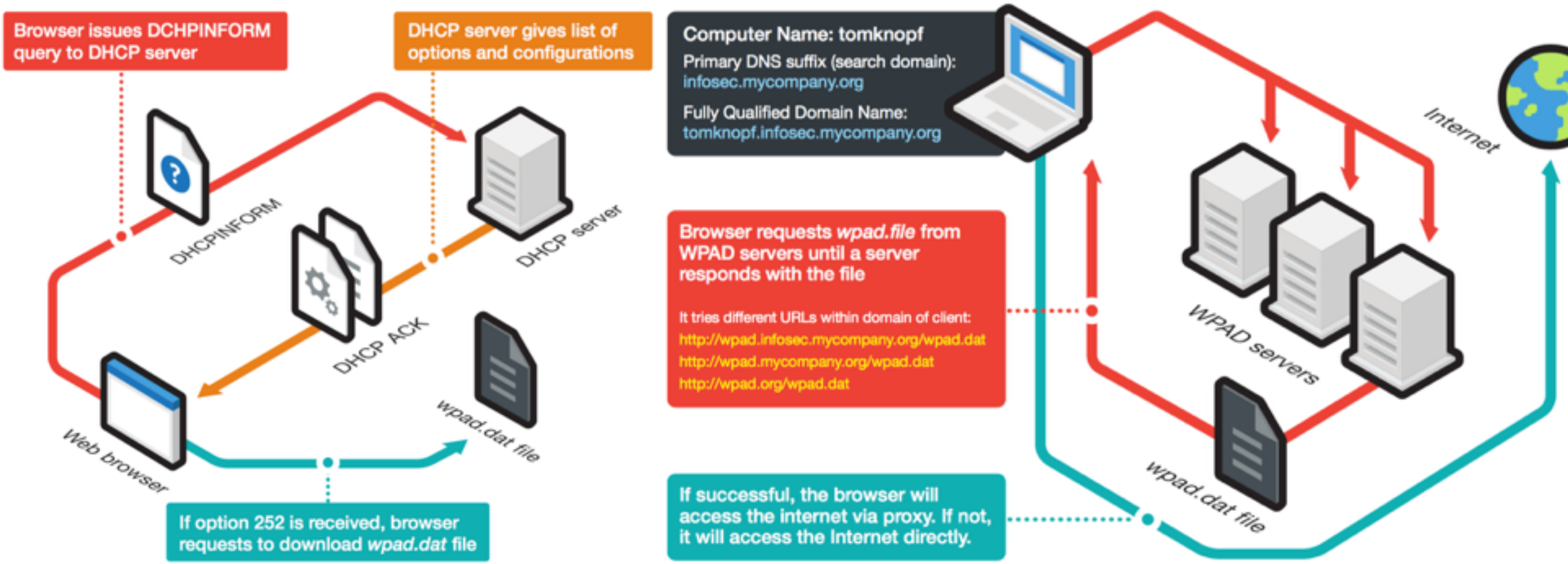
badWPAD

Maxim Goncharov

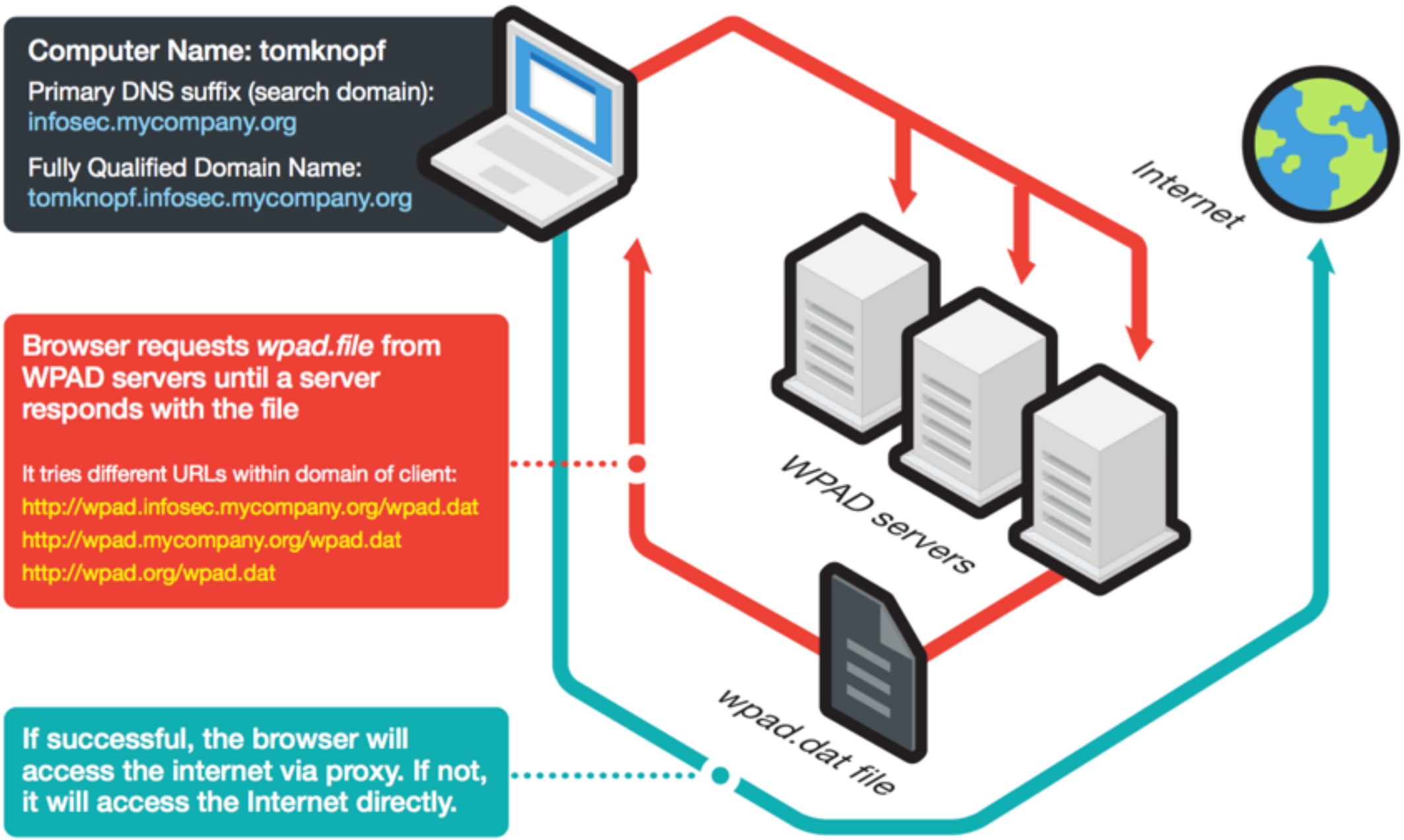
what is WPAD

1996 at Netscape Navigator 2.0

what is WPAD


Browser issues DCHPINFORM query to DHCP server
DHCP server gives list of options and configurations
DHCPINFORM
DHCP server
DHCP ACK
Web browser
wpad.dat file
If option 252 is received, browser requests to download wpad.dat file
Computer Name: tomknopf
Primary DNS suffix (search domain):
infosec.mycompany.org
Fully Qualified Domain Name:
tomknopf.infosec.mycompany.org
Browser requests wpad.file from WPAD servers until a server responds with the file
It tries different URLs within domain of client:
http://wpad.infosec.mycompany.org/wpad.dat
http://wpad.mycompany.org/wpad.dat
http://wpad.org/wpad.dat
If successful, the browser will access the internet via proxy. If not, it will access the Internet directly.
Internet
WPAD servers
wpad.dat file

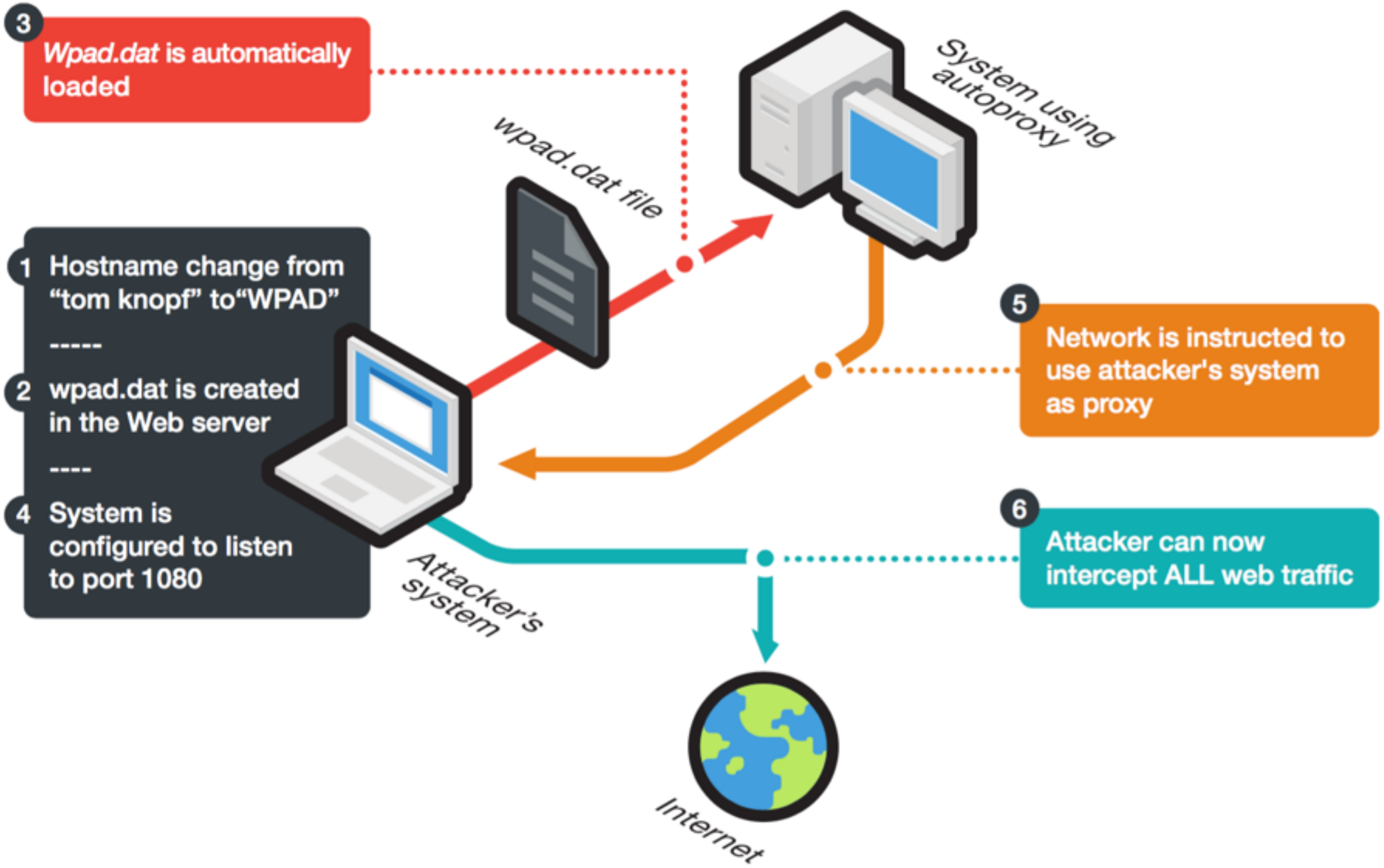
what is WPAD


Computer Name: tomknopf
Primary DNS suffix (search domain):
infosec.mycompany.org
Fully Qualified Domain Name:
tomknopf.infosec.mycompany.org
Internet
WPAD servers
wpad.dat file
Browser requests wpad.file from WPAD servers until a server responds with the file
It tries different URLs within domain of client:
http://wpad.infosec.mycompany.org/wpad.dat
http://wpad.mycompany.org/wpad.dat
http://wpad.org/wpad.dat
If successful, the browser will access the internet via proxy. If not, it will access the Internet directly.

what is WPAD

```
3.168 - - [06/Sep/2015:11:50:34 +200] “GET /wpad.dat HTTP/1.1” 200 303 “-” “-”
3.168 - - [06/Sep/2015:11:50:34 +200] “GET /wpad.dat HTTP/1.1” 200 303 “-” “-”
3.168 - - [06/Sep/2015:11:50:34 +200] “GET /wpad.dat HTTP/1.1” 200 303 “-” “-”
3.168 - - [06/Sep/2015:11:50:35 +200] “GET /wpad.dat HTTP/1.1” 200 303 “-” “-”
3.168 - - [06/Sep/2015:11:50:35 +200] “GET /wpad.dat HTTP/1.1” 200 303 “-” “-”
3.168 - - [06/Sep/2015:11:50:35 +200] “GET /wpad.dat HTTP/1.1” 200 303 “-” “-”
96.103 - - [06/Sep/2015:11:51:19 +200] “GET /wpad.dat HTTP/1.1” 200 304 “-” Mozilla/5.0 (Wi
2454.85 Safari/537.36”
0.253 - - [06/Sep/2015:11:51:28 +200] “GET /wpad.dat HTTP/1.1” 200 304 “-” “WinHTTP-Autopro
96.103 - - [06/Sep/2015:11:51:29 +200] “GET /wpad.dat HTTP/1.1” 200 248 “-” Mozilla/5.0 (co
96.103 - - [06/Sep/2015:11:52:29 +200] “GET /wpad.dat HTTP/1.1” 200 248 “-” Mozilla/5.0 (co
3.168 - - [06/Sep/2015:11:53:34 +200] “GET /wpad.dat HTTP/1.1” 304 178 “-” Mozilla/5.0 (com
208.242 - - [06/Sep/2015:11:53:42 +200] “GET /wpad.dat HTTP/1.1” 200 248 “-” Mozilla/4.0 (c
02.130 - - [06/Sep/2015:11:53:47 +200] “GET /wpad.dat HTTP/1.1” 200 248 “-” Mozilla/4.0 (co
```

WPAD experiment #1



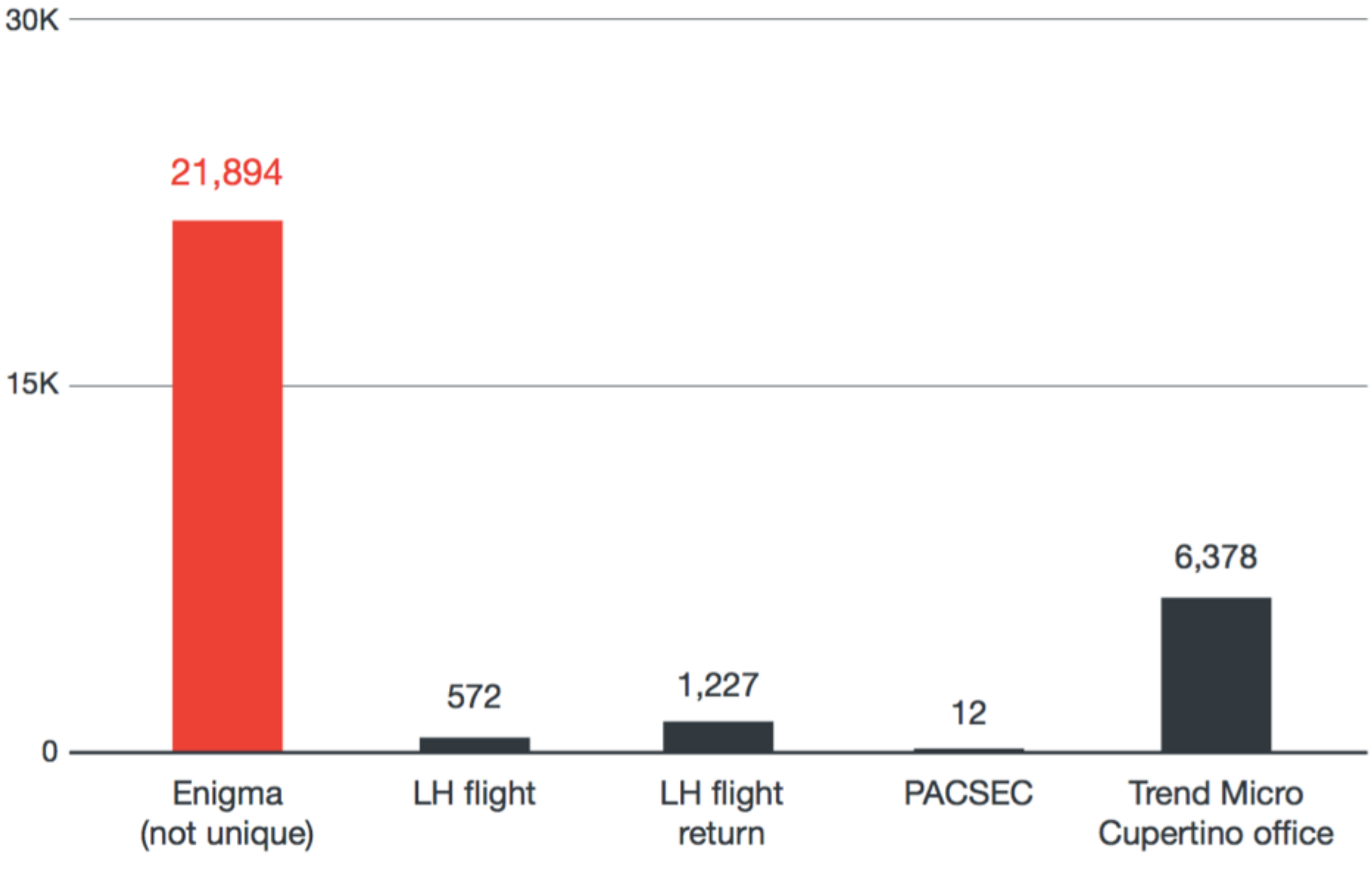
1


Lufthansa
Senator Lounge
Business Lounge
STAR ALLIANCE
GOLD
2
Lufthansa


3
Lufthansa
HotSpot
Politik
Wirtschaft
Panorama
Sport

4

WPAD experiment #1



WPAD experiment #2

Statistics for	Unique visitors	Number of visits	Pages	Hits	Bandwidth
wpad.am	29 882	69 388	2 137 799	2 137 820	381.40 MB
direct	25 816	76 543	4 443 553	4 447 628	963.06 MB
wpad.cm	1 006	4 473	262 637	262 638	51.07 MB
wpad.media	667	4 962	1 492 337	1 492 394	297.21 MB
wpad.pub	633	1 929	52 064	52 154	9.84 MB
wpad.fm	483	1 885	260 274	260 320	50.59 MB
wpad.to	313	1 897	56 206	56 215	10.15 MB
wpad.video	268	1 615	2 159 710	2 159 799	451.23 MB
wpad.education	218	843	80 277	80 340	14.10 MB
wpad.technology	178	705	58 703	58 801	10.76 MB
wpad.today	162	639	49 311	49 392	8.26 MB
wpad.run	133	609	519 738	519 776	90.01 MB
wpad.limited	110	400	24 607	24 692	5.18 MB
wpad.news	60	427	23 522	23 559	4.66 MB
wpad.email	59	139	32 438	32 506	6.40 MB
wpad.university	57	202	22 529	22 617	4.35 MB
Total	60 045	166 656	11 675 705	11 680 651	2.30 GB

WPAD experiment #2

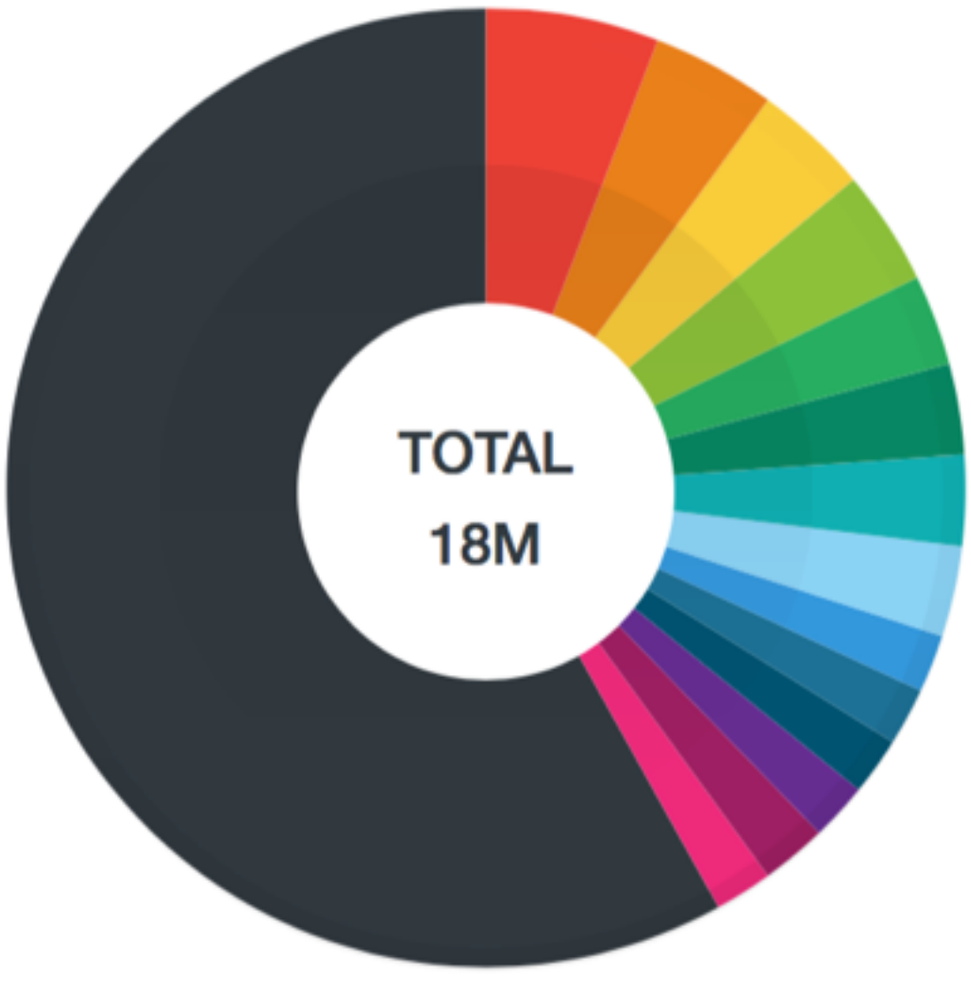
1. root@ip-172-31-13-203: ~ (ssh)

```
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:24 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:24 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:24 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:24 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:24 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:25 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
pad.pub:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 224 "-" "WinHttp-Autoproxy-Service/5.1"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:26 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:27 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:27 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:27 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:27 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 78.11.82.102 - - [18/Oct/2015:19:28:27 +0000] "GET /wpad.dat HTTP/1.1" 200 222 "-" "-"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:27 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
pad.media:80 37.231.90.250 - - [18/Oct/2015:19:28:27 +0000] "GET /wpad.dat HTTP/1.1" 200 224 "-" "Mozilla/5.0 (compatible; IE 11.0; Win64; Trident/7.0)"
p-172-31-13-203.eu-west-1.compute.internal:80 212.71.154.57 - - [18/Oct/2015:19:28:28 +0000] "GET /wpad.dat HTTP/1.1" 200 223 "-" "-"
```

WPAD experiment #2

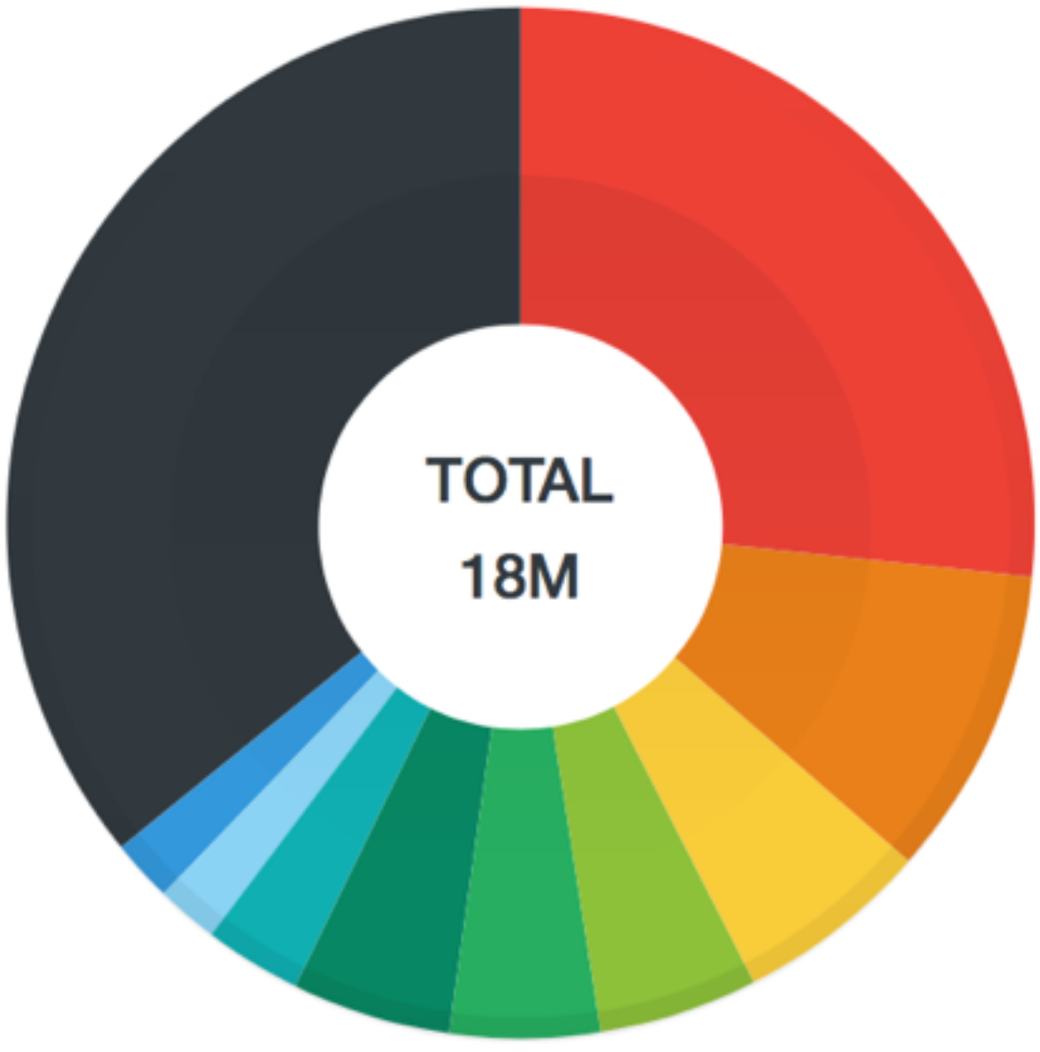
User Agent	Update client count
WindowsUpdateAgent	29,171
AAM%20Updates%20Notifier/1.0.162.0 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)	59
AAM%20Updates%20Notifier/1.0.162.0 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)	57
AAM%20Updates%20Notifier/1.0.162.0 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)	42
avast! Emergency Update Agent	9
XProtectUpdater (unknown version) CFNetwork/596.6.4 Darwin/12.6.0 (x86_64) (MacBookAir5%2C2)	7
Software%20Update (unknown version) CFNetwork/596.6.4 Darwin/12.6.0 (x86_64) (MacBookAir5%2C2)	7
Microsoft%20AutoUpdate/2.3.6 CFNetwork/720.5.7 Darwin/14.5.0 (x86_64)	7
XProtectUpdater (unknown version) CFNetwork/454.12.4 Darwin/10.8.0 (i386) (MacBookPro2%2C2)	6
GoogleSoftwareUpdateAgent/1.2.2.428 CFNetwork/596.6.4 Darwin/12.6.0 (x86_64) (MacBookPro8%2C1)	3
GoogleSoftwareUpdateAgent/1.2.2.428 CFNetwork/596.6.4 Darwin/12.6.0 (x86_64) (MacBookPro8%2C1)	29,368

WPAD experiment #2



Comcast, US	6%
Netia SA, PL	4%
IDOM Technologies, FR	4%
Shaw Communications, CA	4%
Telstra Europe, UK	3%
TW Telecom Holdings, US	3%
Liberty Global Operations, AT	3%
Bell Canada, CA	3%
National Internet Backbone, IN	2%
Cox Communications, US	2%
Emirates Telecommunications, AE	2%
Hughes Network Systems, US	2%
GIN Ipex, CZ	2%
T-Mobile USA, US	2%
Others	58%

WPAD experiment #2



United States	27%
Canada	10%
Poland	6%
India	5%
United Kingdom	5%
France	5%
Russia	3%
Australia	2%
Hungary	2%
Brazil	2%
Others	33%

WPAD experiment #2

Specified	57%
Unidentified	43%

WPAD experiment #3

know your target

register TLD

attack

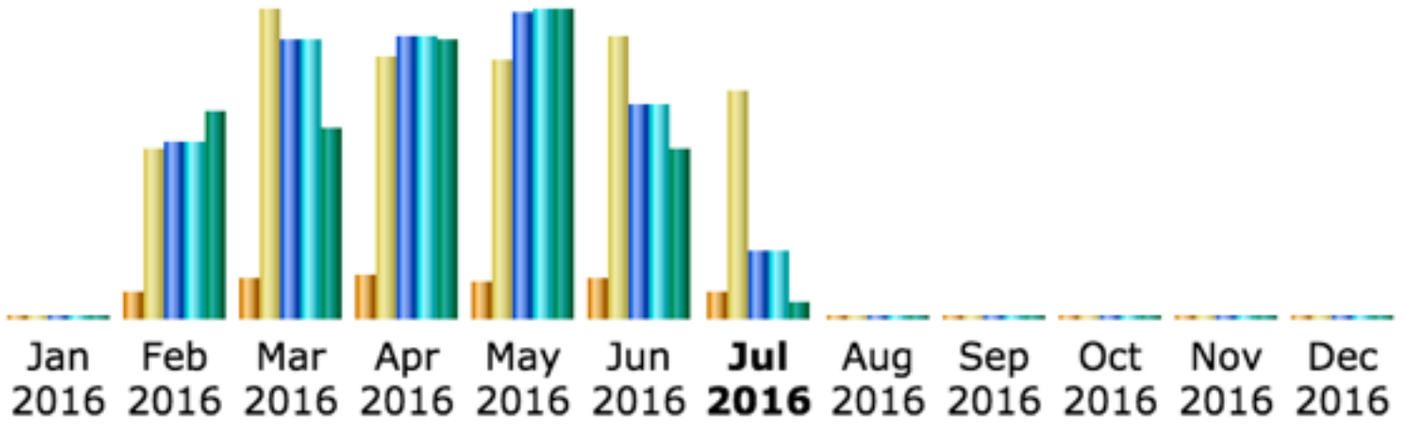
WPAD experiment #3

tokyo area orgs

wpad.tokyo

attack

WPAD experiment #3



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2016	0	0	0	0	0
Feb 2016	230	1,565	8,069,757	8,070,202	1.65 GB
Mar 2016	361	2,822	12,719,884	12,720,009	1.52 GB
Apr 2016	399	2,408	12,900,202	12,900,470	2.22 GB
May 2016	319	2,365	14,118,936	14,119,056	2.46 GB
Jun 2016	359	2,576	9,772,524	9,772,565	1.35 GB
Jul 2016	246	2,071	2,997,977	2,998,018	132.68 MB
Aug 2016	0	0	0	0	0
Sep 2016	0	0	0	0	0
Oct 2016	0	0	0	0	0
Nov 2016	0	0	0	0	0
Dec 2016	0	0	0	0	0
Total	1,914	13,807	60,579,280	60,580,320	9.32 GB

WPAD experiment #3

Hosts (Top 10) - Full list - Last visit - Unresolved IP Address

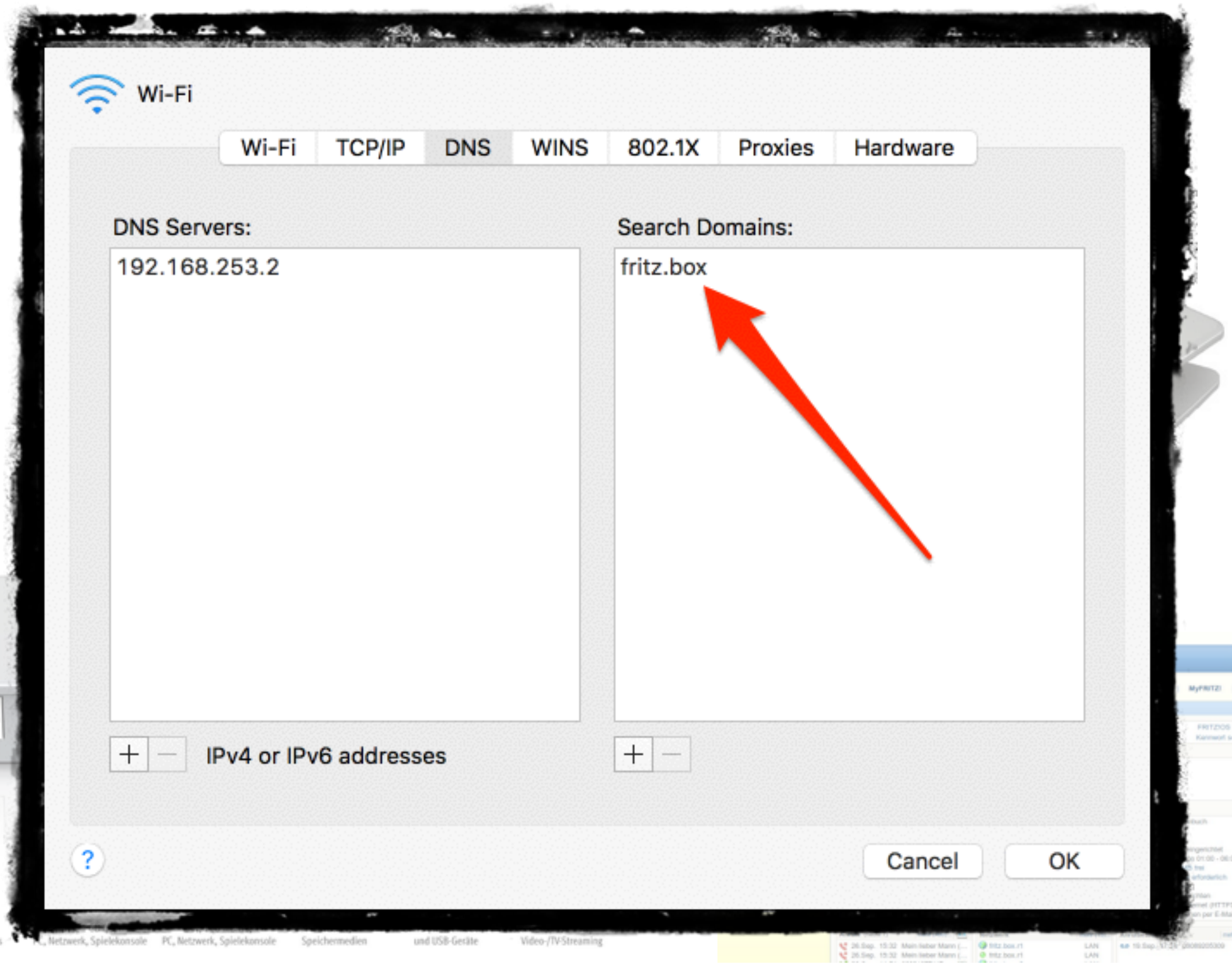
Hosts : 213 Known, 33 Unknown (unresolved ip) 246 Unique visitors	Pages	Hits	Bandwidth	Last visit
61.120.205.101	2,784,827	2,784,827	80.85 MB	25 Jul 2016 - 20:54
fs276ec986.tkyc513.ap.nuro.jp	62,191	62,191	13.18 MB	25 Jul 2016 - 20:52
c-71-195-187-136.hsd1.ca.comcast.net			11.67 MB	25 Jul 2016 - 20:54
p6023-ipngnfx01marunouchi.tokyo.ocn			9.54 MB	25 Jul 2016 - 20:42
61.206.119.125.static.zoot.jp			5.10 MB	25 Jul 2016 - 20:51
ec2-107-22-249-21.compute-1.amazon			3.05 MB	24 Jul 2016 - 19:36
157-14-171-121.tokyo.fdn.vectant.ne.jp	6,039	6,039	1.60 MB	25 Jul 2016 - 13:01
211127187154.cidr.odn.ne.jp	5,326	5,326	1.35 MB	25 Jul 2016 - 20:53
cpe-65-24-64-80.columbus.res.rr.com	4,471	4,471	1.29 MB	25 Jul 2016 - 20:51
p2388113-ipngn18001marunouchi.tokyo.ocn.ne.jp	3,784	3,784	1.02 MB	25 Jul 2016 - 20:54
Others	16,665	16,706	4.03 MB	

61.120.205.101

WPAD experiment #3

WPAD and Hardware

WPAD and Hardware

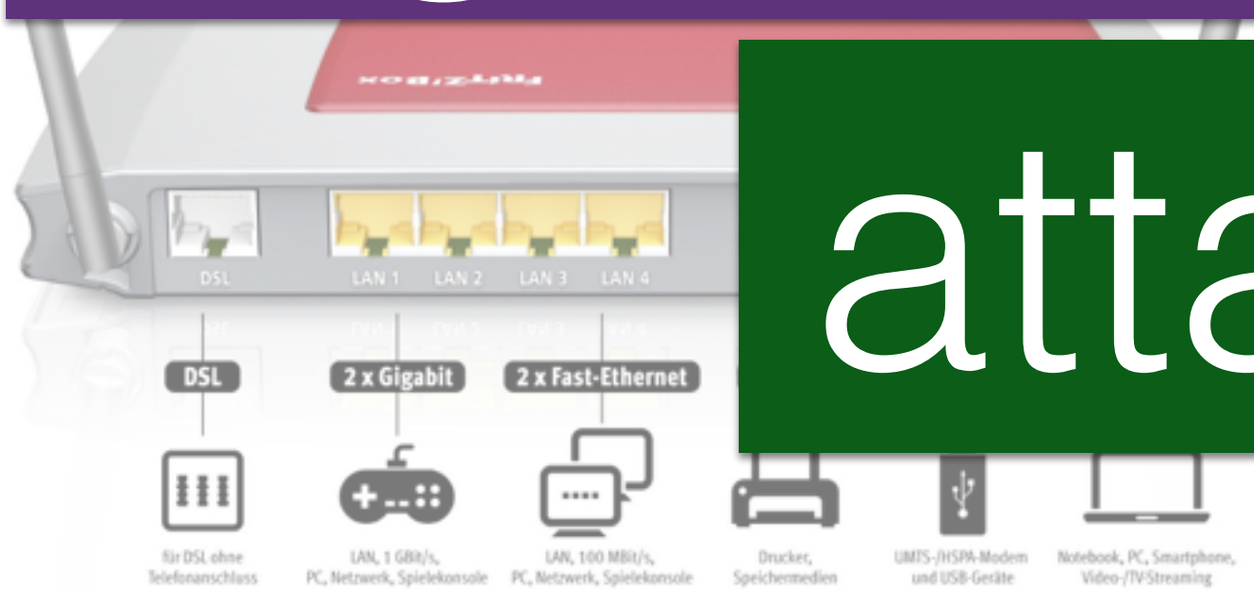


WPAD and Hardware

AVM

register fritz.box

attack



THANKS