



OWASP London
July 2019

Advanced Bots and Security Evasion Techniques

PRESENTED BY:

David Warburton, Snr Threat Research Evangelist
F5 Labs

Who Am I?

David Warburton

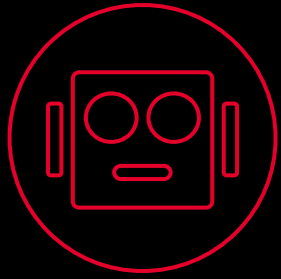
- Senior Threat Research Evangelist
F5 Labs
- Royal Holloway
MSc Information Security (Distinction)
- AppSec, Identity & Auth,
Cryptography & PKI

@warburtr0n



David Warburton, senior threat evangelist at application services organisation F5 Networks, believes the knowledge amassed by cyber-criminals is invaluable for businesses trying to shore up their defences. "When we employ contractors to work on our homes, we tend to look for someone with strong hands-on experience," he says. "So while it may sound counter-intuitive to make use of ex-criminals to help plan and test our cyberdefences, the one thing they have in abundance is hands-on experience. "Security architects have a wealth of knowledge on industry best practice, but what is often lacking is first-hand experience of how attackers perform reconnaissance, chain together multiple attacks and gain access to corporate networks. Application defenders need to consider every single possible angle of attack. With tech





What are bots?

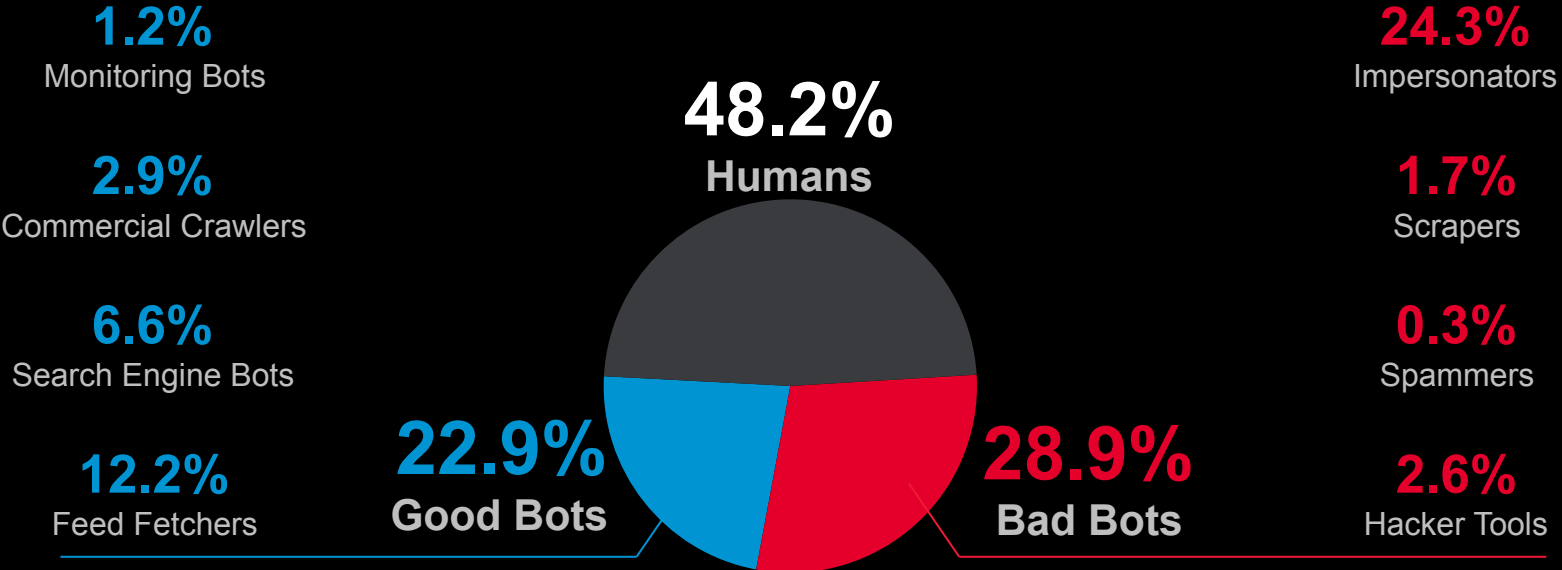


**Advanced Bot
Techniques**



**Detecting and
mitigating Bots**

Bot Breakdown



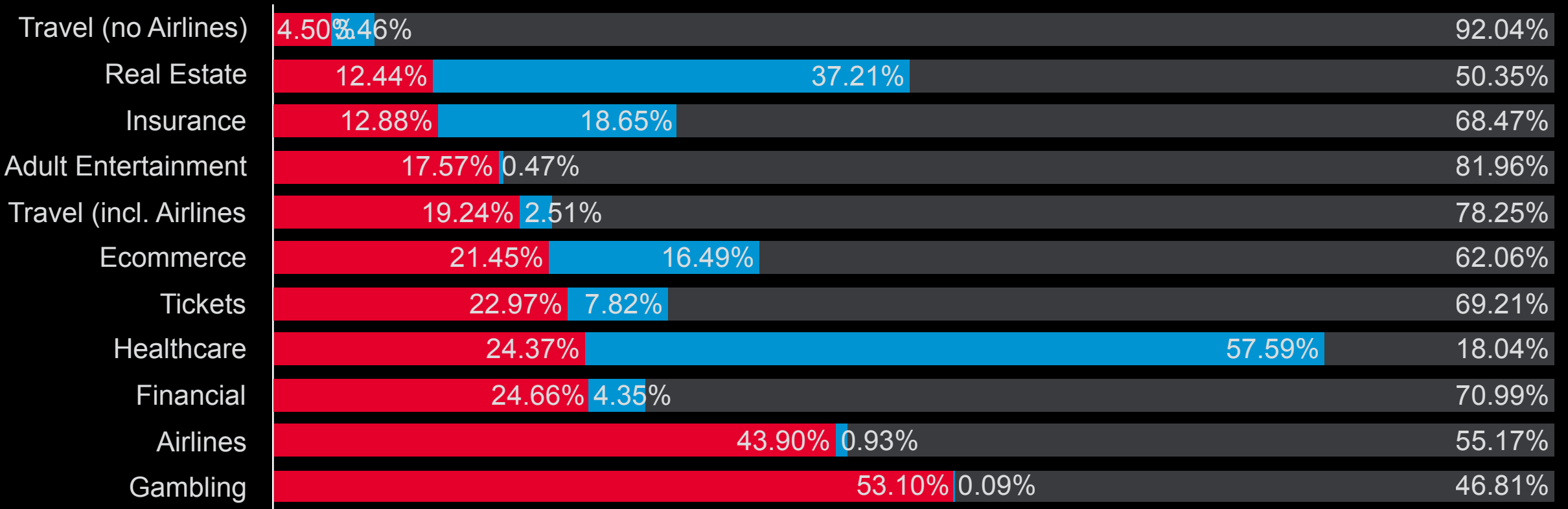
Source: GlobalDots Bot Report



Web app attacks started with botnets

Source: Verizon

Bots by Industry

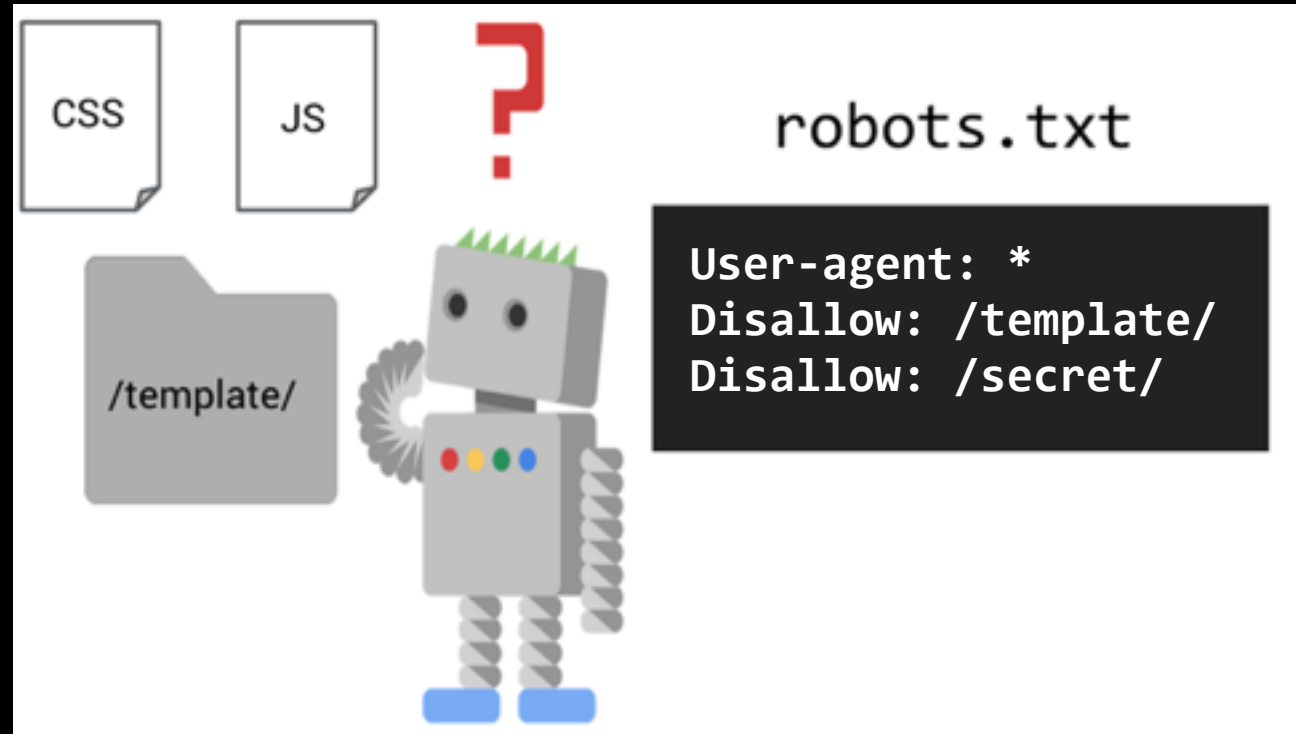
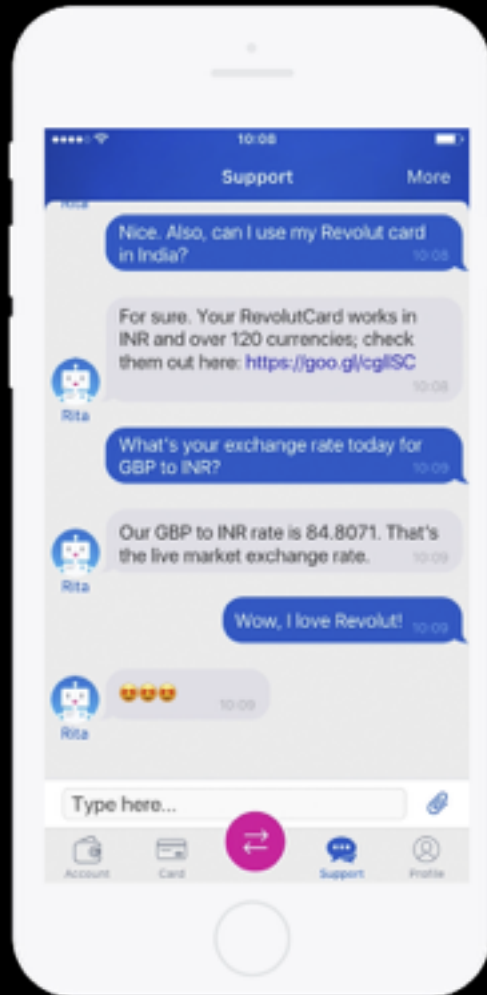


% of Traffic

Bad Bots Good Bots Human

- **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



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](#)



Content Theft

[OAT-011 Scraping](#)



Other Attacks

[OAT-003 Ad Fraud](#)
[OAT-009 CAPTCHA Defeat](#)
[OAT-016 Skewing](#)
[OAT-017 Spamming](#)
[OAT-002 Token Cracking](#)



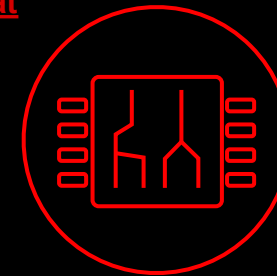
Account Takeover

[OAT-007 Credential Cracking](#)
[OAT-008 Credential Stuffing](#)
[OAT-019 Account Creation](#)
[OAT-020 Account Aggregation](#)



Payment Card Data

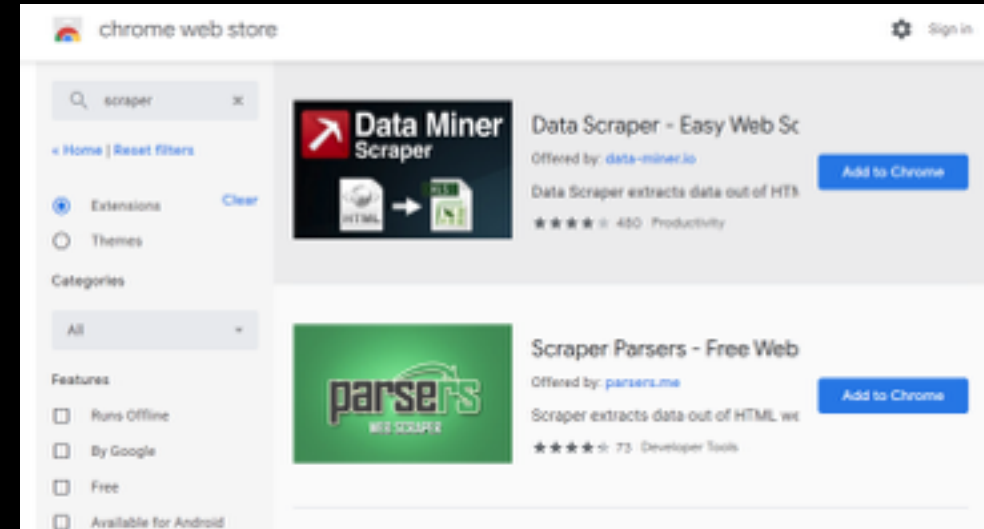
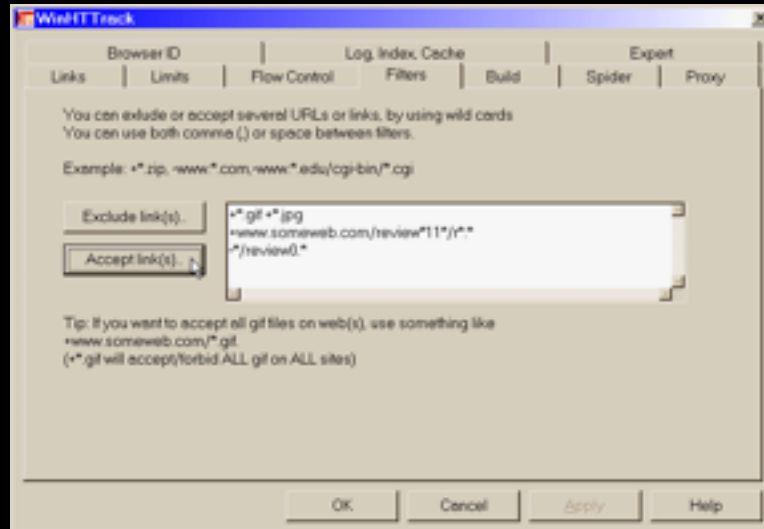
[OAT-010 Card Cracking](#)
[OAT-001 Carding](#)
[OAT-012 Cashing Out](#)



Vulnerability Scanning

[OAT-014 Vulnerability Scanning](#)
[OAT-004 Fingerprinting](#)
[OAT-018 Footprinting](#)

OAT-011 Scraping



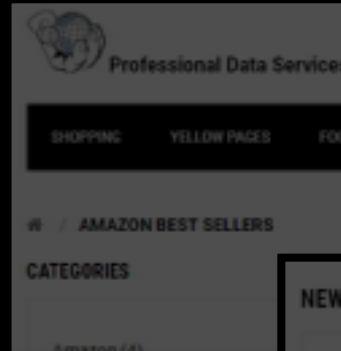
```
def create_json_oneway(self, dump_list):
    for i in range(len(dump_list)):
        temp = '{ "airline" : "' + dump_list[i]['le'][0]['an'] + '"
        temp = temp + ', "price" : "' + str(dump_list[i]['af']) + '"
        temp = temp + ', "total_time" : "' + str(dump_list[i]['td']) + '"
        temp = 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 Scraping-as-a-Service



Developer tools

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



PROJECT BUDGET
\$250 - \$750 USD

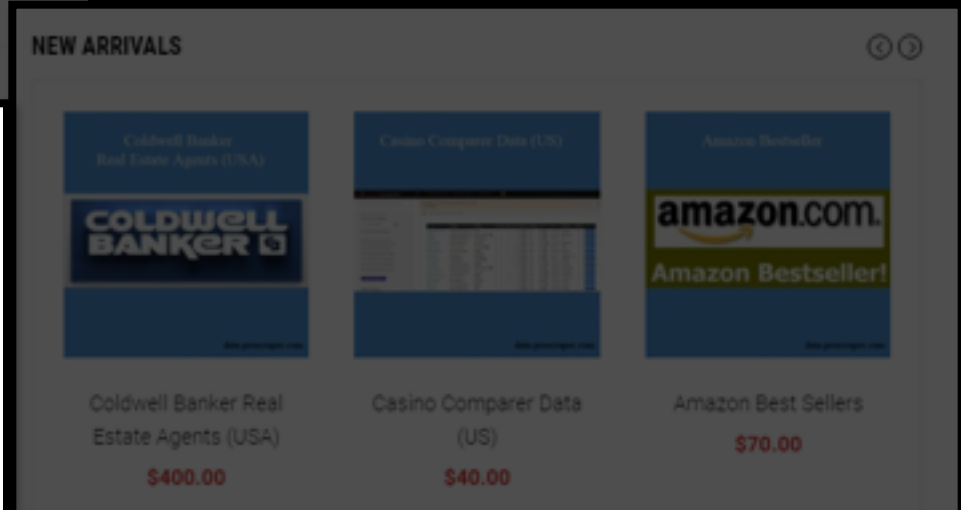
TOTAL BIDS
31

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. i would like to award this project to whoever successfully completes this phase, so when bidding please b



CLOSED

Web Scraping Bots

This project was awarded to **ASyanush** for **\$400 USD**.

Copping, Scalping and Sniping

OAT-005, OAT-013, OAT-021

| Bot Name | URL | Price | Features |
|-------------------|---|-----------------------|------------------|
| Better Nike Bot | http://www.betternikebot.com/ | 200\$ | • Captcha Solver |
| Another Nike Bot | http://www.anothernikebot.com/ | 325\$ - Basic Package | • Captcha Solver |
| Premium Nike Bot | http://www.heatedsneaks.com/store/g57/nikeBot | 49.99\$ | |
| Easy Cop Ultimate | http://www.easycopbots.com | 56\$ - Starters Kit | |
| Just Cop It Bots | https://www.justcopitbots.com/ | 200\$ | |

Shoe Size (points to 'Size Type' and 'Size' dropdowns)

Follow Twitter (points to 'Twitter Settings' section)

Nike Account (points to 'Email Address' field)

Start (points to the 'Start' button)

Twitter Settings: Twitter Account, Twitter Password, Monitor Account

Options: Size Type: All, Size: Nike US

Advanced Options: Use Old ATC Method, Link Booster

Accounts: Email Address, Keywords, Collection Keywords, Early Links

Log: 20-Mar-17 2:10:53 4:11 PM - Waiting for all accounts to log in
 20-Mar-17 2:10:53 4:14 PM - betternikebot@gmail.com: Logging in to Nike
 20-Mar-17 2:10:54 5:36 PM - betternikebot@gmail.com: Login Error! The remote server returned an error: 401 (Unauthorized)
 20-Mar-17 2:10:56 2:16 PM - Stopped by user

chrome web store search results for "sneakers bot"

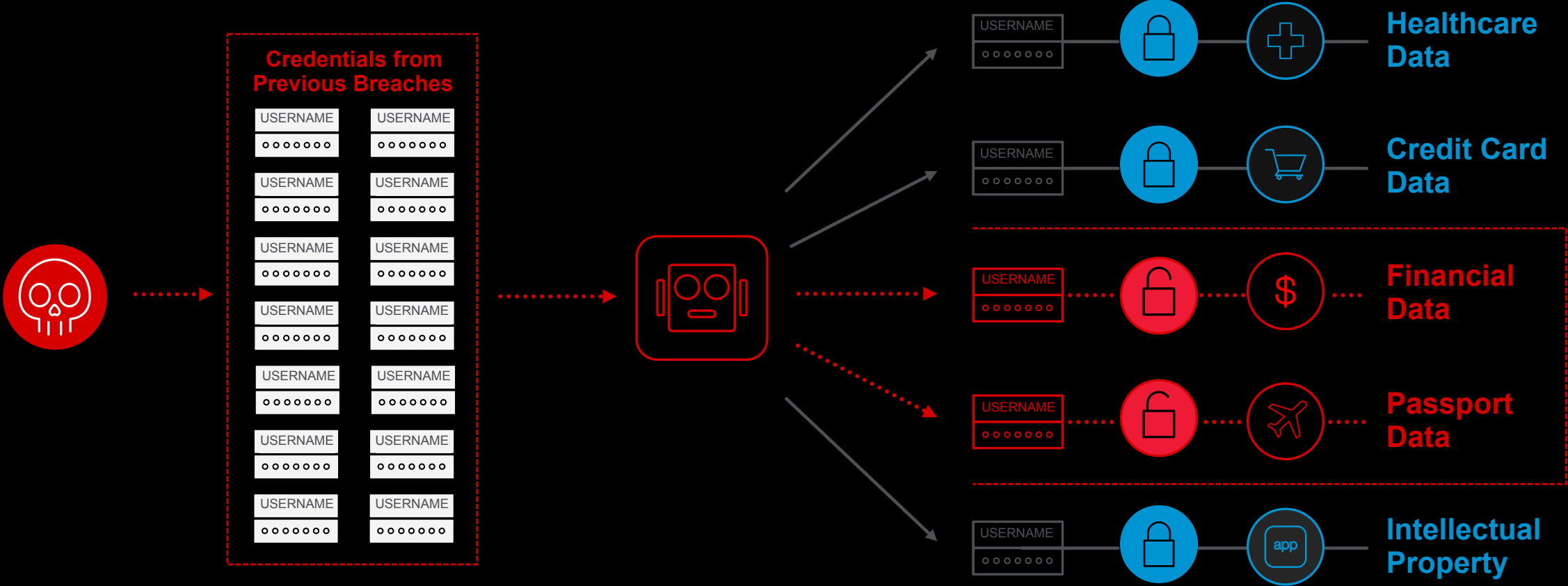
- AddToCart Nike Sneaker Bot** (ETheBusinessMan) - BUY FOR \$4.99
- NIKE SHOE BOT AUTO RETRY & TWITTER SCANNER** (offered by best-bots.com) - BUY FOR \$24.99
- AddToCart Nike 3-in-1 Sneaker Bot** (ETheBusinessMan) - BUY FOR \$5.99
- free prelink Nike shoe bot from best-bots.com** (offered by best-bots.com) - ADD TO CHROME
- The Cart Thief - Eastbay** (Hermes) - BUY FOR \$1.99

Categories: All

Features: Runs Offline, By Google, Free, Available for Android, Works with Google Drive

Ratings: 5 stars, 4 stars & up

OAT-008 Credential Stuffing



Choose Your Bot:

Sentry MBA

Run

Stop

Detection:

Selenium

Phantom

No JavaScript

Known Bot

Not Real Browser

Not Human

Human

Mitigation:

JavaScript Challenge

TCP Reset

Captcha

Blocking Page

No Mitigation

Connected (encrypted) to win-6mr1495sa5k Send CtrlAltDel

Recycle Bin

Scraper - Chrome

Default - Chrome

Mozilla Firefox

Notepad++

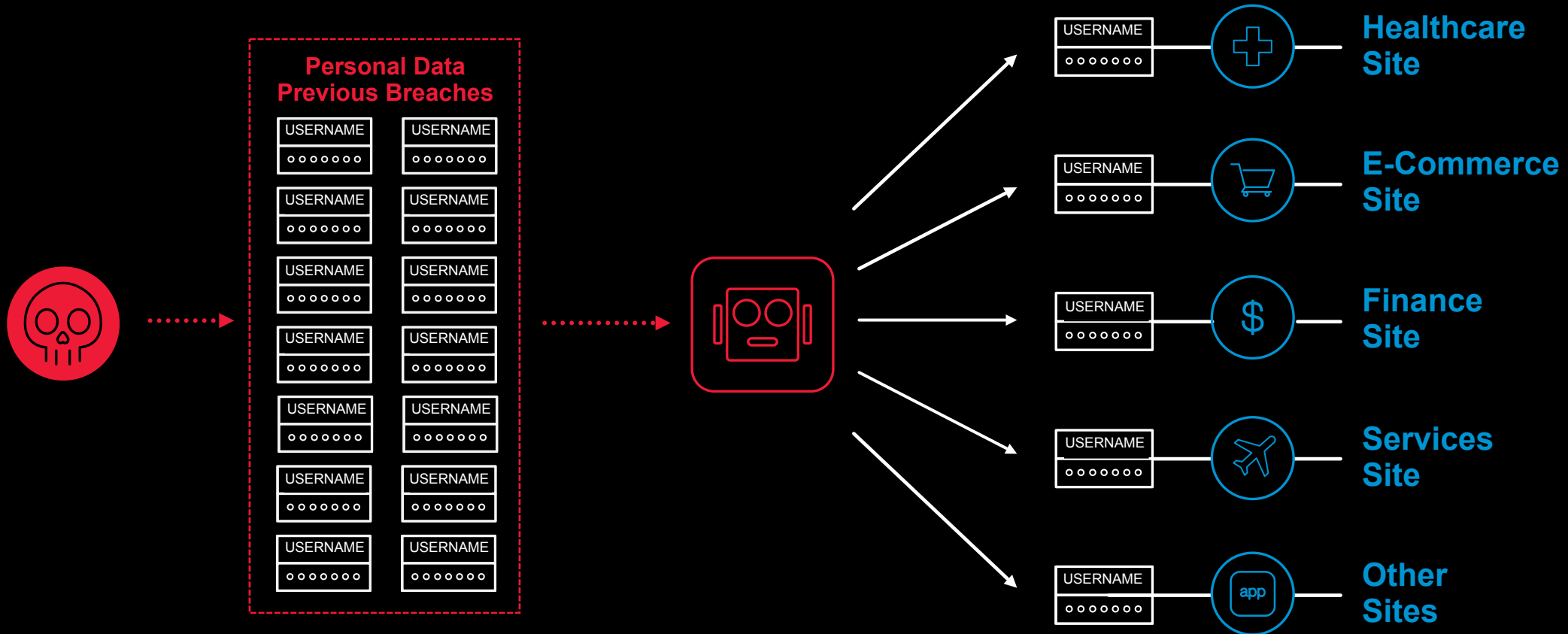
EC2 Feedback

EC2 Microsoft Windows Guide

Start

5:37 PM 7/5/2019

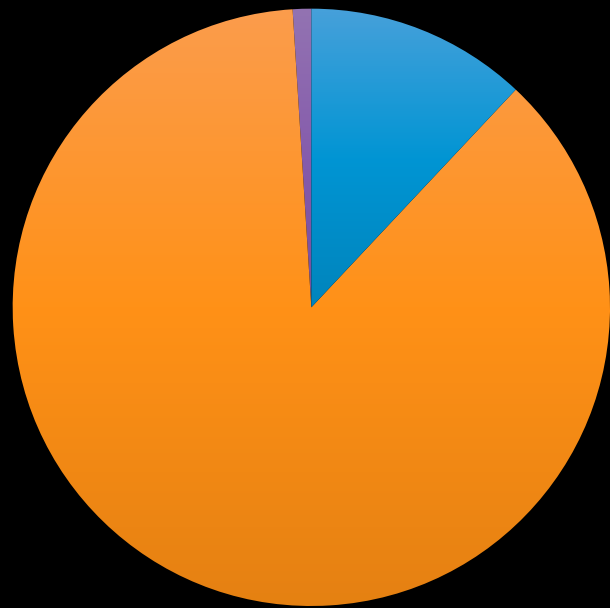
OAT-019 New Account Creation Attacks



OAT-019 New Account Creation Attacks

(FSI 2017)

Volume per Transaction Type



- Payments
- Account logins
- New account creations

Attack rate per Transaction Type



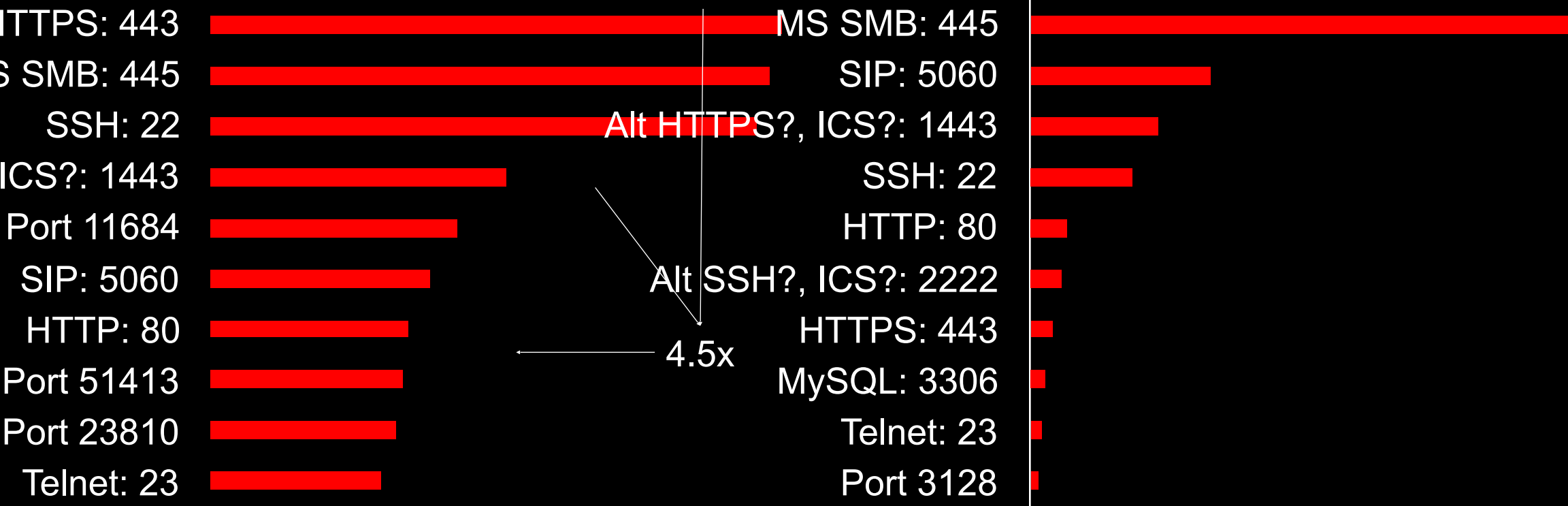
OAT-014 Scanning

Top 10 Attacked Ports Globally



2018

Q1 2019



8.4B
DEVICES

Gartner

2017

>

1T
DEVICES

SoftBank

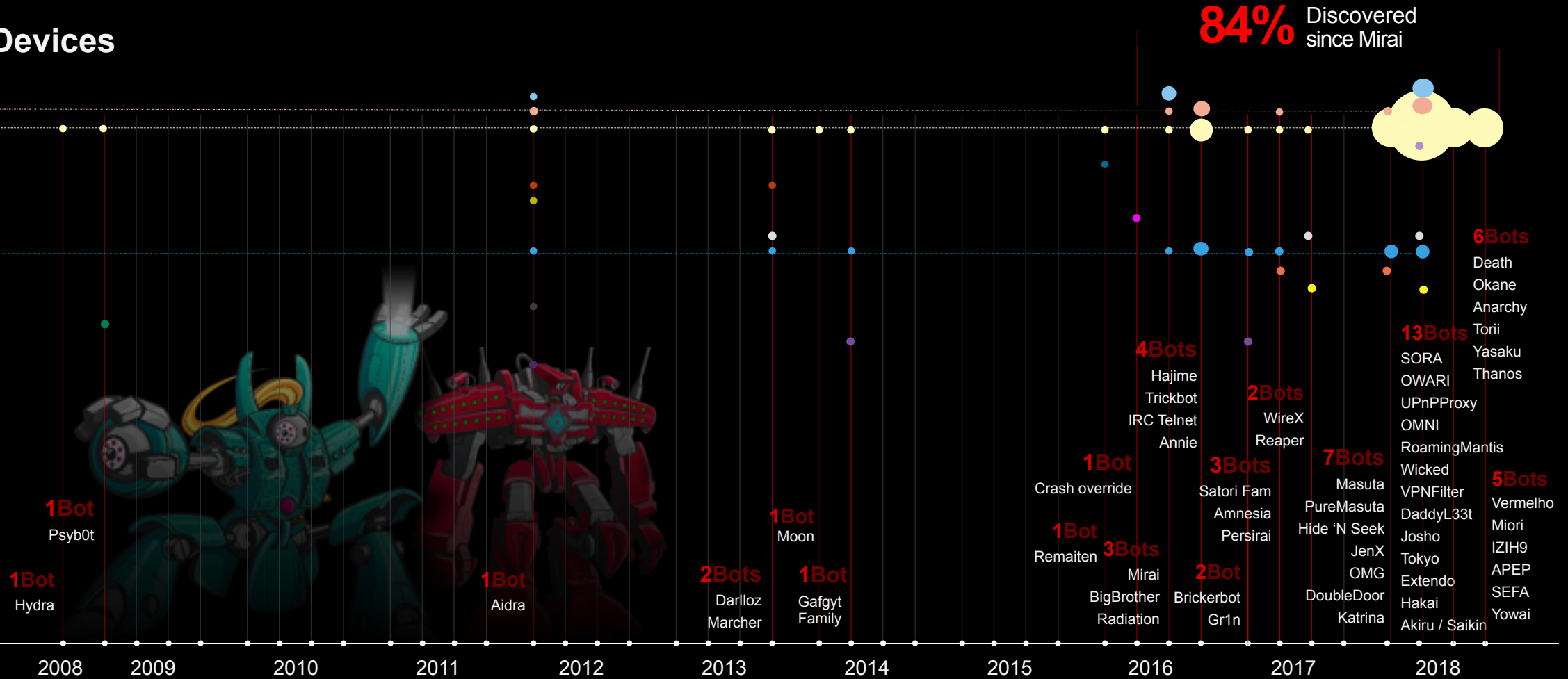
2035

**Excludes smartphones, tablets, and computers*

Thingbots

Affected Devices

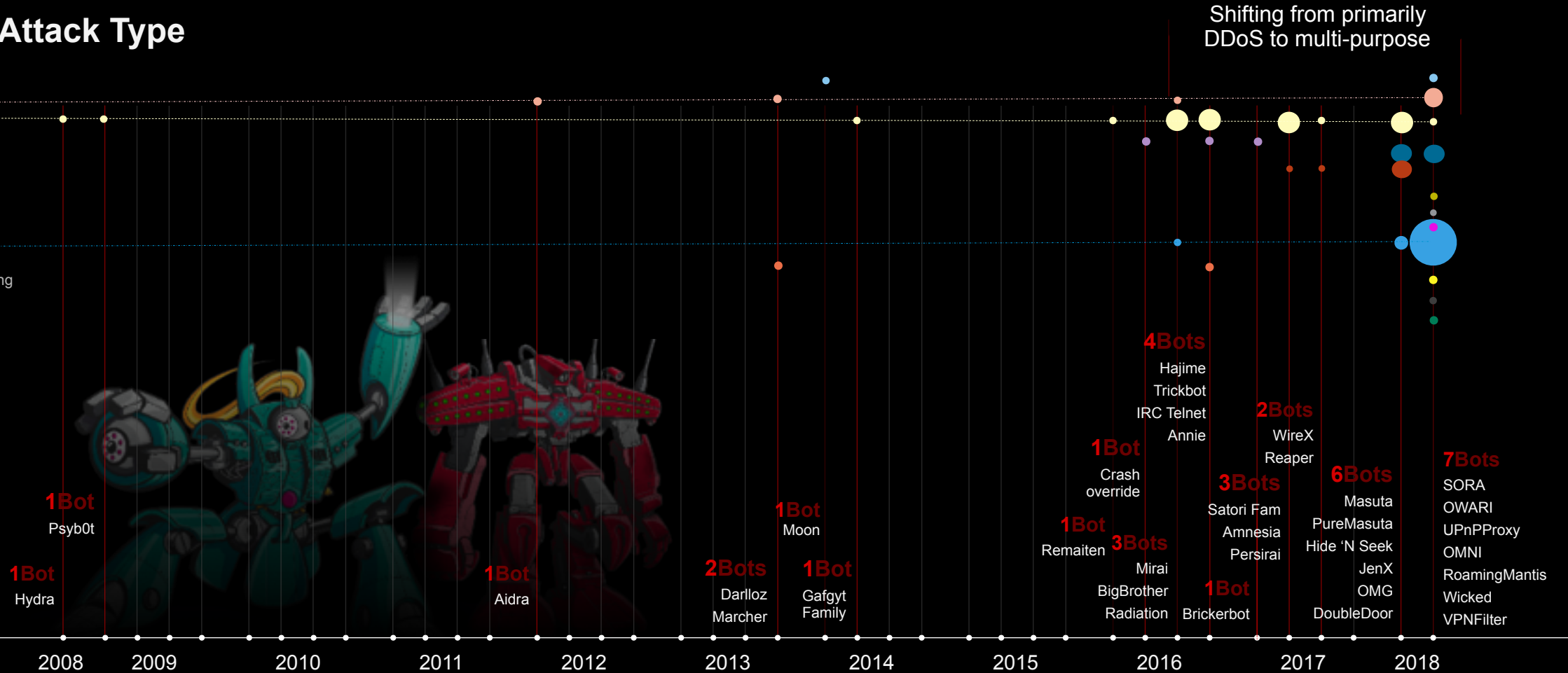
- CCTV
- DVRs
- SOHO routers
- iOS
- WAPs
- Set-Top Boxes
- Media Center
- ICS
- Android
- IP Cameras
- Wireless Chipsets
- NVR Surveillance
- VoIP Devices
- Cable Modems
- Busybox Platforms
- Smart TVs



Thingbots

Thingbot Attack Type

- 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



Mirai

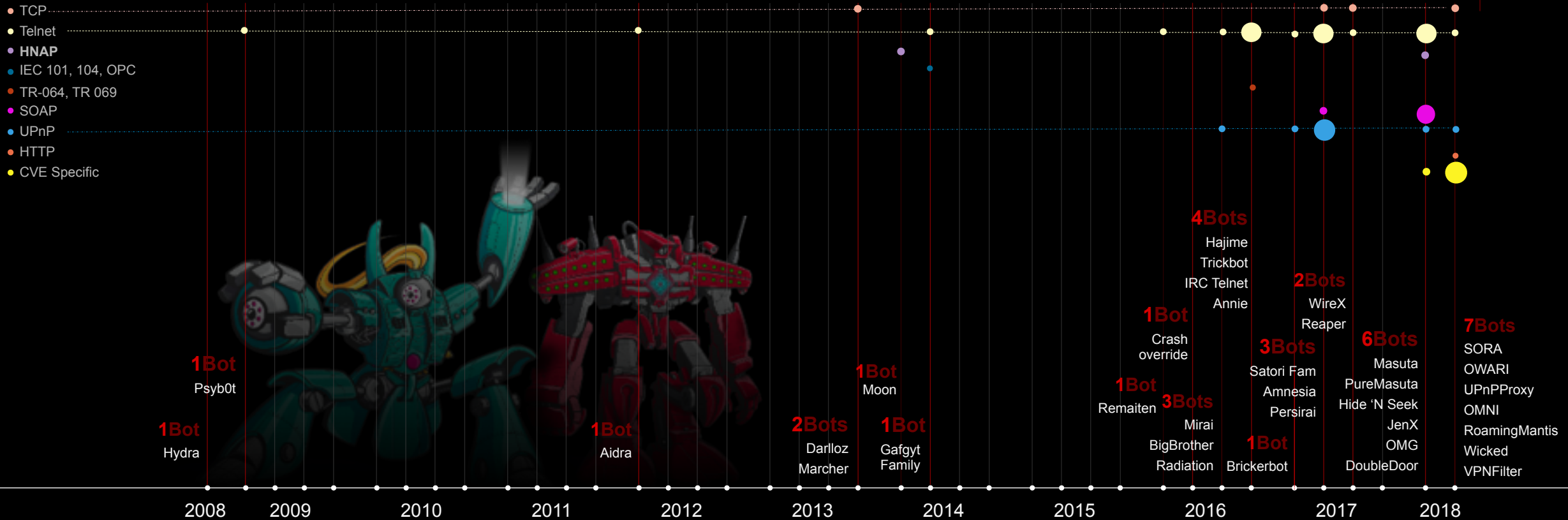
(SOHO Routers, DVRs, IP Cameras - Oct 2018)

- 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



F5 Labs discovers cellular gateway vulns



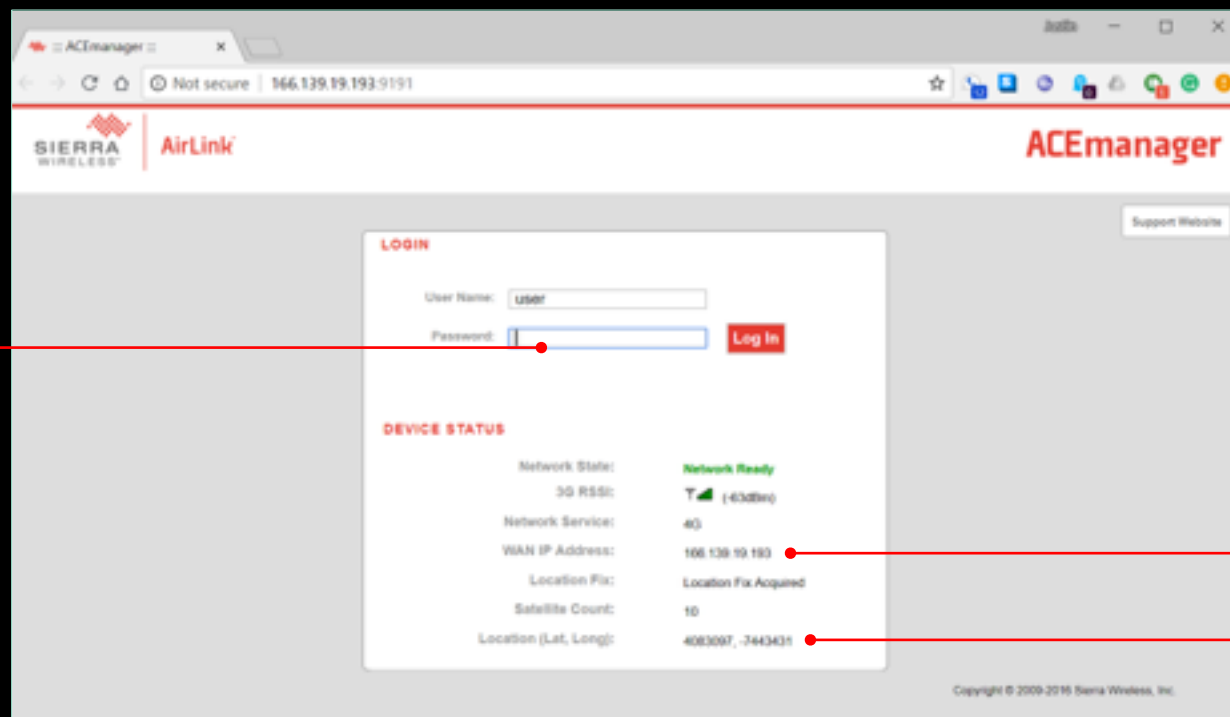
F5 Labs discovers cellular gateway vulns



SIERRA
WIRELESS®



“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

Top 100 Admin Creds Used in SSH Brute Force Attacks

H1 2019

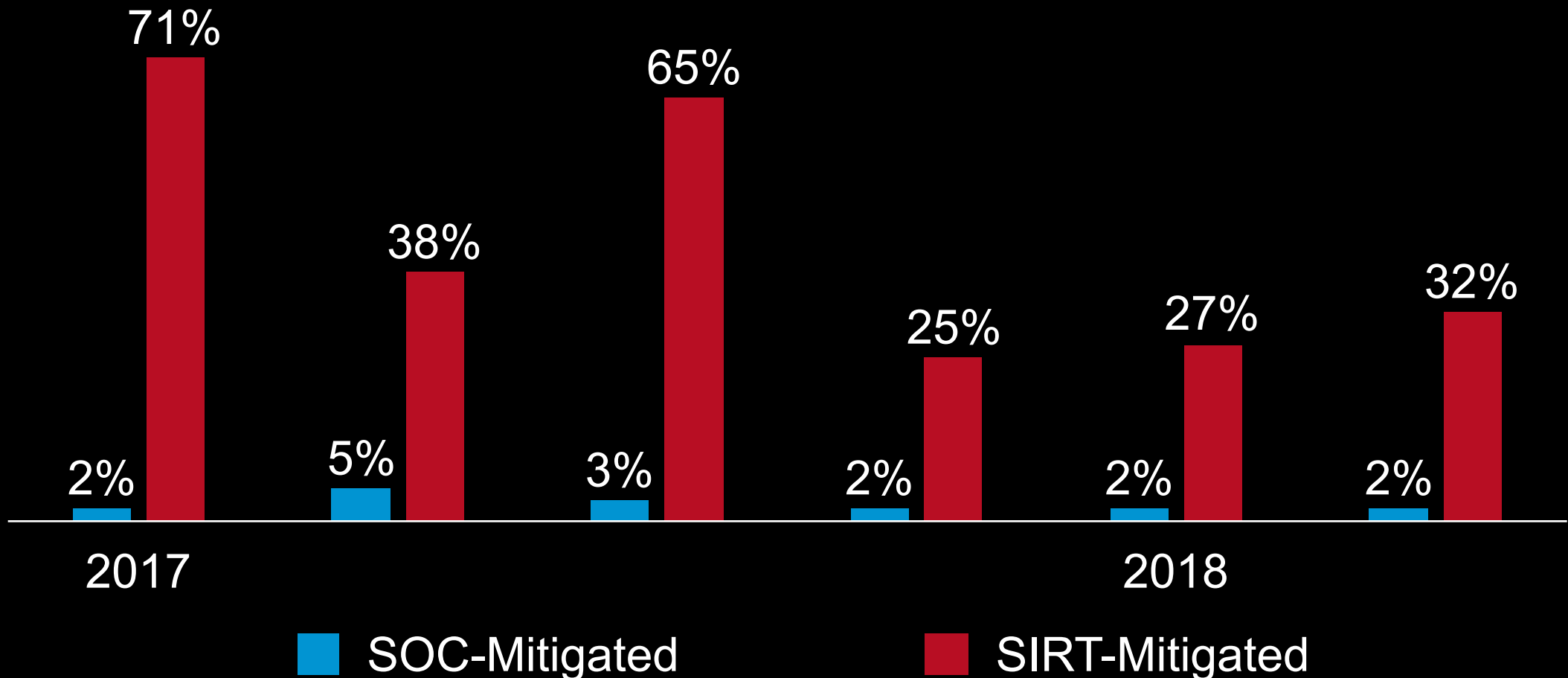
| Username | Password | Username | Password | Username | Password | Username | Password |
|-----------|-------------|---------------|---------------|------------|------------|------------|--------------|
| root | root | ts | ts | manager | manager123 | plcmSPIP | plcmSPIP |
| admin | admin | bot | bot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

Mirai Attack Types

| Attack Type | Attacks | Targets | Class |
|--------------------|----------------|----------------|--------------|
| HTTP flood | 2,736 | 1,035 | A |
| UDP-PLAIN flood | 2,542 | 1,278 | V |
| UDP flood | 2,440 | 1,479 | V |
| ACK flood | 2,173 | 875 | S |
| SYN flood | 1,935 | 764 | S |
| GRE-IP flood | 994 | 587 | A |
| ACK-STOMP flood | 830 | 359 | S |
| VSE flood | 809 | 550 | A |
| DNS flood | 417 | 173 | A |
| GRE-ETH flood | 318 | 210 | A |

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.

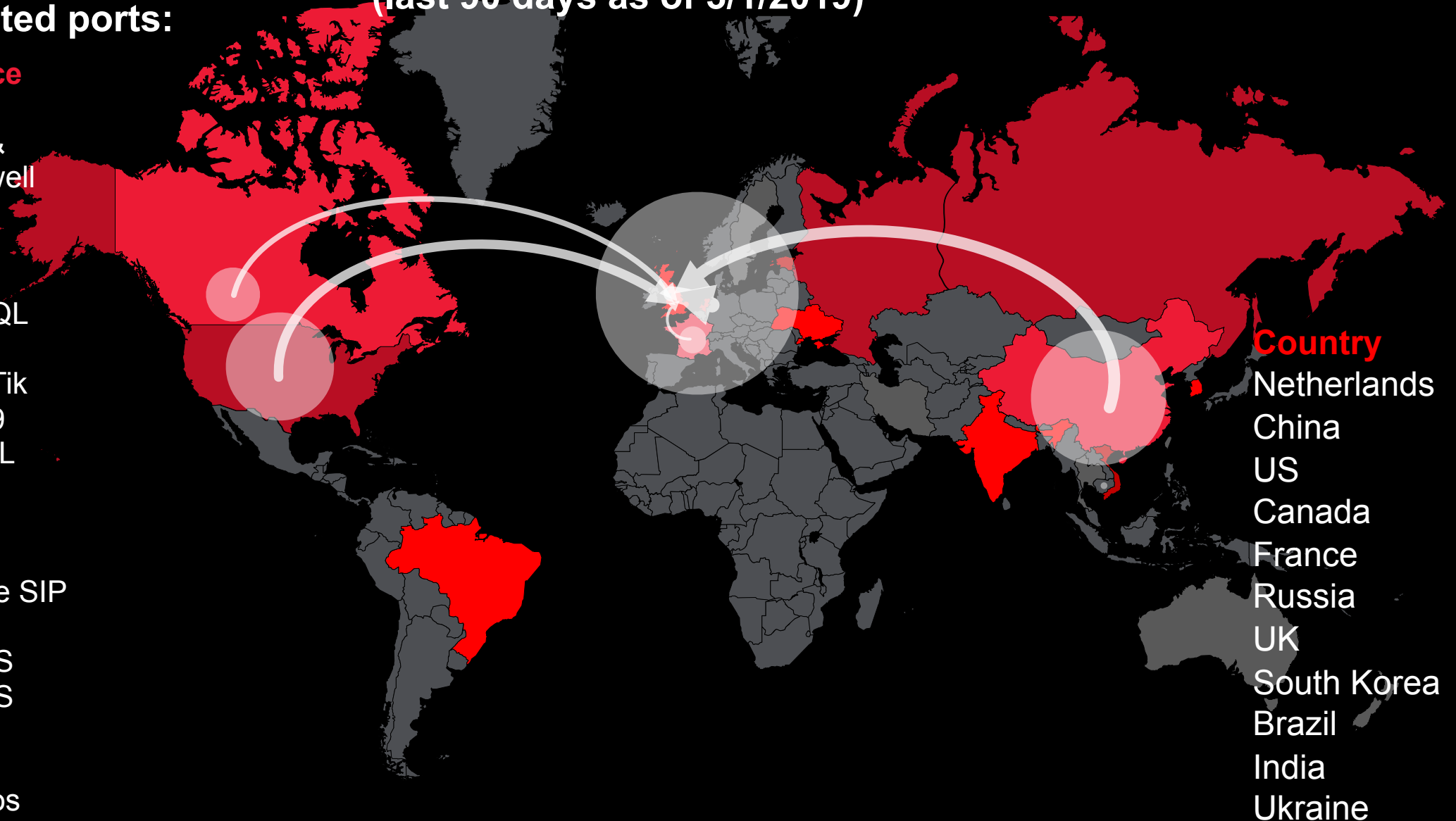


IPs Attacking UK

(last 90 days as of 3/1/2019)

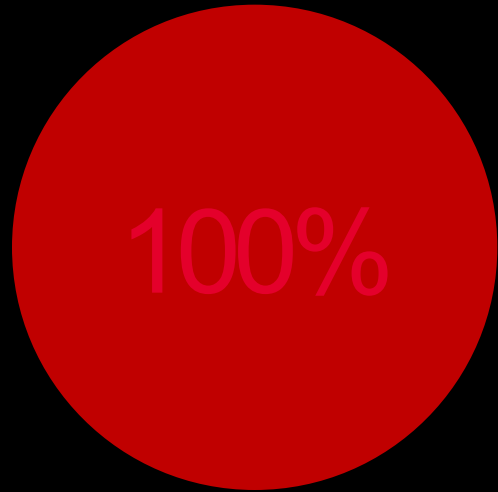
Top 20 targeted ports:

| Port | Service |
|-------|----------------|
| 5060 | SIP |
| 2222 | SSH & Rockwell |
| 22 | SSH |
| 445 | SMB |
| 80 | HTTP |
| 1433 | MS SQL |
| 23 | Telnet |
| 8291 | MikroTik |
| 7547 | TR069 |
| 3306 | MySQL |
| 25 | SMTP |
| 3389 | RDP |
| 1723 | PPTP |
| 5061 | Secure SIP |
| 61137 | |
| 4433 | HTTPS |
| 443 | HTTPS |
| 12555 | |
| 8545 | JSON |
| 139 | NetBios |

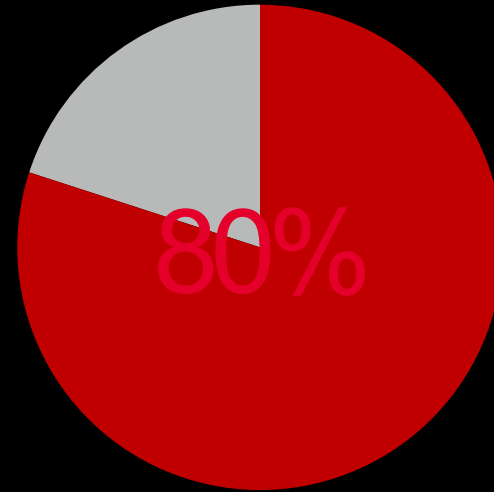


Shifting Sources

Thanks to proxies & IoT devices



Previously
unseen IP
addresses



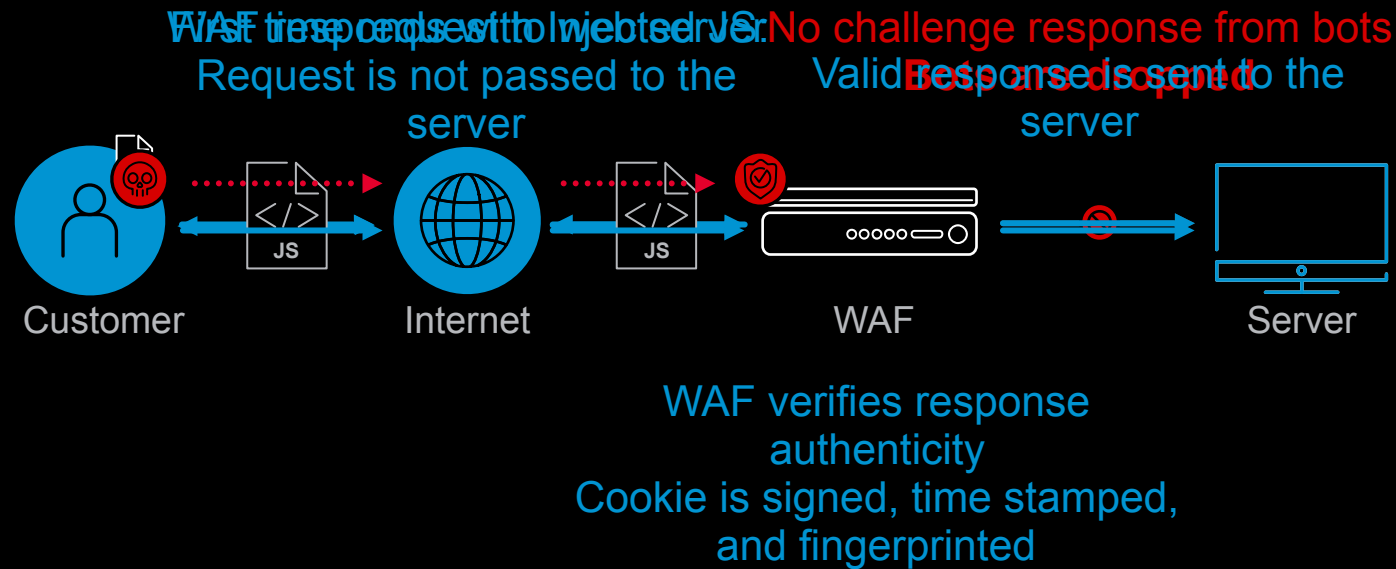
Previously
unseen
networks (ASN)

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



Headless Browsers

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

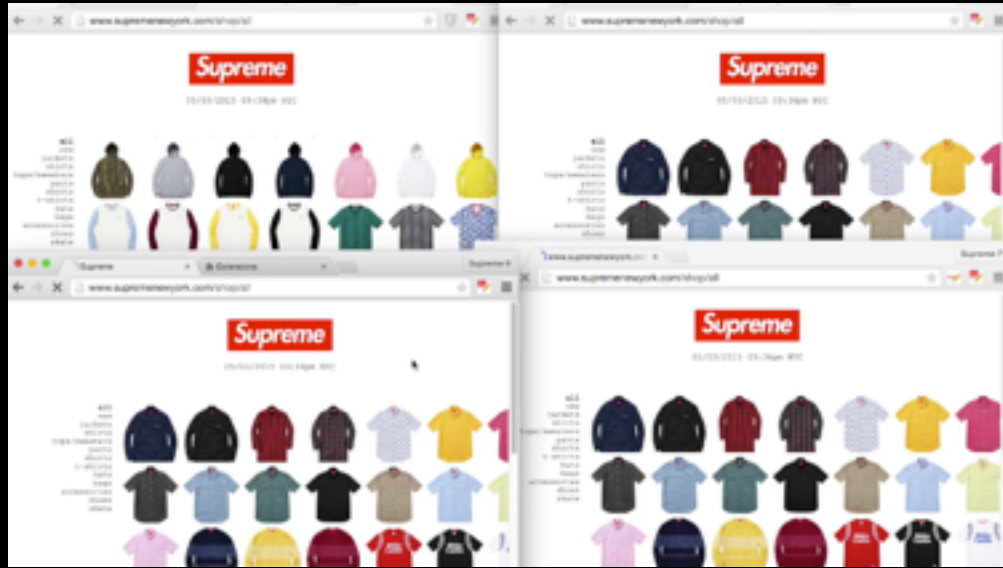
```
The --repl flag runs Headless in a mode where you can evaluate JS expressions in the browser, right from the command line:
```

```
$ chrome --headless --disable-gpu --repl --crash-dumps-dir=./tmp https://www.chromestatus.com/
[0608/112805.245285:INFO:headless_shell.cc(278)] Type a Javascript expression to evaluate or "quit" t
>>> location.href
{"result":{"type":"string","value":"https://www.chromestatus.com/features"}}
>>> quit
$
```

Headless Chrome

| Headless Browser | Website | Rendering Engine | JavaScript Engine | Common Browsers | Other Notes |
|-----------------------------|---|------------------|-------------------|-----------------|--|
| PhantomJS | http://phantomjs.org/ | QtWebKit | JavascriptCore | Safari | http://qt-project.org/wiki/QtWebKit |
| SlimerJS | http://slimerjs.org/ | Gecko | SpiderMonkey | Firefox | http://docs.slimerjs.org/0.8/differences-with-phantomjs.html https://developer.mozilla.org/en-US/docs/Mozilla/Projects/SpiderMonkey |
| Sahi | http://sahi.co.in/ | Any | Any | Any | http://sahi.co.in/w/configuring-sahi-with-xvfb |
| Google WebDriver (Selenium) | http://code.google.com/p/selenium/ | Any | Any | Any | Possibly some limitations in mobile devices (also in Sahi) |
| Zombie.js | http://zombie.labnotes.org/ | Non Standard | V8 (Node.js) | None | http://zombie.labnotes.org/guts https://github.com/aredridel/html5 https://github.com/tmpvar/jsdom |

Selenium



Grid Console v.3.0.0-beta2

DefaultRemoteProxy (version : 3.0.0-beta2)

id : http://172.29.43.203:5555, OS : WINDOWS

Browsers

Configuration

WebDriver

v:     
v:     
v:     
v:     

fb_login.py

```
1 from selenium import webdriver
2 from selenium.common.exceptions import TimeoutException
3
4 browser = webdriver.Firefox()
5 browser.get("http://www.facebook.com")
6
7 username = browser.find_element_by_id("email")
8 password = browser.find_element_by_id("password")
9 submit = browser.find_element_by_id("submit")
10
11 username.send_keys("me")
12 password.send_keys("mykewlpass")
13
14
15 submit.click()
16
17
18 wait = WebDriverWait( browser, 5 )
19
20 try:
21     page_loaded = wait.until_not(
22         lambda browser: browser.current_url == login_page
23     )
24
25 except TimeoutException:
26     self.fail( "Loading timeout expired" )
27
28     self.assertEqual(
29         browser.current_url,
30         correct_page,
31         msg = "Successful Login"
32     )
```


Scriptable Browser as-a-Service

- Detect headless browsers via extensions and browser flags

SCRAPY CLOUD PORTIA SPLASH CRAWLERA

Splash

Lightweight, scriptable browser as a service



Splash is a lightweight, scriptable headless browser with an HTTP API. It is used to:

- Properly render web pages that use JavaScript
- Interact with them
- Get detailed information about requests/responses initiated by a web page
- Apply Adblock Plus filters
- Take screenshots of the crawled websites as they are seen in a browser

Pricing

We offer hosted Splash instances in 3 sizes:

| | SMALL | MEDIUM | LARGE | ENTERPRISE |
|------------------|------------|------------|-------------|------------|
| PRICE | \$25/month | \$50/month | \$100/month | Custom |
| CPU | 1x | 2x | 4x | Custom |
| RAM | 1.25GB | 2.5GB | 5GB | Custom |
| PRIORITY SUPPORT | - | - | - | ✓ |

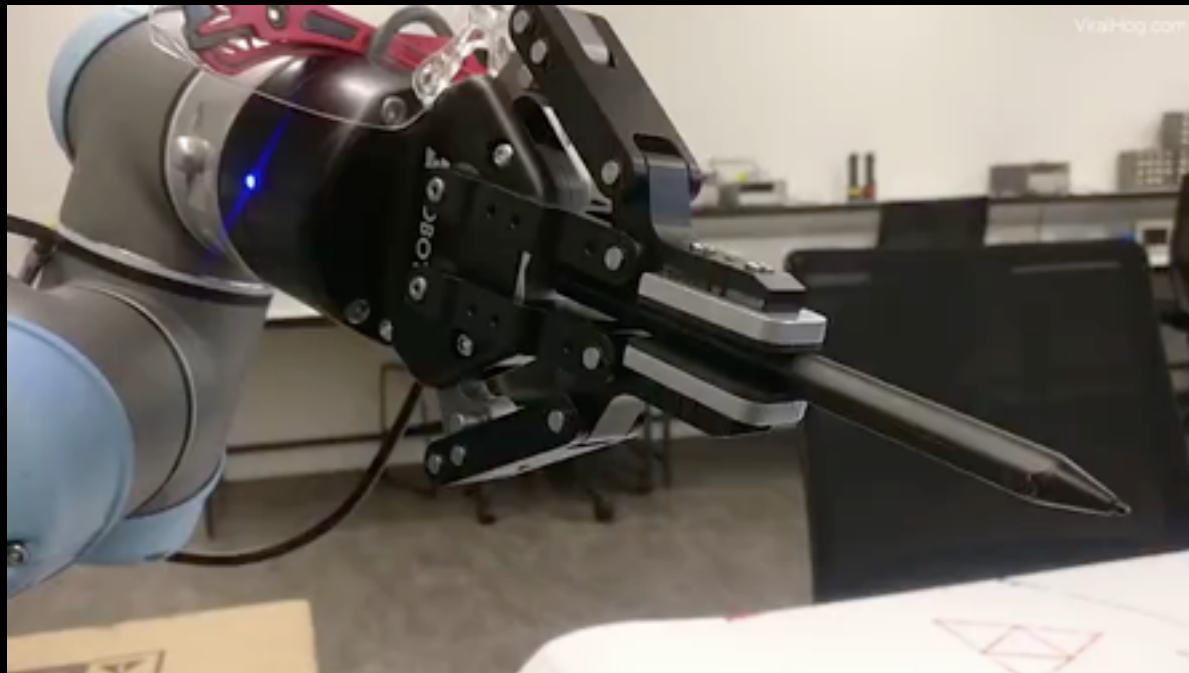
CAPTCHA



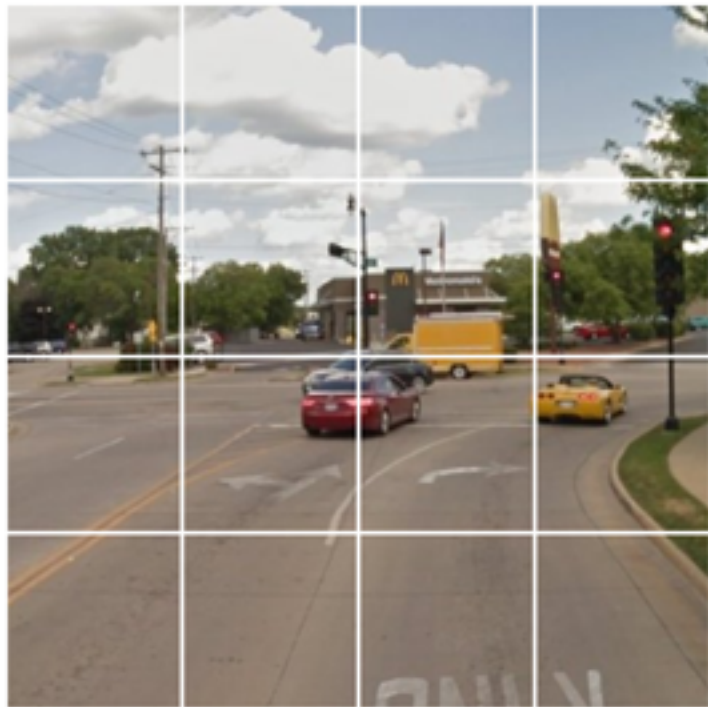
morning overtook

Type the two words:

reCAPTCHA™
stop spam,
read books.



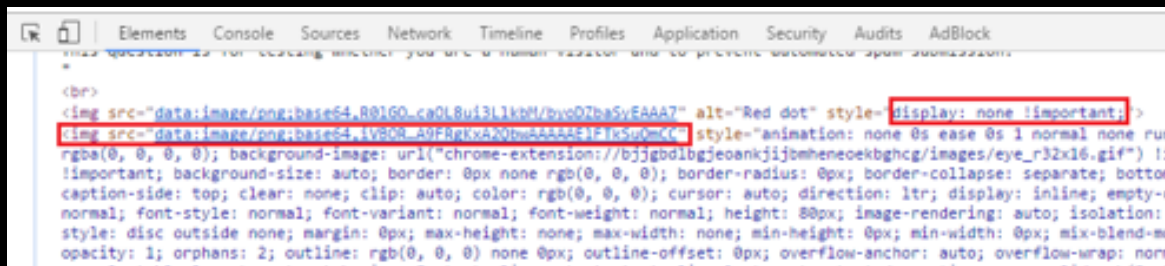
Select all squares with
traffic lights
If there are none, click skip



⌂ 🎧 👤 ✓ SKIP

CAPTCHA Solvers – Browser Extensions

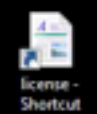
Rumola



AntiCaptcha



- Detect CAPTCHA extensions based on HTML insertion



2CapBot_v1.5.2

Organize Open Share with Burn New folder

Search 2CapBot_v1.5.2

| Name | Date modified | Type | Size |
|----------------------|-------------------|-----------------------|----------|
| bin | 5/20/2017 6:31 AM | File folder | |
| 2CaptchaBot | 5/20/2017 6:31 AM | Application | 347 KB |
| GeckoFx-Core.dll | 5/20/2017 6:31 AM | Application extens... | 1,285 KB |
| GeckoFx-Winforms.dll | 5/20/2017 6:31 AM | Application extens... | 134 KB |

2CaptchaBot

2Captcha

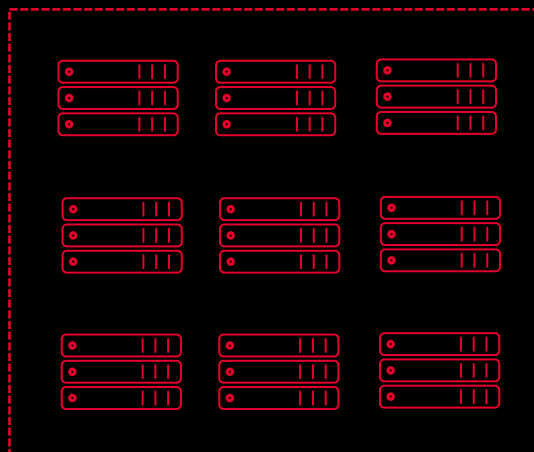
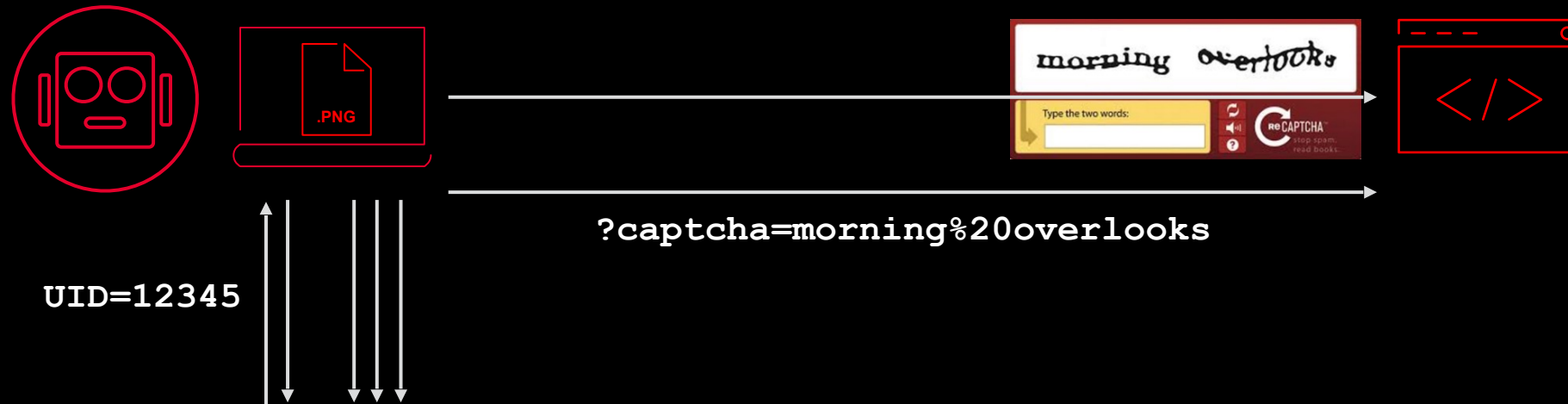
English

Start

2CaptchaBot Date modified: 5/20/2017 6:31 AM Date created: 3/30/2017 4:42 PM
Application Size: 347 KB

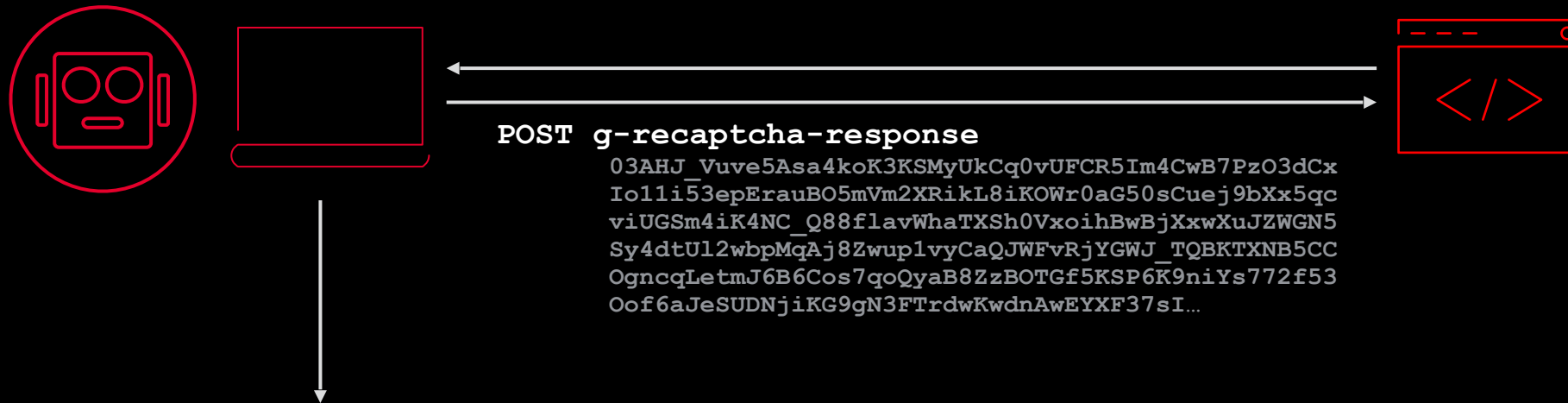


Automated CAPTCHA Solvers



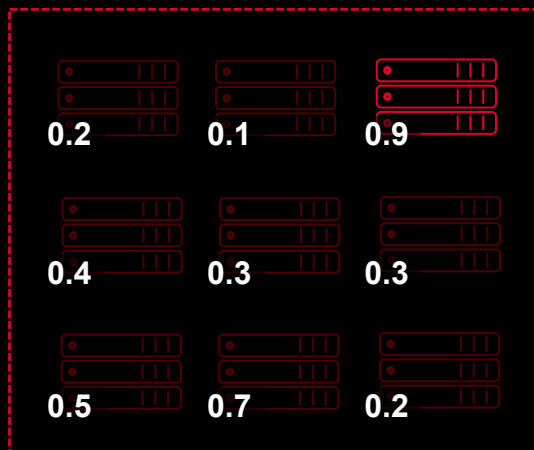
- Bot detects that a CAPTCHA is existing on the page
- Bot saves CAPTCHA into an image file
- Bot uploads the saved image file to the solver servers
- The solver will respond with a CAPTCHA ID
- Bot polls the solver API using the CAPTCHA ID it received until the status of the CAPTCHA id is changed to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

ReCaptcha v3 Solvers



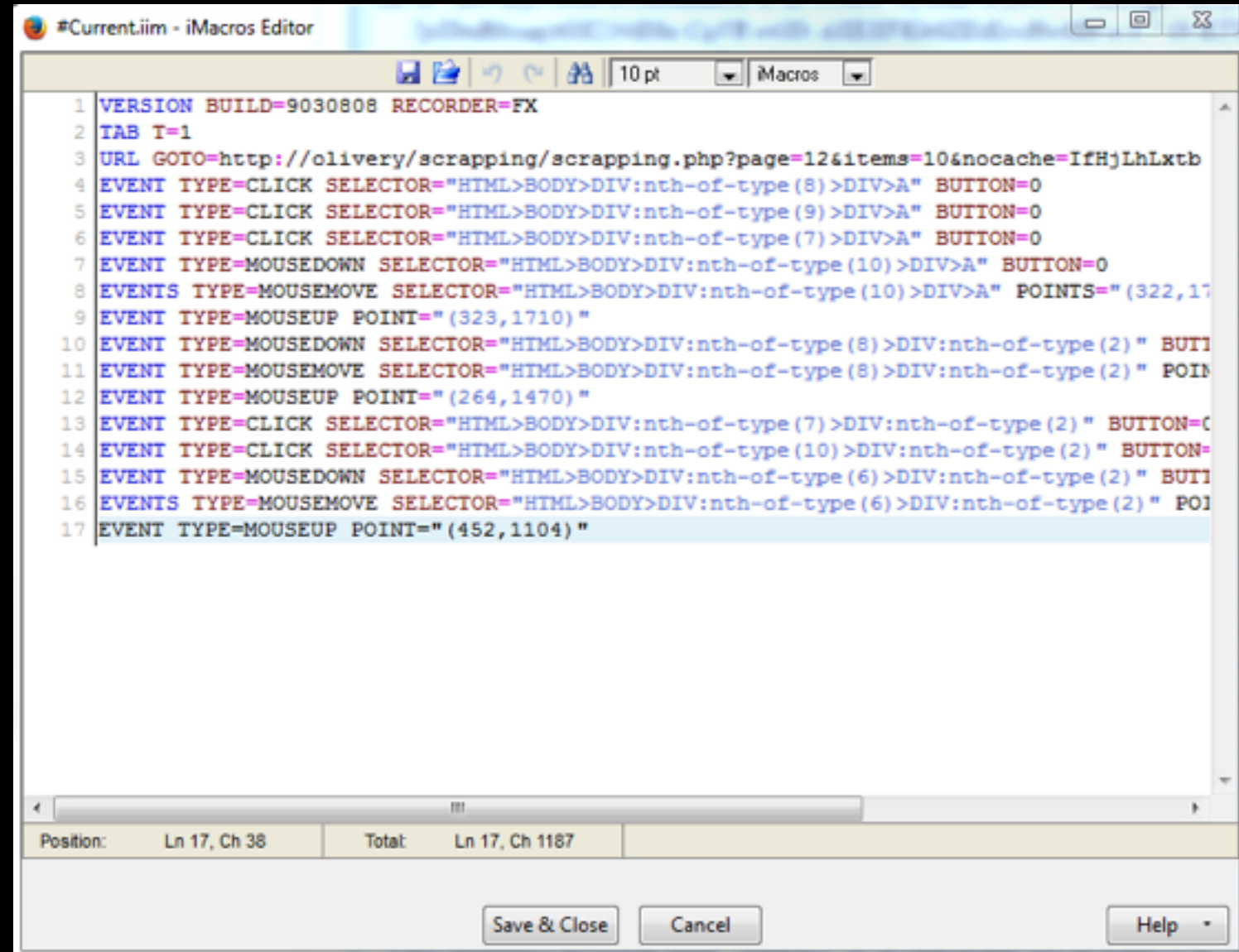
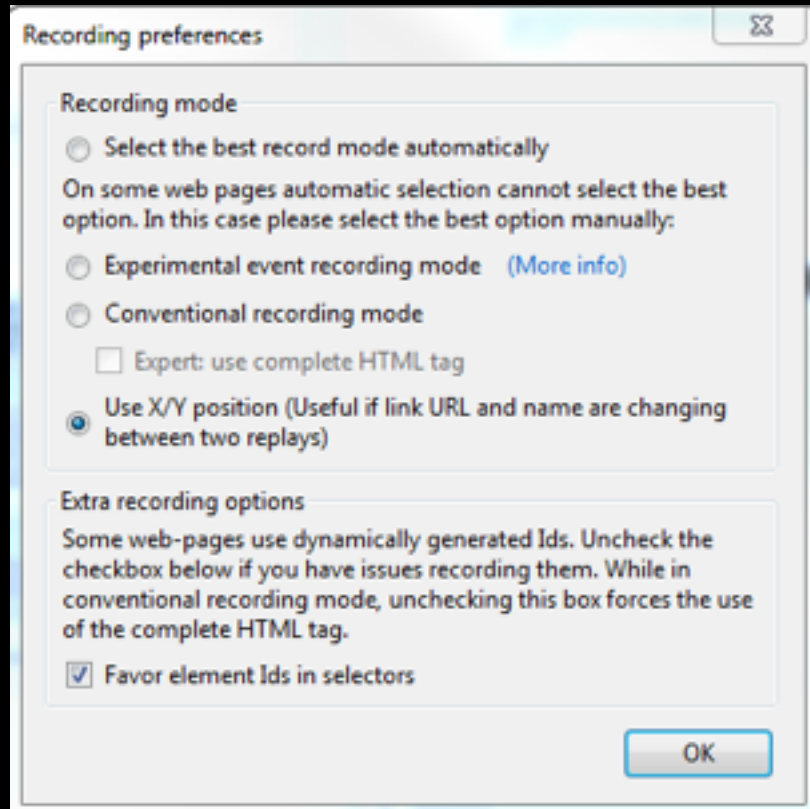
POST g-recaptcha-response

```
03AHJ_Vuve5Asa4koK3KSMYUkCq0vUFcR5Im4CwB7PzO3dCx  
Io11i53epEraUBO5mVm2XRikL8iKOWr0aG50sCuej9bXx5qc  
viUGSm4iK4NC_Q88flavWhaTXSh0VxoihBwBjXxwXuJZWGN5  
Sy4dtU12wbpMqAj8Zwup1vyCaQJWFvRjYGWJ_TQBKTXNB5CC  
OgncqLetmJ6B6Cos7qoQyaB8ZzBOTGf5KSP6K9niYs772f53  
Oof6aJeSUDNjiKG9gN3FTrdwKwdnAwEYXF37sI...
```



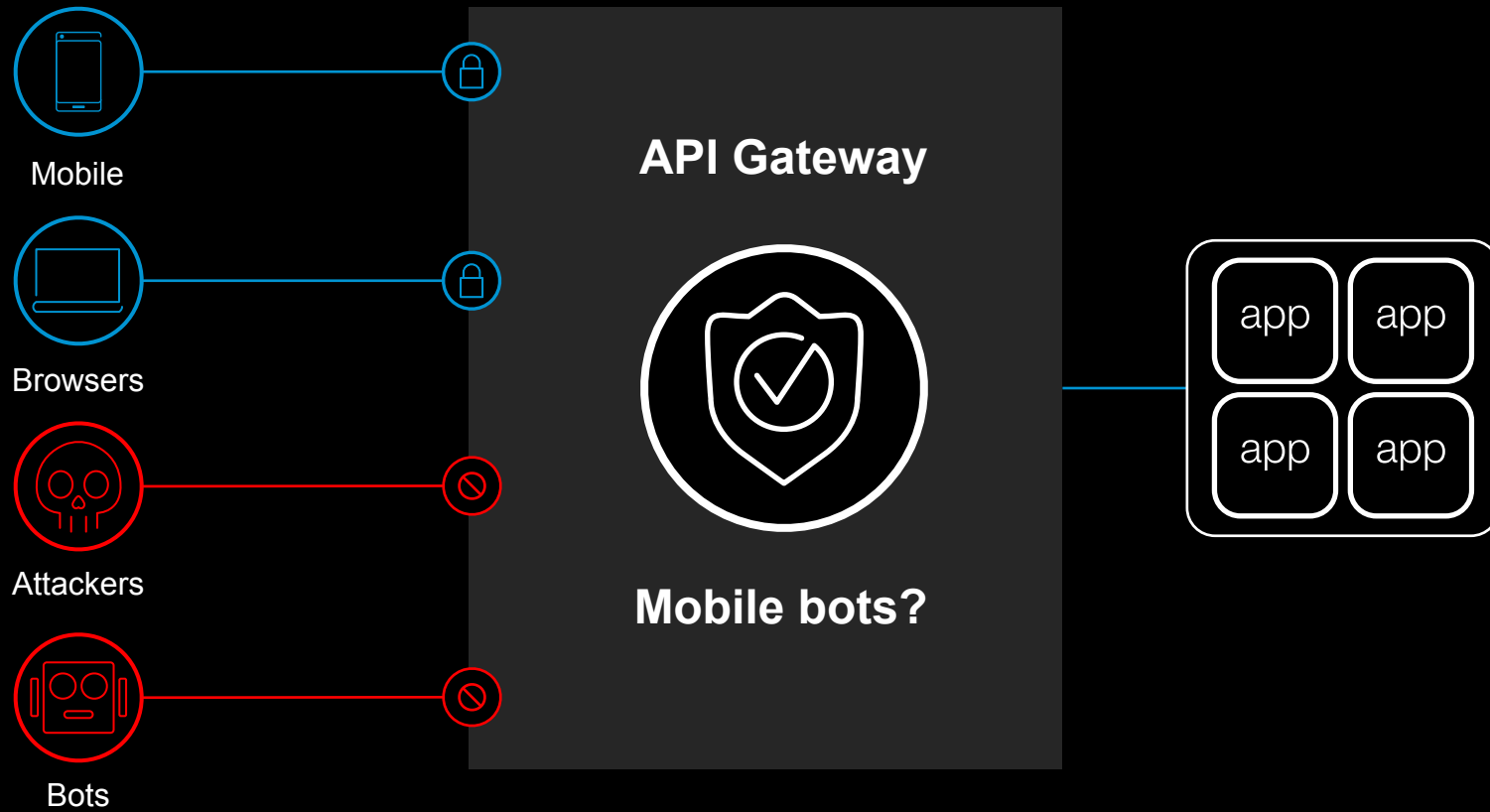
- ReCaptcha v3 uses 'scores' from 0.1 to 0.9 to rate the client
- Typically, a user score will be the same/similar across sites
- ReCaptcha v3 solver monitors scores of workers
- Selected the worker with the highest score to solve the Captcha

Simulated Mouse Events

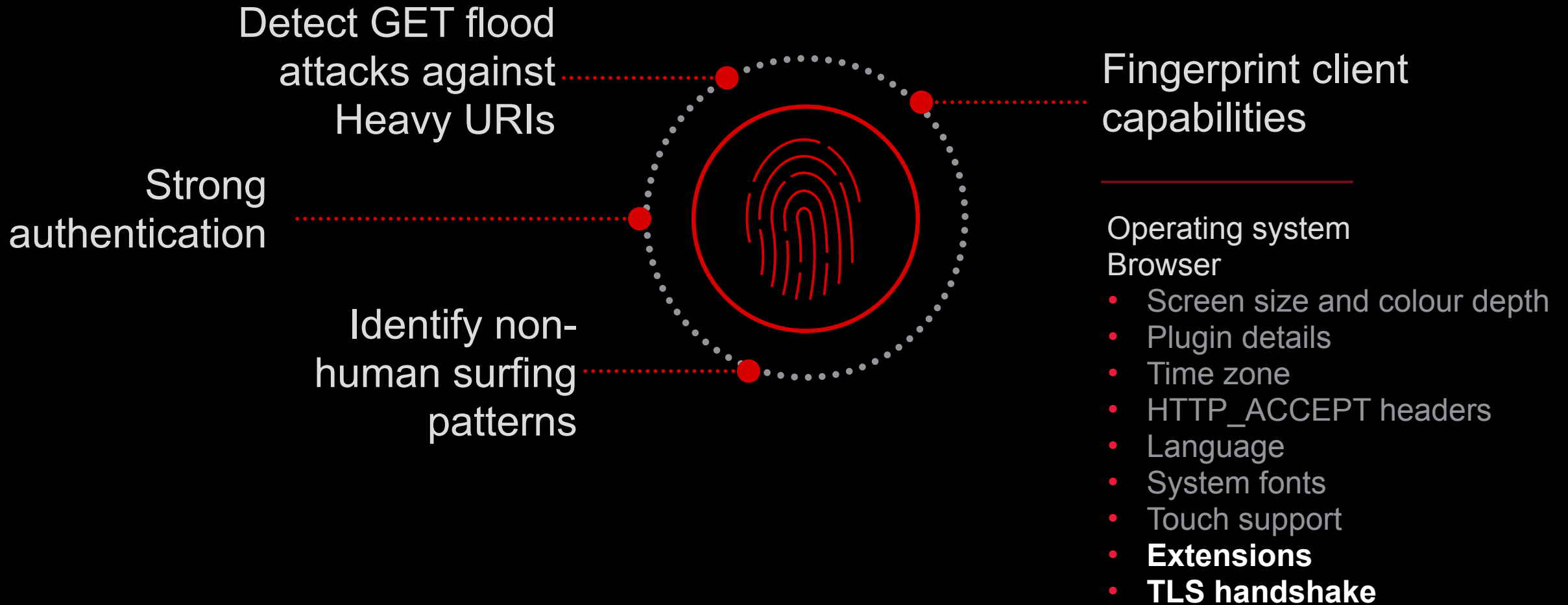


- Fake mouse movements can lack cursor positioning

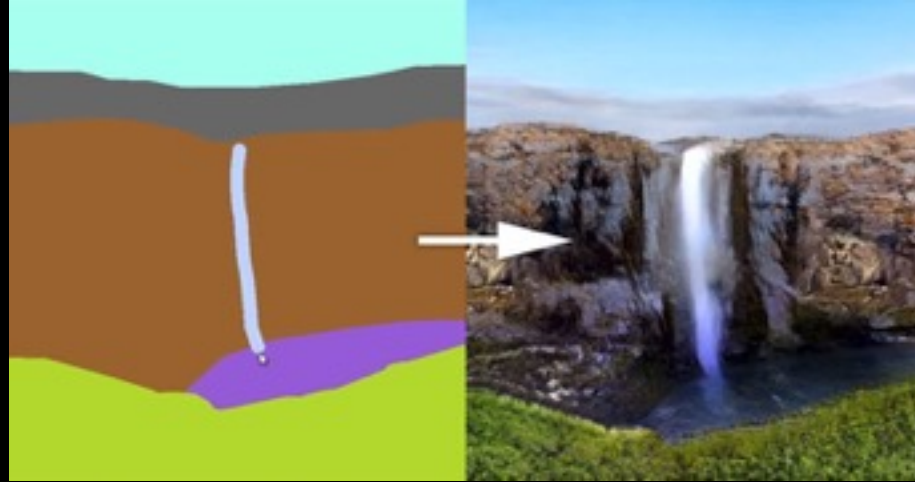
Bots Attacking Mobile APIs



Behavioural Analysis and Fingerprinting



AI and Future Bots



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.



