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

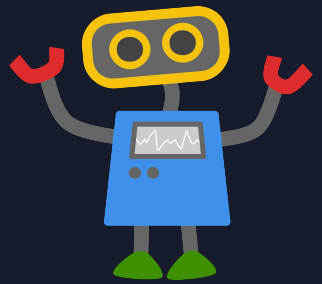
- Ecosystem
- Structure
- Evasion techniques

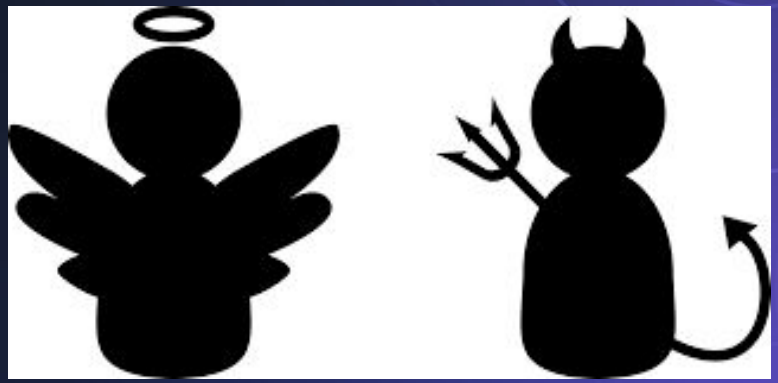
Ecosystem | Structure | Evasions

BOTS : Softwares automating actions on the Internet

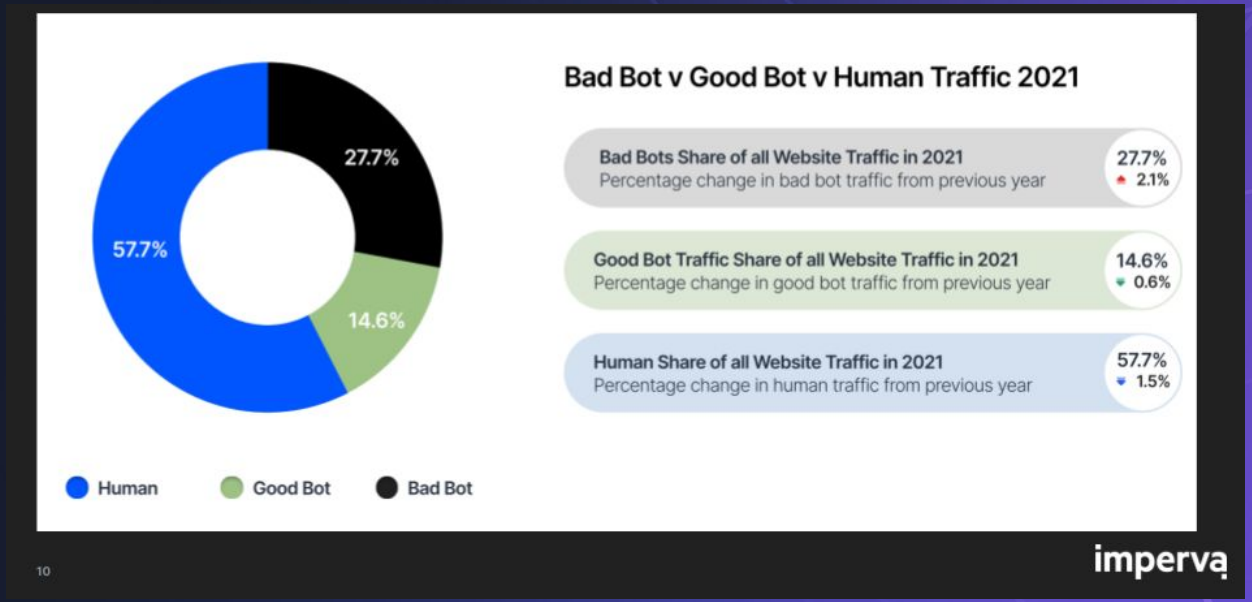
Ecosystem | Structure | Evasions

BOTS : Softwares automating actions on the Internet



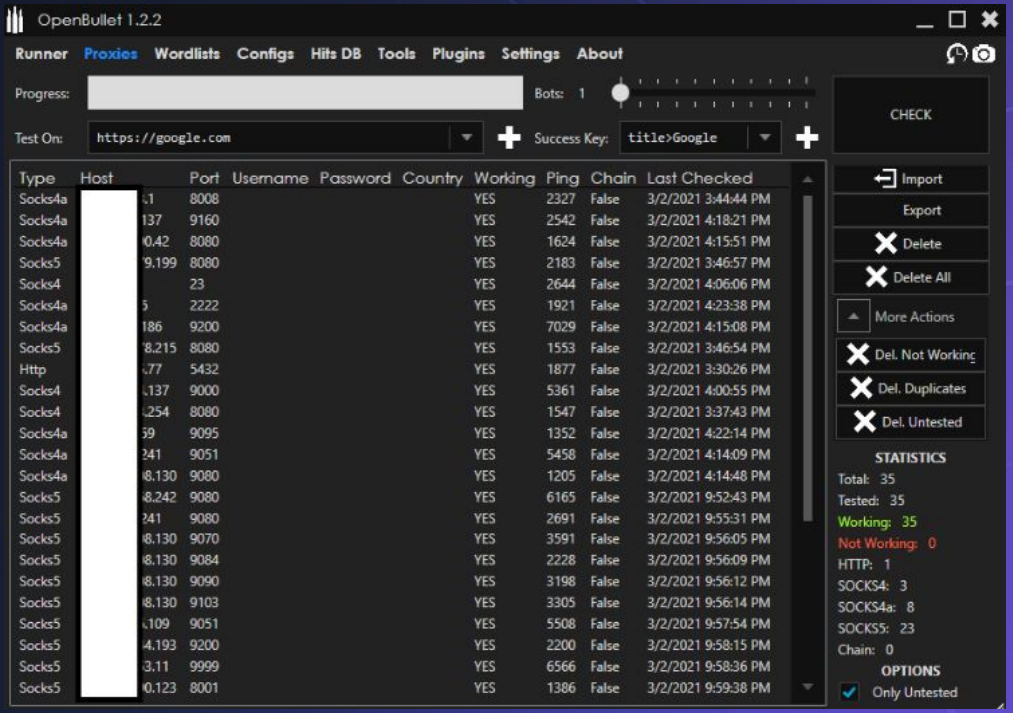


Ecosystem | Structure | Evasions



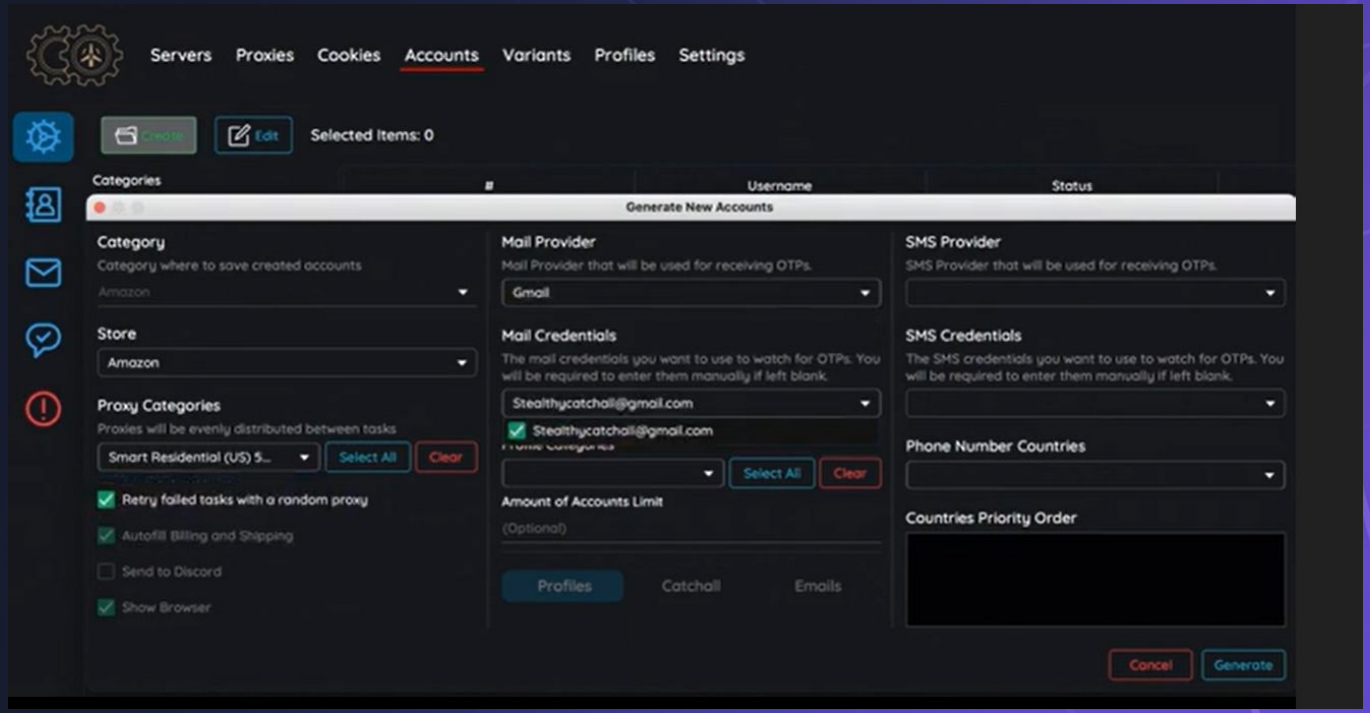
Ecosystem | Structure | Evasions

Bad bots - Credential stuffing (eg OpenBullet)



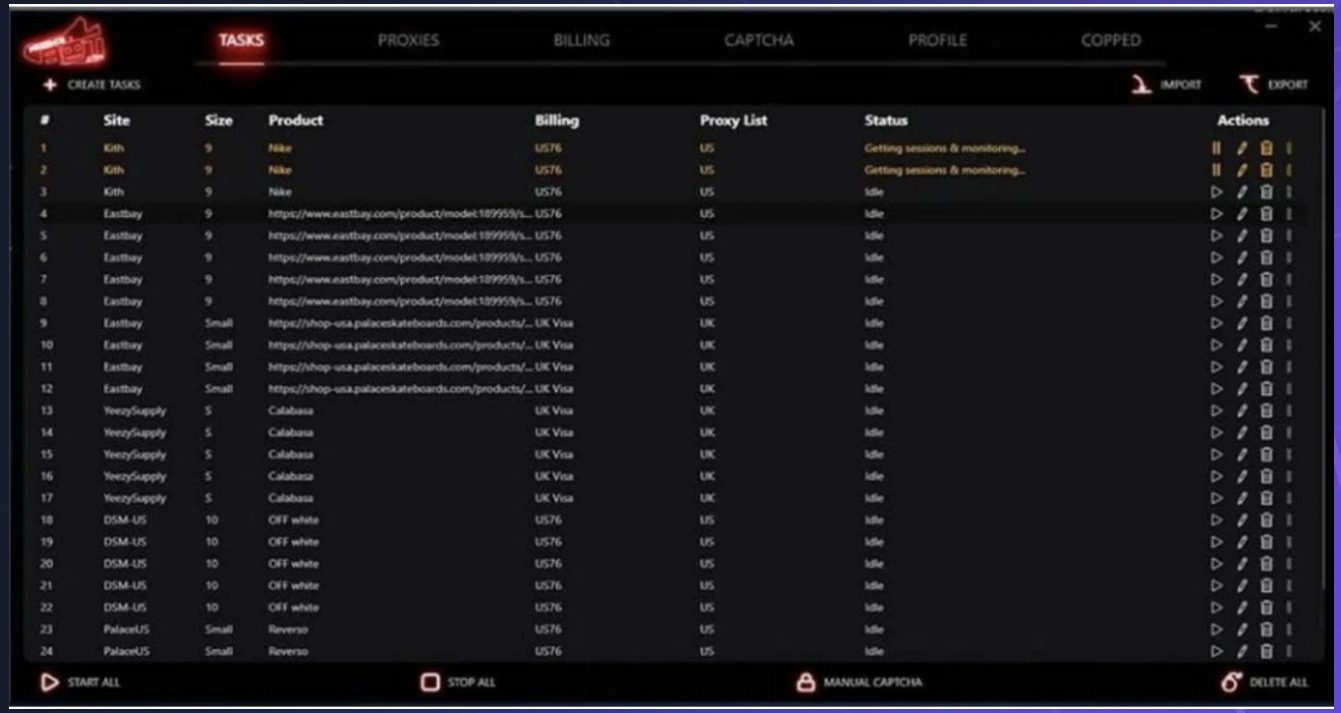
Ecosystem | Structure | Evasions

Bad bots - Account creation bots (eg AYCD)



Ecosystem | Structure | Evasions

Bad bots - Scalping bots (eg NSB)



#	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/s...	US76	US	Idle	
5	Eastbay	9	https://www.eastbay.com/product/model:189959/s...	US76	US	Idle	
6	Eastbay	9	https://www.eastbay.com/product/model:189959/s...	US76	US	Idle	
7	Eastbay	9	https://www.eastbay.com/product/model:189959/s...	US76	US	Idle	
8	Eastbay	9	https://www.eastbay.com/product/model:189959/s...	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	YeezySupply	S	Calabasa	UK Visa	UK	Idle	
14	YeezySupply	S	Calabasa	UK Visa	UK	Idle	
15	YeezySupply	S	Calabasa	UK Visa	UK	Idle	
16	YeezySupply	S	Calabasa	UK Visa	UK	Idle	
17	YeezySupply	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	

Ecosystem | Structure | Evasions

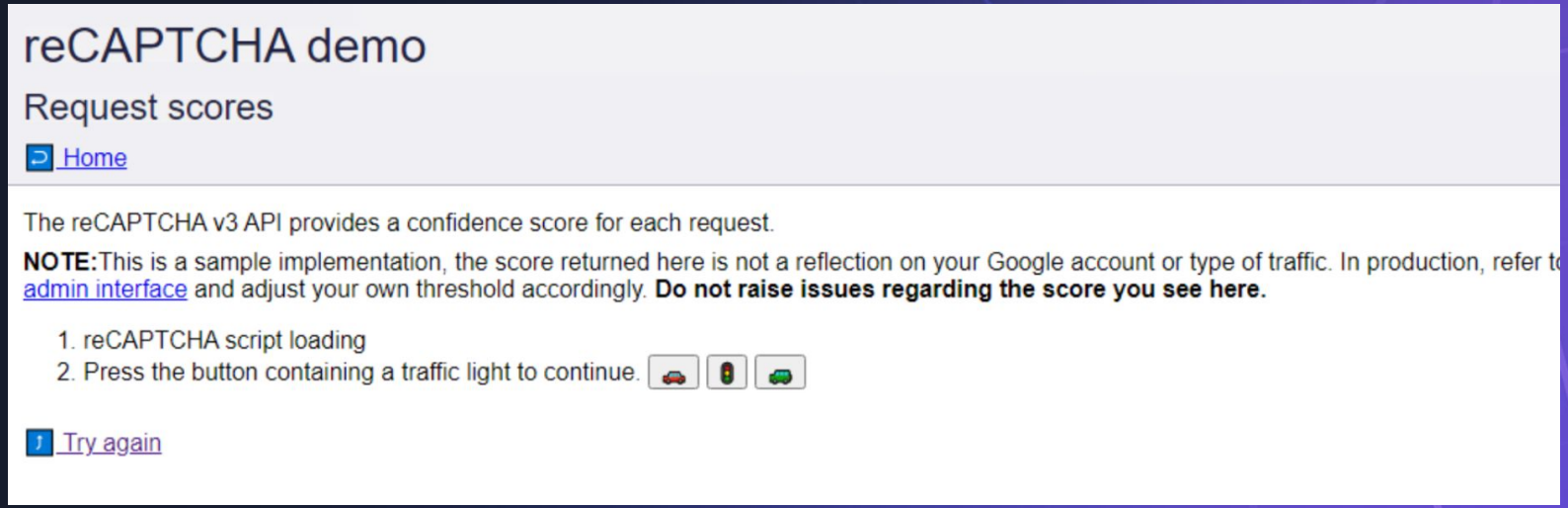
Bad bots - OneClick bot

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

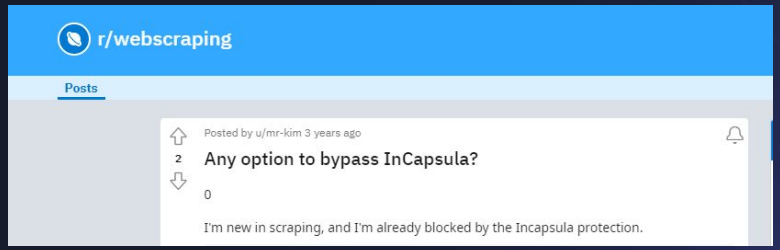
Bad bots - OneClick bot

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



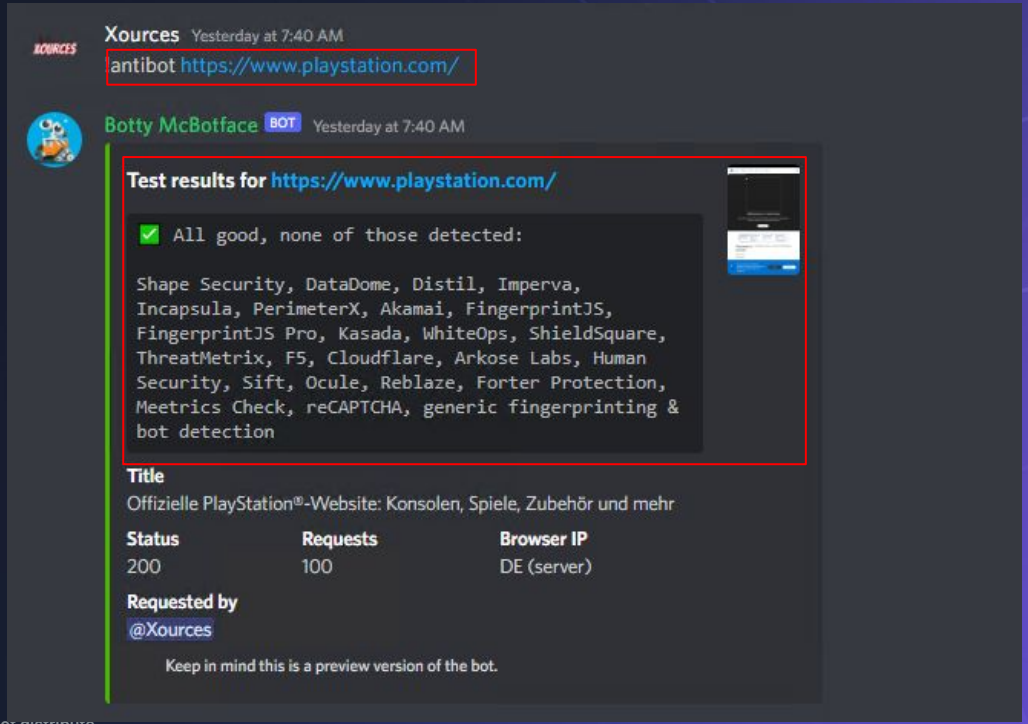
Ecosystem | Structure | Evasions

Developer Communities



Ecosystem | Structure | Evasions

Developer Communities



Ecosystem | Structure | Evasions

User communities - Market places

easyrentals

TIDAL

BOTMART

TicketBots.net 10 YEARS & counting...

BOT-BROKER
Buy and Sell Sneaker Bots

CopSupply

MAB
MOST ADVANCED BOT

botsthatwork

TheCopShop
One-Stop Discord Marketplace

SNEAKER SQUAD

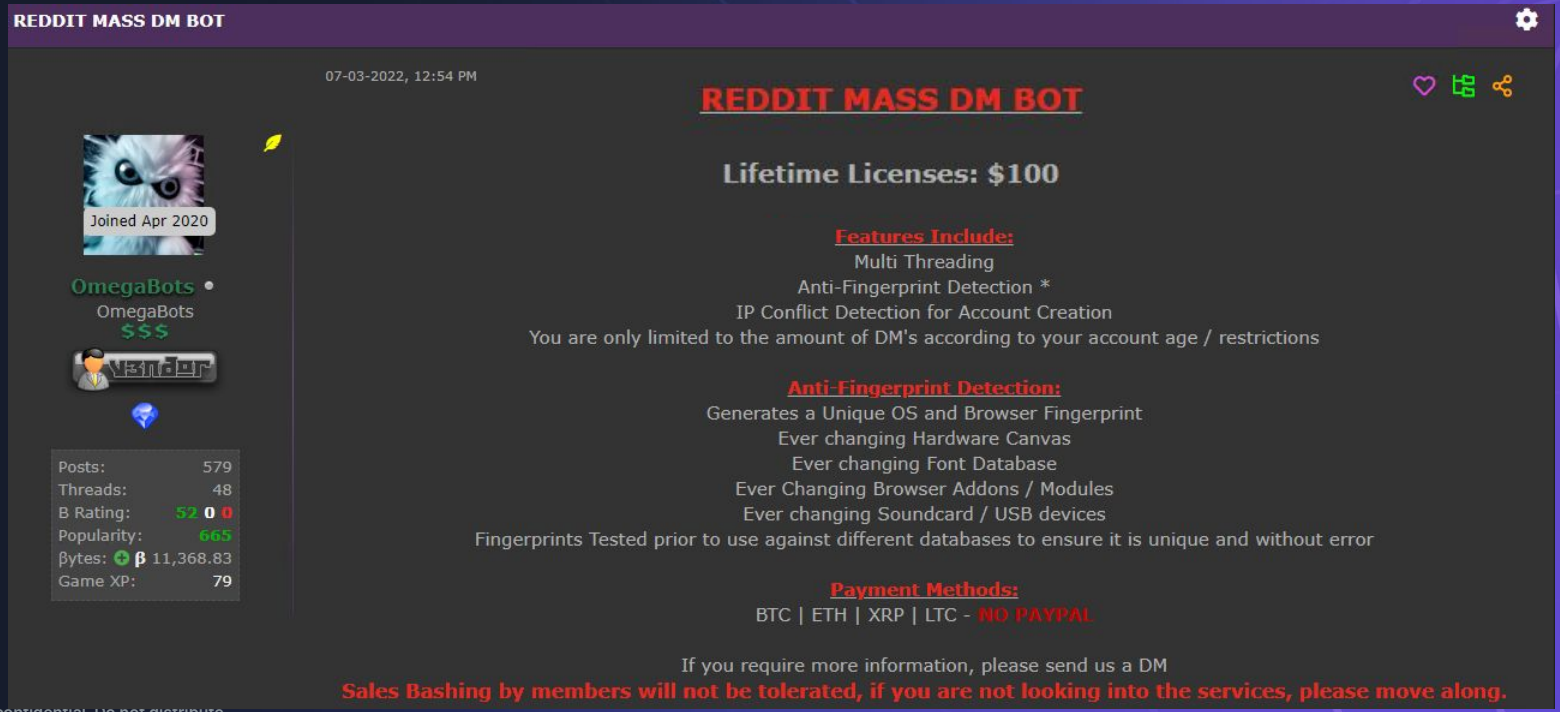
Tiger zone

Botstash

Whop

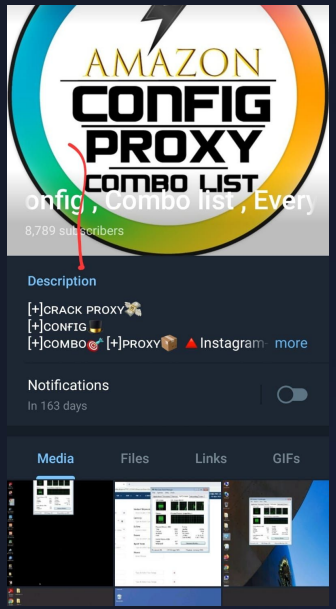
Ecosystem | Structure | Evasions

User communities - Underground forums

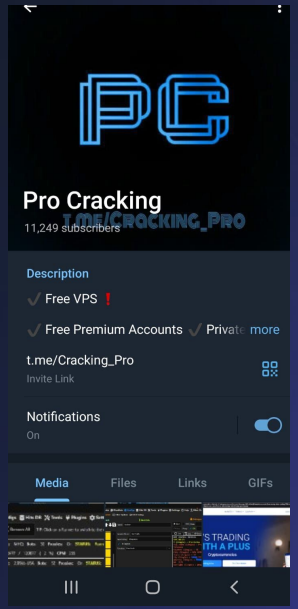


Ecosystem | Structure | Evasions

User Communities - Cracking groups

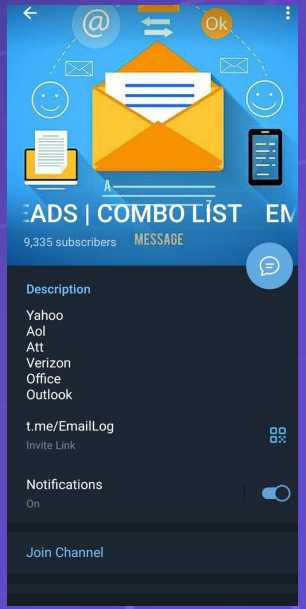


CrackingHit



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

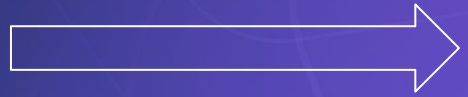
Webdriver vs CDP protocol

/session/:sessionId/url

webdriver

Internal protocol

Webdriver protocol



Page.navigate

CDP protocol

CDP

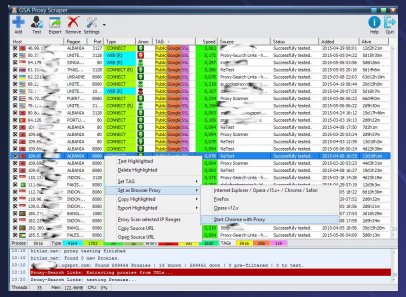
Ecosystem | **Structure** | Evasions

Proxies

oxylabs

bright data

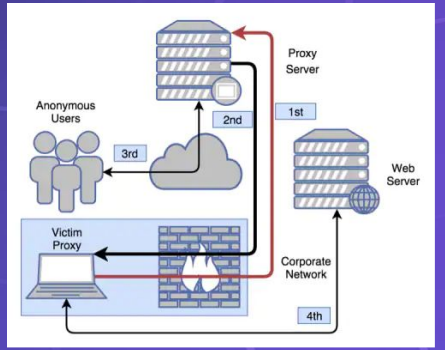
chef proxies



GSA proxy scraper

UProxy scraper tool

ProxyBack malware turns User Systems Into Proxies Without Consent

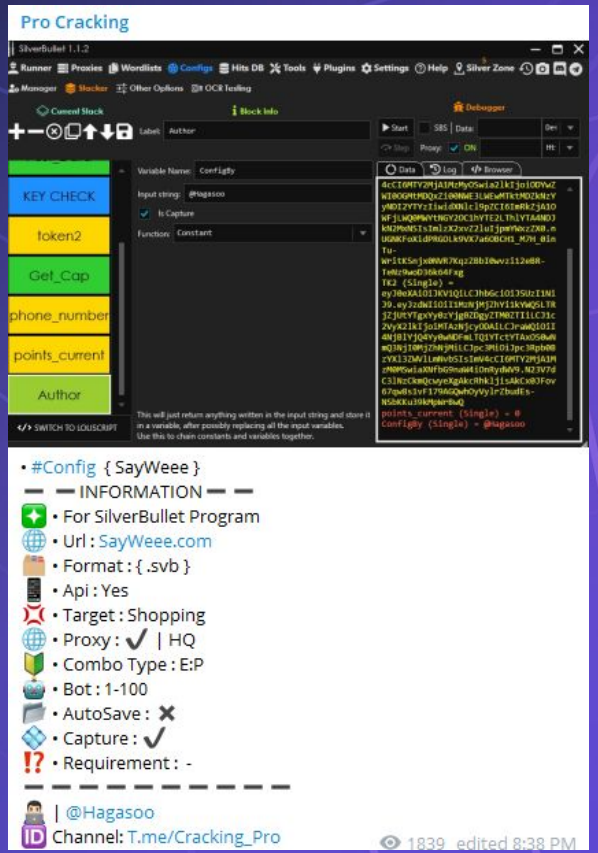


ProxyBack malware

Ecosystem | **Structure** | Evasions

Configuration

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



Ecosystem | **Structure** | Evasions

3rd parties

Anti-Captcha

Human based

Example 2Captcha

AI based

Example CapMonster

Hybrid

Example DeathByCaptcha

Ecosystem | **Structure** | Evasions

3rd parties

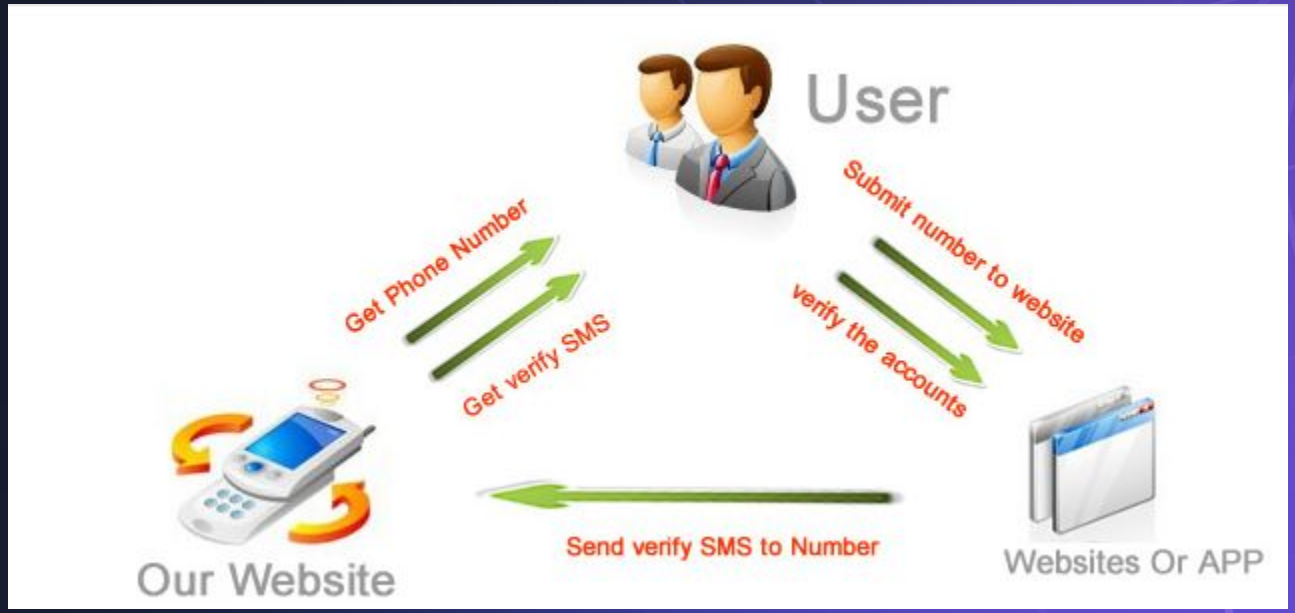
Anti-Captcha Stacking (Ex AYCD Autosolve)

Anti-captcha stacking

Ecosystem | **Structure** | Evasions

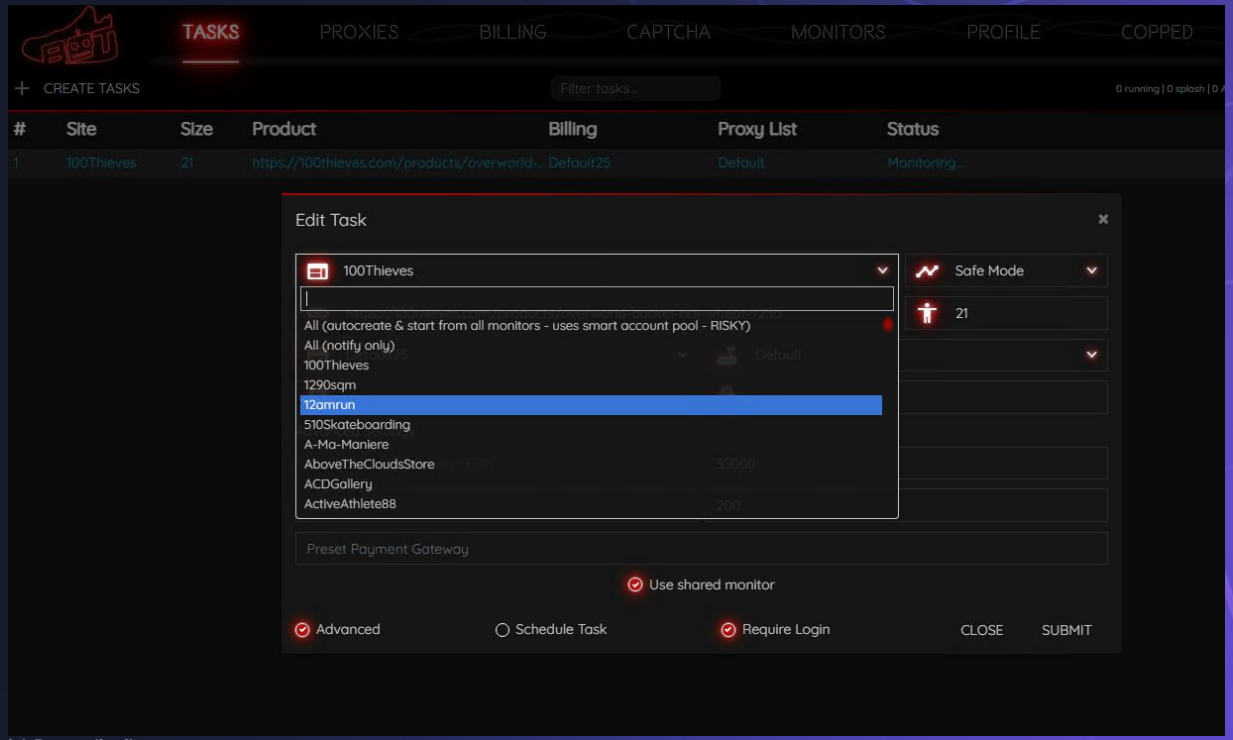
3rd parties

Virtual Phone service



Ecosystem | **Structure** | Evasions

Example use case - NSB bot

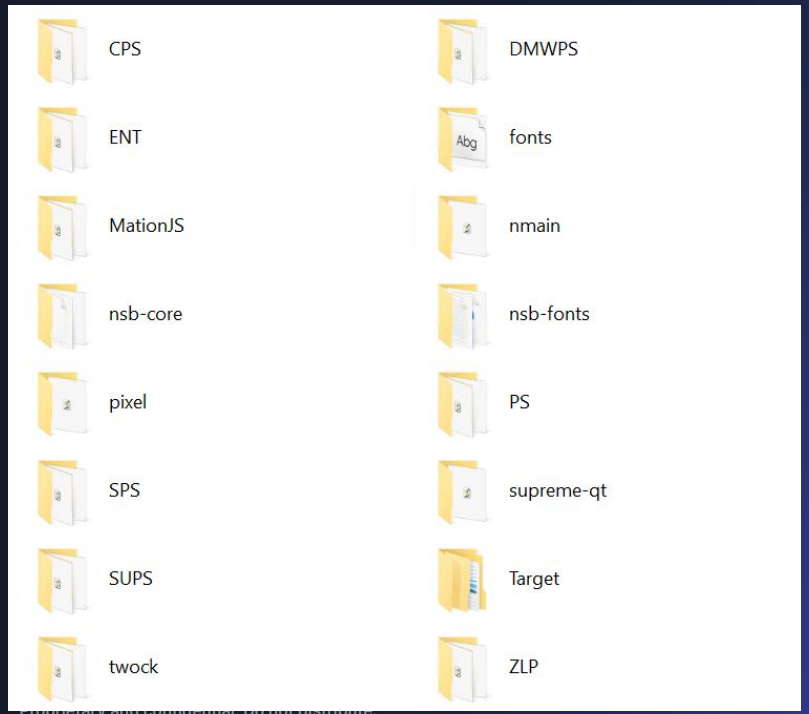


Ecosystem | **Structure** | Evasions

Example use case - NSB bot

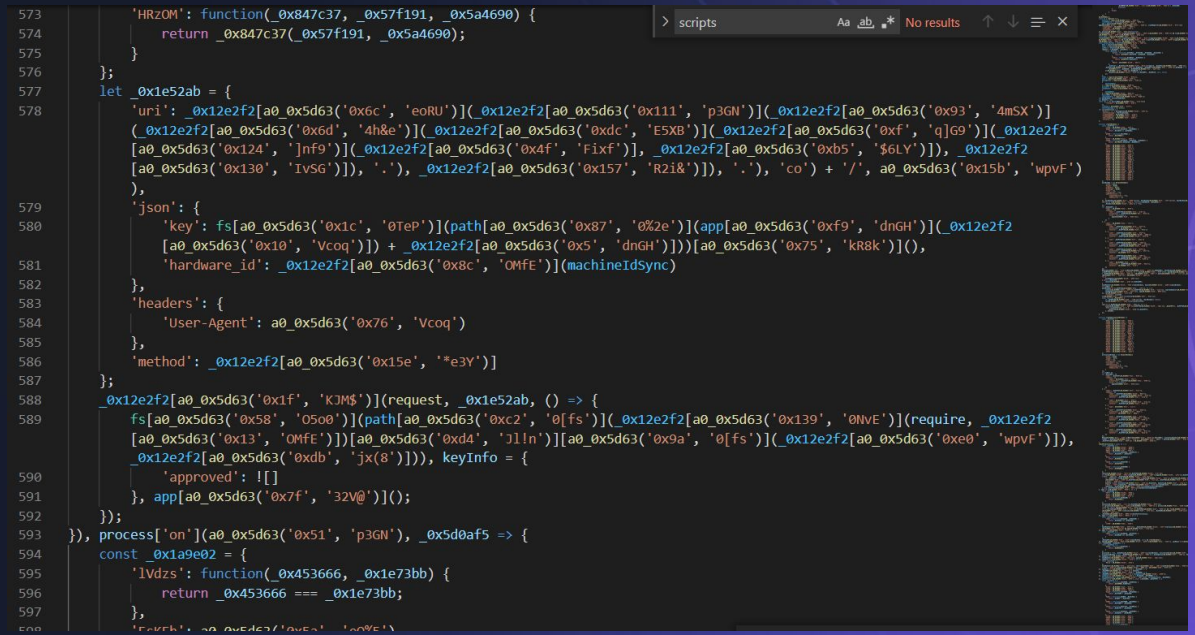
Ecosystem | **Structure** | Evasions

Example use case - NSB bot



Ecosystem | **Structure** | Evasions

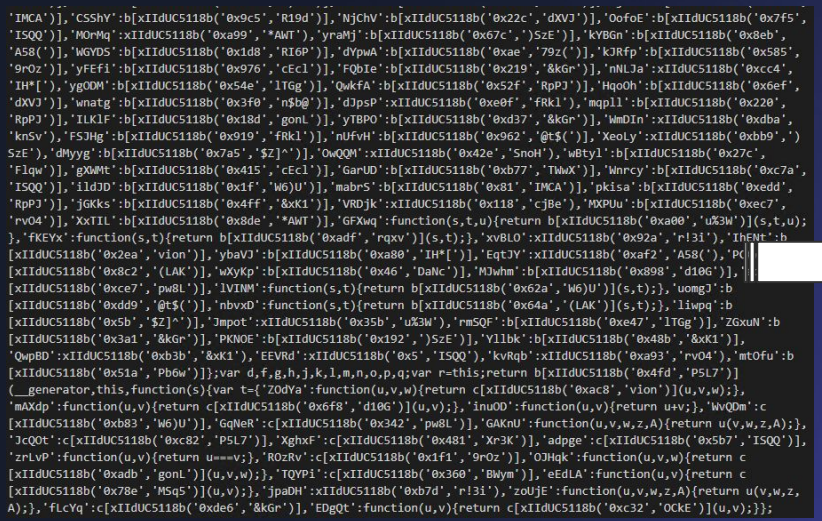
Example use case - NSB bot



Ecosystem | **Structure** | Evasions

Example use case - NSB bot

2 approaches : **Static** | Dynamic




```
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)
    }
```

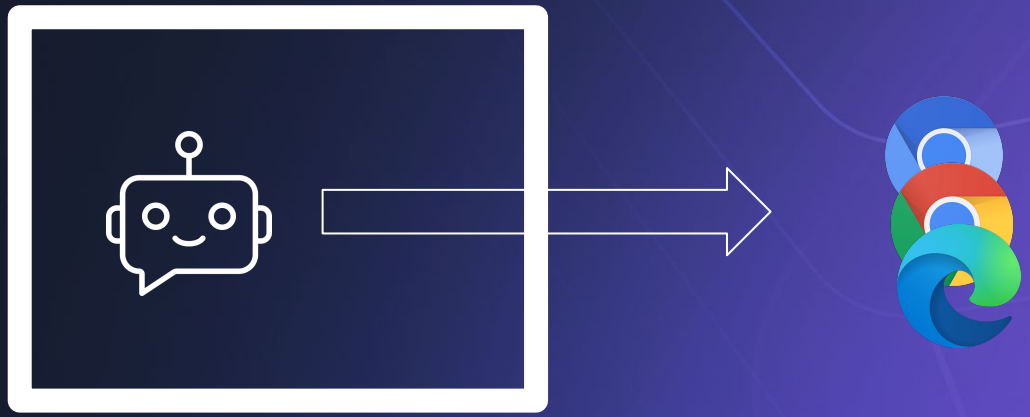
Browser Helper

```
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

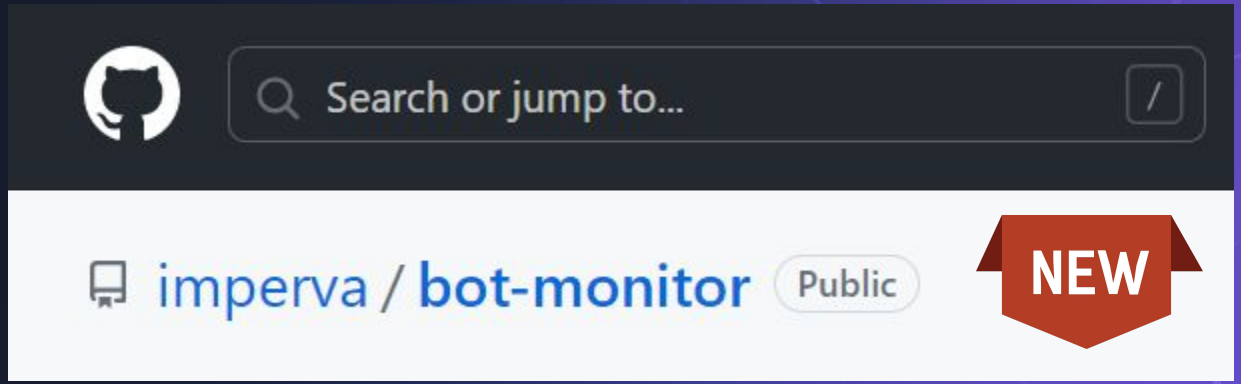


Black box

Ecosystem | **Structure** | Evasions

Example use case - NSB bot

2 approaches : **Static** | Dynamic



Ecosystem | **Structure** | Evasions

Example use case - NSB bot

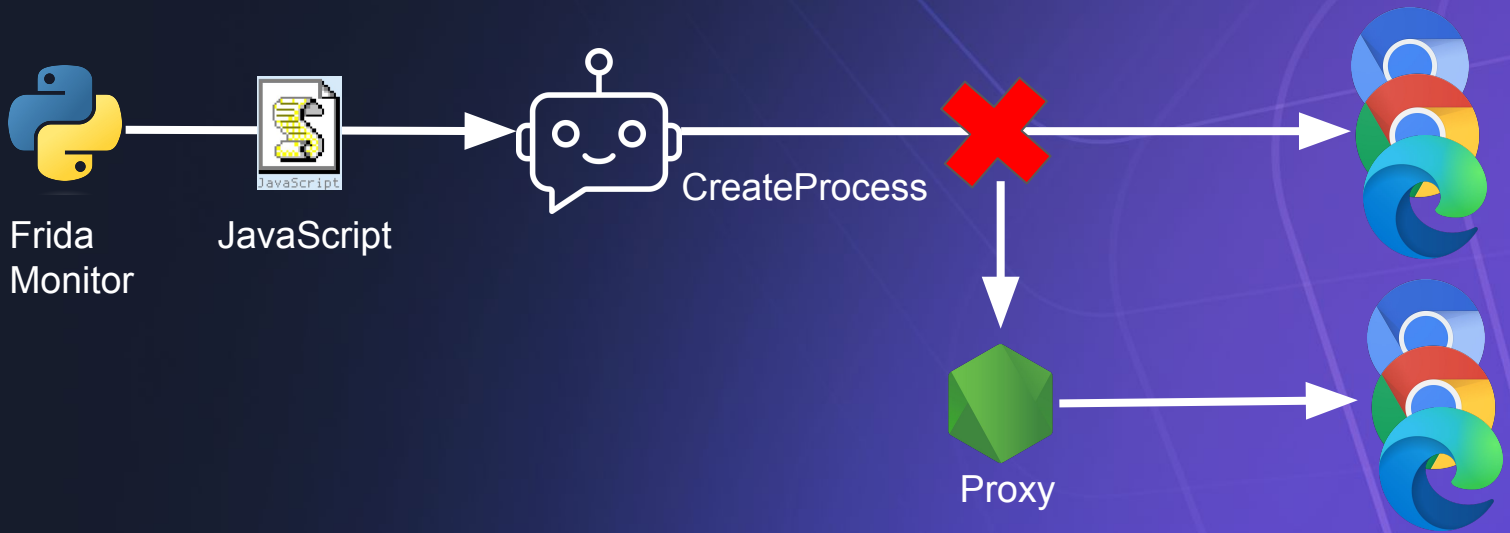
2 approaches : **Static** | Dynamic

- 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;
}
```

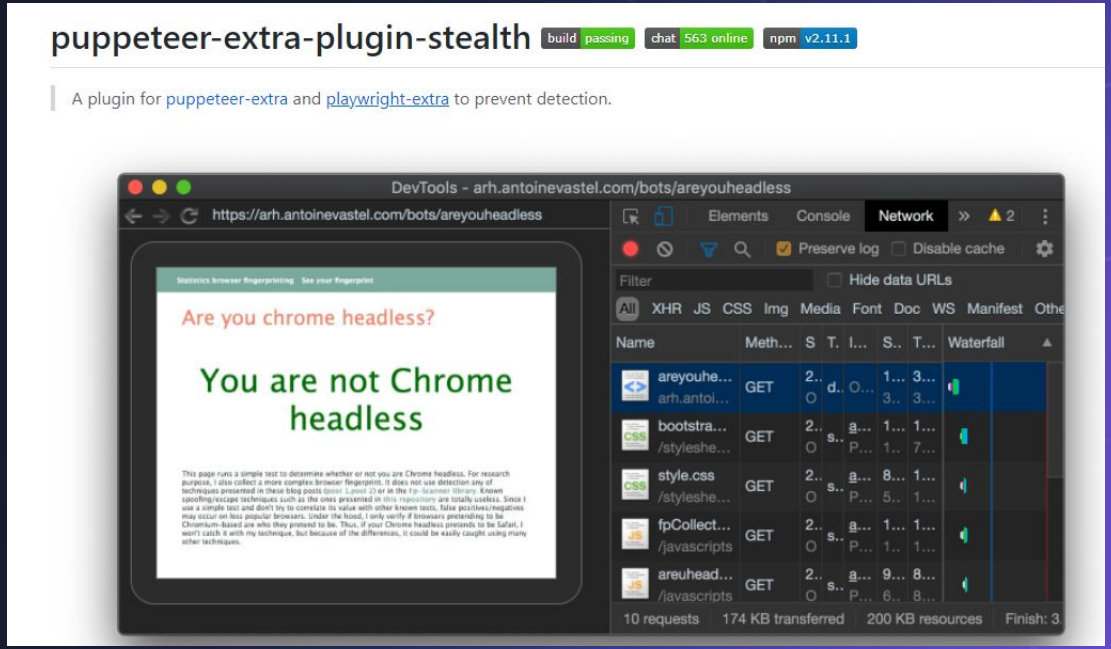
Ecosystem | Structure | **Evasions**

Evasions - Fake Hardware attributes

```
module[`exports`][`window`] = {
    'DeviceOrientationEvent': Function,
    'DeviceMotionEvent': Function,
    'TouchEvent': Function
};
module[`exports`][`screen`] = {                    1000 - 1600
    '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



Ecosystem | Structure | **Evasions**

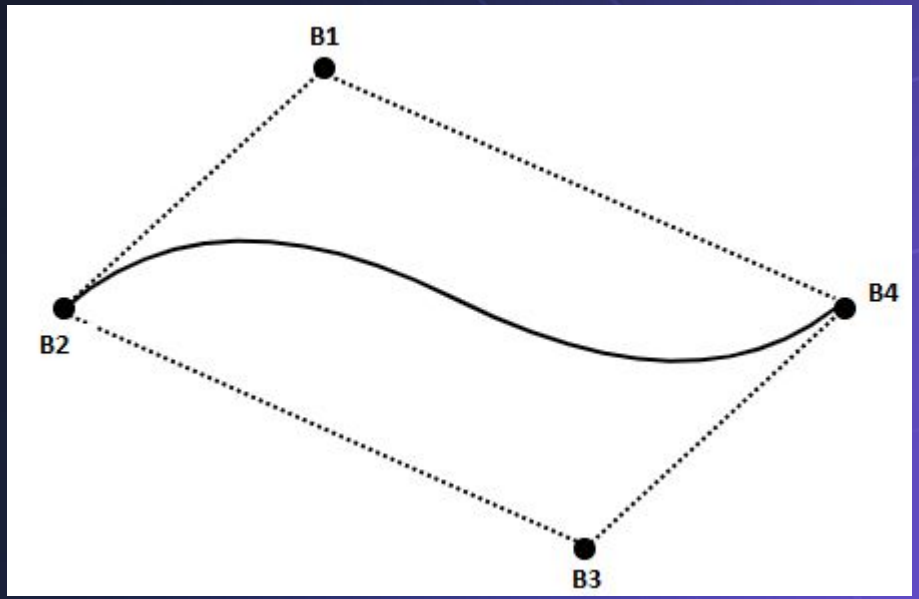
Evasions - Jigging

```
{
    "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", "driv"]
}
```

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

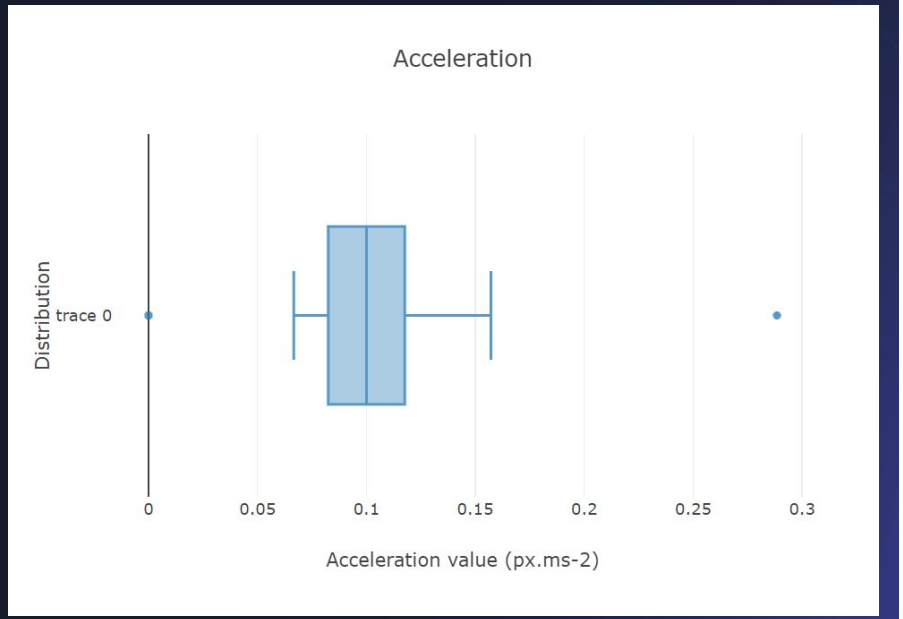
Ecosystem | Structure | **Evasions**

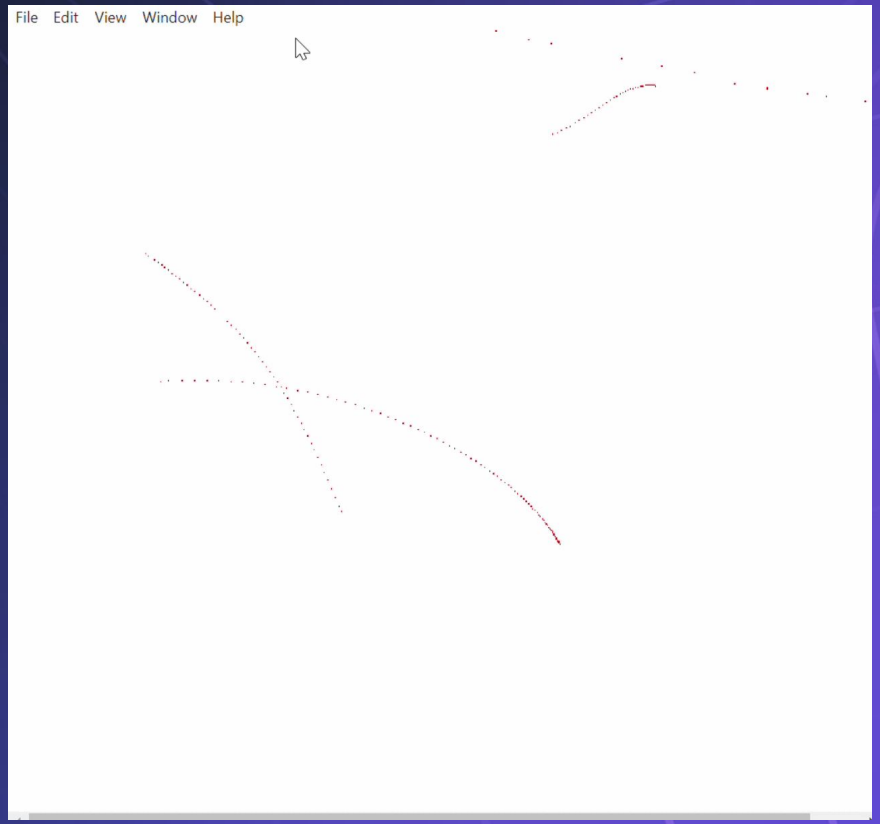
Evasions - Mouse motion



Ecosystem | Structure | **Evasions**

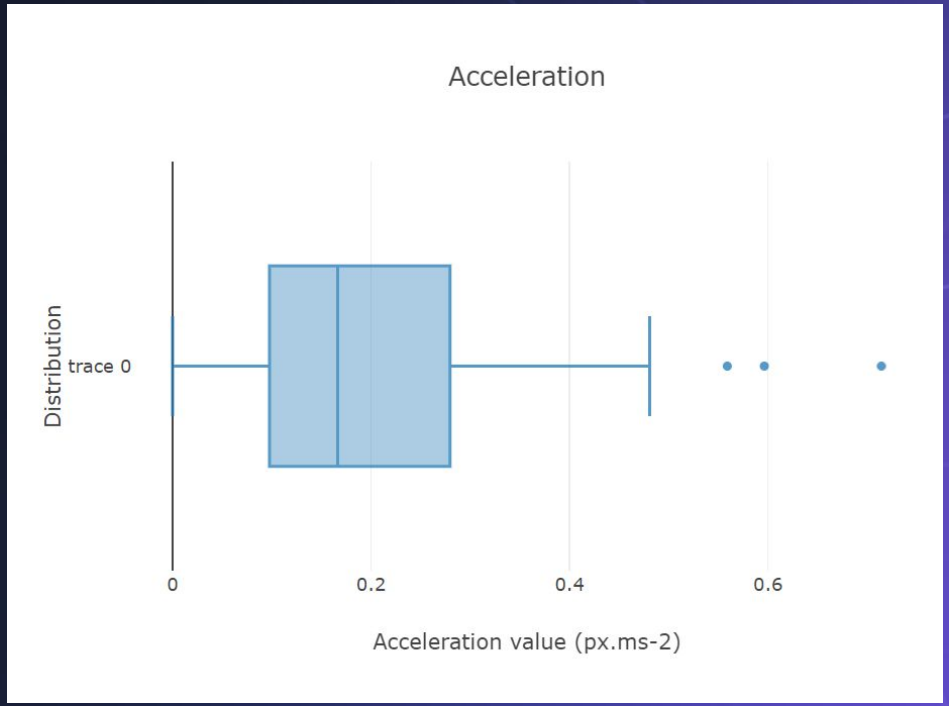
Evasions - Mouse motion





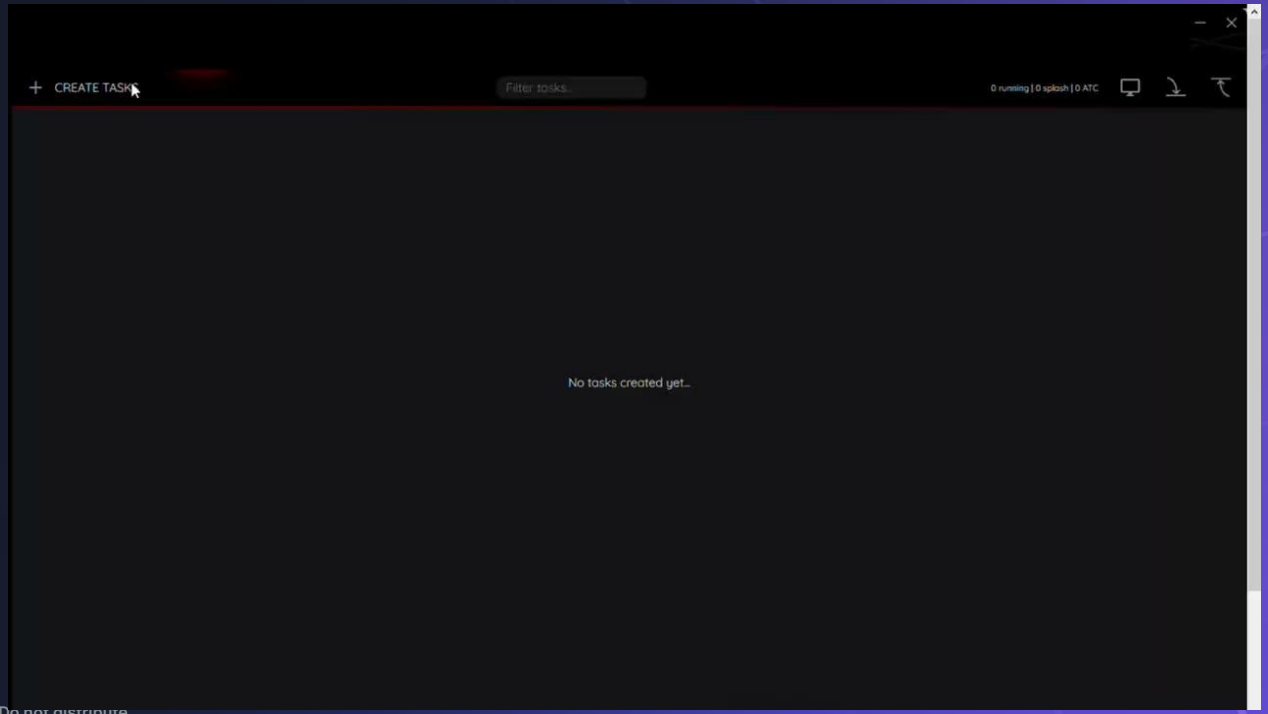
Ecosystem | Structure | **Evasions**

Evasions - Mouse motion



Conclusion

Do you want an RCE with your scalping bot ?



Thank you

botconf
the botnet & malware fighting conference

Questions ?