

POLICIA 
NACIONAL

sealpath™



Ransomware al acecho: *Toc Toc, ¡Tengo tus datos!*

IV EDICIÓN CONGRESO SEGURIDAD
DIGITAL Y CIBERINTELIGENCIA

Y si un día...

SU RED HA SIDO COMPROMETIDA.

Este enlace y su clave expirarán en 14 días tras la infección de sus sistemas.

Compartir este enlace o email le llevará a la irreversible destrucción de sus claves de descifrado.

NO SE DA MAS TIEMPO a precio especial.

Todos los archivos en cada host de la red han sido encriptados con un fuerte algoritmo.

No existe ningún software de descifrado disponible en otras fuentes.

No renombre los archivos infectados o de información de texto. No mueva los archivos infectados ni de información de texto.

Esto podría llevarle a la imposibilidad de recuperar ciertos archivos.

También hemos recopilado toda su información sensible.

Así que, si decide no pagar la haremos pública.

Podría dañar la reputación de su negocio.

Sus ficheros fueron codificados.
Para obtener el programa de decodificación debe pagar **500 USD/EUR**. Si no va a pagar hasta **11/11/14 - 11:34** el precio de decodificación aumentará **2 veces** y va a ser **1000 USD/EUR**.

Antes de incrementar la cantidad que queda:
167h 21m 19s

Su sistema: **Windows XP (x32)** Primera conexión con IP: [REDACTED] Codificados en total 2680 files.

UNTIL FILES
34D01H49M22S
PUBLICATION

Deadline: 06 Aug, 2023 09:16:35 UTC

tsmc.com
In the case of payment refusal, also will be published points of entry into the network and passwords and logins company
ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 29 JUN, 2023 21:16 UTC UPDATED: 29 JUN, 2023 21:16 UTC



La amenaza no para de crecer

 **8°**
+ atacado
del mundo

*Threat Landscape Report de S21sec

1.133 
x semana en Iberia

*Security Report Iberia 2024 de Check Point

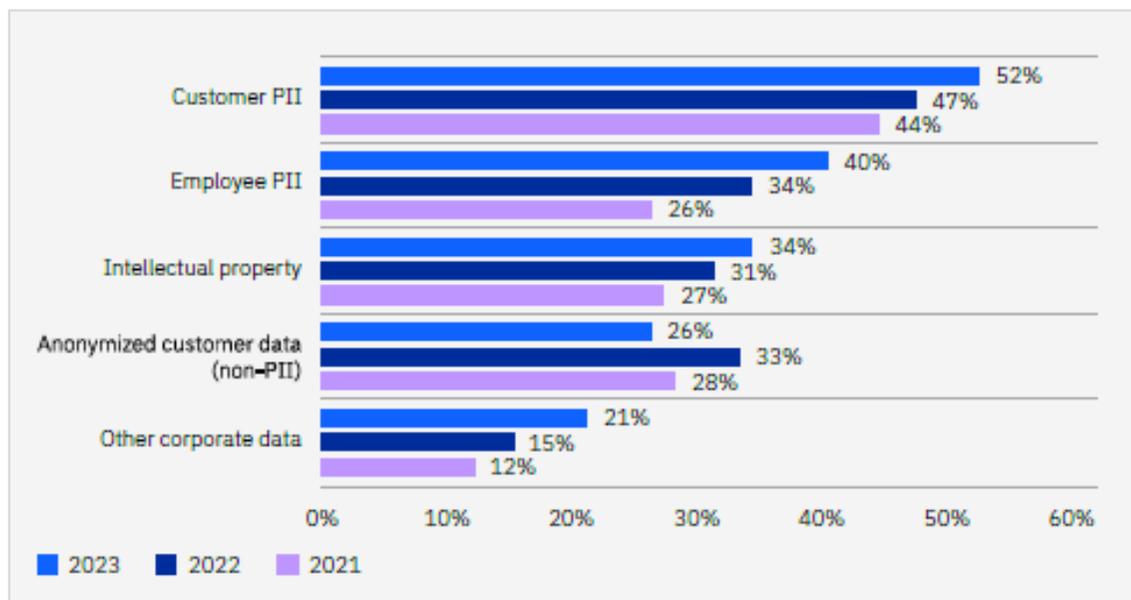
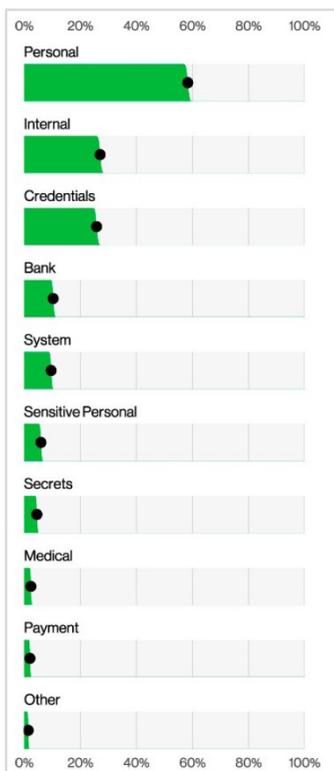
20% de 
empresas
en España

*Informe de Ciberpreparación 2023 de Hiscox

sealpath™



Tipos de Datos



Top Información extraída

Datos personales de clientes

Siguiéndole datos personales de empleados, y propiedad intelectual.

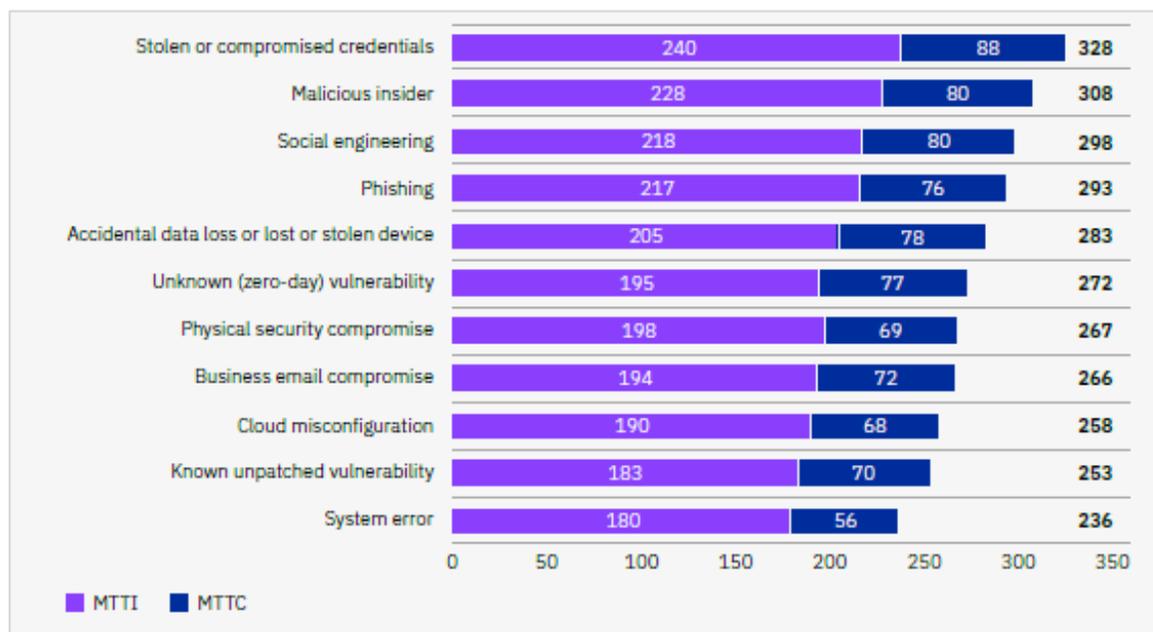


Reaccionamos tarde

Tiempo para contener la fuga

Desde los 180 días a los 240 para identificar una fuga.

Y desde 56 días hasta 88 para contenerla.



sealpath™

*IBM Cost of a data breach report 2023

* Verizon Data Breach Investigations Report 2024



El coste e impacto

1. Costes de detección y escalado

- Actividades forenses y de investigación
- Auditoría, gestión de crisis, comunicación ejecutivos.



2. Costes de notificación

- emails, cartas, etc. a afectados.
- Comunicación con reguladores, involucración expertos.



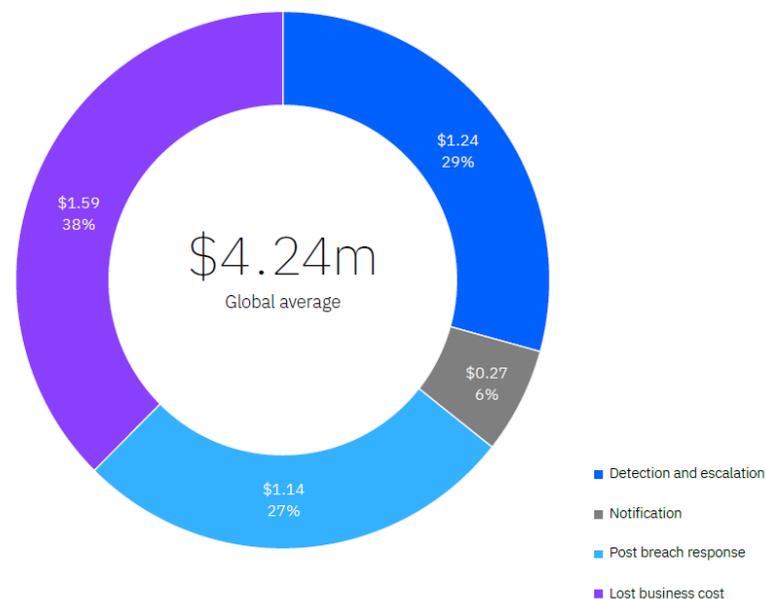
3. Costes de respuesta tras la fuga

- Soporte a afectados y comunicación.
- Expedientes legales, descuentos. Multas.



4. Costes por pérdida de negocio

- Pérdidas por interrupción del negocio, caídas, etc.
- Pérdida de clientes y reputación.



*IBM Cost of a data breach report 2023
* Verizon Data Breach Investigations Report 2024



Evolución del Ransomware Moderno



2013 Cryptolocker

Cifrado de archivos a baja escala, a individuos.



2018 Wannacry

Dirigidos, caza mayor de organizaciones, restaurar operativa.



2019 Maze

La doble extorsión, filtración pública.

sealpath™



Ransomware en la Actualidad

RansomOps

*Diversos actores,
entramado más
complejo.*

IAB

Initial Access Brokers

RaaS

*Ransomware-as-a-
Service*

Presas más valiosas
Botines más grandes

sealpath™



Su infraestructura en la dark web

LOCKBIT 3.0 LEAKED DATA Home FAQ How to Buy Bitcoin? Deal Or Not? Join US Contact Us

www.tcbank.by UNTIL FILES 08:00:35:17 DAYS HRS MINS SECS "If no deal, time until data publish" PUBLICATION Trade Capital Bank (TC Bank) was established on 12.09.2008. Registration number 80700015. The authorized fund of the bank is 61 650 487 (Sixty one million...)	[NEGOTIATED] Work ID : 78B9AF0EBC DEALED DATA DELETED DATA NOT AVAILABLE [Negotiated Data not available.] WORK INFO Work ID :78B9AF0EBCAccess Type :Full AccessSystem Info :1800 GB Data StolenCountry :[Negotiated Data not available.]Potential...	chs.ca Work ID : 5A9FEA61EB PUBLISHED Greedy Company they dont care about their customers and employees data , the Canadian Hearing Society (CHS) provides services that enhance the independence of... PUBLISHED Building communities for more than 75 years Groupe Montclair not only builds high-quality residences, but also seeks to reduce the ecological footprint of each one...	groupemontclair.com Work ID : 00FE1F9218 PUBLISHED
[NEGOTIATED] Work ID : 17CFEE61C3 DEALED DATA DELETED DATA NOT AVAILABLE [Negotiated Data not available.] WORK INFO Work ID :17CFEE61C3Access Type :Full AccessSystem Info :9 GB Data StolenCountry :[Negotiated Data not available.]Potential...	[NEGOTIATED] Work ID : 8F201F79F5 DEALED DATA DELETED DATA NOT AVAILABLE [Negotiated Data not available.] WORK INFO Work ID :8F201F79F5Access Type :Full AccessSystem Info :245 GB Data StolenCountry :[Negotiated Data not available.]Potential...	onyx-fire.com Work ID : 76910375B7 PUBLISHED Onyx-Fire Protection Services Inc is a company that operates in the Security and Investigations industry 800 GB Financial documents (balance sheets, budget, PL reports,...	[NEGOTIATED] Work ID : 145B826D2D DEALED DATA DELETED DATA NOT AVAILABLE [Negotiated Data not available.] WORK INFO Work ID :145B826D2DAccess Type :Full AccessSystem Info :3.5 GB Data StolenCountry :[Negotiated Data not available.]Potential...

Darkside Main Press Releases TOR Mirror

Let's start Pinned 08.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere. We received millions of dollars profit by partnering with other well-known cryptolockers. We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (hospitals, hospices).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business. Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your netirn. You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others

dread frontpage all dread

AlphaBay Market

/d/AlphaBay

Rules Easy Install & Run I2P PGP Keys Links About Us / FAQ

AlphaBay is Back
by [JulDeSnake](#) [Administrator](#) 13 weeks ago in [d/AlphaBay](#)

Welcome back to AlphaBay

We are proud to be back in business. To learn how we have improved, what has changed and what is our vision for the future head over to our FAQ section. If you have read our we are back message ([we are back message](#), [reacted](#) on official links or [commented](#) on this subreddit: [We Are Back Message](#)) then you know we are working on a decentralized marketplace project. We ask you to join and help out, or by using our marketplace you automatically help fund the project.

Remember to always check [/mirrors.txt](#) to make sure you are not on a phishing link. All Market-related PGP information is available on [/pgp_information](#)

Happy Trading!

EDIT: It was brought to my attention that for some reason the old ghostbin link did not work properly when inserted to PGP software to verify

108 comments Hide

Comments

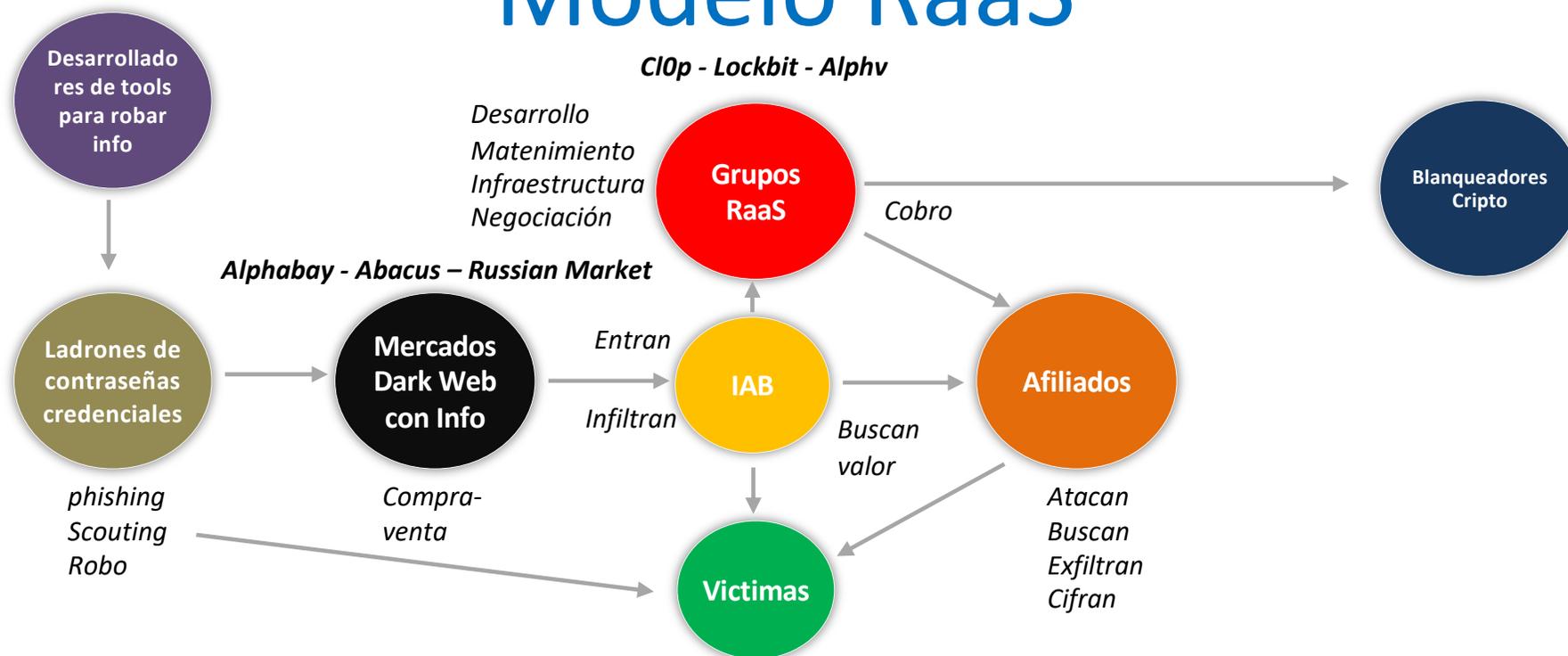
Sort comments by Top

- [JulParis](#) 1 point 3 weeks ago
To reduce any-kind of FUD that comes from this announcement. This user did verify his identity and provide proof that he was the tech staff at the original AlphaBay. It's legitimate. I'm not saying he isn't compromised, but if what he offers is true, at least some people will want to know about it.
- [Auldiss0](#) 3 points 3 weeks ago
Paris I recently spoke with DeSnake and he asked me to confirm that it is him. Using PGP keys and more importantly with things that only he knew as a staff member of AlphaBay and I can say this account / market is owned by the former AlphaBay security admin.
Everyone who knows me, knows that I believe the community needs a better market, a market the way AlphaBay and Dream and Hansa were. I wont lie I am

sealpath™



Modelo RaaS



sealpath™



¿Cómo seleccionan organizaciones?

Ingresos



Organizaciones con capacidad para hacer frente a un pago alto por extorsión.

Sectores



Priorizan los menos maduros en ciberseguridad-

Acceso

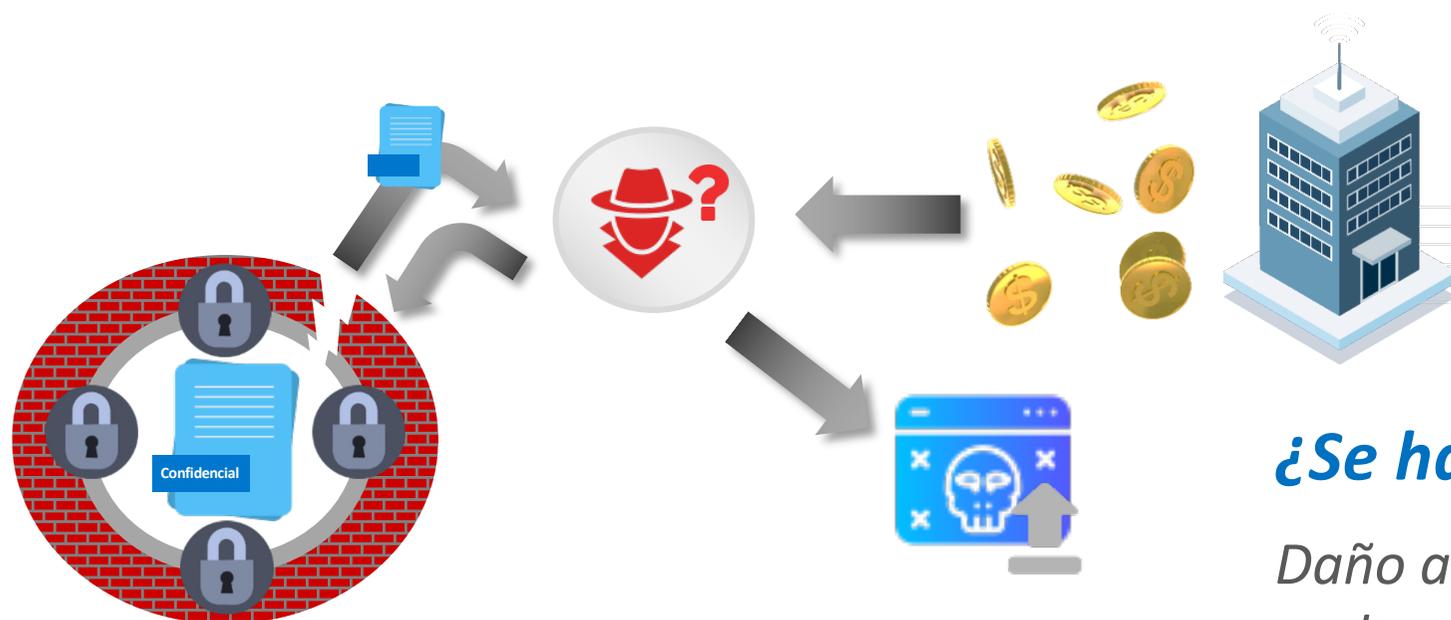


Compran cualquier tipo de acceso que les provean, comenzando por RDP y VPN.

sealpath™



La doble Extorsión

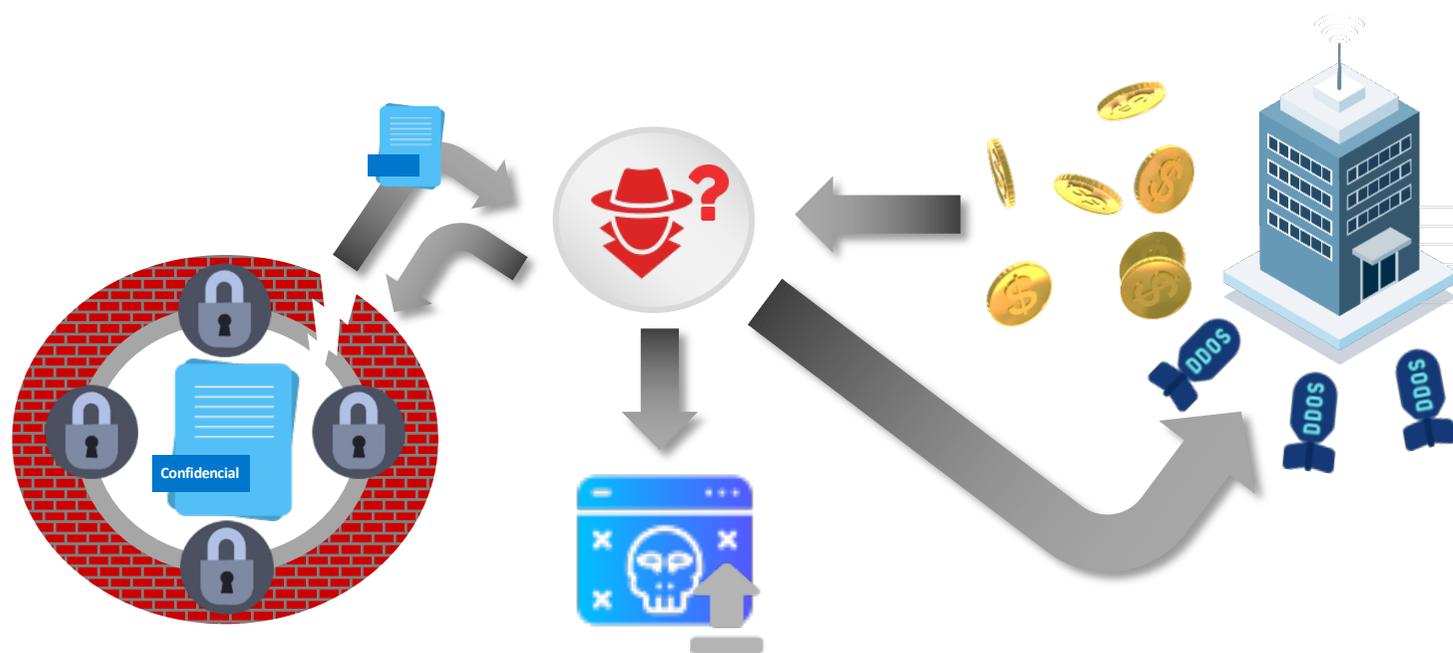


¿Se hace público?

*Daño a la reputación,
multas, pérdidas
económicas...*

sealpath™

Incluso triple Extorsión



¿Te hago más daño?

- Ataques DDoS
- Ataques a terceros: Clientes, socios, proveedores...

sealpath™

Y cuádruple



¿Te añado presión social?

Contactan con terceros asociados notificando que se niegan a pagar y los daños van a ser catastróficos para todos.

sealpath™

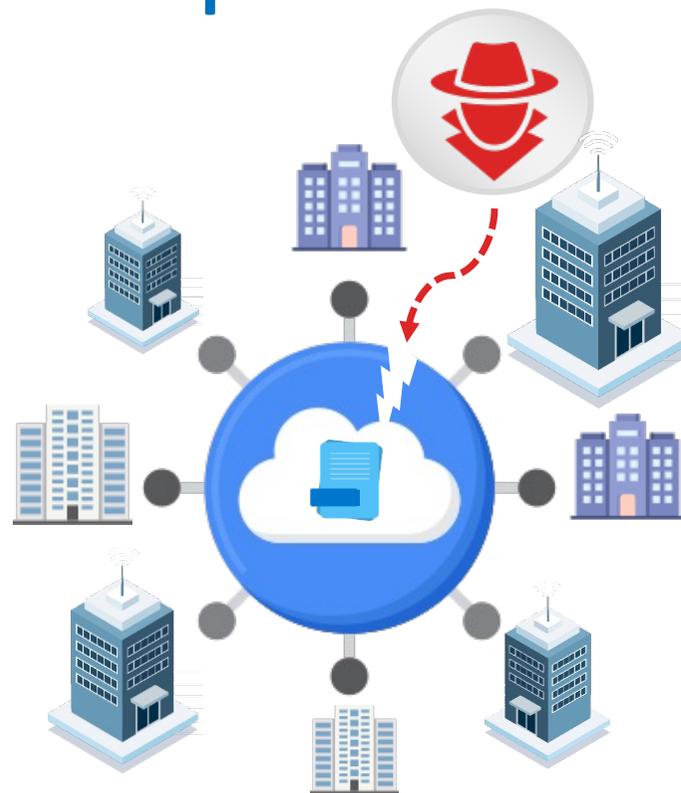


Los Mega-ataques

Dirigidos a
Proveedores de
servicios Cloud

Aprovechan
Vulnerabilidades
Zero-day

1 ataque,
cientos de
empresas
afectadas



Anatomía de un ataque

1. Acceso Inicial

Phishing y vulnerabilidades. Algunas conocidas otras compran en la dark web, ZeroDay.

2. Escalado de Privilegios

AD, Políticas de Grupo

3. Infiltración

Creación de cuentas, credenciales

*Cobalt Strike

*Mimikatz

4. Movimiento Lateral

phishing más interno

*IPScanner, Splashtop, Anydesk

*Rclone, Mega Upload

6. Recopilan los datos, extraen y despliegan

Crean paquetes de datos y los mandan fuera para luego cifrar.

5. Evaden las Defensas

Limpian los logs, desactivan EDRs y herramientas.



Medidas para protegerse



Cifrado

Evitas la extorsión por filtración.



Formación

Usuarios concienciados contra el phishing.



Backups

Completos y aislados para restaurar datos.



Patching

Tapar agujeros de acceso.



Controlar Accesos

Principio del Mínimo privilegio.



Monitorizar

Supervisión constante.



Detectar

Ser proactivos.



Plan IR

Establecer procedimientos.



Medidas para protegerse



Segmentación

Aislando contra la propagación.



End-points

Protección antimalware.



MFA

Una barrera más a la entrada.



Whitelisting

Para prevenir ejecución de apps no conocidas



Antiphishing

Controles y herramientas.



Políticas

Políticas de Control y uso.



Email Security

Proteger emails y adjuntos.

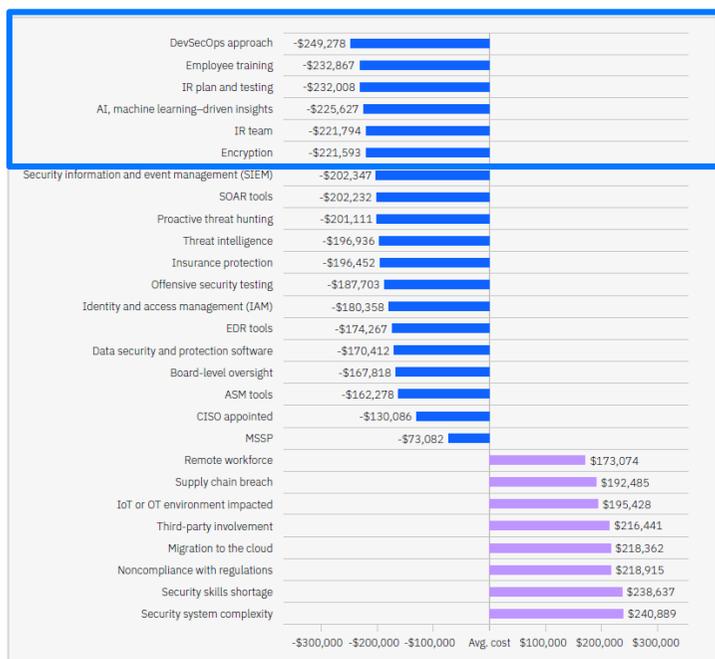


Contraseñas

Fuertes y gestión segura.



¿Cómo mitigar el impacto?



Factores que mitigan el impacto

Formación de empleados, plan de respuesta a incidentes, uso de IA para detección, y uso del cifrado..



Plan IR



Formación



Cifrado



DevSecOps



IA



Equipo IR



sealpath™



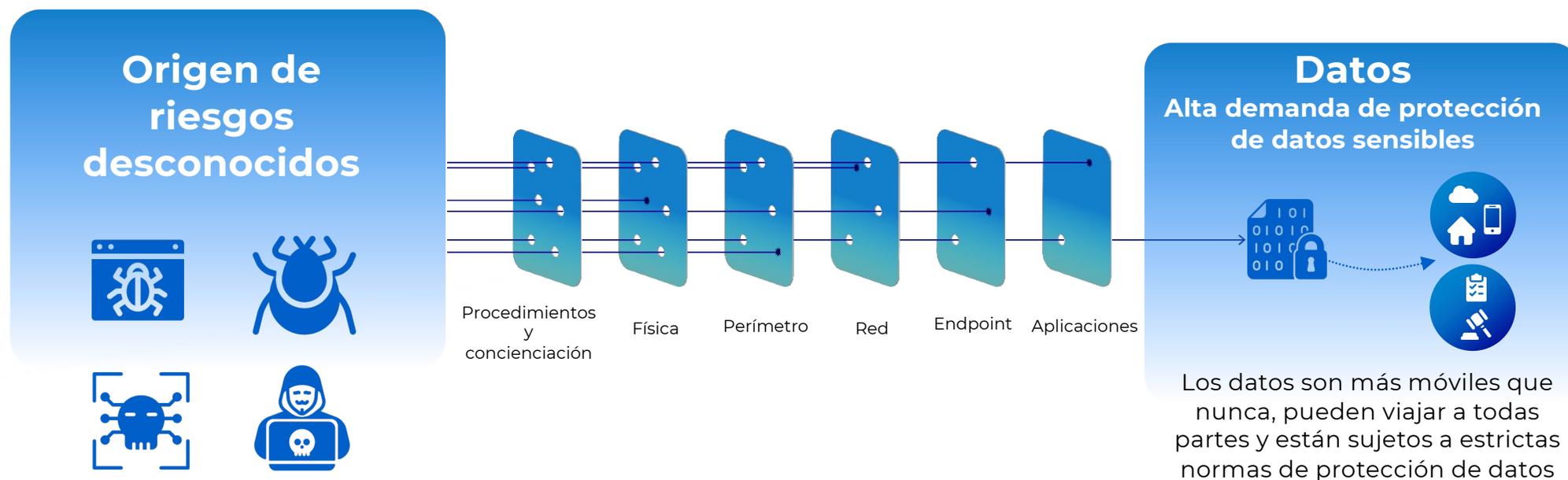
El dato es lo más valioso

Su protección debe ser un pilar desde el que extender nuestras defensas



sealpath™

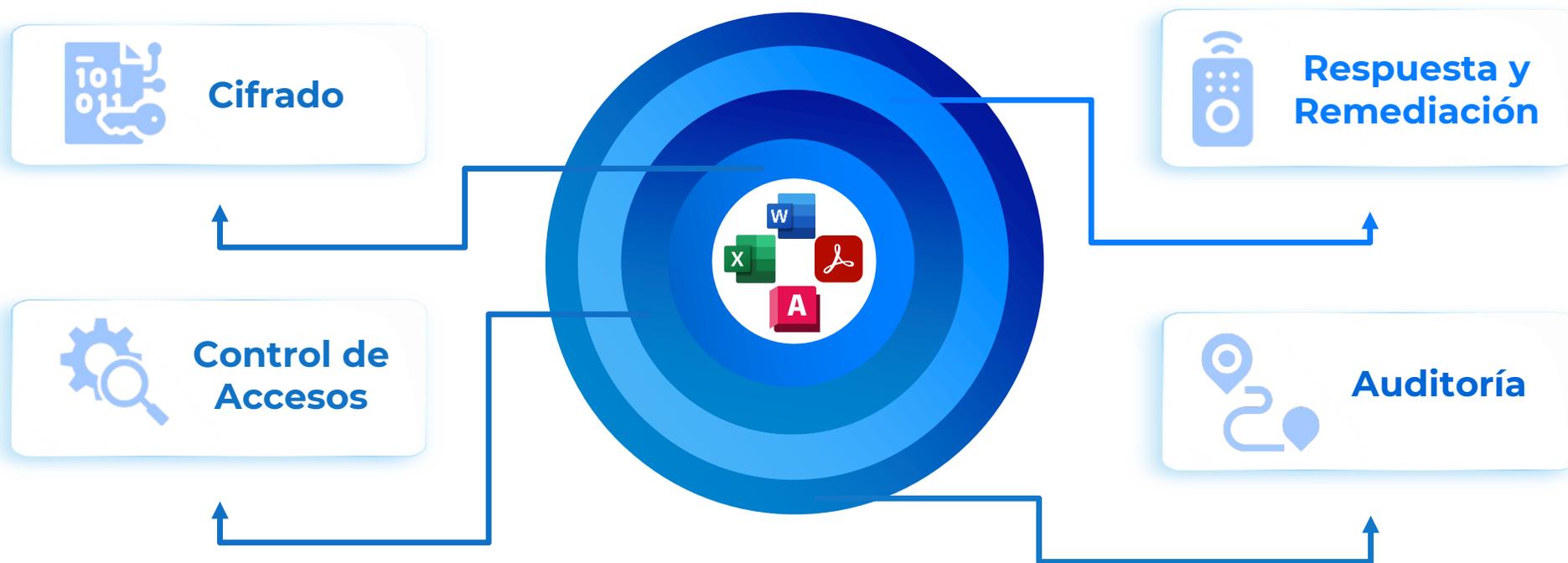
Cuando atraviesan cada capa...



Capas de seguridad de la red de una organización



¿Cómo blindar el dato con IRM?



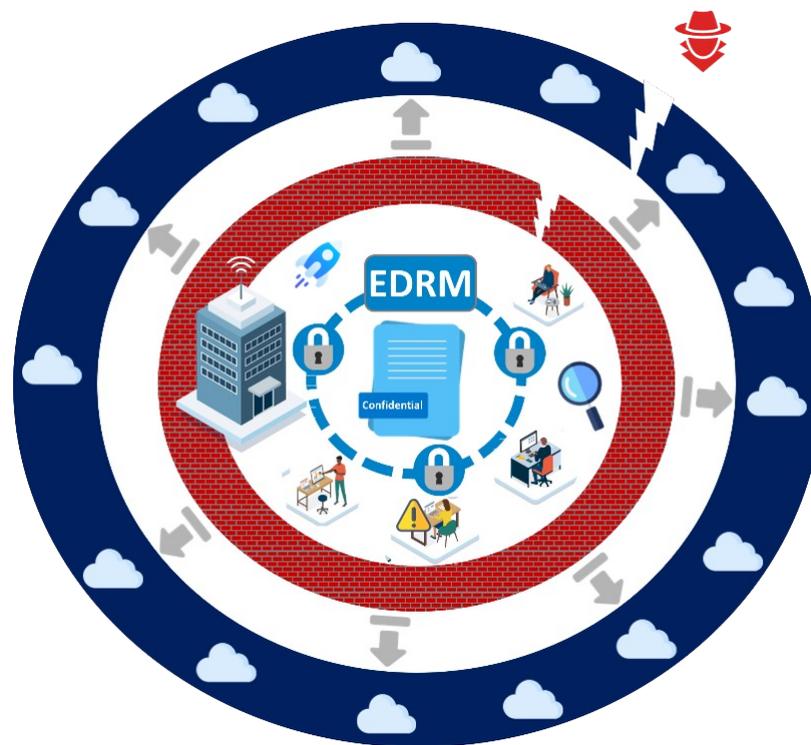
Protección centrada en el dato

Proteger dentro y fuera

No importa dónde viaje o se ubique el dato, la protección es persistente.

Identificar a los usuarios

Todas las personas accediendo a los datos deben identificarse.



Auditar los accesos

Debemos mantener el control en todo momento para decidir quién accede.

Responder y Revocar

Es necesario poder responder con rapidez y medidas correctoras para frenar el daño.

Protección del Dato VS Ransomware



Evita la Extorsión

Nadie puede acceder a la información aunque la publiquen.



Ayuda a detectar acciones sospechosas

La trazabilidad otorga visibilidad en tiempo real para respuesta temprana



Evita daños desde terceros

Ya sea un proveedor o un socio el que es atacado, tu información se mantiene a salvo.



Otorga capacidad de respuesta

Reaccionar ante eventos anómalos con rapidez minimiza el impacto.



Ejemplo real



Multinacional Europea Sector Metalúrgico
Ataque de Ransomware



1. Contacto

Contactan a la empresa para hacer saber que han cifrado información sensible y que paguen rescate por descifrarla.



2. Extorsión

Tenían backup y al decir que no pagan, amenazan con publicarla abiertamente.



3. Pruebas

Mandan una muestra para corroborar que tienen los datos en su poder y la criticidad de estos.



4. Validación

En la muestra de los datos que habían robado **vieron que estaba protegida y por tanto era inaccesible.**



“ Prevenir el acceso no autorizado a los datos es crucial
Que no haya pasado no significa que estés a salvo ”





+10 años ayudando a
proteger la información de
las organizaciones



**Mejor empresa de
Seguridad de Datos y
Producto de Europa
2023**



**La mejor
solución E-
DRM
2022**



**Finalistas
en 3
categorías
2022**



**Seguridad del Dato
Avanzada**
www.sealpath.com

Gartner

**Nombrados en 2 ciclos
hype y 1 investigación
de Octubre 2022**

kuppingercoie
ANALYSTS

**Uno de los líderes de la
colaboración segura
por su informe de
mercado**



POLICIA NACIONAL



sealpath™

