Advanced Bots and Security Evasion Techniques

PRESENTED BY:
David Warburton, Snr Threat Research Evangelist
F5 Labs
Who Am I?

David Warburton

- Senior Threat Research Evangelist
  F5 Labs
- Royal Holloway
  MSc Information Security (Distinction)
- AppSec, Identity & Auth,
  Cryptography & PKI

@warburtr0n
What are bots?

Advanced Bot Techniques

Detecting and mitigating Bots
Bot Breakdown

- 48.2% Humans
- 28.9% Bad Bots
- 22.9% Good Bots
- 1.2% Monitoring Bots
- 2.9% Commercial Crawlers
- 6.6% Search Engine Bots
- 12.2% Feed Fetchers
- 24.3% Impersonators
- 1.7% Scrapers
- 0.3% Spammers
- 2.6% Hacker Tools

Source: GlobalDots Bot Report

Web app attacks started with botnets
Source: Verizon
Bots by Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Bad Bots</th>
<th>Good Bots</th>
<th>Human</th>
<th>% of Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Travel (no Airlines)</td>
<td>4.50%</td>
<td>46%</td>
<td>92.04%</td>
<td></td>
</tr>
<tr>
<td>Real Estate</td>
<td>12.44%</td>
<td>37.21%</td>
<td>50.35%</td>
<td></td>
</tr>
<tr>
<td>Insurance</td>
<td>12.88%</td>
<td>18.65%</td>
<td>68.47%</td>
<td></td>
</tr>
<tr>
<td>Adult Entertainment</td>
<td>17.57%</td>
<td>0.47%</td>
<td>62.86%</td>
<td></td>
</tr>
<tr>
<td>Travel (incl. Airlines)</td>
<td>19.24%</td>
<td>2.51%</td>
<td>78.25%</td>
<td></td>
</tr>
<tr>
<td>Ecommerce</td>
<td>21.45%</td>
<td>16.49%</td>
<td>62.06%</td>
<td></td>
</tr>
<tr>
<td>Tickets</td>
<td>22.97%</td>
<td>7.82%</td>
<td>69.21%</td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td>24.37%</td>
<td>57.59%</td>
<td>18.04%</td>
<td></td>
</tr>
<tr>
<td>Financial</td>
<td>24.66%</td>
<td>4.35%</td>
<td>70.99%</td>
<td></td>
</tr>
<tr>
<td>Airlines</td>
<td>24.90%</td>
<td>0.93%</td>
<td>55.17%</td>
<td></td>
</tr>
<tr>
<td>Gambling</td>
<td>53.10%</td>
<td>0.09%</td>
<td>46.81%</td>
<td></td>
</tr>
</tbody>
</table>

Source: GlobalDots Bad Bot Report 2018
• Crawler
• DOS Tool
• E-Mail collector
• Exploit tool
• Headless browser
• HTTP library
• Network Scanner
• RSS Reader
• Search bot
• Search engine
• Service agent
• Site monitor
• Social media agent
• Spam bot
• Spyware
• Vulnerability scanner
• Web downloader
• Web spider
• Webserver stress tool
Good Bots

User-agent: *
Disallow: /template/
Disallow: /secret/

CSS
JS
/template/

robots.txt

Support

Type here...

Account  Card  Support  Profile
Bad Bots – OWASP Automated Threats

DoS / Resource Hoarding
- OAT-015 Denial of Service
- OAT-005 Scalping
- OAT-021 Denial of Inventory
- OAT-013 Sniping
- OAT-006 Expediting

Account Takeover
- OAT-007 Credential Cracking
- OAT-008 Credential Stuffing
- OAT-019 Account Creation
- OAT-020 Account Aggregation

Content Theft
- OAT-011 Scraping

Payment Card Data
- OAT-010 Card Cracking
- OAT-001 Carding
- OAT-012 Cashing Out

Other Attacks
- OAT-003 Ad Fraud
- OAT-009 CAPTCHA Defeat
- OAT-016 Skewing
- OAT-017 Spamming
- OAT-002 Token Cracking

Vulnerability Scanning
- OAT-014 Vulnerability Scanning
- OAT-004 Fingerprinting
- OAT-018 Footprinting
def create_json_oneway(self, dump_list):
    for i in range(len(dump_list)):
        temp = '{ "airline" : "' + dump_list[i]['le'][0]['an'] + '"
        temp = temp + ', "price" : "' + str(dump_list[i]['af']) + '"
        temp = temp + ', "total_time" : "' + str(dump_list[i]['td']) + '"
        temp = temp + ', "depart_date" : "' + str(dump_list[i]['le'][0]['fd']) + '"
        temp = temp + ', "depart_time" : "' + str(dump_list[i]['le'][0]['fdt']) + '"
        temp_dump_list = dump_list[i]['le']
        for x in range(len(temp_dump_list)):
            if x == (len(temp_dump_list)-1):
                temp = temp + ', "arrival_date" : "' + str(temp_dump_list[x]['fa']) + '"'
                temp = temp + ', "arrival_time" : self.trip_json.append(temp)
        return json.dumps(self.trip_json)
OAT-011 Scaping-as-a-Service

Developer tools
Ideal for: developers, data scientists, data teams looking to execute web scraping projects.

PROJECT BUDGET  TOTAL BIDS
$250 - $750 USD  31

PROJECT DESCRIPTION
i need a bot that will scrape odds on various sporting events from a number of bookie websites. some of these have real-time XML feeds which can be used, others, the actual odds need to be scraped. the odds are then to be stored into a SQL database for analysis, provisions need to be made to ensure that the pages that are being scraped are not done too regularly in order to avoid IP being blocked. i can provide guidance on this area. some formatting needs to be done between some sites, as different bookies have different ways of representing data.

i would like the application ideally written in either C sharp or .net (c sharp).

there will be a further phase of this project which will involve automating logon to the bookie site. the objective of this is to award this project to whoever successfully completes this phase, so when bidding please be sure to consider this.

Web Scraping Bots

This project was awarded to ASYanush for $400 USD.
Copping, Scalping and Sniping
OAT-005, OAT-013, OAT-021

Follow Twitter

Shoe Size

Nike Account
OAT-019 New Account Creation Attacks

Personal Data
Previous Breaches

USERNAME
**********
USERNAME
**********
USERNAME
**********
USERNAME
**********
USERNAME
**********
USERNAME
**********
USERNAME
**********
USERNAME
**********

Healthcare Site

E-Commerce Site

Finance Site

Services Site

Other Sites
OAT-019 New Account Creation Attacks (FSI 2017)

Volume per Transaction Type

- Payments: Blue
- Account logins: Orange
- New account creations: Purple

Attack rate per Transaction Type

- Payments: 4.50%
- Account logins: 1.50%
- New account creations: 3.00%

Source: threatmetrix.com
# OAT-014 Scanning

## Top 10 Attacked Ports Globally

### 2018

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS: 443</td>
<td></td>
</tr>
<tr>
<td>MS SMB: 445</td>
<td></td>
</tr>
<tr>
<td>SSH: 22</td>
<td></td>
</tr>
<tr>
<td>ICS?: 1443</td>
<td></td>
</tr>
<tr>
<td>Port 11684</td>
<td></td>
</tr>
<tr>
<td>SIP: 5060</td>
<td></td>
</tr>
<tr>
<td>HTTP: 80</td>
<td></td>
</tr>
<tr>
<td>Port 51413</td>
<td></td>
</tr>
<tr>
<td>Port 23810</td>
<td></td>
</tr>
<tr>
<td>Telnet: 23</td>
<td></td>
</tr>
</tbody>
</table>

### Q1 2019

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS SMB: 445</td>
<td></td>
</tr>
<tr>
<td>SIP: 5060</td>
<td></td>
</tr>
<tr>
<td>SSH: 22</td>
<td></td>
</tr>
<tr>
<td>ICS?: 2222</td>
<td></td>
</tr>
<tr>
<td>Port 3128</td>
<td></td>
</tr>
</tbody>
</table>

### Source

F5 Labs & Baffin Bay Networks
8.4B DEVICES
Gartner

1T DEVICES
SoftBank

2017 > 2035

*Excludes smartphones, tablets, and computers
Thingbots

Affected Devices

- CCTV
- DVRs
- SOHO routers
- iOS
- WAPs
- Set-Top Boxes
- Media Center
- ICS
- Android
- IP Cameras
- Wireless Chipsets
- NVR Surveillance
- VoIP Devices
- Cable Modems
- Busybox Platforms
- Smart TVs

84% Discovered since Mirai

- 6 Bots: Death, Okane, Anarchy, Torii, Yasaku, Thanos
- 13 Bots: SORA, OWARI, UPNP, OMNI, RoamingMantis, Wicked, VPFilter, DaddyL33t, Josho, Tokyo, Extendo, Hakai, Akira / Saito
Shifting from primarily DDoS to multi-purpose

- DNS Hijack
- Crypto-miner
- DDoS
- PDoS
- Proxy Servers
- Unknown...
- Rent-a-bot
- Credential Collector
- Install-a-bot
- Multi-purpose Bot
- Fraud trojan
- ICS protocol monitoring
- Tor Node
- Sniffer

PayBot
Hydra
Aidra
Moon
Darlloz
Marcher
Gafgyt
Family
Crash
crash override
Satori Fam
Amnesia
Persiaral
Masuta
PureMasuta
Hide N Seek
JenX
OMG
DoubleDoor
Sora
OWARI
UPnPProxy
OMNI
RoamingMantis
Wicked
VPNFilter
Mirai
(SOHO Routers, DVRs, IP Cameras - Oct 2018)

• 20,000 devices in less than 24 hours

• Peak of over 600,000 devices

• Conducted over 15,000 attacks as of early 2017

• Has spun-off at least 10 variants since source code went public
  • ‘Wicked’ installs rentable bots

• Effective
  • Efficient internet-wide scanning
  • Simple cross-platform architecture
  • Default credentials
How “Things” Are Compromised

Service Attacked To Infect IoT Device

- TCP
- Telnet
- HNAP
- IEC 101, 104, OPC
- TR-064, TR 069
- SOAP
- UPnP
- HTTP
- CVE Specific


1 Bot Hydra
1 Bot Payb0t
1 Bot Aidra
28 Bots Darloz, Marcher
1 Bot Moon
8 Bots Hajime, Trickbot, IRC, Telnet, Annie
1 Bot Crash override
1 Bot Remaiten
3 Bots Mirai, BigBrother, Radiation
1 Bot Brickerbot
4 Bots Satori Fam, Amnesia, Penairal
2 Bots WireX, Reaper
25 Bots Masuta, PureMasuta, Hide ‘N Seek, JenX, OMG, DoubleDoor
65 Bots SORA, OWARI, UPnPProxy, OMNI, RoamingMantis, Wicked, VPNFilter
7 Bots
F5 Labs discovers cellular gateway vulns
F5 Labs discovers cellular gateway vulns
"Exploiting" the Vulnerability

NO DEPENDENCY on any vulnerability within the hardware or software.

DEFAULT PASSWORD  *****

Bruteforce attack(s) are unnecessary.

WAN IP 166.139.19.193

PUBLIC GPS COORDINATES
40° 49' 51.5" N
47° 26' 03.5" W

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>root</td>
<td>ts</td>
<td>ts</td>
<td>manager</td>
<td>manager123</td>
<td>plcmspipp</td>
<td>plcmspipp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin</td>
<td>admin</td>
<td>bot</td>
<td>bot</td>
<td>teamspeak3</td>
<td>teamspeak3</td>
<td>weblogic</td>
<td>weblogic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user</td>
<td>user</td>
<td>deploy</td>
<td>deploy</td>
<td>nobody</td>
<td>nobody</td>
<td>redhat</td>
<td>redhat123456</td>
<td></td>
<td></td>
</tr>
<tr>
<td>test</td>
<td>test</td>
<td>monitor</td>
<td>monitor</td>
<td>csgoserver</td>
<td>csgoserver</td>
<td>developer</td>
<td>developer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ubuntu</td>
<td>ubuntu</td>
<td>administrator</td>
<td>administrator</td>
<td>test2</td>
<td>test2</td>
<td>public</td>
<td>public</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ubnt</td>
<td>ubnt</td>
<td>bin</td>
<td>bin</td>
<td>demo</td>
<td>demo</td>
<td>student</td>
<td>student</td>
<td></td>
<td></td>
</tr>
<tr>
<td>support</td>
<td>support</td>
<td>default</td>
<td>nopass</td>
<td>0</td>
<td></td>
<td>webmaster</td>
<td>webmaster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>oracle</td>
<td>oracle</td>
<td>adm</td>
<td>adm</td>
<td>a</td>
<td>a</td>
<td>osmc</td>
<td>osmc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pi</td>
<td>raspberry</td>
<td>vagrant</td>
<td>vagrant</td>
<td>minecraft</td>
<td>minecraft</td>
<td>c</td>
<td>c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>guest</td>
<td>guest</td>
<td>anonymous</td>
<td>any@</td>
<td>alex</td>
<td>q1w2e3r4t5</td>
<td>server</td>
<td>server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>postgres</td>
<td>postgres</td>
<td>uucp</td>
<td>uucp</td>
<td>postfix</td>
<td>postfix</td>
<td>supervisor</td>
<td>supervisor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ftpuser</td>
<td>asteriskftp</td>
<td>www</td>
<td>www</td>
<td>glassfish</td>
<td>glassfish</td>
<td>22</td>
<td>backup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>usuario</td>
<td>usuario</td>
<td>jenkins</td>
<td>jenkins</td>
<td>jboss</td>
<td>jboss</td>
<td>hdfs</td>
<td>hdfs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nagios</td>
<td>nagios</td>
<td>apache</td>
<td>apache</td>
<td>master</td>
<td>master</td>
<td>linux</td>
<td>linux</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1234</td>
<td>1234</td>
<td>sshd</td>
<td>sshd</td>
<td>ghost</td>
<td>ghost</td>
<td>postmaster</td>
<td>postmaster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ftp</td>
<td>ftp</td>
<td>P1cmSpIp</td>
<td>PlcmSpIp</td>
<td>vnc</td>
<td>vnc</td>
<td>csserver</td>
<td>csserver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>operator</td>
<td>operator</td>
<td>cisco</td>
<td>cisco</td>
<td>info</td>
<td>info</td>
<td>prueba</td>
<td>prueba</td>
<td></td>
<td></td>
</tr>
<tr>
<td>git</td>
<td>git</td>
<td>sinusbot</td>
<td>sinusbot</td>
<td>111111</td>
<td>856149100</td>
<td>matt</td>
<td>matt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hadoop</td>
<td>hadoop</td>
<td>user1</td>
<td>user1</td>
<td>debian</td>
<td>debian</td>
<td>vyatta</td>
<td>vyatta</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ts3</td>
<td>ts3</td>
<td>backup</td>
<td>backup</td>
<td>centos</td>
<td>centos</td>
<td>hduser</td>
<td>hduser</td>
<td></td>
<td></td>
</tr>
<tr>
<td>teamspeak</td>
<td>teamspeak</td>
<td>Management</td>
<td>TestingR2</td>
<td>testuser</td>
<td>testuser</td>
<td>nexus</td>
<td>nexus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mysql</td>
<td>mysql</td>
<td>steam</td>
<td>steam</td>
<td>system</td>
<td>sytem</td>
<td>ethos</td>
<td>live</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tomcat</td>
<td>tomcat</td>
<td>mother</td>
<td>fucker</td>
<td>www-data</td>
<td>www-data</td>
<td>Admin</td>
<td>Admin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>service</td>
<td>dev</td>
<td>dev</td>
<td>test1</td>
<td>test1</td>
<td>mc</td>
<td>mc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>butter</td>
<td>xuelp123</td>
<td>zabbix</td>
<td>zabbix</td>
<td>upload</td>
<td>upload</td>
<td>telnet</td>
<td>telnet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Top 100 Admin Creds Used in SSH Brute Force Attacks**

**H1 2019**

Source: F5 Labs
<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Attacks</th>
<th>Targets</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP flood</td>
<td>2,736</td>
<td>1,035</td>
<td>A</td>
</tr>
<tr>
<td>UDP-PLAIN flood</td>
<td>2,542</td>
<td>1,278</td>
<td>V</td>
</tr>
<tr>
<td>UDP flood</td>
<td>2,440</td>
<td>1,479</td>
<td>V</td>
</tr>
<tr>
<td>ACK flood</td>
<td>2,173</td>
<td>875</td>
<td>S</td>
</tr>
<tr>
<td>SYN flood</td>
<td>1,935</td>
<td>764</td>
<td>S</td>
</tr>
<tr>
<td>GRE-IP flood</td>
<td>994</td>
<td>587</td>
<td>A</td>
</tr>
<tr>
<td>ACK-STOMP flood</td>
<td>830</td>
<td>359</td>
<td>S</td>
</tr>
<tr>
<td>VSE flood</td>
<td>809</td>
<td>550</td>
<td>A</td>
</tr>
<tr>
<td>DNS flood</td>
<td>417</td>
<td>173</td>
<td>A</td>
</tr>
<tr>
<td>GRE-ETH flood</td>
<td>318</td>
<td>210</td>
<td>A</td>
</tr>
</tbody>
</table>
Application DDoS Attacks (F5 SIRT vs SOC)

Application targeted DDoS attacks are a large portion of the attack types that get escalated to our SIRT for assistance.

<table>
<thead>
<tr>
<th>Year</th>
<th>SOC-Mitigated</th>
<th>SIRT-Mitigated</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>2%</td>
<td>71%</td>
</tr>
<tr>
<td>2018</td>
<td>2%</td>
<td>32%</td>
</tr>
</tbody>
</table>

SOC-Mitigated: 
- 2017: 2%
- 2018: 2%

SIRT-Mitigated: 
- 2017: 71%
- 2018: 32%
Top 20 targeted ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>SIP</td>
</tr>
<tr>
<td>2222</td>
<td>SSH &amp; Rockwell</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>445</td>
<td>SMB</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
</tr>
<tr>
<td>1433</td>
<td>MS SQL</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
</tr>
<tr>
<td>8291</td>
<td>MikroTik</td>
</tr>
<tr>
<td>7547</td>
<td>TR069</td>
</tr>
<tr>
<td>3306</td>
<td>MySQL</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
</tr>
<tr>
<td>3389</td>
<td>RDP</td>
</tr>
<tr>
<td>1723</td>
<td>PPTP</td>
</tr>
<tr>
<td>5061</td>
<td>Secure SIP</td>
</tr>
<tr>
<td>61137</td>
<td></td>
</tr>
<tr>
<td>4433</td>
<td>HTTPS</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>12555</td>
<td></td>
</tr>
<tr>
<td>8545</td>
<td>JSON</td>
</tr>
<tr>
<td>139</td>
<td>NetBios</td>
</tr>
</tbody>
</table>

Country:
- Netherlands
- China
- US
- Canada
- France
- Russia
- UK
- South Korea
- Brazil
- India
- Ukraine

IPs Attacking UK
(last 90 days as of 3/1/2019)
Shifting Sources

Thanks to proxies & IoT devices

- Previously unseen IP addresses: 100%
- Previously unseen networks (ASN): 80%
User-agent

- 1,080,598 user-agents
- 3,999 of which are bots
- Fake GoogleBot: 13,037 IP’s in June 2019 alone
  - e.g. 38.124.xxx.xx
- MikroTik device - lots of known vulns
- Combat with reverse DNS lookups
Combating Bots with Client-side Challenge

1. **First time request to web server**: WAF responds with Injected JS. Request is not passed to the server.

2. **No challenge response from bots**: Bots are dropped.

3. **WAF verifies response authenticity**.
   - Cookie is signed, time stamped, and fingerprinted.
   - Valid response is sent to the server.

4. **WAF response to web server**.
# Headless Browsers

- Command line and scriptable execution of browsers
- Chrome without the chrome!
- Able to render HTML and execute JavaScript & AJAX
- Often Selenium based

---

**Headless Chrome**

- The `--headless` flag runs Headless in a mode where you can evaluate JS expressions in the browser, right from the command line:

```bash
$ chrome --headless --disable-gpu --no-sandbox --disable-dev-shm-usage --user-data-dir=. --remote-debugging-port=9222
```

---

<table>
<thead>
<tr>
<th>Headless Browser</th>
<th>Website</th>
<th>Rendering Engine</th>
<th>JavaScript Engine</th>
<th>Common Browsers</th>
<th>Other Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sahi</td>
<td><a href="http://sahi.co.in/">http://sahi.co.in/</a></td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td><a href="http://sahi.co.in/w/configuring-sahi-with-xvfb">http://sahi.co.in/w/configuring-sahi-with-xvfb</a></td>
</tr>
<tr>
<td>Google WebDriver (Selenium)</td>
<td><a href="http://code.google.com/p/selenium/">http://code.google.com/p/selenium/</a></td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Possibly some limitations in mobile devices (also in Sahi)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://github.com/aredridel/html5">https://github.com/aredridel/html5</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://github.com/tmpvar/jsdom">https://github.com/tmpvar/jsdom</a></td>
</tr>
</tbody>
</table>
Selenium

```python
from selenium import webdriver
from selenium.common.exceptions import TimeoutException

browser = webdriver.Firefox()
browser.get("http://www.facebook.com")
username = browser.find_element_by_id(\"email\")
password = browser.find_element_by_id(\"password\")
submit = browser.find_element_by_id(\"submit\")
username.send_keys(\"me\")
password.send_keys(\"mykewlpass\")
submit.click()
wait = WebDriverWait(browser, 5)
try:
    page_loaded = wait.until_not(
        lambda browser: browser.current_url == login_page
    )
except TimeoutException:
    self.fail("Loading timeout expired")
self.assertEqual(
browser.current_url,
correct_page,
msg = \"Successful Login\"
)
```
Scriptable Browser as-a-Service

- Detect headless browsers via extensions and browser flags
CAPTCHA Solvers – Browser Extensions

Rumola

- Detect CAPTCHA extensions based on HTML insertion

AntiCaptcha

- Detect CAPTCHA extensions based on HTML insertion
Automated CAPTCHA Solvers

• Bot detects that a CAPTCHA is existing on the page
• Bot saves CAPTCHA into an image file
• Bot uploads the saved image file to the solver servers
• The solver will respond with a CAPTCHA ID
• Bot polls the solver API using the CAPTCHA ID it received until the status of the CAPTCHA id is changed to solved
• Bot sends solution to the scraped website and continues attack process
ReCaptcha v3 Solvers

- ReCaptcha v3 uses ‘scores’ from 0.1 to 0.9 to rate the client
- Typically, a user score will be the same/similar across sites
- ReCaptcha v3 solver monitors scores of workers
- Selected the worker with the highest score to solve the Captcha

https://2captcha.com/2captcha-api#solving_recaptchav3
Simulated Mouse Events

- Fake mouse movements can lack cursor positioning
Bots Attacking Mobile APIs

- Mobile
- Browsers
- Attackers
- Bots

API Gateway

Mobile bots?
Detect GET flood attacks against Heavy URIs

Identify non-human surfing patterns

Fingerprint client capabilities

Operating system
Browser
• Screen size and colour depth
• Plugin details
• Time zone
• HTTP_ACCEPT headers
• Language
• System fonts
• Touch support
• Extensions
• TLS handshake

Strong authentication
In a shocking finding, scientist discovered a herd of unicorns living in a remote, previously unexplored valley, in the Andes Mountains. Even more surprising to the researchers was the fact that the unicorns spoke perfect English.

The scientist named the population, after their distinctive horn, Ovid’s Unicorn. These four-horned, silver-white unicorns were previously unknown to science.

Now, after almost two centuries, the mystery of what sparked this odd phenomenon is finally solved.

Dr. Jorge Pérez, an evolutionary biologist from the University of La Paz, and several companions, were exploring the Andes Mountains when they found a small valley, with no other animals or humans. Pérez noticed that the valley had what appeared to be a natural fountain, surrounded by two peaks of rock and silver snow.