OWASP London
July 2019

Advanced Bots and Security Evasion Techniques

PRESENTED BY:

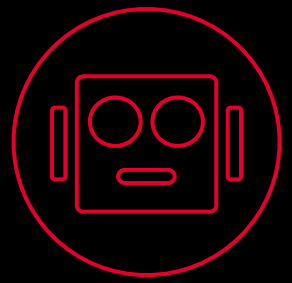
David Warburton, Snr Threat Research Evangelist
F5 Labs

Who Am I?

David Warburton

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

@warburtr0n

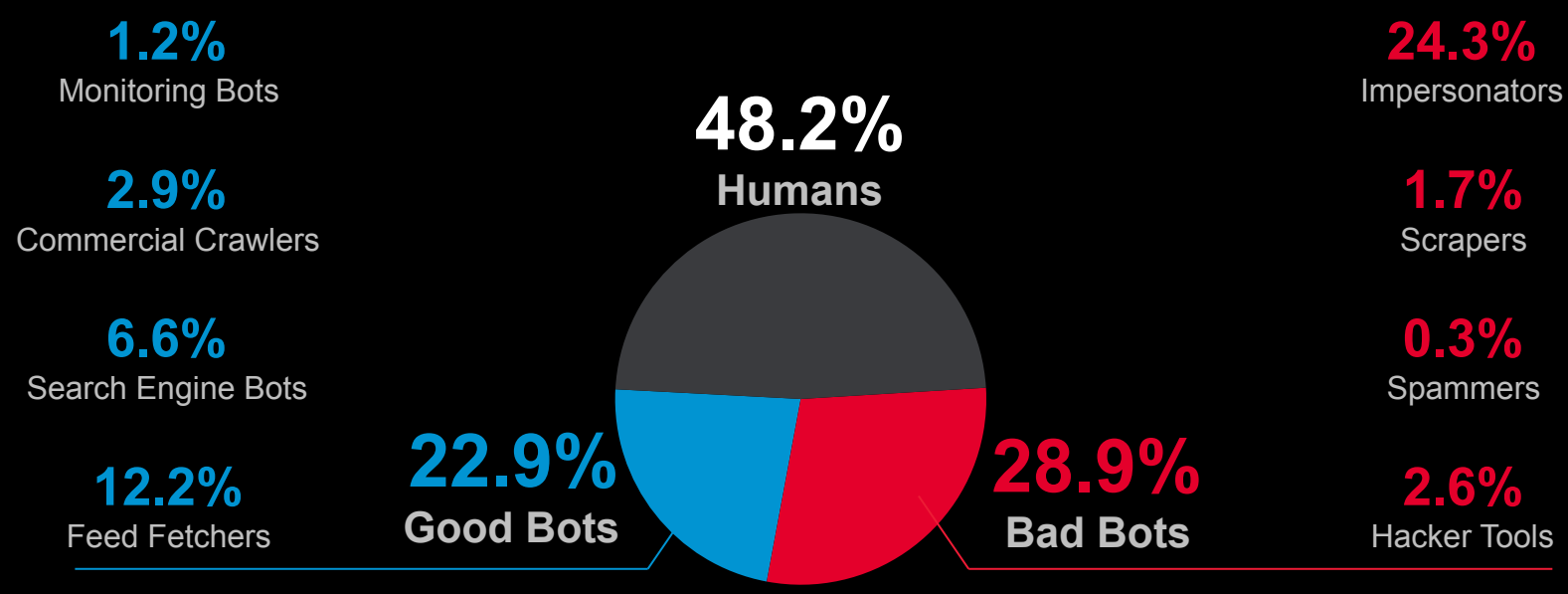


What are bots?

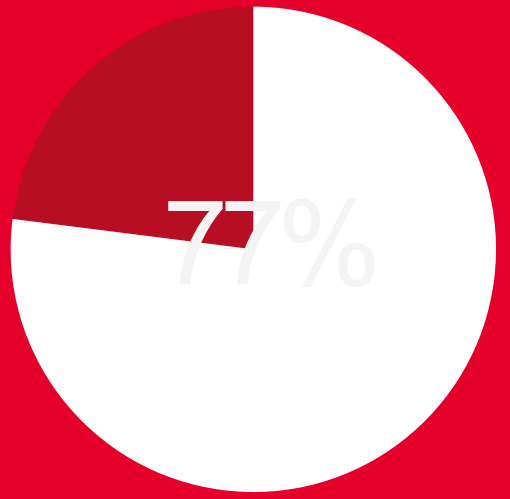
Advanced Bot Techniques

Detecting and mitigating Bots

Bot Breakdown



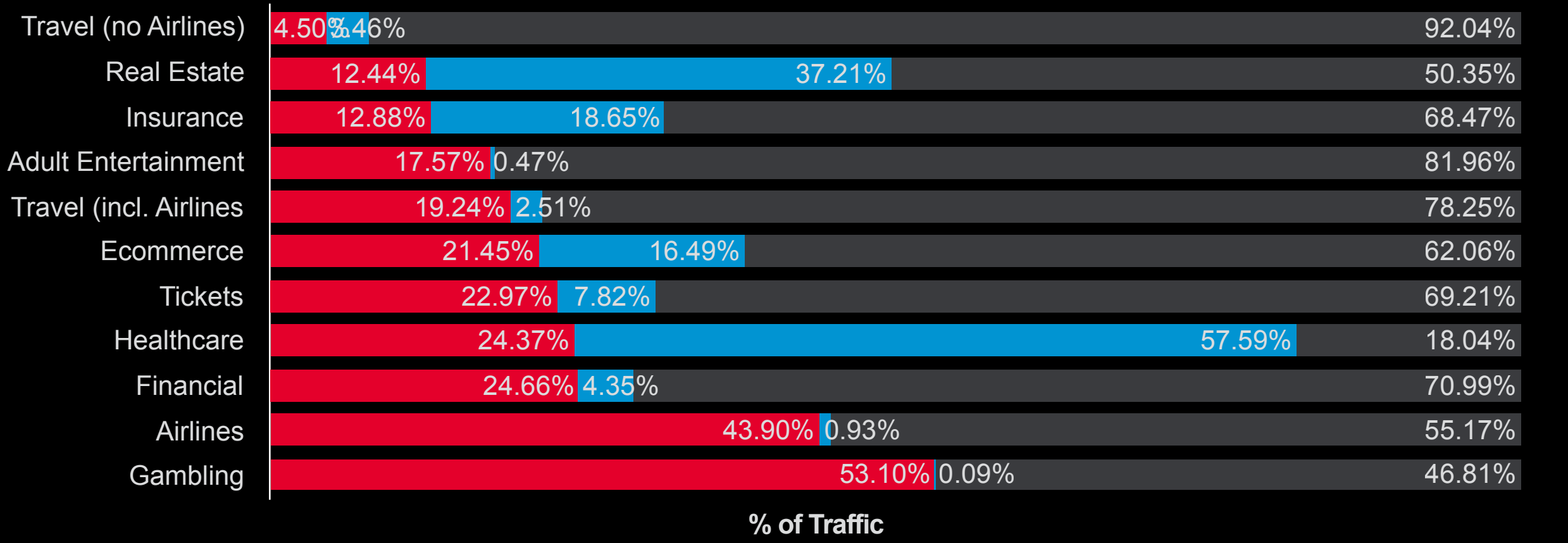
Source: GlobalDots Bot Report



Web app attacks started with botnets

Source: Verizon

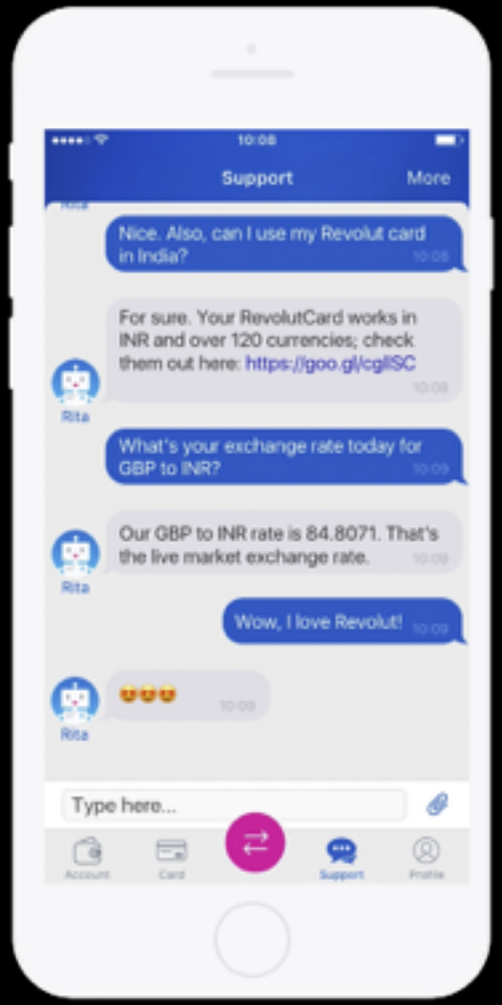
Bots by Industry

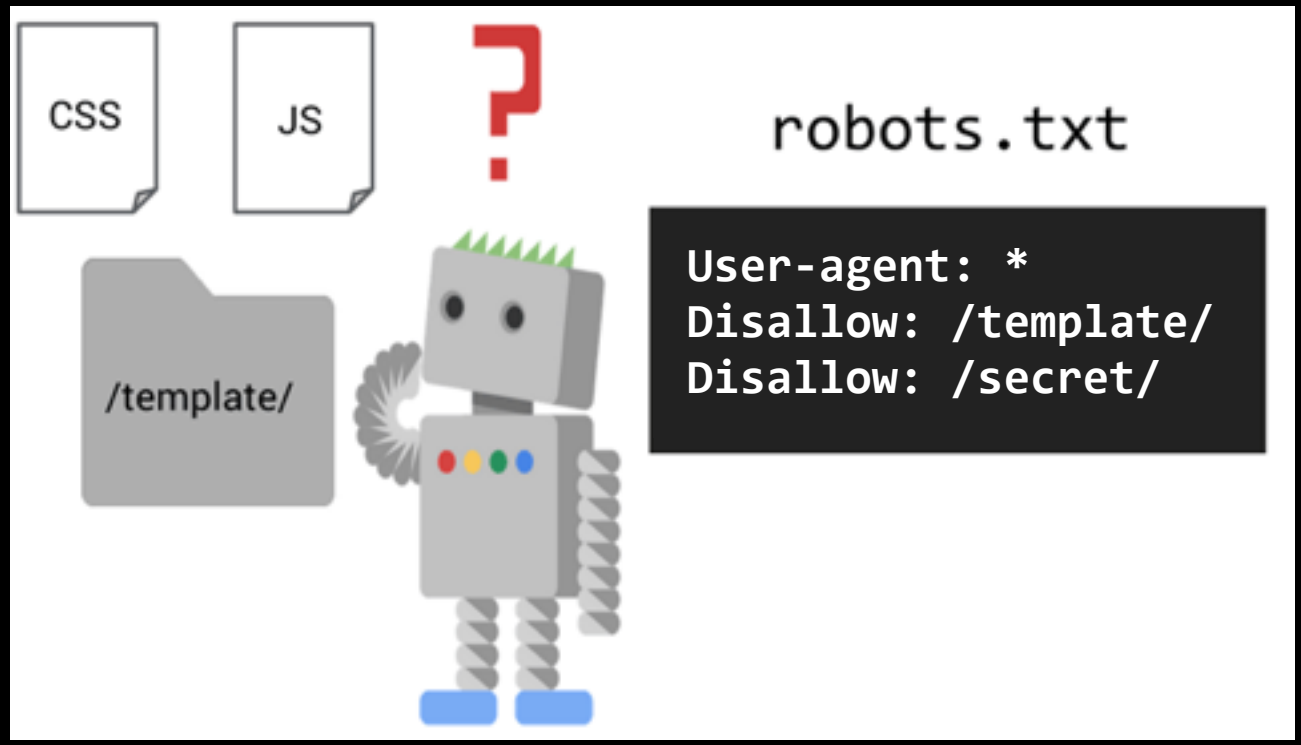


Source: GlobalDots Bad Bot Report 2018

- 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


10:08
Support
More
Nice. Also, can I use my Revolut card in India?
For sure. Your RevolutCard works in INR and over 120 currencies; check them out here: https://goo.gl/cgIlSC
Rita
What's your exchange rate today for GBP to INR?
Our GBP to INR rate is 84.8071. That's the live market exchange rate.
Rita
Wow, I love Revolut!
Rita
Type here...
Account
Card
Support
Profile


CSS
JS
?
/template/
robots.txt
User-agent: *
Disallow: /template/
Disallow: /secret/

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

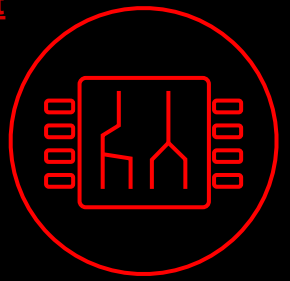
OAT-011 Scraping

Payment Card Data

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

Other Attacks

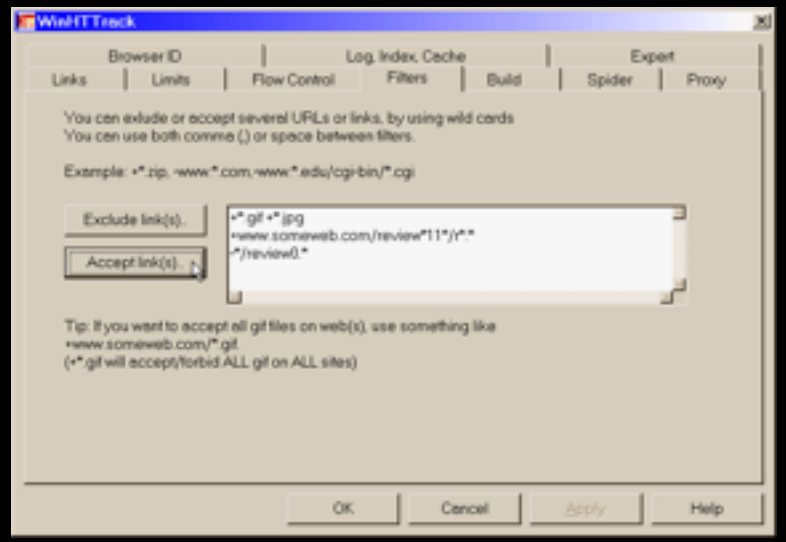
OAT-003 Ad Fraud
OAT-009 CAPTCHA Defeat
OAT-016 Skewing
OAT-017 Spamming
OAT-002 Token Cracking

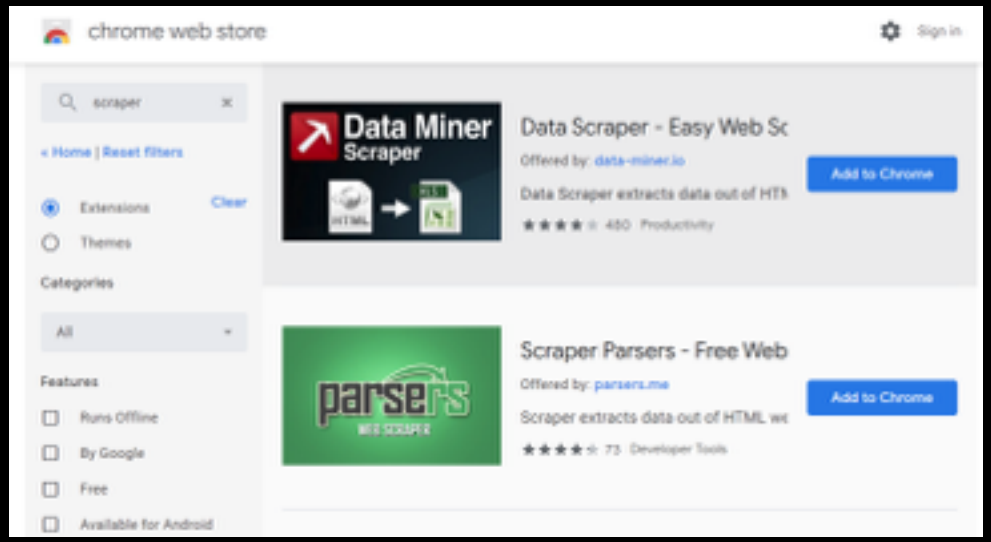


Vulnerability Scanning

OAT-014 Vulnerability Scanning
OAT-004 Fingerprinting
OAT-018 Footprinting

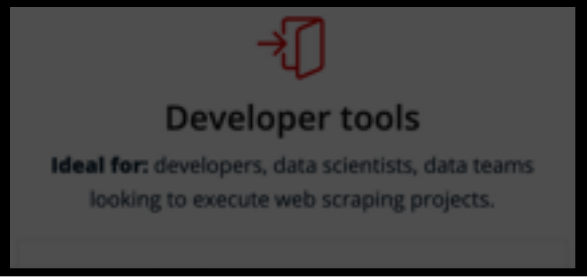
OAT-011 Scraping

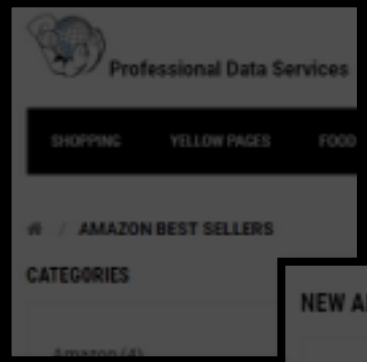





```
 def create_json_oneway(self, dump_list):
        for i in range(len(dump_list)):
            temp = '{ "airline" : "' + dump_list[i]['le'][0]['an'] + '"'
            temp = temp + ', "price" : "' + str(dump_list[i]['af']) + '"'
            temp = temp + ', "total_time" : "' + str(dump_list[i]['td'])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





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
is to award this project to whoever successfully completes this phase, so when bidding please b

CLOSED

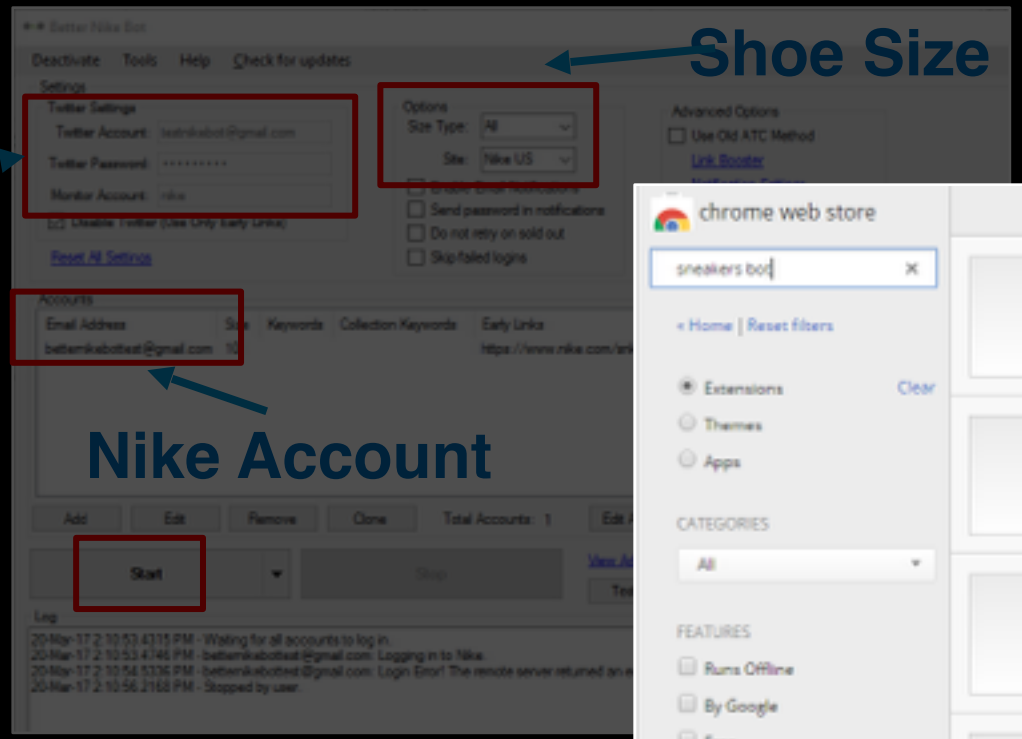
Web Scraping Bots

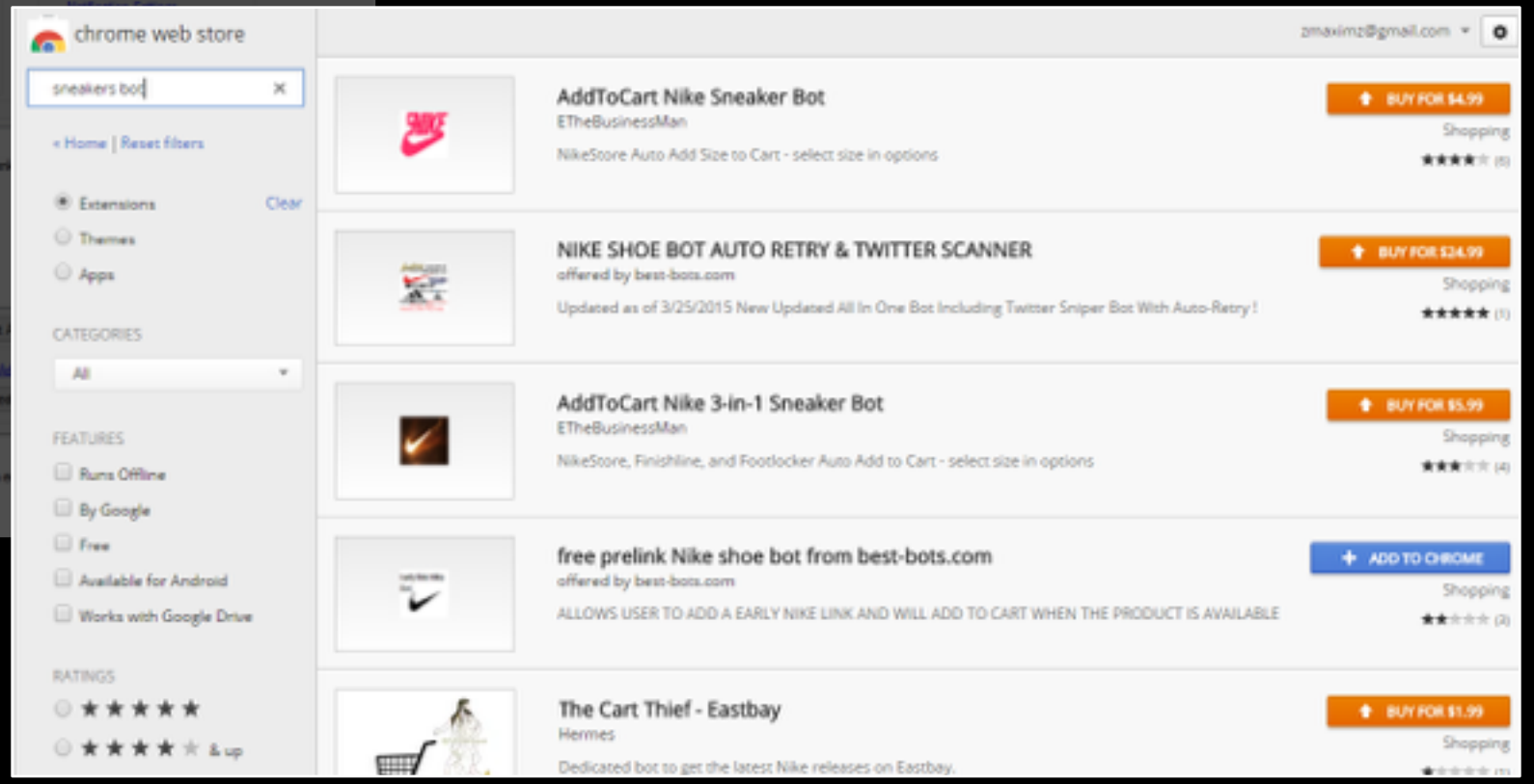
This project was awarded to **ASYanush** for **$400 USD**.

Copping, Scalping and Sniping

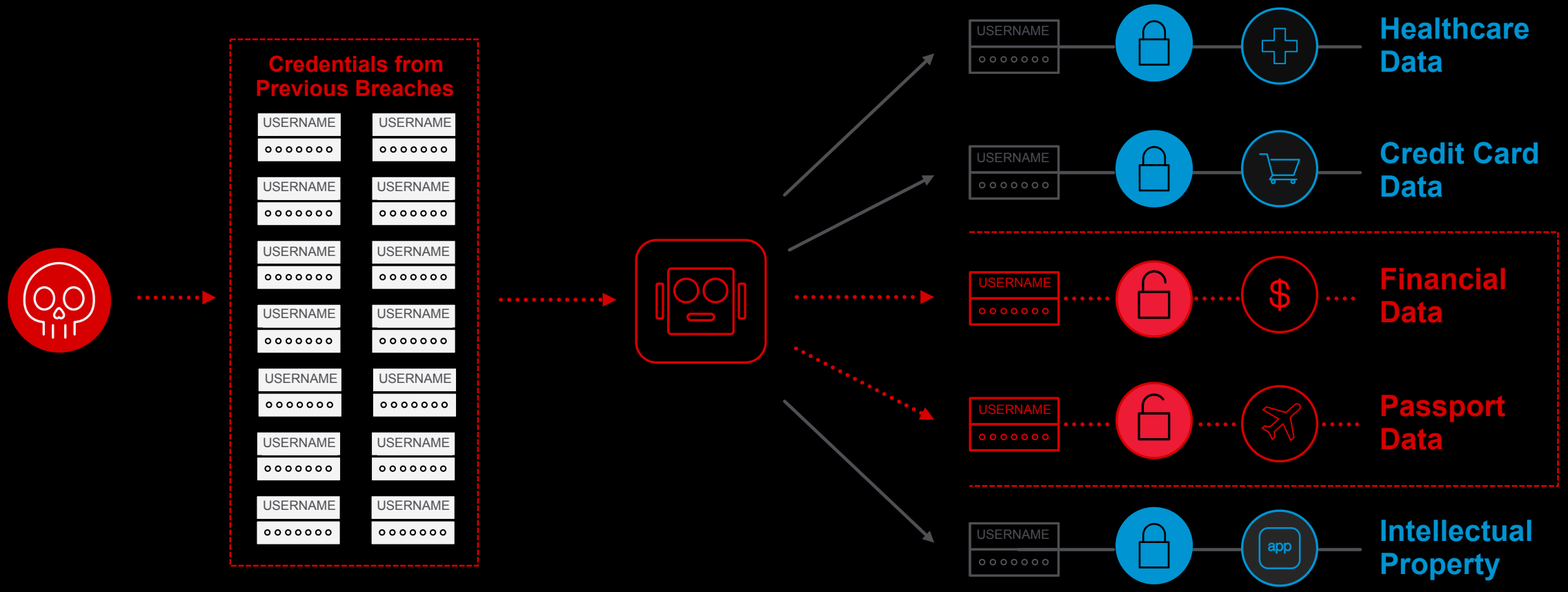
OAT-005, OAT-013, OAT-021

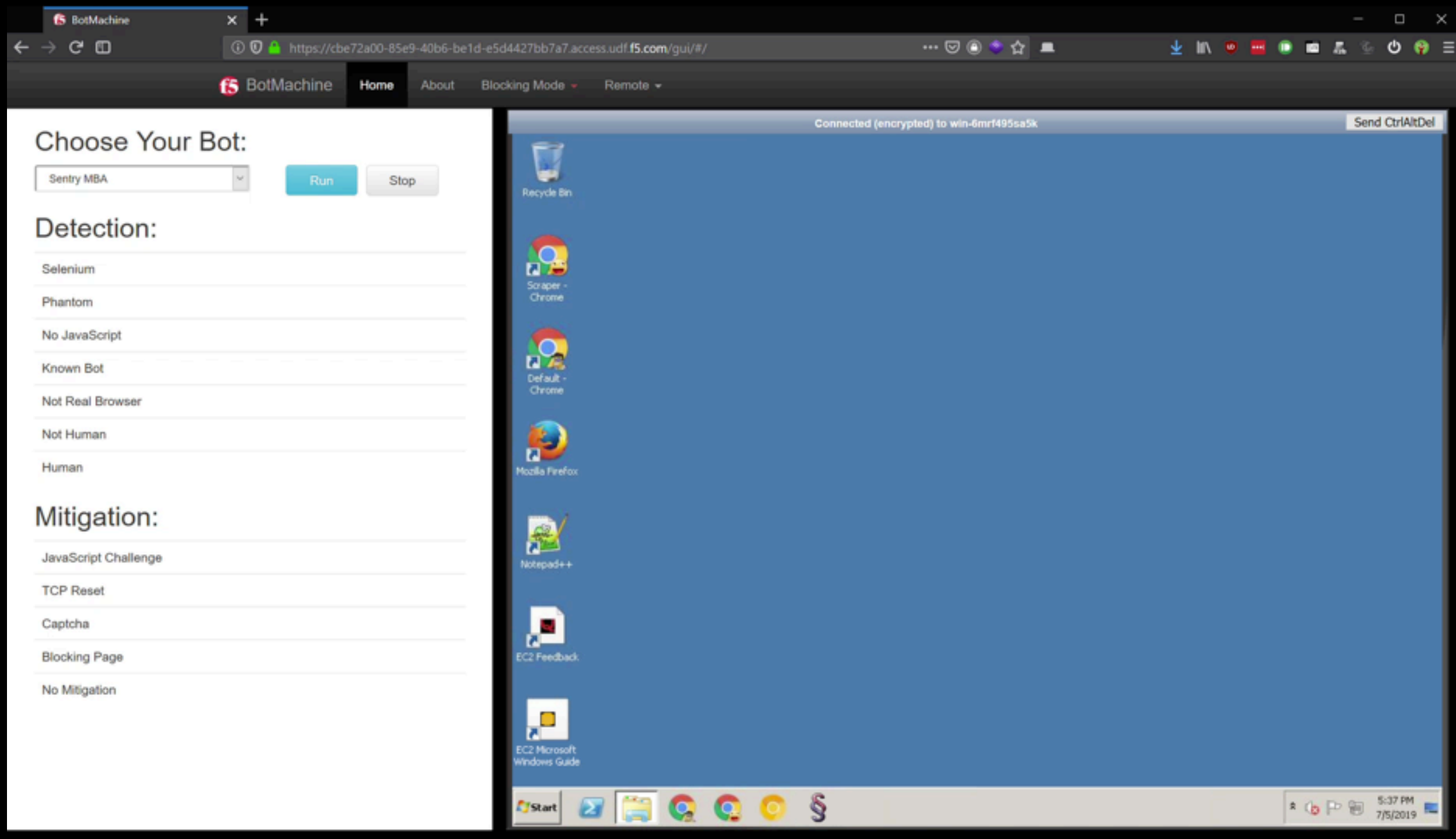
Bot Name	URL	Price	Features
Better Nike Bot	http://www.betternikebot.com/	200$	• Captcha Solver
Another Nike Bot	http://www.anothernikebot.com/	325$ - Basic Package	• Captcha Solver
Premium Nike Bot	http://www.heatedsneaks.com/store/p57/NikeBot	49.99$	
Easy Cop Ultimate	http://www.easycopbots.com	95$ - Starters Kit	
Just Cop It Bots	https://www.justcopitbots.com/	200$	



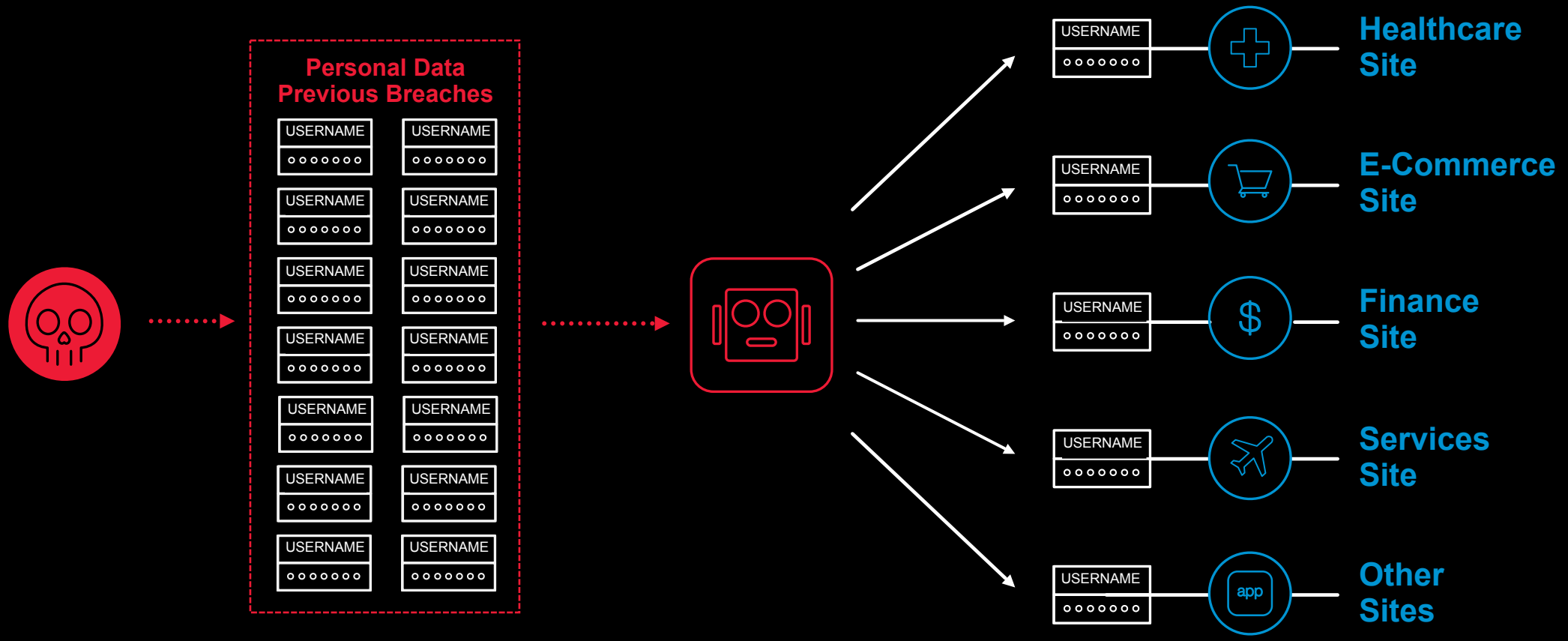


OAT-008 Credential Stuffing

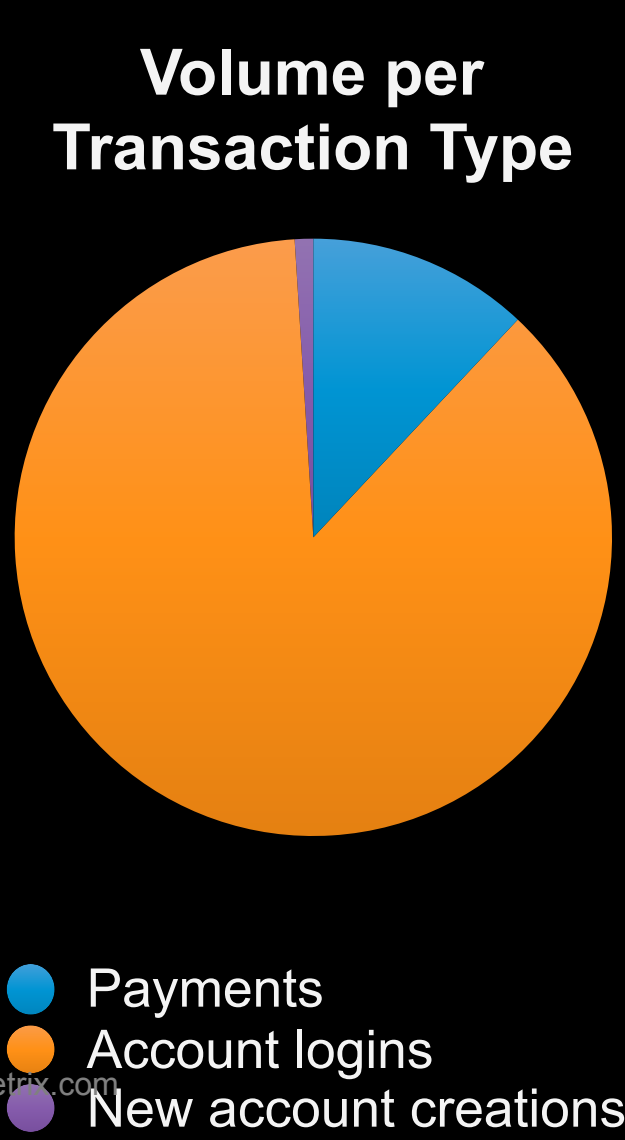


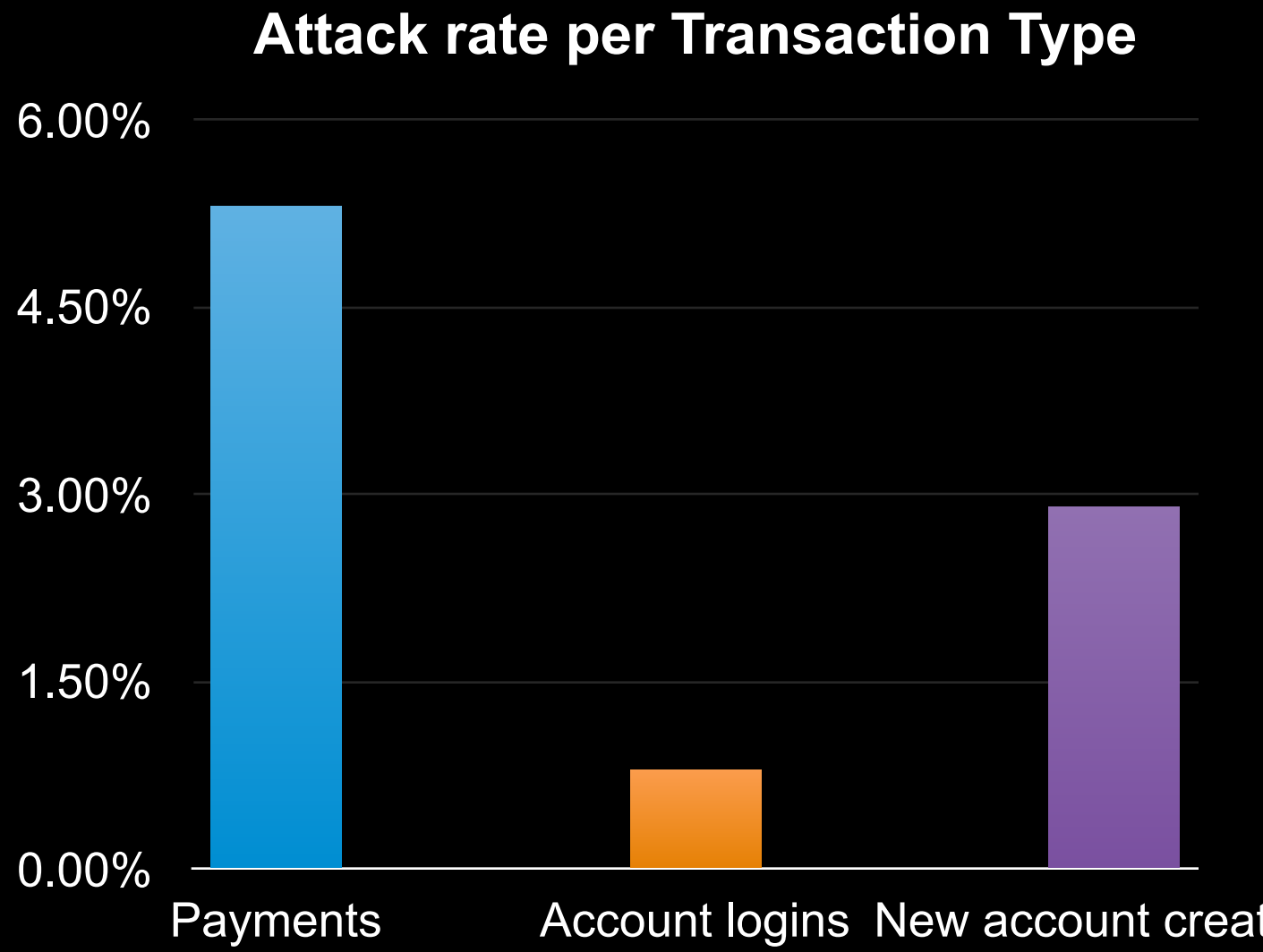

BotMachine
https://cbe72a00-85e9-40b6-be1d-e5d4427bb7a7.access.udf.f5.com/gui/#/
BotMachine
Home
About
Blocking Mode
Remote
Choose Your Bot:
Sentry MBA
Run
Stop
Detection:
Selenium
Phantom
No JavaScript
Known Bot
Not Real Browser
Not Human
Human
Mitigation:
JavaScript Challenge
TCP Reset
Captcha
Blocking Page
No Mitigation
Connected (encrypted) to win-6mrf495sa5k
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)

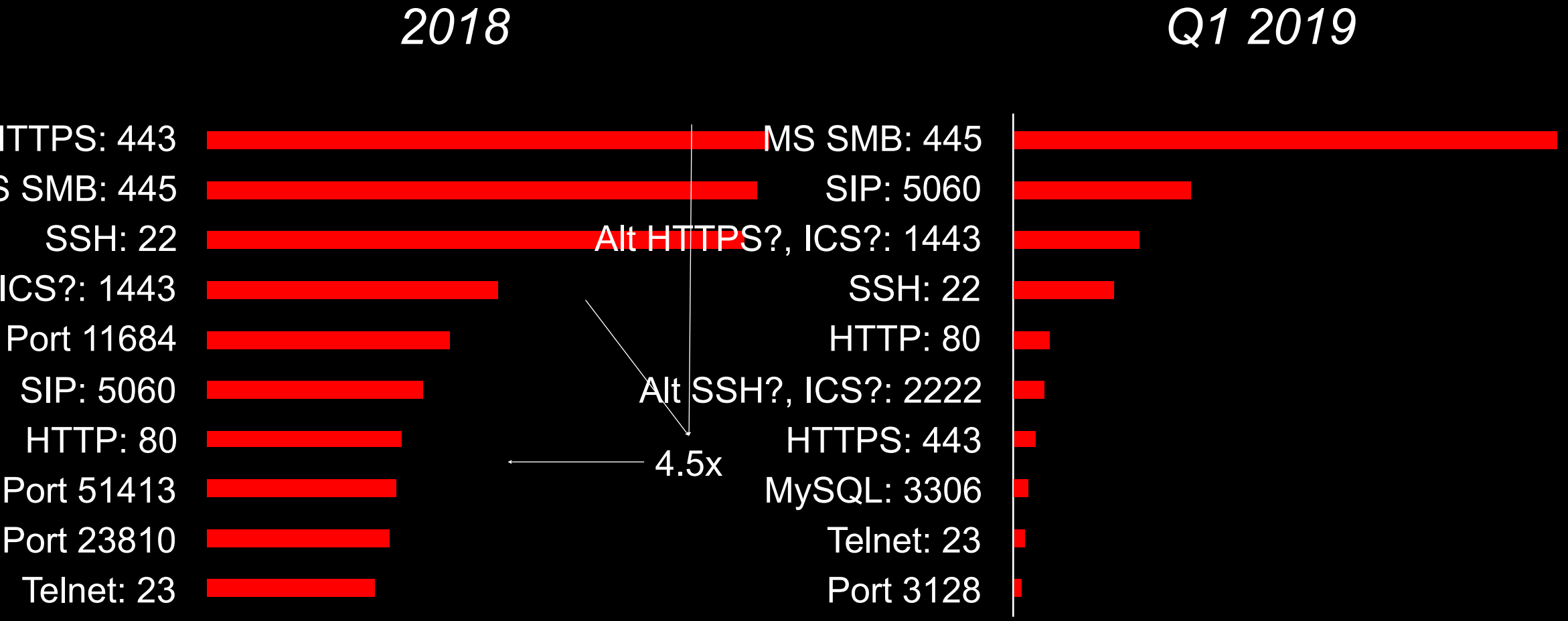




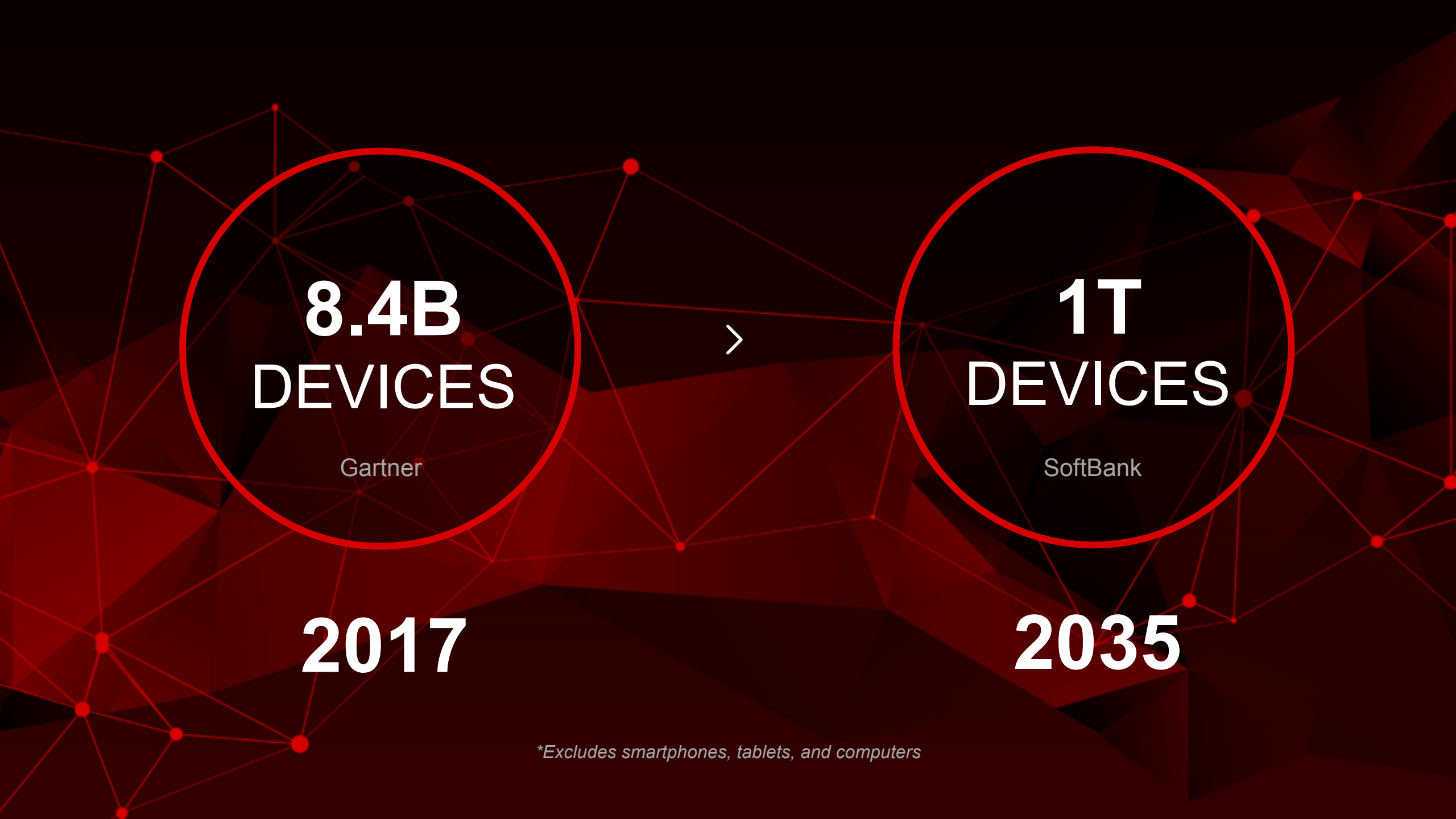
Source: threatmetrix.com

OAT-014 Scanning

Top 10 Attacked Ports Globally



SOURCE: F5 Labs & Baffin Bay Networks

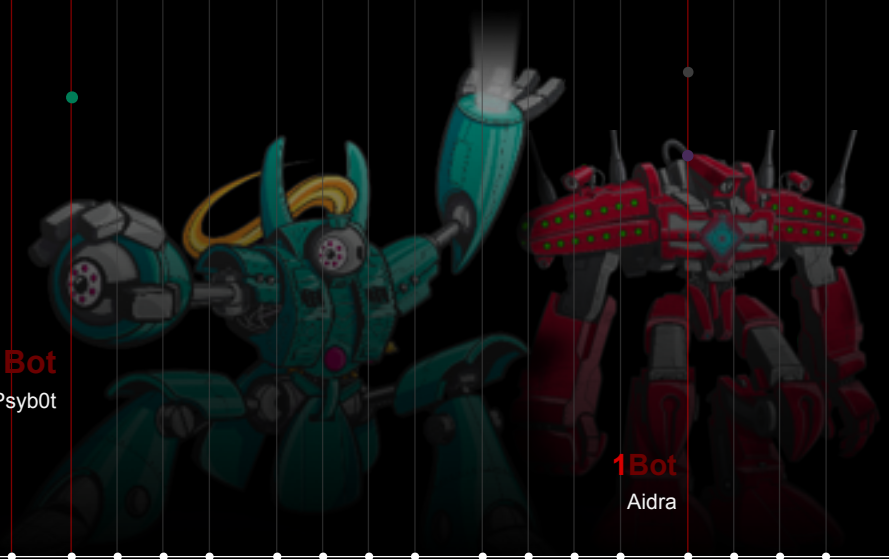

8.4B
DEVICES
Gartner
1T
DEVICES
SoftBank
2017
2035
*Excludes smartphones, tablets, and computers

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



1Bot Psyb0t

1Bot Hydra

1Bot Aidra

1Bot Moon

2Bots Darlloz, Marcher

1Bot Gafgyt Family

1Bot Crash override

1Bot Remaiten

4Bots Hajime, Trickbot, IRC Telnet, Annie

3Bots Mirai, BigBrother, Radiation

3Bots Satori Fam, Amnesia, Persirai

2Bot Brickerbot, Gr1n

2Bots WireX, Reaper

7Bots Masuta, PureMasuta, Hide 'N Seek, JenX, OMG, DoubleDoor, Katrina

13Bots SORA, OWARI, UPnPProxy, OMNI, RoamingMantis, Wicked, VPNFilter, DaddyL33t, Josho, Tokyo, Extendo, Hakai, Akiru / Saikin

6Bots Death, Okane, Anarchy, Torii, Yasaku, Thanos

5Bots Vermelho, Miori, IZIH9, APEP, SEFA, Yowai

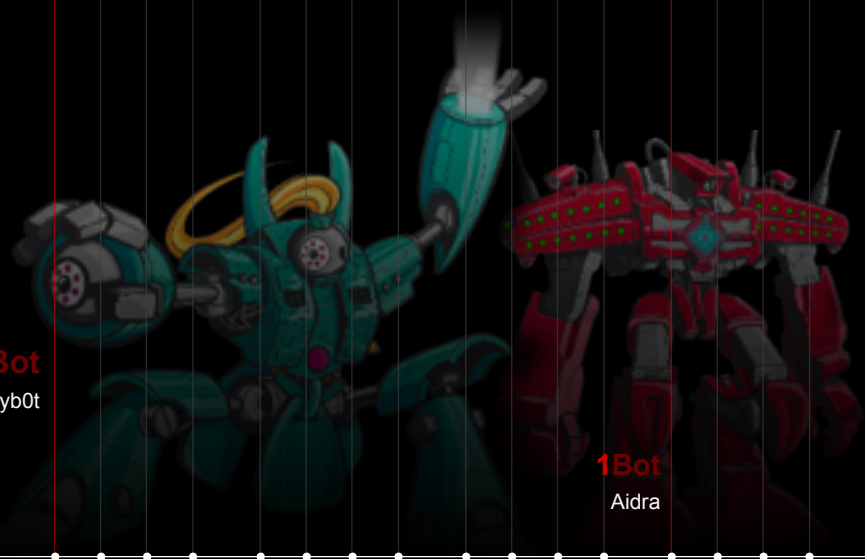
2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

Thingbots

Thingbot Attack Type

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



1Bot
Psyb0t

1Bot
Hydra

1Bot
Aidra

1Bot
Moon

2Bots
Darlloz
Marcher

1Bot
Gafgyt
Family

4Bots
Hajime
Trickbot
IRC Telnet
Annie

1Bot
Crash override

1Bot
Remaiten

3Bots
Mirai
BigBrother
Radiation

2Bots
WireX
Reaper

3Bots
Satori Fam
Amnesia
Persirai

1Bot
Brickerbot

6Bots
Masuta
PureMasuta
Hide 'N Seek
JenX
OMG
DoubleDoor

7Bots
SORA
OWARI
UPnPProxy
OMNI
RoamingMantis
Wicked
VPNFilter

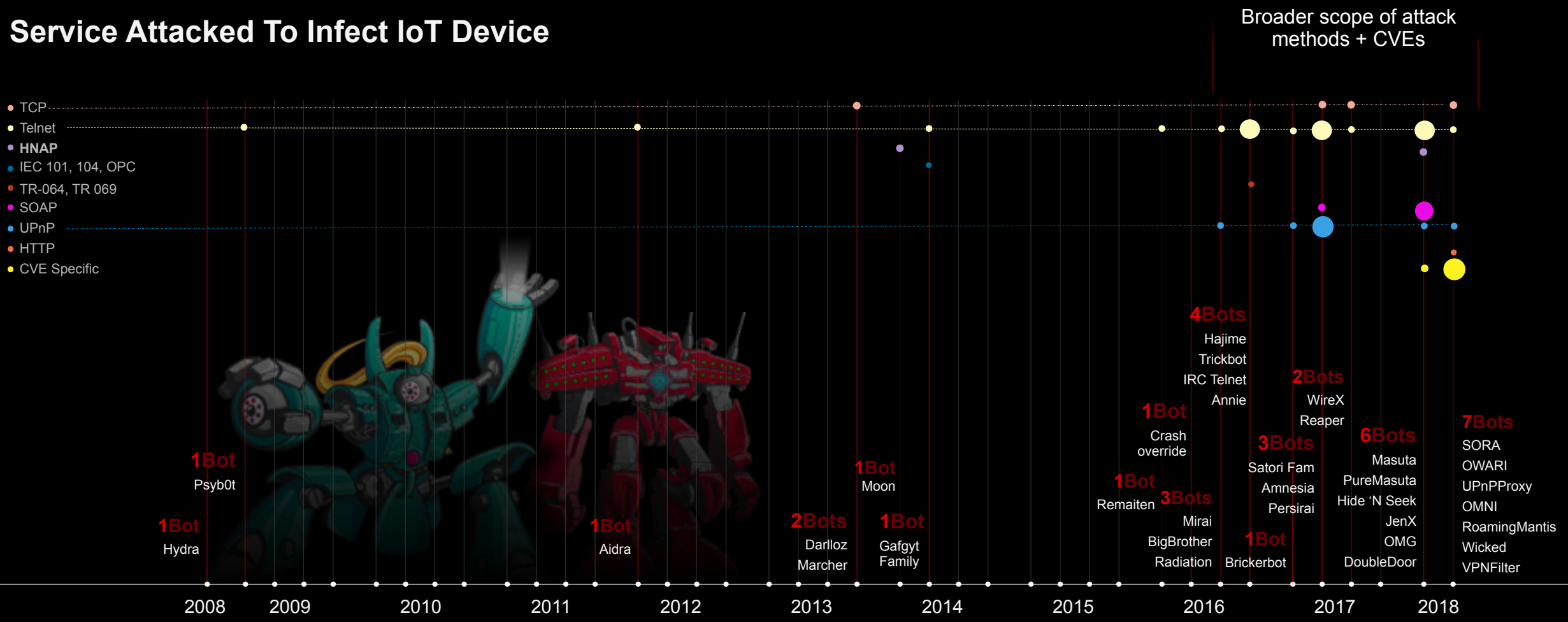
2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

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

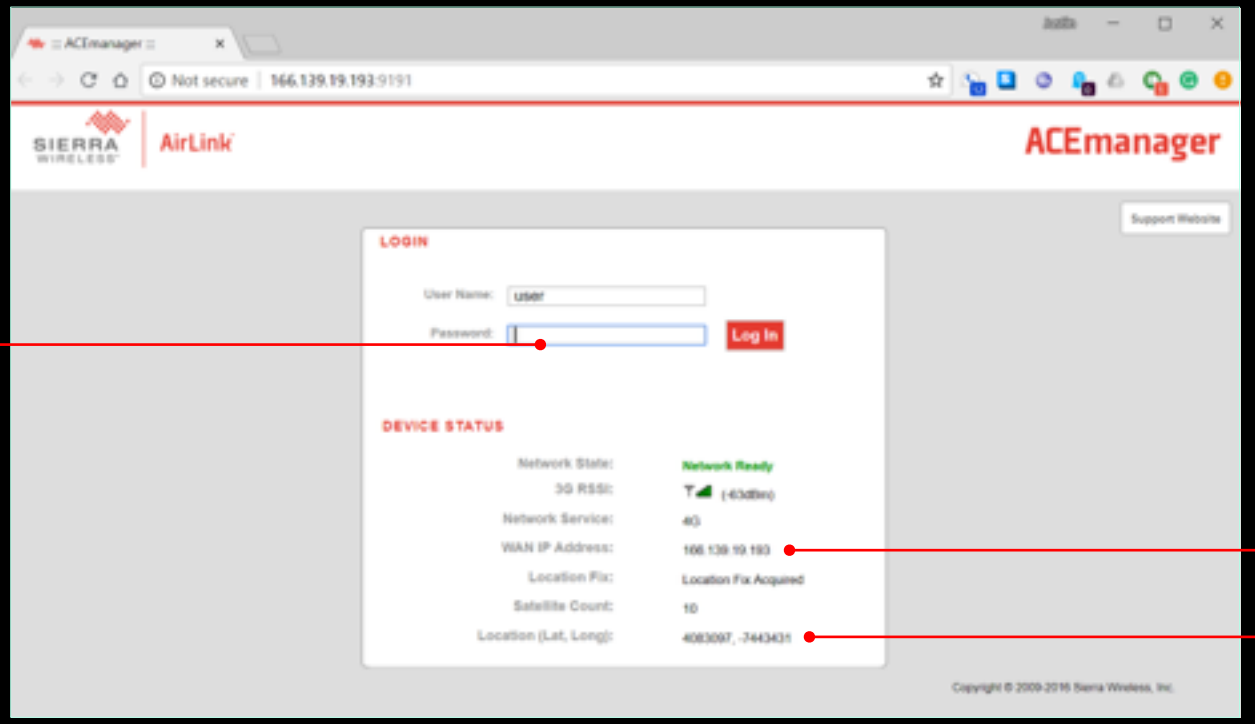


F5 Labs discovers cellular gateway vulns

F5 Labs discovers cellular gateway vulns

SIERRA WIRELESS

“Exploiting” the Vulnerability



DEFAULT PASSWORD
*****

Bruteforce attack(s) are unnecessary.

NO DEPENDENCY on any vulnerability within the hardware or software.

WAN IP
166.139.19.193

PUBLIC GPS COORDINATES
40° 49’ 51.5” N
47° 26’ 03.5” W

https://www.f5.com/labs/articles/threat-intelligence/breaking-down-the-door-to-emergency-services-through-cellular-io

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
ftpuser	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	PlcmSpIp	PlcmSpIp	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

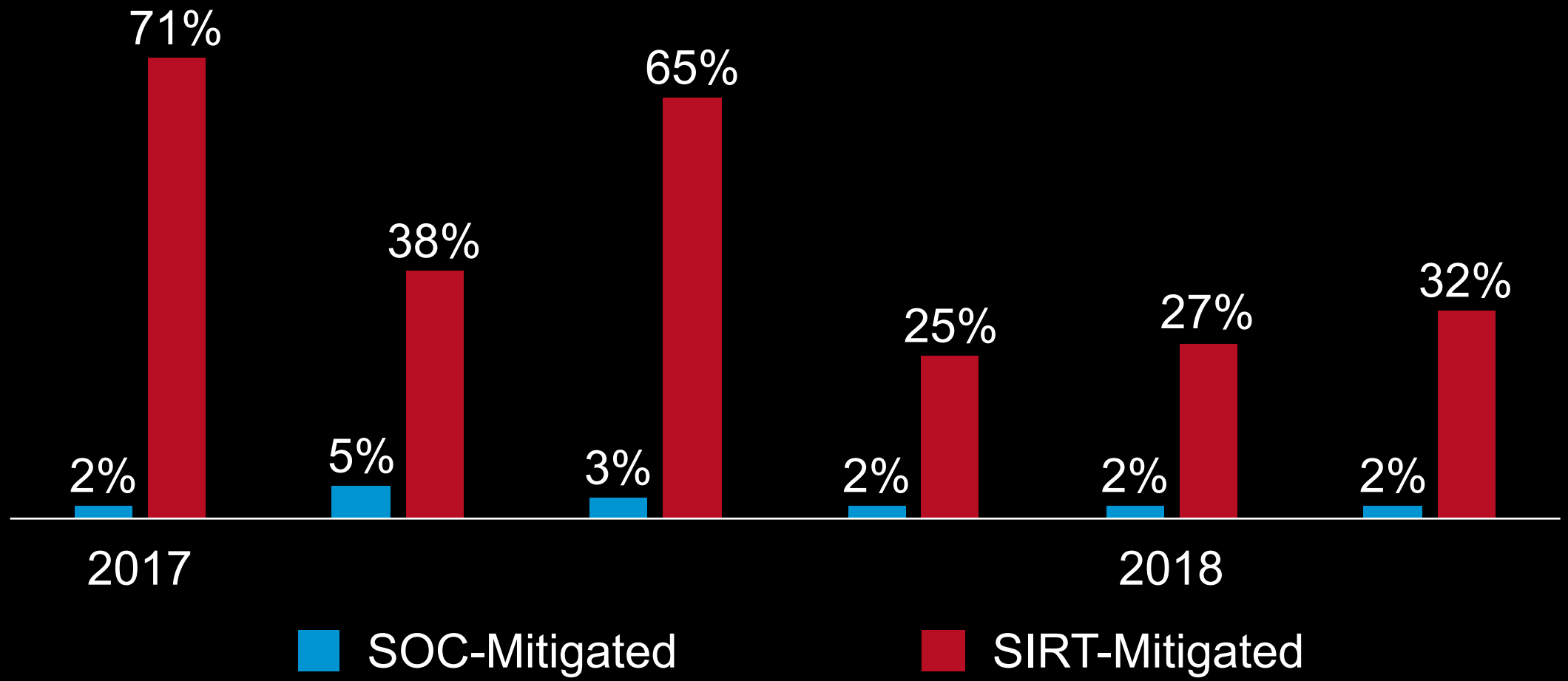
Source: F5 Labs

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.

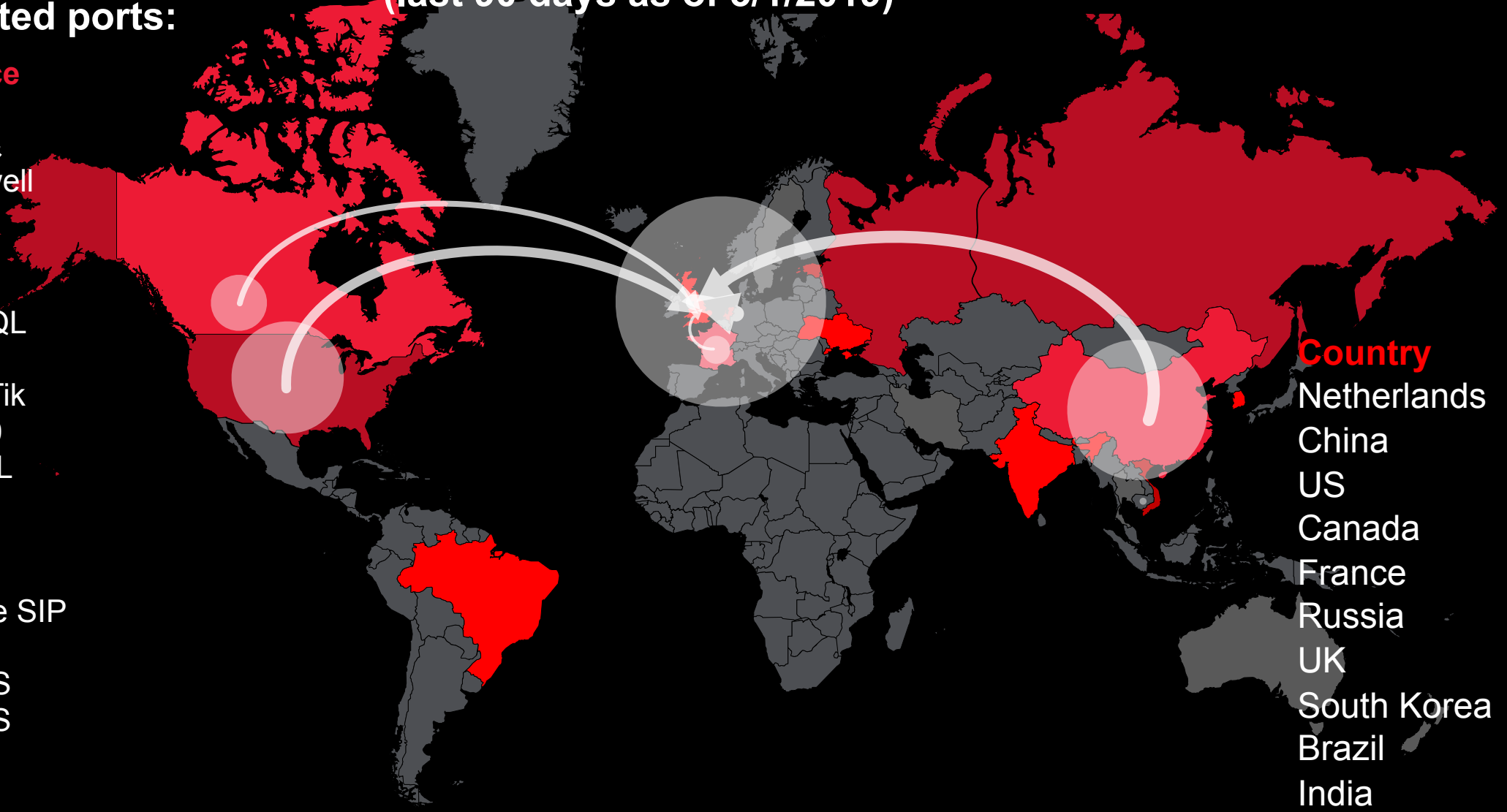


IPs Attacking UK

(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

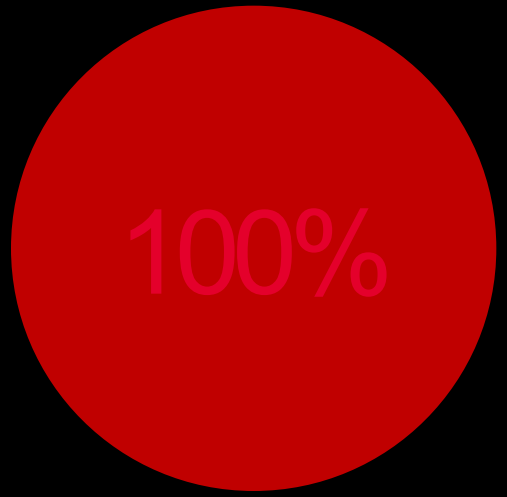


Country

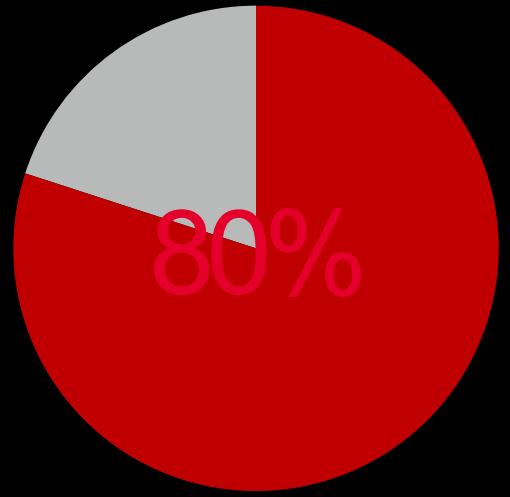
Netherlands
China
US
Canada
France
Russia
UK
South Korea
Brazil
India
Ukraine

Shifting Sources

Thanks to proxies & IoT devices



Previously unseen IP addresses

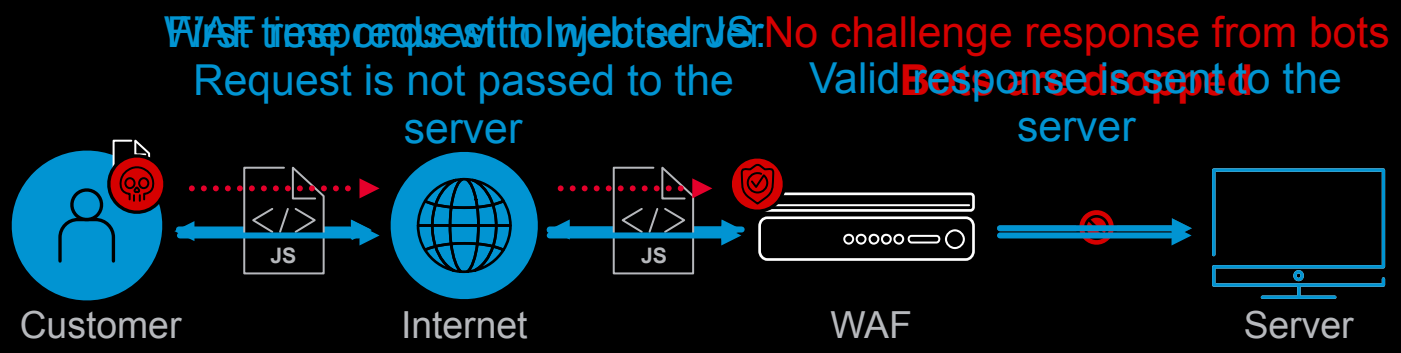


Previously unseen networks (ASN)

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



WAF verifies response authenticity
Cookie is signed, time stamped, and fingerprinted

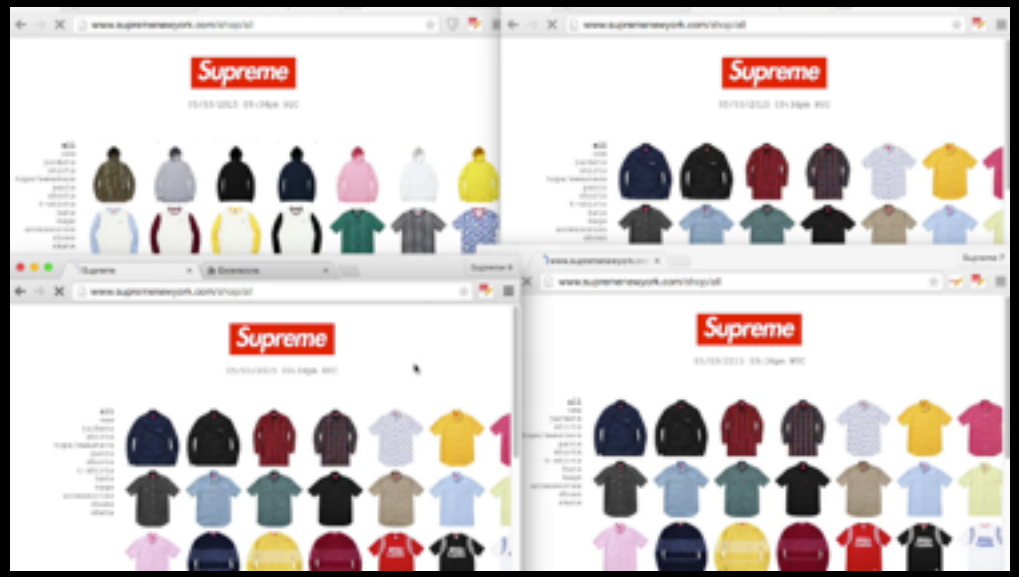
Headless Browsers

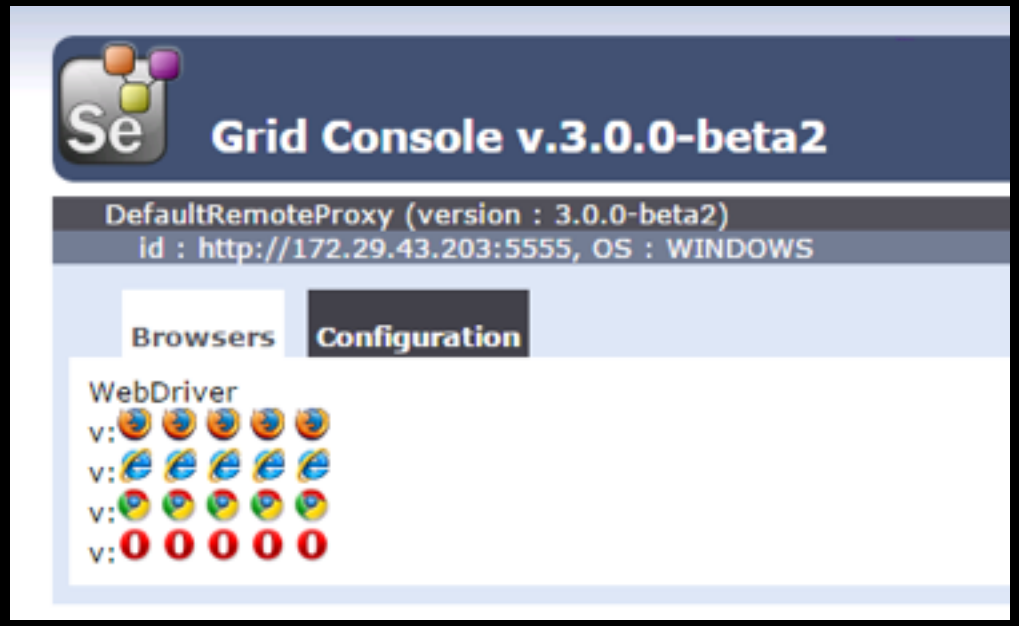
- Command line and scriptable execution of browsers
- Chrome without the chrome!
- Able to render HTML and execute JavaScript & AJAX
- Often Selenium based

Headless Chrome

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-xvbf
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



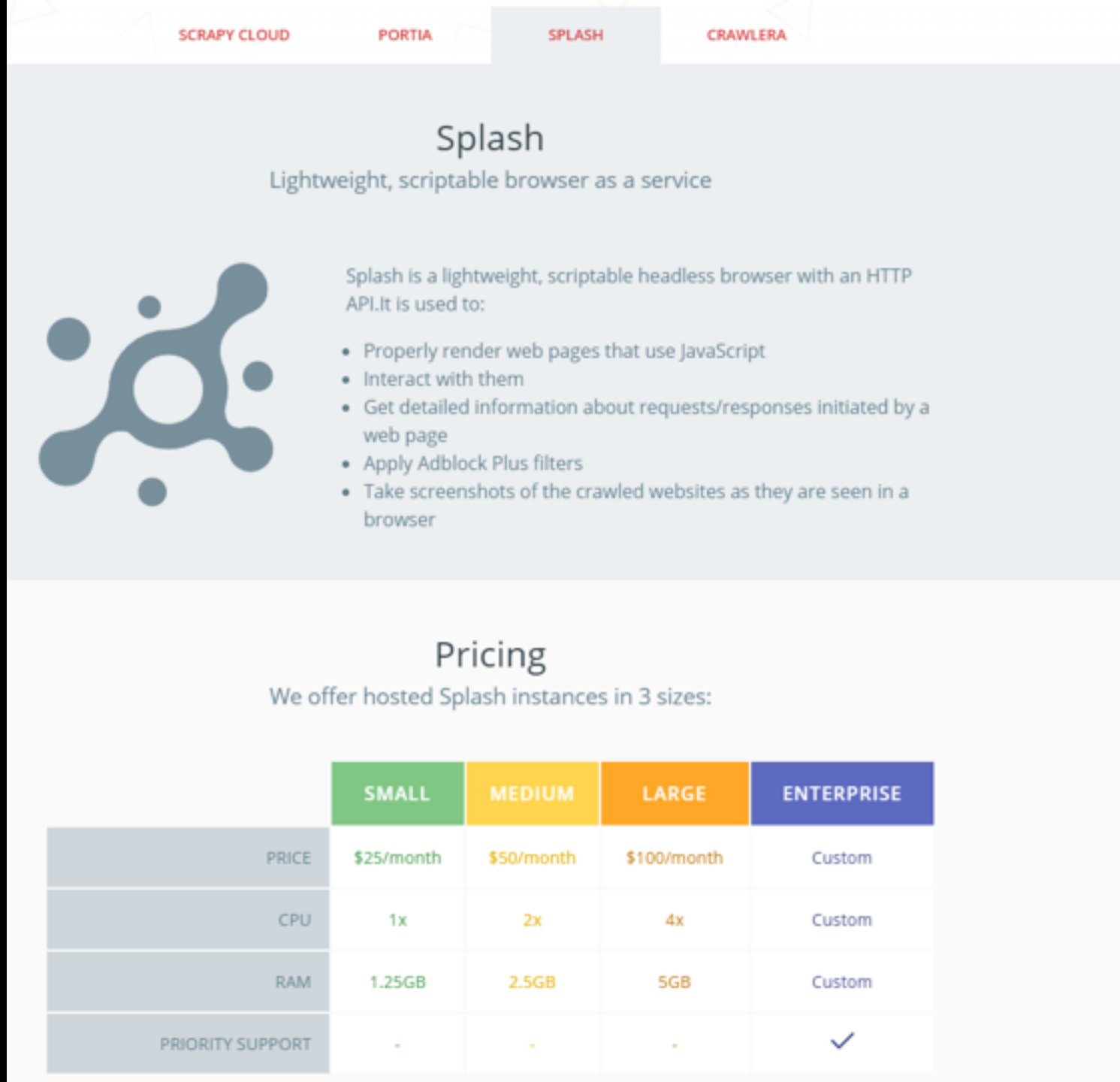


fb_login.py

```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"
)
```

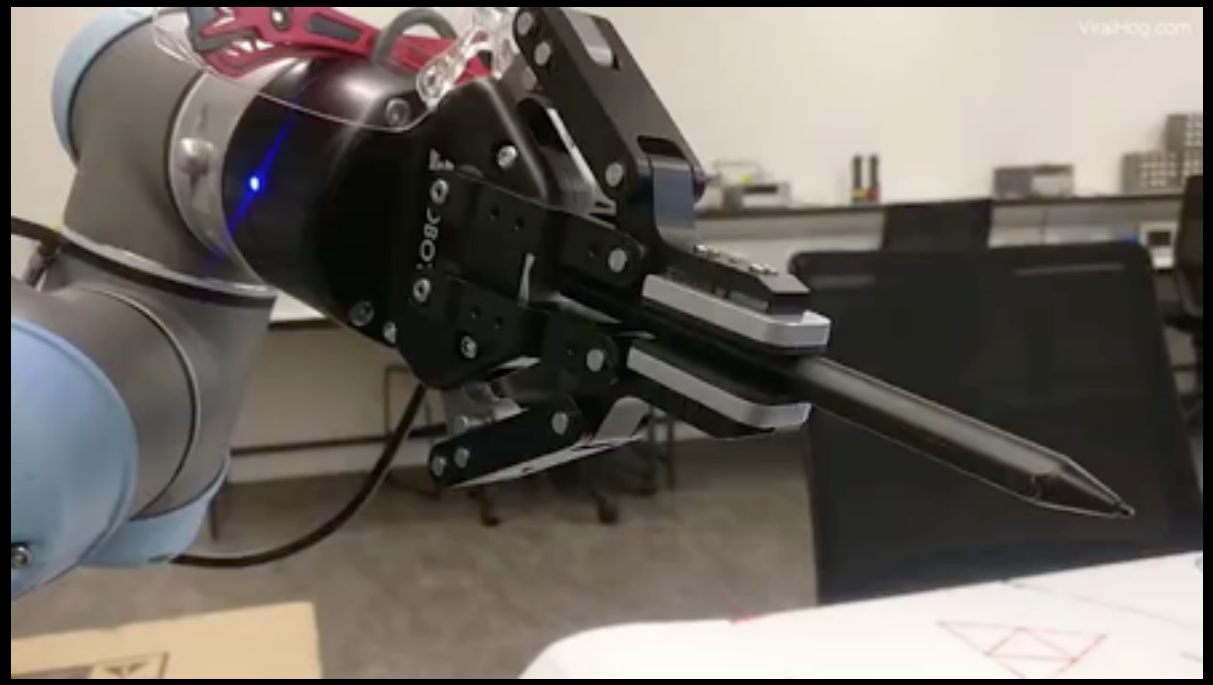
Scriptable Browser as-a-Service

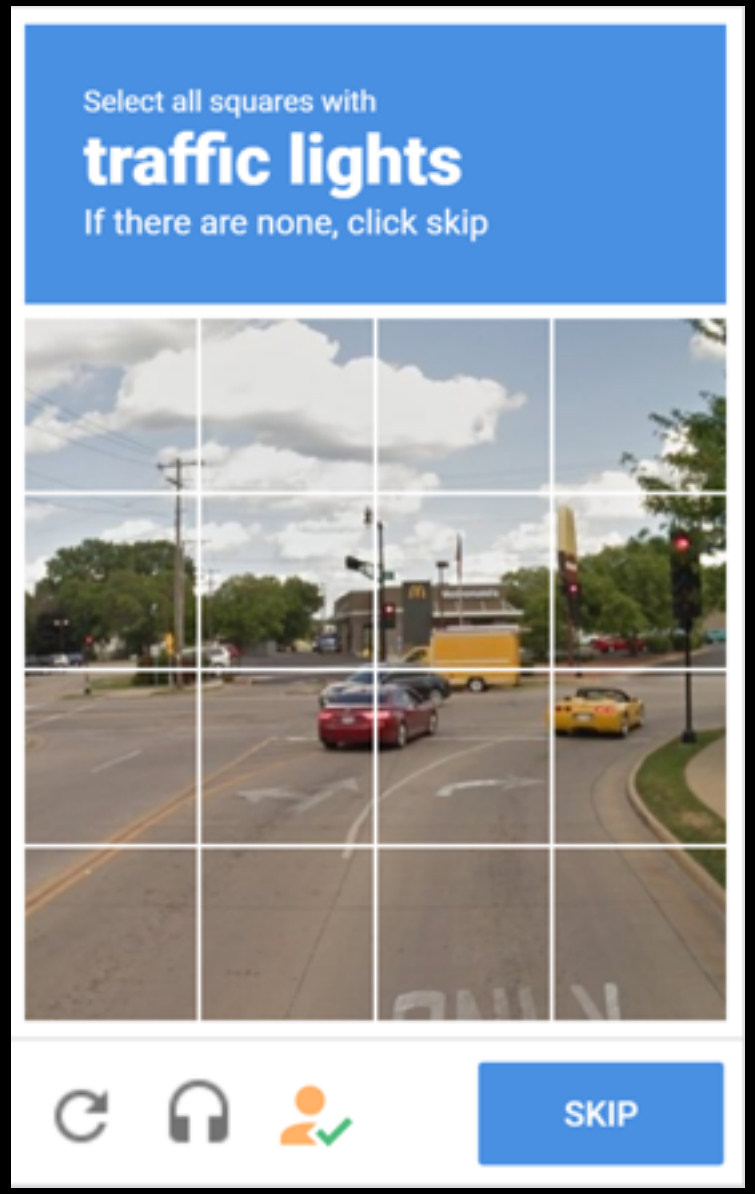
- Detect headless browsers via extensions and browser flags



CAPTCHA

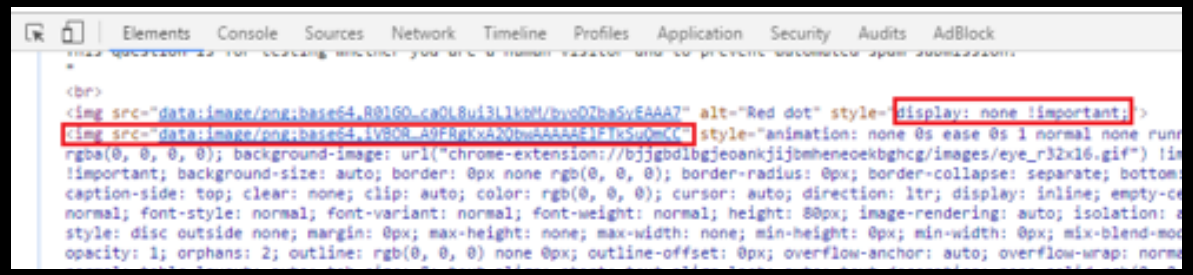

morning
overlooks
Type the two words:
reCAPTCHA
stop spam.
read books.




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

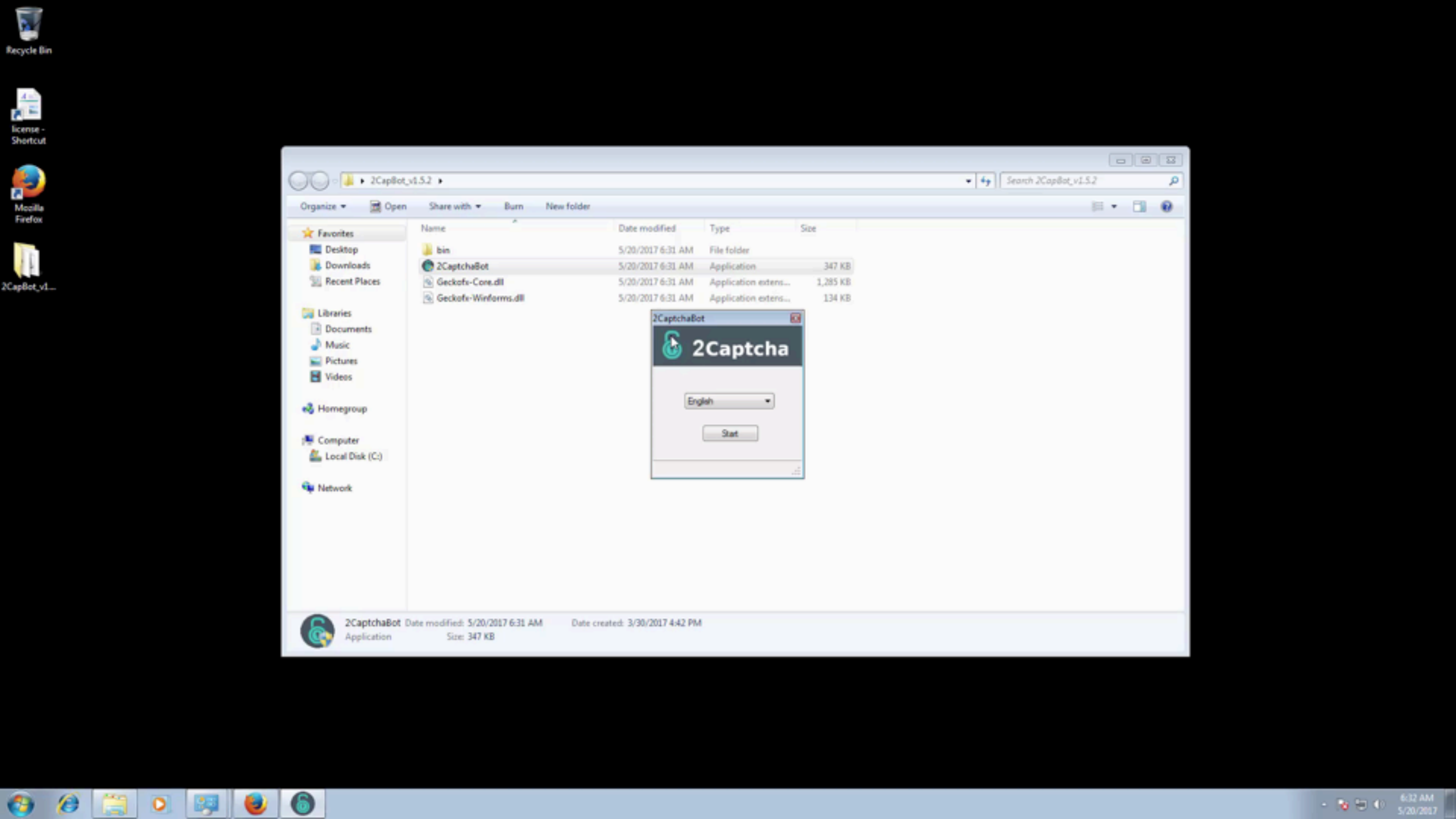
CAPTCHA Solvers – Browser Extensions

Rumola

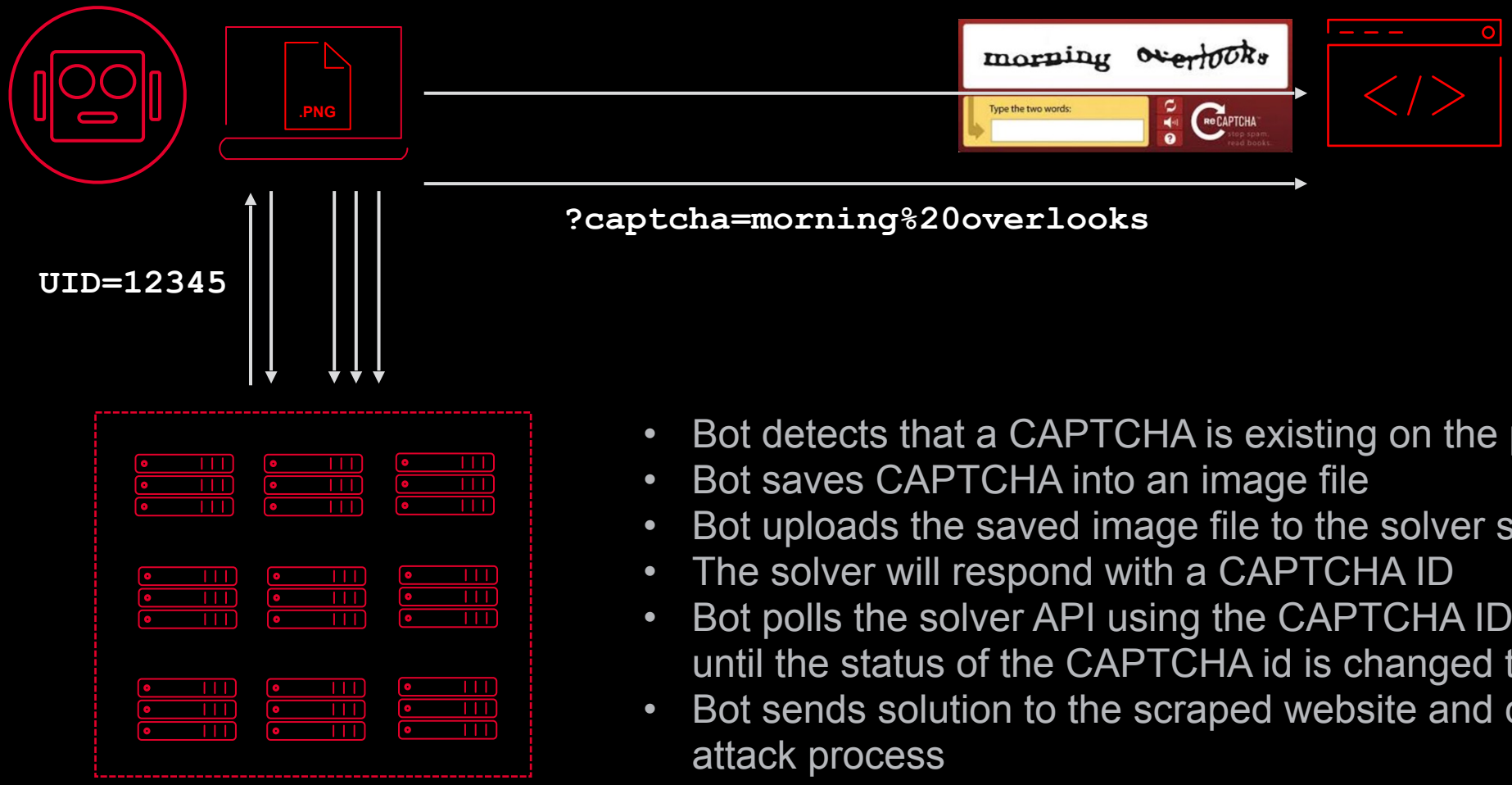


AntiCaptcha

- Detect CAPTCHA extensions based on HTML insertion

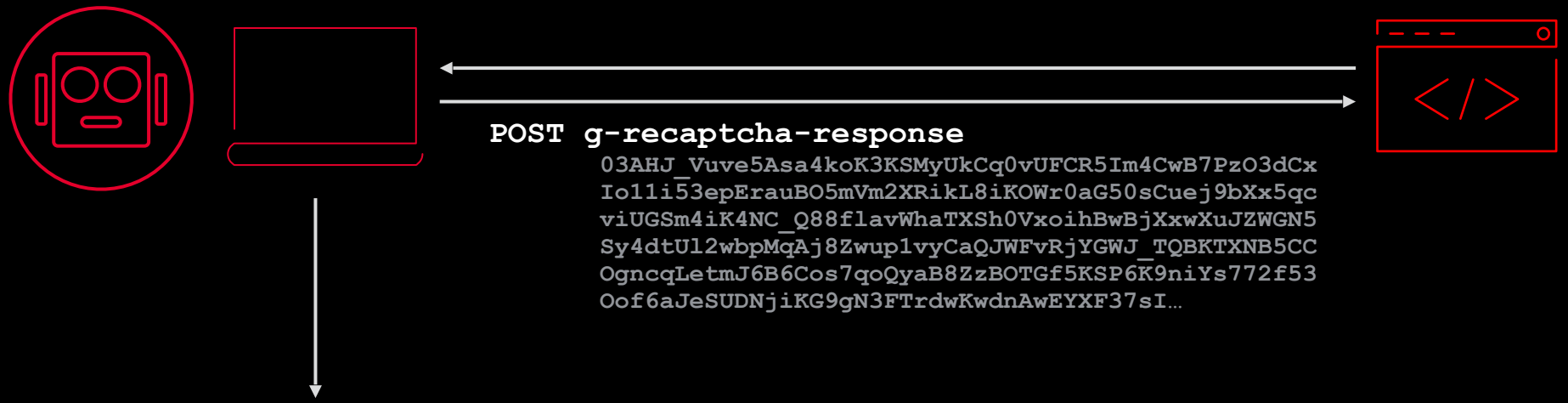

Recycle Bin
license - Shortcut
Mozilla Firefox
2CapBot_v1...
2CapBot_v1.5.2
Search 2CapBot_v1.5.2
Organize
Open
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
bin
5/20/2017 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
6:32 AM
5/20/2017

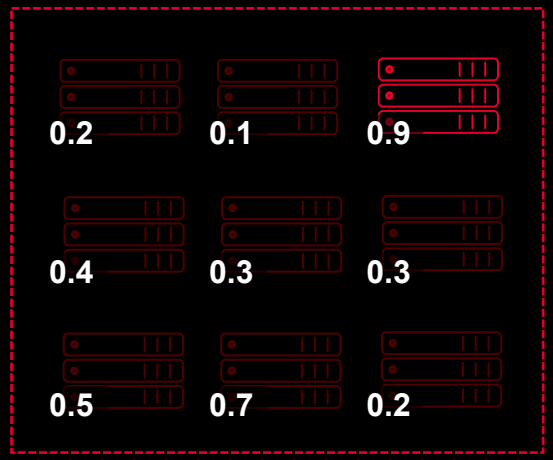
Automated CAPTCHA Solvers



- 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

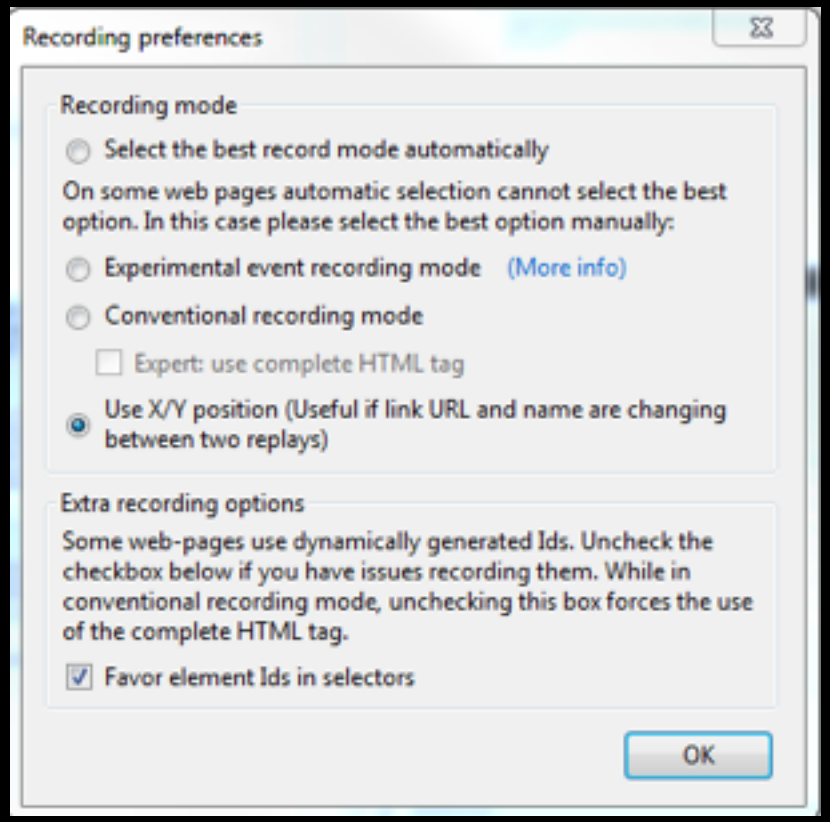


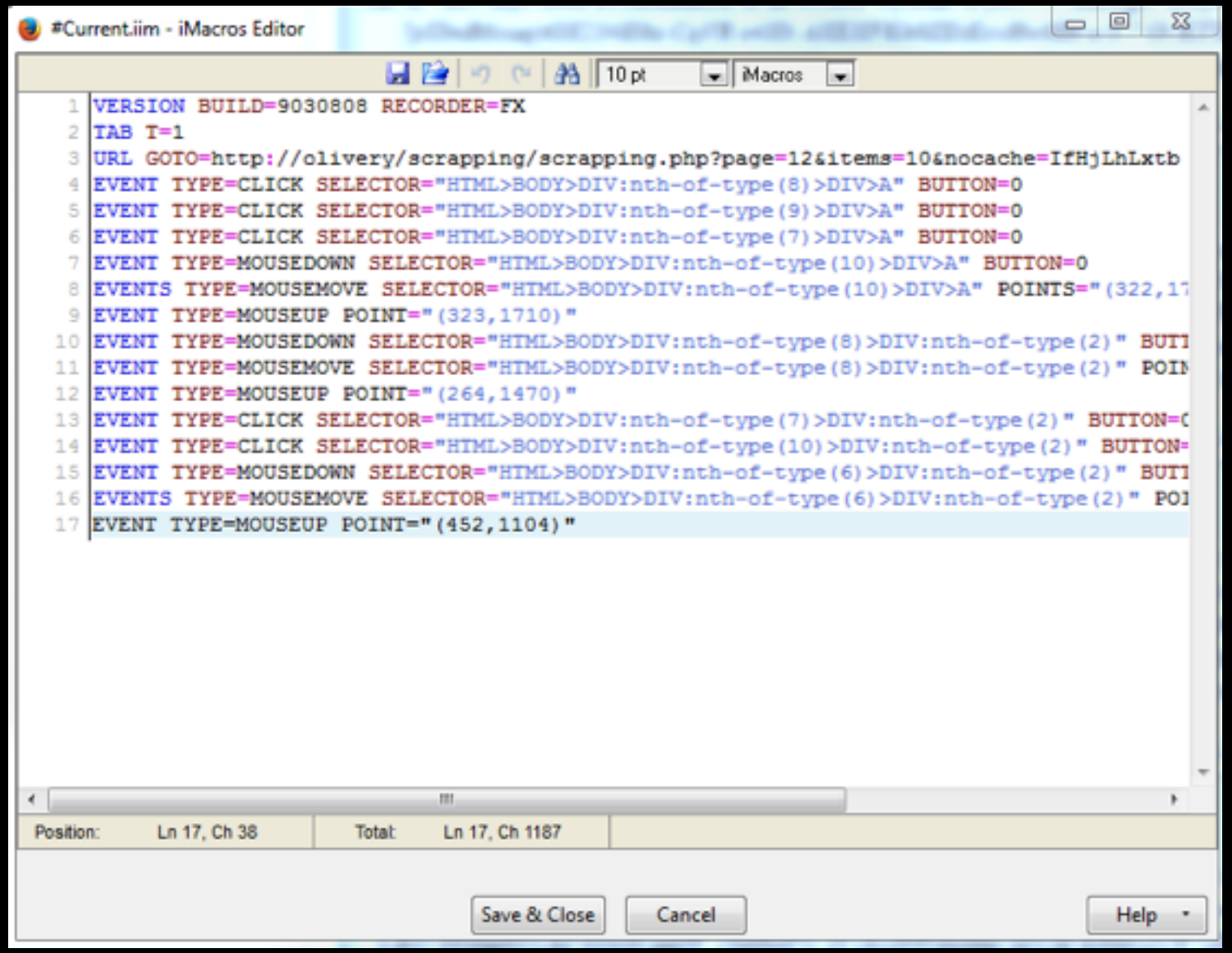


- ReCaptcha v3 uses ‘scores’ from 0.1 to 0.9 to rate the client
- Typically, a user score will be the same/similar across sites
- ReCaptcha v3 solver monitors scores of workers
- Selected the worker with the highest score to solve the Captcha

https://2captcha.com/2captcha-api#solving_recaptchav3

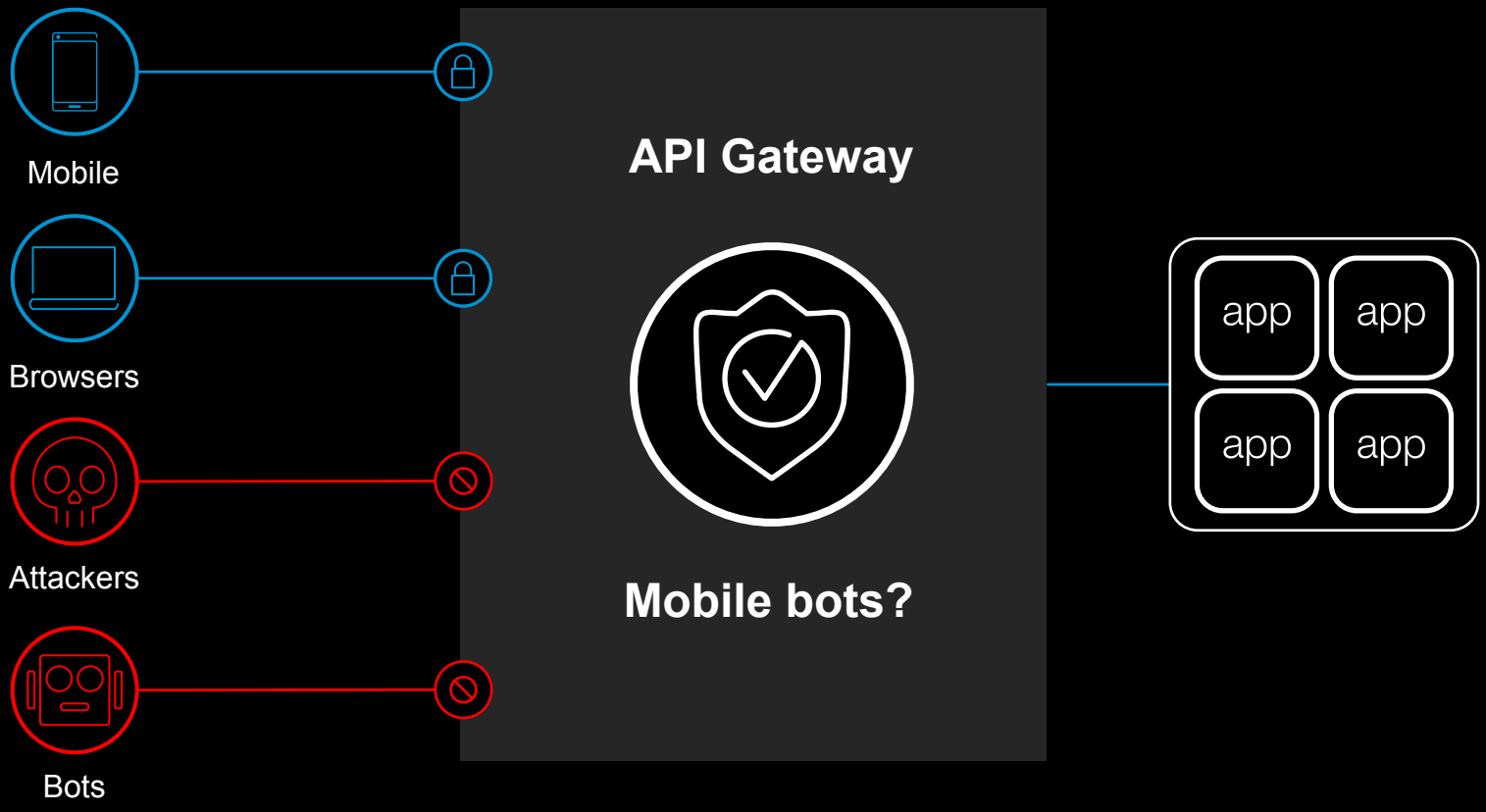
Simulated Mouse Events





- Fake mouse movements can lack cursor positioning

Bots Attacking Mobile APIs

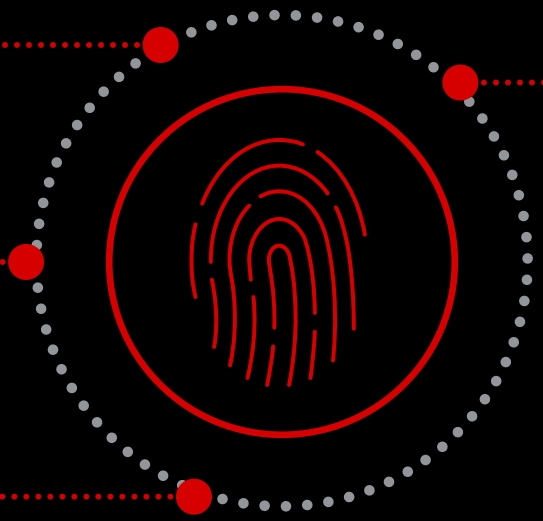


Behavioural Analysis and Fingerprinting

Detect GET flood attacks against Heavy URIs

Strong authentication

Identify non-human surfing patterns

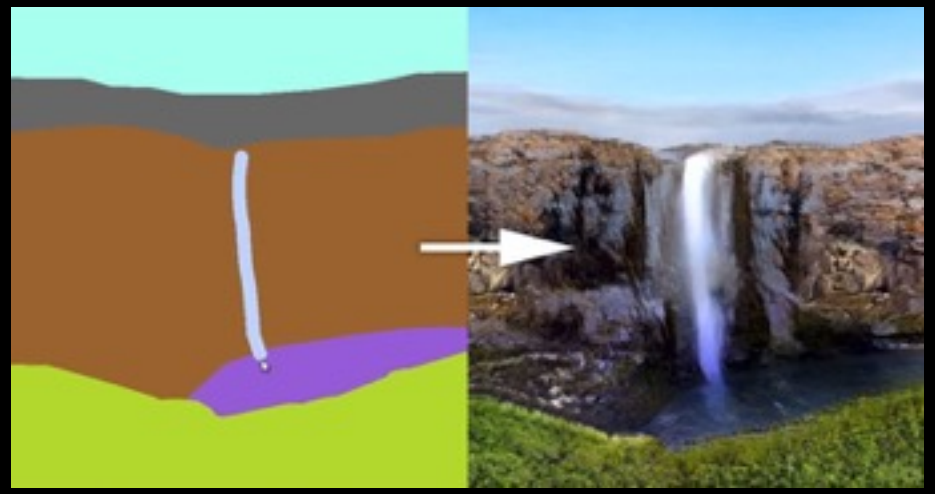


Fingerprint client capabilities

Operating system
Browser

- Screen size and colour depth
- Plugin details
- Time zone
- HTTP_ACCEPT headers
- Language
- System fonts
- Touch support
- **Extensions**
- **TLS handshake**

AI and Future Bots

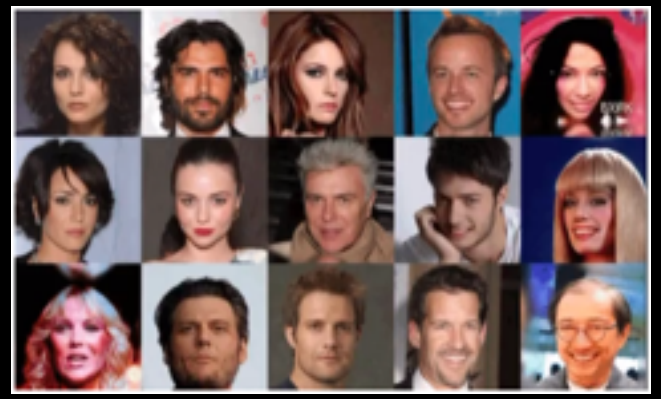


In a shocking finding, scientist discovered a herd of unicorns living in a remote, previously unexplored valley, in the Andes Mountains. Even more surprising to the researchers was the fact that the unicorns spoke perfect English.

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.




F5
LABS