

imperva

The Plague of Advanced Bad Bots

Deconstructing the Malicious Bot

Problem

Yohann Sillam
Security Researcher

VINTED, THE ONLINE SALES PLATFORM, VICTIM OF A MAJOR HACKING

Presentation

Yohann Sillam

Security Researcher at Imperva

4 years of research in cyber security

Malware Analysis

Web application security



Agenda

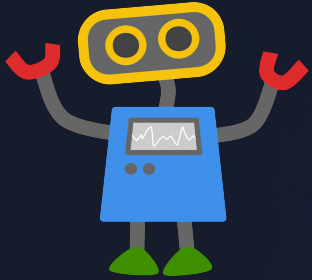
- Ecosystem
- Structure
- Evasion techniques

Ecosystem | Structure | Evasions

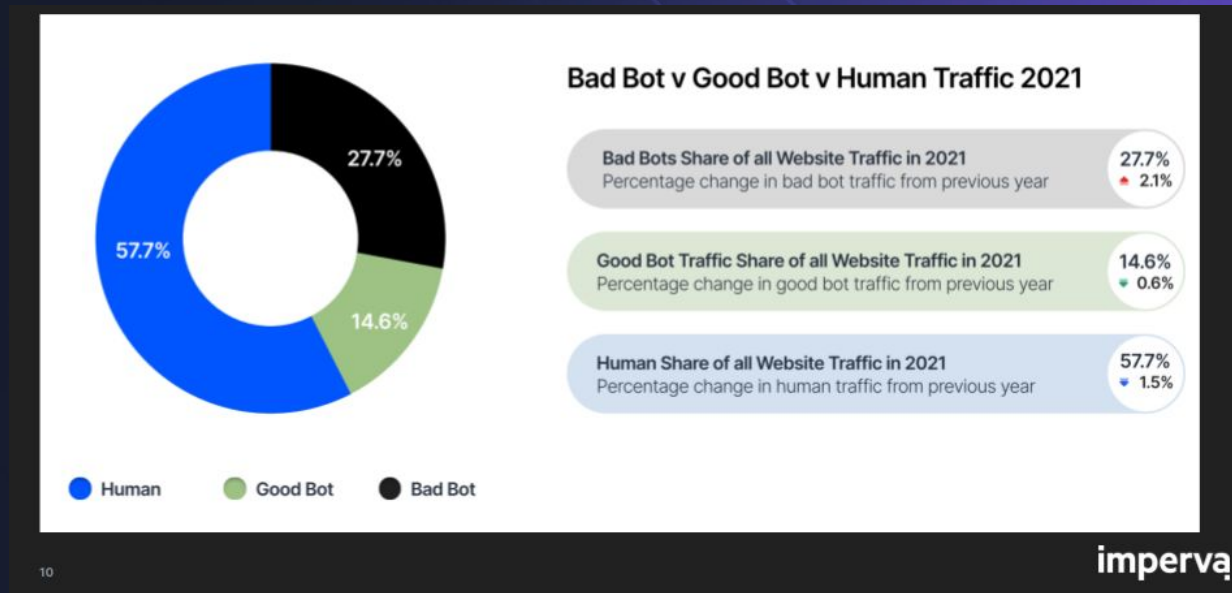
BOTS : Softwares automating actions on the Internet

Ecosystem | Structure | Evasions

BOTS : Softwares automating actions on the Internet



Ecosystem | Structure | Evasions



Ecosystem | Structure | Evasions

Bad bots - Credential stuffing (eg OpenBullet)

The screenshot shows the OpenBullet 1.2.2 application interface. At the top, there is a menu bar with options: Runner, Proxies, Wordlists, Configs, Hits DB, Tools, Plugins, Settings, and About. Below the menu, there is a progress bar and a 'Bots: 1' indicator. The 'Test On:' field is set to 'https://google.com' and the 'Success Key:' is 'title>Google'. A table of proxies is displayed with columns: Type, Host, Port, Username, Password, Country, Working, Ping, Chain, and Last Checked. The table contains 35 rows of proxy data. On the right side, there are buttons for 'CHECK', 'Import', 'Export', 'Delete', 'Delete All', 'More Actions', 'Del. Not Working', 'Del. Duplicates', and 'Del. Untested'. Below these buttons is a 'STATISTICS' section showing: Total: 35, Tested: 35, Working: 35, Not Working: 0, HTTP: 1, SOCKS4: 3, SOCKS4a: 8, SOCKS5: 23, Chain: 0. At the bottom right, there is an 'OPTIONS' section with a checked box for 'Only Untested'.

| Type | Host | Port | Username | Password | Country | Working | Ping | Chain | Last Checked |
|---------|------|-------|----------|----------|---------|---------|------|-------|---------------------|
| Socks4a | | 51 | 8008 | | | YES | 2327 | False | 3/2/2021 3:44:44 PM |
| Socks4a | | 137 | 9160 | | | YES | 2542 | False | 3/2/2021 4:18:21 PM |
| Socks4a | | 0.42 | 8080 | | | YES | 1624 | False | 3/2/2021 4:15:51 PM |
| Socks5 | | 9.199 | 8080 | | | YES | 2183 | False | 3/2/2021 3:46:57 PM |
| Socks4 | | | 23 | | | YES | 2644 | False | 3/2/2021 4:06:06 PM |
| Socks4a | | 5 | 2222 | | | YES | 1921 | False | 3/2/2021 4:23:38 PM |
| Socks4a | | 186 | 9200 | | | YES | 7029 | False | 3/2/2021 4:15:08 PM |
| Socks5 | | 8.215 | 8080 | | | YES | 1553 | False | 3/2/2021 3:46:54 PM |
| Http | | 77 | 5432 | | | YES | 1877 | False | 3/2/2021 3:30:26 PM |
| Socks4 | | 137 | 9000 | | | YES | 5361 | False | 3/2/2021 4:00:55 PM |
| Socks4 | | 254 | 8080 | | | YES | 1547 | False | 3/2/2021 3:37:43 PM |
| Socks4a | | 59 | 9095 | | | YES | 1352 | False | 3/2/2021 4:22:14 PM |
| Socks4a | | 241 | 9051 | | | YES | 5458 | False | 3/2/2021 4:14:09 PM |
| Socks4a | | 8.130 | 9080 | | | YES | 1205 | False | 3/2/2021 4:14:48 PM |
| Socks5 | | 8.242 | 9080 | | | YES | 6165 | False | 3/2/2021 9:52:43 PM |
| Socks5 | | 241 | 9080 | | | YES | 2691 | False | 3/2/2021 9:55:31 PM |
| Socks5 | | 8.130 | 9070 | | | YES | 3591 | False | 3/2/2021 9:56:05 PM |
| Socks5 | | 8.130 | 9084 | | | YES | 2228 | False | 3/2/2021 9:56:09 PM |
| Socks5 | | 8.130 | 9090 | | | YES | 3198 | False | 3/2/2021 9:56:12 PM |
| Socks5 | | 8.130 | 9103 | | | YES | 3305 | False | 3/2/2021 9:56:14 PM |
| Socks5 | | 109 | 9051 | | | YES | 5508 | False | 3/2/2021 9:57:54 PM |
| Socks5 | | 4.193 | 9200 | | | YES | 2200 | False | 3/2/2021 9:58:15 PM |
| Socks5 | | 3.11 | 9999 | | | YES | 6566 | False | 3/2/2021 9:58:36 PM |
| Socks5 | | 0.123 | 8001 | | | YES | 1386 | False | 3/2/2021 9:59:38 PM |

Ecosystem | Structure | Evasions

Bad bots - Account creation bots (eg AYCD)

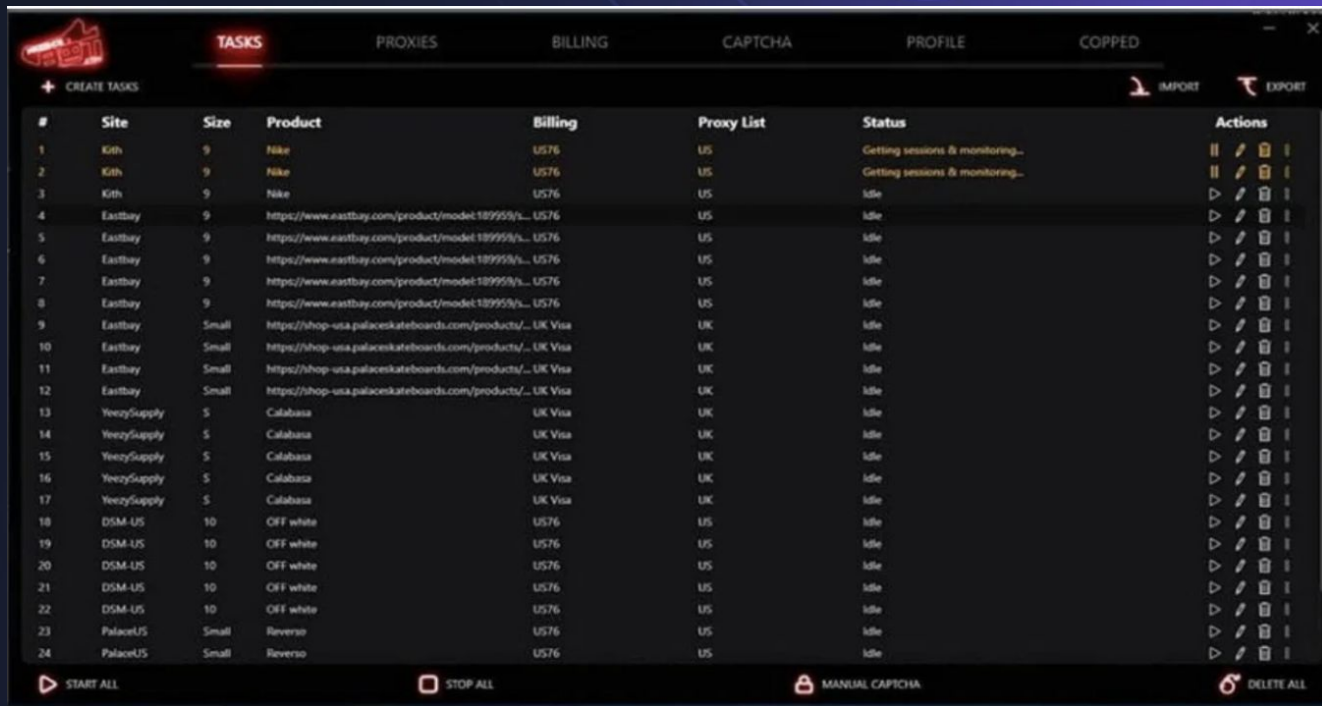
The screenshot shows a web interface for generating accounts. At the top, there are navigation tabs: Servers, Proxies, Cookies, Accounts, Variants, Profiles, and Settings. Below the navigation, there are buttons for 'Create' and 'Edit', and a status indicator 'Selected Items: 0'. The main content area is titled 'Generate New Accounts' and contains several configuration sections:

- Categories:** A table with columns for Categories, #, Username, and Status.
- Category:** A dropdown menu set to 'Amazon'.
- Store:** A dropdown menu set to 'Amazon'.
- Proxy Categories:** A dropdown menu set to 'Smart Residential (US) 5...', with 'Select All' and 'Clear' buttons. Below it are checkboxes for 'Retry failed tasks with a random proxy', 'Autofill Billing and Shipping', 'Send to Discord', and 'Show Browser'.
- Mail Provider:** A dropdown menu set to 'Gmail'.
- Mail Credentials:** A dropdown menu set to 'Stealthycatchall@gmail.com', with a checked checkbox and 'Select All' and 'Clear' buttons.
- Amount of Accounts Limit:** A dropdown menu set to 'Profiles', with 'Catchall' and 'Emails' options.
- SMS Provider:** An empty dropdown menu.
- SMS Credentials:** An empty dropdown menu.
- Phone Number Countries:** An empty dropdown menu.
- Countries Priority Order:** An empty text area.

At the bottom right, there are 'Cancel' and 'Generate' buttons.

Ecosystem | Structure | Evasions

Bad bots - Scalping bots (eg NSB)



The screenshot shows a software interface with a dark theme. At the top, there are navigation tabs: TASKS (highlighted), PROXIES, BILLING, CAPTCHA, PROFILE, and COPPED. Below the tabs is a '+ CREATE TASKS' button and 'IMPORT' and 'EXPORT' icons. The main area contains a table with 24 rows of task configurations. The table has columns for #, Site, Size, Product, Billing, Proxy List, Status, and Actions. The 'Status' column shows 'Getting sessions & monitoring...' for the first two rows and 'Idle' for the rest. The 'Actions' column contains icons for play, stop, refresh, and delete.

| # | Site | Size | Product | Billing | Proxy List | Status | Actions |
|----|------------|-------|---|---------|------------|----------------------------------|---------|
| 1 | Kith | 9 | Nike | US76 | US | Getting sessions & monitoring... | ⏮ ⏪ ⏩ ⏭ |
| 2 | Kith | 9 | Nike | US76 | US | Getting sessions & monitoring... | ⏮ ⏪ ⏩ ⏭ |
| 3 | Kith | 9 | Nike | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 4 | Eastbay | 9 | https://www.eastbay.com/product/model/189959/... | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 5 | Eastbay | 9 | https://www.eastbay.com/product/model/189959/... | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 6 | Eastbay | 9 | https://www.eastbay.com/product/model/189959/... | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 7 | Eastbay | 9 | https://www.eastbay.com/product/model/189959/... | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 8 | Eastbay | 9 | https://www.eastbay.com/product/model/189959/... | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 9 | Eastbay | Small | https://shop-usa.palaceskateboards.com/products/... | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 10 | Eastbay | Small | https://shop-usa.palaceskateboards.com/products/... | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 11 | Eastbay | Small | https://shop-usa.palaceskateboards.com/products/... | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 12 | Eastbay | Small | https://shop-usa.palaceskateboards.com/products/... | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 13 | YezySupply | S | Calabasa | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 14 | YezySupply | S | Calabasa | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 15 | YezySupply | S | Calabasa | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 16 | YezySupply | S | Calabasa | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 17 | YezySupply | S | Calabasa | UK Visa | UK | Idle | ▶ ⏪ ⏩ ⏭ |
| 18 | DSM-US | 10 | OFF white | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 19 | DSM-US | 10 | OFF white | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 20 | DSM-US | 10 | OFF white | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 21 | DSM-US | 10 | OFF white | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 22 | DSM-US | 10 | OFF white | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 23 | PalaceUS | Small | Reverso | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |
| 24 | PalaceUS | Small | Reverso | US76 | US | Idle | ▶ ⏪ ⏩ ⏭ |

At the bottom of the interface, there are four buttons: 'START ALL' (play icon), 'STOP ALL' (stop icon), 'MANUAL CAPTCHA' (lock icon), and 'DELETE ALL' (trash icon).

Ecosystem | Structure | Evasions

Bad bots - OneClick bot

| Name | Proxy | Action Log | Status |
|---------------------|-------------------|----------------|--------|
| aycdtest1@gmail.com | 99.99.88.12:12... | Taking a break | Good |
| aycdtest2@gmail.com | 99.99.88.12:1111 | Taking a break | Good |
| aycdtest3@gmail.com | 99.99.88.12:4... | Reading Mail | Good |
| aycdtest4@gmail.com | 99.99.88.12:4... | Reading Mail | Good |
| aycdtest5@gmail.com | 99.99.88.12:14... | Scheduled | Good |
| aycdtest6@gmail.com | 99.99.88.12:4... | Scheduled | Good |

Ecosystem | Structure | Evasions

Bad bots - OneClick bot

<https://recaptcha-demo.appspot.com/recaptcha-v3-request-scores.php>




reCAPTCHA demo

Request scores

[Home](#)

The reCAPTCHA v3 API provides a confidence score for each request.

NOTE: This is a sample implementation, the score returned here is not a reflection on your Google account or type of traffic. In production, refer to [admin interface](#) and adjust your own threshold accordingly. **Do not raise issues regarding the score you see here.**

1. reCAPTCHA script loading
2. Press the button containing a traffic light to continue.   

[Try again](#)

Ecosystem | Structure | Evasions


Developer Communities



Ecosystem | Structure | Evasions

Developer Communities

XOURCES Sources Yesterday at 7:40 AM
antibot <https://www.playstation.com/>

 **Botty McBotface** BOT Yesterday at 7:40 AM

Test results for <https://www.playstation.com/>

✓ All good, none of those detected:

Shape Security, DataDome, Distil, Imperva, Incapsula, PerimeterX, Akamai, FingerprintJS, FingerprintJS Pro, Kasada, WhiteOps, ShieldSquare, ThreatMetrix, F5, Cloudflare, Arkose Labs, Human Security, Sift, Ocule, Reblaze, Forter Protection, Meetrics Check, reCAPTCHA, generic fingerprinting & bot detection

Title
Offizielle PlayStation®-Website: Konsolen, Spiele, Zubehör und mehr

| Status | Requests | Browser IP |
|--------|----------|-------------|
| 200 | 100 | DE (server) |

Requested by
[@Xources](#)

Keep in mind this is a preview version of the bot.

Ecosystem | Structure | Evasions

User communities - Market places

easyrentals

TIDAL

BOTMART

TicketBots.net 10 YEARS & counting...

BOT-BROKER

Buy and Sell Sneaker Bots

CopSupply

MLAB
MOST ADVANCED BOT

bots^{that}work

TheCopShop

One-Stop Discord Marketplace

SNEAKER SQUAD

Tiger

Tiger zone



Botstash

Whop

Ecosystem | Structure | Evasions

User communities - Underground forums

REDDIT MASS DM BOT

07-03-2022, 12:54 PM

REDDIT MASS DM BOT

Lifetime Licenses: \$100

Features Include:
Multi Threading
Anti-Fingerprint Detection *
IP Conflict Detection for Account Creation
You are only limited to the amount of DM's according to your account age / restrictions

Anti-Fingerprint Detection:
Generates a Unique OS and Browser Fingerprint
Ever changing Hardware Canvas
Ever changing Font Database
Ever Changing Browser Addons / Modules
Ever changing Soundcard / USB devices
Fingerprints Tested prior to use against different databases to ensure it is unique and without error

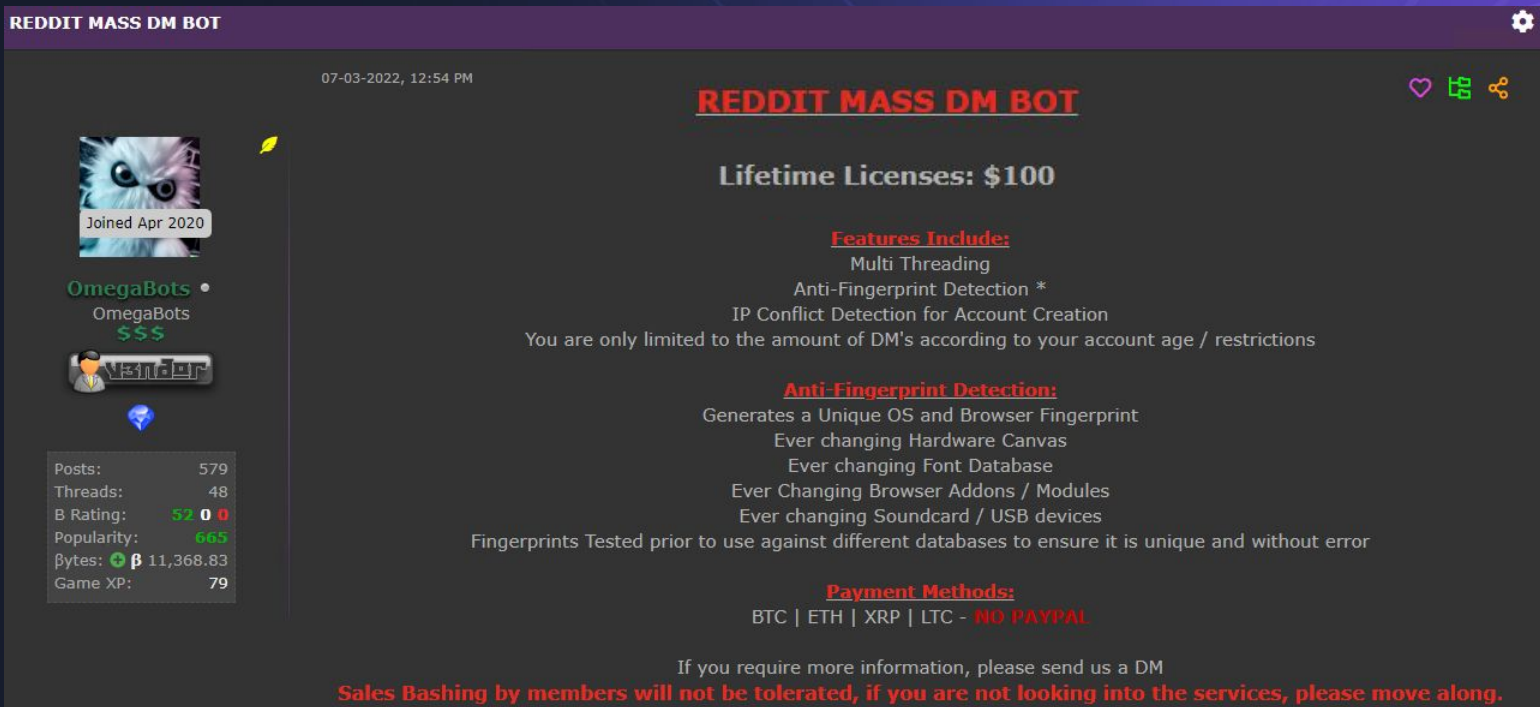
Payment Methods:
BTC | ETH | XRP | LTC - **NO PAYPAL**

If you require more information, please send us a DM
Sales Bashing by members will not be tolerated, if you are not looking into the services, please move along.

Joined Apr 2020

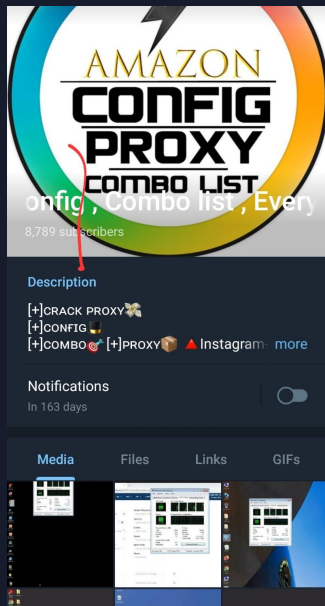
OmegaBots
OmegaBots
\$\$\$

Posts: 579
Threads: 48
B Rating: 52 0 0
Popularity: 665
Bytes: 11,368.83
Game XP: 79

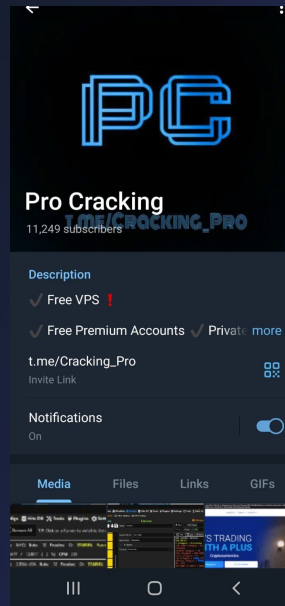


Ecosystem | Structure | Evasions

User Communities - Cracking groups



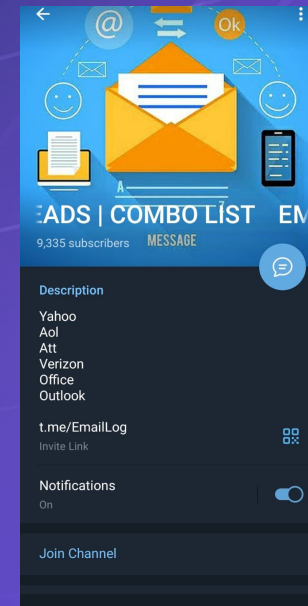
CrackingHit



Pro Cracking



Config's Combo



EmailLog

Agenda

- Ecosystem
- Structure
- Evasion techniques

Ecosystem | **Structure** | Evasions

Automation framework



Ecosystem | **Structure** | Evasions

Automation framework

Webdriver

- High level control
- Simpler management of multiple windows / tabs
- Cross browser
- Miss low level capability
- Slower



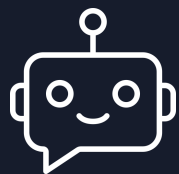
(Chrome Devtool Protocol) CDP

- Low level control
- Chromium based browsers
- Faster



Ecosystem | **Structure** | Evasions

Webdriver vs CDP protocol



`/session/:sessionId/url`



webdriver

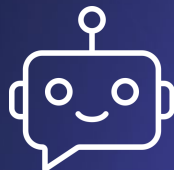


Internal protocol



Webdriver protocol

CDP



Page.navigate

CDP protocol



Ecosystem | Structure | Evasions

Proxies



| Page | Type | Status | Level | Name | Date |
|------|-------|---------|-------|--------------|------------------|
| 1 | Elite | Success | 1 | 192.168.1.1 | 2015-04-10 12:30 |
| 2 | Elite | Success | 1 | 192.168.1.2 | 2015-04-10 12:30 |
| 3 | Elite | Success | 1 | 192.168.1.3 | 2015-04-10 12:30 |
| 4 | Elite | Success | 1 | 192.168.1.4 | 2015-04-10 12:30 |
| 5 | Elite | Success | 1 | 192.168.1.5 | 2015-04-10 12:30 |
| 6 | Elite | Success | 1 | 192.168.1.6 | 2015-04-10 12:30 |
| 7 | Elite | Success | 1 | 192.168.1.7 | 2015-04-10 12:30 |
| 8 | Elite | Success | 1 | 192.168.1.8 | 2015-04-10 12:30 |
| 9 | Elite | Success | 1 | 192.168.1.9 | 2015-04-10 12:30 |
| 10 | Elite | Success | 1 | 192.168.1.10 | 2015-04-10 12:30 |

GSA proxy scraper

UnitedCracker | Account Cracking | Combs | Config | Proxy | ...
UPProxy Tool | Scraper And Checker | Latest Version
#Tool

Always use rdp for cracking tools.

Features:
- Auto Scrape & Check
- Auto save proxies separately (Elite/Anon/Transparent/Scraped)
- Multi Threaded
- Simple & HQ GUI

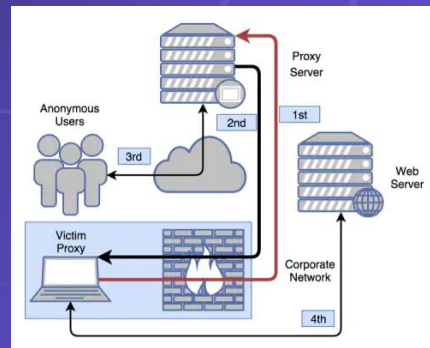
<https://gofile.io/d/pCrv5E>

@UnitedCracker
Share & Support

© 2652 edited 9:10 AM

UPProxy scraper tool

ProxyBack malware turns User Systems Into Proxies Without Consent

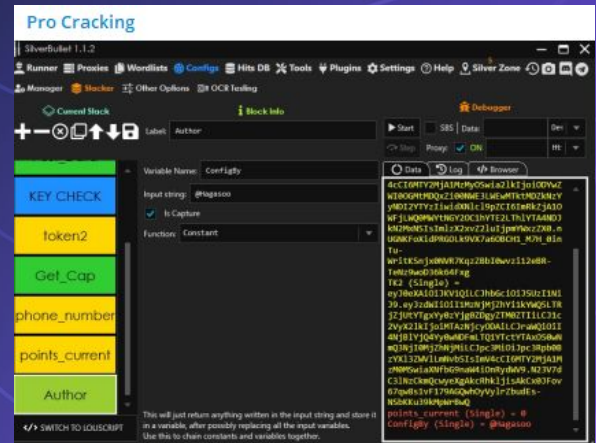


ProxyBack malware

Ecosystem | Structure | Evasions

Configuration

- Scraping Template
- Credential Stuffing Config
- Scalping Task and Account



```
• #Config { SayWeee }
-- -- INFORMATION -- --
🌱 • For SilverBullet Program
🌐 • Url : SayWeee.com
📁 • Format : { .svb }
📱 • Api : Yes
🚫 • Target : Shopping
🌐 • Proxy : ✓ | HQ
🌐 • Combo Type : E:P
📱 • Bot : 1-100
💾 • AutoSave : ✗
🔍 • Capture : ✓
❗ • Requirement : -

-----
👤 | @Hagaso
📍 Channel: T.me/Cracking_Pro
```

Ecosystem | **Structure** | Evasions

3rd parties

Anti-Captcha

Human based

Example 2Captcha



AI based

Example CapMonster



Hybrid

Example
DeathByCaptcha



Ecosystem | **Structure** | Evasions

3rd parties

Anti-Captcha Stacking (Ex AYCD Autosolve)

Anti-captcha stacking

Disconnect Sync Dashboard Go To Das

| Priority | Service | Status | Service | Name | Balance | Selected |
|----------|-------------|---------|-------------|-------------------|---------|-------------------------------------|
| 1 | CapMonster | Primary | 2Captcha | 2Cap Test | \$0 | <input checked="" type="checkbox"/> |
| 2 | 2Captcha | Active | AntiCaptcha | AntiCap - Eman | \$4.9 | <input checked="" type="checkbox"/> |
| 3 | AntiCaptcha | Active | CapMonster | CapMonster - E... | \$9.84 | <input checked="" type="checkbox"/> |

Ecosystem | Structure | Evasions

3rd parties

Virtual Phone service



Ecosystem | Structure | Evasions

Example use case - NSB bot

The screenshot displays the 'TASKS' management interface. At the top, there are navigation tabs: TASKS, PROXIES, BILLING, CAPTCHA, MONITORS, PROFILE, and COPPED. Below the tabs, there is a 'CREATE TASKS' button and a search filter 'Filter tasks...'. A table lists tasks with columns: #, Site, Size, Product, Billing, Proxy List, and Status. One task is visible: #1, Site: 100Thieves, Size: 21, Product: https://100thieves.com/products/overworld..., Billing: Default25, Proxy List: Default, Status: Monitoring... An 'Edit Task' modal window is open, showing a dropdown menu for '100Thieves' with a list of products: All (autocreate & start from all monitors - uses smart account pool - RISKY), All (notify only), 100Thieves, 1290sqm, 12amrun (highlighted), 510Skateboarding, A-Ma-Manlere, AboveTheCloudsStore, ACDGallery, and ActiveAthlete88. Other settings in the modal include 'Safe Mode', '21', 'Preset Payment Gateway', and 'Use shared monitor' (checked). At the bottom, there are radio buttons for 'Advanced' (checked), 'Schedule Task', and 'Require Login' (checked), along with 'CLOSE' and 'SUBMIT' buttons.

| # | Site | Size | Product | Billing | Proxy List | Status |
|---|------------|------|--|-----------|------------|---------------|
| 1 | 100Thieves | 21 | https://100thieves.com/products/overworld... | Default25 | Default | Monitoring... |

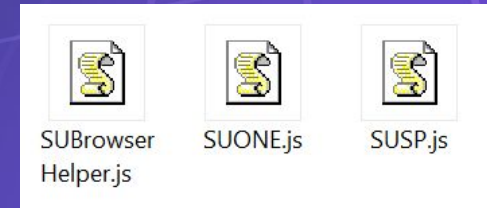
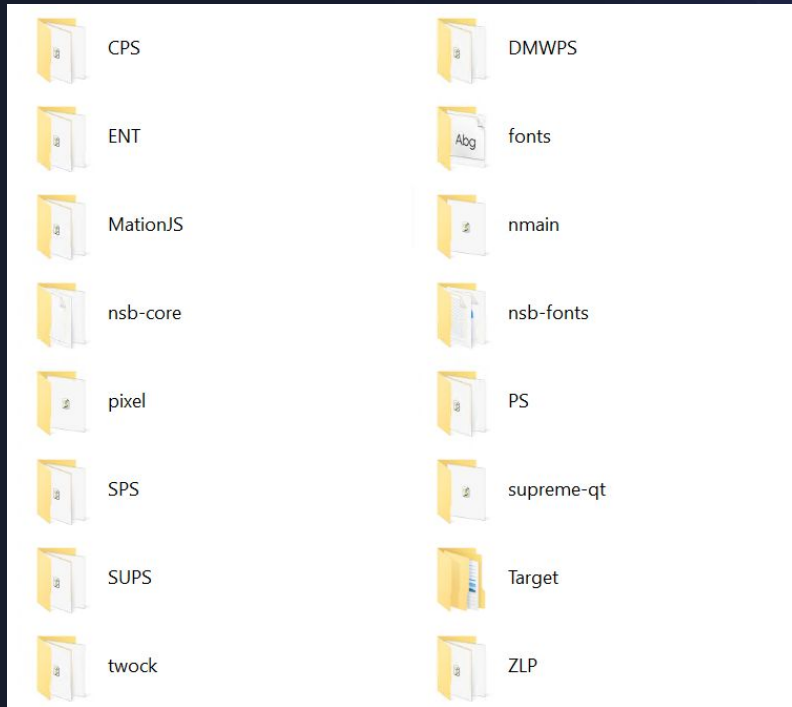
Ecosystem | **Structure** | Evasions

Example use case - NSB bot



Ecosystem | **Structure** | Evasions

Example use case - NSB bot



Ecosystem | Structure | Evasions

Example use case - NSB bot

```
573 'HRzOM': function(_0x847c37, _0x57f191, _0x5a4690) {
574     return _0x847c37(_0x57f191, _0x5a4690);
575 }
576 };
577 let _0x1e52ab = {
578     'uri': _0x12e2f2[a0_0x5d63('0x6c', 'e0RU')]( _0x12e2f2[a0_0x5d63('0x111', 'p3GN')]( _0x12e2f2[a0_0x5d63('0x93', '4MSX')](
    (_0x12e2f2[a0_0x5d63('0x6d', '4h&e')]( _0x12e2f2[a0_0x5d63('0xdc', 'ESXB')]( _0x12e2f2[a0_0x5d63('0xf', 'q]G9')]( _0x12e2f2
    [a0_0x5d63('0x124', ']nf9')]( _0x12e2f2[a0_0x5d63('0x4f', 'F1xf')], _0x12e2f2[a0_0x5d63('0xb5', '$6LY')]), _0x12e2f2
    [a0_0x5d63('0x130', 'IvSG')]), '.', _0x12e2f2[a0_0x5d63('0x157', 'R2i&')]), '.', 'co') + '/', a0_0x5d63('0x15b', 'wpvF')
    ),
    'json': {
    579     'key': fs[a0_0x5d63('0x1c', '0TeP')](path[a0_0x5d63('0x87', '%2e')](app[a0_0x5d63('0xf9', 'dnGH')]( _0x12e2f2
    [a0_0x5d63('0x10', 'Vcoq')]) + _0x12e2f2[a0_0x5d63('0x5', 'dnGH')]))[a0_0x5d63('0x75', 'kR8k')]( ),
    581     'hardware_id': _0x12e2f2[a0_0x5d63('0x8c', '0MFE')](machineIdSync)
    582     },
    583     'headers': {
    584         'User-Agent': a0_0x5d63('0x76', 'Vcoq')
    585     },
    586     'method': _0x12e2f2[a0_0x5d63('0x15e', '*e3Y')]
    587     };
    588     _0x12e2f2[a0_0x5d63('0x1f', 'KJM$')](request, _0x1e52ab, () => {
    589         fs[a0_0x5d63('0x58', '0500')](path[a0_0x5d63('0xc2', '0[fs')]( _0x12e2f2[a0_0x5d63('0x139', '0NVE')](require, _0x12e2f2
    [a0_0x5d63('0x13', '0MFE')]))[a0_0x5d63('0xd4', 'j]ln')][a0_0x5d63('0x9a', '0[fs')]( _0x12e2f2[a0_0x5d63('0xe0', 'wpvF')]),
    _0x12e2f2[a0_0x5d63('0xdb', 'jx(8')]))], keyInfo = {
    590             'approved': !![]
    591         }, app[a0_0x5d63('0x7f', '32V@')]( );
    592     });
    593     }, process['on'](a0_0x5d63('0x51', 'p3GN'), _0x5d0af5 => {
    594         const _0x1a9e02 = {
    595             'lVdzs': function(_0x453666, _0x1e73bb) {
    596                 return _0x453666 === _0x1e73bb;
    597             },
    598             'FrkRk': a0_0x5d63('0x5a', '0x85')
```

Ecosystem | Structure | Evasions

Example use case - NSB bot

2 approaches : **Static** | Dynamic

```
'IMCA''], 'CS5Hy':b[xIIdUC5118b('0x9e5', 'R19d')], 'NjChV':b[xIIdUC5118b('0x22c', 'dXVJ')], 'oofoe':b[xIIdUC5118b('0x7f5', 'ISQ0')], 'MORmq':xIIdUC5118b('0xa99', 'AMT'), 'yramJ':b[xIIdUC5118b('0x67c', '5zE')], 'kVBgn':b[xIIdUC5118b('0x8eb', 'AS8(')], 'WGVDS':b[xIIdUC5118b('0x1d8', 'RI6P')], 'dYpWA':b[xIIdUC5118b('0xae', '79z(')], 'k3Rfp':b[xIIdUC5118b('0x585', '9r0z')], 'yFefi':b[xIIdUC5118b('0x976', 'cEcl')], 'Fobie':b[xIIdUC5118b('0x219', '8kGn')], 'nMLJa':xIIdUC5118b('0xcc4', 'IH[')], 'yGDH':b[xIIdUC5118b('0x54e', 'lTg')], 'Qwkfa':b[xIIdUC5118b('0x52f', 'RpP')], 'Hqo0h':b[xIIdUC5118b('0x6ef', 'dXVJ')], 'wnatg':b[xIIdUC5118b('0x3fo', 'ng5g')], 'dJpsP':xIIdUC5118b('0xe0f', 'frk1'), 'mqpl1':b[xIIdUC5118b('0x220', 'RpP')], 'ILKIF':b[xIIdUC5118b('0x18d', 'gont')], 'yTBPO':b[xIIdUC5118b('0xd37', '8kGr')], 'WmDIn':xIIdUC5118b('0xdba', 'knsV'), 'FS3Hg':b[xIIdUC5118b('0x919', 'frk1')], 'nUFVH':b[xIIdUC5118b('0x962', '@tS(')], 'Xeoly':xIIdUC5118b('0xbb9', 'zE(')], 'dMyyg':b[xIIdUC5118b('0x7a5', '5Z')], 'OwQQM':xIIdUC5118b('0x42e', 'SnoH'), 'wBtyl':b[xIIdUC5118b('0x27c', 'Flaw')], 'gXMMt':b[xIIdUC5118b('0x415', 'cEcl')], 'GarUD':b[xIIdUC5118b('0xb77', 'TmWx')], 'Wnrcy':b[xIIdUC5118b('0xc7a', 'ISQ0')], 'lIdJD':b[xIIdUC5118b('0xif', 'W6U')], 'mabrS':b[xIIdUC5118b('0x81', 'IMCA')], 'pkisa':b[xIIdUC5118b('0xedd', 'RpP')], 'jGkks':b[xIIdUC5118b('0x4ff', '8xK1')], 'VRDjk':xIIdUC5118b('0x118', 'cJbE'), 'MXPuU':b[xIIdUC5118b('0xec7', 'rv04')], 'xTIL':b[xIIdUC5118b('0x8de', 'AWT')], 'GFxWq':function(s,t,u){return b[xIIdUC5118b('0xa00', 'uX3W')](s,t,u)}; 'FKEYx':function(s,t){return b[xIIdUC5118b('0xadf', 'rqxv')](s,t)}; 'xvBLO':xIIdUC5118b('0x92a', 'r131'), 'IHent':b[xIIdUC5118b('0x2ea', 'vion')], 'ybaVJ':b[xIIdUC5118b('0xa80', 'IH[')], 'EqTJY':xIIdUC5118b('0xaf2', 'A58(')], 'Pc':b[xIIdUC5118b('0x8c2', 'LAK')], 'wXyKp':b[xIIdUC5118b('0x46', 'DaNc')], 'MJWhm':b[xIIdUC5118b('0x898', 'd10G')], 'uomgJ':b[xIIdUC5118b('0xc67', 'pw8L')], 'lVINW':function(s,t){return b[xIIdUC5118b('0x62a', 'W6U')](s,t)}; 'uomgJ':b[xIIdUC5118b('0xdd9', '@tS(')], 'nbvxD':function(s,t){return b[xIIdUC5118b('0x64a', 'LAK')](s,t)}; 'liWpq':b[xIIdUC5118b('0x5b', '5Z')], 'Jmopt':xIIdUC5118b('0x35b', 'uX3W'), 'rm5QF':b[xIIdUC5118b('0xe47', 'lTg')], 'ZGxun':b[xIIdUC5118b('0x3a1', '8kGr')], 'PKNOE':b[xIIdUC5118b('0x192', '5zE')], 'Yllbk':b[xIIdUC5118b('0x48b', '8xK1')], 'QwPpD':xIIdUC5118b('0xb3b', '8xK1'), 'EEVRd':xIIdUC5118b('0xs', 'ISQ0'), 'kvrqB':xIIdUC5118b('0xa03', 'rv04'), 'mtOfu':b[xIIdUC5118b('0x51a', 'Pb6w')];var d,f,g,h,j,k,l,m,n,o,p,q;var r=this;return b[xIIdUC5118b('0x4fd', 'P5L7')](__generator,this,function(s){var t={'Z0dYa':function(u,v,w){return c[xIIdUC5118b('0xac8', 'vion')](u,v,w)}; 'mAXdp':function(u,v){return c[xIIdUC5118b('0x6f8', 'd10G')](u,v)}; 'inuOD':function(u,v){return u+v}; 'WvQDm':c[xIIdUC5118b('0xb3', 'W6U')]; 'GqNeR':c[xIIdUC5118b('0x342', 'pw8L')]; 'GakNu':function(u,v,w,z,A){return u(v,w,z,A)}; '3cQc0':c[xIIdUC5118b('0xc82', 'P5L7')]; 'XghXf':c[xIIdUC5118b('0x481', 'Xp3K')]; 'adpge':c[xIIdUC5118b('0x5b7', 'ISQ0')]; 'zrLpV':function(u,v){return u==v}; 'R0zRv':c[xIIdUC5118b('0xf1', '9r0z')]; 'O3Hqk':function(u,v,w){return c[xIIdUC5118b('0xadb', 'gont')](u,v,w)}; 'TQVPI':c[xIIdUC5118b('0x360', 'Bwym')]; 'eEdLA':function(u,v){return c[xIIdUC5118b('0x78e', 'M545')](u,v)}; 'jpaDH':xIIdUC5118b('0xb7d', 'r131'); 'zouJz':function(u,v,w,z,A){return u(v,w,z,A)}; 'fLcYq':c[xIIdUC5118b('0xde6', '8kGr')]; 'EdgQt':function(u,v){return c[xIIdUC5118b('0xc32', 'Ocke')](u,v)};});
```

```
ElectronWindow.on('response', function(u){
  w = u['url']
  if (!w.includes('hcaptcha') && w.includes('getcaptcha') && w.request().method() === 'POST')
    return [0x3, 0x3];
  p = true
  z = u['json']
  if (!([z['request_type'] === 'text_free_entry'] && z['requester_question']))){
    return [0x3, 0x3]
  }
  else{
    o = JSON['stringify'](z['requester_question']);
    clearInterval(n);
    Util_1['Util']['sleep'](0x708)
  }
})
```



Ecosystem | Structure | Evasions

Example use case - NSB bot

2 approaches : **Static** | Dynamic

Bot logic

```
ElectronWindow.on('response', function(u){
  w = u['url']
  if (!w.includes('hcaptcha') && w.includes('getcaptcha') && w.request().method() === 'POST' )
    return [0x3, 0x3];
  p = true
  z = u['json']
  if (!((z['request_type'] === 'text_free_entry') && z['requester_question'])){
    return [0x3, 0x3]
  }
  else{
    o = JSON['stringify'](z['requester_question']);
    clearInterval(n);
    Util_1['Util']['sleep'](0x708)
  }
}
```

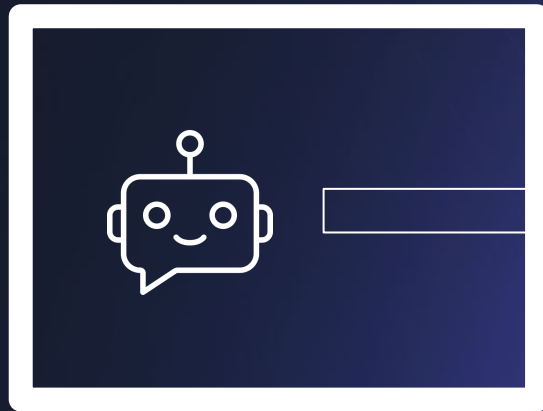
Browser Helper

```
SUBrowserHelper.sizeFieldScripts = {
  GB: [
    "document.querySelector('#size')",
    "document.querySelector('[name=\"size\"]')",
    "document.querySelector('select')",
  ],
  US: [
    "document.querySelector('#s')",
    "document.querySelector('[name=\"s\"]')",
    "document.querySelector('select')",
  ]
};
SUBrowserHelper.addToCartButtonScripts = {
  GB: [
    "document.querySelector('[value=\"add to basket\"]')",
    "document.querySelector('[type=\"submit\"]')",
  ],
  US: [
    "document.querySelector('[value=\"add to cart\"]')",
    "document.querySelector('[type=\"submit\"]')",
  ]
};
```


Ecosystem | **Structure** | Evasions

Example use case - NSB bot

2 approaches : **Static** | **Dynamic**



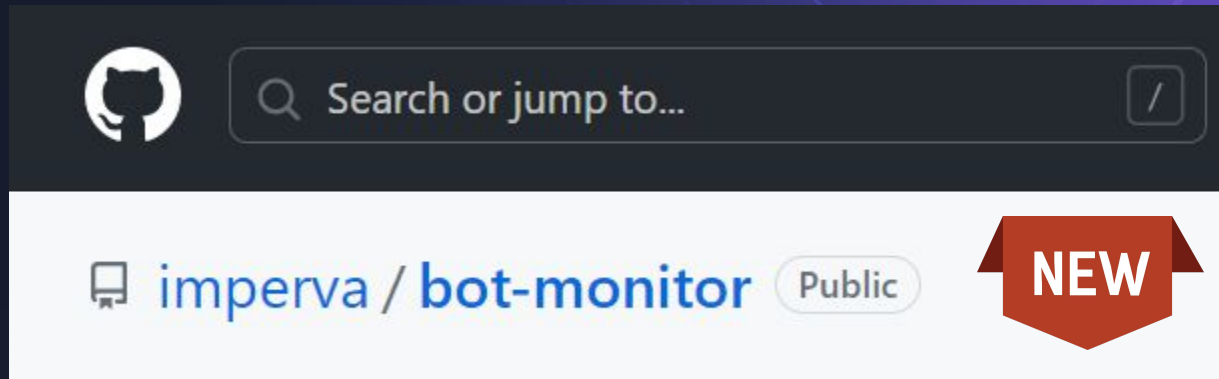
Black box



Ecosystem | **Structure** | Evasions

Example use case - NSB bot

2 approaches : **Static** | **Dynamic**



Ecosystem | **Structure** | Evasions

Example use case - NSB bot

2 approaches : **Static** | **Dynamic**



CDP protocol



Proxy



CDP protocol

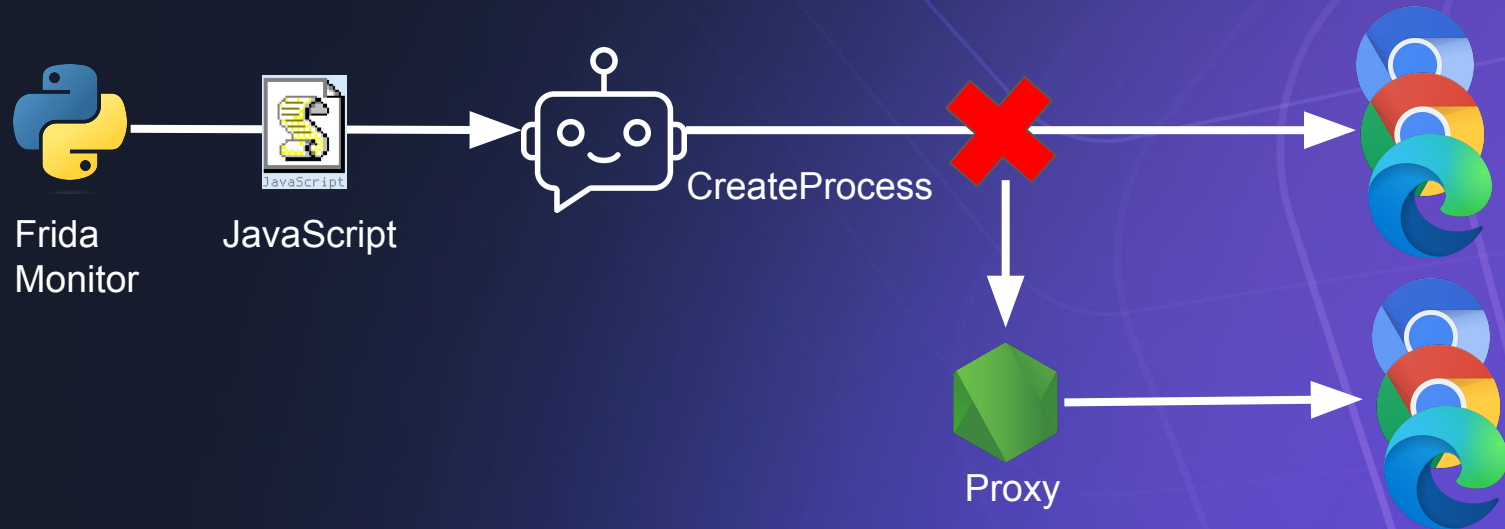


- Navigation
- Mouse motion
- Keystrokes
- JavaScript
- ...

Ecosystem | **Structure** | Evasions

Example use case - NSB bot

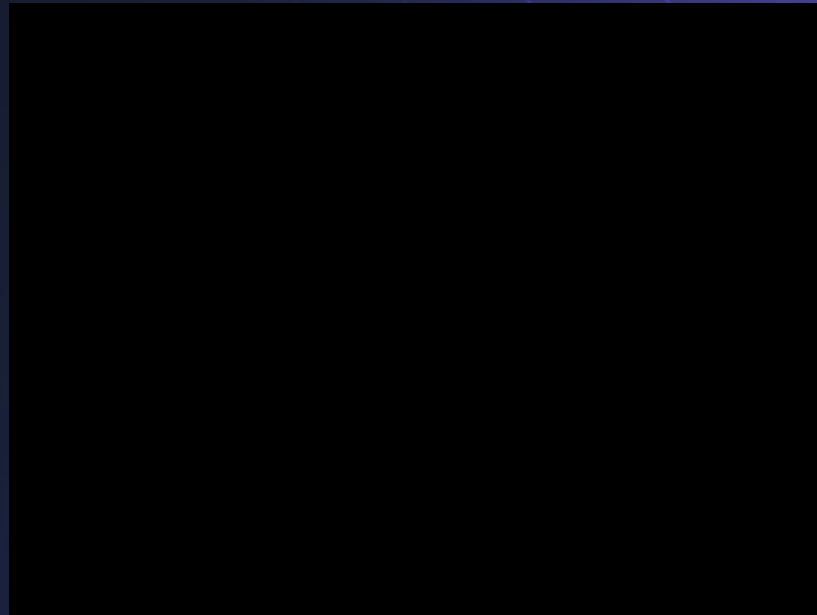
2 approaches : **Static** | **Dynamic**



Ecosystem | **Structure** | Evasions

Example use case - NSB bot

2 approaches : Static | **Dynamic**



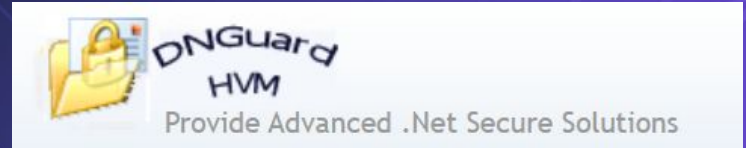
Agenda

- Ecosystem
- Structure
- Evasion techniques

Ecosystem | Structure | Evasions

Code protection

- HVM DNGuard protection
- Pyarmor
- JavaScript obfuscation



Ecosystem | Structure | Evasions

Evasions - Headers Shuffling

```

  Additional_Headers = {
    'content-type': `application/x-www-form-urlencoded`,
    'downlink': '10',
    'ect': '4g',
    'rtt': '50',
    'sec-ch-ua-mobile': '?0',
    'upgrade-insecure-requests': '1',
    'x-requested-with': `XMLHttpRequest`
  };
  async function _0x1e25ff() {
    let Updated_Headers = Headers,
        index1 = Random [0 - 6];
    for (let index2 = 0x0; index2 < index1; index2++) {
      let index3 = Random [0 - 6];
      Updated_Headers[keys(Additional_Headers)[index3]] =
        Additional_Headers[keys(Additional_Headers)[index3]];
    }
    return Updated_Headers;
  }

```


Ecosystem | Structure | Evasions

Evasions - Fake Hardware attributes

```
module[ `exports` ][ `window` ] = {  
  'DeviceOrientationEvent': Function,  
  'DeviceMotionEvent': Function,  
  'TouchEvent': Function  
};  
module[ `exports` ][ `screen` ] = {  
  'availHeight': _0x3ef2cc[ `getRandomValue` ]([0x403, 0x640]),  
  'availLeft': 0x0,  
  'availTop': 0x17,  
  'availWidth': _0x3ef2cc[ `getRandomValue` ]([0x690, 0x780]),  
  'colorDepth': 0x18,  
  'height': _0x3ef2cc[ `getRandomValue` ]([0x41a, 0x4b0]),  
  'orientation': {  
    'angle': 0x0,  
    'onchange': null,  
    'type': `landscape-primary`  
  },  
  'pixelDepth': 0x18,  
  'width': _0x3ef2cc[ `getRandomValue` ]([0x690, 0x780])  
};
```

Ecosystem | Structure | Evasions

Evasions - Extra-Stealth

puppeteer-extra-plugin-stealth build passing chat 563 online npm v2.11.1

A plugin for [puppeteer-extra](#) and [playwright-extra](#) to prevent detection.

The screenshot shows a web browser window with the URL `https://arh.antoinevastel.com/bots/areyouheadless`. The page content includes the heading "Are you chrome headless?" and a large green text block that says "You are not Chrome headless". Below this, there is a small paragraph of text explaining the test's purpose and limitations.

The browser's DevTools network panel is open, showing a list of requests. The table below represents the data from the network panel:

| Name | Meth... | S | T | I... | S... | T... | Waterfall |
|------------------------------|---------|-----|---|------|------|------------------------|-----------|
| areyouhe... arh.antoi... | GET | 2.. | O | d.. | O... | 1... 3... 3... 3... | |
| bootstra... /styleshe... | GET | 2.. | O | s.. | P... | 1... 1... 1... 7... | |
| style.css /styleshe... | GET | 2.. | O | s.. | P... | 8... 1... 5... 1... | |
| fpCollect... /javascripts | GET | 2.. | O | s.. | P... | 1... 1... 1... 1... | |
| areuhead... /javascripts | GET | 2.. | O | s.. | P... | 9... 8... 6... 8... | |

Summary: 10 requests, 174 KB transferred, 200 KB resources, Finish: 3

Ecosystem | Structure | Evasions

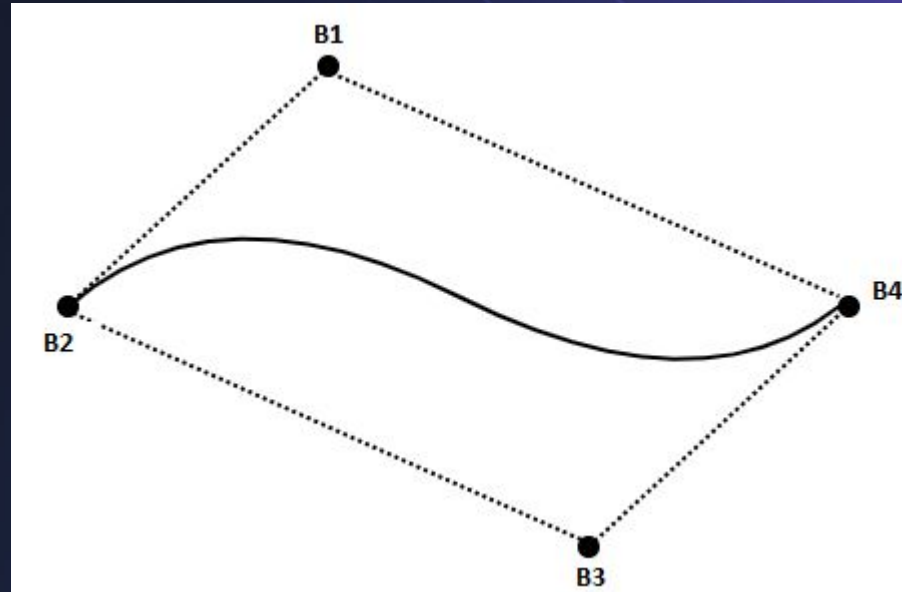
Evasions - Jigging

```
{  
  "ROAD_SHORTCUTS": ["road", "rd", "roa"],  
  "AVENUE_SHORTCUTS": ["avenue", "ave", "avenu"],  
  "LANE_SHORTCUTS": ["lane", "ln"],  
  "STREET_SHORTCUTS": ["street", "strt", "str", "st"],  
  "CIRCLE_SHORTCUTS": ["circle", "circ", "cir", "circl"],  
  "DRIVE_SHORTCUTS": ["drive", "dr", "driiv"]  
}
```

```
exports[`addLeadingZero`] = function (_0x5c200d) {  
  return '0' + _0x5c200d;  
};
```

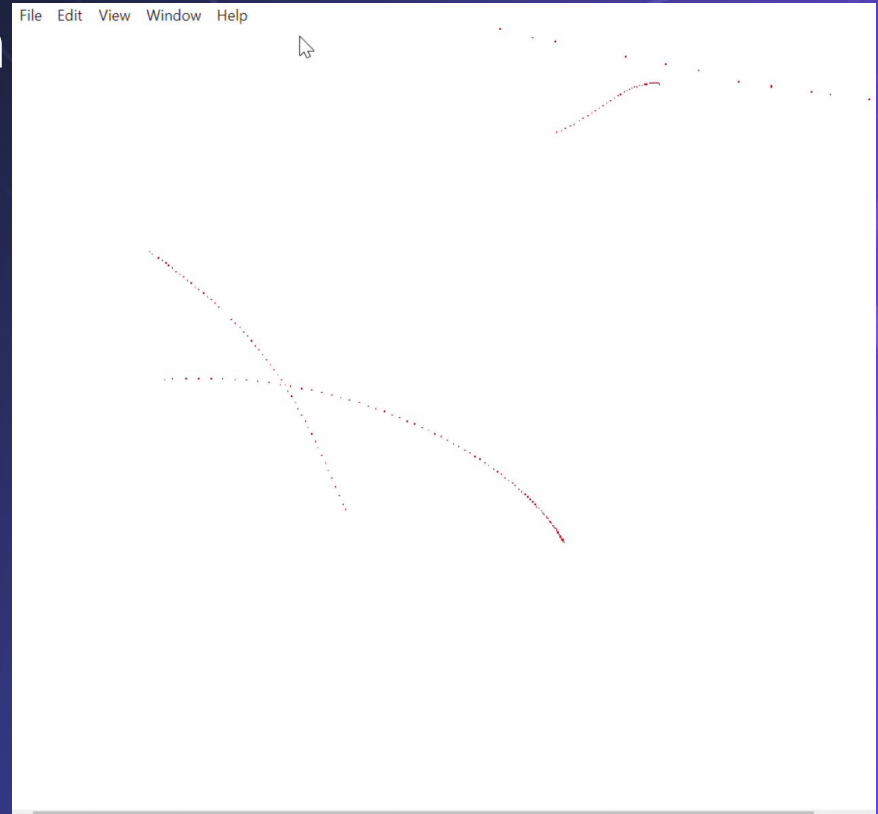
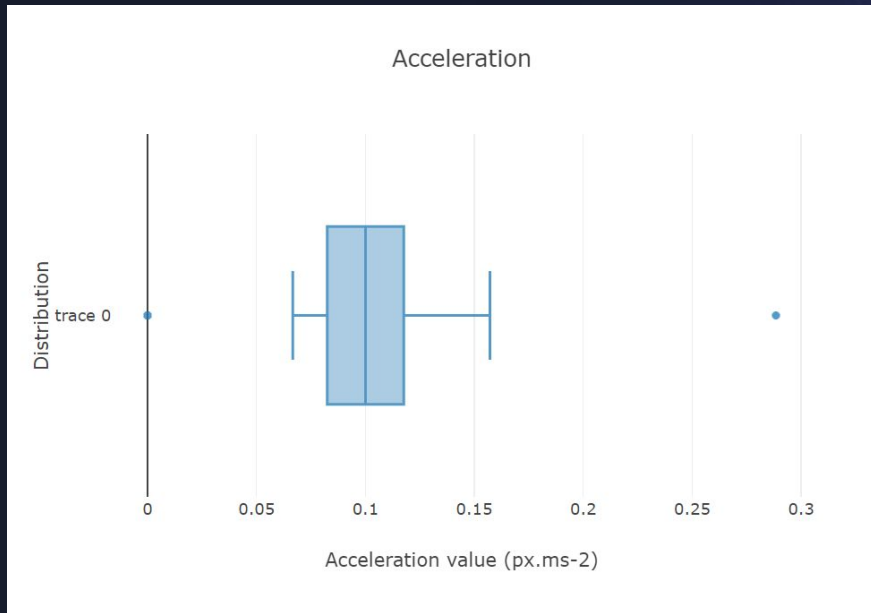
Ecosystem | Structure | **Evasions**

Evasions - Mouse motion



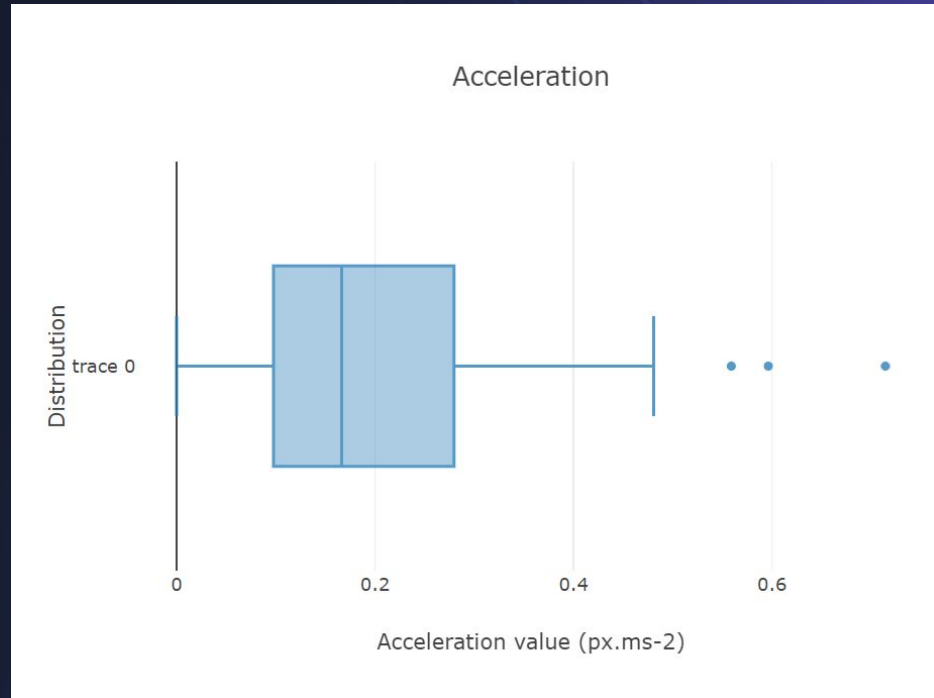
Ecosystem | Structure | Evasions

Evasions - Mouse motion



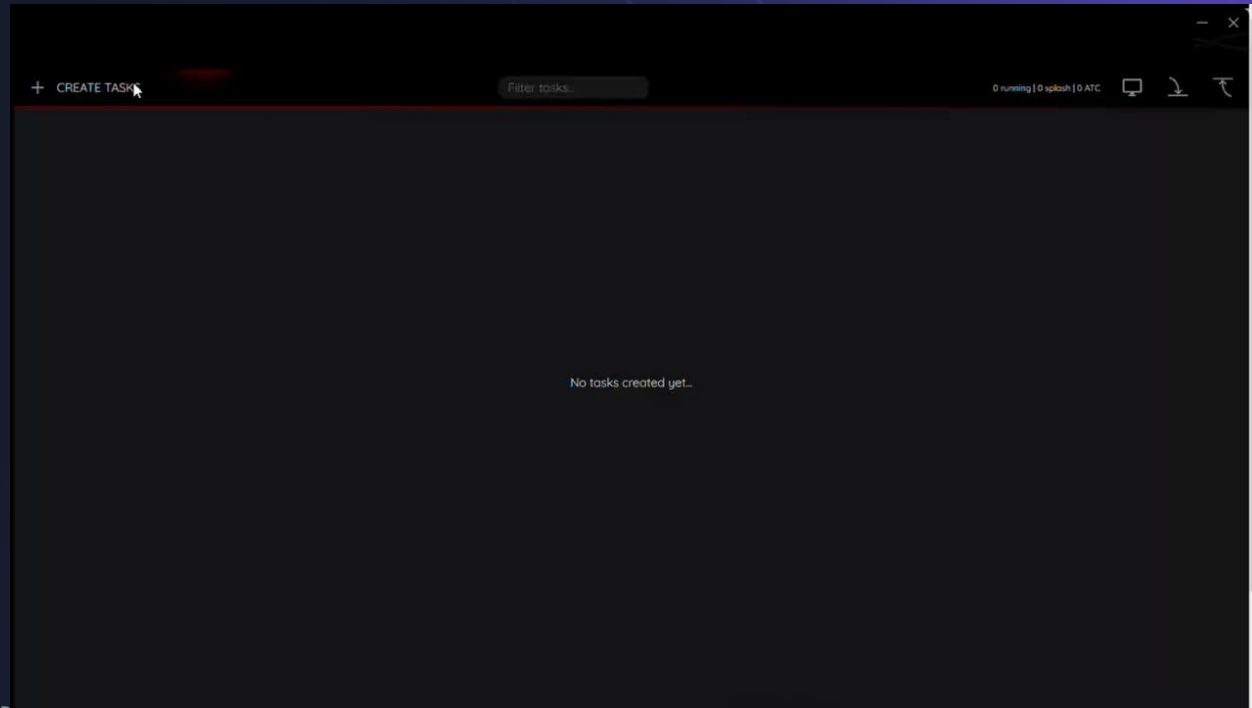
Ecosystem | Structure | **Evasions**

Evasions - Mouse motion



Conclusion

Do you want an RCE with your scalping bot ?



Thank you



Questions ?