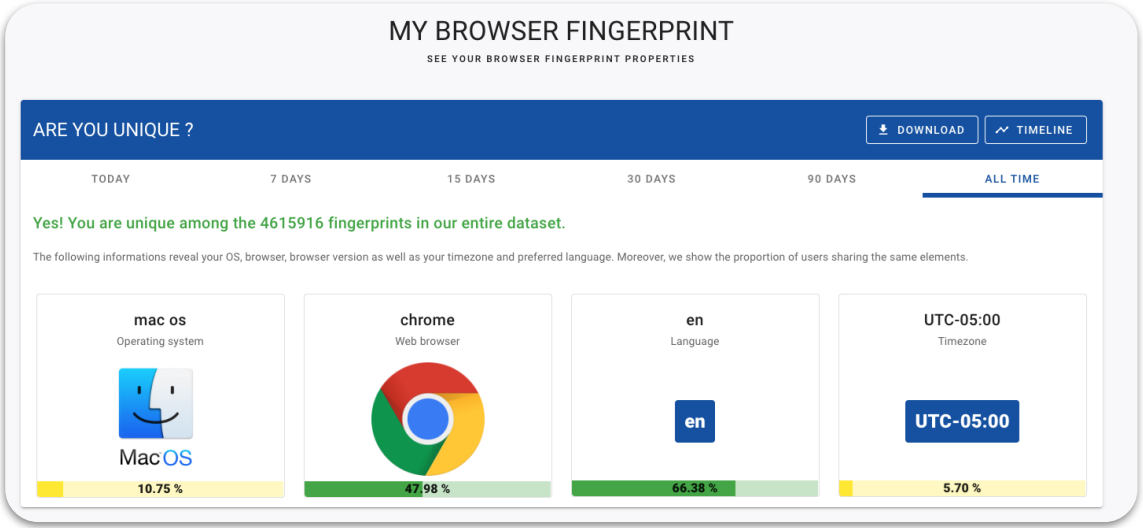


Name	Date Modified	Size	Kind
All Passwords.txt	Nov 6, 2024 at 1:34 PM	256 KB	Plain Text
Brute.txt	Nov 6, 2024 at 1:34 PM	7 KB	Plain Text
Chrome	Today at 10:39 AM	--	Folder
Clipboard.txt	Nov 6, 2024 at 1:34 PM	4 bytes	Plain Text
CocCoc	Today at 10:38 AM	--	Folder
Cookies	Dec 6, 2024 at 11:12 AM	--	Folder
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

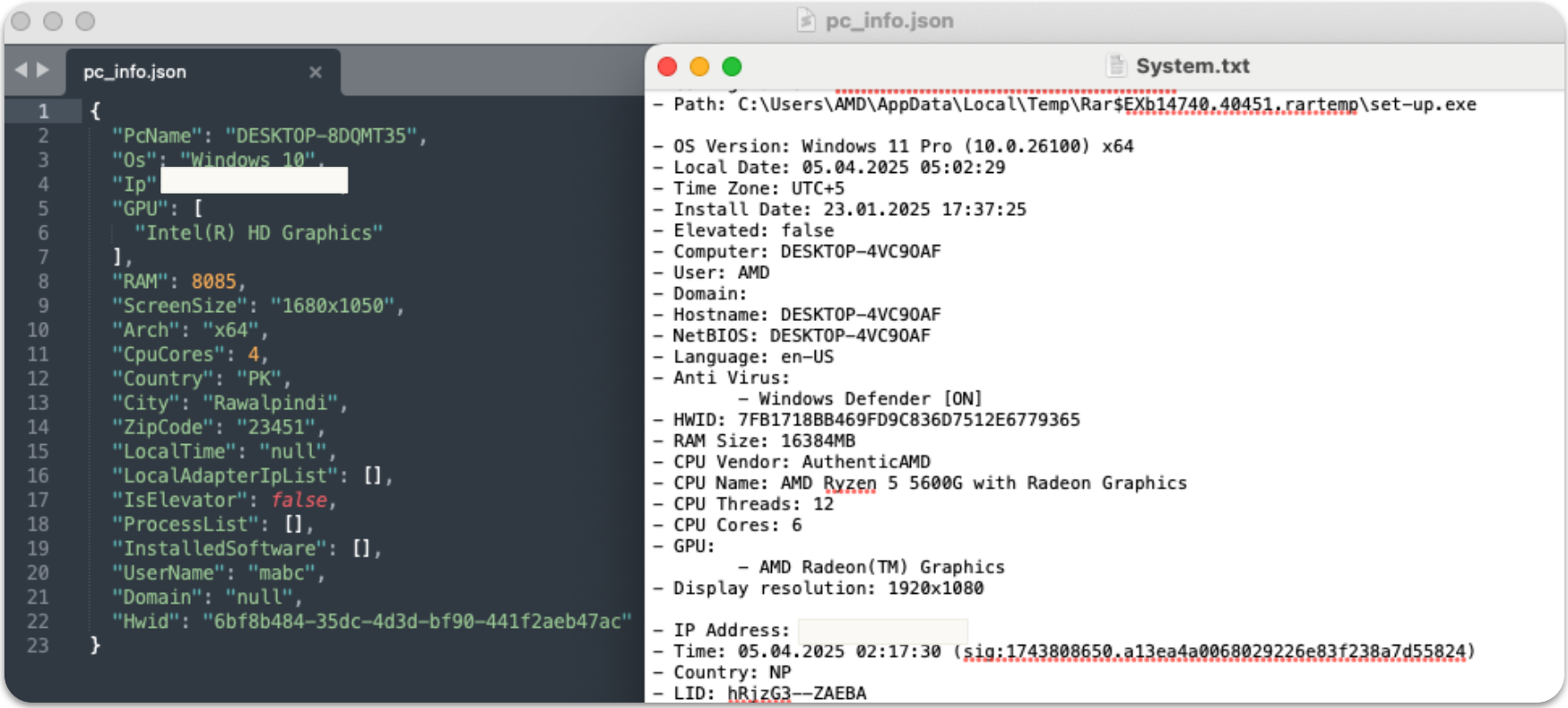
```
3501    nk.com.vn  TRUE    /   FALSE   1764044448  _ga GA1.1.2053379062.1729484447
3502    inhplus.com    TRUE    /   FALSE   1738642819  _gcl_aw GCL.1730866819.Cj0KCQiAoae5BhCNARIsADVLzZeqtR7O88Xp_FghYXJ10Z-2cojSSH
3503    uviet.vn   FALSE   /   TRUE    0   twk_idm_key RvqZ1eHjYxnly49ka6E-j
3504    bbank.com.vn   FALSE   /   FALSE   0   ASP.NET_SessionId   g35gnelrjwrxs3c1k5vncbdt
3505    bbank.com.vn   FALSE   /   FALSE   0   __RequestVerificationToken
        G1vwPWoUeMquHZnB030XjhULGEFUUK6s3pEJwhcVX62mzp9Xshu-uKXMVAIMrEWeYkWgfGYs3EKcZvpwlMQKmZKQmQ8szViL98fMT01
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%22uuid%22%3A%221.1vXHjdekfgTUAelU4ziaaZtn
        V0LENIzin8mENUx6izNuTJmkTh1E8YgclPsscaR3RJEToR0%22%2C%22version%22%3A3%2C%22domain%22%3A%22maychuviet.vn%22%2C%22ts%22%3A173
3509    bbank.com.vn   FALSE   /   FALSE   0   f5avr0932598578aaaaaaaaaaaaaaaa_cspm_
        GKLJIKLLMBAMDFHFIAPFOHFPKEIEBNDAGDKAFJDAJBAAOKFPMDJPGENJKONCPFCDHOCKNDNAKNKBCJADBEFABMLHGGEEHFLOMADEFOIJOBODCDFOIACENHHEIDA
3510    bbank.com.vn   FALSE   /   TRUE    0   f5avraaaaaaaaaaaaaaaa_session_
        INNPECKLEPJINOFEBFKIKKAPJCBLDHJADBHIBJNEIMBNDHBECNBAJDEDEEAPDBGICPFDJIICCGGKJNINBCJAINKMFNNNLLHCBHBDGDHBKCOKGPCIJHFCIEMDMPNFDDMH
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_c2WucdGJOrZ7IrK2bqm-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    362d7fe3904dfbfb2ndcae00lzmg7kqp~~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 user 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

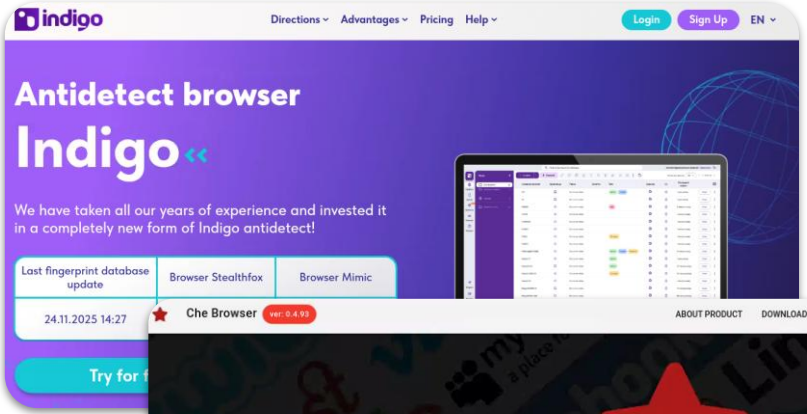


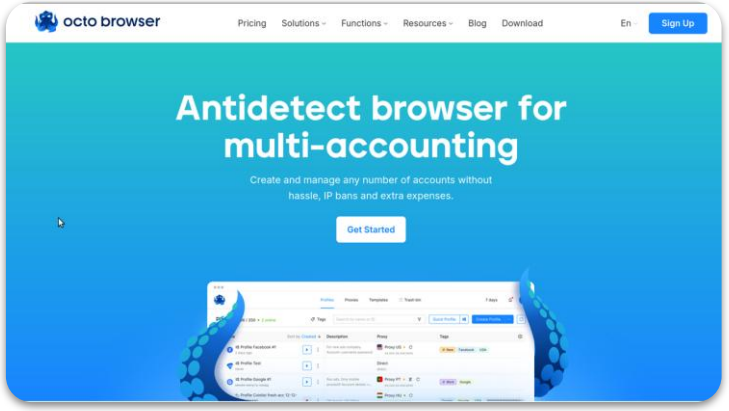
Browser Fingerprinting continued

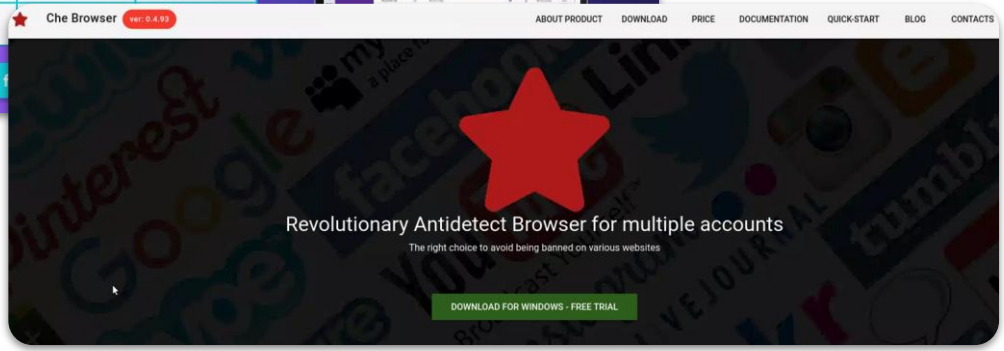


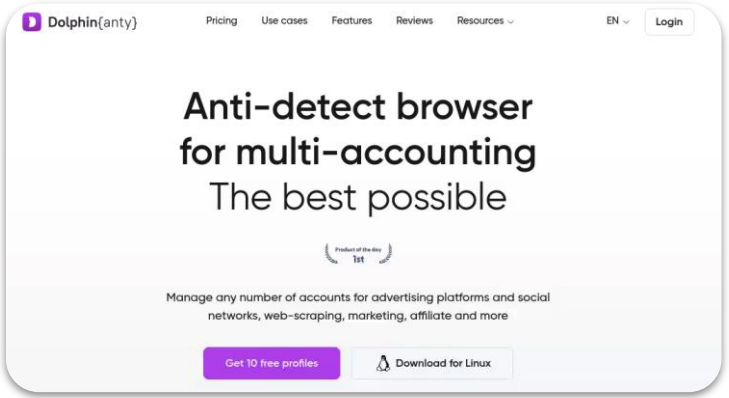
Anti-Detect Browsers

- Software designed to change and modify browser fingerprints

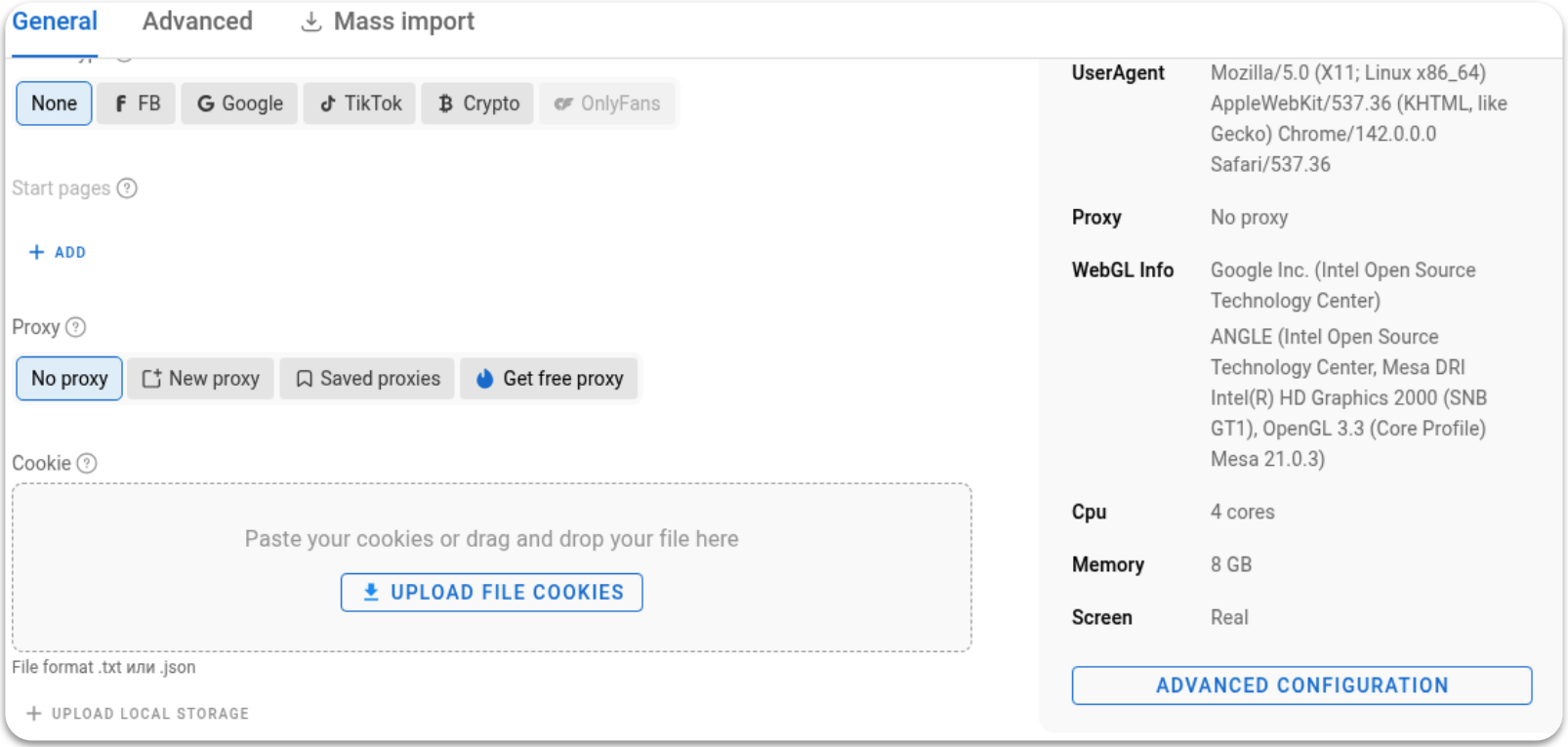




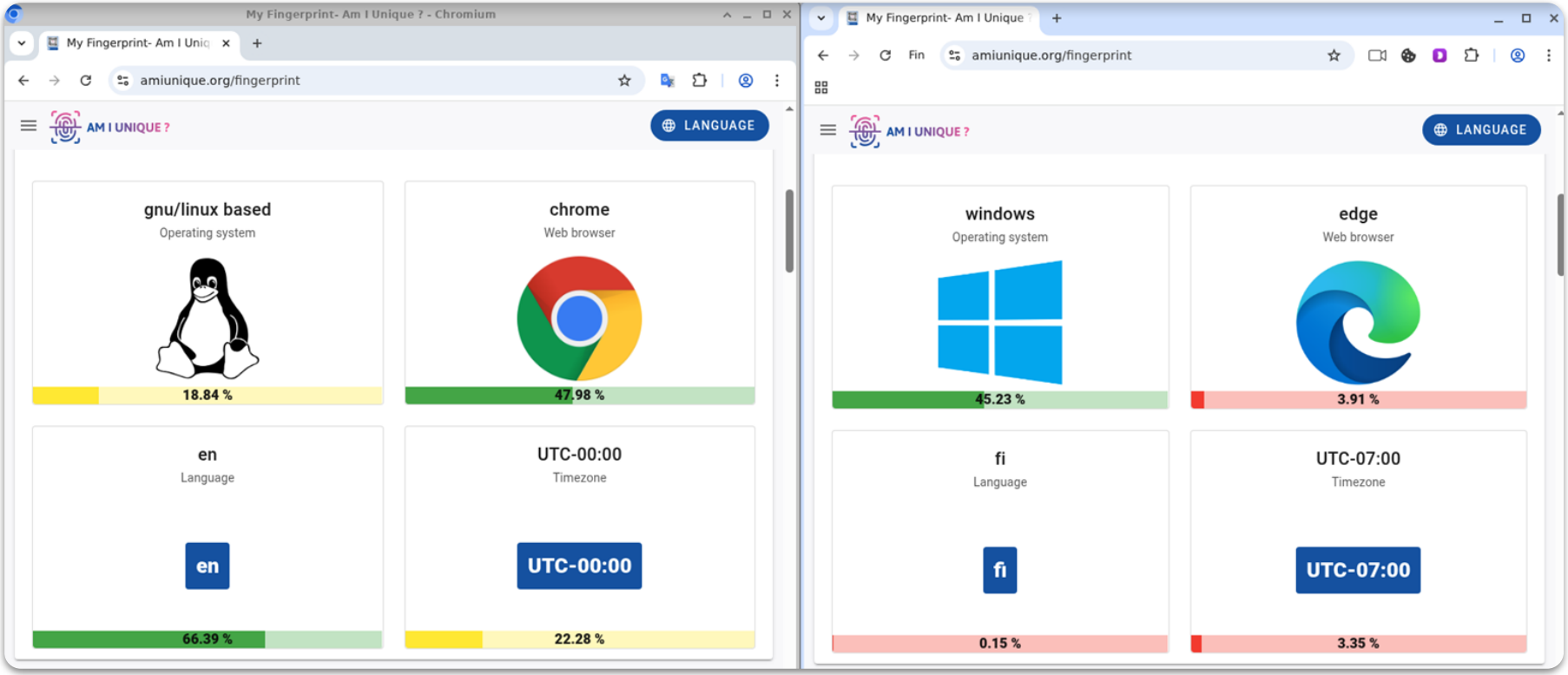




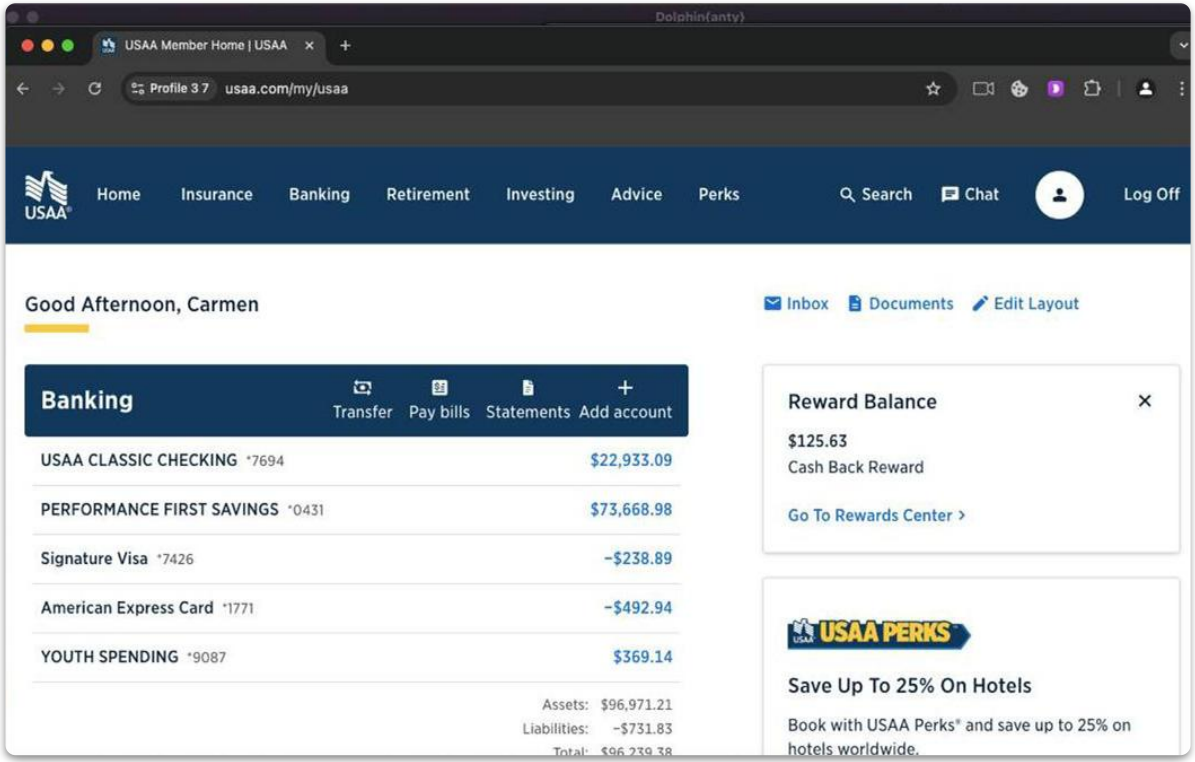
Anti-Detect Browsers



Anti-Detect Browsers

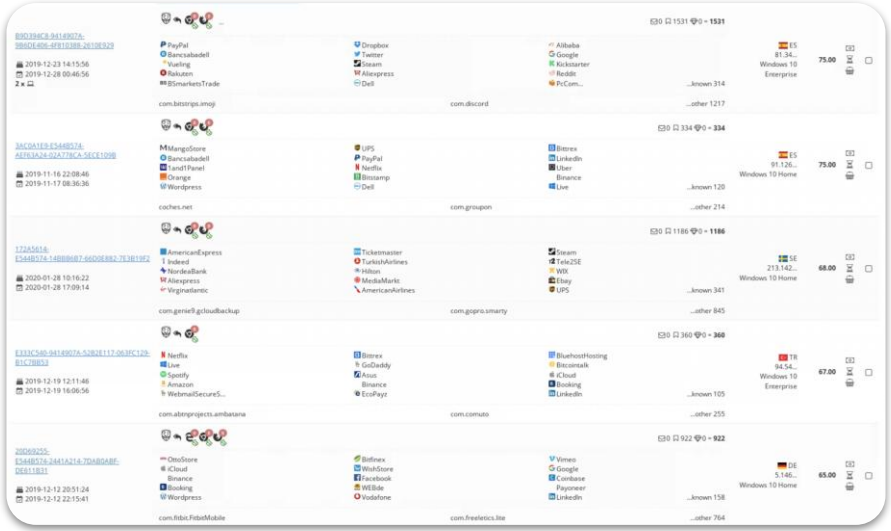


Antidetect Browsers



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.

The 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 fingeprints
   - bot with both logs and fingeprints +
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. **Congrads!** 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**

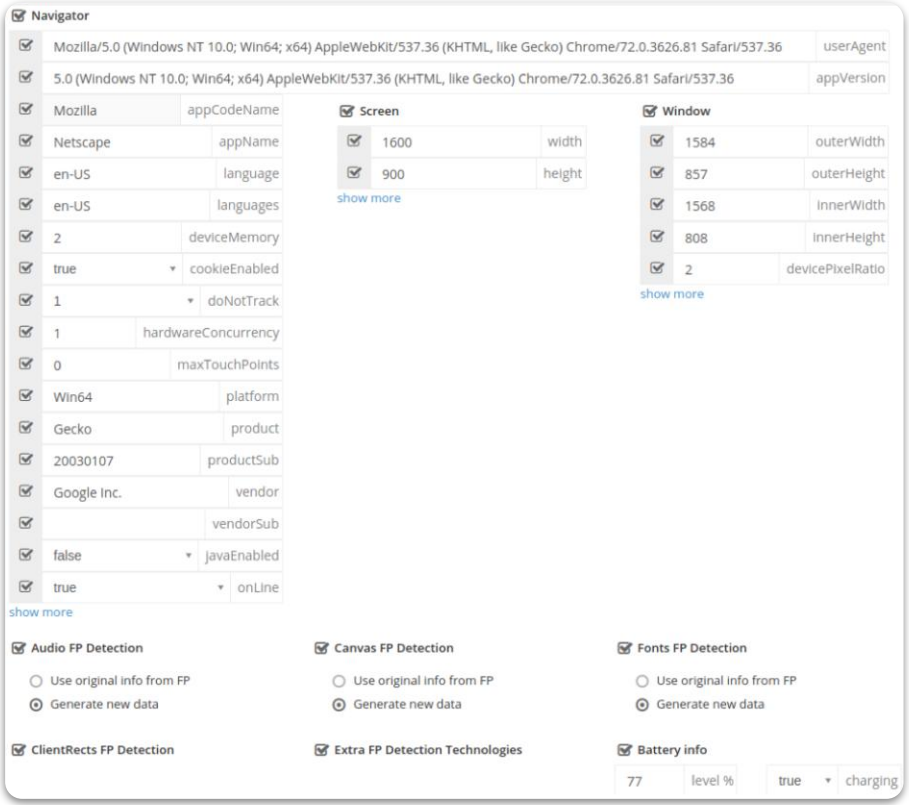
* Most relevant and stable Chrome-like Browser at the moment **SRWare Iron**
Use **old versions** of the browser: 69, 70, 71, 72.
http://download1.srware.net/old/iron/win/installer/
Starting from version 73 cookies may be imported **not correctly**.

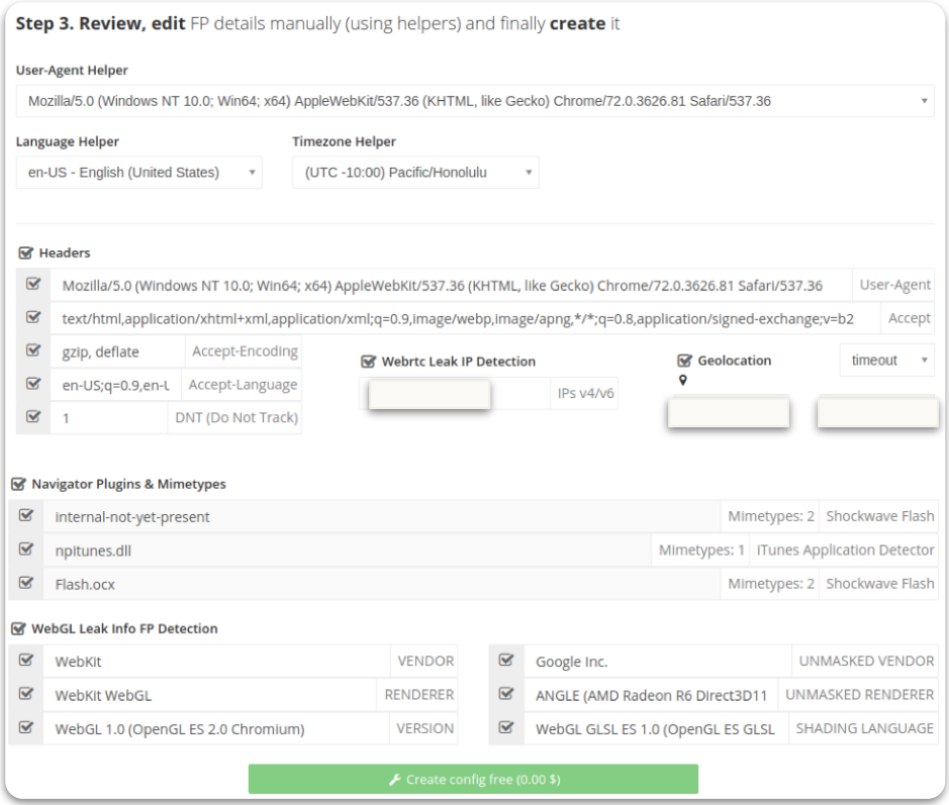
The plugin may be installed **automatically** or **manually** by dragging and dropping into the More Tools -> Extensions of your browser.

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 differrent Chromium-based browsers:

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


Navigator
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36 userAgent
5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36 appVersion
Mozilla appCodeName
Netscape appName
en-US language
en-US languages
2 deviceMemory
true cookieEnabled
1 doNotTrack
1 hardwareConcurrency
0 maxTouchPoints
Win64 platform
Gecko product
20030107 productSub
Google Inc. vendor
vendorSub
false javaEnabled
true onLine
show more
Screen
1600 width
900 height
show more
Window
1584 outerWidth
857 outerHeight
1568 innerWidth
808 innerHeight
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
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
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b2 Accept
gzip, deflate Accept-Encoding
en-US;q=0.9,en-L Accept-Language
1 DNT (Do Not Track)
Webrtc Leak IP Detection
IPs v4/v6
Geolocation
timeout
Navigator Plugins & Mimetypes
internal-not-yet-present Mimetypes: 2 Shockwave Flash
npitunes.dll Mimetypes: 1 iTunes Application Detector
Flash.ocx Mimetypes: 2 Shockwave Flash
WebGL Leak Info FP Detection
WebKit VENDOR
WebKit WebGL RENDERER
WebGL 1.0 (OpenGL ES 2.0 Chromium) VERSION
Google Inc. UNMASKED VENDOR
ANGLE (AMD Radeon R6 Direct3D11 UNMASKED RENDERER
WebGL GLSL ES 1.0 (OpenGL ES GLSL SHADING LANGUAGE
Create config free (0.00 $)