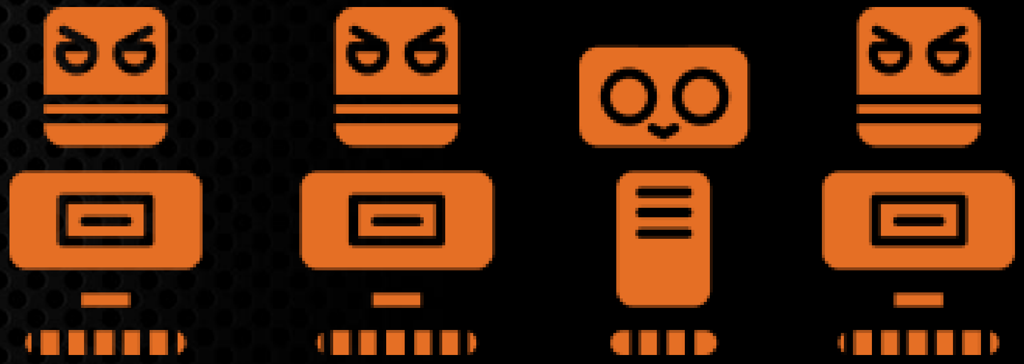
radware
Every second counts

IP Agnostic Bot Detection

Michael Groskop
Director, Web Application Security
OWASP January 2017



About me

Director of Web Application Security @Radware

Over 12 years in the Security Space:

- Web Applications Security
- Authentication & SSO
- Cloud solutions
- Database Security

✉ michaelgro@radware.com

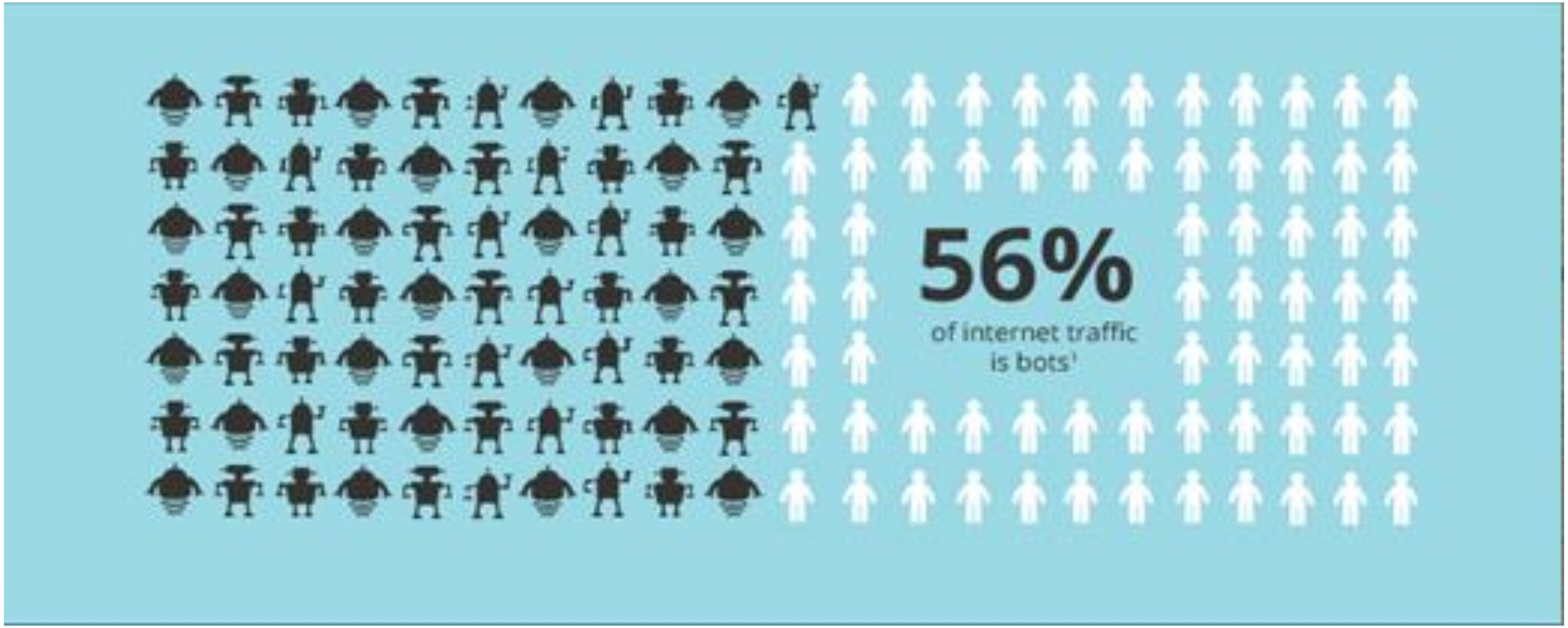
in https://www.linkedin.com/in/michaelgroskop

AGENDA

radware
Every second counts

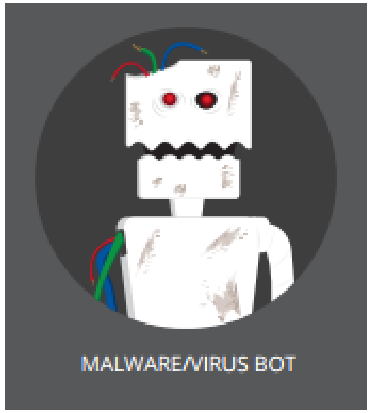
- Scoping the Bot Problem
- Bots Behavioral Attributes
- IP Agnostic Bot Detection

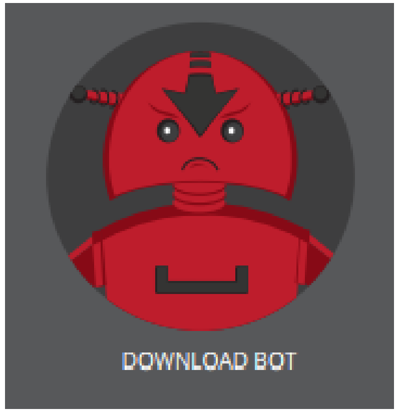
Bots Generate ~½ of the Internet Traffic

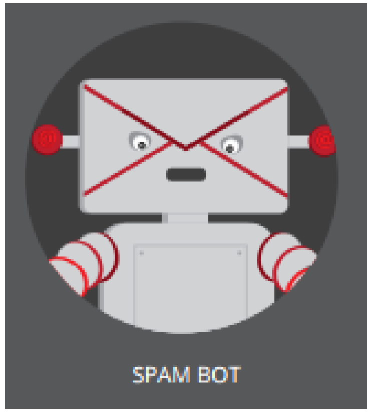


~30% of the Web traffic is generated by **Bad Bots**

HACKER BOT

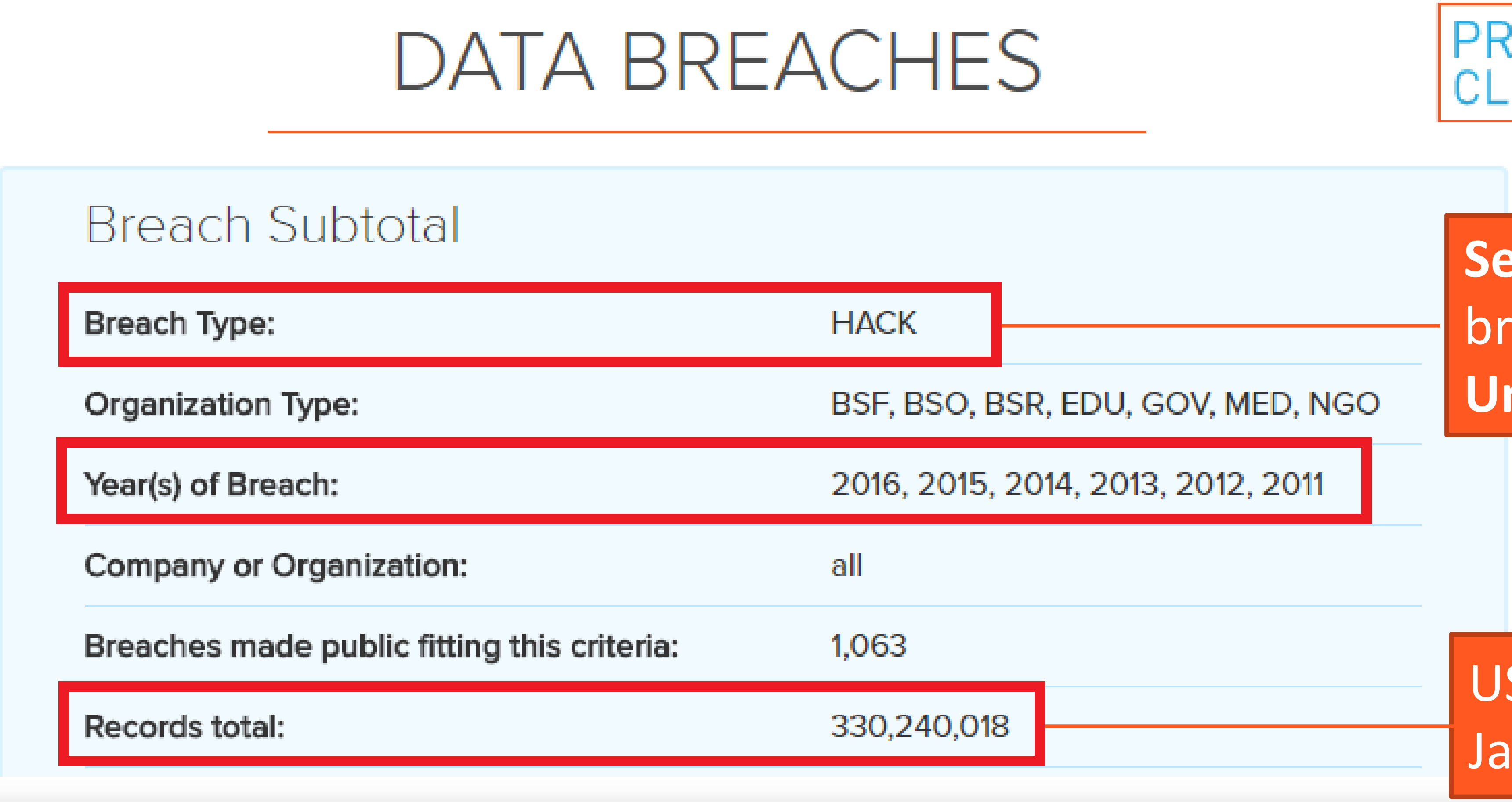

MALWARE/VIRUS BOT


DOWNLOAD BOT


SPAM BOT

330 Million Records Breached in the US since 2011

PRIVACY RIGHTS CLEARINGHOUSE



DATA BREACHES

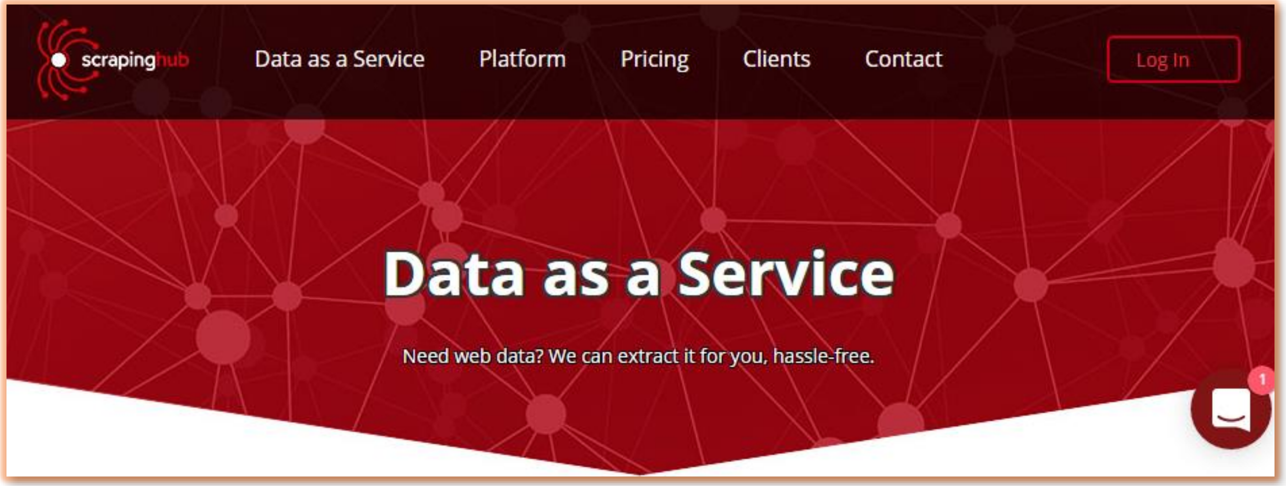
Breach Subtotal

Breach Type:	HACK
Organization Type:	BSF, BSO, BSR, EDU, GOV, MED, NGO
Year(s) of Breach:	2016, 2015, 2014, 2013, 2012, 2011
Company or Organization:	all
Breaches made public fitting this criteria:	1,063
Records total:	330,240,018

Sensitive data records breached by hacking in the **United States 2011 - 2016**

US population projected to Jan 2017 is **325,400,000**

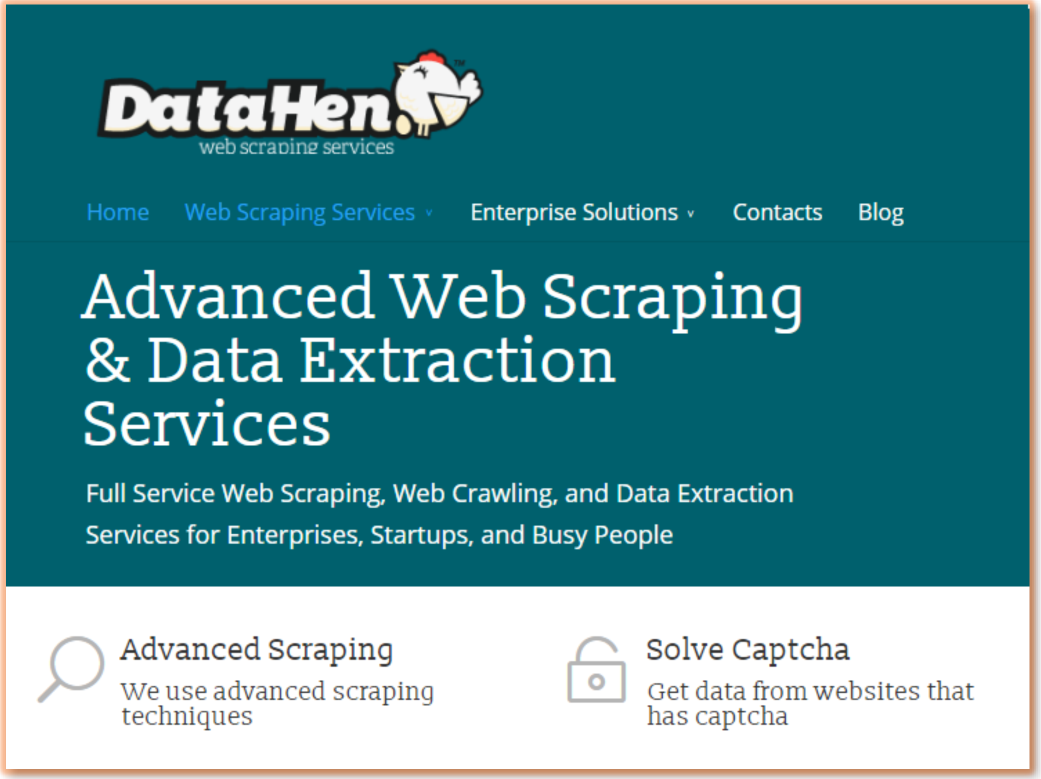
Scraping services are “Just a Google Away”



Data as a Service

Need web data? We can extract it for you, hassle-free.

Get data and images from any website



Advanced Web Scraping & Data Extraction Services

Full Service Web Scraping, Web Crawling, and Data Extraction Services for Enterprises, Startups, and Busy People

Advanced Scraping

We use advanced scraping techniques

Solve Captcha

Get data from websites that has captcha

Are you a Bot?

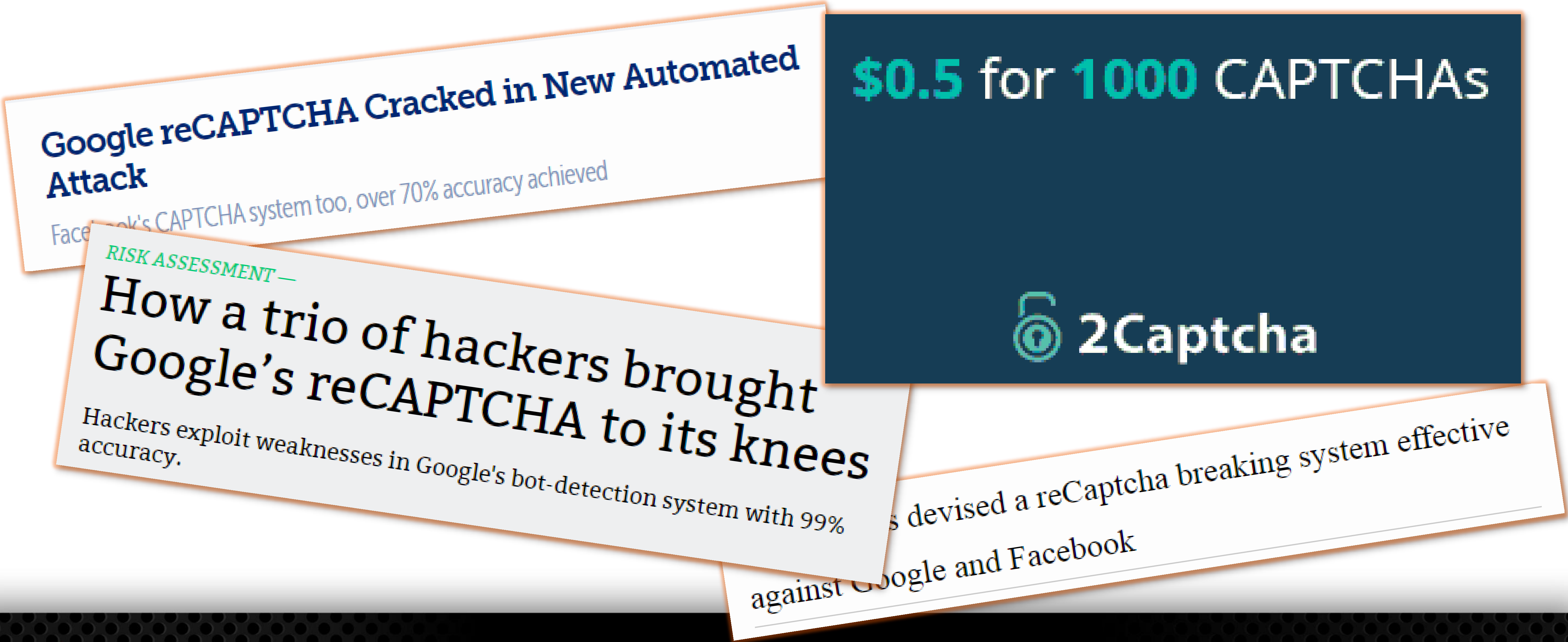
Alan Turing Test (1950)

Eugene Goostman (2013)

ChatBots (2017)

In a “reverse” Turing test, **a computer is to determine whether it is interacting with a human or another computer.**

Google reCAPTCHA ?



Google reCAPTCHA Cracked in New Automated Attack

Facebook's CAPTCHA system too, over 70% accuracy achieved

$0.5 for 1000 CAPTCHAs

2Captcha

RISK ASSESSMENT —

How a trio of hackers brought Google's reCAPTCHA to its knees

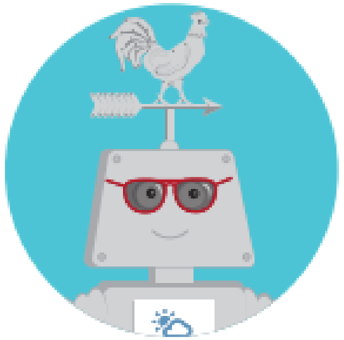
Hackers exploit weaknesses in Google's bot-detection system with 99% accuracy.

s devised a reCaptcha breaking system effective against Google and Facebook

~25% of the Web traffic is generated by **Good Bots**

Crawler Bot

Trader Bot



Data Bot

FeedFetcher Bot

Travel Industry Good Bots ?!

Expedia

priceline.com

FAIRFLY

Booking.com

Travelist
your smart choice

Hotels Scanner
hotels-scanner.com

trivago

Protecting the Most valuable Asset - Data

- Competitors' bots are extracting your data:
  - Price comparison to beat your prices
  - Content Theft & Data Aggregation
  - Faux buyers:
    continuously creating but never completing reservations

AGENDA

radware
Every second counts

Scoping the Bot Problem

- **Bots Behavioral Attributes**

IP Agnostic Bot Detection

Single Request vs. Continuous Attacks

Single Request Attack

- SQL Injection
- XSS
- CSRF
- …

Continuous Attack

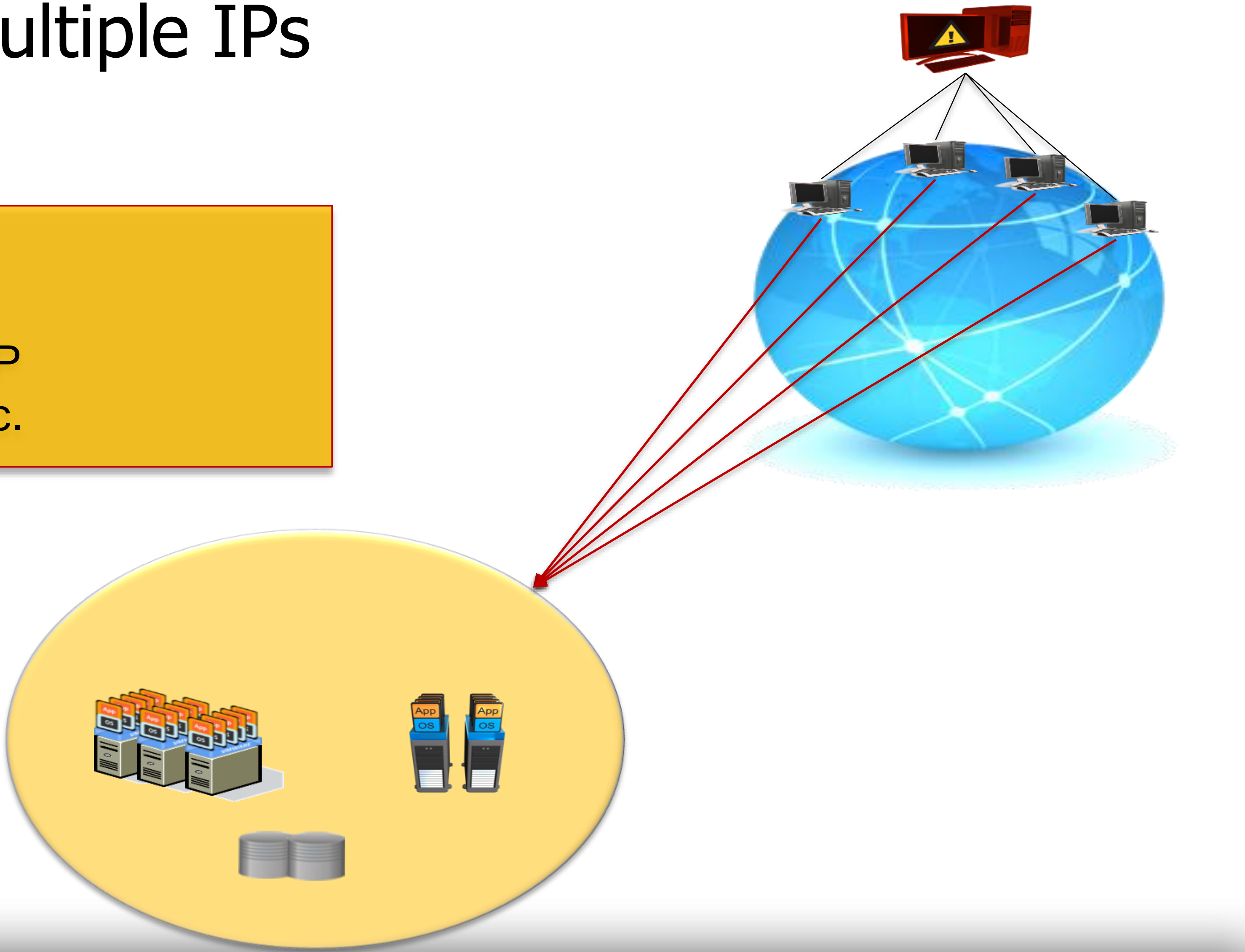
- Application DDoS
- Password Cracking / Brute Force
- Site Scraping / Data Harvesting
- Account Lockdown
- …

Commonly Used Frameworks

Single Source with multiple IPs

The Problem:

- Single Attack source
- Attacker **dynamically changes** its IP
- DHCP reset, Anonymous proxies etc.



AGENDA

Scoping the Bot Problem

Bots Behavioral Attributes

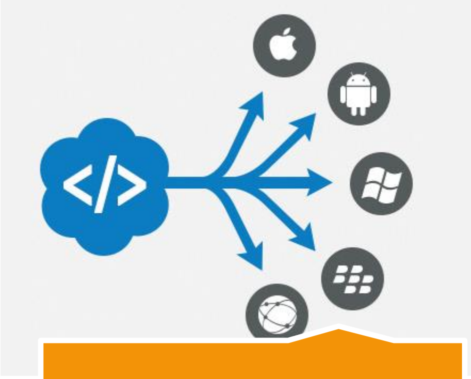
- IP Agnostic Bot Detection

radware
Every second counts

Solution Requirements

IP Agnostic

Unique

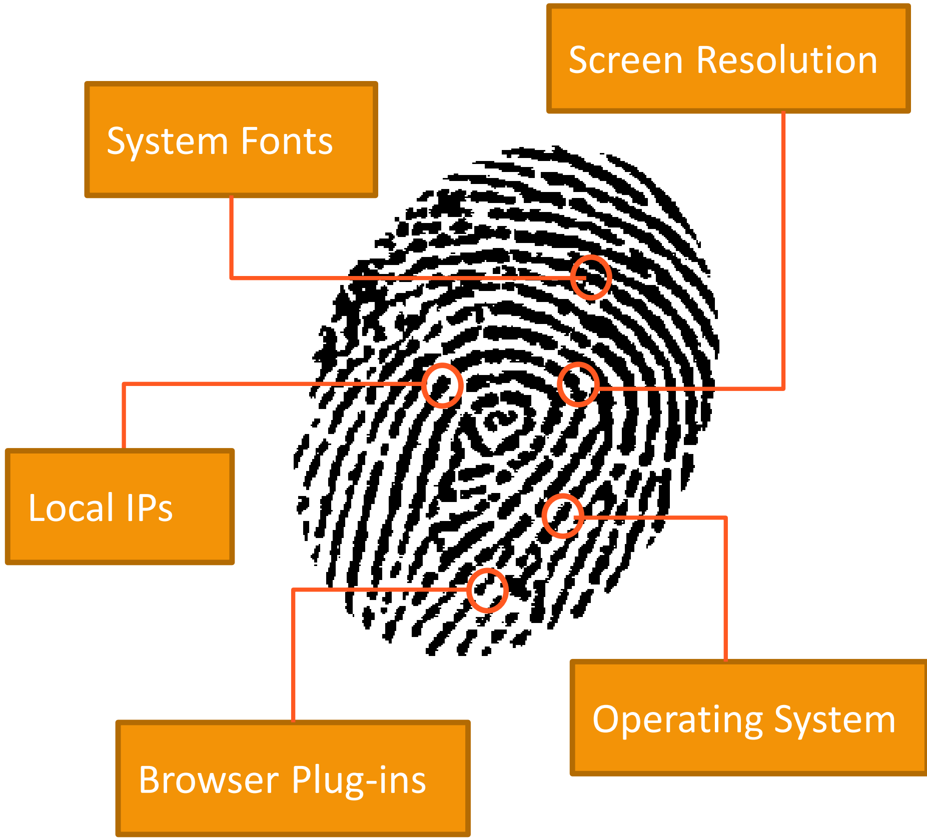


Cross Platform

Correlation

Device Fingerprint

- **Identify a browser/bot** through info collection.
- Dozens of browser attributes can be collected on the client side.
- JavaScript allows collecting detailed browser info.
- The power of the fingerprint is in the **consolidated information**.



How distinct does a fingerprint need to be?

- The current estimated world population: **7,477,780,179**.

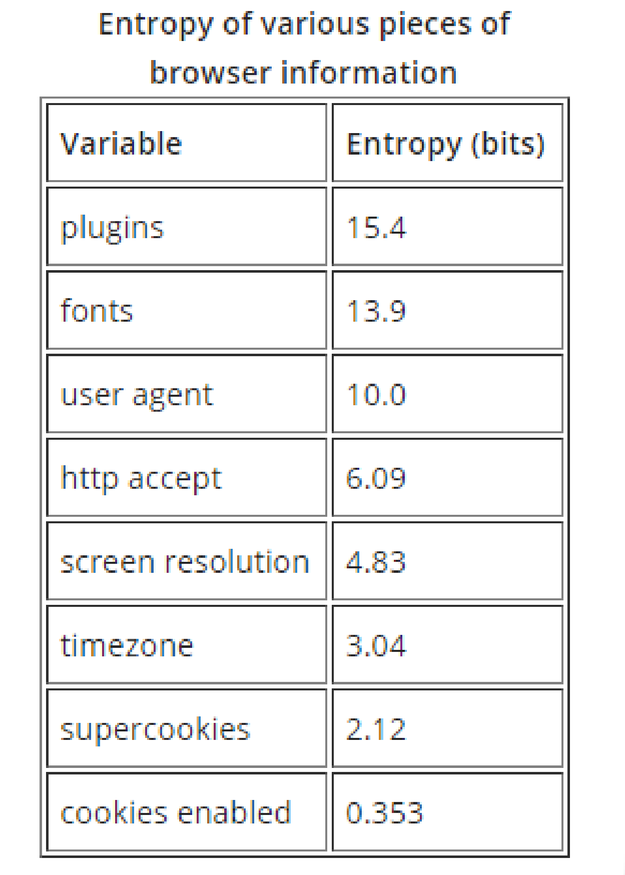
- **How many bits** of information are required to **uniquely identify** an individual from the entire population?

log2 (7,477,780,179) < 33

Entropy of Browser Fingerprint

To differentiate between 1,000,000 unique users, who access the secured environment requires 20 bits of information:

$$\mathbf{\log 2\ (1{,}000{,}000) < 20}$$



Entropy of various pieces of browser information

Variable	Entropy (bits)
plugins	15.4
fonts	13.9
user agent	10.0
http accept	6.09
screen resolution	4.83
timezone	3.04
supercookies	2.12
cookies enabled	0.353

JavaScript Variables

Navigator variable

- UserAgent
- App Name
- App Code Name
- App Version
- Build ID
- Platform
- CPU Class
- OS CPU
- Product
- Product Sub
- Vendor
- Vendor Sub
- Language
- User Language
- Browser Language
- System Language

Screen variable

- Screen W x H
- Available W x H
- Color Depth
- Pixel Depth
- Device DPI (X, Y)
- Logical DPI (X, Y)
- Update Interval
- System DPI (X, Y)

Other Fingerprinting Approaches

HTTP Headers

- User Agent
- Accept
- Accept-Language
- Accept-Charset
- Accept-Encoding
- X-FORWARDED-FOR
- TRUE-CLIENT-IP
- Via
- DNT (Do not track)

TCP Packet Parameters

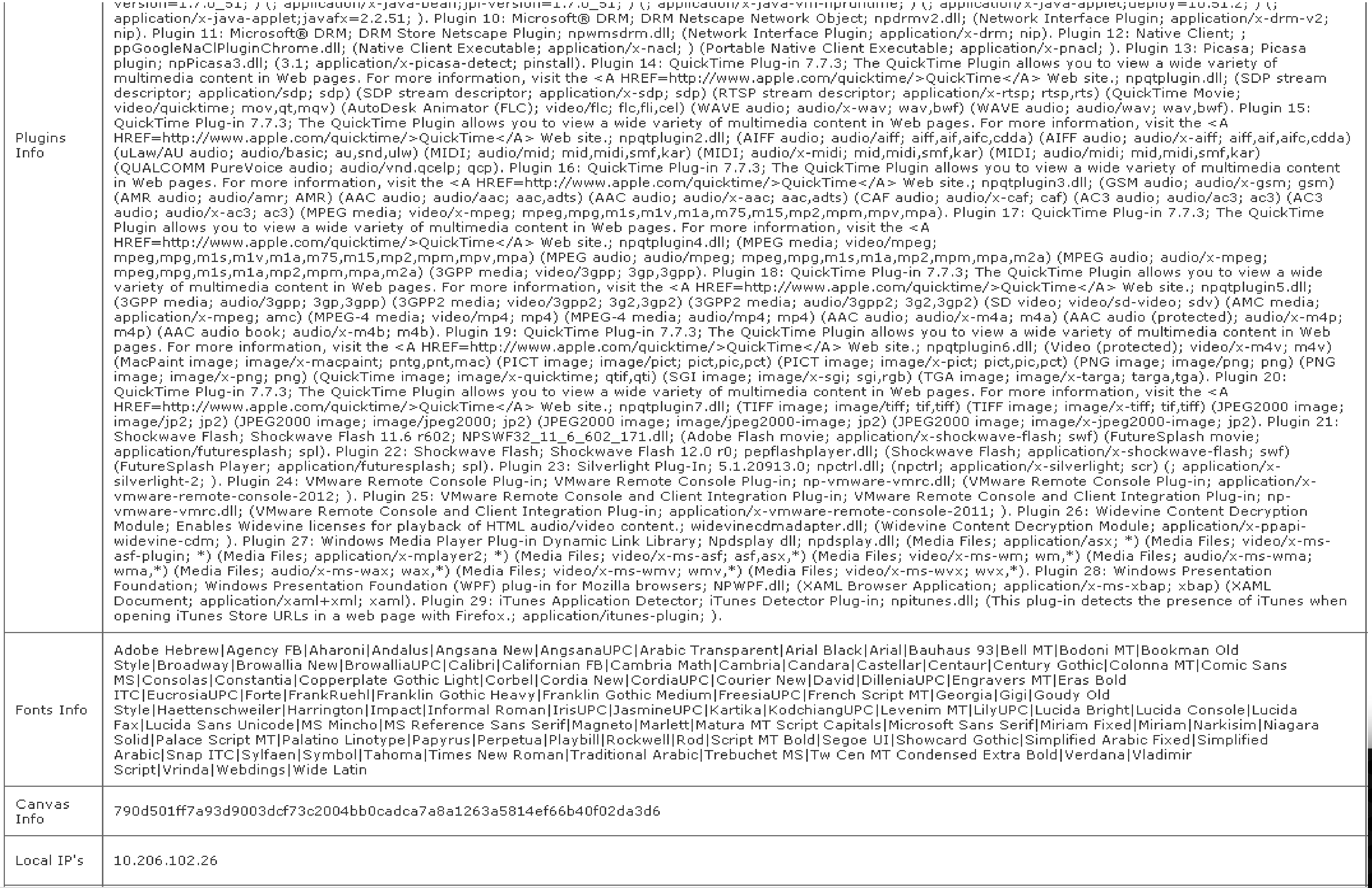
- Initial packet size
- IP Initial TTL
- TCP Window size
- Window scaling value
- Max segment size
- TCP Options
- IP flags
- IP Type of service
- IP Total Length
- "don't fragment" flag
- "sackOK" flag
- "nop" flag

navigator.plugins

```
for (plugin of navigator.plugins) { console.log(plugin.name); }

"Shockwave Flash‟
"QuickTime Plug-in 7.7.3‟
"Default Browser Helper‟
"Unity Player‟
"Google Earth Plug-in‟
"Silverlight Plug-In‟
"Java Applet Plug-in‟
"Adobe Acrobat NPAPI Plug-in, Version 11.0.02‟
"WacomTabletPlugin‟
```

Fingerprint Example

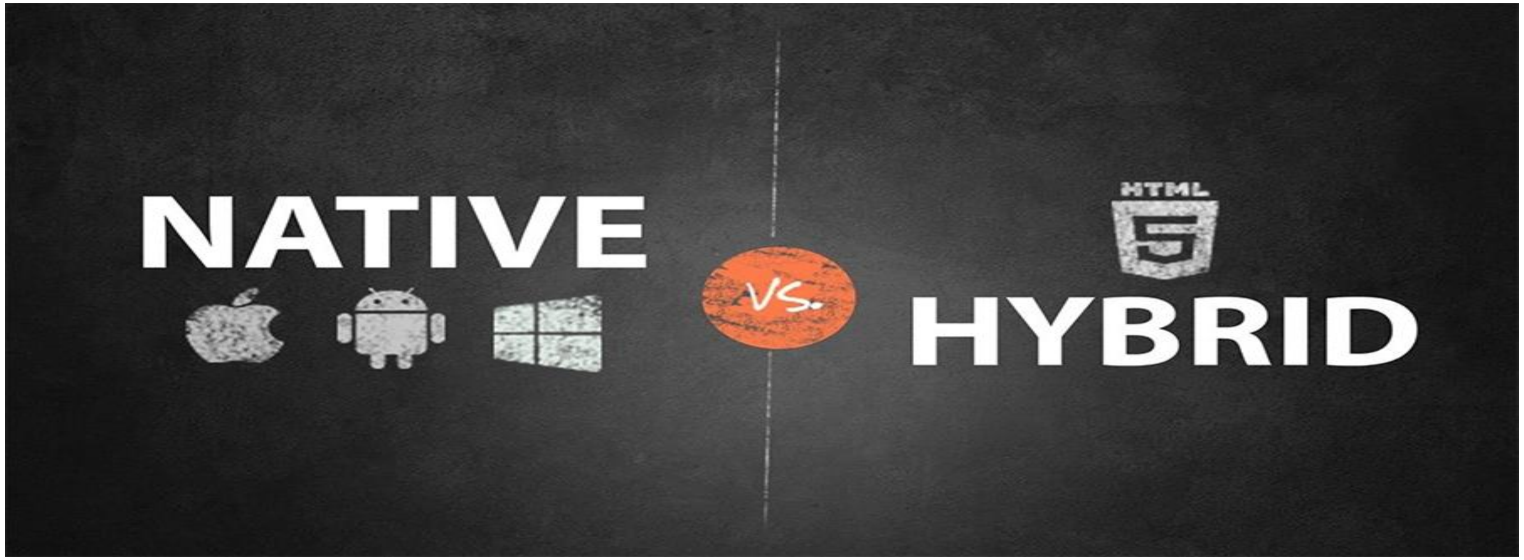


Plugins Info	version=1.7.0_51;) (; application/x-java-bean;jpi-version=1.7.0_51;) (; application/x-java-vm-npruntime;) (; application/x-java-applet;deploy=10.51.2;) (; application/x-java-applet;javafx=2.2.51;). Plugin 10: Microsoft® DRM; DRM Netscape Network Object; npdrmv2.dll; (Network Interface Plugin; application/x-drm-v2; nip). Plugin 11: Microsoft® DRM; DRM Store Netscape Plugin; npwmsdrm.dll; (Network Interface Plugin; application/x-drm; nip). Plugin 12: Native Client; ; ppGoogleNaClPluginChrome.dll; (Native Client Executable; application/x-nacl;) (Portable Native Client Executable; application/x-pnacl;). Plugin 13: Picasa; Picasa plugin; npPicasa3.dll; (3.1; application/x-picasa-detect; pinstall). Plugin 14: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin.dll; (SDP stream descriptor; application/sdp; sdp) (SDP stream descriptor; application/x-sdp; sdp) (RTSP stream descriptor; application/x-rtsp; rtsp,rts) (QuickTime Movie; video/quicktime; mov,qt,mqv) (AutoDesk Animator (FLC); video/flc; flc,fli,cel) (WAVE audio; audio/x-wav; wav,bwf) (WAVE audio; audio/wav; wav,bwf). Plugin 15: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin2.dll; (AIFF audio; audio/aiff; aiff,aif,aifc,cdda) (AIFF audio; audio/x-aiff; aiff,aif,aifc,cdda) (uLaw/AU audio; audio/basic; au,snd,ulw) (MIDI; audio/mid; mid,midi,smf,kar) (MIDI; audio/x-midi; mid,midi,smf,kar) (MIDI; audio/midi; mid,midi,smf,kar) (QUALCOMM PureVoice audio; audio/vnd.qcelp; qcp). Plugin 16: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin3.dll; (GSM audio; audio/x-gsm; gsm) (AMR audio; audio/amr; AMR) (AAC audio; audio/aac; aac,adts) (AAC audio; audio/x-aac; aac,adts) (CAF audio; audio/x-caf; caf) (AC3 audio; audio/ac3; ac3) (AC3 audio; audio/x-ac3; ac3) (MPEG media; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa). Plugin 17: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin4.dll; (MPEG media; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (MPEG audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a) (MPEG audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a) (3GPP media; video/3gpp; 3gp,3gpp). Plugin 18: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin5.dll; (3GPP media; audio/3gpp; 3gp,3gpp) (3GPP2 media; video/3gpp2; 3g2,3gp2) (3GPP2 media; audio/3gpp2; 3g2,3gp2) (SD video; video/sd-video; sdv) (AMC media; application/x-mpeg; amc) (MPEG-4 media; video/mp4; mp4) (MPEG-4 media; audio/mp4; mp4) (AAC audio; audio/x-m4a; m4a) (AAC audio (protected); audio/x-m4p; m4p) (AAC audio book; audio/x-m4b; m4b). Plugin 19: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin6.dll; (Video (protected); video/x-m4v; m4v) (MacPaint image; image/x-macpaint; pntg,pnt,mac) (PICT image; image/pict; pict,pic,pct) (PICT image; image/x-pict; pict,pic,pct) (PNG image; image/png; png) (PNG image; image/x-png; png) (QuickTime image; image/x-quicktime; qtif,qti) (SGI image; image/x-sgi; sgi,rgb) (TGA image; image/x-targa; targa,tga). Plugin 20: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin7.dll; (TIFF image; image/tiff; tif,tiff) (TIFF image; image/x-tiff; tif,tiff) (JPEG2000 image; image/jp2; jp2) (JPEG2000 image; image/jpeg2000; jp2) (JPEG2000 image; image/jpeg2000-image; jp2) (JPEG2000 image; image/x-jpeg2000-image; jp2). Plugin 21: Shockwave Flash; Shockwave Flash 11.6 r602; NPSWF32_11_6_602_171.dll; (Adobe Flash movie; application/x-shockwave-flash; swf) (FutureSplash movie; application/futuresplash; spl). Plugin 22: Shockwave Flash; Shockwave Flash 12.0 r0; pepflashplayer.dll; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 23: Silverlight Plug-In; 5.1.20913.0; npctrl.dll; (npctrl; application/x-silverlight; scr) (; application/x-silverlight-2;). Plugin 24: VMware Remote Console Plug-in; VMware Remote Console Plug-in; np-vmware-vmrc.dll; (VMware Remote Console Plug-in; application/x-vmware-remote-console-2012;). Plugin 25: VMware Remote Console and Client Integration Plug-in; VMware Remote Console and Client Integration Plug-in; np-vmware-vmrc.dll; (VMware Remote Console and Client Integration Plug-in; application/x-vmware-remote-console-2011;). Plugin 26: Widevine Content Decryption Module; Enables Widevine licenses for playback of HTML audio/video content.; widevinecdmadapter.dll; (Widevine Content Decryption Module; application/x-ppapi-widevine-cdm;). Plugin 27: Windows Media Player Plug-in Dynamic Link Library; Npdsplay dll; npdsplay.dll; (Media Files; application/asx; *) (Media Files; video/x-ms-asf-plugin; *) (Media Files; application/x-mplayer2; *) (Media Files; video/x-ms-asf; asf,asx,*) (Media Files; video/x-ms-wm; wm,*) (Media Files; audio/x-ms-wma; wma,*) (Media Files; audio/x-ms-wax; wax,*) (Media Files; video/x-ms-wmv; wmv,*) (Media Files; video/x-ms-wvx; wvx,*). Plugin 28: Windows Presentation Foundation; Windows Presentation Foundation (WPF) plug-in for Mozilla browsers; NPWPF.dll; (XAML Browser Application; application/x-ms-xbap; xbap) (XAML Document; application/xaml+xml; xaml). Plugin 29: iTunes Application Detector; iTunes Detector Plug-in; npitunes.dll; (This plug-in detects the presence of iTunes when opening iTunes Store URLs in a web page with Firefox.; application/itunes-plugin;).
Fonts Info	Adobe Hebrew|Agency FB|Aharoni|Andalus|Angsana New|AngsanaUPC|Arabic Transparent|Arial Black|Arial|Bauhaus 93|Bell MT|Bodoni MT|Bookman Old Style|Broadway|Browallia New|BrowalliaUPC|Calibri|Californian FB|Cambria Math|Cambria|Candara|Castellar|Centaur|Century Gothic|Colonna MT|Comic Sans MS|Consolas|Constantia|Copperplate Gothic Light|Corbel|Cordia New|CordiaUPC|Courier New|David|DilleniaUPC|Engravers MT|Eras Bold ITC|EucrosiaUPC|Forte|FrankRuehl|Franklin Gothic Heavy|Franklin Gothic Medium|FreesiaUPC|French Script MT|Georgia|Gigi|Goudy Old Style|Haettenschweiler|Harrington|Impact|Informal Roman|IrisUPC|JasmineUPC|Kartika|KodchiangUPC|Levenim MT|LilyUPC|Lucida Bright|Lucida Console|Lucida Fax|Lucida Sans Unicode|MS Mincho|MS Reference Sans Serif|Magneto|Marlett|Matura MT Script Capitals|Microsoft Sans Serif|Miriam Fixed|Miriam|Narkisim|Niagara Solid|Palace Script MT|Palatino Linotype|Papyrus|Perpetua|Playbill|Rockwell|Rod|Script MT Bold|Segoe UI|Showcard Gothic|Simplified Arabic Fixed|Simplified Arabic|Snap ITC|Sylfaen|Symbol|Tahoma|Times New Roman|Traditional Arabic|Trebuchet MS|Tw Cen MT Condensed Extra Bold|Verdana|Vladimir Script|Vrinda|Webdings|Wide Latin
Canvas Info	790d501ff7a93d9003dcf73c2004bb0cadca7a8a1263a5814ef66b40f02da3d6
Local IP's	10.206.102.26

Mobile App Support

NO ✗

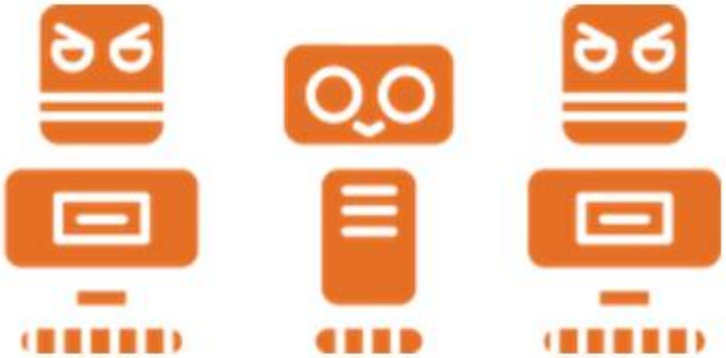
YES ✓



radware
Every second counts

Summary

What have we talked about?



- Scoping the Bot Problem
- Bots Behavioral Attributes
- IP Agnostic Bot Detection
- Device Fingerprint

radware

Every second counts

✉ michaelgro@radware.com

in https://il.linkedin.com/in/michaelgroskop