

**XIII
JORNADAS
STIC
CCN-CERT**



**Por un puñado de
bases de datos**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Simón Roses Femerling

Fundador & CEO, VULNEX
www.vulnex.com

@simonroses

@vulnexsl

www.simonroses.com

AGENDA

1. Fugas de Información
2. Fugas y Contraseñas en España
3. Conclusiones

1. Fugas de Información



<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

information is beautiful

home everything about blog data training books contact      

World's Biggest Data Breaches & Hacks

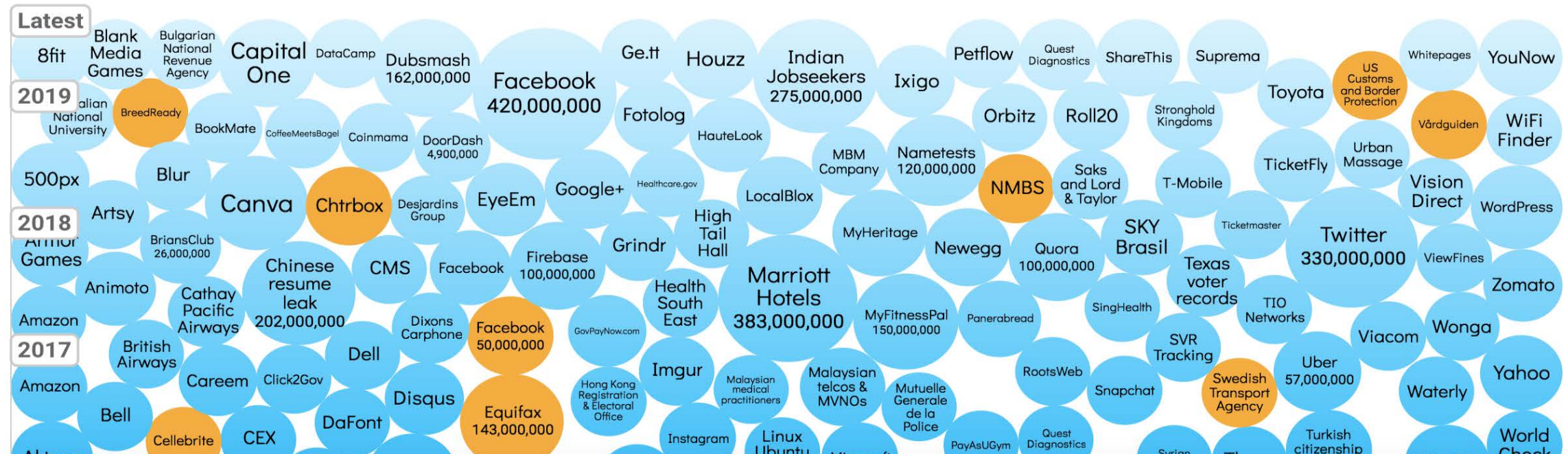
interesting story

Select losses greater than 30,000 records

Last updated: 1 April 2019

Colour YEAR DATA SENSITIVITY Filter

2009  2019 Search...



¡Fugas de Información en números!

- Numero de fugas de información: 9362
- Entre 4 y 6 mil millones de cuentas expuestas

Largest breaches		
	772,904,991	<u>Collection #1 accounts</u>
 verifications.io	763,117,241	<u>Verifications.io accounts</u>
	711,477,622	<u>Onliner Spambot accounts</u>
	622,161,052	<u>Data Enrichment Exposure From PDL Customer accounts</u>
	593,427,119	<u>Exploit.In accounts</u>
	457,962,538	<u>Anti Public Combo List accounts</u>
	393,430,309	<u>River City Media Spam List accounts</u>
	359,420,698	<u>MySpace accounts</u>
	234,842,089	<u>NetEase accounts</u>
	164,611,595	<u>LinkedIn accounts</u>

1. Yahoo - 3 billion
2. Aadhaar - 1.1 billion
3. Verifications.io - 763 million
4. Yahoo - 500 million
5. Marriott/Starwood - 500 million
6. Adult Friend Finder - 412.2 million
7. MySpace - 360 million
8. Exactis - 340 million
9. Twitter - 330 million
10. NetEase - 234 million
11. LinkedIn - 165 million
12. Dubsmash - 162 million
13. Adobe - 152 million
14. MyFitnessPal - 150 million
15. Equifax - 148 million
16. eBay - 145 million
17. Canva - 137 million
18. Apollo - 126 million
19. Badoo - 112 million
20. Evite - 101 million
21. Quora - 100 million
22. VK - 93 million
23. MyHeritage - 92 million
24. Youku - 92 million
25. Rambler - 91 million
26. Facebook - 87 million
27. Dailymotion - 85 million
28. Dropbox - 69 million
29. tumblr - 66 million
30. Biggest data breaches infographic
31. How UpGuard can prevent data breaches and find leaked credentials

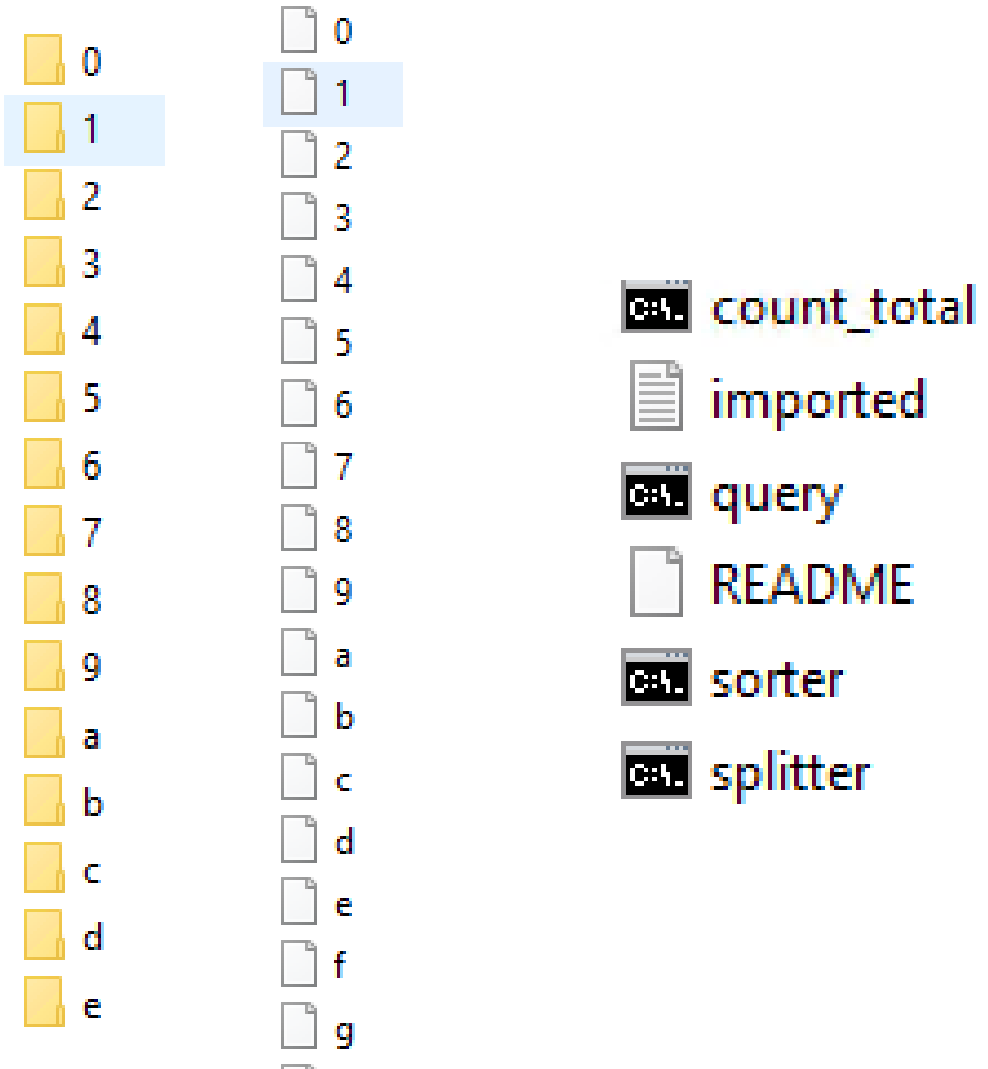
¿Cómo es posible y tipo de información expuesta?

- Incidente de seguridad
 - Malas prácticas de seguridad > AWS S3, MongoDB, ElasticSearch, etc.
 - Ciberataque
- Información expuesta:
 - Nombre
 - Usuario
 - Contraseñas
 - Dirección de correo
 - Dirección física
 - Número de teléfono
 - Comentarios
 - DNI / Identificador
 - Información de identificación personal (PII)



Base de Datos Real

- Navidad 2017: una BBDD con 1.4 mil millones de credenciales en texto claro
- Correos/contraseñas



Direcciones de correo

```
- ^ea.mde.es');  
- @oc.mde.es');  
- @oc.mde.es');  
- rezaller@oc.mde.es');  
- @et.mde.es');  
- @et.mde.es');  
- esm@et.mde.es');  
- @oc.mde.es');  
- @fn.mde.es');  
- @ea.mde.es');  
- m@fn.mde.es');  
- @oc.mde.es');  
- @et.mde.es');  
- @oc.mde.es');  
- u@et.mde.es');  
- @et.mde.es');  
- @et.mde.es');
```

Credenciales

haw
noal
marc
spb@
dren
mad
w_n
evel
don
Taft.
pete
zai@

7f664d97a024b827a2eecd288e
90c95641442f2be0ef7774e139fb1f

1c22fb716136e92b8d072a97cdc
e09395d14db107f20874057076a5ce
7b7661d753069044a7c629cb9ca94f
ea450873d68d525ae55ffb2d87a2bfe9b85
32ad9a4e65c90172376774c298a8ef547
cfo4f83f42fd86d35a0aff3fea20dcb94938a
70854e336318fd1fd04023f3580b29de8
0x
017b0c300fa343f643f731

Cracking de contraseñas

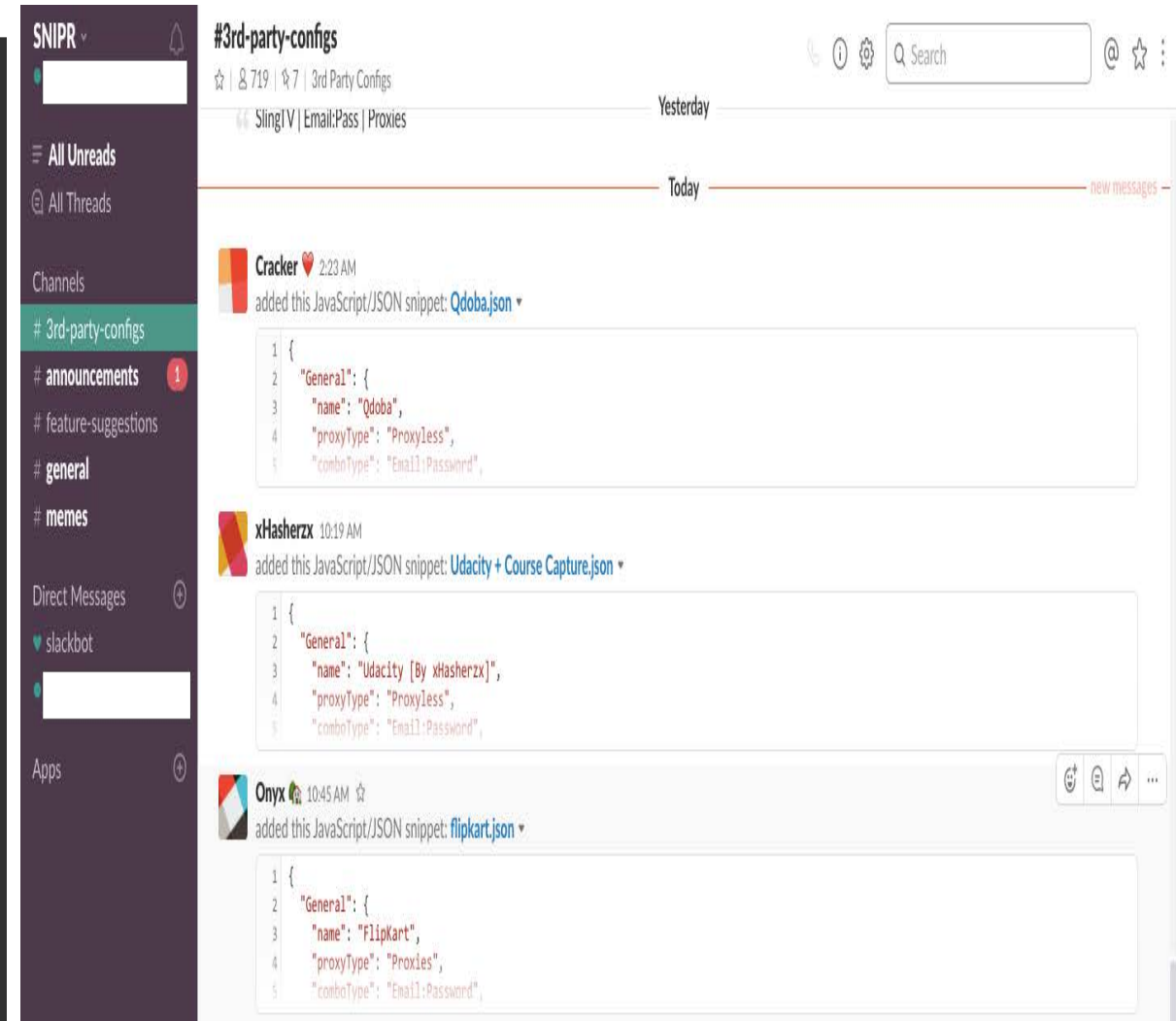
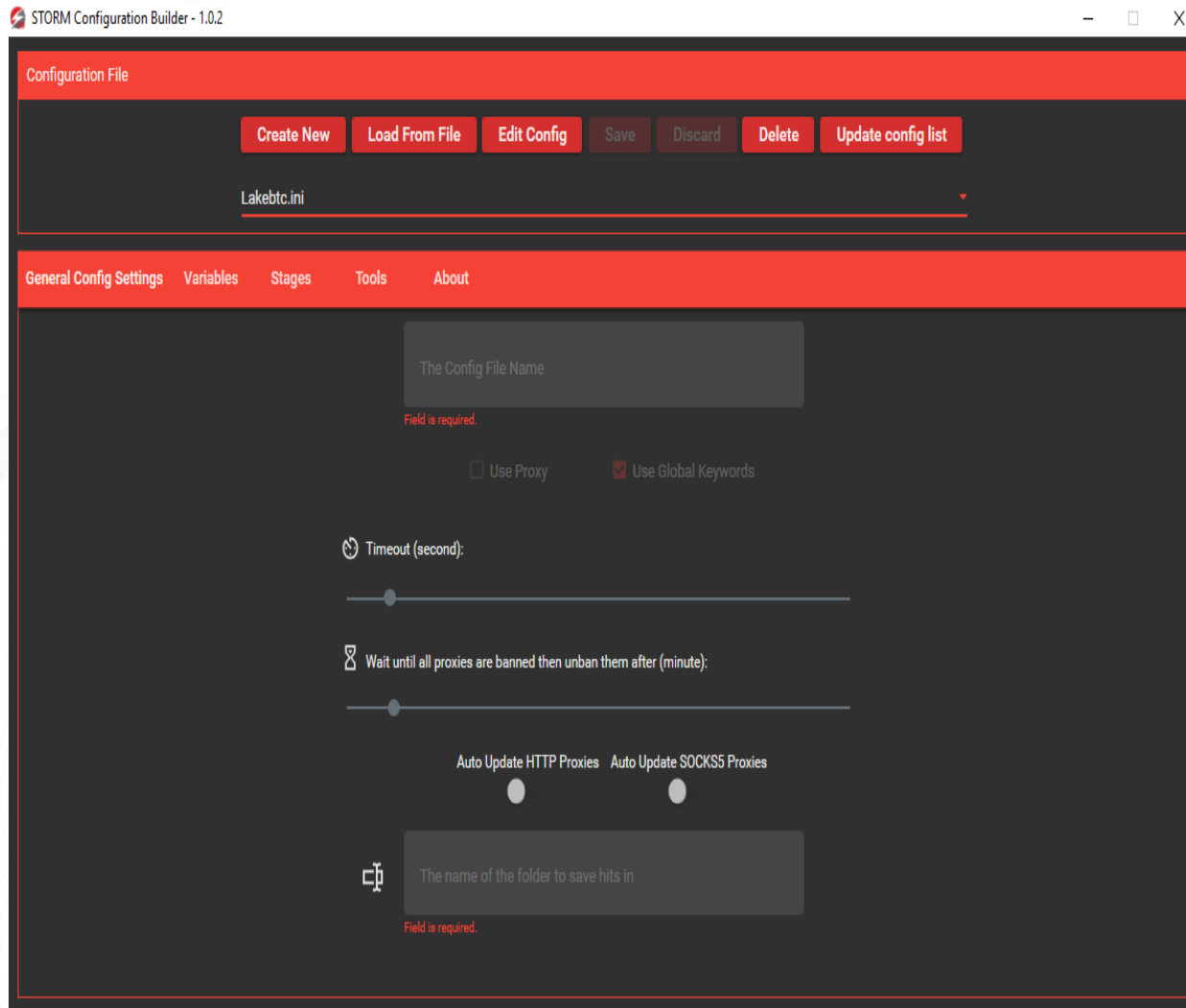
- Muchos expertos en seguridad compiten en:
 - Número contraseñas rotas en 24-48 horas
 - Total de contraseñas rotas



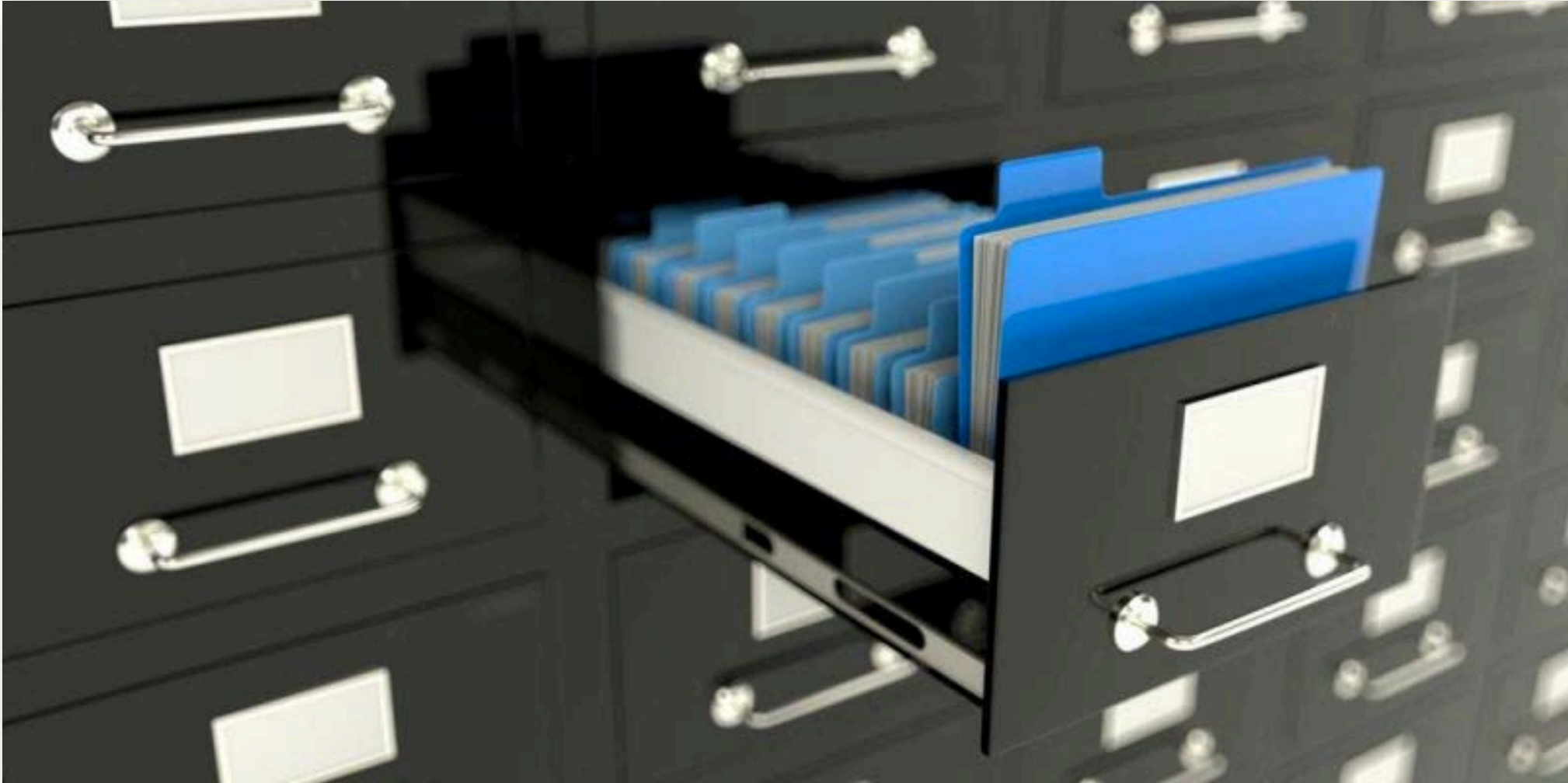
Credential Stuffing

- “”” un tipo de ciberataque en el que las credenciales de cuentas robadas, que generalmente consisten en listas de nombres de usuario y / o direcciones de correo electrónico y las contraseñas correspondientes (a menudo debido a una fuga de datos), se utilizan para obtener acceso no autorizado a cuentas de usuario a través de solicitudes de inicio de sesión automatizadas a gran escala dirigidas contra una aplicación web”””
- https://en.wikipedia.org/wiki/Credential_stuffing
- https://www.owasp.org/index.php/Credential_stuffing
- <https://attack.mitre.org/tactics/TA0006/>

Herramientas de *Credential Stuffing*



2. Fugas y Contraseñas en España



Fuga de datos en España

- Telefónica tapa un agujero de seguridad que dejó al descubierto millones de datos de sus clientes
https://www.lespanol.com/economia/empresas/20180716/telefonica-agujero-seguridad-descubierto-millones-datos-clientes/322967853_0.html
- El gran 'hackeo' de la prostitución española (09/08/19)
https://www.elconfidencial.com/tecnologia/2019-08-09/chicas-compania-scorts-valencia-barcelona-datos-personales_2170179/
- Caja Rural (30/11/19)
<https://lacronicadesalamanca.com/256575-la-fuga-de-datos-de-caja-rural-afecta-sobre-todo-a-castilla-y-leon/>

¿A quién afecta?

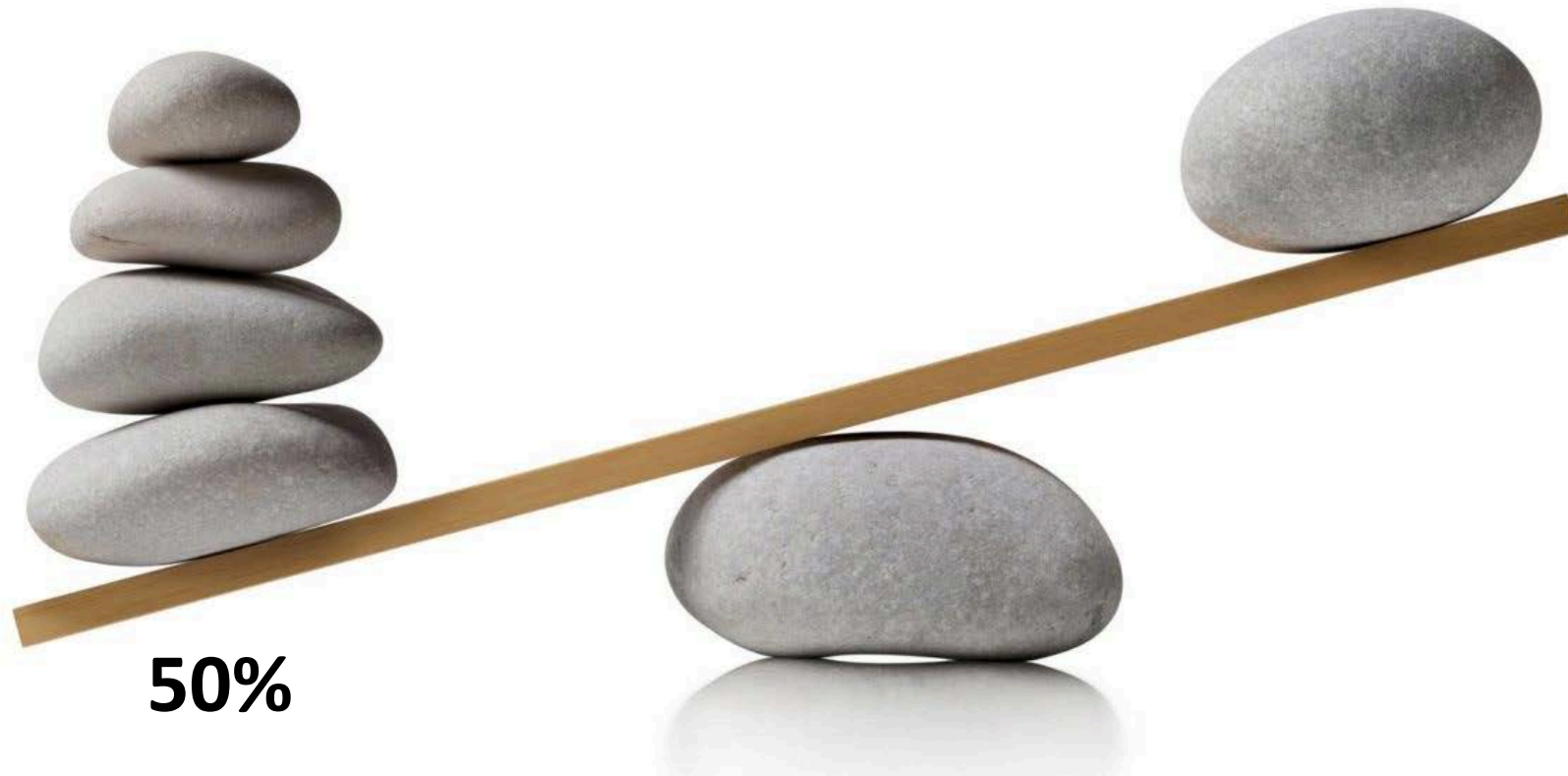
- Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE)
- Defensa
- Gobierno y partidos políticos
- IBEX35
- Tu cuenta de empresa, personal, etc....
- ¡Millones de cuentas!



Ashley Madison

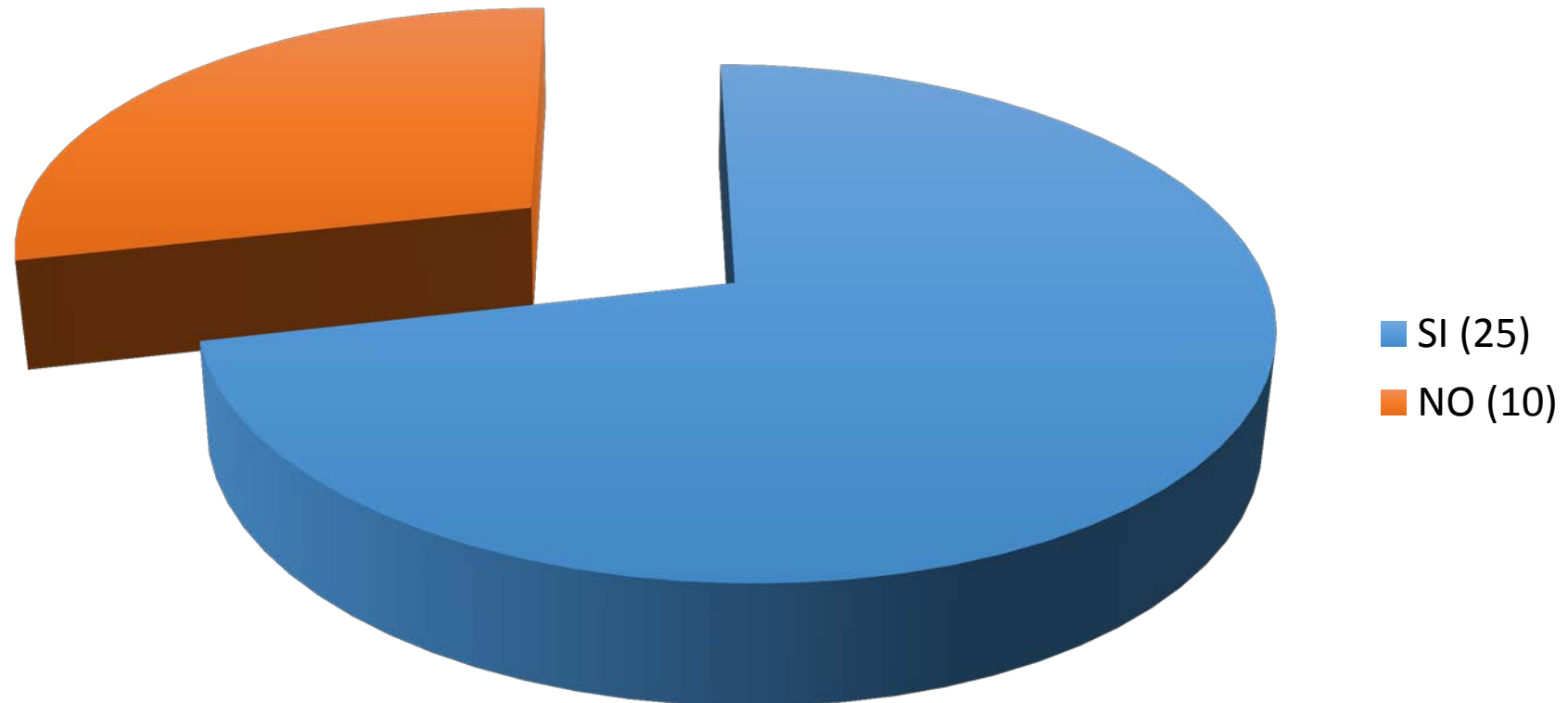


Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE)



IBEX35

Empresas IBEX35 aparecidas en fugas de información



Algunas contraseñas nacionales...

- 1111111111
- trabajoeneuropa
- **123456**
- *9999999999*
- 12345678901234567890
- guardiacivil
- MalagaCF
- Rmadrid
- viscaelbarca1
- superman
- spiderman
- gazpacho
- soylamejor
- Zurullo
- pollon
- pene1coño2
- ---sexo---
- pordebajodelamesa123456789
- Gilipollas
- gilipollasmenorquin
- PïCЪP»PïCЪP»PïP»
- \$HEX[6c61f1656d61]
- hacker

3. Conclusiones



Conclusiones

- Problema global
- Analizar nuestra superficie de ataque
- Comprobar tu correo, contraseña en <https://haveibeenpwned.com/>



Gestionar la fuga de información

- Como gestionar una fuga de información en un despacho de abogados
<https://www.aepd.es/media/guias/guia-incibe-aepd-gestionar-fuga-de-informacion.pdf>
- GUIA DE GESTIÓN DE FUGA DE INFORMACIÓN
https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/protege_tu_informacion/guia_gestion_fuga_informacion.pdf
- Guía para la gestión y notificación de brechas de seguridad
<https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf>



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional