

Panorama actual de la **CIBERDELINCUENCIA** en las empresas

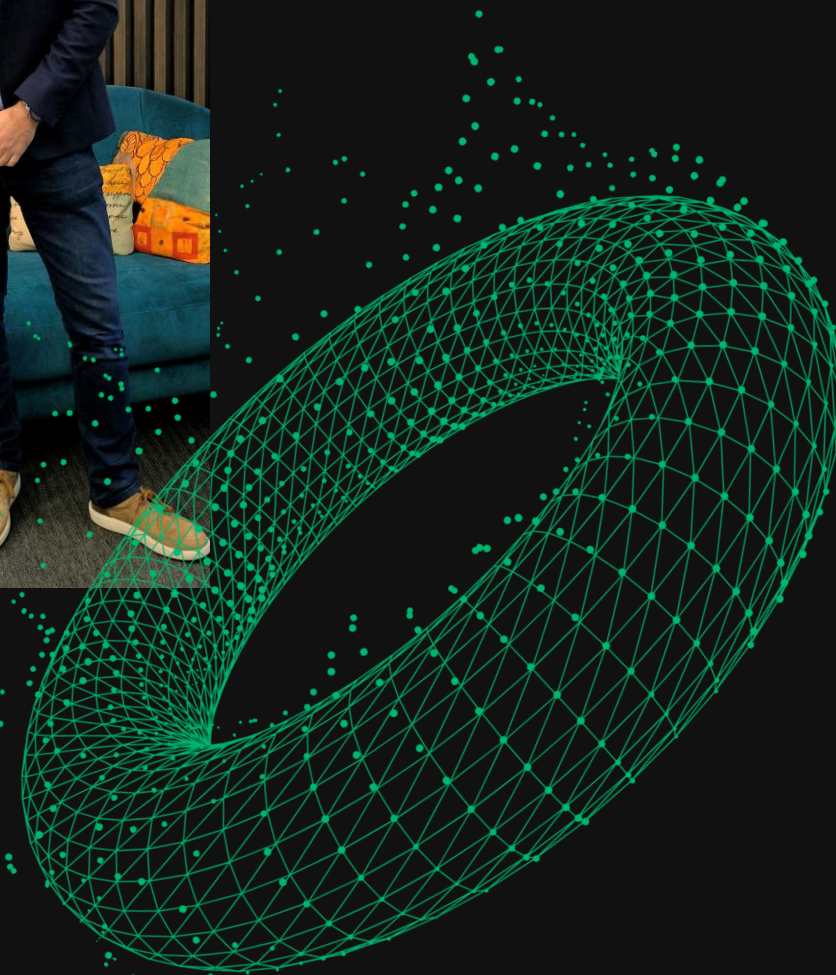
¿Cómo combatirla? **CIBERRESILIENCIA**



IÑAKI CALVO

KUIK IT MANAGER

inaki.calvo@kuik.tech





Estado actual de la ciberdelincuencia



BASADO EN INFORME DE SOPHOS SOBRE AMENAZAS 2024

Análisis de los datos de Sophos MDR, Sophos Incident Response y SophosLabs



Hace hincapié en los **CIBERATAQUES CONTRA LAS EMPRESAS INDUSTRIALES**



Se basa en los datos de más de **150.000 detecciones de malware y 500 casos de clientes**

TENDENCIAS CLAVE

Tendencias clave para las EMPRESAS INDUSTRIALES

1

PROTECCIÓN DE DATOS

El mayor reto para las empresas

2

BEC

Estafas en auge y más avanzadas que nunca

3

RANSOMWARE

La mayor amenaza en términos de repercusión

4

VULNERABILIDADES y controladores vulnerables

Un vector común de infección para las pymes

5

DISTRIBUCIÓN DE MALWARE a través de la web

Usada para eludir la protección contra malware



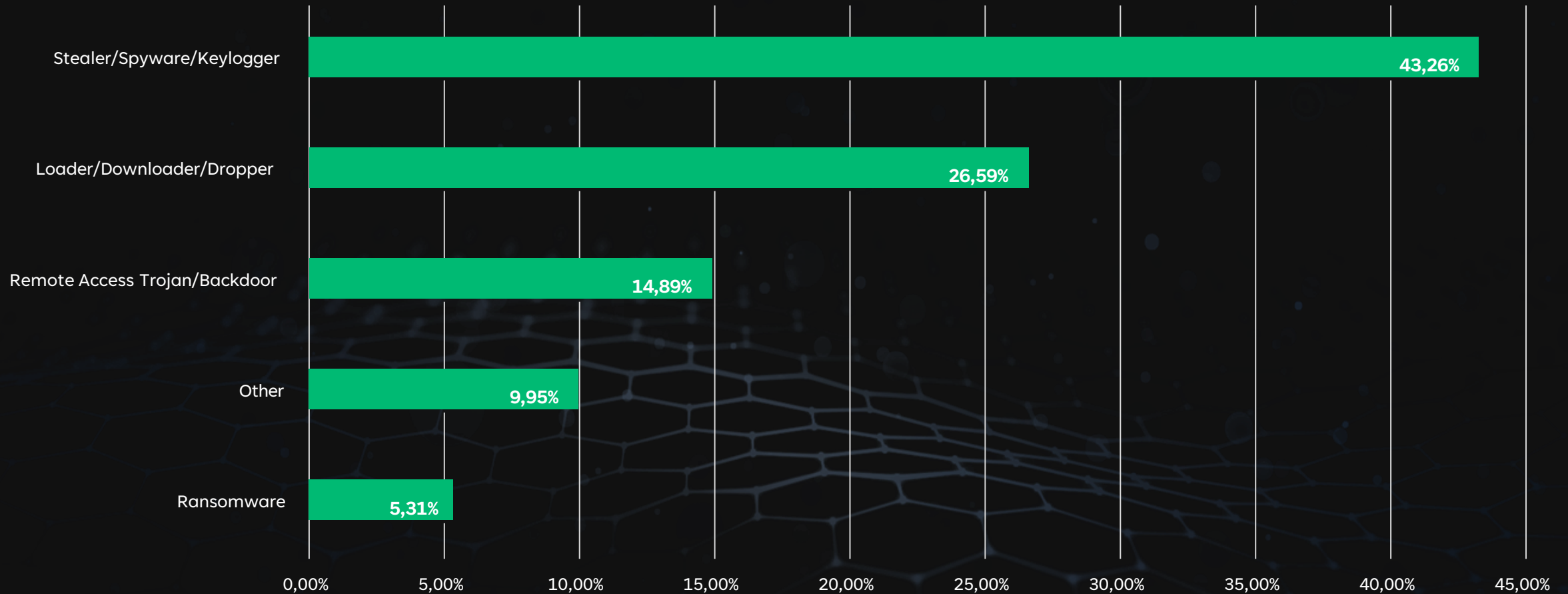
LA PROTECCIÓN DE DATOS
es el reto Nº 1 para las empresas





El robo de datos y credenciales fue la amenaza más importante para las empresas en 2023

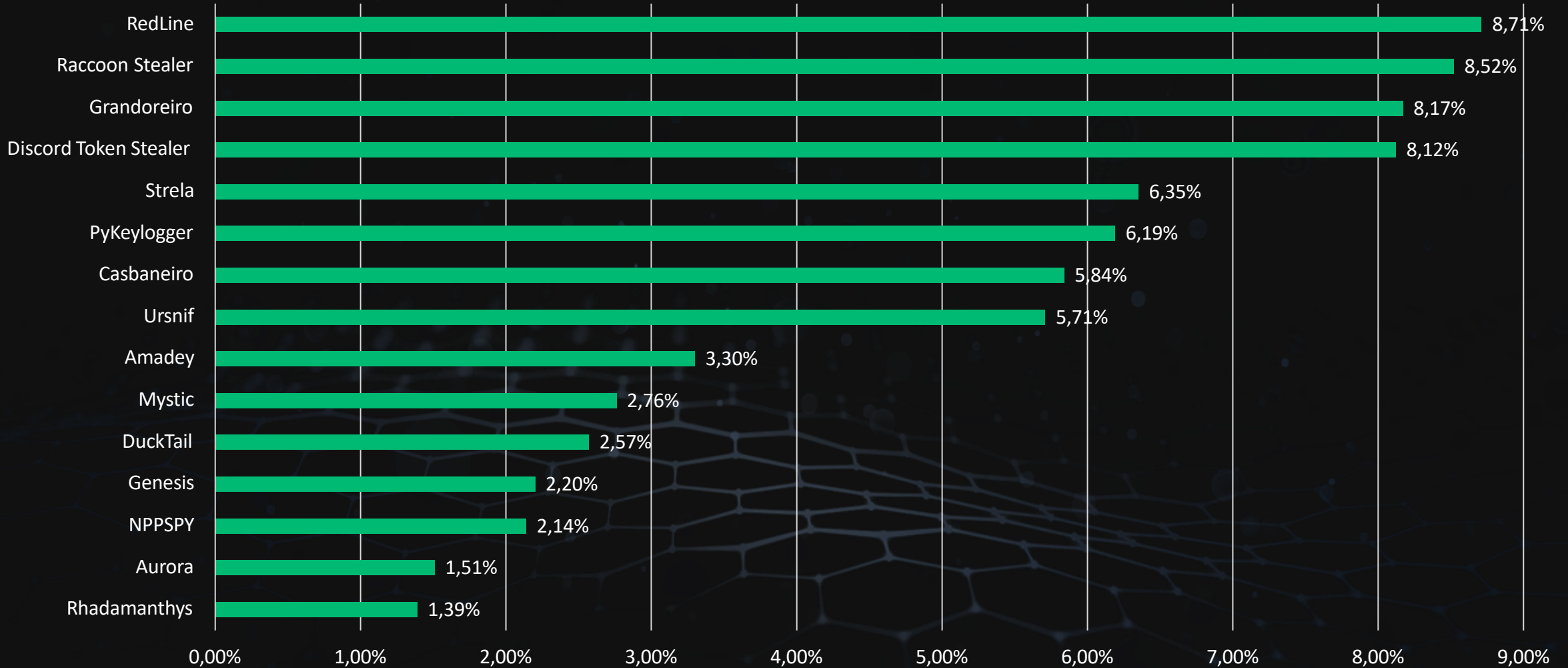
Categorías de malware por número de actualizaciones de firmas en 2023





Los ladrones de información más habituales

Principales ladrones de información por número de denuncias de clientes en 2023



Los brókeres de acceso inicial (IAB)


Profesión con futuro?

RDweb = Download ICON , Connect to Remote Desktop
Zoom/Rev = 5kk
Industry = Law Firm, ADVOCATEN
Country = BE, Belgium
Domain Computers = 36
Domain Controlers = 2
Level User Rights
Network = Local Network
Trust Domains = Only Primary
Windows 2016
AV = G Data Security + Windows Defender
Extra Info : 500 GB + On C:/ Driver
600 GB + Data on Local Share With Important data

Start 2000\$
step 200\$
Blitz 3000\$



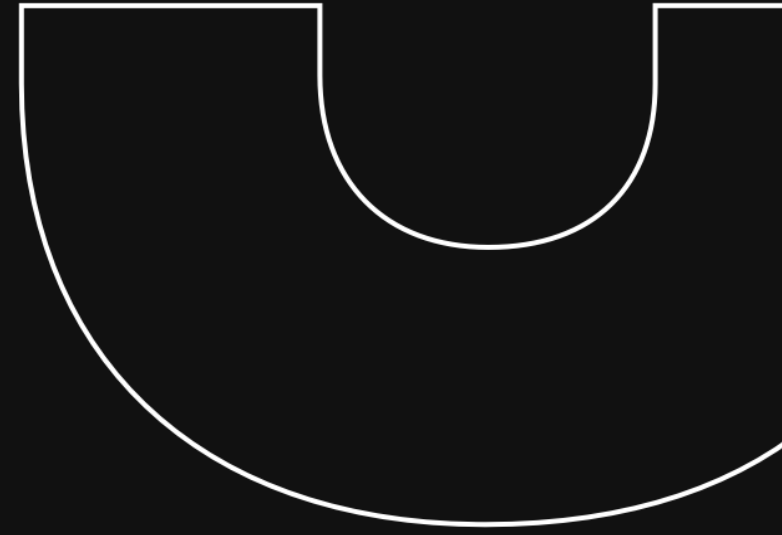
Country: Italy
Revenue: >\$60k
Access type: RDP
Low Priv
40 hosts
AV: Windows Defender
Price: \$190



Crece el valor de los datos como «moneda»

- Los atacantes utilizan los datos y las credenciales que **ROBAN DE MUCHAS MANERAS**
- Los atacantes se aprovechan de empresas que tienen **MENOS RECURSOS DE SEGURIDAD**
- **EXTORSIÓN Y CHANTAJE** para monetizar el secuestro de datos. Daño empresarial y/o reputacional en la empresas afectadas.

```
41
42
43 class Invite {
44     public message();
45 }
46
47 class Invite2 {
48     public message1();
49     public message2();
50 }
51
52 $obj1 = new Invite();
53 $obj1->message();
54
55 $obj2 = new Invite2();
56 $obj2->msg1();
57 $obj2->msg2();
58
59 $x = 12345678;
60 var_dump(is_int($x));
61
62 $s = "2017-12-31";
63 $v = strtotime($s);
64
65 $d1=strtotime("December 31, 2017");
66 $v1 = strtotime($s);
67 echo ($v1 == $d1) ? "Integer is valid" : "Integer is not valid";
68
69 if (!filter_var($int, FILTER_VALIDATE_INT)) {
70     echo("Integer is valid");
71 } else {
72     echo("Integer is not valid");
73 }
74
75
76
77 include 'f1.p';
78
79 ?>
80
81 </
82 </
```

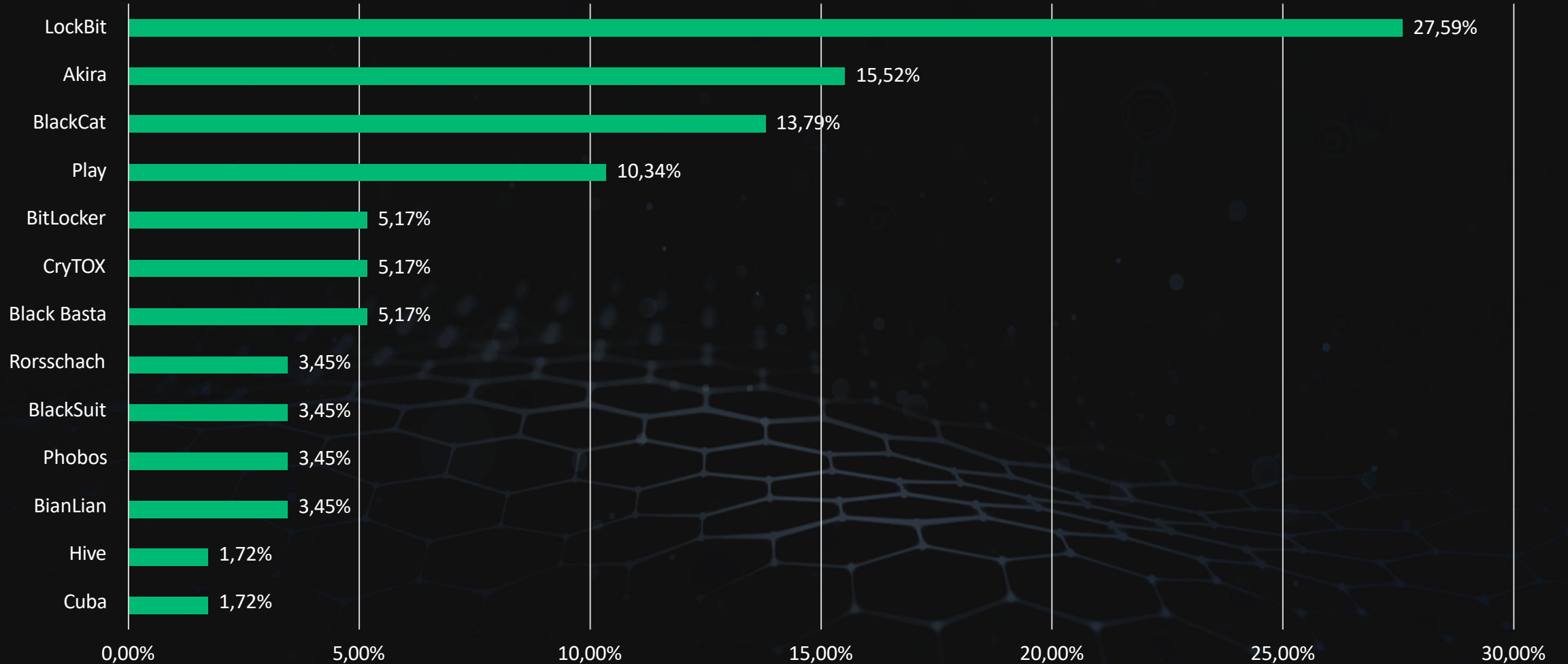


EL RANSOMWARE
sigue siendo la mayor amenaza
en términos de repercusión



Las empresas se enfrentan a una gran variedad de amenazas de ransomware

Desglose de los operadores de ransomware detrás de los incidentes investigados por Sophos Incident Response en 2023



THE SITE IS NOW UNDER CONTROL OF

This site is now under the control of The National Crime Agency with the FBI and the international law enforcement

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

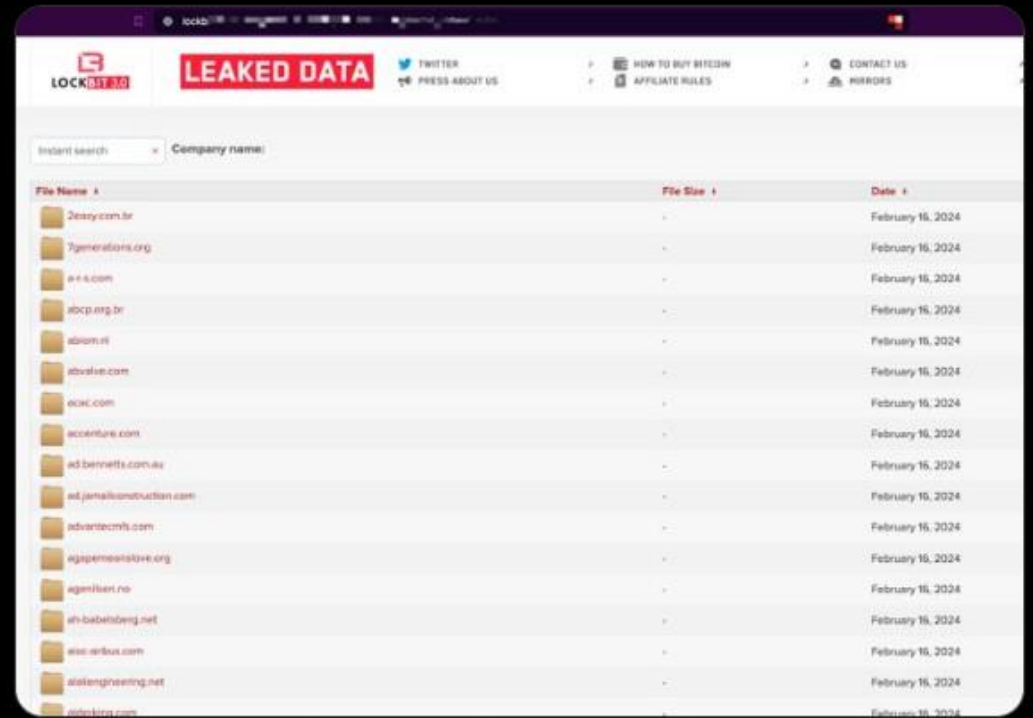
Return here for more information at:

11:30 GMT on Tuesday 20th Feb.



🌟 Hace unas horas, Agencias Gubernamentales contra el crimen de 11 países , anunciaron que tomaron el control de los servidores del grupo de ransomware [#Lockbit3](#)

Pero... los administradores de Lockbit3, ya tienen otro sitio funcionando correctamente con la información de 709 víctimas



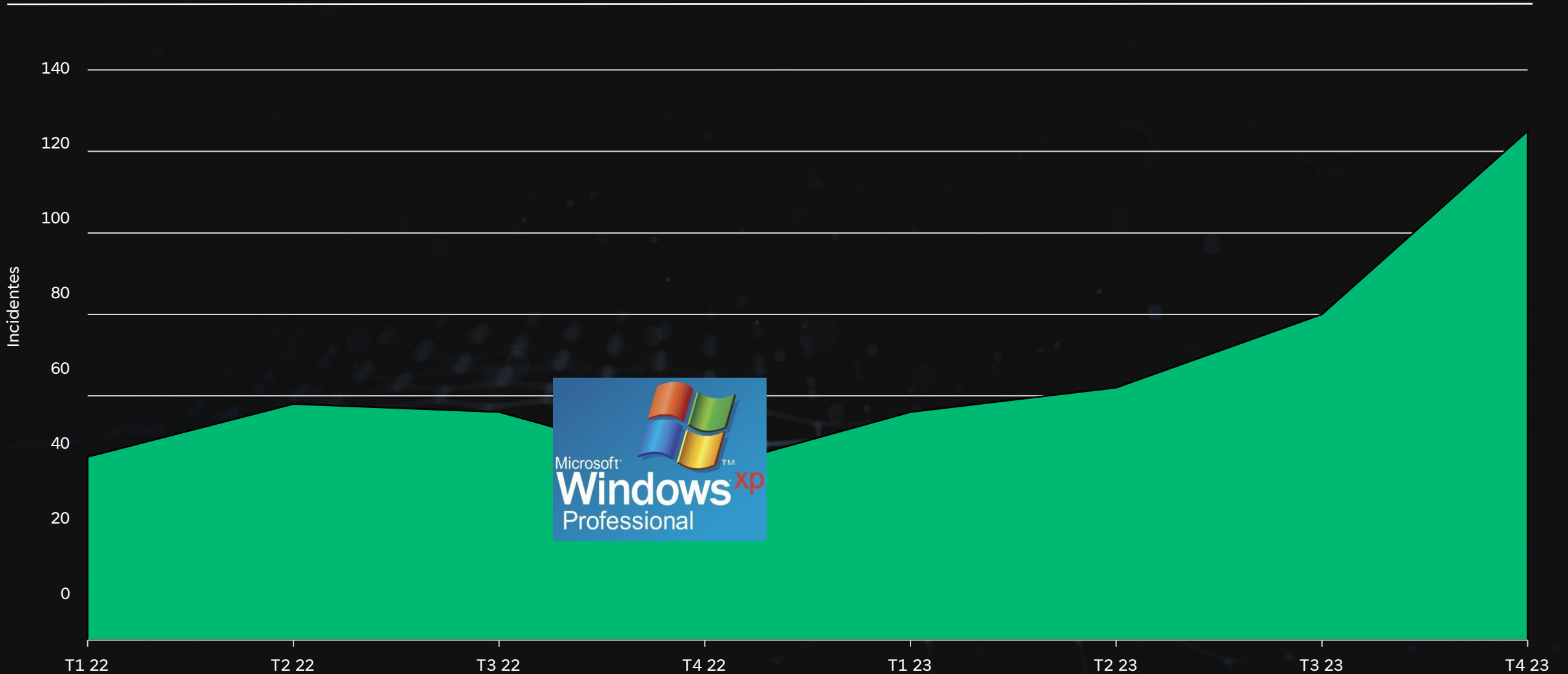
3:16 a. m. · 20 feb. 2024 · 27,2 mil Reproducciones





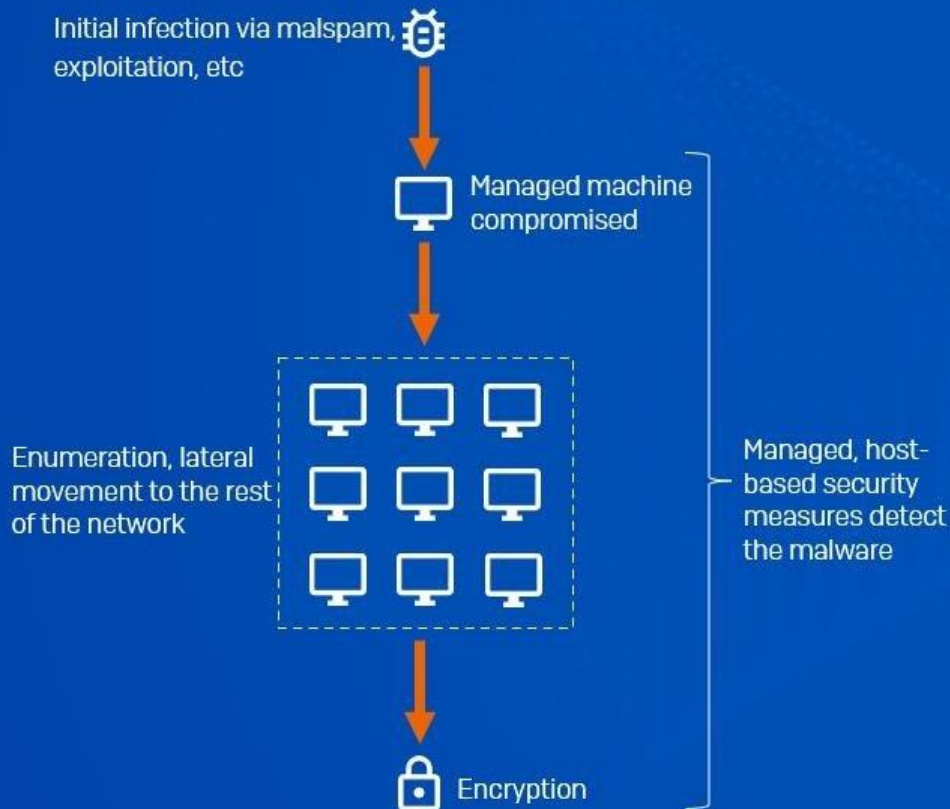
Los operadores de ransomware añaden nuevos trucos a su arsenal de estrategias

Incidentes de ransomware remoto, 2022-2023

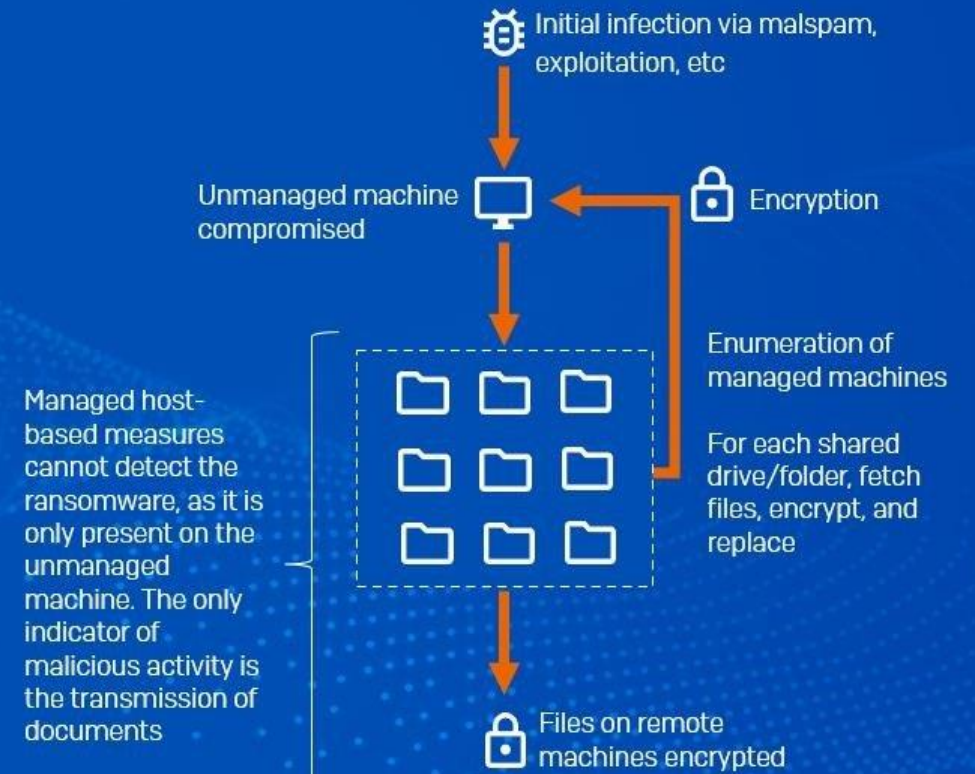


Why remote ransomware is a big problem

How local ransomware works



How remote ransomware works





AUMENTAN LAS ESTAFAS

por correo electrónico corporativo comprometido, así como las tácticas de ingeniería social más sofisticadas



Siguen creciendo las estafas por correo electrónico corporativo comprometido (BEC)

hotel info - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From caroline <caroline.deknuddt@telenet.be>

Subject hotel info

To undisclosed-recipients;

12/3/2023 3:43 PM

You don't often get email from caroline.deknuddt@telenet.be. [Learn why this is important](#)

Greetings,

I am writing to inquire about reserving a room at your esteemed hotel for my mother. She is planning to travel from the UK and is expected to arrive between the 7th and 10th of next month. Her stay will be for one night.

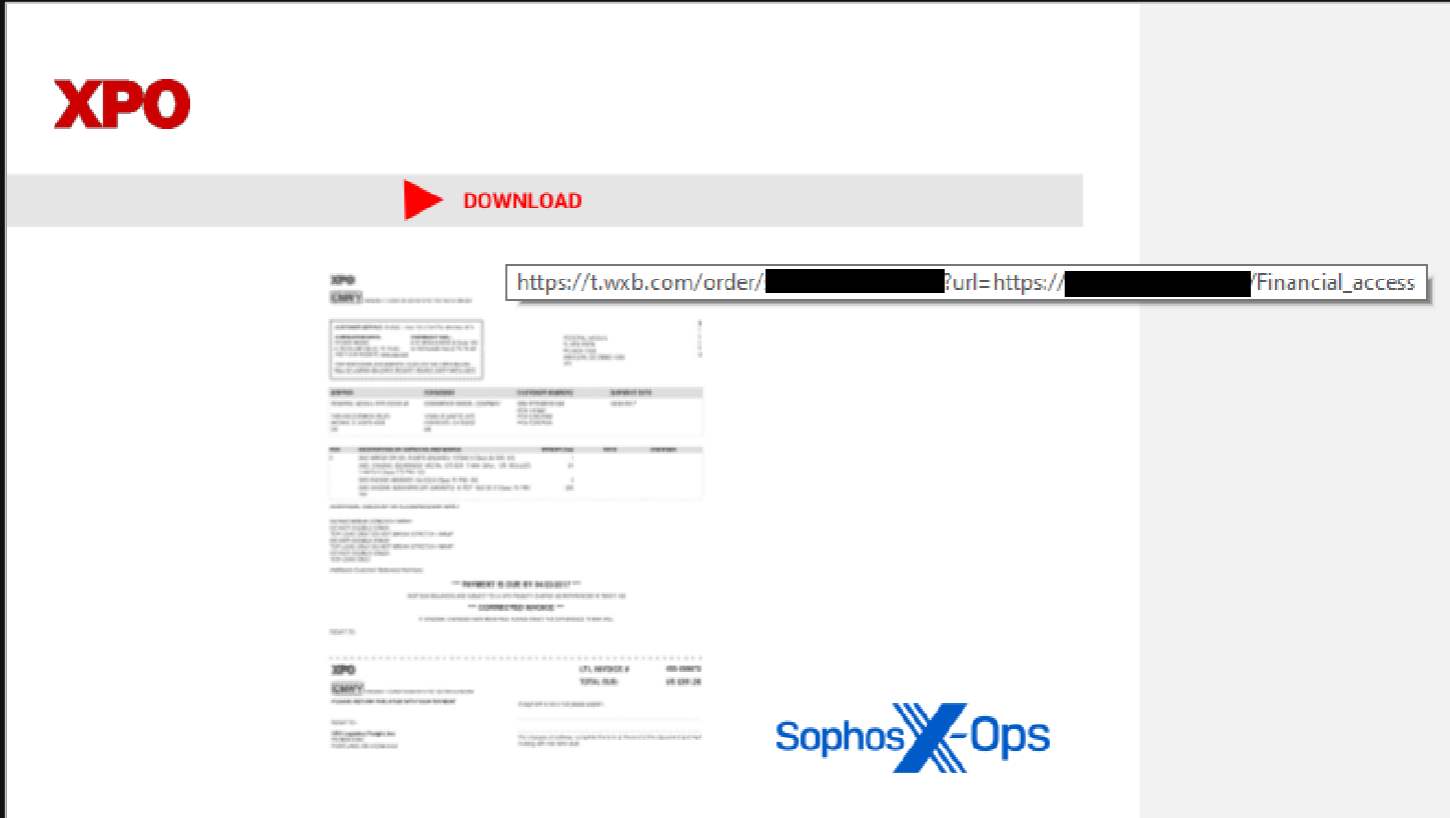
My mother name is Carolina Bernandez Blanca, born on May 12th, 1961. Her document number is DNI531273604T.

Considering her age of 62, I am concerned about her ability to navigate an unfamiliar location. Unfortunately, she does not possess a smartphone with navigation capabilities, as her familiarity with modern technology is limited.

I kindly request your assistance in providing clear directions to ensure her safe arrival at your hotel. I have marked the suggested route on a map, and I would greatly appreciate it if you could review and confirm it. To access the route, please click on the link provided for [Google Maps](#) (password: 123456).

I am eagerly awaiting your feedback regarding the proposed route. Your invaluable assistance in ensuring a secure journey for our senior guests is sincerely appreciated. Thank you.

Los delincuentes están dejando de usar adjuntos maliciosos



Incrustan enlaces a código malicioso en imágenes y archivos pdf.

En un caso, **incrustaron una imagen de código qr** que llevaba a una página de phishing.

En otro, **enviaron un documento pdf** con una **miniatura borrosa e ilegible** de una «factura». El botón de descarga contenía un **enlace a un sitio web malicioso**.

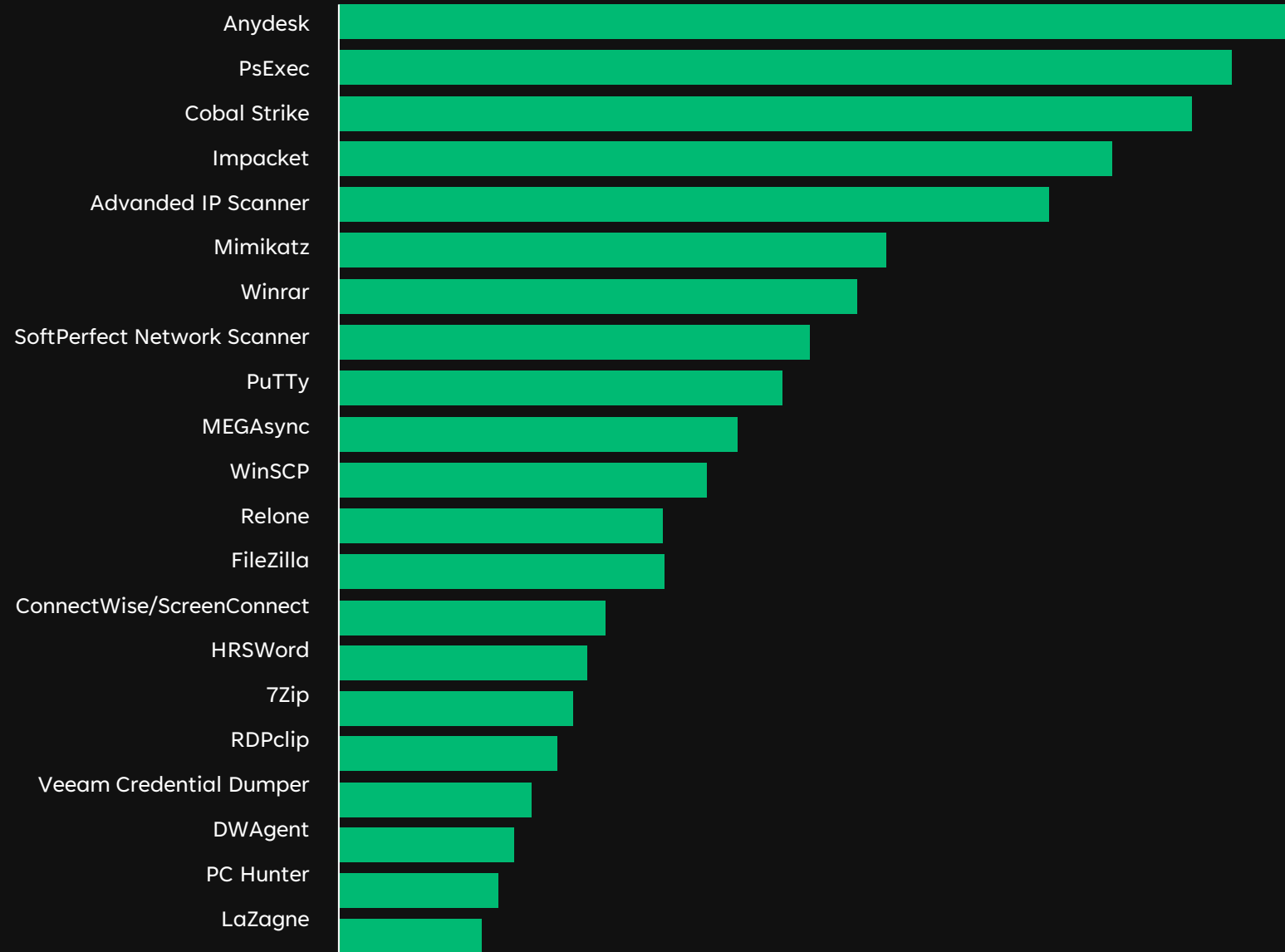


HERRAMIENTAS de "doble uso"





Principales herramientas de "doble uso" observadas en los incidentes gestionados por MDR





Los atacantes vuelven a distribuir **MALWARE A TRAVÉS DE LA WEB**

Aumentan la publicidad maliciosa y el envenenamiento de SEO



Into the tank with Nitrogen

The element originally known as "foul air" stinks up computers as a new initial-access campaign exhibiting some uncommon techniques

Written by Gabor Szappanos, Morgan Demboski, Benjamin Sollman

Los delincuentes se han visto obligados a **encontrar una vía diferente** para distribuir su malware después de que microsoft empezara a **bloquear automáticamente las macros**.



Los atacantes emplean **trucos de seo, sitios web falsos y anuncios falsos** para engañar a sus objetivos y hacer que **descarguen malware**.



Los atacantes se aprovechan de
**CONTROLADORES Y SOFTWARE
DE SERVIDOR VULNERABLES**
para burlar las defensas



Aumentan la publicidad maliciosa y el envenenamiento de SEO



Update 2: Increased exploitation of PaperCut drawing blood around the Internet

A recent remote code execution (RCE) vulnerability is increasingly in use to deliver Cobalt Strike and other remote management software, along with multiple ransomware threats – what you need to know about CVE-2023-27350 (and now CVE-2023-39143)

Vulnerabilidades como las de **PaperCut y MOVEit** coparon los titulares cuando fueron explotadas por bandas de ransomware.

Los delincuentes también van a por **firewalls y software de servidor web** antiguos y obsoletos.

Los exploits fueron un vector de infección habitual en 2023



The image shows a screenshot of a news article on the Sophos News website. The article is titled "Multiple vulnerabilities discovered in widely used security driver" and is dated January 25, 2024. The article is written by Andreas Klopsch. The article content is partially visible, starting with "A false-alarm incident involving Panda Security software leads to three very real CVEs". The article is categorized under Threat Research, CVE-2023-6330, CVE-2023-6331, CVE-2023-6332, Drivers, Featured, and Panda Software. The article is accompanied by a large image of bamboo stalks and leaves, with a Sophos X-ops logo overlaid on the top left of the image.

SOPHOS NEWS Products & Services Security Operations **Threat Research** AI Research Naked Security Sophos Life



Multiple vulnerabilities discovered in widely used security driver

A false-alarm incident involving Panda Security software leads to three very real CVEs

Written by Andreas Klopsch

JANUARY 25, 2024

THREAT RESEARCH CVE-2023-6330 CVE-2023-6331 CVE-2023-6332 DRIVERS FEATURED PANDA SOFTWARE

Los atacantes se ensañan cada vez más con los controladores



Microsoft Revokes Malicious Drivers in Patch Tuesday Culling

Written by Andrew Brandt

JULY 11, 2023

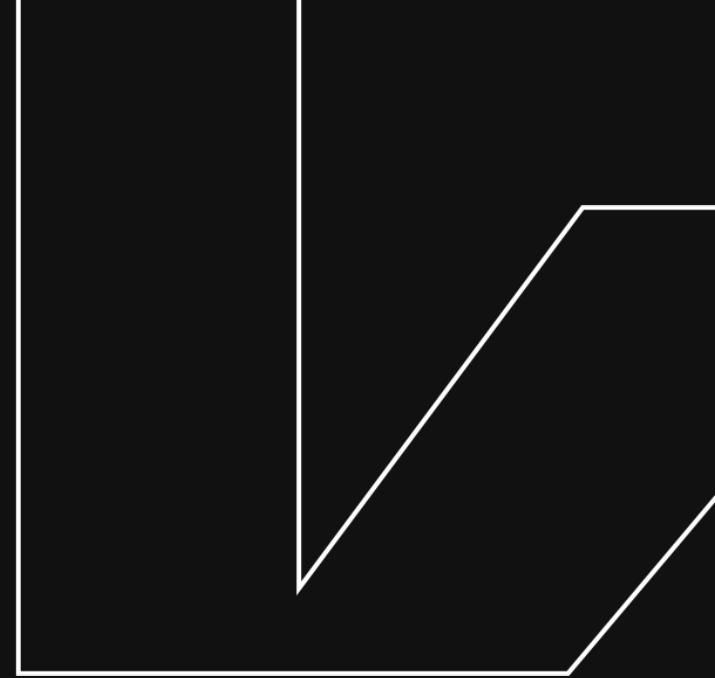
En 2023, Sophos X-Ops registró varios casos de delincuentes que **utilizaban controladores de kernel para desactivar la protección de endpoints.**

Algunos de estos controladores vulnerables son de software antiguo y todavía tienen **firmas digitales válidas.**

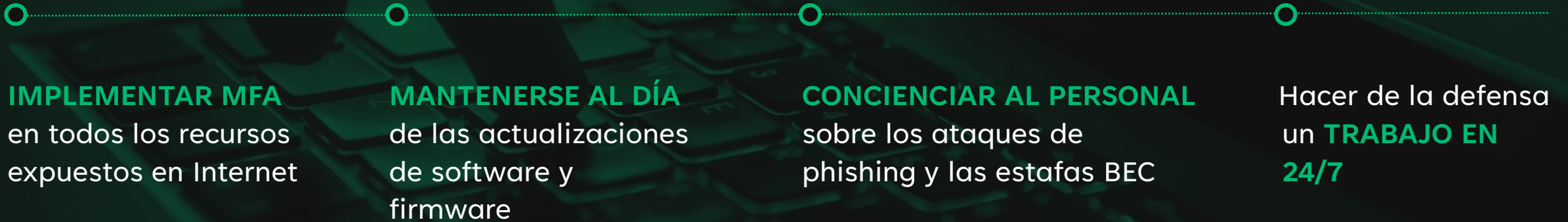
En otros casos, utilizaban controladores maliciosos **cuyas firmas digitales se obtenían de forma fraudulenta.**



¿Cómo pueden las empresas
MEJORAR SU SEGURIDAD?



Las claves de una estrategia de seguridad sólida





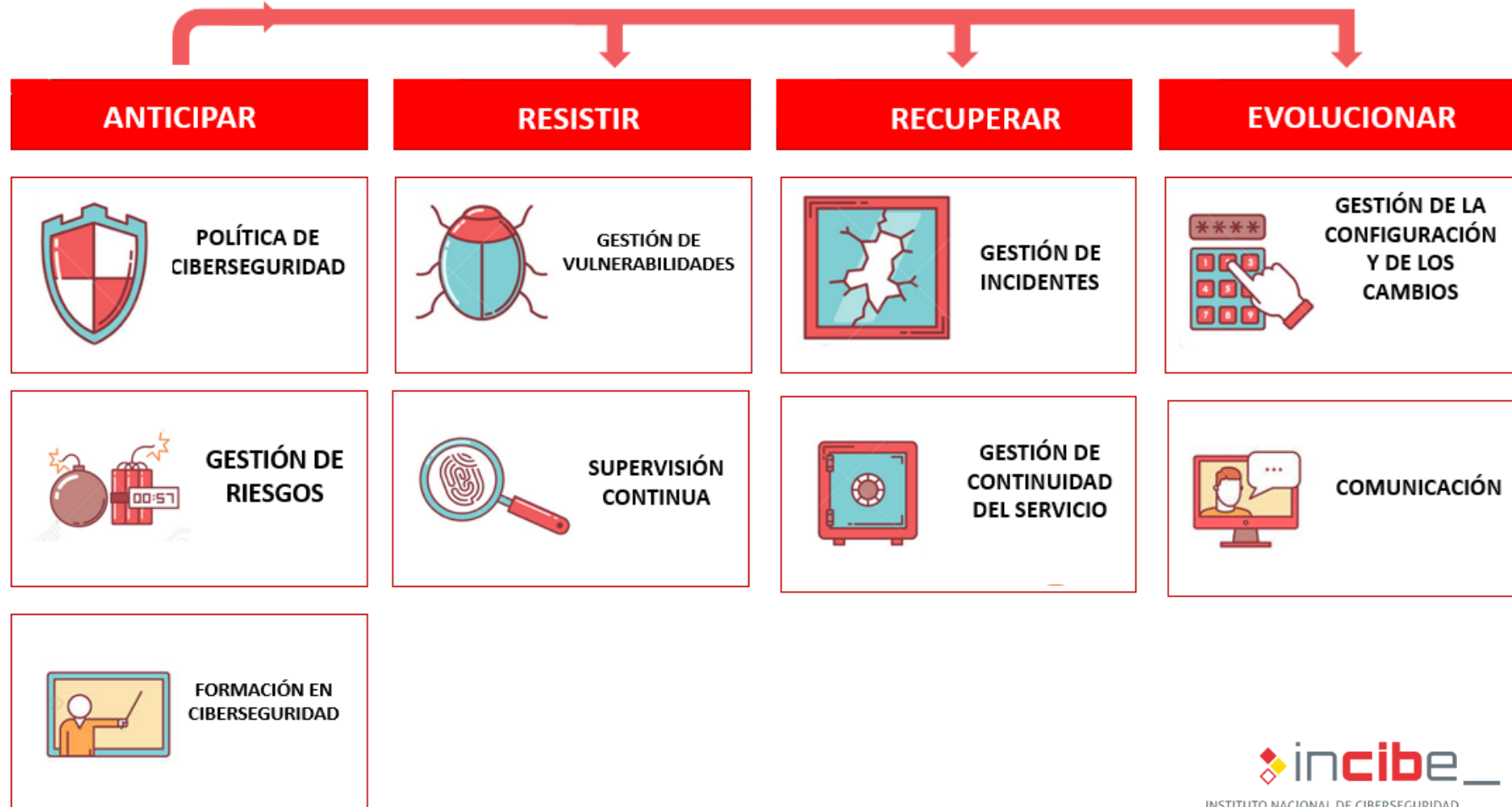
CIBERRESILIENCIA

La ciberresiliencia es la capacidad de una organización de **resistir** a los ataques cibernéticos y de **recuperarse** de forma rápida y efectiva.

Las claves de una estrategia de seguridad sólida

CIBERRESILIENCIA

LA CLAVE PARA SOBREPONERSE A LOS INCIDENTES



CIBERRESILIENCIA: **ANTICIPAR**



**AUDITORÍAS
DE SEGURIDAD
IT / CÓDIGO**



**FORMACIÓN
/ CONCIENCIACIÓN A
USUARIOS**

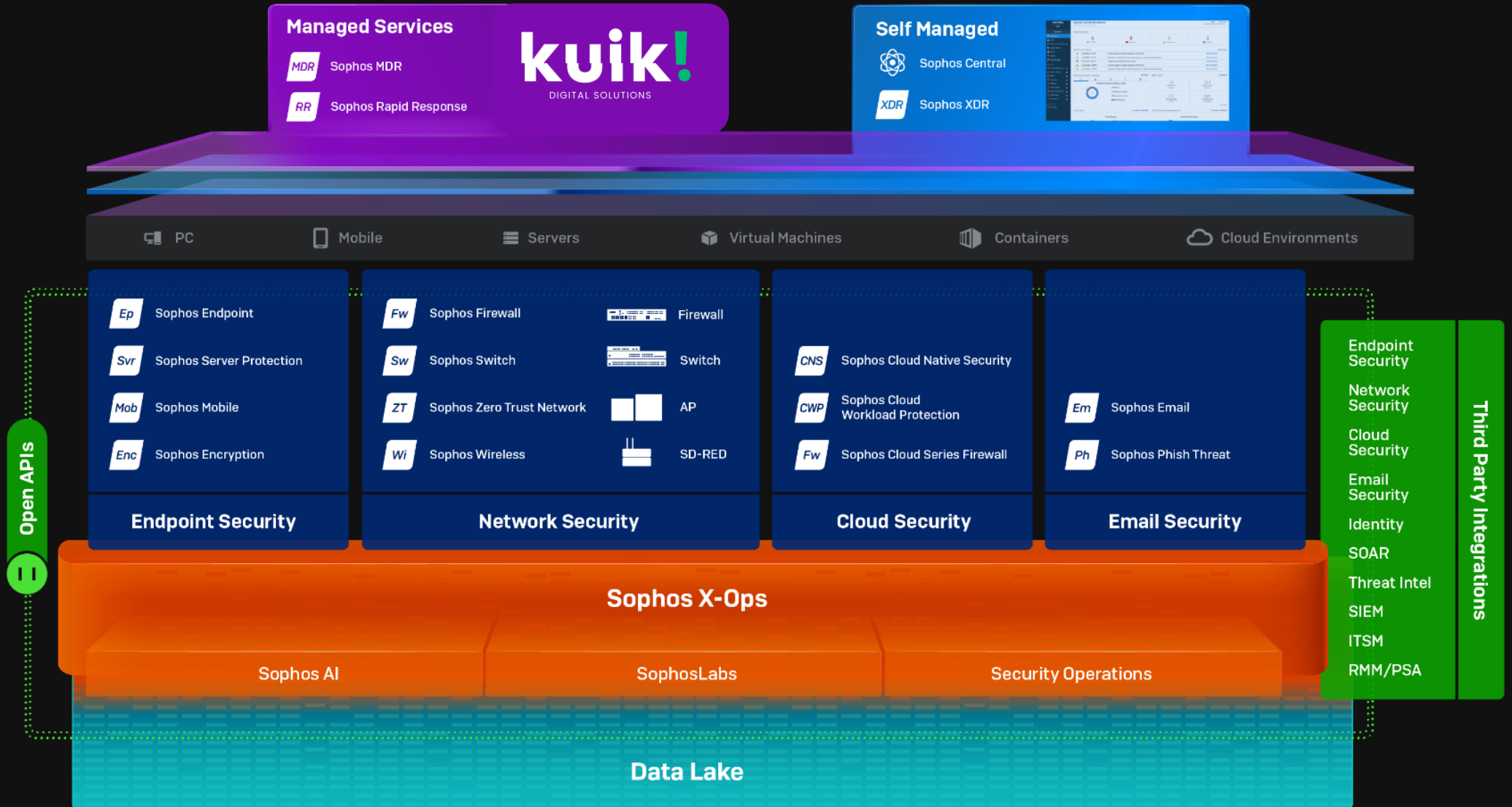
¿Te has preguntado alguna vez si tus aplicativos son seguros o suponen una brecha de seguridad para tu compañía?

AUDITORÍA DE SEGURIDAD A NIVEL DE CÓDIGO





CIBERRESILIENCIA: RESISTIR



REGLA FUNDAMENTAL BACKUPS

3 - 2 - 1

EVOLUCIÓN

3 - 2 - 1 - 1 - 0

3

Different copies
of data



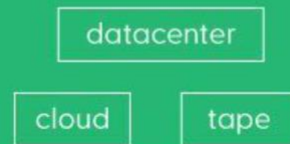
2

Different media



1

of which is
off-site



1

is offline,
air-gapped or
immutable



0

No errors after
backup
recoverability
verification





**BACKUPS
INMUTABLES**



**KUIK CLOUD
BACKUP**



CIBERRESILIENCIA: EVOLUCIONAR

Evolucionar dentro de la ciberresiliencia implica **adoptar un enfoque proactivo y adaptable** para proteger los activos y datos críticos de la organización contra las ciberamenazas.

**LA IMPLEMENTACIÓN
DE CONTROLES** de seguridad
robustos



**LA FORMACIÓN DEL
PERSONAL** en concienciación
sobre seguridad



EL DESARROLLO DE PLANES
de respuesta a incidentes





CIBERRESILIENCIA: EVOLUCIONAR

¡Fortalece tus **CIBERDEFENSAS** apoyándote en un **proveedor estratégico!**

kuik!
DIGITAL SOLUTIONS

kuik!

DIGITAL SOLUTIONS

¡Gracias!

Eskerrik asko!

Thank you!

Merci!



Txirrita-Maleo Biribil, 1, 1ª Planta
20100 Errenteria, Gipuzkoa

Tel. (+34) 943 092 805
inaki.calvo@kuik.tech

www.kuik.tech