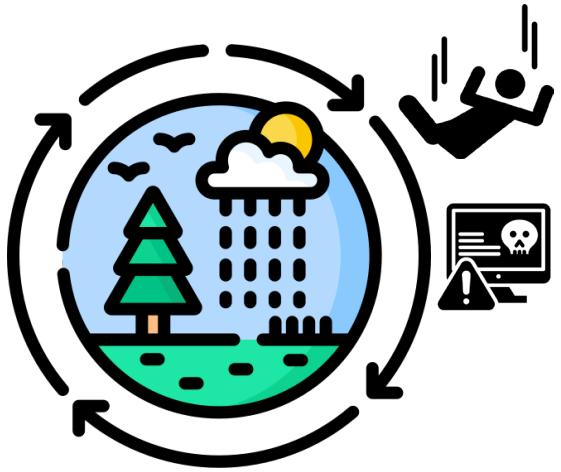
60' Express – PYME

Ciberperiplo

v.1.2.24

un viaje ¿inesperado?



"Lo que necesitamos son optimistas que estén totalmente convencidos de que la catástrofe es ciertamente inevitable ..."

E.F. Schumacher, 24 de Enero de 1974
Prefacio en "Lo pequeño es Hermoso"

Jorge Medina

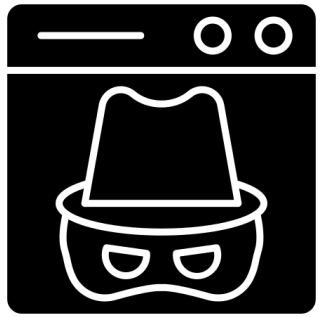
GRUPOTELCIA Tecnología con Alma!

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

CEEI Centro Europeo de Empresas e Innovación de Valencia

Última versión disponible en https://ciberperiplo.org

tamaño usuarios / equipo de apoyo
¿psicólogo, abogado?



¿ALGÚN DATO EN LA DARKWEB?

¿QUÉ INFORMACIÓN?

Base tecnológica, invitados al viaje

Objetivos Charla

La solución al problema está en comprenderlo

SOLUCIONES CONCRETAS

Objetivos Charla

La solución al problema está en comprenderlo

SOLUCIONES CONCRETAS

ignorancia = ¿felicidad?

+ complejo(fab.) = - libertad

"El conocimiento es la fuente más democrática de poder"
Alvin Toffler

Lecturas para entender contexto (para humanos curiosos):
El shock del futuro (1970), La tercera ola (1980), El cambio del poder (1990)
Alvin Toffler

Estructura charla

CONTEXTO ACTUAL

de dónde venimos

a dónde vamos

CIBERPERIPLO

el viaje, el ¿regreso?

errores y problemas

¿DARKWEB?

no tan oscura

¿qué datos realmente?

SOLUCIONES

bueno, bonito, barato

checklist, ejemplos 

Preguntas

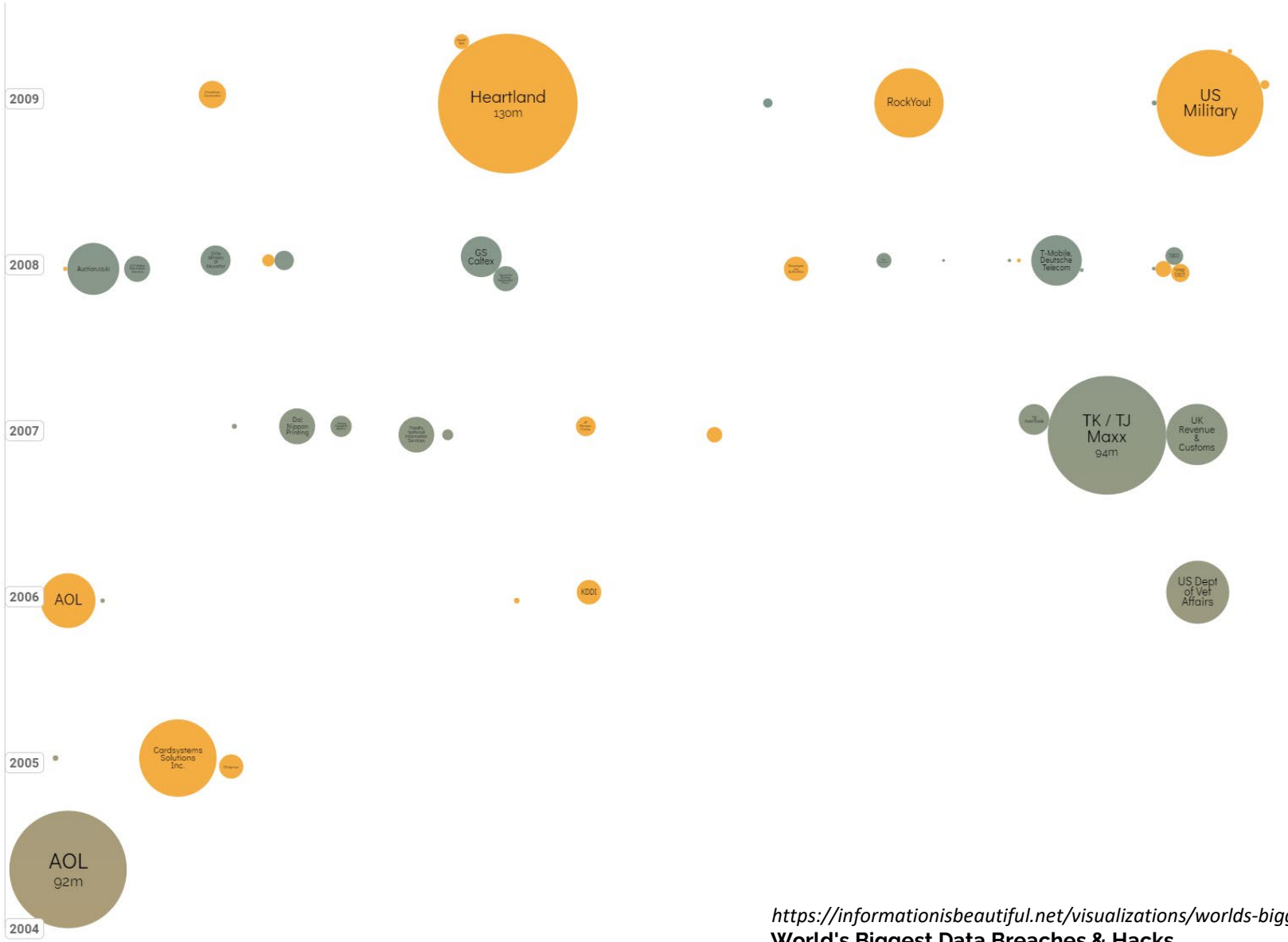
CONTEXTO ACTUAL

de dónde venimos

a dónde vamos

"La realidad y el significado no estaban ocultos en algún lugar detrás de las cosas, estaban en ellas, en todas ellas.“

Hermann Hesse



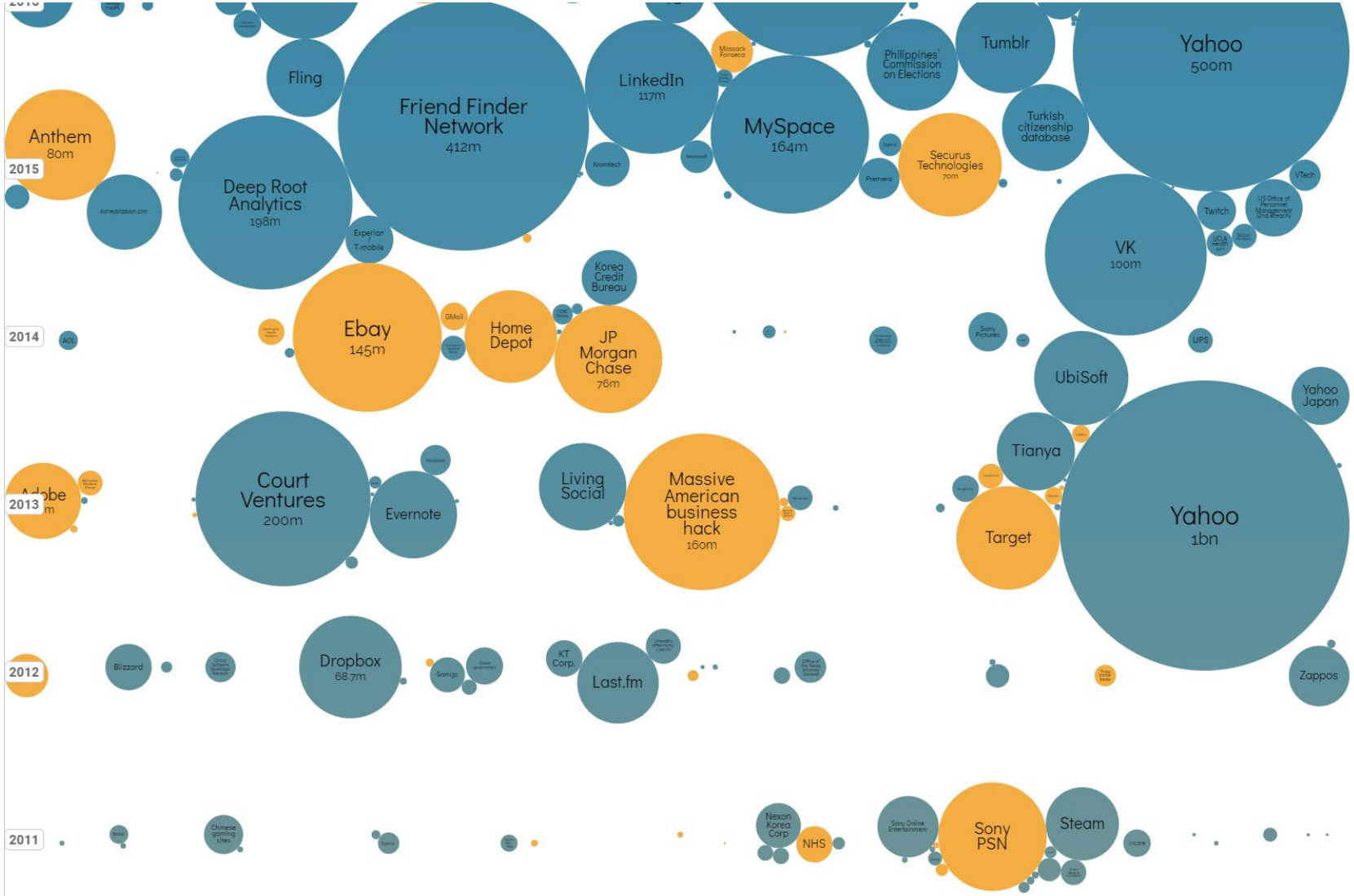
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

World's Biggest Data Breaches & Hacks

David McCandless & Tom Evans
Information is Beautiful

sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others
see the data

Contexto

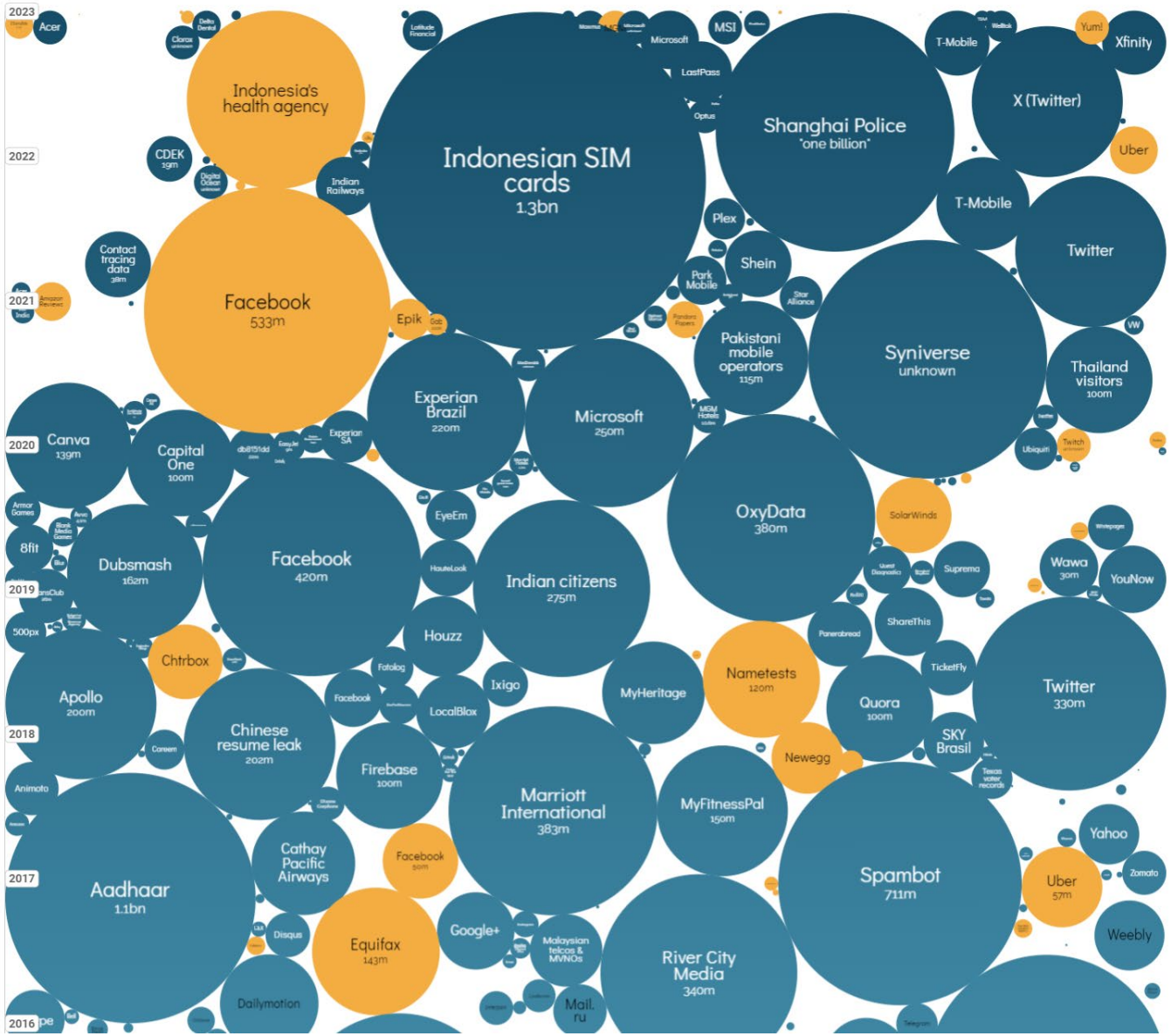


World's Biggest Data Breaches & Hacks

David McCandless & Tom Evans
Information is Beautiful

sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others
see the data

Contexto

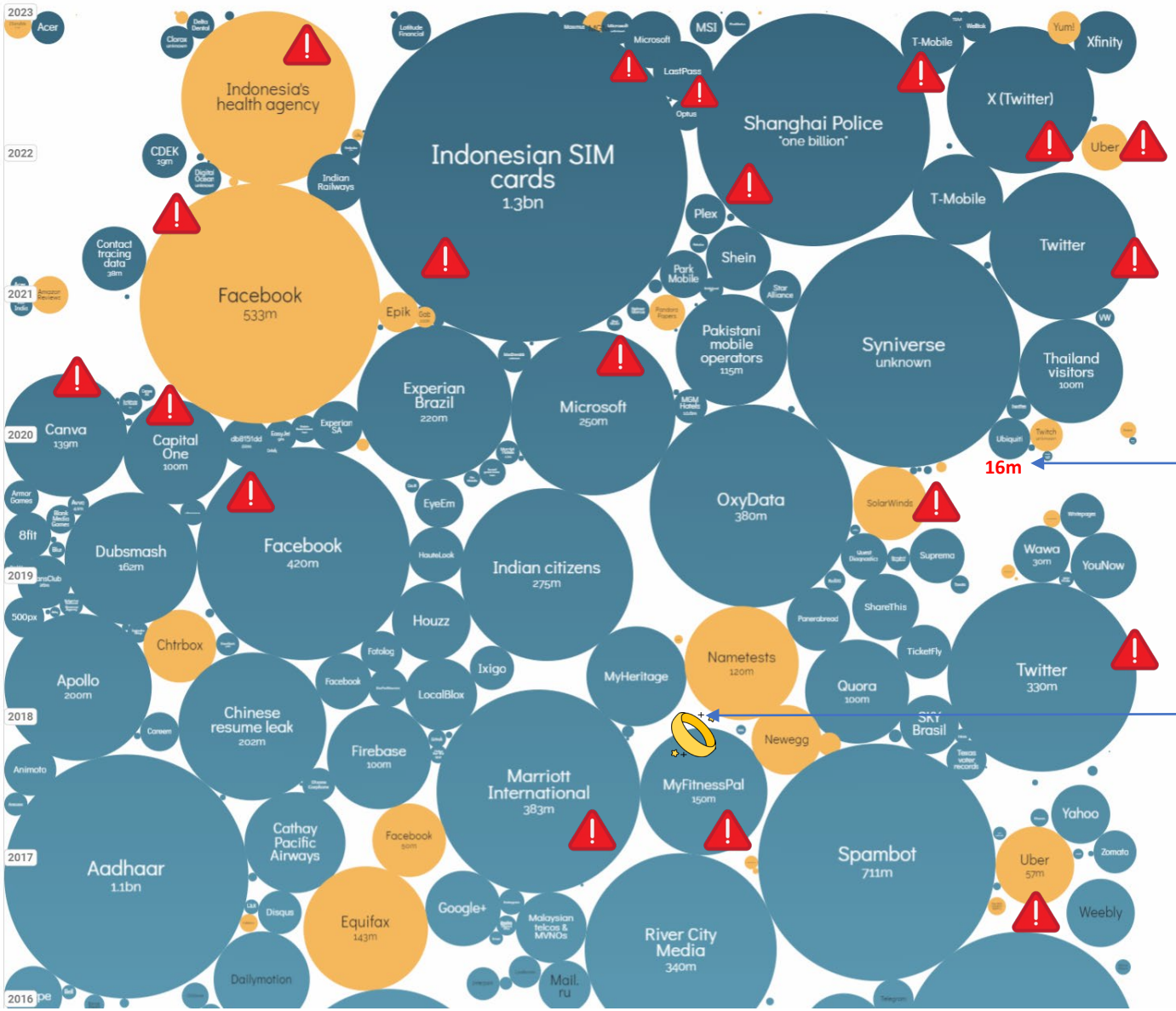


World's Biggest Data Breaches & Hacks

David McCandless & Tom Evans
Information is Beautiful

sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others
see the data

Contexto

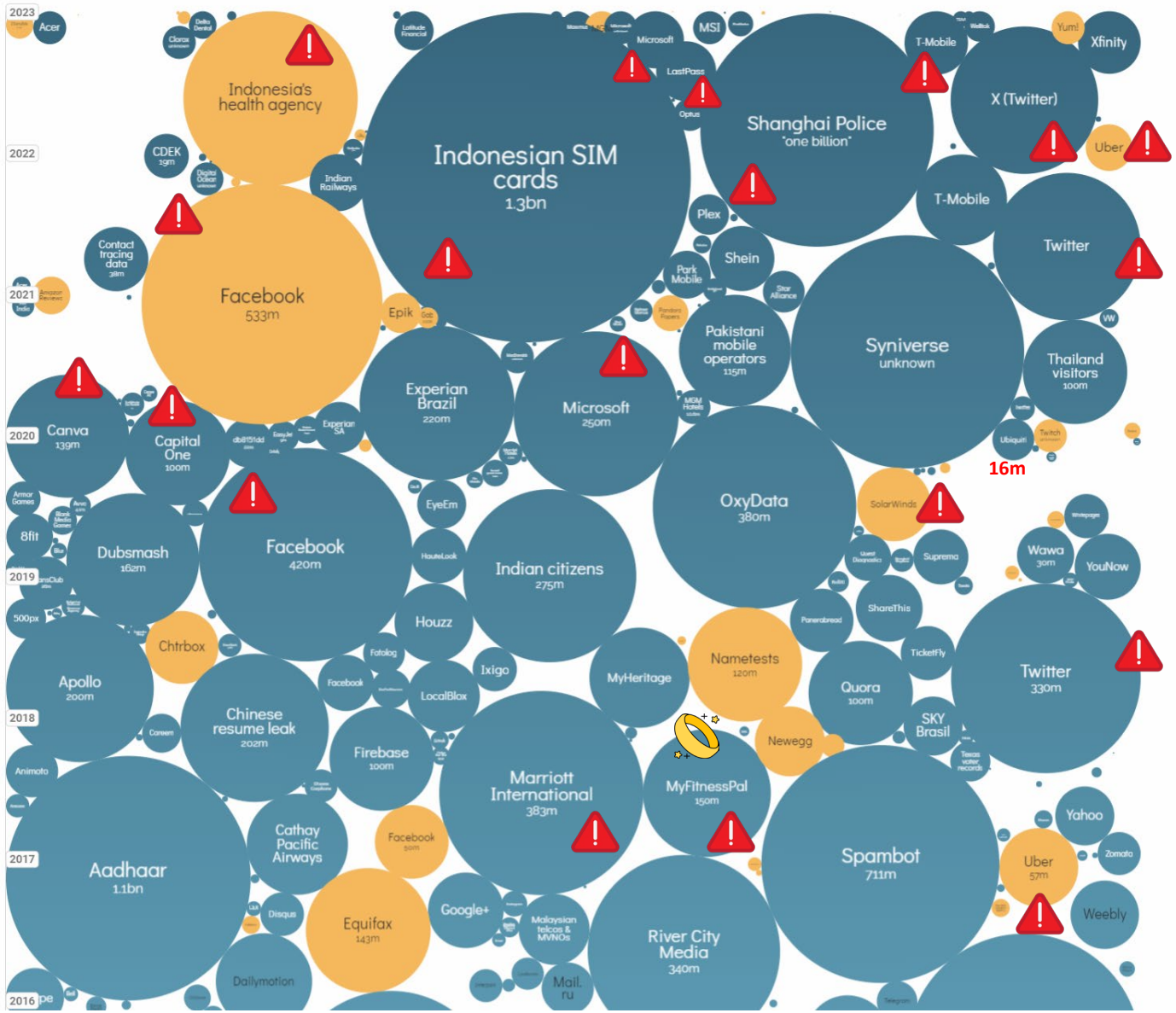


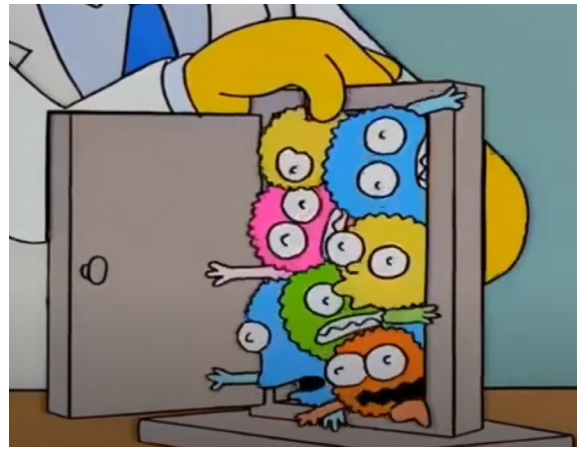
World's Biggest Data Breaches & Hacks

David McCandless & Tom Evans
Information is Beautiful

sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others
see the data

Contexto





Los Simpson
Sr. Burns "indestructible"

Ojo a nuestras Realidades

World's Biggest Data Breaches & Hacks
David McCandless & Tom Evans
Information is Beautiful

sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others
see the data

¿Realidades?

Ahora todo es más sencillo…

Todo funciona mejor y sin fallos…

¿Realidades?

Ahora todo es más sencillo…

Todo funciona mejor y sin fallos…

Ticket con gestor passwords (entre los top3 mundiales) más de 1 semana abierto sin contestación

Intento de recuperación de acceso a dominio de Google Workspace teniendo el control de DNS y correos. 2 semanas.

Intento de recuperación de acceso a dominio Microsoft por doble factor de auth perdido de exempleado rol admin. zZZzzzzZZZzz

¿Realidades?

Ahora todo es más sencillo…

Todo funciona mejor y sin fallos…

Ticket con gestor passwords (entre los top3 mundiales) más de 1 semana abierto sin contestación

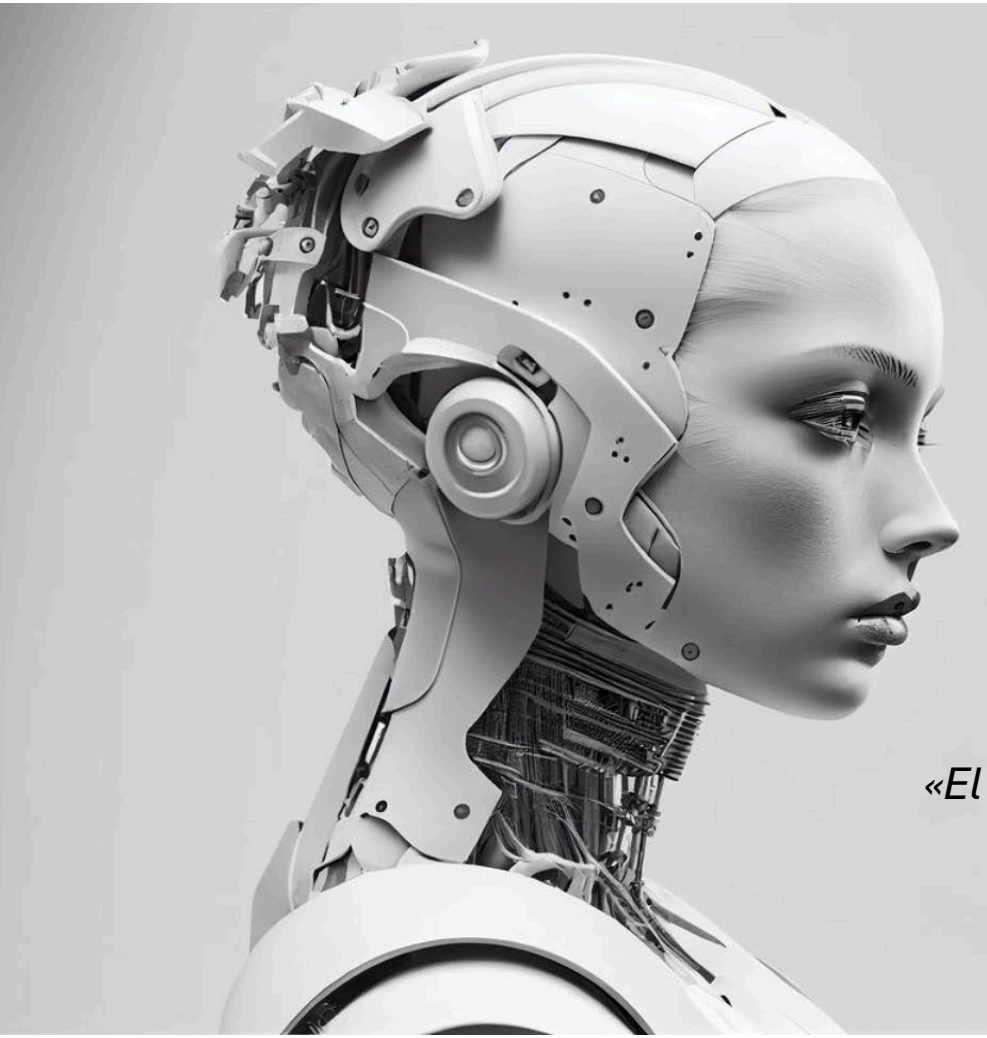
Intento de recuperación de acceso a dominio de Google Workspace teniendo el control de DNS y correos. 2 semanas.

Intento de recuperación de acceso a dominio Microsoft por doble factor de auth perdido de exempleado rol admin. zZZzzzzZZZzz

Es por seguridad…

dependencia = control = poder = subscripción pago por uso

¿Y ahora?



IA <10

¿TransHumanos?

«El futuro no está escrito. Es lo que hacemos hoy lo que puede cambiarlo»

Sarah Connor. Terminator 2

¿Y ahora?

Realidad Virtual Mixta

¿DARKWEB?

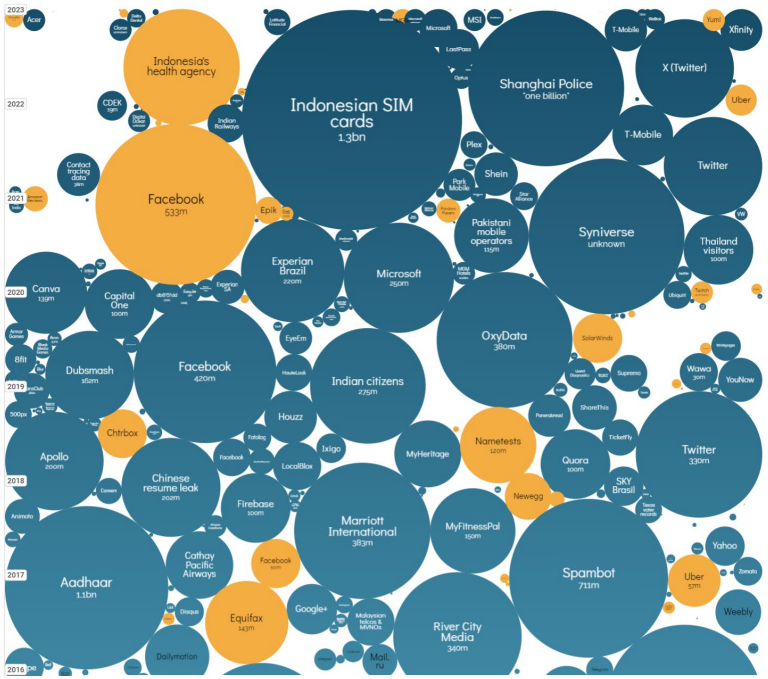
no tan oscura

¿qué datos realmente?

"A mitad del camino de la vida,
en una selva oscura me encontraba
porque mi ruta había extraviado."

Dante Alighieri: La divina comedia. Infierno, Canto I

Formato
Filtraciones en darkweb



sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others
see the data

David McCandless & Tom Evans
Information is Beautiful

Date Found	Email	Password Hit	Source	Type	Origin	PII Hit
03/27/20	[redacted]@bird.com	liny****	id theft forum	Not Disclosed	Not Disclosed	None
03/26/20	[redacted]@bird.com	ab3c****	id theft forum	Not Disclosed	Not Disclosed	None
03/19/20	[redacted]bird.com		id theft forum	Not Disclosed	Not Disclosed	None
03/16/20	[redacted]r@bird.com	DRAG****	id theft forum	Not Disclosed	Not Disclosed	None
02/19/20	[redacted]ey18@bird.com	ilov****	id theft forum	Not Disclosed	Not Disclosed	None
02/19/20	[redacted]ird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]y@bird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]@bird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]e@bird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]ird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]ird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]ird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]@bird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]3@bird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/17/20	[redacted]bird.com		id theft forum	Not Disclosed	Not Disclosed	None
02/09/20	[redacted]g@bird.com	ilov****	id theft forum	Not Disclosed	Not Disclosed	None

¡Ojo fines comerciales! nuevo sistema para :
call centers
spammers

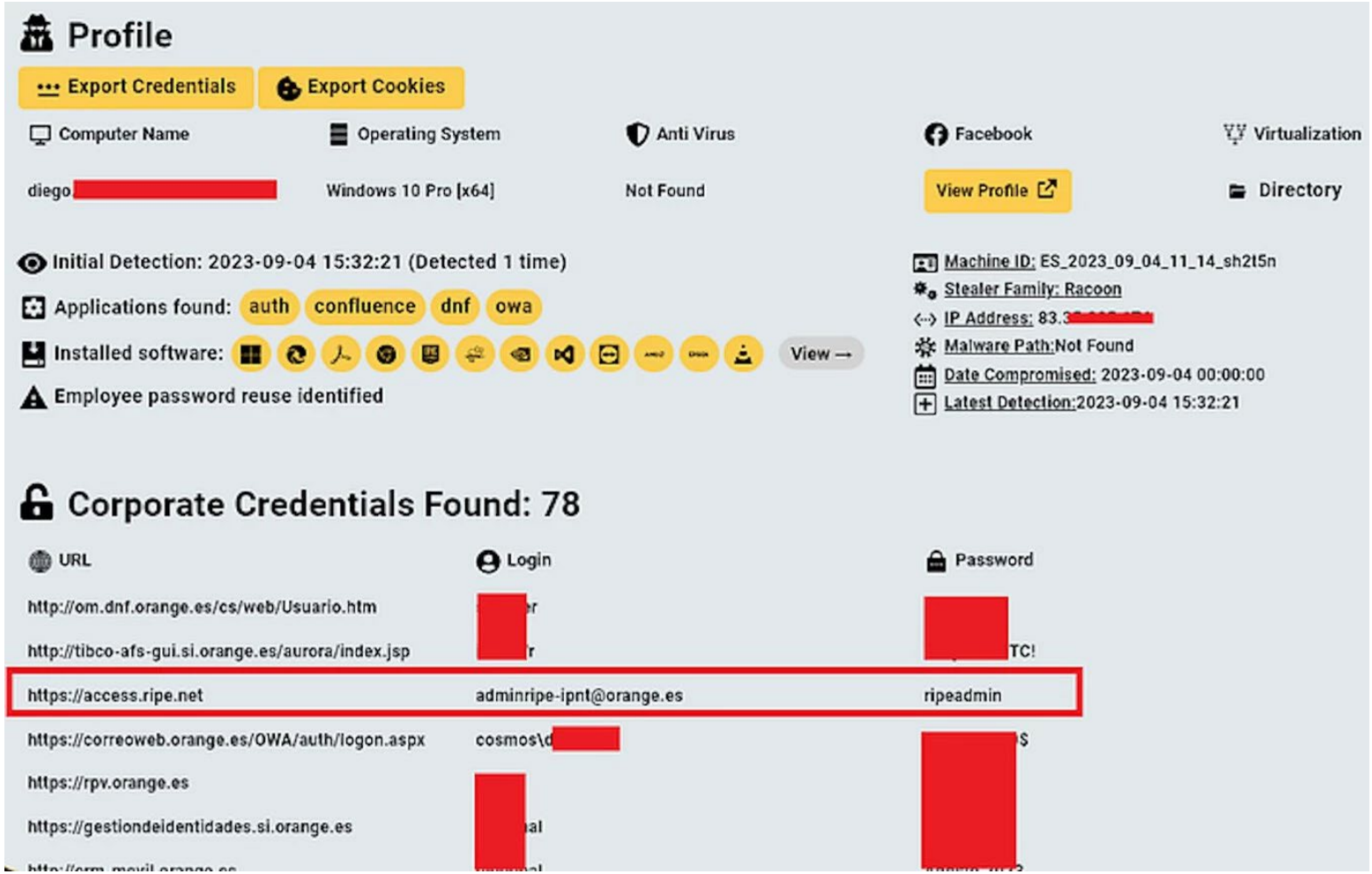
¿darkweb?

Orange Enero 2024

RIPE NCC

A las pocas horas mail a todos los miembros invitándonos a activar MFA (hasta a los que ya lo teníamos)

2FA ?



Hudson Rock

¿darkweb?

Consulta de infiltraciones

Google One

Estás monitorizando la dark web

Resumen de los resultados

17 brechas de seguridad de datos han provocado que tu información se filtre en la dark web. Consulta los detalles y toma medidas para protegerte.

Ver todos los resultados

Resultados con tu información

Se han encontrado datos de tu perfil de monitorización en la dark web. Has añadido **3 de 5** tipos de información. Editar perfil de monitorización

Nombre	1 resultado	Número de teléfono	2 resultados	Correo electrónico	16 resultados

Resultados con otros datos

Se ha encontrado más información en la dark web junto con la que se incluía en tu perfil de monitorización.

Contraseña	9 resultados	Nombre	2 resultados	Dirección	2 resultados
Número de teléfono	2 resultados	Mostrar menos			

Tus resultados

Consulta los detalles sobre las brechas de seguridad de datos que han filtrado tu información en la dark web. Descubre cómo protegerte mejor según cada resultado.

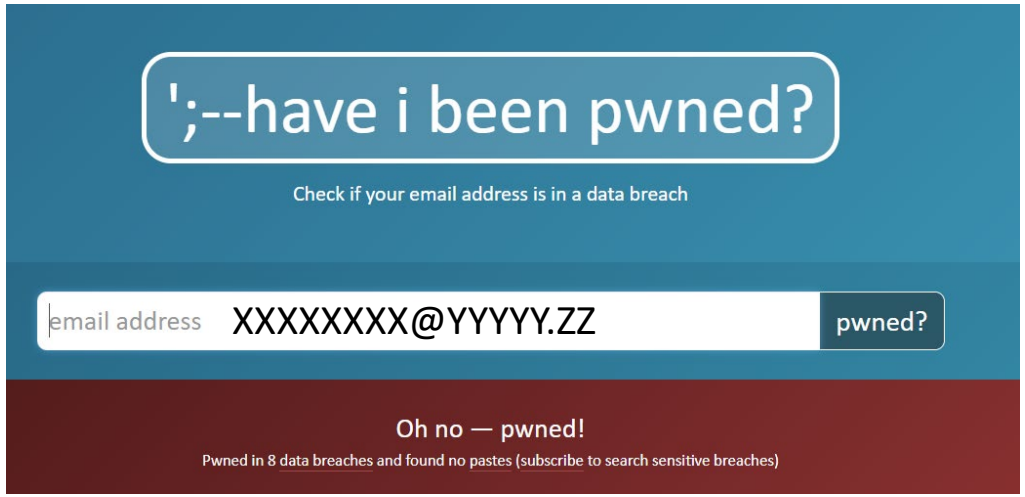
Todo • 17

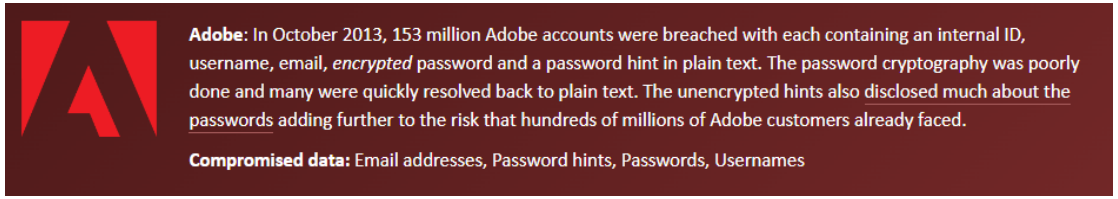
opentable.com 6 feb 2024	CORREO ELECTRÓNICO, CONTRASEÑA	>
Qakbot Botnet 29 sept 2023	CORREO ELECTRÓNICO	>
Spanish Consumer Data Leak 17 nov 2022	CORREO ELECTRÓNICO, NOMBRE, DIRECCIÓN, NÚMERO DE TELÉFONO	>
October 2021 Combolist 28 oct 2021	CORREO ELECTRÓNICO, CONTRASEÑA	>
Scraped Facebook Profile Data 8 abr 2021	NOMBRE, NÚMERO DE TELÉFONO	>
Sensitive Source 4 mar 2021	NÚMERO DE TELÉFONO, CORREO ELECTRÓNICO, DIRECCIÓN	>
presteamshop.com 17 dic 2020	CORREO ELECTRÓNICO	>
Leadhunter 12 mar 2020	CORREO ELECTRÓNICO	>
Verifications.io 28 mar 2019	CORREO ELECTRÓNICO	>
Collection #5 Combo List 6 feb 2019	CORREO ELECTRÓNICO, CONTRASEÑA	>
AP MYR and Zabugor Combo List 6 feb 2019	CORREO ELECTRÓNICO, CONTRASEÑA	>
Collection #4 Combo List 6 feb 2019	CORREO ELECTRÓNICO, CONTRASEÑA	>
Collection #2 Combo List 29 ene 2019	CORREO ELECTRÓNICO, CONTRASEÑA	>
Collection #1 Combo List 25 ene 2019	CORREO ELECTRÓNICO, CONTRASEÑA	>

¿darkweb?

Consulta de infiltraciones

https://haveibeenpwned.com/





CIBERPERIPLO

el viaje, el ¿regreso?

errores y problemas

"Los mitos son metáforas de la potencialidad espiritual del ser humano, y los mismos poderes que animan nuestra vida animan la vida del mundo..."

Joseph Campbell
Joseph Campbell Foundation (https://www.jcf.org/)

El viaje es lo importante, EVITA hacerlo

Si lo <u>preparas antes</u>, pero te toca hacerlo:

– NO lo harás ¿SOLO? *("Espera mi llegada con la primera luz del quinto día al alba, mira al este"*)
– NO te tocará pedir un préstamo para poder pagarlo* *servicios pre*
– NO verás a tus empleados jugando al juego del calamar

¿Cuándo suele iniciarse?
¿Cuándo se inició realmente?

El viaje es lo importante, EVITA hacerlo

Si lo <u>preparas antes</u>, pero te toca hacerlo:

– NO lo harás ¿SOLO? *("Espera mi llegada con la primera luz del quinto día al alba, mira al este"*)
– NO te tocará pedir un préstamo para poder pagarlo* *servicios pre*
– NO verás a tus empleados jugando al juego del calamar

¿Cuándo suele iniciarse?
¿Cuándo se inició realmente?

Escenarios:

1. Tienes **Backup** SEGURO, <u>REVISADO por HUMANOS</u> Y **A SALVO**
2. Tu primo/sobrino/contable/tú, no había revisado los backups (o no sabes que es un backup)
3. Ni te suena qué es eso de lopd…

4.- Gran Empresa, Arquitecturas complejas, Operadores, Centros de Datos.

¿Por qué empieza el viaje?

La llamada a la acción

Puntos de entrada más comunes en pyme
bot/scan puertos abiertos router. RDP (terminal server). Servicios sin updates (CVE)
VPN con vulnerabilidades o 0Day
descargas software aparentemente lícito
adjuntos correos electrónicos
cámaras/grabadores de empresas de seguridad abiertas al mundo sin updates periódicas con acceso al resto de la red
software ilegal con “regalito”
passwords débiles, reusadas y sin MFA

inscrito en el pronaos (delante) del templo de Apolo en Delfos

MOTIVO: rescate $$$

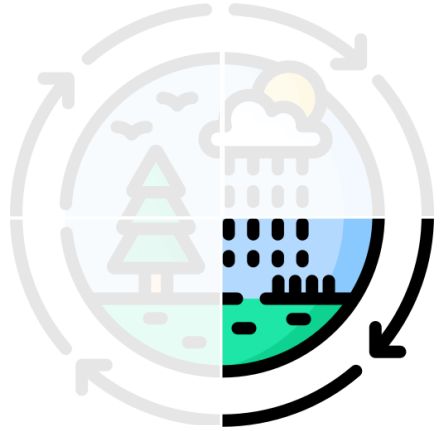
Backup

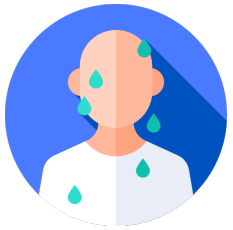
CVE, Common Vulnerabilities and Exposures
0Day, Ataque de día cero, cve desconocido

¿Por qué empieza el viaje?

Iniciación. Las pruebas

Errores y Realidades *(suele ser combinación de varias) revisar documento de seguridad LOPD*
¿formación/concienciación del personal?
¿política de passwords?¿reusados?¿gestor de passwords?¿MFA?
¿solución antivirus/firewall/aplicaciones? ¿no gratuito?¿NGFW?
¿copia de seguridad segura y usable? ¿revisadas? ¿aisladas?
¿ordenadores encendidos 24 horas (anydesk/teamviewer/RDP por comodidad)?
¿softwares ilegales?
¿sistemas viejos, win7, servers < win2016. no updates?
¿rebotes internos, segmentación?
¿mantenimientos proactivos de algún tipo? ¿alguien llevando IT, LOPD?
¿usuarios permisos admin?
¿personal IT con acceso a todo, buenas prácticas?
¿disaster recovery previsto?





Backup

¿Dónde estamos?

Revelación

¿darkweb?
¿el qué?

¿sabemos punto de entrada?¿datos?
¿siguen dentro?

purgatorio / infierno

psicológico
clientes
empleados
incertidumbre

legal, notificación AGPD, clientes, etc...
antes/después

¿destrucción de pruebas?
¿informático de la esquina?
¿se prioriza servicio?

¿disponibilidad?
¿backups?

¿Y ahora?

¿Transformación?

¿Análisis del por qué?

Causas REALES y por eso volverán

Velocidad, tiempo

Déficit de atención

Hibris (orgullo, vanidad, arrogancia)

¿Y ahora?

Regreso, integración

¿Hemos aprendido?

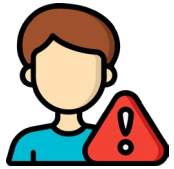
El viaje se va a repetir, es una ***historia interminable…***

“No existe un llegar, solo existe el movimiento de aprender y en eso radica la belleza de la vida.”

Krishnamurti

Páginas web, tiendas on-line, reservas, intranet, erp, crm...

¿Wordpress?
¿WooCommerce?



¿Entorno cloud más robusto, seguro, controlado?

Respuesta: *goto páginas 11, 14*

SOLUCIONES

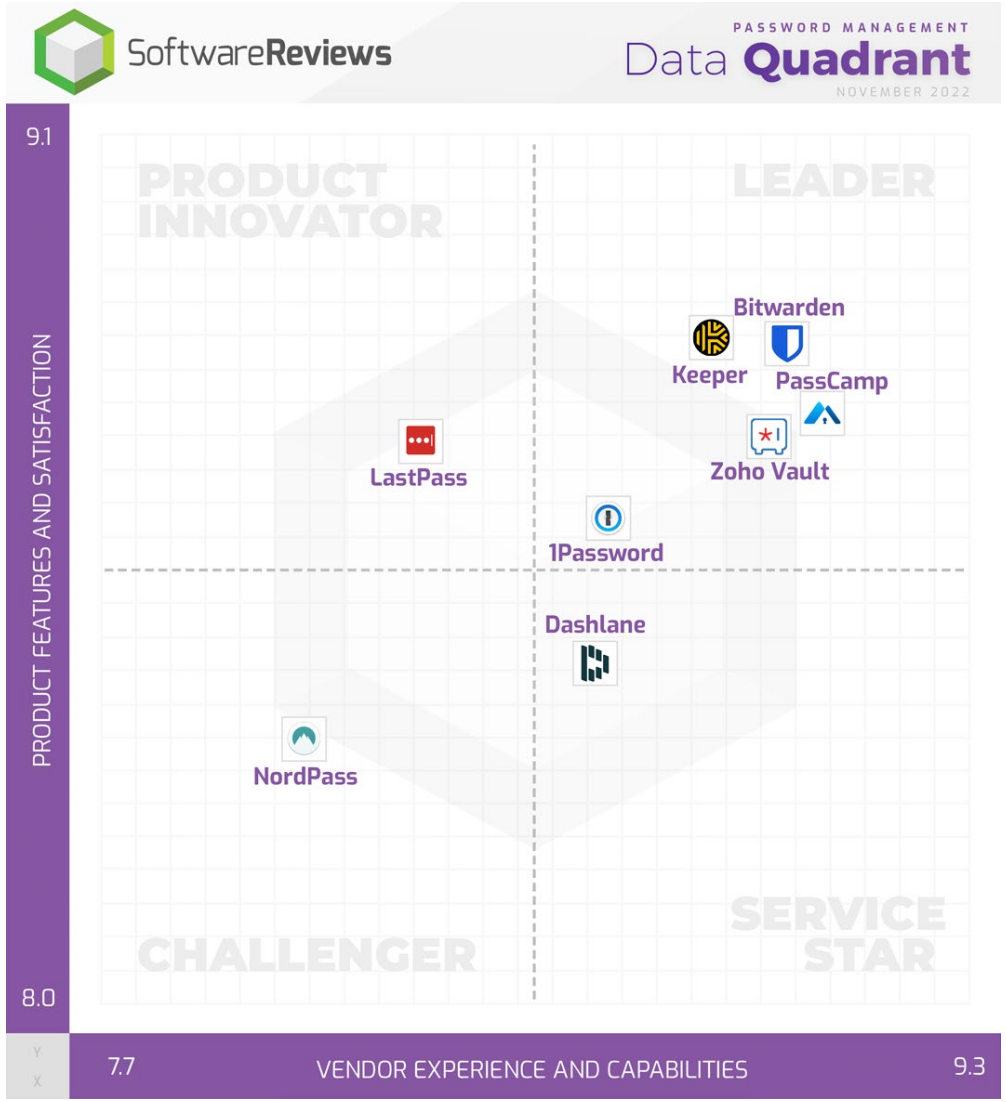
bueno, bonito, barato

checklist, ejemplos 

"Cuando emprendas tu viaje a Ítaca
pide que el camino sea largo,
lleno de aventuras, lleno de experiencias.
No temas a los lestrigones ni a los cíclopes
ni al colérico Poseidón, ..."

Konstantino Kavafis. Ítaca

Gestión passwords, MFA



Online

Offline

KeePass
no plugins, gracias

KeePassXC
Cross-Platform Password Manager

Combinación

** las herramientas son ejemplos, existen infinidad de ellas...*

Passkeys

PRIVACIDAD & SEGURIDAD

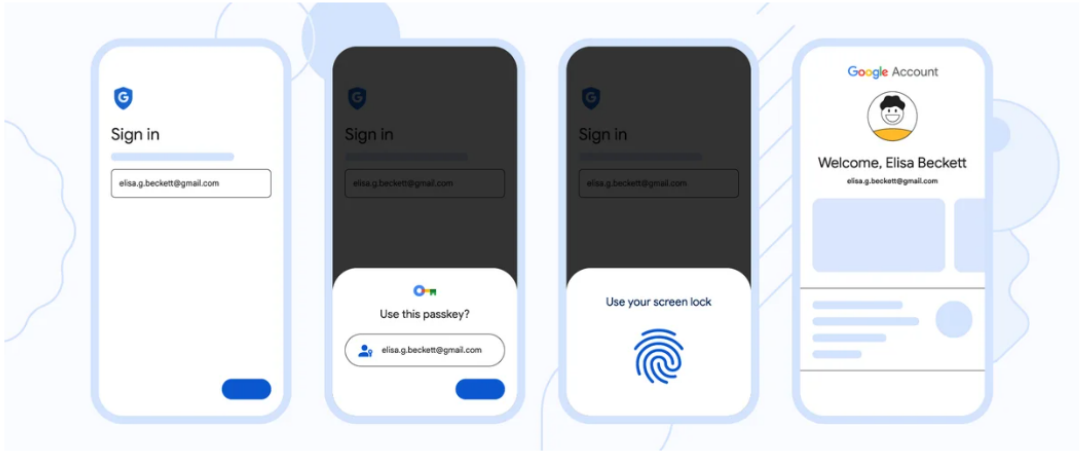
El principio del fin de la contraseña ?

Todo final, es un nuevo comienzo ...

May 03, 2023 · 2 mins de lectura

Sriram Karra
Senior Product Manager

Compartir



Día Mundial de la Contraseña

En este **Día Mundial de la Contraseña** hemos dado un gran paso en nuestro viaje hacia un futuro sin contraseñas. Comenzamos a implementar la compatibilidad con las claves de acceso (*passkeys*) en las cuentas de Google en todas las plataformas principales. Esto significa que los usuarios ahora pueden aprovechar las claves de acceso *(passkeys)* en los servicios de Google para una experiencia de inicio de sesión sin contraseña.

Las claves de acceso *(passkeys)* son una nueva forma de iniciar sesión en aplicaciones y sitios web. Estas son más fáciles de usar y más seguras que las contraseñas, por lo que los usuarios ya no necesitan confiar en los nombres de las mascotas, los cumpleaños o contraseñas simples, y poco seguras, como *"contraseña123"*.

soluciones

Checklist

- [ ] Backup seguro, revisado por humanos y a salvo (*varios sitios 1 sin acceso desde origen*)
- [ ] Router propio, Upnp off, todo cerrado salvo ip fijas. Wifi no integrado en router del operador
- [ ] Gestor de passwords, no reusarlos, no guardarlas en navegadores, comprobador filtraciones darkweb
- [ ] Solución antivirus, de pago, con firewall integrado por equipo, control de aplicaciones todavía mejor
- [ ] No tener ordenadores encendidos 24 horas sin atención si no es necesario
- [ ] Prohibir y sancionar el uso de cualquier tipo de software ilegal (*penal administradores*)
- [ ] Cuidado con accesos desatendidos anydesk, teamviewer, RDP. VPN si segura mejor
- [ ] Red con segmentación por servicios, no todo junto con acceso a todo, ojo cámaras/alarma
- [ ] Softwares y sistemas al día de Updates de cada fabricante. Especialmente servidores, equipos, NAS
- [ ] No EOL (End Of Life), Win7, < Win2016
- [ ] Formación y concienciación empleados
- [ ] Mantenimientos periódicos proactivos, revisión LOPD y obligaciones
- [ ] Limitar permisos de usuarios tanto en los equipos locales como en accesos a cosas
- [ ] Personal de IT con procesos rigurosos y buenas prácticas
- [ ] Probar el Disaster Recovery
- [ ] No usar Wifi abiertas o con contraseña de hoteles, aeropuertos etc… El 5G es tu amigo
- [ ] No guardar las passwords y el MFA en el mismo sitio
- [ ] Un Next Generation Firewall NO lo soluciona todo, pero ayuda (*si alguien lo revisa*)
- [ ] Cifra los datos críticos de usuarios (*online, b.d.'s…*)
- [ ] Portátiles y dispositivos susceptibles de robo con información encriptados discos duros

Extras. Bonus final if < ⏱️

Análisis según el ayurveda de los perfiles de empleados IT y sus combinaciones

Extras. Bonus final if < ⏱️

Teletrabajo

Hogar ¿inteligente?

Déficit atención

Alteración estado de conciencia

$$

Criptomonedas, neobancos, tarjetas bancarias

y ahora ...

Esta presentación será destruida por una IA haciéndola arder a 451 grados Fahrenheit