OPSEC

Against APT's reconnaissance phase

Antonio Villalón
Chief Security Officer
S2 Grupo CERT

APT stages

What is OPSEC?

Let's start!

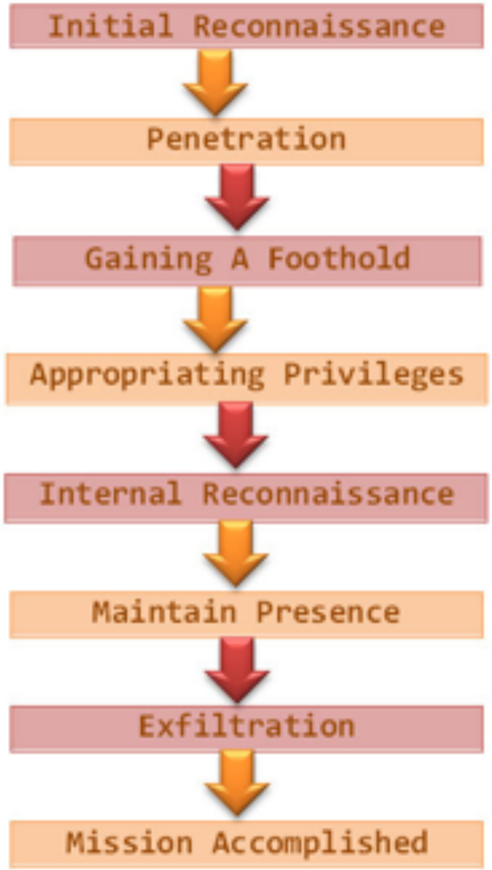
Sample scenario

Conclusions

APT stages

S2 GRUPO
CERT

APT stages


Initial Reconnaissance

Penetration

Gaining A Foothold

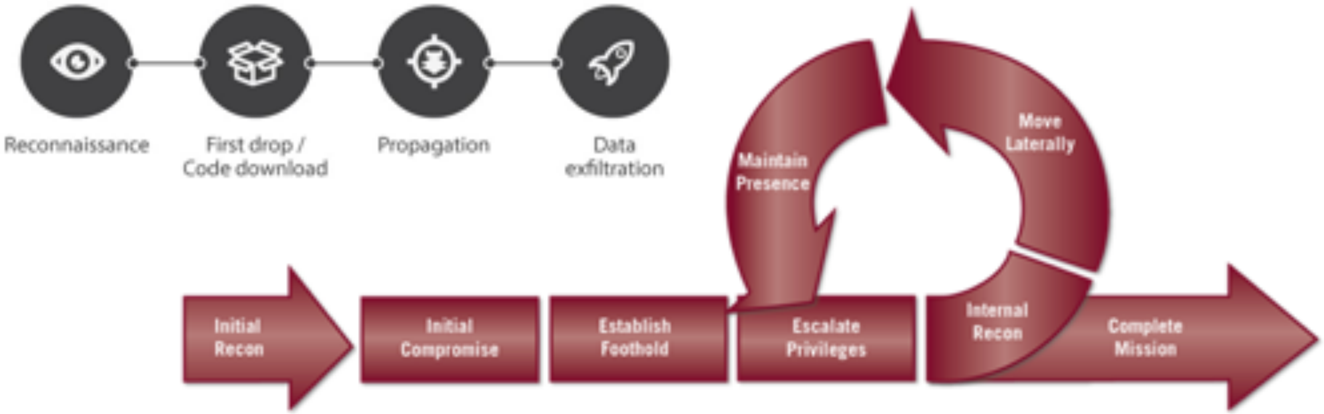
Appropriating Privileges

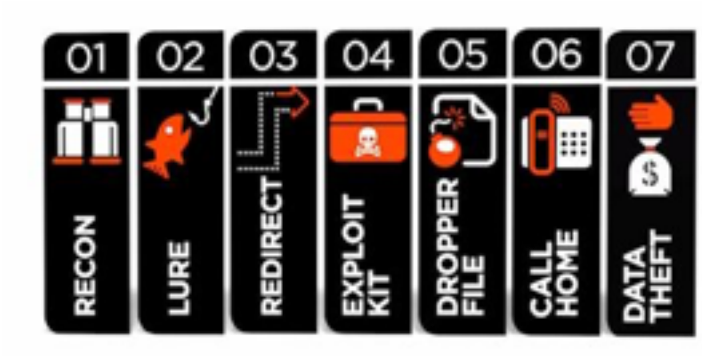
Internal Reconnaissance

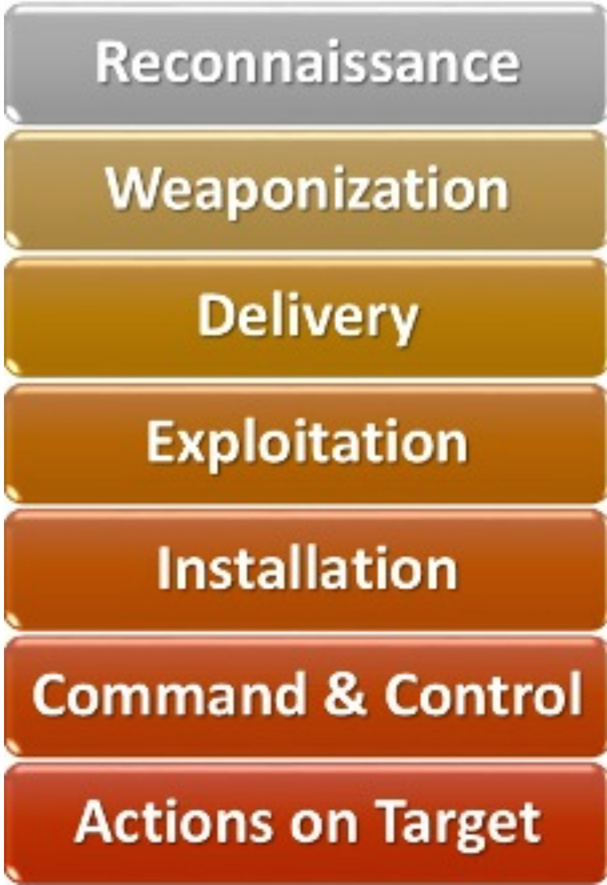
Maintain Presence

Exfiltration

Mission Accomplished






Reconnaissance

Weaponization

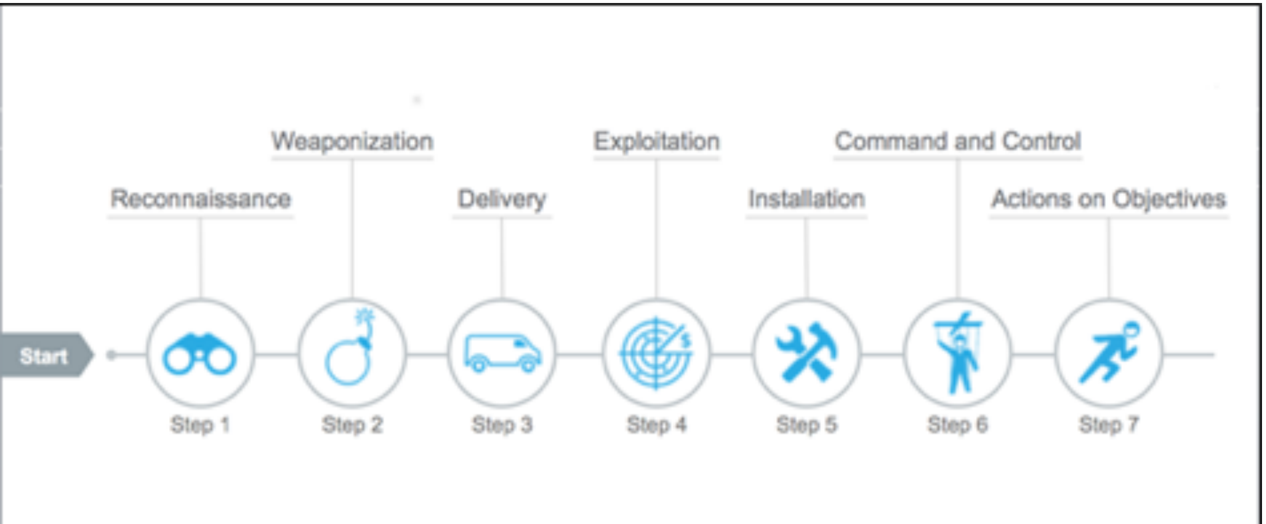
Delivery

Exploitation

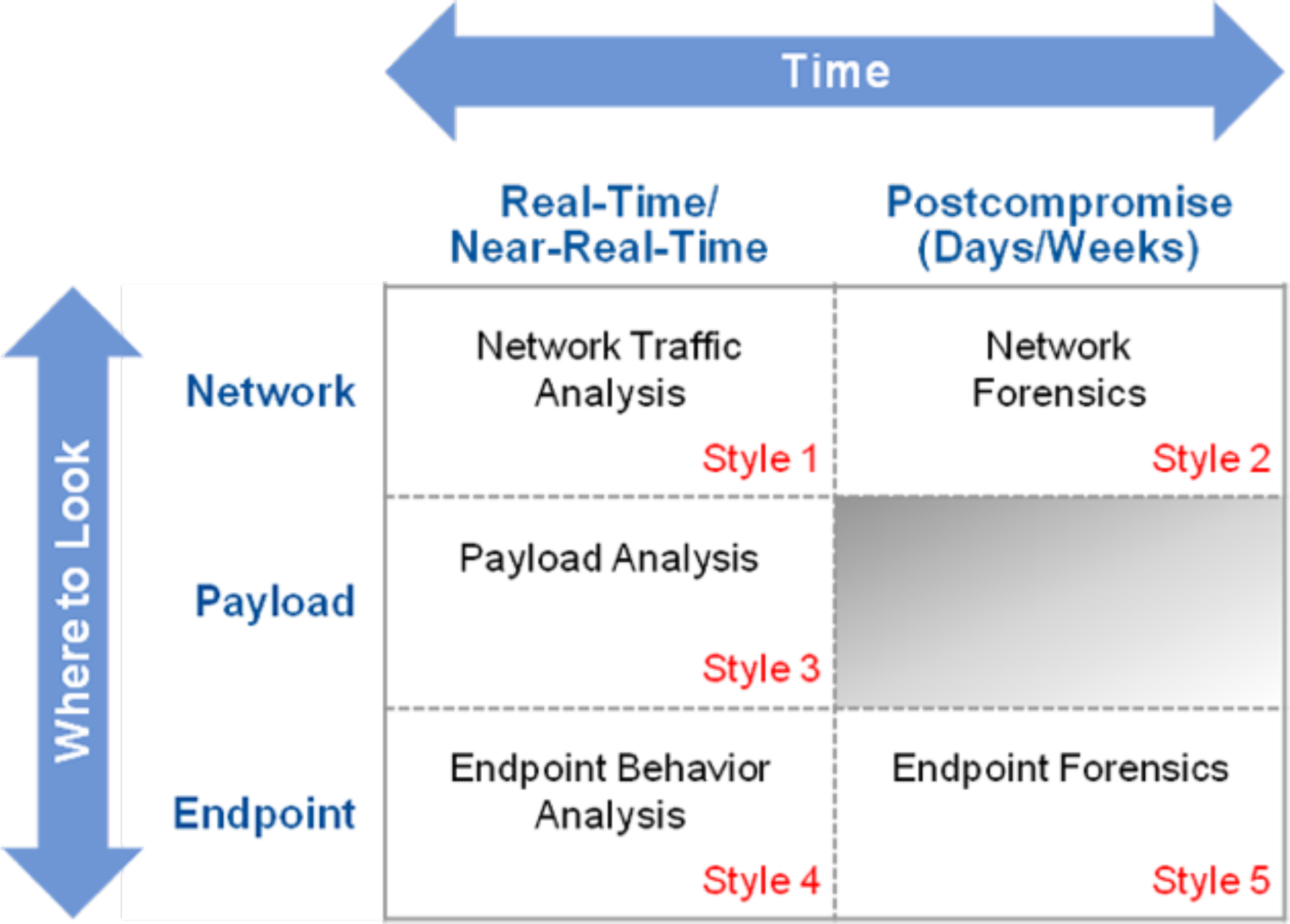
Installation

Command & Control

Actions on Target



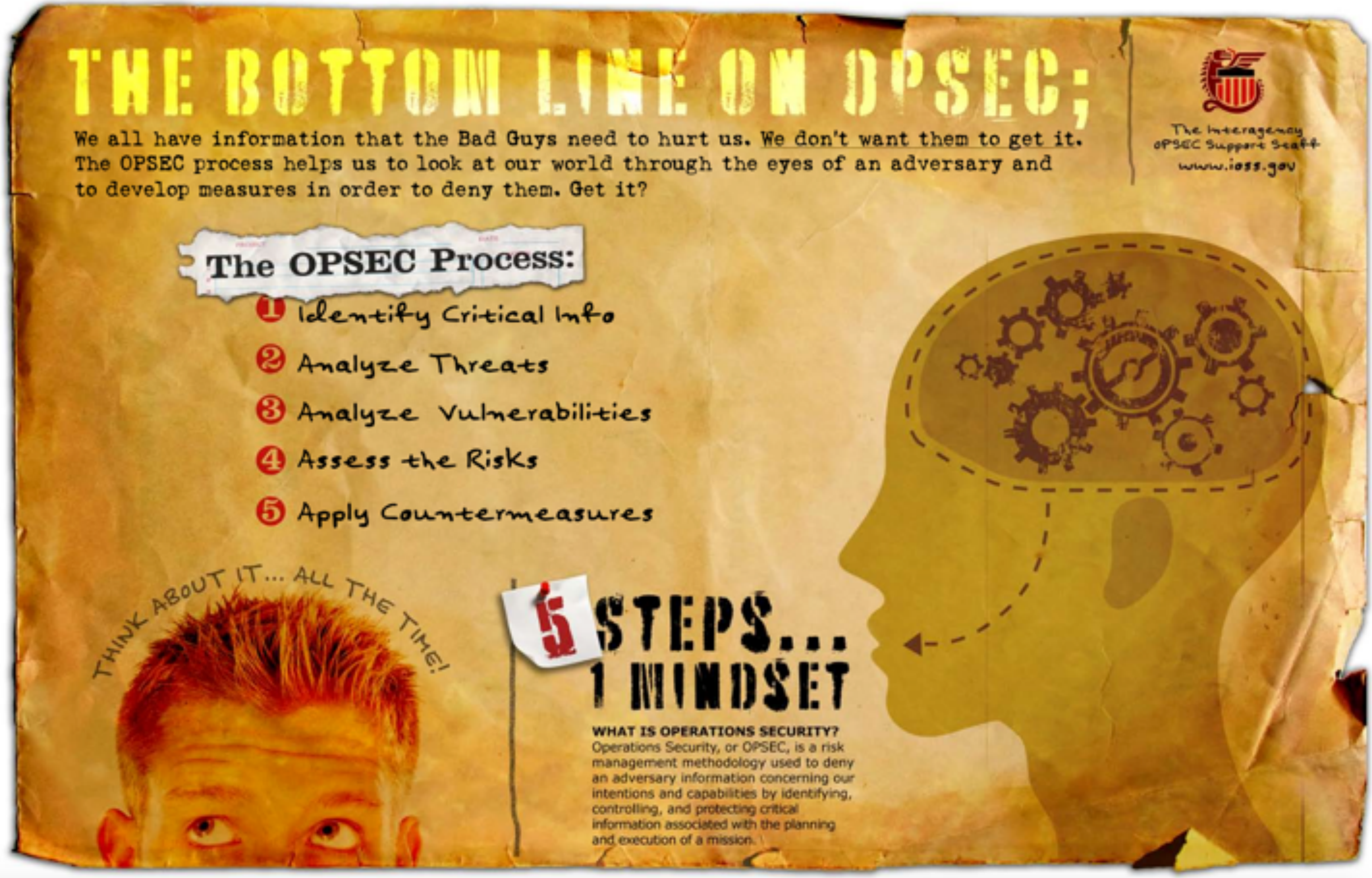
APT stages



	Real-Time/ Near-Real-Time	Postcompromise (Days/Weeks)
Network	Network Traffic Analysis Style 1	Network Forensics Style 2
Payload	Payload Analysis Style 3	
Endpoint	Endpoint Behavior Analysis Style 4	Endpoint Forensics Style 5

OPSEC

S2 GRUPO
CERT



THE BOTTOM LINE ON OPSEC;

We all have information that the Bad Guys need to hurt us. We don't want them to get it. The OPSEC process helps us to look at our world through the eyes of an adversary and to develop measures in order to deny them. Get it?

The Interagency
OPSEC Support Staff
www.ioss.gov

The OPSEC Process:

1. Identify Critical Info
2. Analyze Threats
3. Analyze Vulnerabilities
4. Assess the Risks
5. Apply Countermeasures

5 STEPS... 1 MINDSET

WHAT IS OPERATIONS SECURITY?
Operations Security, or OPSEC, is a risk management methodology used to deny an adversary information concerning our intentions and capabilities by identifying, controlling, and protecting critical information associated with the planning and execution of a mission.

OPSEC

Cambridge
Bedford
Stevenage
Luton
St Albans
Harlow
Watford
Enfield
Braintree
Colchester
Sudbury
Chelmsford
Brentwood
Basildon
Southend
Slough
London
TG LA7
WI-FI
SSID:
Senato-Wireless
PASSWORD:
XZh4442T4632

SOMEONE
TALKED!

SOMEONE
BLOGGED!

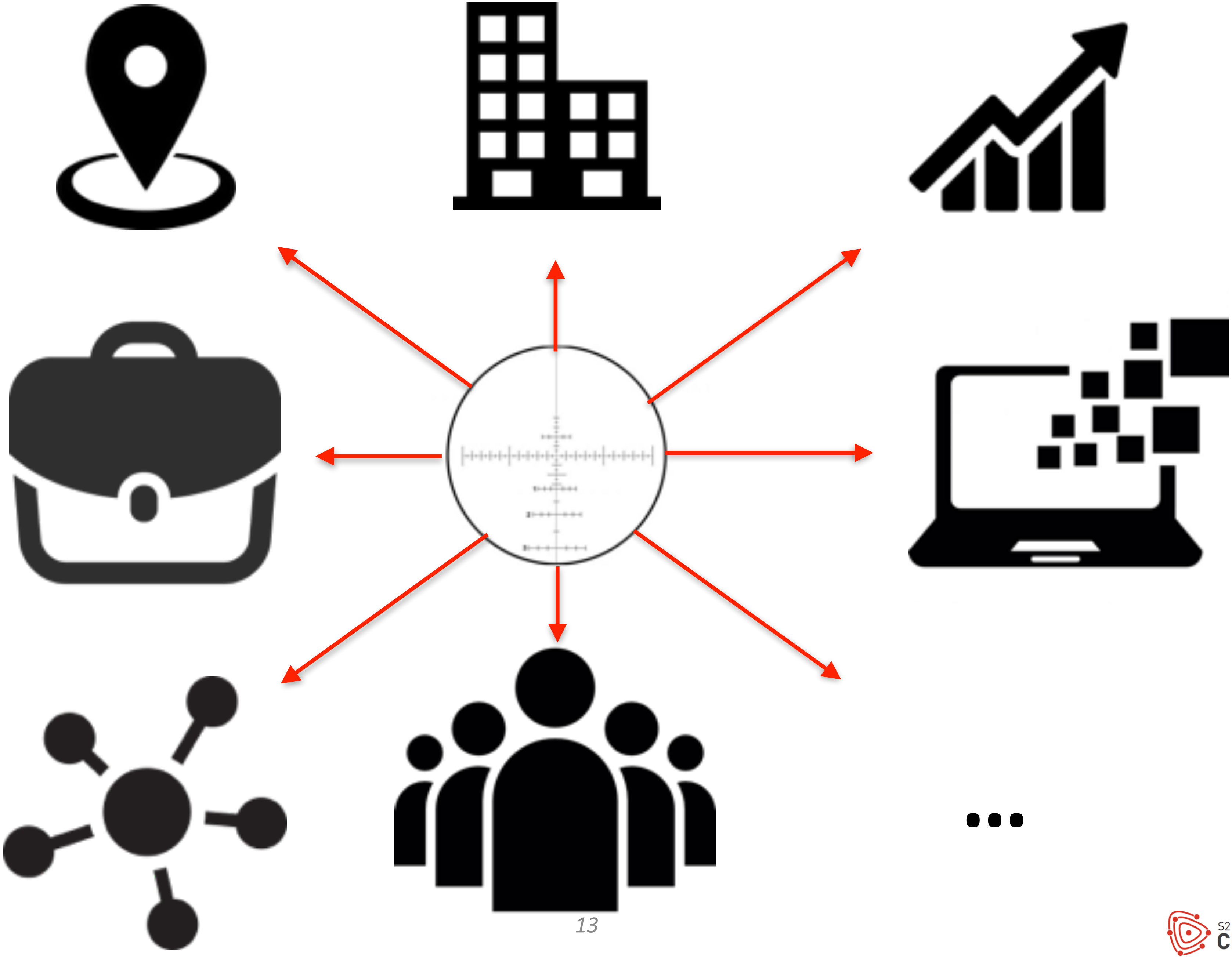
SOMEONE
TWEETED!

Let’s start!

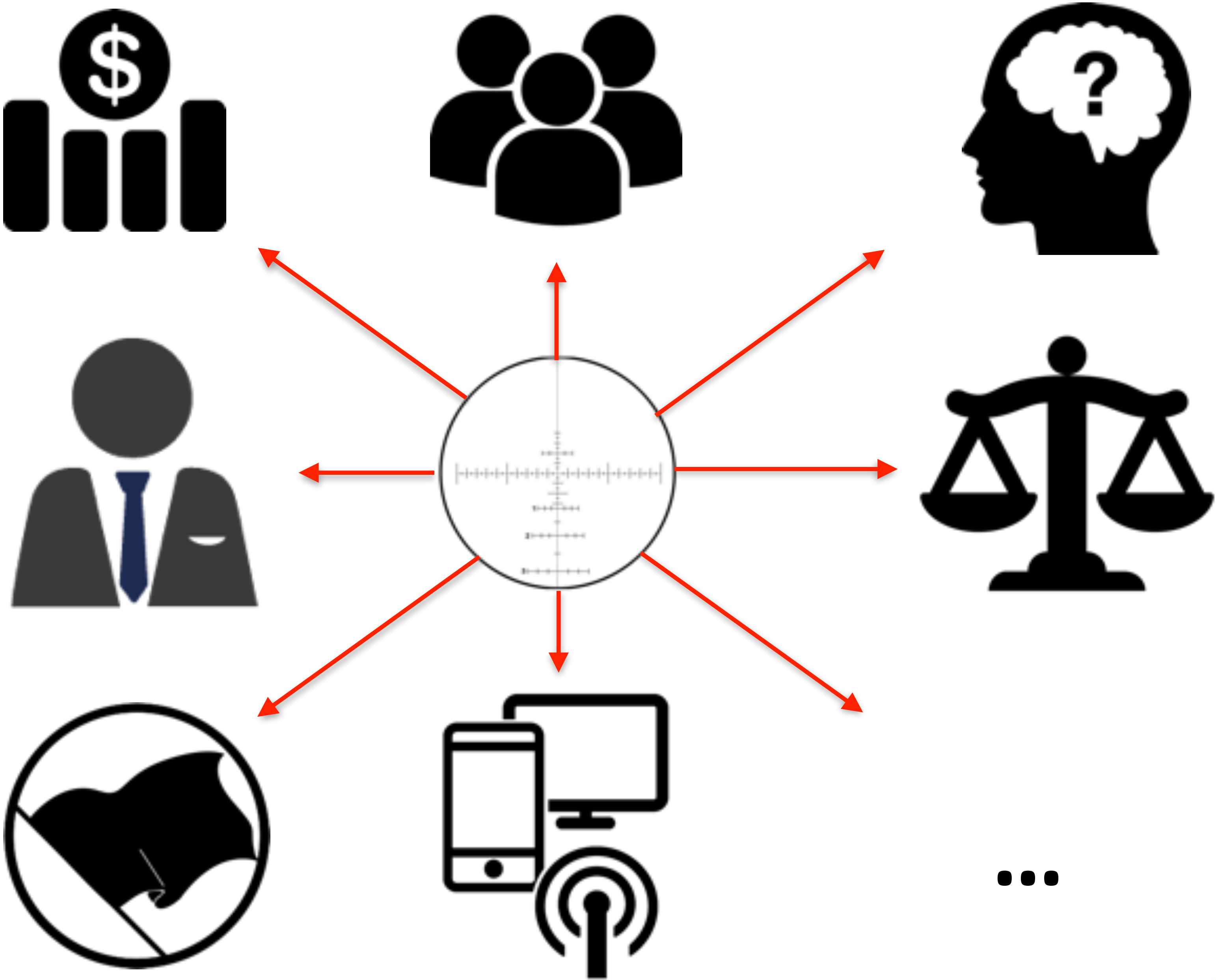
S2 GRUPO CERT

Our goal

Which info is valuable (org)?



Which info is valuable (ppl)?

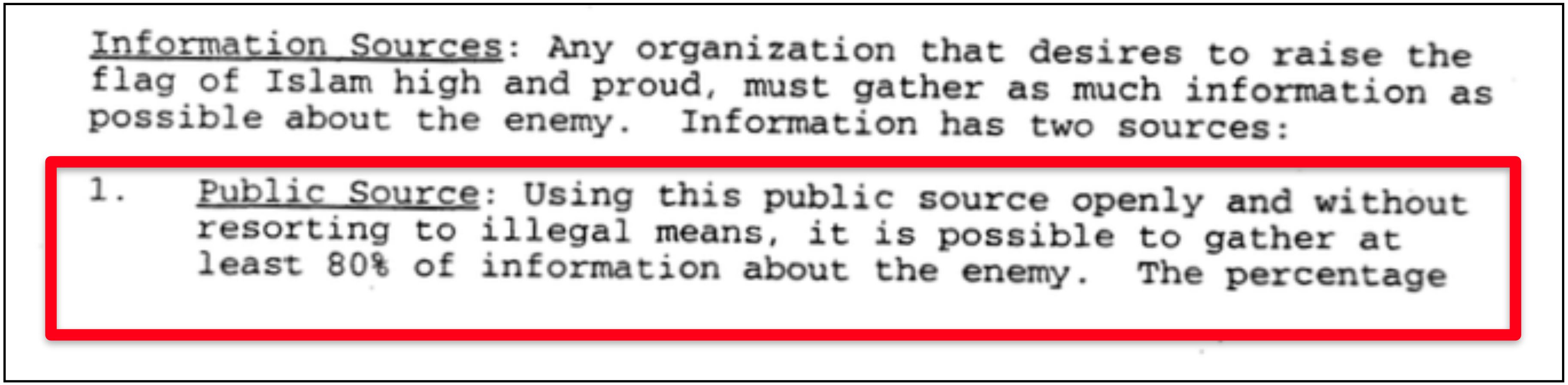


Which info is NOT valuable?

Which are the threats?

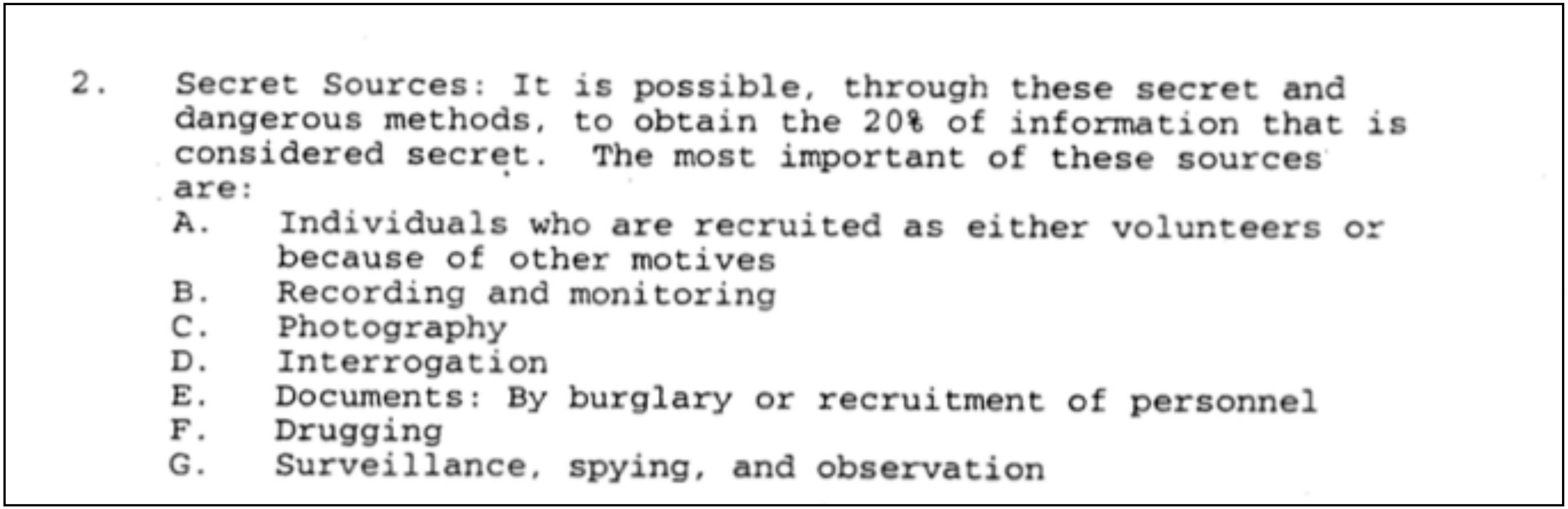
INSERT YOUR FAVOURITE FLAG <HERE>

Where is the info?



Information Sources: Any organization that desires to raise the flag of Islam high and proud, must gather as much information as possible about the enemy. Information has two sources:

1. Public Source: Using this public source openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy. The percentage



2. Secret Sources: It is possible, through these secret and dangerous methods, to obtain the 20% of information that is considered secret. The most important of these sources are:
   - A. Individuals who are recruited as either volunteers or because of other motives
   - B. Recording and monitoring
   - C. Photography
   - D. Interrogation
   - E. Documents: By burglary or recruitment of personnel
   - F. Drugging
   - G. Surveillance, spying, and observation

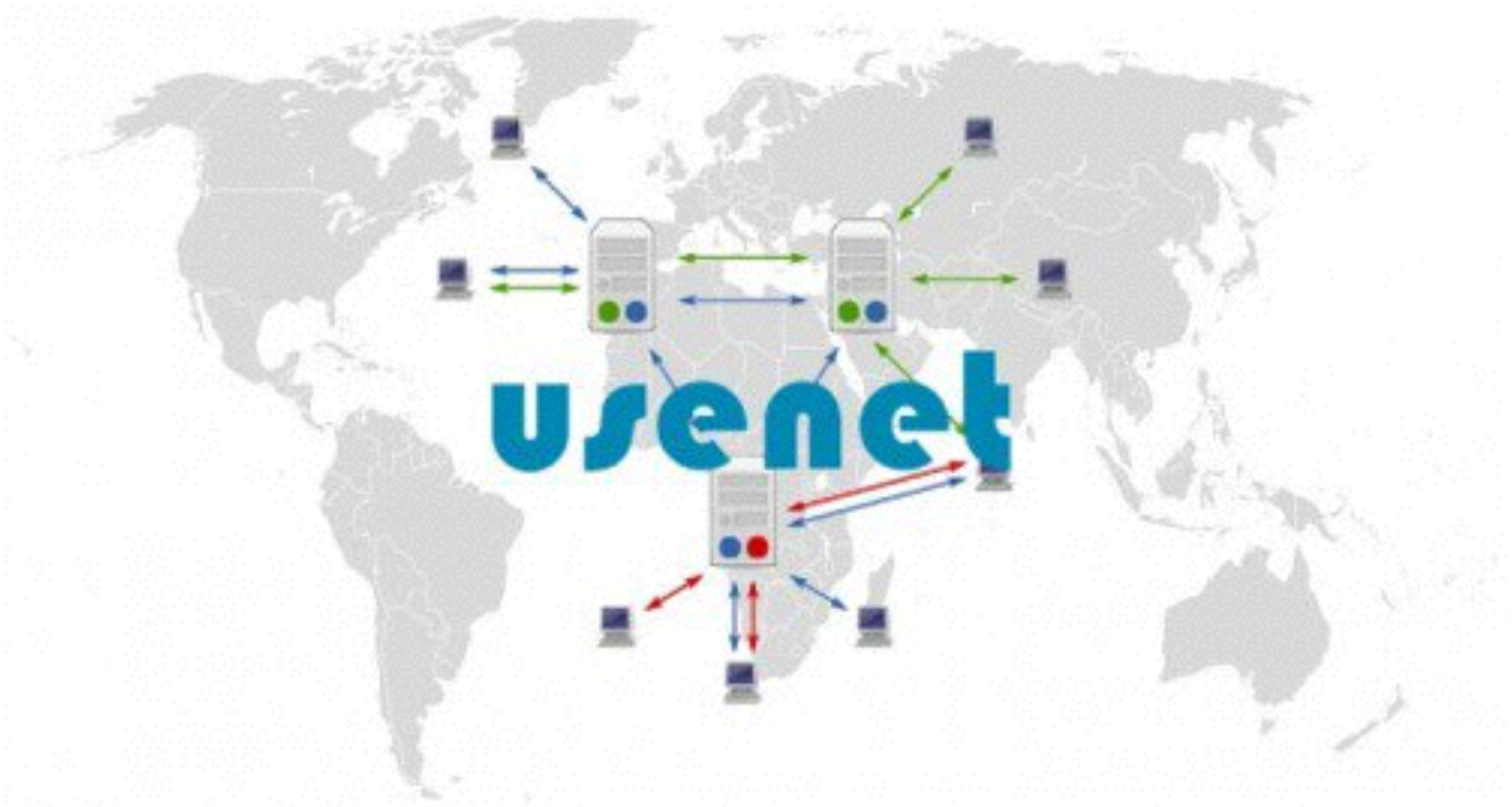
WALL STREET JOURNAL
What's News—
FINANCIAL TIMES
Le Monde
INITIATIVES
Horst Stern: Reise durch ostdeutsche Landschaften (Seite 6
DIE ZEIT
WOCHENZEITUNG FÜR POLITIK · WIRTSCHAFT · HANDEL UND KULTUR
Tea amo!
Tension entre Damas et Ankara
Libération
Tiberi
Le Marais poitevin
Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND
Herald INTERNATIONAL Tribune
PUBLISHED WITH THE NEW YORK TIMES AND THE WASHINGTON POST
Yeltsin Dismisses Hard-
peans Face
Russie : un général arbitre du second tour
La Tribune

Open sources

alt.2600

comp.security

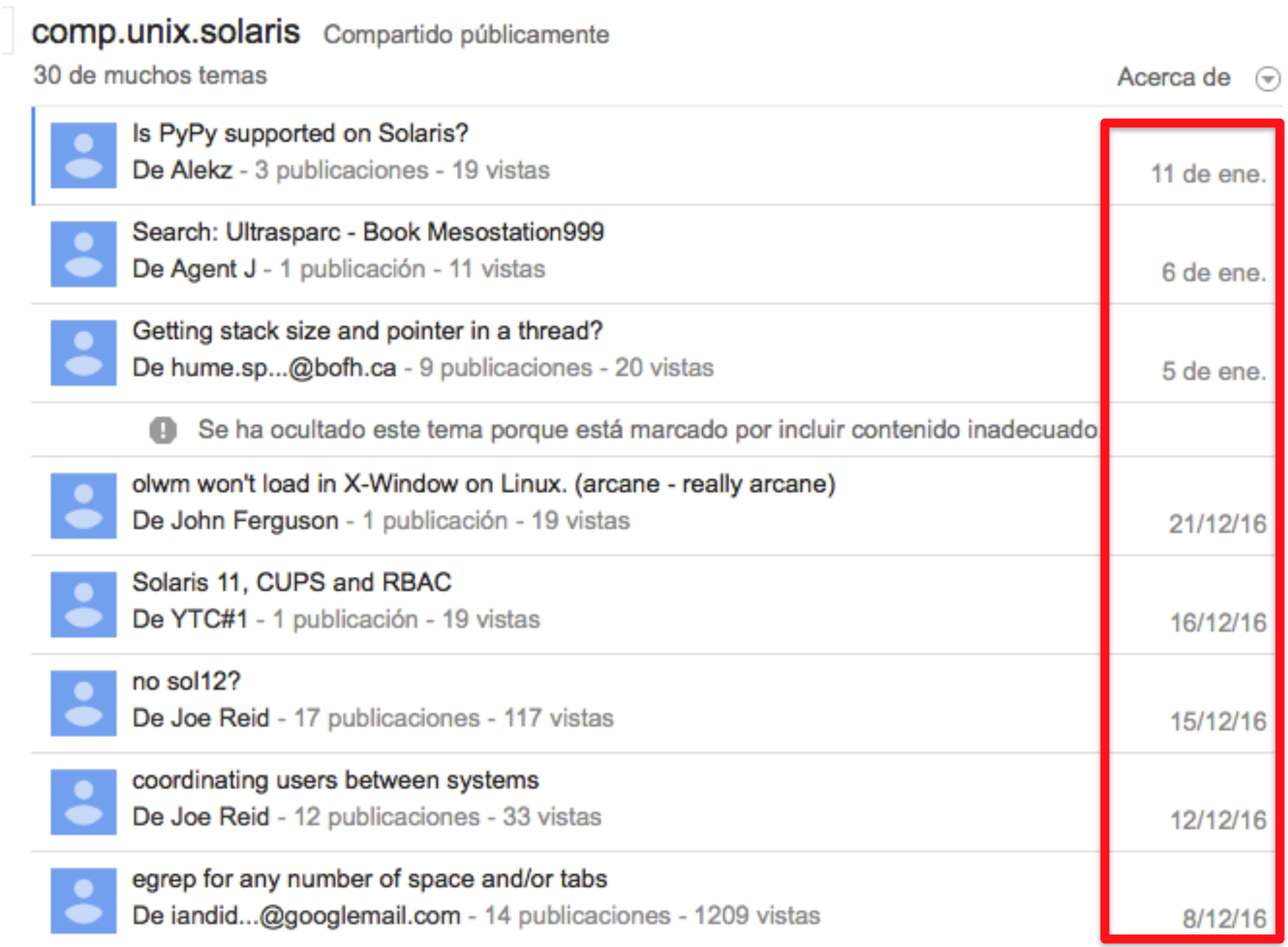
comp.security.unix



comp.hackers

comp.os.minix

comp.unix.solaris



comp.unix.solaris Compartido públicamente

30 de muchos temas

Is PyPy supported on Solaris?
De Alekz - 3 publicaciones - 19 vistas
11 de ene.

Search: Ultrasparc - Book Mesostation999
De Agent J - 1 publicación - 11 vistas
6 de ene.

Getting stack size and pointer in a thread?
De hume.sp...@bofh.ca - 9 publicaciones - 20 vistas
5 de ene.

Se ha ocultado este tema porque está marcado por incluir contenido inadecuado

olwm won't load in X-Window on Linux. (arcane - really arcane)
De John Ferguson - 1 publicación - 19 vistas
21/12/16

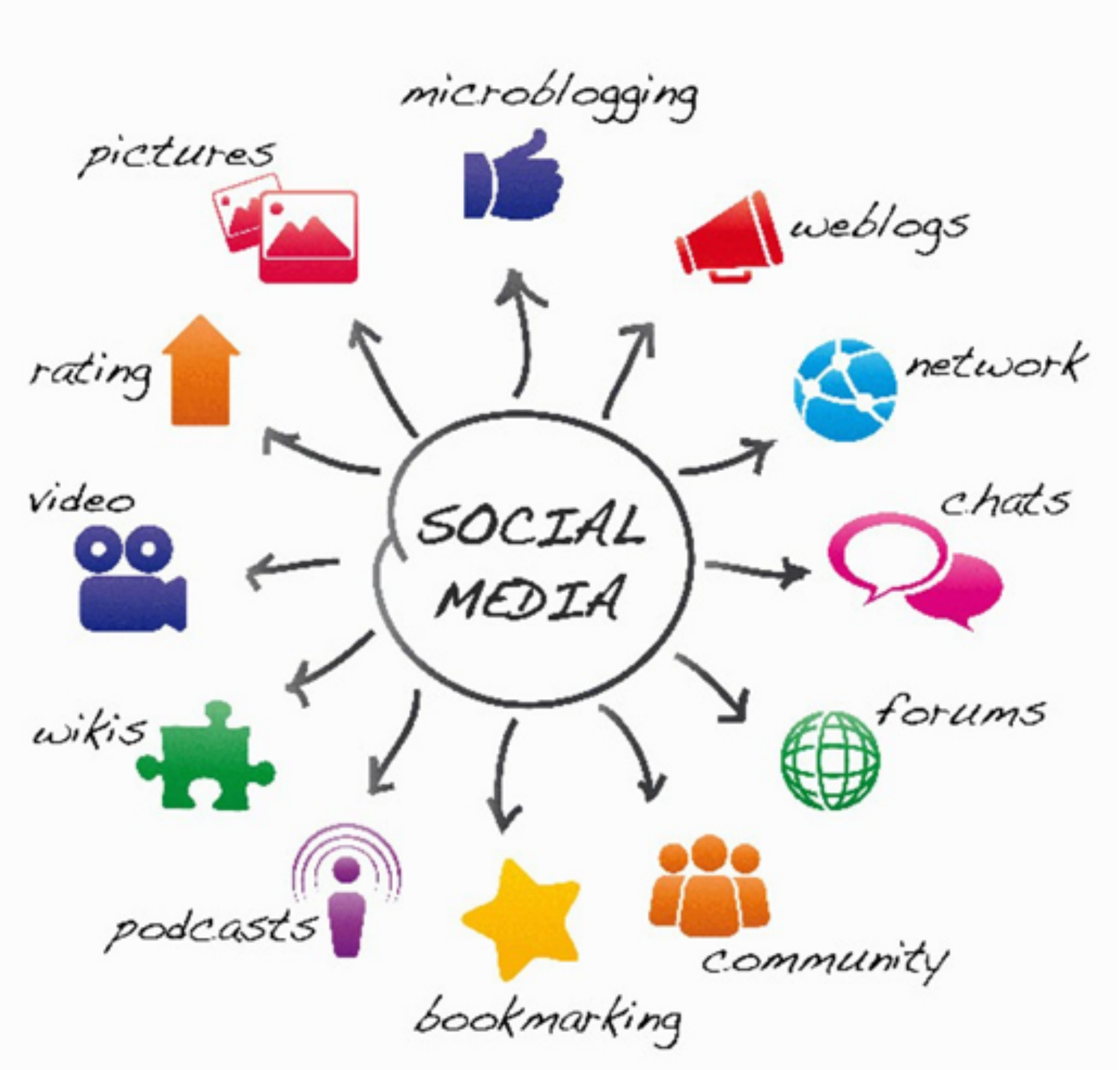
Solaris 11, CUPS and RBAC
De YTC#1 - 1 publicación - 19 vistas
16/12/16

no sol12?
De Joe Reid - 17 publicaciones - 117 vistas
15/12/16

coordinating users between systems
De Joe Reid - 12 publicaciones - 33 vistas
12/12/16

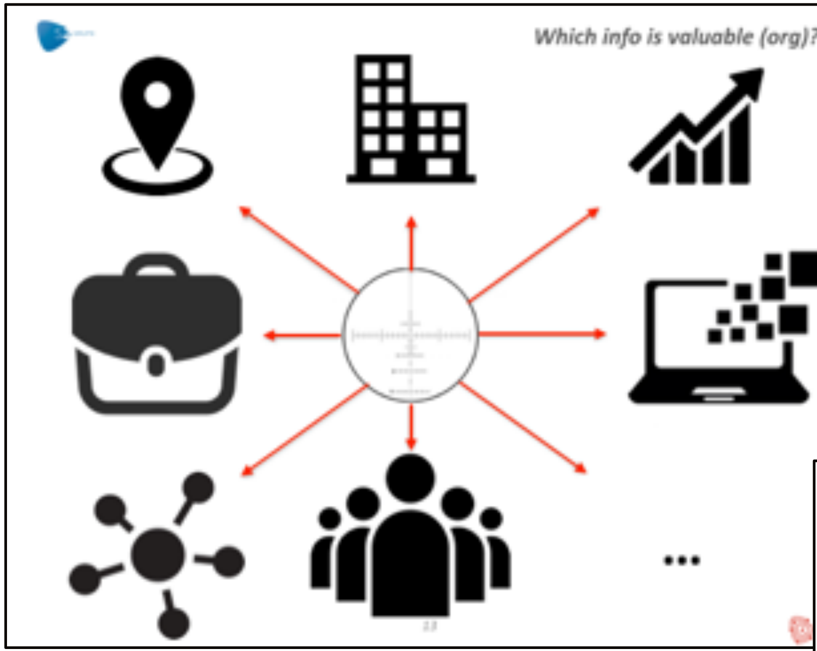
egrep for any number of space and/or tabs
De iandid...@googlemail.com - 14 publicaciones - 1209 vistas
8/12/16

Open sources



What are the bad guys doing?

What are the bad guys doing?



Which info is valuable (org)?

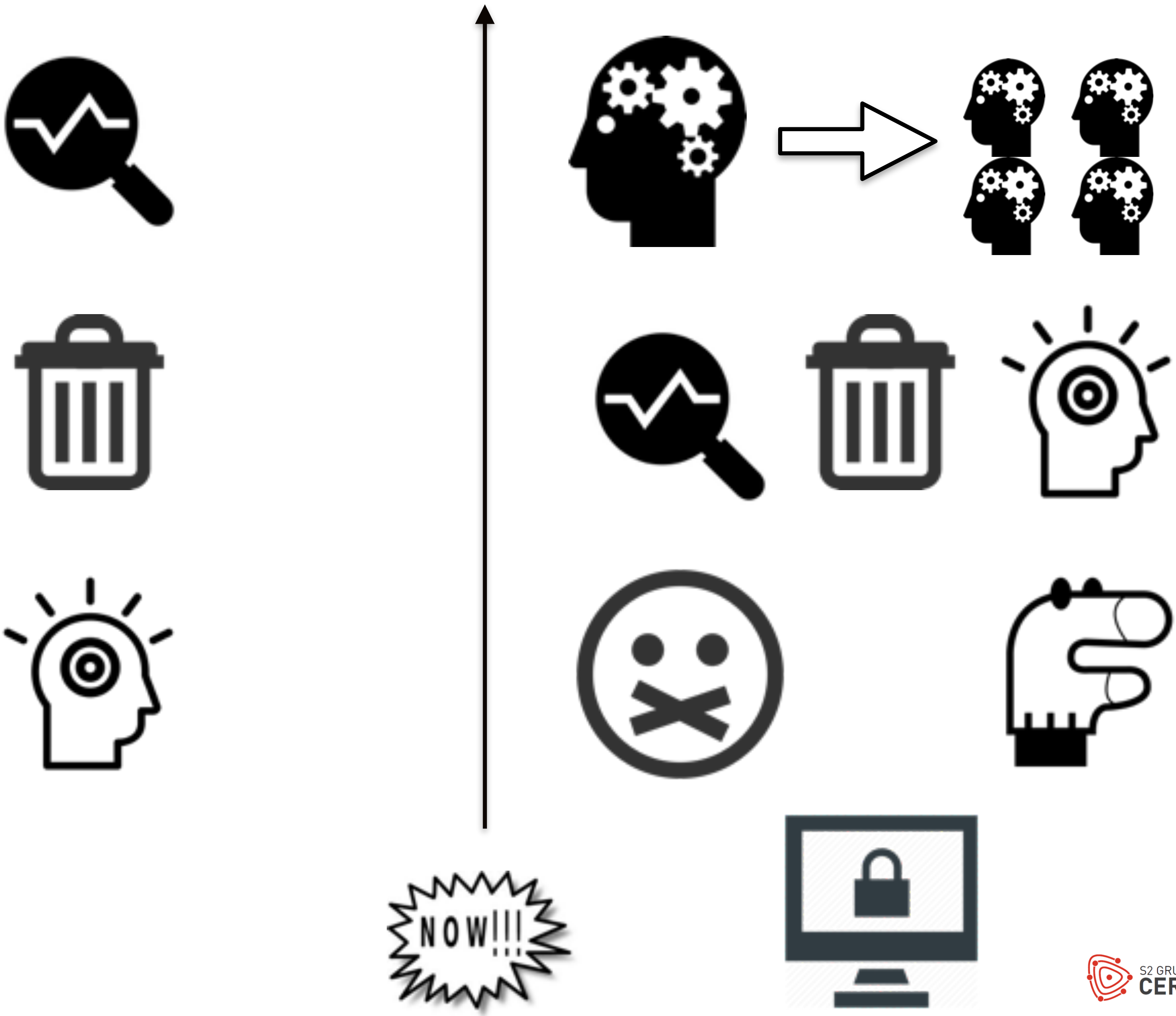
Which info is valuable (ppl)?

What are the bad guys doing?

What are the bad guys doing?

> *Know your enemy and know yourself and you can fight a hundred battles without disaster*
>
> *Sun Tzu, The art of war*

What to do?



Sample scenario

S2 GRUPO CERT

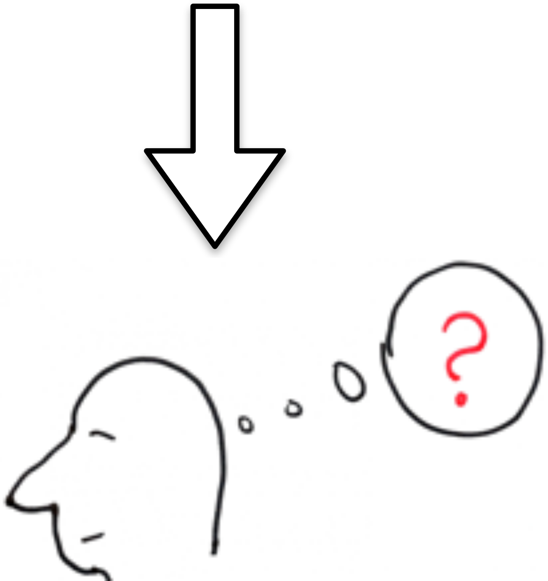
Sample scenario

☑ We need to establish our own CERT

☑ We need security procedures, policies…

☑ ACME, our main competitor, has its own CERT up and running

☑ Copying is easier than creating

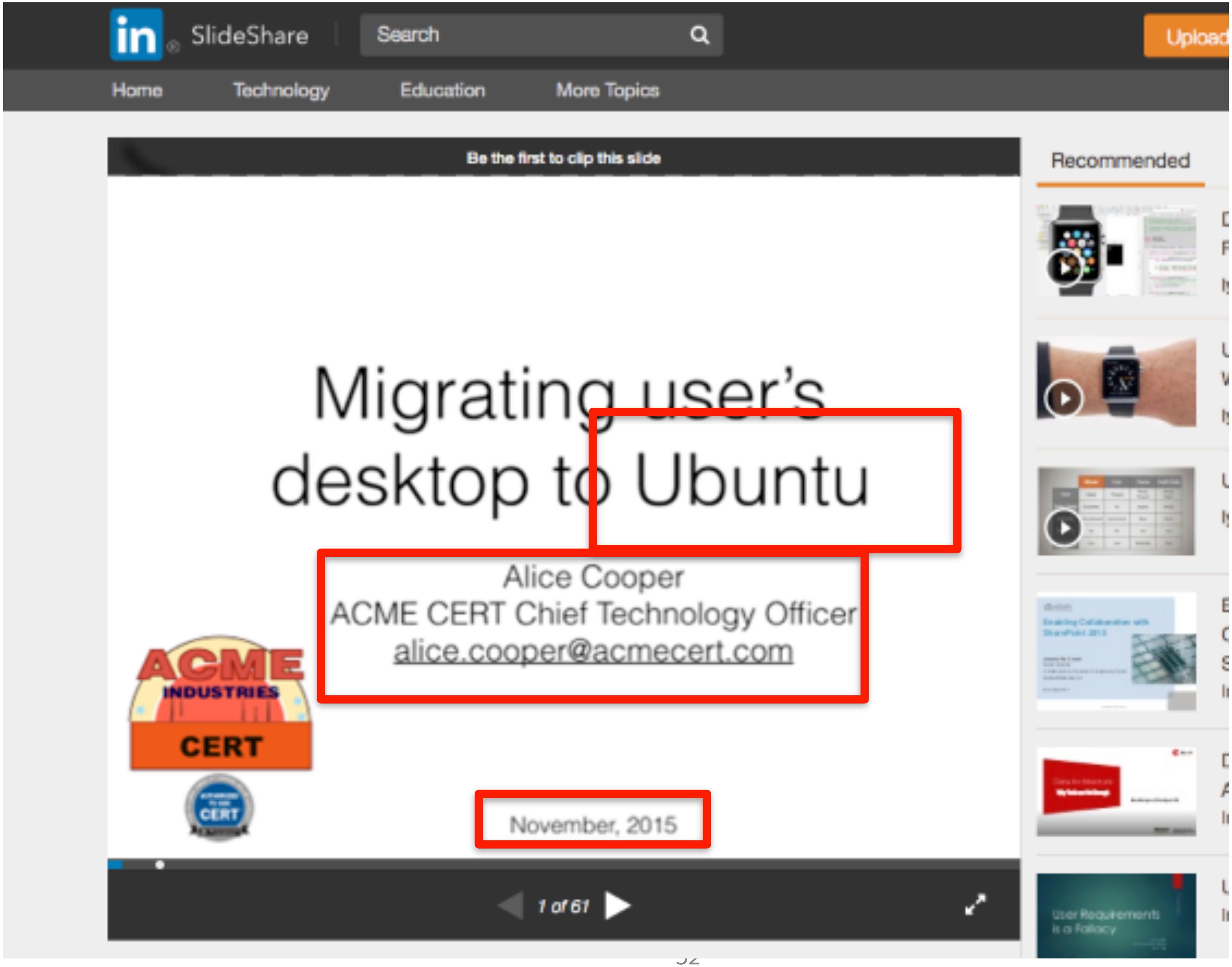


What is ACME CERT? What is ACME?

More about ACME CERT?

acme CERT

Sample scenario

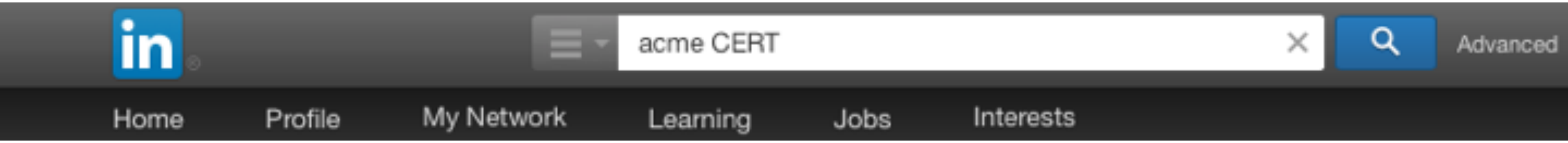


Migrating user's desktop to Ubuntu

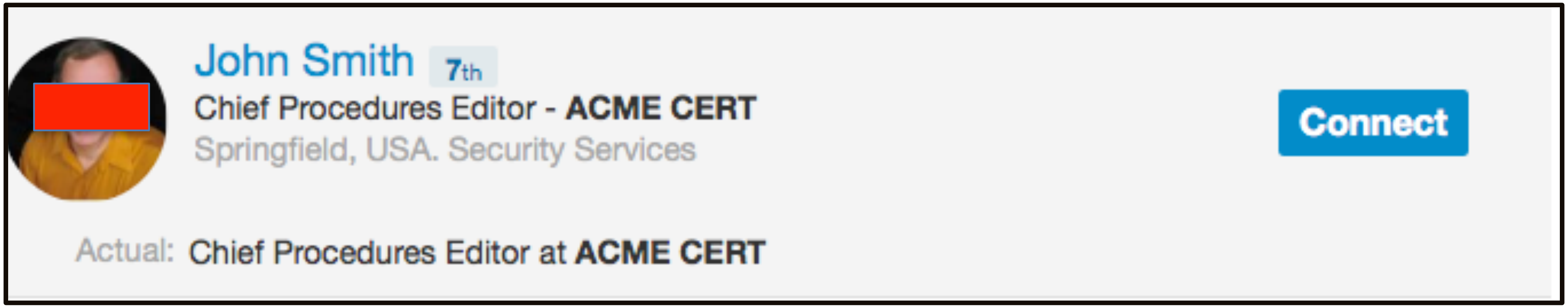
Alice Cooper
ACME CERT Chief Technology Officer
alice.cooper@acmecert.com

November, 2015

Who works there?



acme CERT



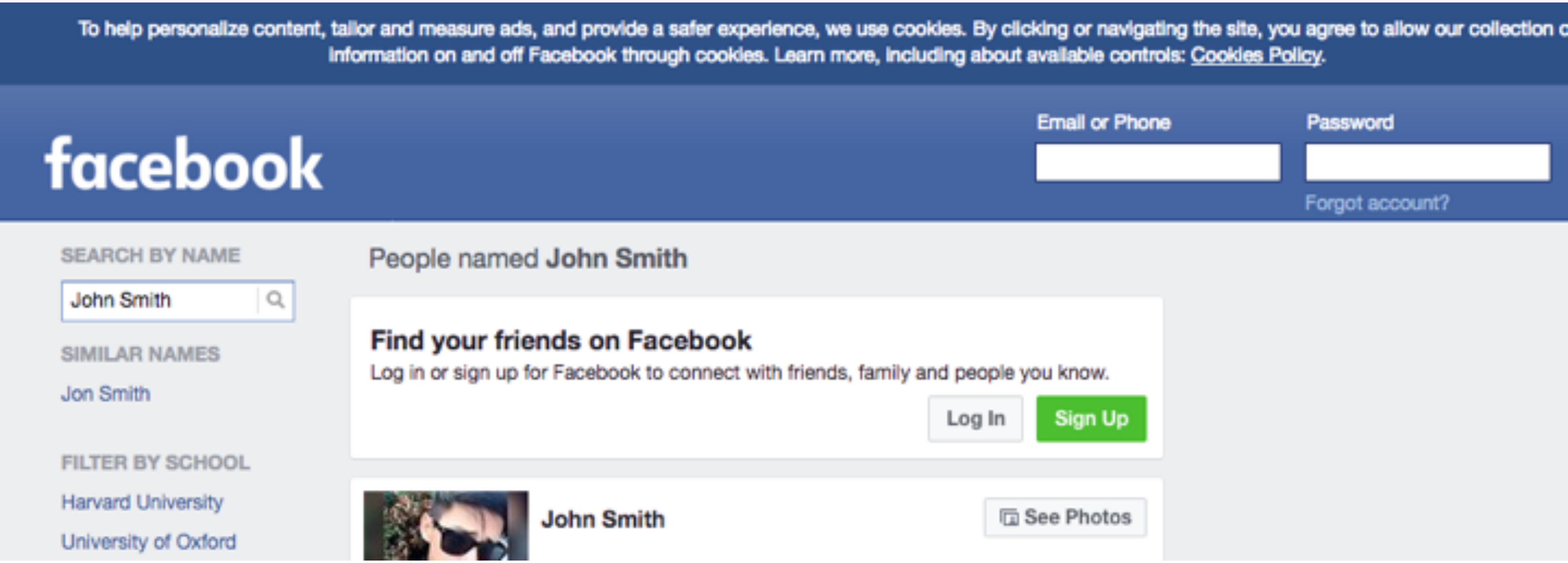
John Smith 7th

Chief Procedures Editor - **ACME CERT**

Springfield, USA. Security Services

Actual: Chief Procedures Editor at **ACME CERT**

Who is John Smith?

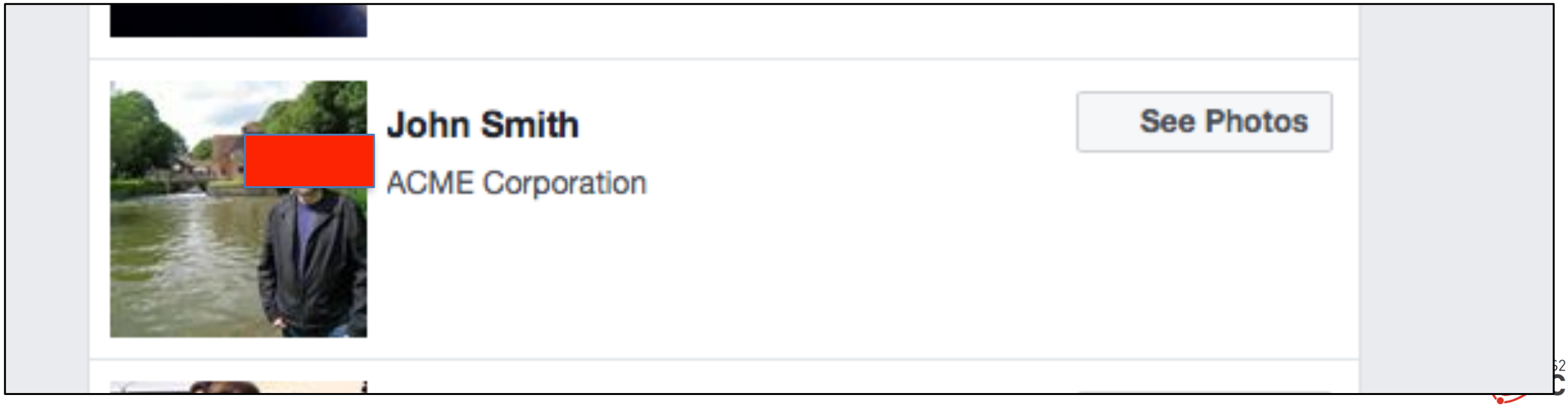


To help personalize content, tailor and measure ads, and provide a safer experience, we use cookies. By clicking or navigating the site, you agree to allow our collection
information on and off Facebook through cookies. Learn more, including about available controls: Cookies Policy.

People named **John Smith**

Find your friends on Facebook

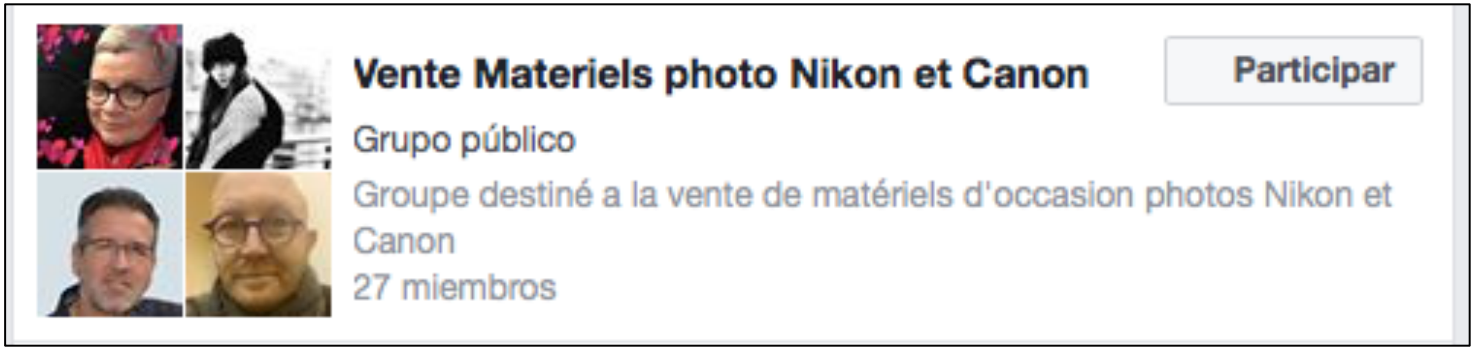
Log in or sign up for Facebook to connect with friends, family and people you know.



John Smith

ACME Corporation

Who is John Smith?

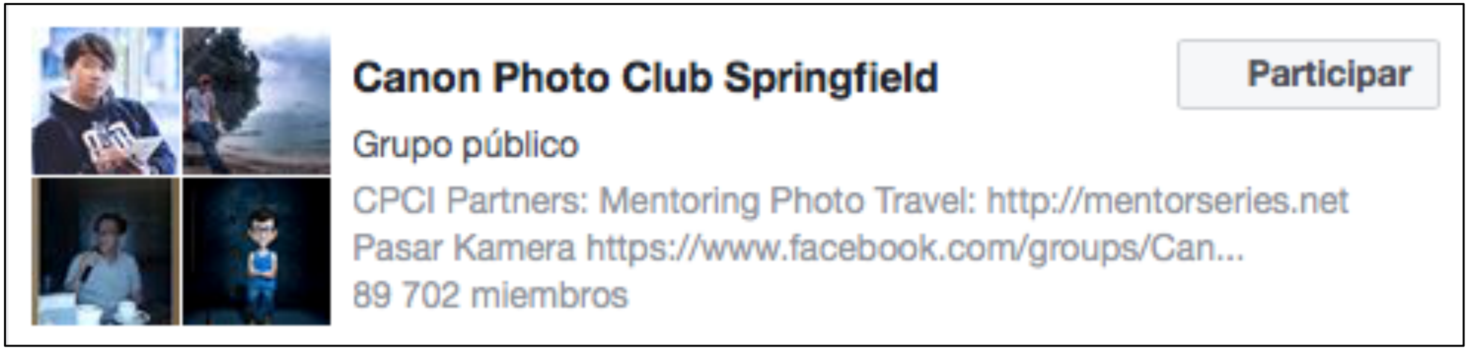


Vente Materiels photo Nikon et Canon

Grupo público

Groupe destiné a la vente de matériels d'occasion photos Nikon et Canon

27 miembros

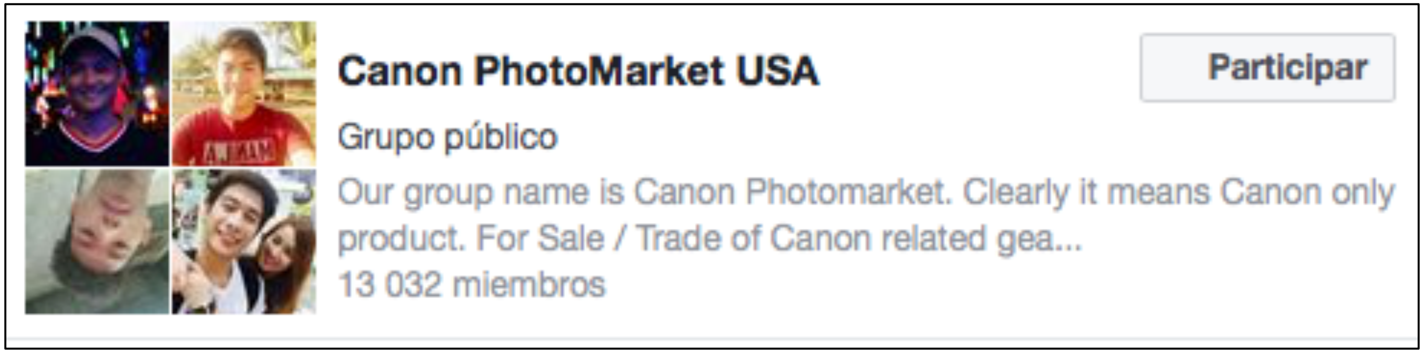


Canon Photo Club Springfield

Grupo público

CPCI Partners: Mentoring Photo Travel: http://mentorseries.net Pasar Kamera https://www.facebook.com/groups/Can...

89 702 miembros



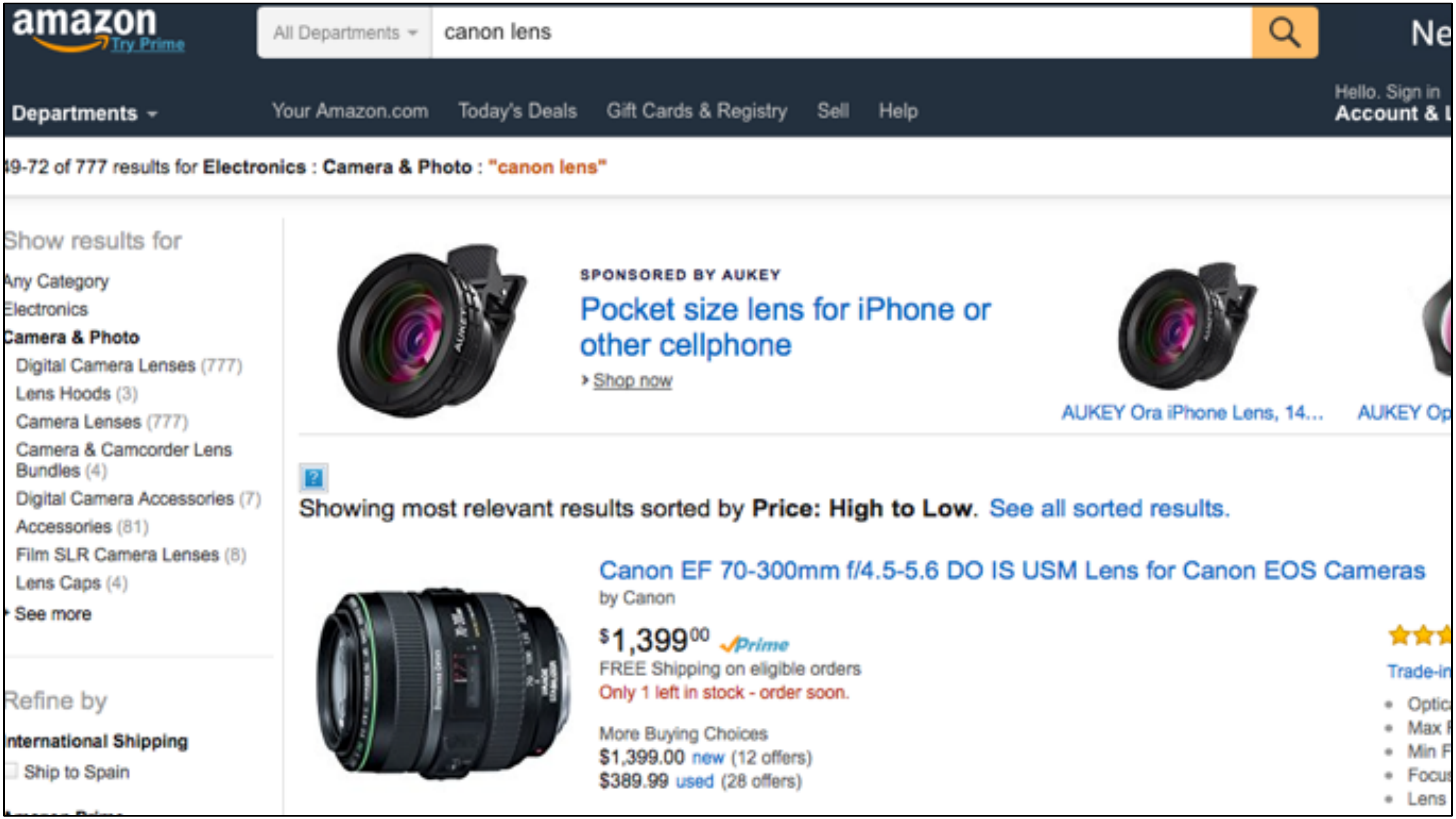
Canon PhotoMarket USA

Grupo público

Our group name is Canon Photomarket. Clearly it means Canon only product. For Sale / Trade of Canon related gea...

13 032 miembros

Let’s build the attack…



amazon Try Prime

All Departments canon lens

Ne

Departments Your Amazon.com Today's Deals Gift Cards & Registry Sell Help

Hello. Sign in Account & L

49-72 of 777 results for **Electronics** : **Camera & Photo** : "canon lens"

Show results for

Any Category
Electronics
Camera & Photo
- Digital Camera Lenses (777)
- Lens Hoods (3)
- Camera Lenses (777)
- Camera & Camcorder Lens Bundles (4)
- Digital Camera Accessories (7)
- Accessories (81)
- Film SLR Camera Lenses (8)
- Lens Caps (4)
- See more

Refine by

International Shipping

□ Ship to Spain

SPONSORED BY AUKEY

Pocket size lens for iPhone or other cellphone

› Shop now

AUKEY Ora iPhone Lens, 14...

AUKEY Op

Showing most relevant results sorted by **Price: High to Low**. See all sorted results.

Canon EF 70-300mm f/4.5-5.6 DO IS USM Lens for Canon EOS Cameras

by Canon

$1,399^{00} Prime

FREE Shipping on eligible orders

Only 1 left in stock - order soon.

More Buying Choices

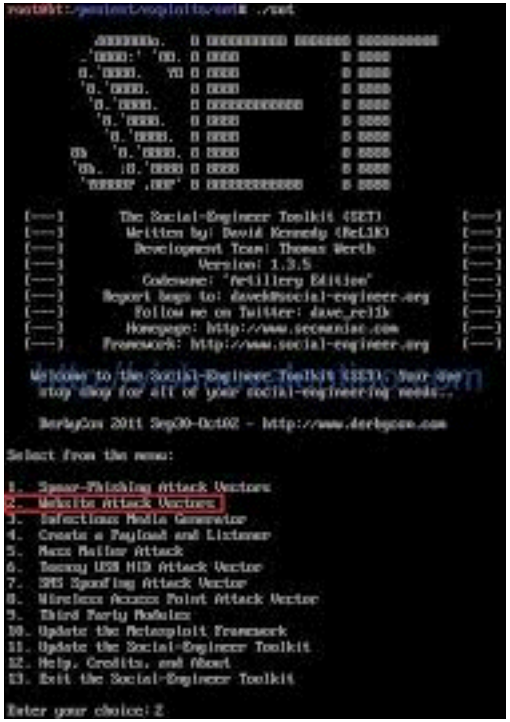
$1,399.00 new (12 offers)

$389.99 used (28 offers)

Trade-in

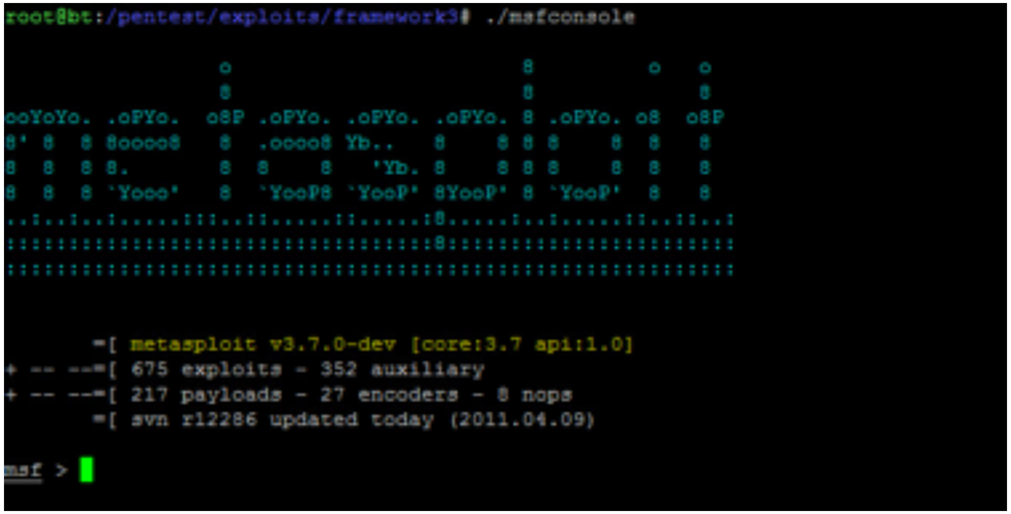
- Optic
- Max F
- Min F
- Focus
- Lens

Let’s build the attack…

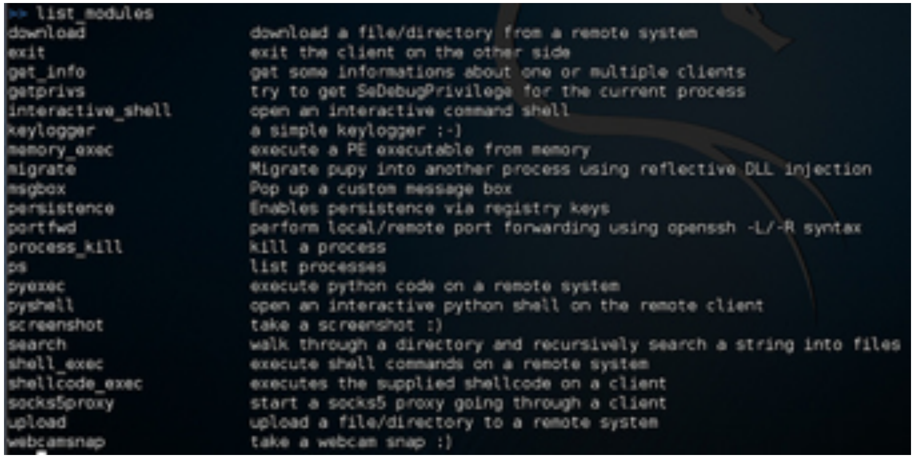


```
root@bt:/pentest/exploits/set# ./set

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Written by: David Kennedy (ReL1K)         [---]
[---]       Development Team: Thomas Werth             [---]
[---]              Version: 1.3.5                      [---]
[---]        Codename: 'Artillery Edition'             [---]
[---]   Report bugs to: davek@social-engineer.org      [---]
[---]        Follow me on Twitter: dave_rel1k          [---]
[---]      Homepage: http://www.secmaniac.com          [---]
[---]   Framework: http://www.social-engineer.org      [---]

  Welcome to the Social-Engineer Toolkit (SET). Your one
   stop shop for all of your social-engineering needs..

   DerbyCon 2011 Sep30-Oct02 - http://www.derbycon.com

Select from the menu:

1.  Spear-Phishing Attack Vectors
2.  Website Attack Vectors
3.  Infectious Media Generator
4.  Create a Payload and Listener
5.  Mass Mailer Attack
6.  Teensy USB HID Attack Vector
7.  SMS Spoofing Attack Vector
8.  Wireless Access Point Attack Vector
9.  Third Party Modules
10. Update the Metasploit Framework
11. Update the Social-Engineer Toolkit
12. Help, Credits, and About
13. Exit the Social-Engineer Toolkit

Enter your choice: 2
```

KALI™

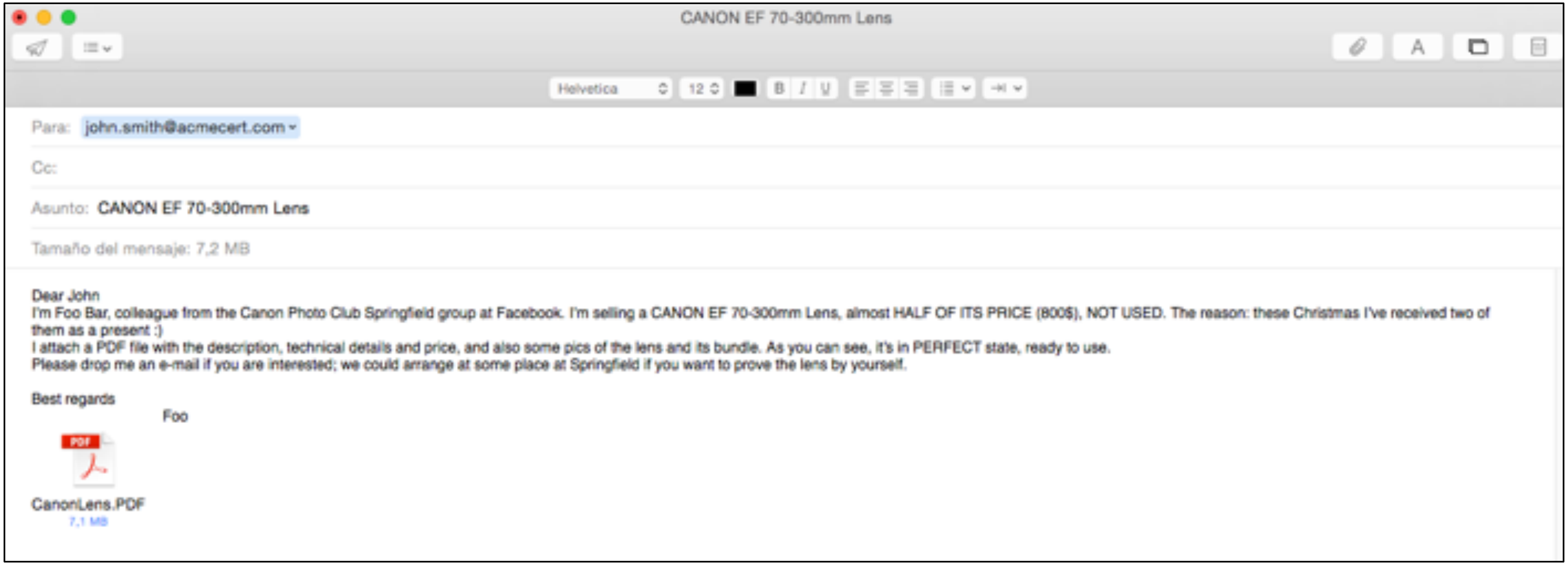


```
root@bt:/pentest/exploits/framework3# ./msfconsole

                                                                  
       =[ metasploit v3.7.0-dev [core:3.7 api:1.0]
+ -- --=[ 675 exploits - 352 auxiliary
+ -- --=[ 217 payloads - 27 encoders - 8 nops
       =[ svn r12286 updated today (2011.04.09)

msf >
```



```
>> list_modules
download                    download a file/directory from a remote system
exit                        exit the client on the other side
get_info                    get some informations about one or multiple clients
getprivs                    try to get SeDebugPrivilege for the current process
interactive_shell           open an interactive command shell
keylogger                   a simple keylogger :-)
memory_exec                 execute a PE executable from memory
migrate                     Migrate pupy into another process using reflective DLL injection
msgbox                      Pop up a custom message box
persistence                 Enables persistence via registry keys
portfwd                     perform local/remote port forwarding using openssh -L/-R syntax
process_kill                kill a process
ps                          list processes
pyexec                      execute python code on a remote system
pyshell                     open an interactive python shell on the remote client
screenshot                  take a screenshot :)
search                      walk through a directory and recursively search a string into files
shell_exec                  execute shell commands on a remote system
shellcode_exec              executes the supplied shellcode on a client
socks5proxy                 start a socks5 proxy going through a client
upload                      upload a file/directory to a remote system
webcamsnap                  take a webcam snap :)
```

…and deliver it!



Para: john.smith@acmecert.com

Cc:

Asunto: CANON EF 70-300mm Lens

Tamaño del mensaje: 7,2 MB

Dear John
I'm Foo Bar, colleague from the Canon Photo Club Springfield group at Facebook. I'm selling a CANON EF 70-300mm Lens, almost HALF OF ITS PRICE (800$), NOT USED. The reason: these Christmas I've received two of them as a present :)
I attach a PDF file with the description, technical details and price, and also some pics of the lens and its bundle. As you can see, it's in PERFECT state, ready to use.
Please drop me an e-mail if you are interested; we could arrange at some place at Springfield if you want to prove the lens by yourself.

Best regards
Foo

CanonLens.PDF
7,1 MB

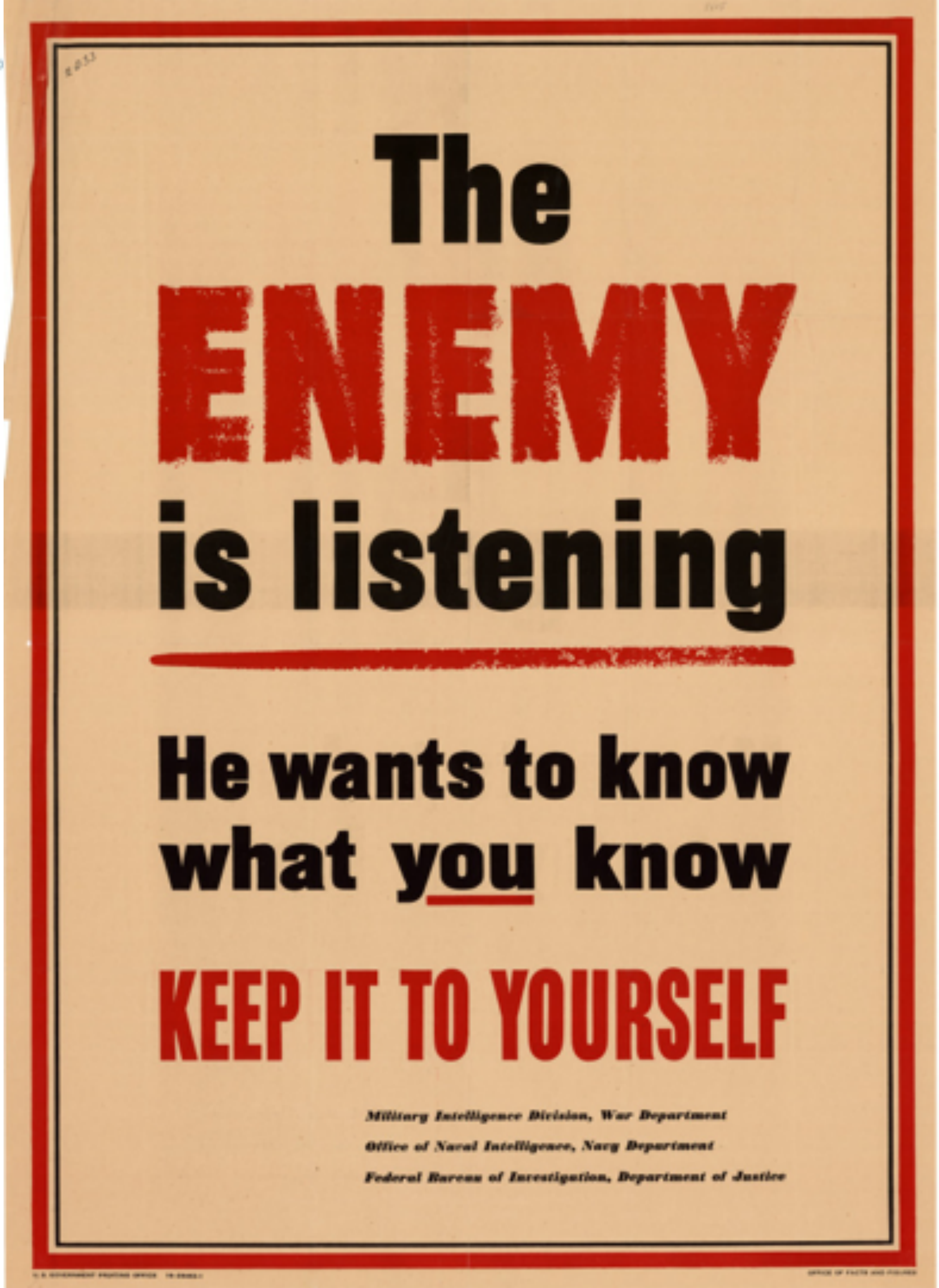
BOOM!

Conclusions

S2 GRUPO
CERT

Main conclusions

Main conclusions



The

ENEMY

is listening

He wants to know what you know

KEEP IT TO YOURSELF

Military Intelligence Division, War Department
Office of Naval Intelligence, Navy Department
Federal Bureau of Investigation, Department of Justice

U. S. GOVERNMENT PRINTING OFFICE 16-[illegible]

OFFICE OF FACTS AND FIGURES

Main conclusions

★ SILENCE MEANS SECURITY ★

БУДЬ НА ЧЕКУ,
В ТАКИЕ ДНИ
ПОДСЛУШИВАЮТ СТЕНЫ.
НЕДАЛЕКО ОТ БОЛТОВНИ
И СПЛЕТНИ
ДО ИЗМЕНЫ.
НЕ БОЛТАЙ!

STRZEŻ
TAJEMNICY
PANSTWOWEJ

THANK YOU!