badWPAD

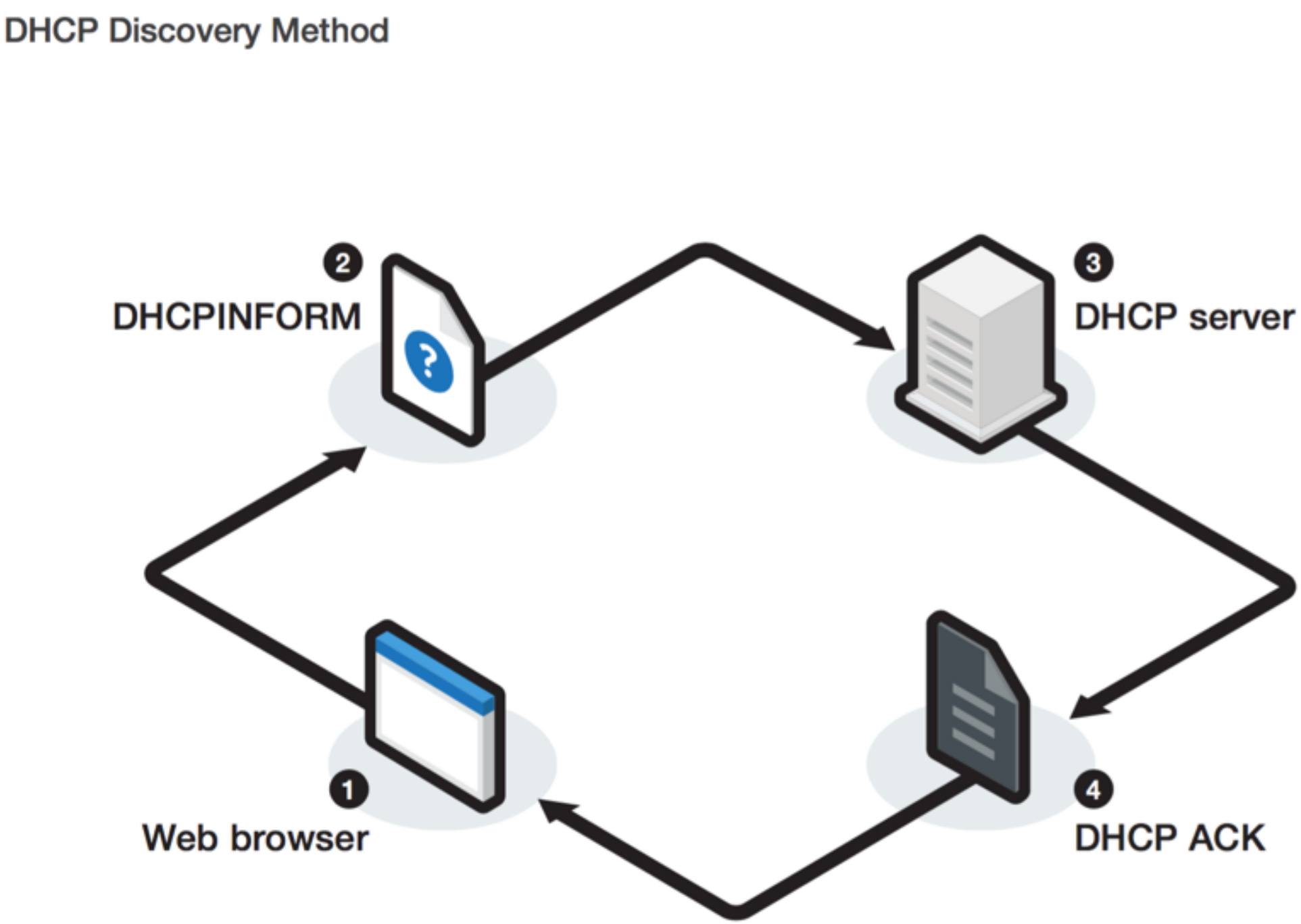
Maxim Goncharov

what is WPAD

1996 at Netscape Navigator 2.0

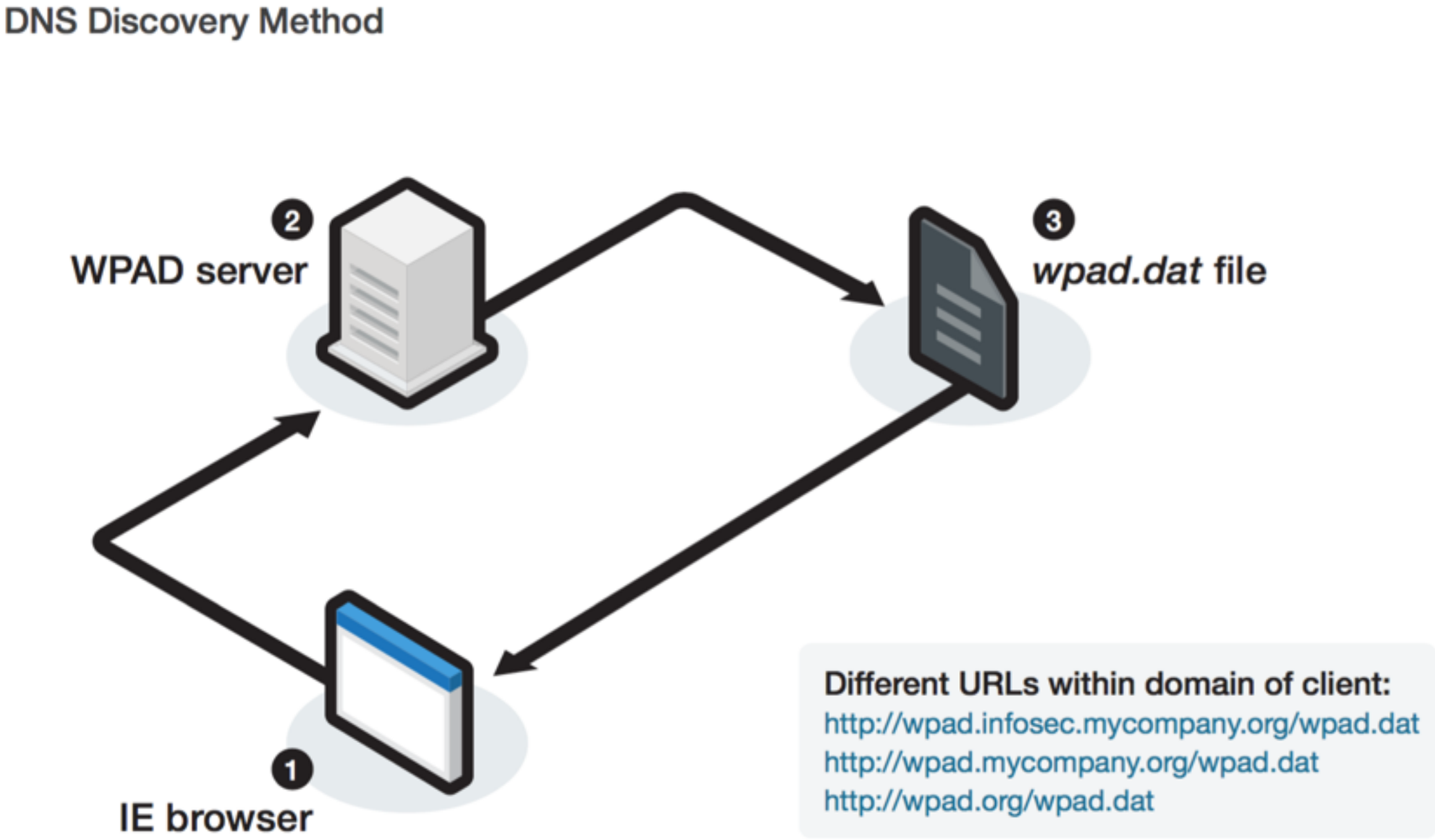
gmax@paranoid.email

what is WPAD



gmax@paranoid.email

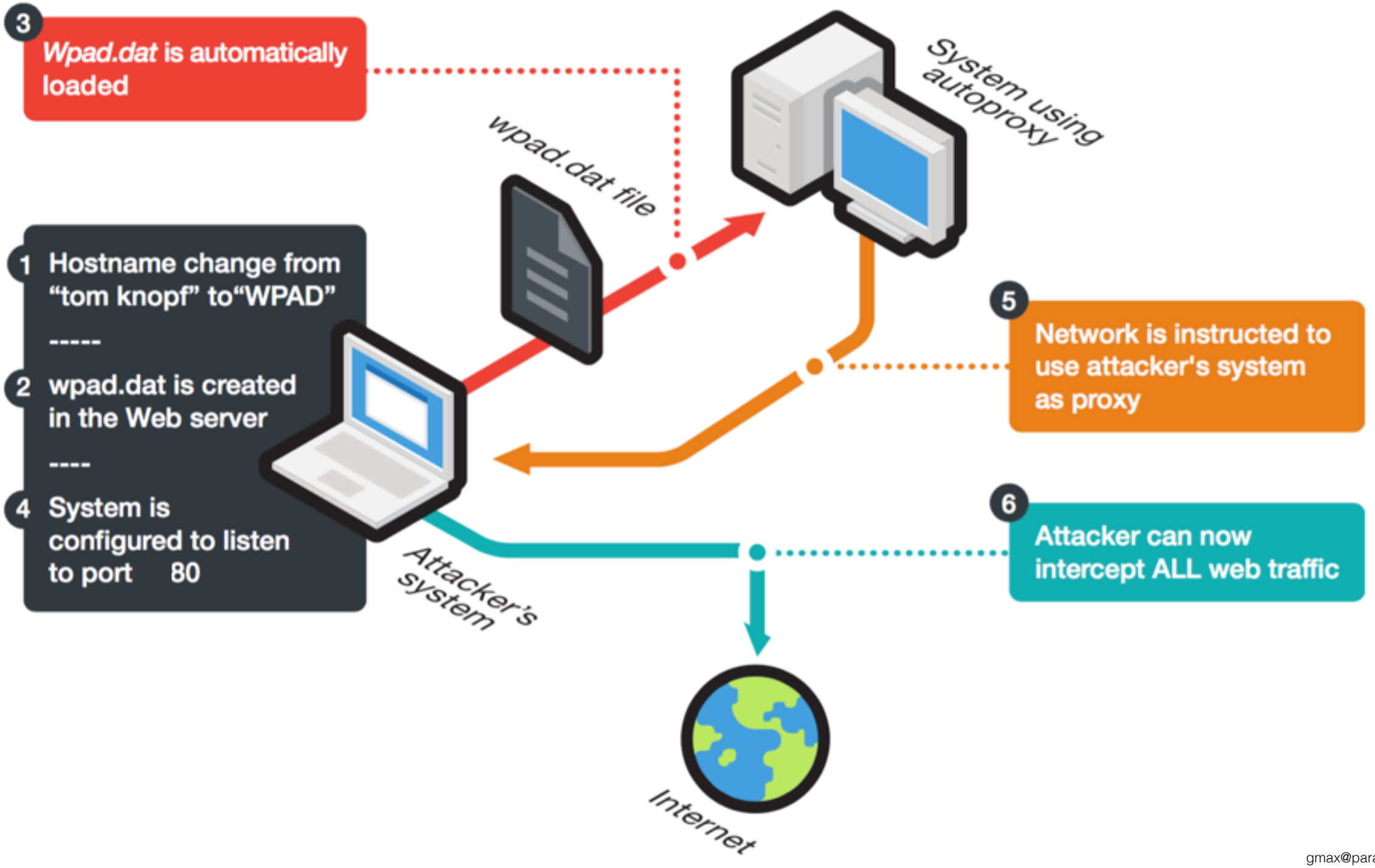
what is WPAD


DNS Discovery Method
2
WPAD server
3
wpad.dat file
1
IE browser
Different URLs within domain of client:
http://wpad.infosec.mycompany.org/wpad.dat
http://wpad.mycompany.org/wpad.dat
http://wpad.org/wpad.dat

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

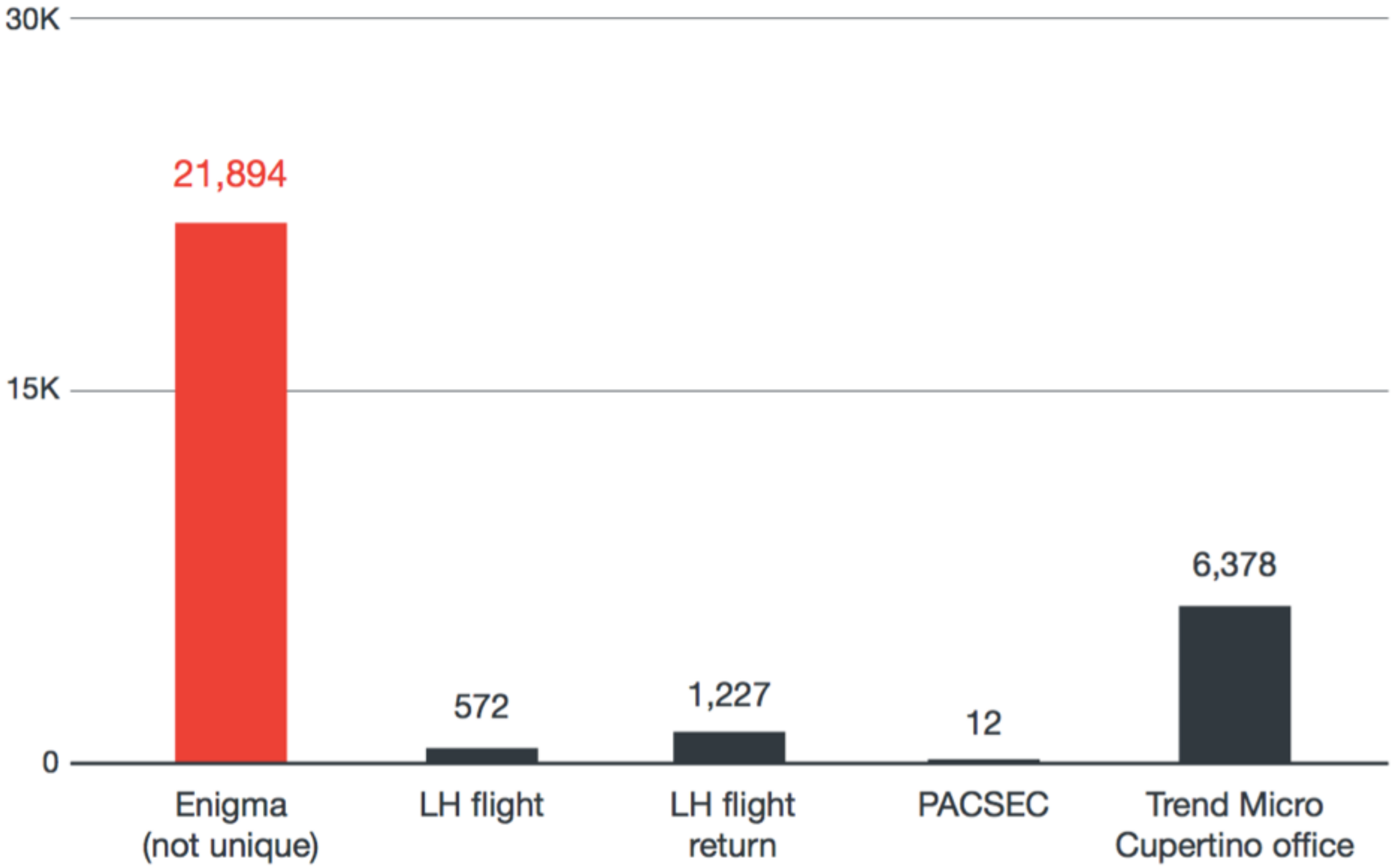

Lufthansa
Senator Lounge
Business Lounge
STAR ALLIANCE
GOLD
2
Lufthansa


3
Lufthansa
HotSpot
Politik
Wirtschaft
Panorama
Sport

4

5

WPAD experiment #1



gmax@paranoid.email

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

gmax@paranoid.email

wpad.de

Who is **Carsten Krueger** ?

Why he has bought wpad.de ?

His server provide **wpad.dat** file which looks legit

wpad.de - potential attack vector on german users

wpad.de/wpad.dat

```
function FindProxyForURL(url, host) {
   return "DIRECT";
}
```

```
Type: PERSON
Name: Carsten Krueger
Address: Foersterweg 5
PostalCode: 12353
City: Berlin
CountryCode: DE
Phone: +49306055774
Fax: +493066709417
Email: cakruege@gmail.com
Changed: 2009-02-17T17:48:48+01:00
```

gmax@paranoid.email

Weblock

The ultimate AdBlock solution for iOS is finally here!

Home | FAQ | WeBLOG

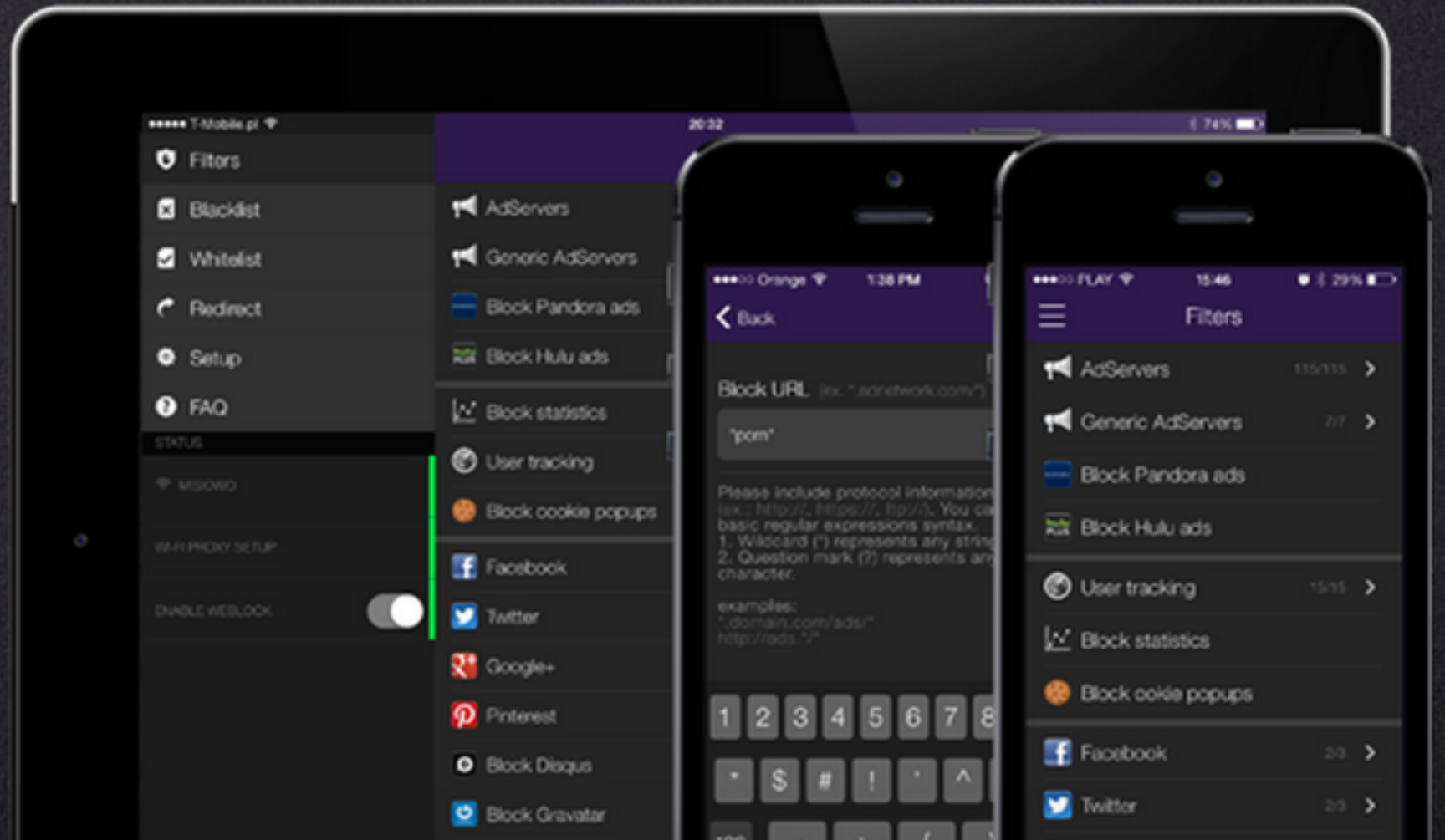
Block ads... and whatever you want.

On any iOS device, in any browser or app.

Like Share 15 Tweetnij 113

k app allows you to
rious types of online
ent while you are
nected to Wi-Fi

redefined filters or
your own rules to
t/whitelist any URL,
ain, IP or network



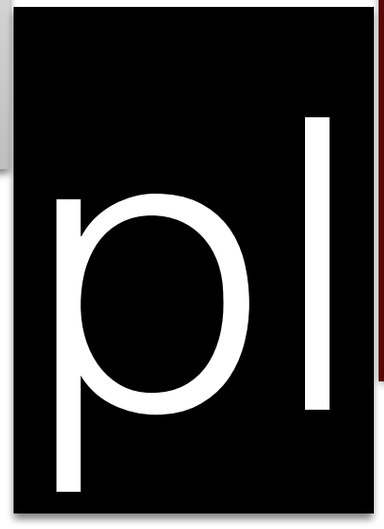
Block web and m
advertising (incud
app and video ads
browser or ap

Synchronise

24 TLDs

wpad.*/wpad.dat

wpad.cat
wpad.im
wpad.it
wpad.gr
wpad.cc
wpad.cz
wpad.ws
wpad.es
wpad.ee
wpad.info
wpad.pro
wpad.sk
wpad.name
wpad.xxx
wpad.be
wpad.tv
wpad.pl
wpad.lv
wpad.tw
wpad.com.co
wpad.com.tw
wpad.net.cn
wpad.org.cn
wpad.ws



gmax@paranoid.email

DANGER?

tomasz koperski

DOMAINTOOLS PROFILE CONNECT MONITOR ACQUIRE SUPPORT Whois Lookup

Whois Record for WpAd.tw

Whois & Quick Stats

Risk Score	5.27	
Email	admin@tek.pl is associated with ~9 domains	
Registrant Org	Tomasz Koperski is associated with ~42 other domains	
Dates	Created on 2007-07-27 - Expires on 2017-07-27	Whois History
IP Address	144.76.184.43 - 73 other sites hosted on this server	
IP Location	- Bayern - Nuremberg - Hetzner Online Ag	
ASN	AS24940 HETZNER-AS , DE (registered Jun 03, 2002)	
Domain Status	Registered And Active Website	
Whois History	36 records have been archived since 2009-09-28	
Whois Server	whois.twnic.net.tw	

Why?

tomasz koperski

wpad.cat
wpad.im
wpad.it
wpad.gr
wpad.cc
wpad.cz
wpad.ws
wpad.es
wpad.ee
wpad.info
wpad.pro
wpad.sk
wpad.name
wpad.xxx
wpad.be
wpad.tv
wpad.pl
wpad.lv
wpad.com.co
wpad.tw
wpad.com.tw
wpad.net.cn
wpad.org.cn
wpad.ws

tw

com.tw

NET.CN

org.cn

gmax@paranoid.email

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

79.000.000 hits

400.000 unique

gmax@paranoid.email

WPAD experiment #2

user agents

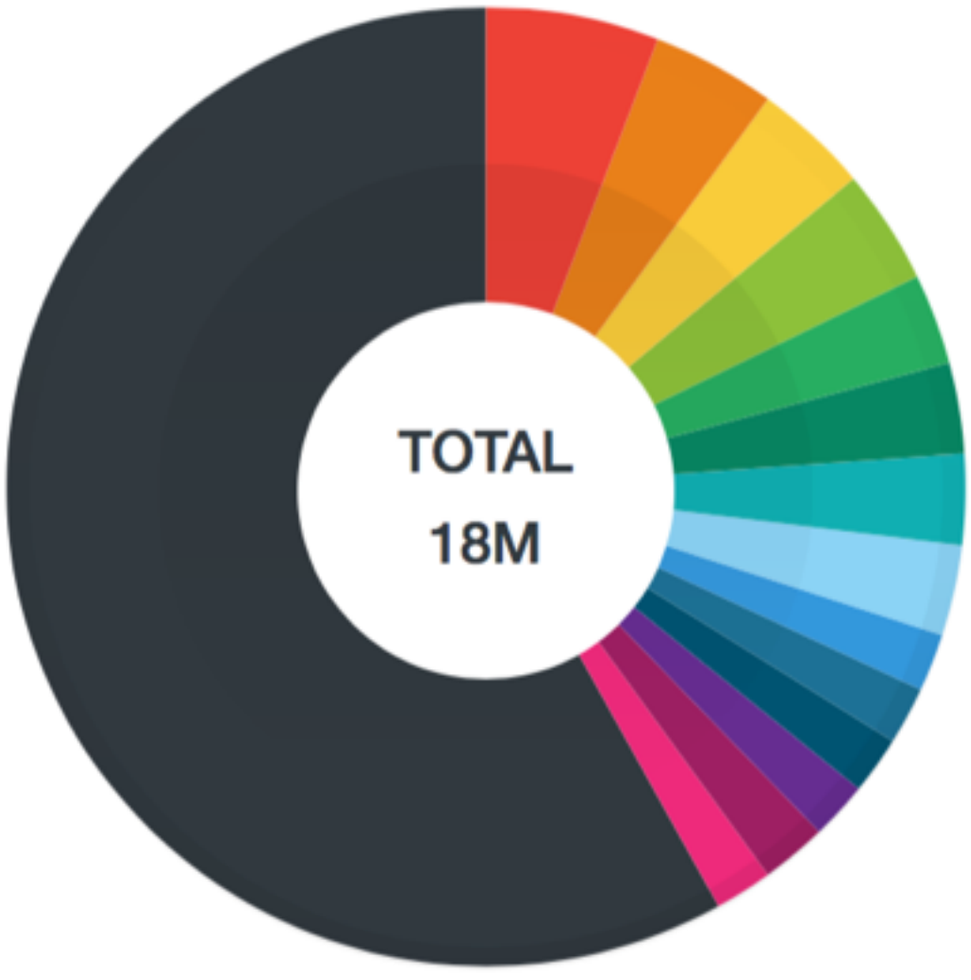
Specified	57%
Unidentified	43%

gmax@paranoid.email

Total_Count	user_agent_zoom
10963610	Empty UA
7476593	Mozilla/
2915311	WinHttp-Autoproxy-Service/
338471	networkd (unknown version) CFNetwork/
67661	Java/
44172	locationd/
38804	securityd (unknown version) CFNetwork/
34355	Microsoft-CryptoAPI/
32182	owncloud/
31736	Microsoft-WebDAV-MiniRedir/
25755	kugou/
23934	apsd (unknown version) CFNetwork/
21435	syncdefaultsd (unknown version) CFNetwork/
20591	itunesstored (unknown version) CFNetwork/
19181	WeChat/
17579	WordsWithFriendsFreeiPad/
17308	WinHTTP AutoProxy /
13227	mediaserverd (unknown version) CFNetwork/
13065	ubd/
11447	%E9%85%B7%E6%88%91%E9%9F%B3%E4%B9%90/
10821	Mail/
9754	mstreamd/
7470	dataaccessd (unknown version) CFNetwork/
7382	DeviceHealth/
7036	%E5%A4%A9%E6%B0%97/
6587	mobileassetd (unknown version) CFNetwork/
6528	SXL/

gmax@paranoid.email

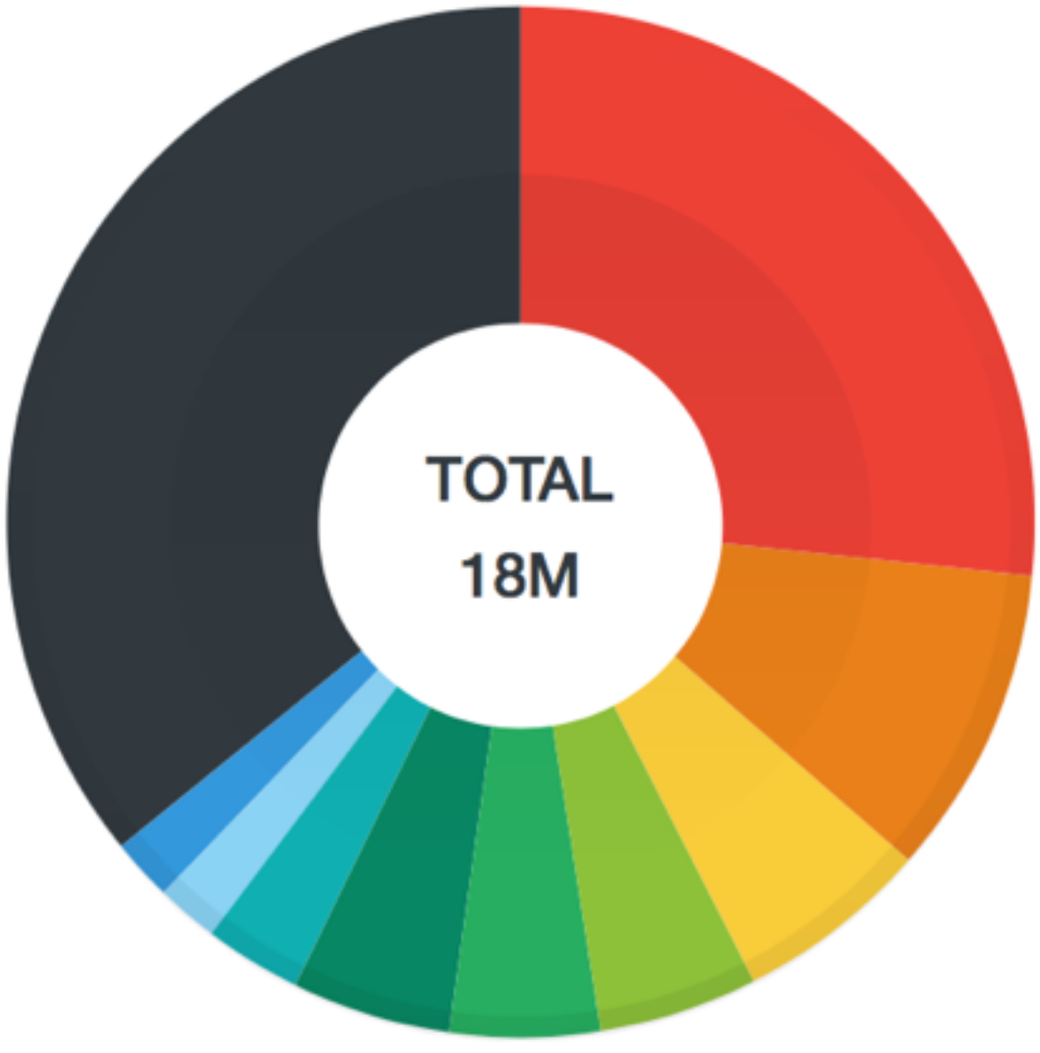
WPAD experiment #2



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%

gmax@paranoid.email

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%

gmax@paranoid.email

WPAD experiment #3

oldTLDs

newTLDs

gmax@paranoid.email

WPAD experiment #3

know your target

register TLD

attack

gmax@paranoid.email

WPAD experiment #3

know your target

gmax@paranoid.email

WPAD experiment #3

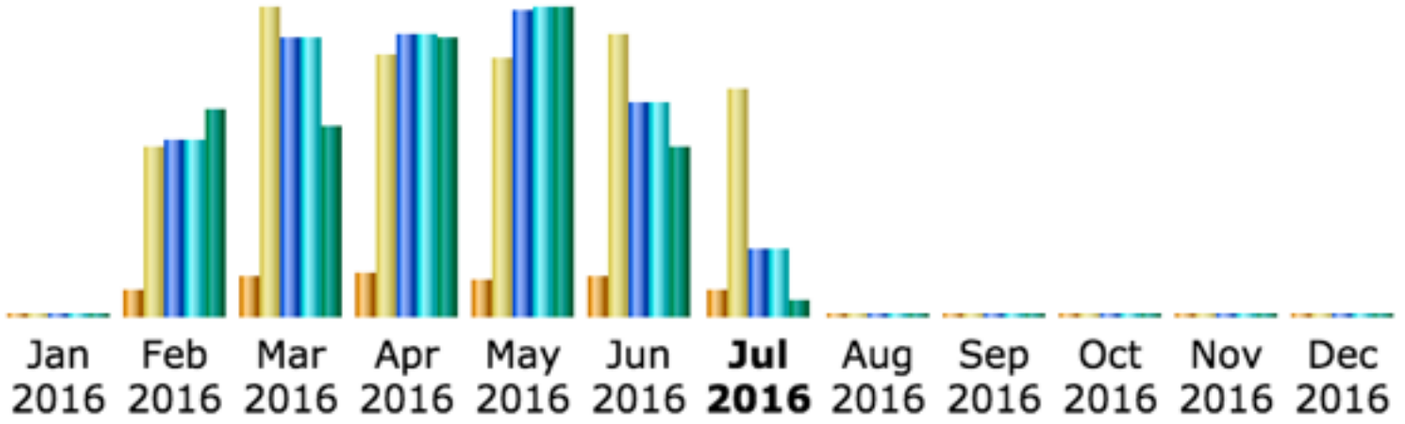
tokyo area orgs

wpad.tokyo

attack

gmax@paranoid.email

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

gmax@paranoid.email

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.hsd				Jul 2016 - 20:54
p6023-ipngnfx01maru				Jul 2016 - 20:42
61.206.119.125.static				Jul 2016 - 20:51
ec2-107-22-249-21.c				Jul 2016 - 19:36
157-14-171-121.toky				Jul 2016 - 13:01
211127187154.cidr.od				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	

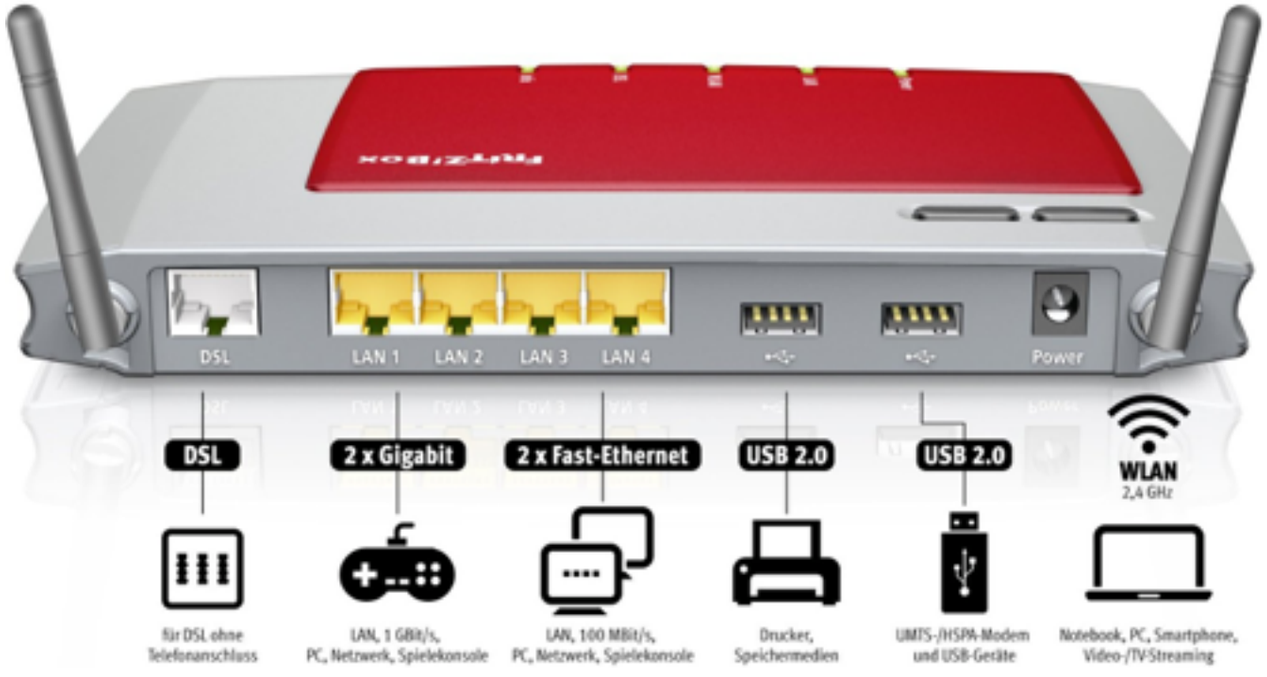
61.120.205.101

gmax@paranoid.email

WPAD experiment #3

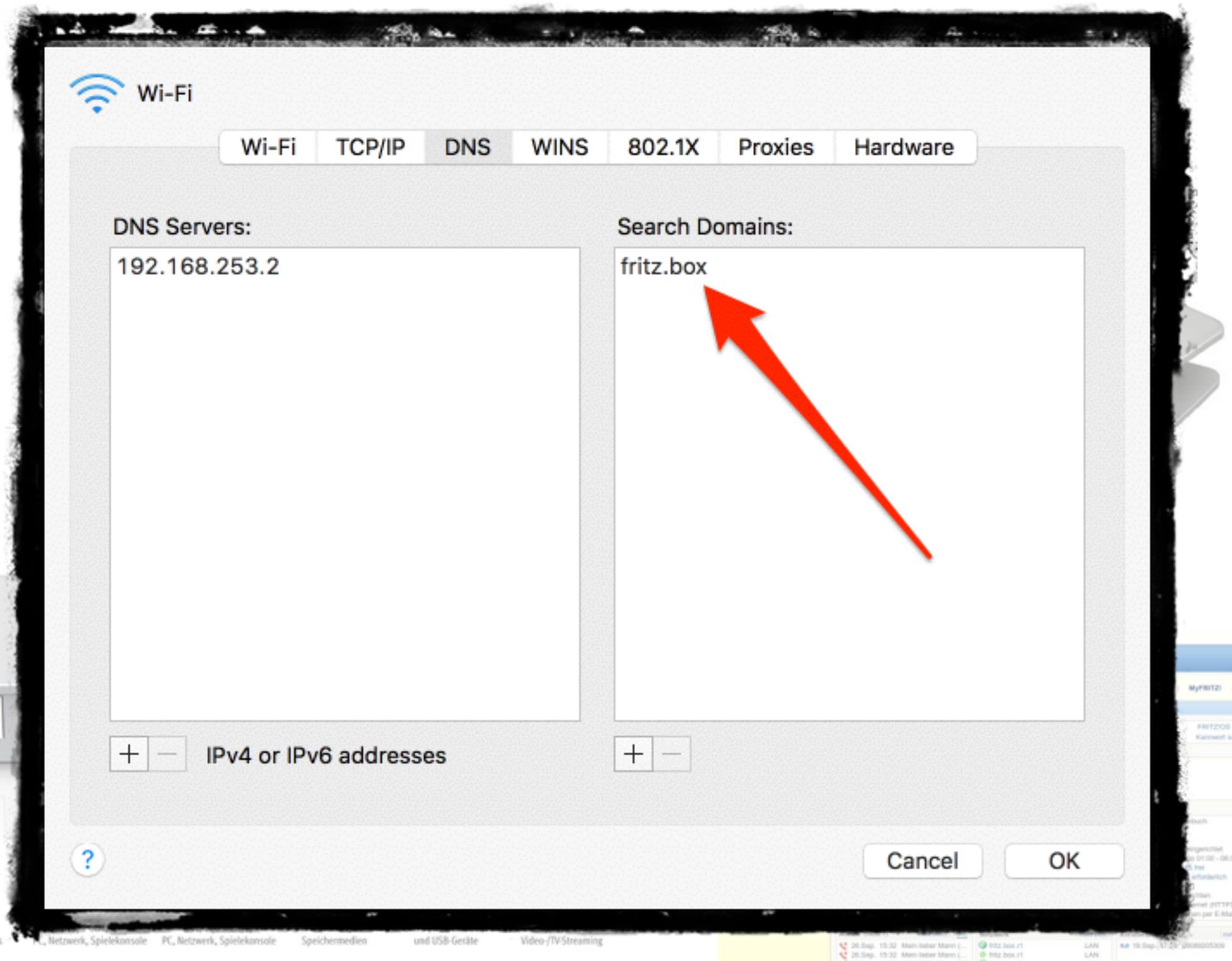
gmax@paranoid.email

WPAD and Hardware



gmax@paranoid.email

WPAD and Hardware



gmax@paranoid.email

WPAD and Hardware

```
pi@raspiradio ~ $ cat /etc/resolv.conf
domain fritz.box
search fritz.box
nameserver 192.168.253.2
```

WPAD and Hardware

AVM

register fritz.box

attack

gmax@paranoid.email

THANKS

gmax@paranoid.email