Advanced Bot Landscape

Yohann Sillam

Introduction to Advanced Bots

Yohann Sillam

Security Researcher at Imperva

4 years of research in cyber security

Malware Analysis

Web Application Security

Agenda

- **Advanced bot ecosystem**
- Internal structure of an advanced bot
- Evasion techniques and detection

Advanced Bot Ecosystem

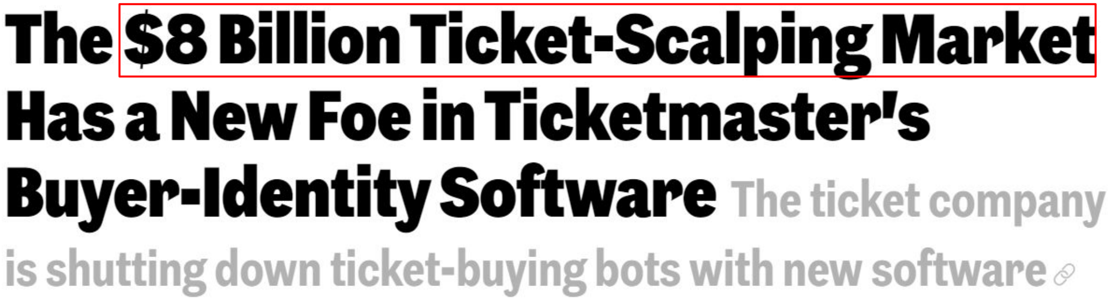
Bot definition

Bots

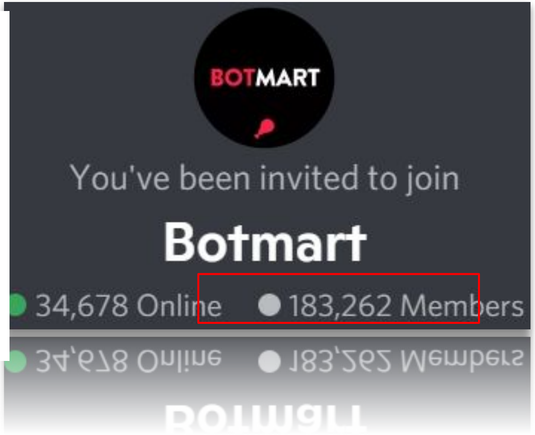
Softwares automating actions on the Internet

Advanced Bot Ecosystem

Billion dollar industry



The $8 Billion Ticket-Scalping Market Has a New Foe in Ticketmaster's Buyer-Identity Software The ticket company is shutting down ticket-buying bots with new software



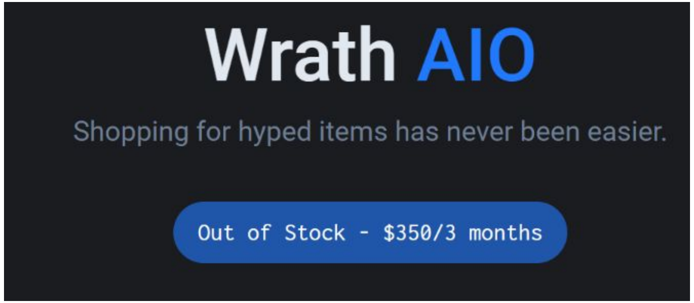
BOTMART

You've been invited to join

Botmart

● 34,678 Online ● 183,262 Members

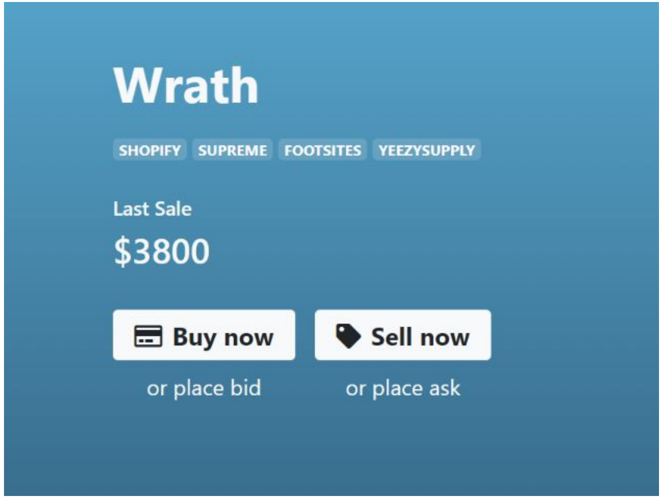
Advanced Bot Ecosystem
Billion dollar industry



Wrath AIO

Shopping for hyped items has never been easier.

Out of Stock - $350/3 months



Wrath

SHOPIFY SUPREME FOOTSITES YEEZYSUPPLY

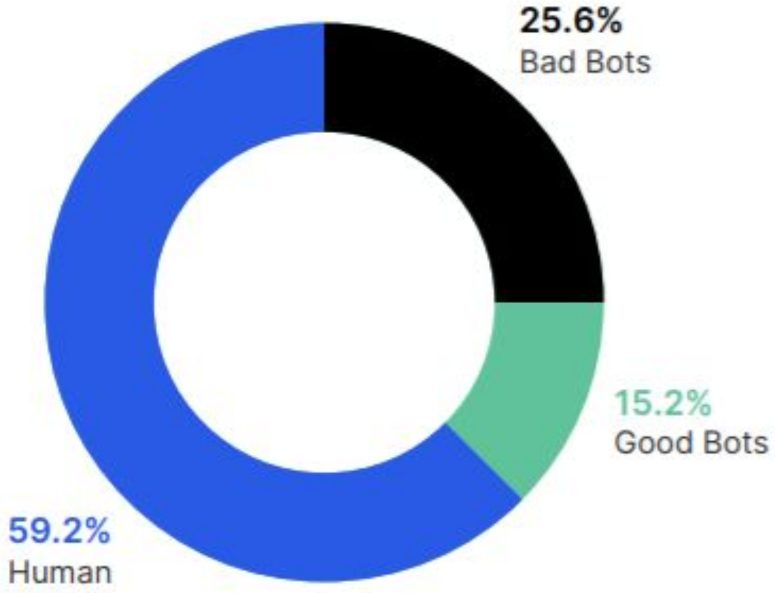
Last Sale

$3800

Advanced Bot Ecosystem

Statistics

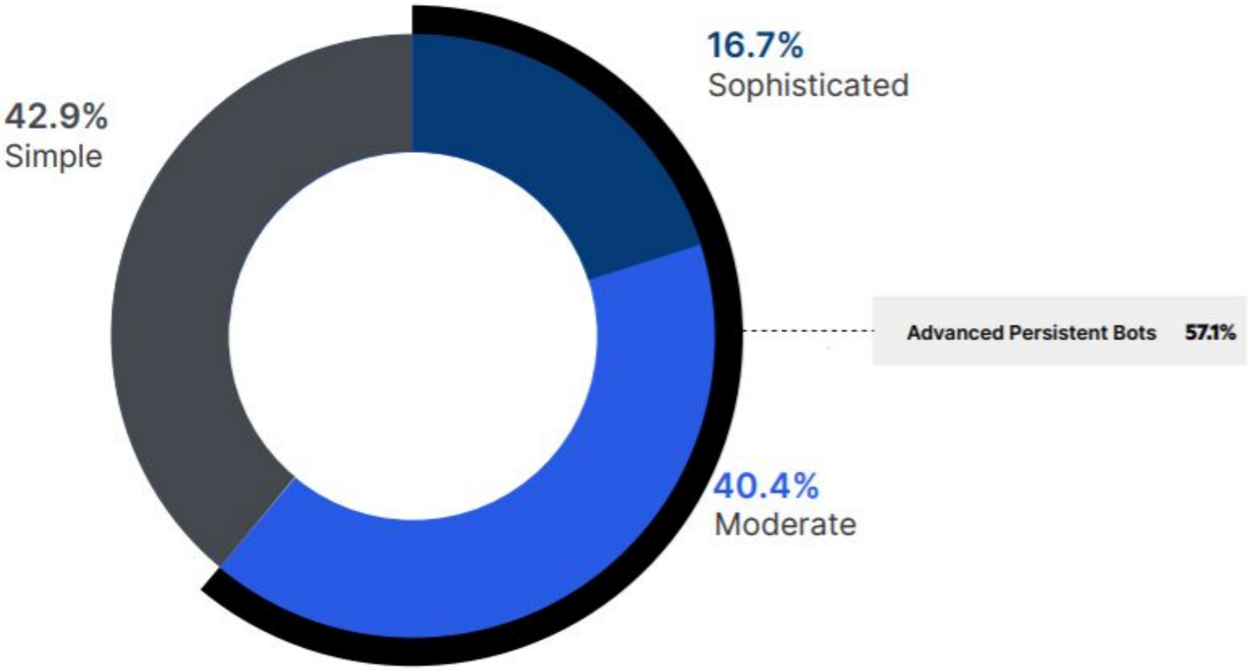
Bad Bot v Good Bot v Human Traffic 2020



Bad Bots Amount all Website Traffic in 2020 Percentage change in bad bot traffic from previous year	**25.6%** ▲ 6.2%
Good Bots Traffic Percentage in 2020 Percentage change in good bot traffic from previous year	**15.2%** ▲ 16.0%
Human Website Traffic Percentage in 2020 Percentage change in human traffic from previous year	**59.2%** ▼ 5.7%

Advanced Bot Ecosystem
Statistics

Bad Bot Sophistication Levels 2020



Advanced Bot Ecosystem
Advanced bots

Advanced Bots

- Headless browser
- Rotation between anonymous proxies
- Advanced anti-detection mechanisms

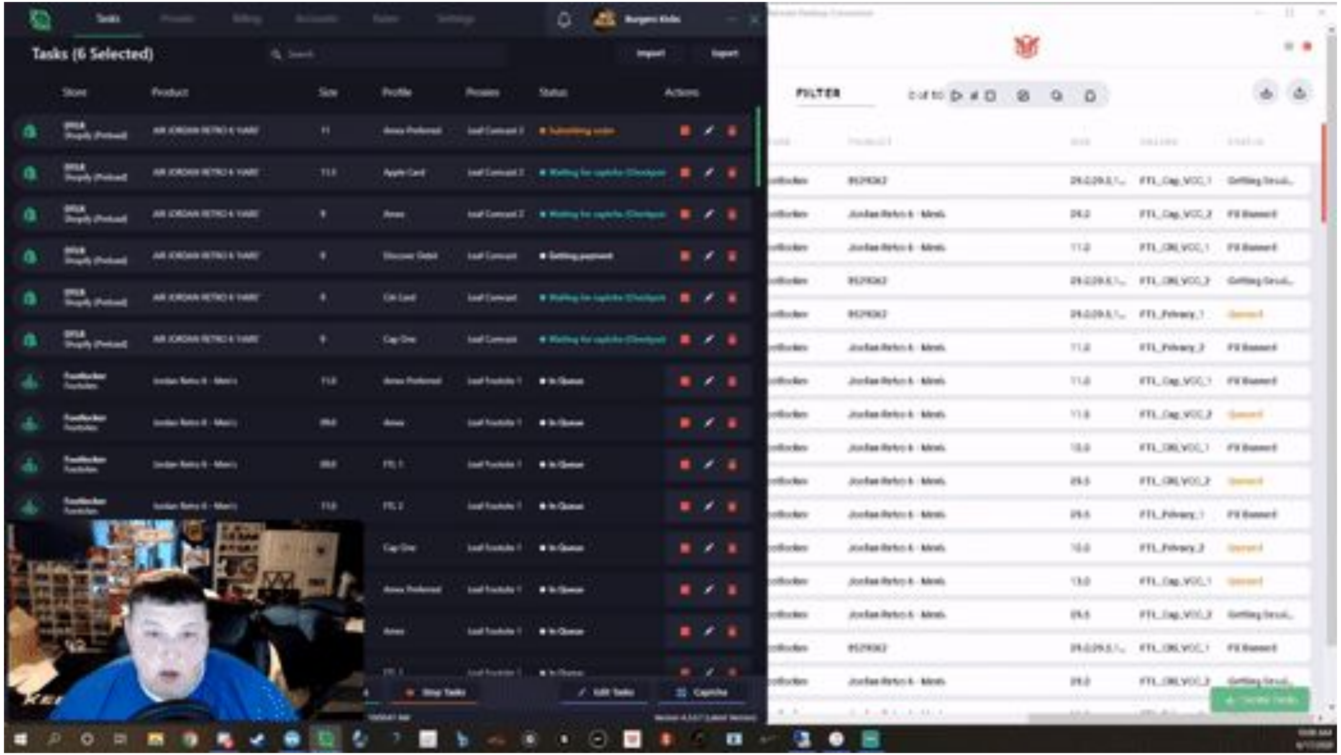
Advanced Bot Ecosystem

Advanced bots purpose

Advanced Bots

- Carding
- Credential stuffing
- Scalping
- Denial of Inventory
- …

Advanced Bot Ecosystem
Botting as a sport



Advanced Bot Ecosystem

Challenge of the research

Advanced Bot Ecosystem
Challenge of the research

General source of bots

HACK FORUMS

CRACKED.IO
BEYOND THE LIMITS

NULLED
EXPECT THE UNEXPECTED

SQUAD
LEAKS & EARN

SINISTER

Specialized marketplaces

TicketBots.net 10 YEARS & counting...

BOT BROKER
Buy and Sell Sneaker Bots

BOTMART

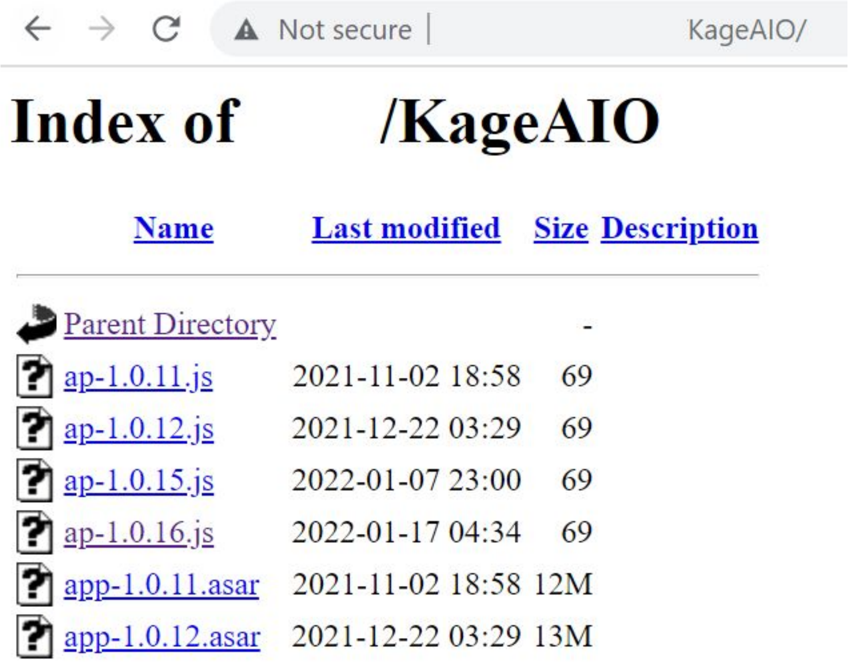
MAB
MOST ADVANCED BOT

Advanced Bot Ecosystem
Challenge of the research

Advanced Bots executables - source code

GitHub

anonfiles
anonymous file upload



Index of /KageAIO

Name	Last modified	Size	Description
Parent Directory		-	
ap-1.0.11.js	2021-11-02 18:58	69	
ap-1.0.12.js	2021-12-22 03:29	69	
ap-1.0.15.js	2022-01-07 23:00	69	
ap-1.0.16.js	2022-01-17 04:34	69	
app-1.0.11.asar	2021-11-02 18:58	12M	
app-1.0.12.asar	2021-12-22 03:29	13M	

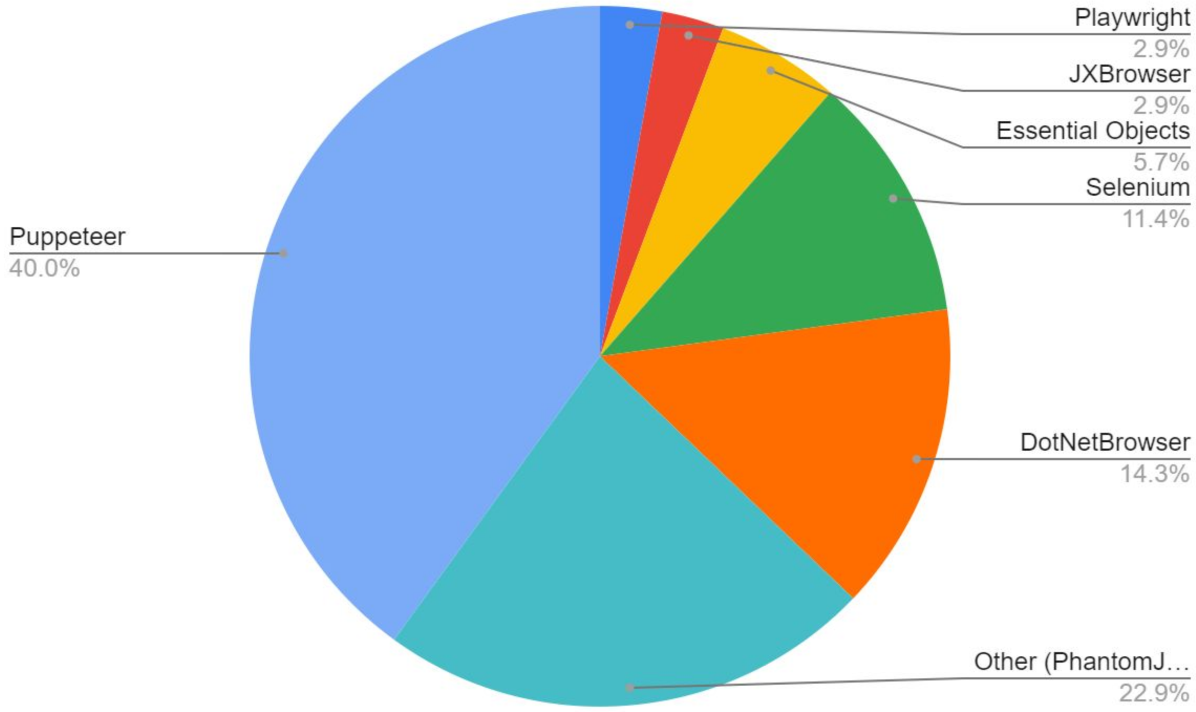
Advanced Bot Ecosystem
Goals

Statistics

Evasion techniques

Advanced Bot Ecosystem

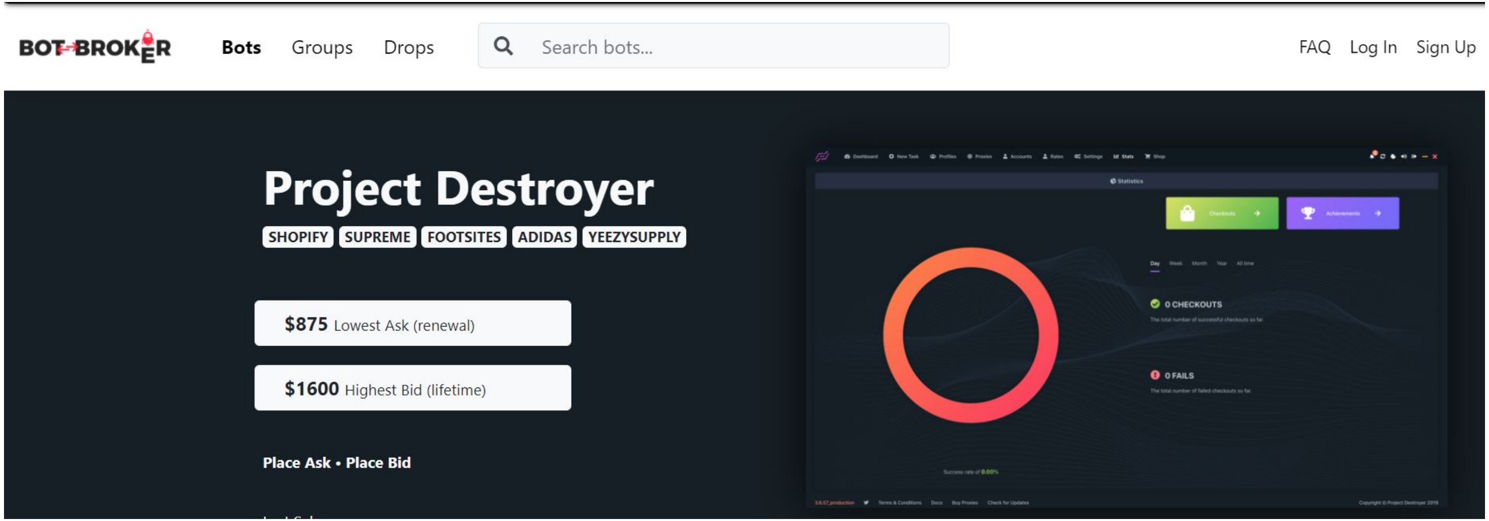
Statistics



Agenda

- Advanced bot market
- **Internal structure of an advanced bot**
- Evasion techniques and detection

Internal structure
Picking an example



Project Destroyer

$875 Lowest Ask (renewal)

$1600 Highest Bid (lifetime)

0 CHECKOUTS

The total number of successful checkouts so far.

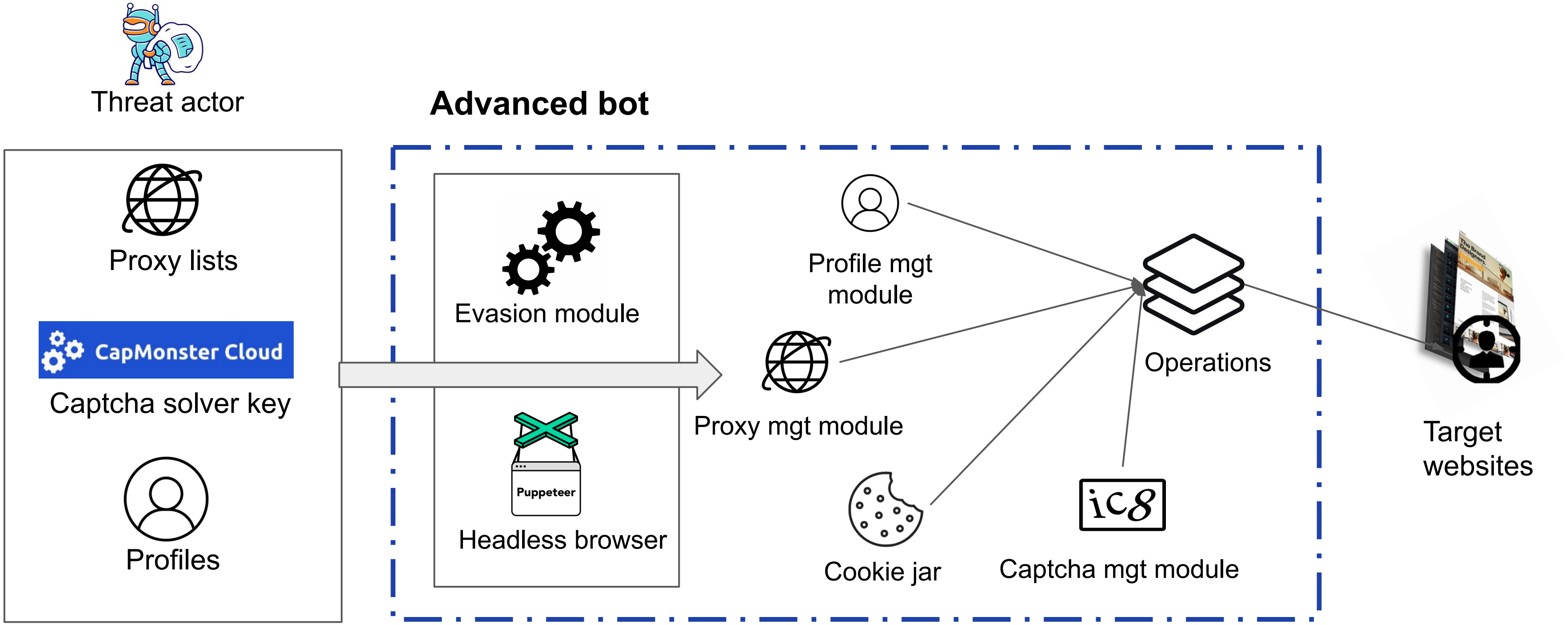
0 FAILS

The total number of failed checkouts so far.

Success rate of 0.00%

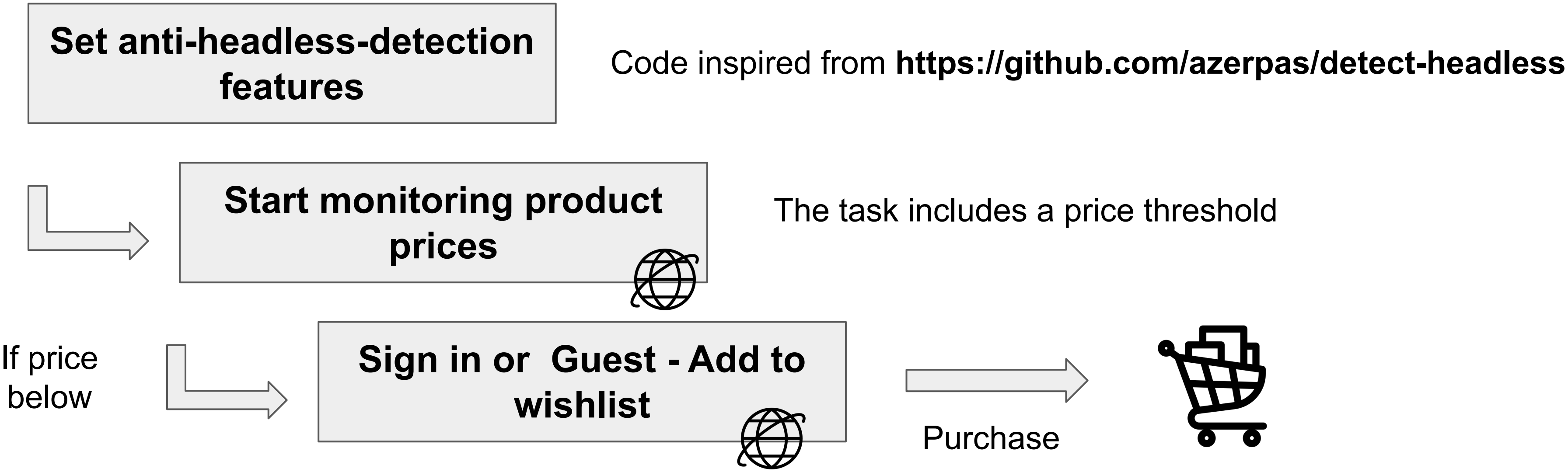
Copyright © Project Destroyer 2019

Internal structure
Picking an example



Internal Structure

- Procedure for **net-a-porter.com**



Set anti-headless-detection features

Code inspired from **https://github.com/azerpas/detect-headless**

Start monitoring product prices

The task includes a price threshold

If price below

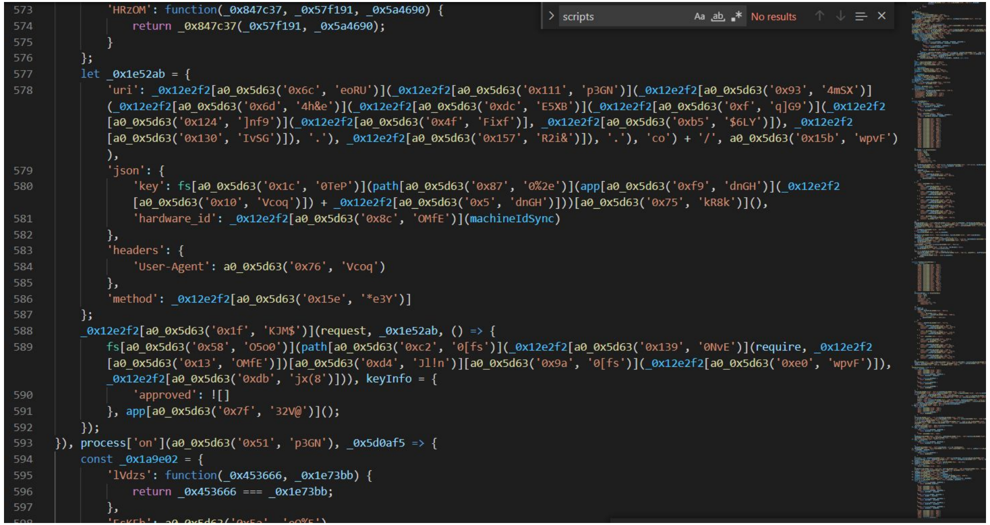
Sign in or Guest - Add to wishlist

Purchase

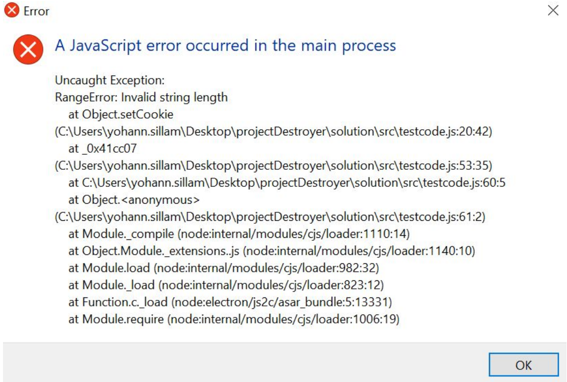
Agenda

- Advanced bot market
- Internal structure of an advanced bot
- **Evasion techniques and detection**

Code Protection
Obfuscation and anti-debug



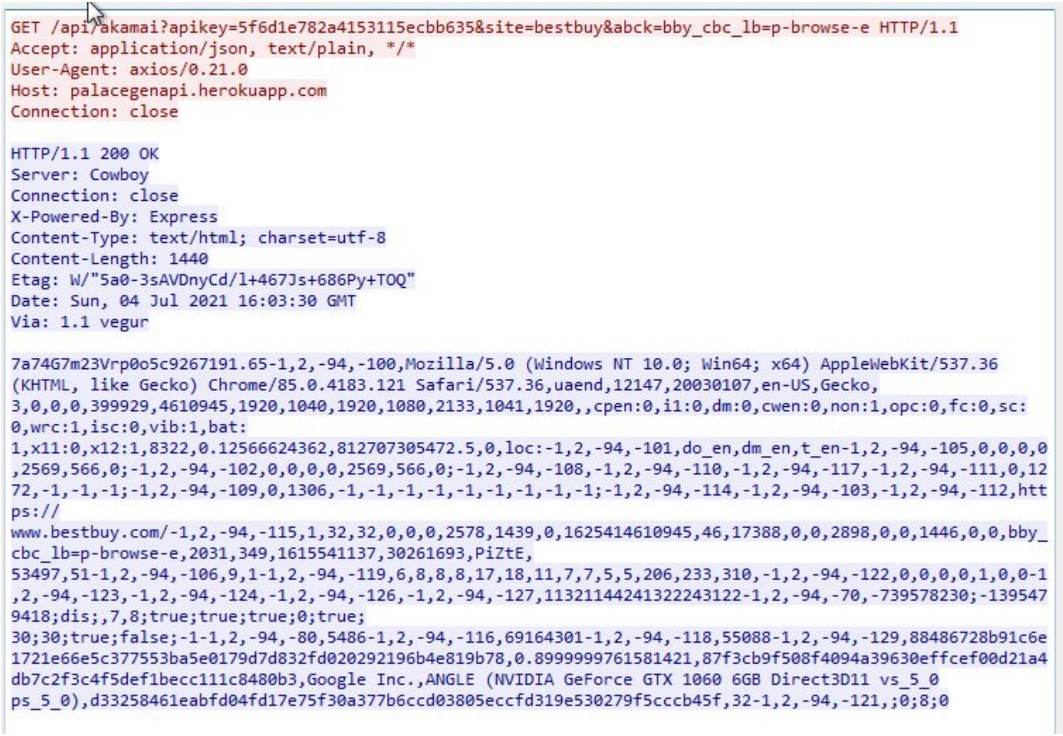
```
            'HRzOM': function(_0x847c37, _0x57f191, _0x5a4690) {
                return _0x847c37(_0x57f191, _0x5a4690);
            }
        };
        let _0x1e52ab = {
            'uri': _0x12e2f2[a0_0x5d63('0x6c', 'eoRU')](_0x12e2f2[a0_0x5d63('0x111', 'p3GN')](_0x12e2f2[a0_0x5d63('0x93', '4mSX')]
            (_0x12e2f2[a0_0x5d63('0x6d', '4h&e')](_0x12e2f2[a0_0x5d63('0xdc', 'E5XB')](_0x12e2f2[a0_0x5d63('0xf', 'q]G9')](_0x12e2f2
            [a0_0x5d63('0x124', ']nf9')](_0x12e2f2[a0_0x5d63('0x4f', 'Fixf')], _0x12e2f2[a0_0x5d63('0xb5', '$6LY')]), _0x12e2f2
            [a0_0x5d63('0x130', 'IvSG')]), '.'), _0x12e2f2[a0_0x5d63('0x157', 'R2i&')]), '.'), 'co') + '/', a0_0x5d63('0x15b', 'wpvF')
            ),
            'json': {
                'key': fs[a0_0x5d63('0x1c', '0TeP')](path[a0_0x5d63('0x87', '0%2e')](app[a0_0x5d63('0xf9', 'dnGH')](_0x12e2f2
                [a0_0x5d63('0x10', 'Vcoq')]) + _0x12e2f2[a0_0x5d63('0x5', 'dnGH')]))[a0_0x5d63('0x75', 'kR8k')](),
                'hardware_id': _0x12e2f2[a0_0x5d63('0x8c', 'OMfE')](machineIdSync)
            },
            'headers': {
                'User-Agent': a0_0x5d63('0x76', 'Vcoq')
            },
            'method': _0x12e2f2[a0_0x5d63('0x15e', '*e3Y')]
        };
        _0x12e2f2[a0_0x5d63('0x1f', 'KJM$')](request, _0x1e52ab, () => {
            fs[a0_0x5d63('0x58', 'O5o0')](path[a0_0x5d63('0xc2', '0[fs')](_0x12e2f2[a0_0x5d63('0x139', '0NvE')](require, _0x12e2f2
            [a0_0x5d63('0x13', 'OMfE')])[a0_0x5d63('0xd4', 'Jl!n')][a0_0x5d63('0x9a', '0[fs')](_0x12e2f2[a0_0x5d63('0xe0', 'wpvF')]),
            _0x12e2f2[a0_0x5d63('0xdb', 'jx(8')])), keyInfo = {
                'approved': ![]
            }, app[a0_0x5d63('0x7f', '32V@')]();
        });
    }), process['on'](a0_0x5d63('0x51', 'p3GN'), _0x5d0af5 => {
        const _0x1a9e02 = {
            'lVdzs': function(_0x453666, _0x1e73bb) {
                return _0x453666 === _0x1e73bb;
            },
            'EsKFh': a0_0x5d63('0x5a', 'e0%F')
```



A JavaScript error occurred in the main process

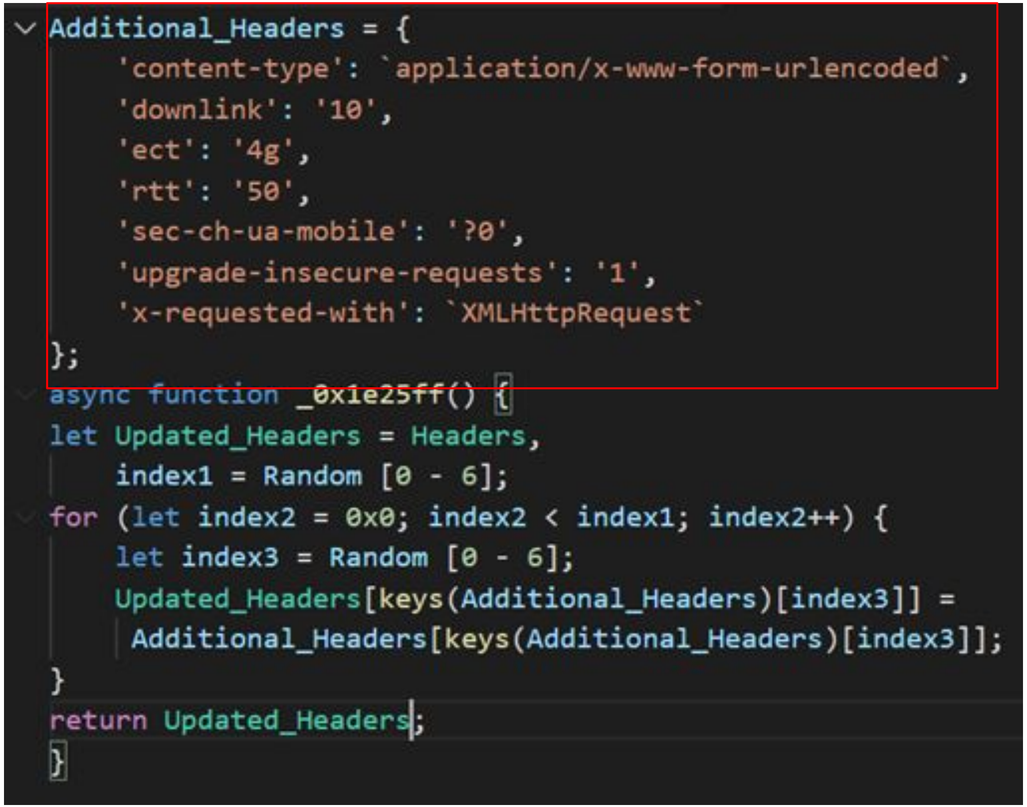
```
Uncaught Exception:
RangeError: Invalid string length
    at Object.setCookie
(C:\Users\yohann.sillam\Desktop\projectDestroyer\solution\src\testcode.js:20:42)
    at _0x41cc07
(C:\Users\yohann.sillam\Desktop\projectDestroyer\solution\src\testcode.js:53:35)
    at C:\Users\yohann.sillam\Desktop\projectDestroyer\solution\src\testcode.js:60:5
    at Object.<anonymous>
(C:\Users\yohann.sillam\Desktop\projectDestroyer\solution\src\testcode.js:61:2)
    at Module._compile (node:internal/modules/cjs/loader:1110:14)
    at Object.Module._extensions..js (node:internal/modules/cjs/loader:1140:10)
    at Module.load (node:internal/modules/cjs/loader:982:32)
    at Module._load (node:internal/modules/cjs/loader:823:12)
    at Function.c._load (node:electron/js2c/asar_bundle:5:13331)
    at Module.require (node:internal/modules/cjs/loader:1006:19)
```

Code Protection
Obfuscation and anti-debug



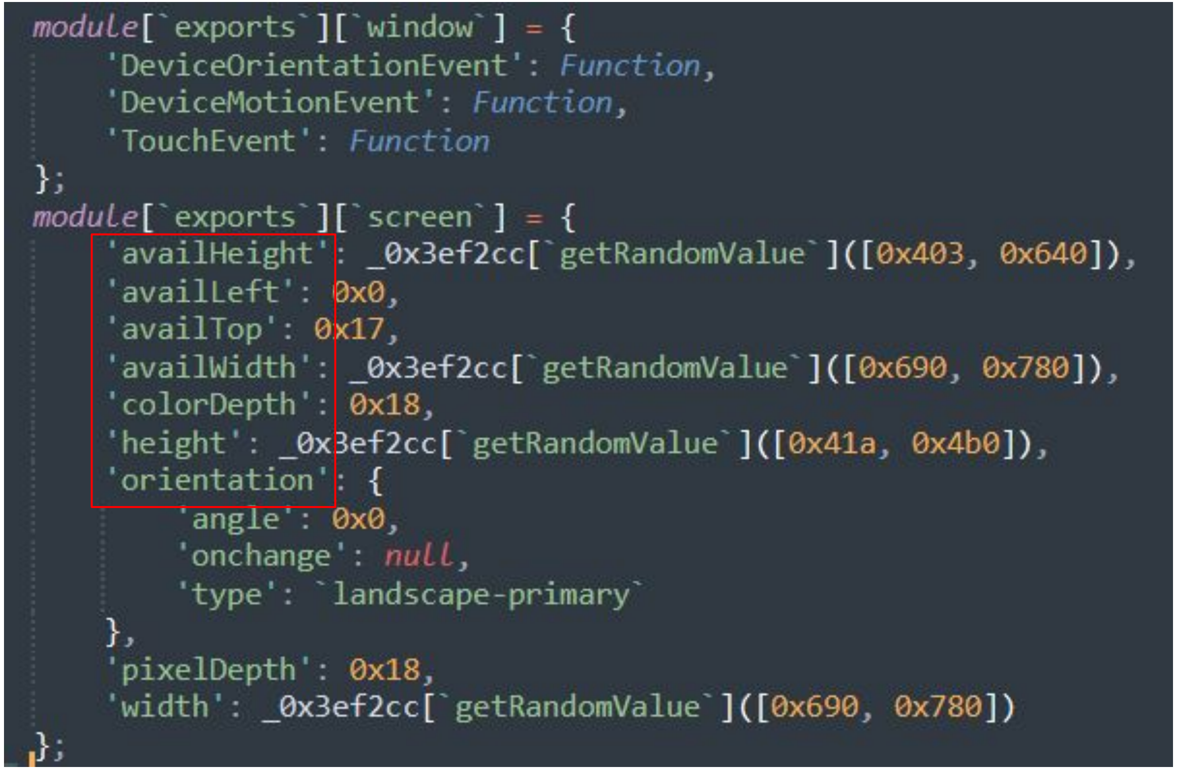
```
GET /api/akamai?apikey=5f6d1e782a4153115ecbb635&site=bestbuy&abck=bby_cbc_lb=p-browse-e HTTP/1.1
Accept: application/json, text/plain, */*
User-Agent: axios/0.21.0
Host: palacegenapi.herokuapp.com
Connection: close

HTTP/1.1 200 OK
Server: Cowboy
Connection: close
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 1440
Etag: W/"5a0-3sAVDnyCd/l+467Js+686Py+TOQ"
Date: Sun, 04 Jul 2021 16:03:30 GMT
Via: 1.1 vegur

7a74G7m23Vrp0o5c9267191.65-1,2,-94,-100,Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36,uaend,12147,20030107,en-US,Gecko,
3,0,0,0,399929,4610945,1920,1040,1920,1080,2133,1041,1920,,cpen:0,i1:0,dm:0,cwen:0,non:1,opc:0,fc:0,sc:
0,wrc:1,isc:0,vib:1,bat:
1,x11:0,x12:1,8322,0.12566624362,812707305472.5,0,loc:-1,2,-94,-101,do_en,dm_en,t_en-1,2,-94,-105,0,0,0,0
,2569,566,0;-1,2,-94,-102,0,0,0,0,2569,566,0;-1,2,-94,-108,-1,2,-94,-110,-1,2,-94,-117,-1,2,-94,-111,0,12
72,-1,-1,-1;-1,2,-94,-109,0,1306,-1,-1,-1,-1,-1,-1,-1,-1,-1;-1,2,-94,-114,-1,2,-94,-103,-1,2,-94,-112,htt
ps://
www.bestbuy.com/-1,2,-94,-115,1,32,32,0,0,0,2578,1439,0,1625414610945,46,17388,0,0,2898,0,0,1446,0,0,bby_
cbc_lb=p-browse-e,2031,349,1615541137,30261693,PiZtE,
53497,51-1,2,-94,-106,9,1-1,2,-94,-119,6,8,8,8,17,18,11,7,7,5,5,206,233,310,-1,2,-94,-122,0,0,0,0,1,0,0-1
,2,-94,-123,-1,2,-94,-124,-1,2,-94,-126,-1,2,-94,-127,11321144241322243122-1,2,-94,-70,-739578230;-139547
9418;dis;,7,8;true;true;true;0;true;
30;30;true;false;-1-1,2,-94,-80,5486-1,2,-94,-116,69164301-1,2,-94,-118,55088-1,2,-94,-129,88486728b91c6e
1721e66e5c377553ba5e0179d7d832fd020292196b4e819b78,0.8999999761581421,87f3cb9f508f4094a39630effcef00d21a4
db7c2f3c4f5def1becc111c8480b3,Google Inc.,ANGLE (NVIDIA GeForce GTX 1060 6GB Direct3D11 vs_5_0
ps_5_0),d33258461eabfd04fd17e75f30a377b6ccd03805eccfd319e530279f5cccb45f,32-1,2,-94,-121,;0;8;0
```

Evasion techniques
Faking HTTP Headers



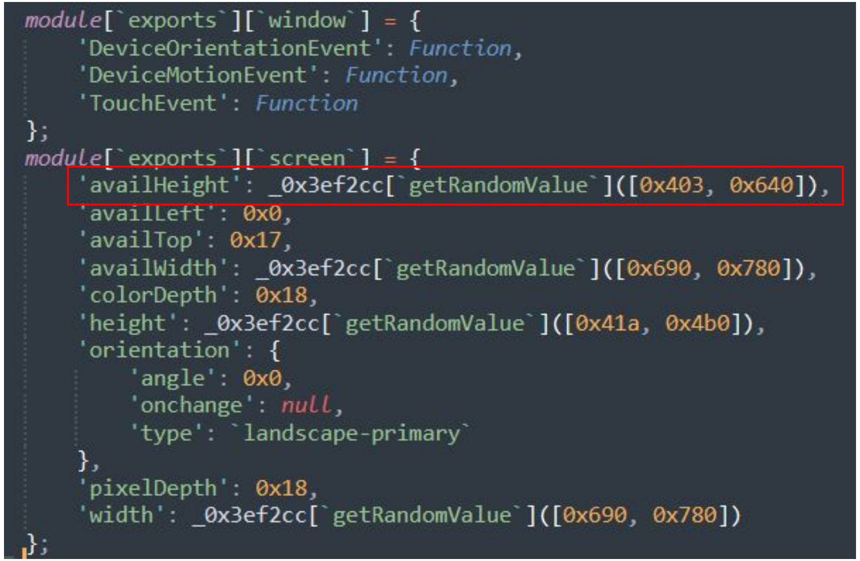
```
Additional_Headers = {
    'content-type': `application/x-www-form-urlencoded`,
    'downlink': '10',
    'ect': '4g',
    'rtt': '50',
    'sec-ch-ua-mobile': '?0',
    'upgrade-insecure-requests': '1',
    'x-requested-with': `XMLHttpRequest`
};
async function _0x1e25ff() {
let Updated_Headers = 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;
}
```

Evasion techniques
Faking device attributes

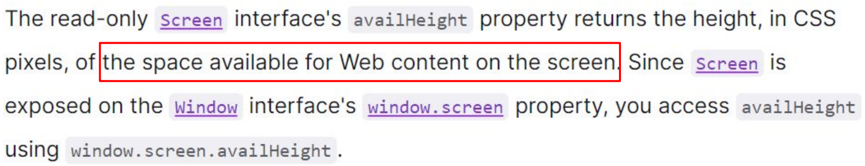


```
module[`exports`][`window`] = {
    'DeviceOrientationEvent': Function,
    'DeviceMotionEvent': Function,
    'TouchEvent': Function
};
module[`exports`][`screen`] = {
    'availHeight': _0x3ef2cc[`getRandomValue`]([0x403, 0x640]),
    'availLeft': 0x0,
    'availTop': 0x17,
    'availWidth': _0x3ef2cc[`getRandomValue`]([0x690,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

Evasion techniques
Faking device attributes

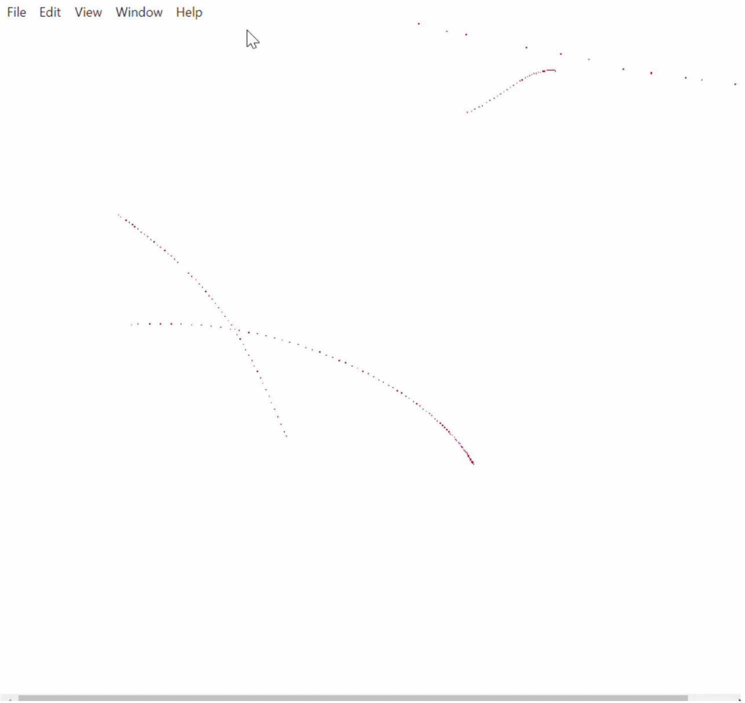


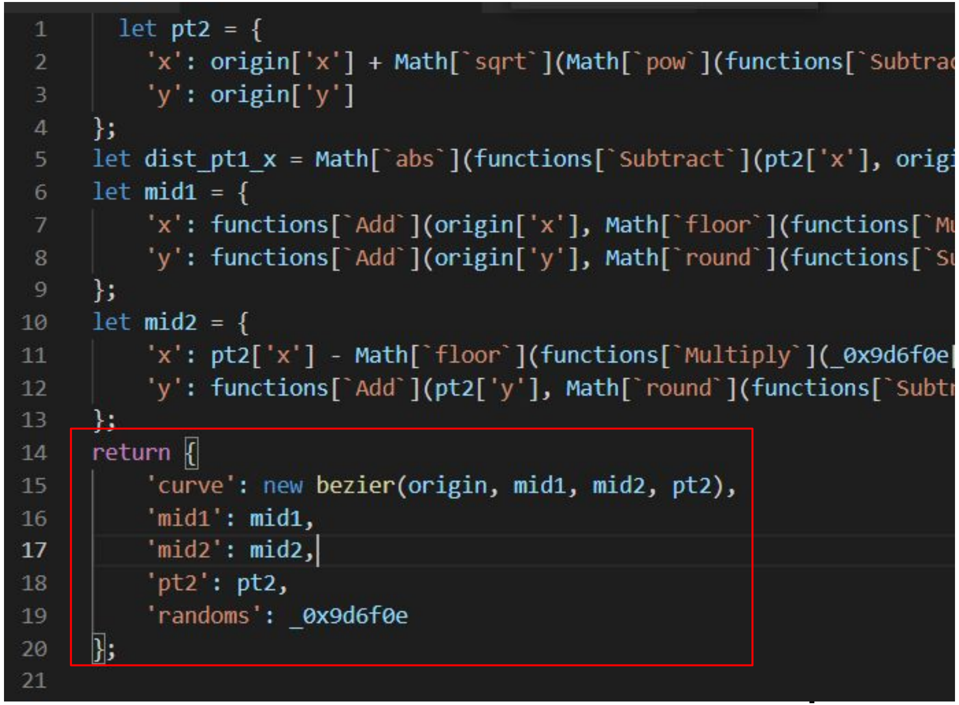
```
module[`exports`][`window`] = {
    'DeviceOrientationEvent': Function,
    'DeviceMotionEvent': Function,
    'TouchEvent': Function
};
module[`exports`][`screen`] = {
    'availHeight': _0x3ef2cc[`getRandomValue`]([0x403, 0x640]),
    'availLeft': 0x0,
    'availTop': 0x17,
    'availWidth': _0x3ef2cc[`getRandomValue`]([0x690,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



The read-only `Screen` interface's `availHeight` property returns the height, in CSS pixels, of the space available for Web content on the screen. Since `Screen` is exposed on the `Window` interface's `window.screen` property, you access `availHeight` using `window.screen.availHeight`.

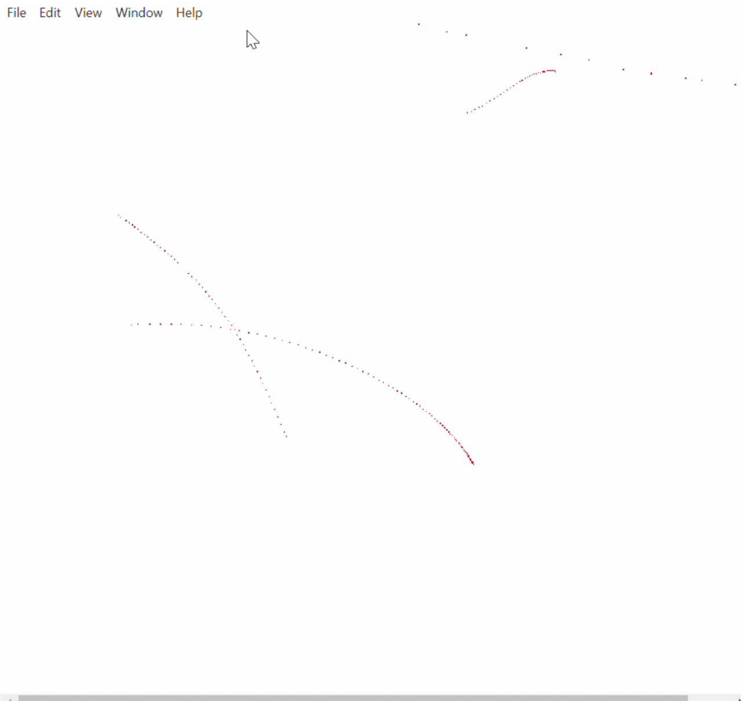
Evasion techniques
Simulated human mouse motion

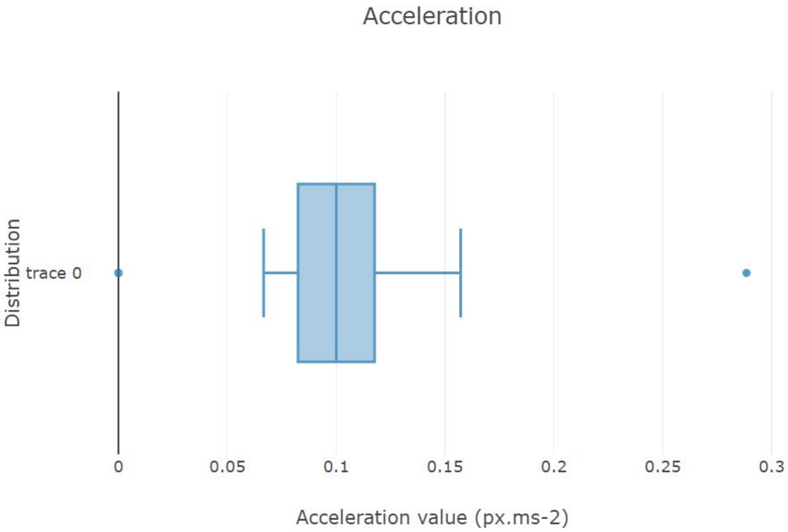




```
  let pt2 = {
    'x': origin['x'] + Math[`sqrt`](Math[`pow`](functions[`Subtrac
    'y': origin['y']
};
let dist_pt1_x = Math[`abs`](functions[`Subtract`](pt2['x'], origi
let mid1 = {
    'x': functions[`Add`](origin['x'], Math[`floor`](functions[`Mu
    'y': functions[`Add`](origin['y'], Math[`round`](functions[`Su
};
let mid2 = {
    'x': pt2['x'] - Math[`floor`](functions[`Multiply`](_0x9d6f0e[
    'y': functions[`Add`](pt2['y'], Math[`round`](functions[`Subtr
};
return {
    'curve': new bezier(origin, mid1, mid2, pt2),
    'mid1': mid1,
    'mid2': mid2,
    'pt2': pt2,
    'randoms': _0x9d6f0e
};
```

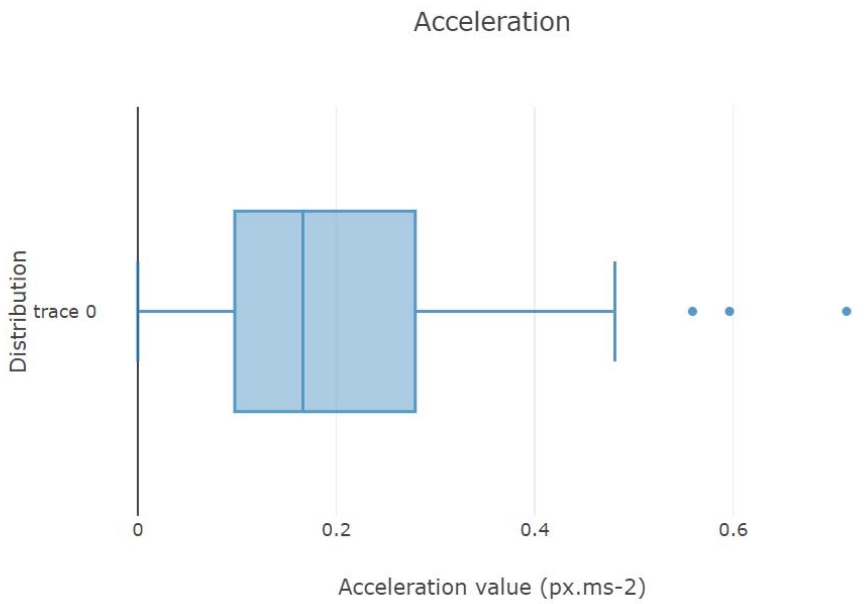
Evasion techniques
Simulated human mouse motion





Evasion techniques

Simulated human mouse motion



Key Takeaways

Malicious bots market is large and expanding

Predominance of Electron & puppeteer

A cat and mouse game

Questions