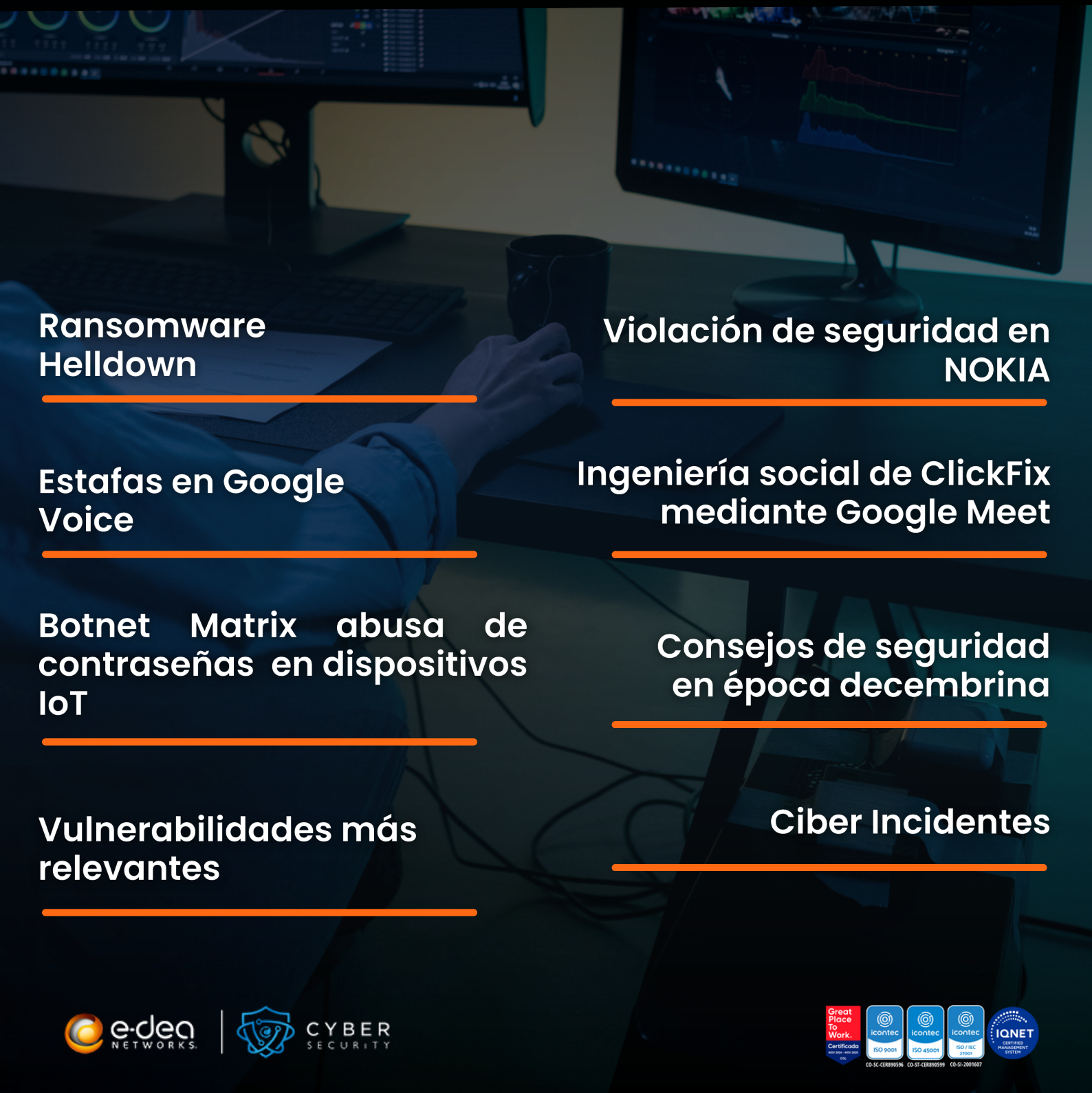
CIBER E-DEA

Boletín de Seguridad



Ransomware Helldown

Violación de seguridad en NOKIA

Estafas en Google Voice

Ingeniería social de ClickFix mediante Google Meet

Botnet Matrix abusa de contraseñas en dispositivos IoT

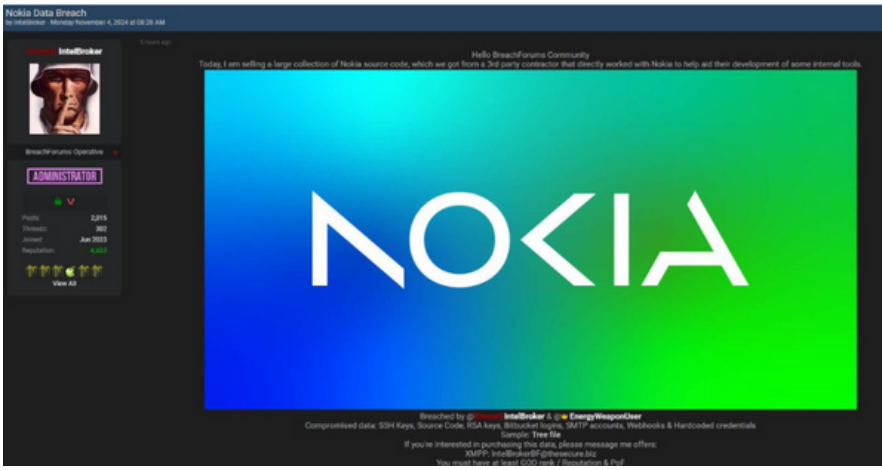
Consejos de seguridad en época decembrina

Vulnerabilidades más relevantes

Ciber Incidentes

VIOLACIÓN DE SEGURIDAD EN NOKIA

La multinacional de tecnología y telecomunicaciones, NOKIA investiga un intento no autorizado a información interna a través de un contratista externo que provocó el robo de datos sensibles como claves RSA y cuentas de protocolo de transferencia de correo (SMTP).



El ataque ha sido reivindicado por 'IntelBroker' quien estaría vendiendo el código fuente de Nokia por 20.000 dólares en foros de la dark web donde asegura haber accedido a un servidor 'SonarQube' con credenciales predeterminadas de uno de los proveedores de Nokia, descargando desde allí información crítica y archivos confidenciales.

Nokia ha confirmado que hasta el momento no se han encontrado evidencias de que sus sistemas internos o datos personales de clientes y empleados hayan sido directamente comprometidos. No obstante, la empresa ha puesto en marcha un plan de contingencia y está colaborando estrechamente con expertos en ciberseguridad para investigar a fondo el incidente.

¿QUIEN ES INTELBROKER?

Se sabe que es serbio y vive en Rusia donde orquesta sus operaciones cibernéticas. y se comunica a través de los 'BreachForums' que se encuentran en la dark web.
Ha estado implicado en otros incidentes de ciberseguridad, incluyendo ataques a empresas como Hewlett Packard Enterprise (HPE) Además, ha filtrado datos de empresas como T-Mobile y Apple, también obtenidos a través de proveedores externos de software.
Ha robado archivos de los Departamentos de Estado y Seguridad Nacional de Estados Unidos, filtrando 5,8 millones de registros de vuelos del Departamento de Transporte e incluso la vulneración de los sistemas del aeropuerto de Los Ángeles, por esto es que se cree que su mayor motivación es "socavar al gobierno"

Más información

Google elimina sitios de noticias falsas

Más Información

Google ha bloqueado cientos de servicios de noticias falsas y sitios web de sus resultados de búsqueda con el argumento de que estaban sirviendo propaganda china.

El Grupo de Análisis de Amenazas de Google indicó que un grupo llamado Glassbridge, ha estado creando y operando cientos de dominios que se hacen pasar por sitios web de noticias independientes de docenas de países.

El gigante tecnológico dijo que ha bloqueado más de mil sitios web para que no aparezcan en sus productos Google News y Google Discover.

Estos sitios se hacían pasar por medios de comunicación independientes y, a menudo, locales, los actores de IO pueden adaptar su contenido a audiencias regionales específicas y presentar sus narrativas como noticias y contenido editorial aparentemente legítimos.

Botnet de Matrix abusa de contraseñas en dispositivos IoT

Un actor de amenazas, apodado como Matrix ha sido vinculado a una campaña de ataques de Denegación de Servicio Distribuido (DDoS) a gran escala. Estos ataques aprovechan vulnerabilidades y configuraciones incorrectas en dispositivos del Internet de las Cosas (IoT), permitiendo su incorporación a una botnet para actividades disruptivas.

Hace uso de una amplia variedad de scripts y herramientas de código abierto disponibles en GitHub, con el objetivo de desplegar el malware Mirai y otros programas de DDoS en los dispositivos comprometidos.

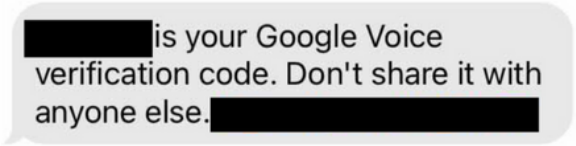
Más Información

Modus operandi de las estafas de Google Voice.

Google Voice es un servicio gratuito de VOZ IP que permite configurar un número de teléfono virtual a tu cuenta de google, se puede usar para enviar y recibir mensajes, llamadas e incluso realizar videollamadas.

Este se encuentra vinculado a tu número, de modo que cuando alguien llama al número de Google Voice puedes descolgar utilizando tu teléfono físico.
Los estafadores aprovechan esto y te contactan argumentando que quieren comprar algo que tú estás vendiendo fingiendo tener dudas de seguir adelante con la compra ya que se han enterado de que hay listados falsos y que quieren verificar que eres una persona real.

Google Voice



Luego proceden a enviarte un mensaje de texto con un código de verificación de Google y donde te solicitan ese código para supuestamente corroborar que no seas un estafador ni bot.
Al darles el código de verificación, tratarán de usarlo para crear un número de Google Voice vinculado a tu número de teléfono y así podría usar ese número para estafar a otra gente o suplantar tu identidad y así acceder a tus cuentas o para abrir nuevas cuentas bajo tu nombre.

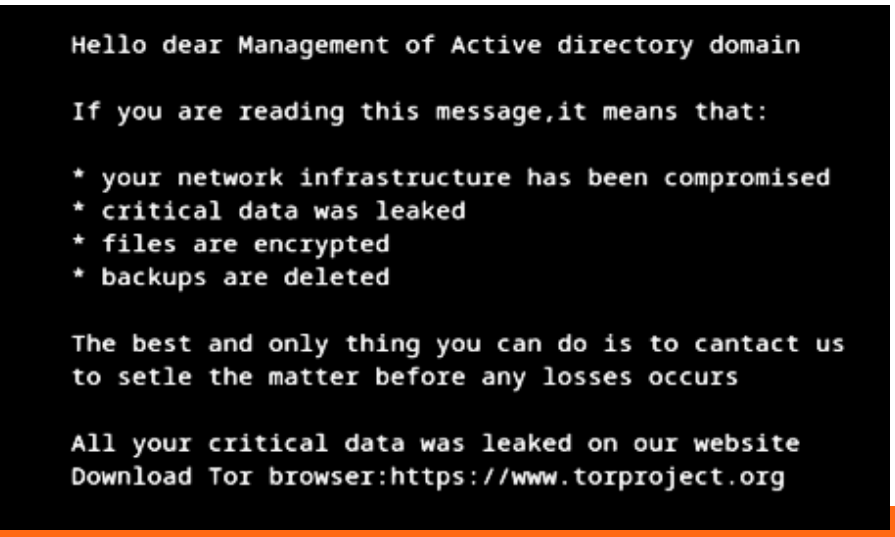
¿Cómo protegerse de las estafas en Google Voice?

- Nunca compartir códigos de verificación: Los códigos de autenticación enviados por Google u otras plataformas están destinadas para un uso exclusivamente personas y no deben compartirse con desconocidos.
- Tener cuidado en las plataformas de compraventa: Si alguien pide verificar que no eres un bot o un estafador, explora métodos alternativos de verificación que no impliquen compartir información sensible .
- Evitar llevar la conversación a otros canales: Cualquier solicitud de pasar la conversación a WhatsApp o a una llamada directa debería ser una señal de alerta de posible estafa.
- En caso de que ya haya sido víctima de esta estafa, Google cuenta con una **página de soporte** que permite recuperar el número en un plazo de 45 días.

Más información

NUEVA VARIANTE DE RANSOMWARE HELLDOWN

Helldown llamó la atención por primera vez a mediados de 2024, cuando atacó a los sistemas Windows.



Se basa en LockBit 3.0, una conocida familia de ransomware.
Su última variante para Linux va dirigido a las máquinas virtuales (VM) de VMware, con el objetivo de matar las VM activas antes del cifrado.

Helldown utiliza la explotación de vulnerabilidades en dispositivos Zyxel para obtener acceso inicial a las redes, seguido de actividades como recolección de credenciales y movimientos laterales para desplegar el ransomware.

Una vez dentro, utiliza herramientas sencillas pero eficaces para aumentar los privilegios, desactivar la seguridad y extraer datos. La variante de Linux llama la atención porque, a diferencia de su homóloga de Windows, carece de trucos de evasión habituales como la ofuscación. Esta simplicidad sugiere que se trata de un trabajo en proceso, pero sigue siendo peligroso. El ataque a las máquinas virtuales permite a los operadores de ransomware maximizar el daño.
Al eliminar las máquinas virtuales, pueden interrumpir operaciones críticas en TI y otras industrias.

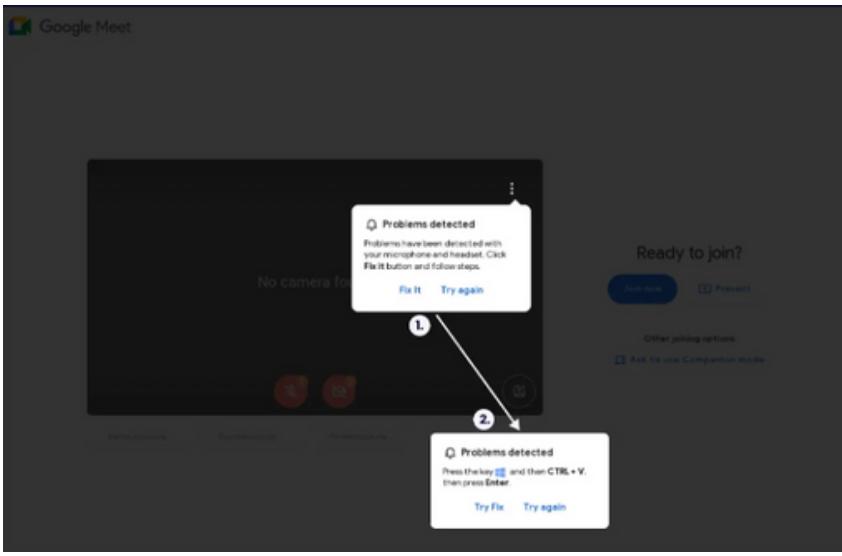
Recomendaciones:

- Zyxel ha emitido un aviso instando a los clientes a actualizar su firmware y cambiar las contraseñas de administrador luego de un informe de Sekoia de que los actores de amenazas están apuntando a sus firewalls para realizar ataques de ransomware.

Más información

Ingeniería social de ClickFix mediante Google Meet

ClickFix es una nueva amenaza que utiliza tácticas de ingeniería social para suplantar sitios web legítimos, como Google Meet, con el objetivo de engañar a los usuarios para que ejecuten scripts maliciosos.



Distribuida principalmente a través de phishing, esta campaña logra que los sistemas afectados instalen malware sin ser detectados por las soluciones de seguridad convencionales, representando un riesgo significativo tanto para usuarios individuales como corporativos.

El ataque comienza con un correo electrónico que parece una invitación legítima de Google Meet para una reunión de trabajo o algún evento relevante.
Los enlaces en estos correos son casi idénticos a los reales, lo que dificulta a simple vista sobre si es un enlace legitimo.

El ataque comienza con un correo electrónico que parece una invitación legítima de Google Meet para una reunión de trabajo o algún evento relevante.
Los enlaces en estos correos son casi idénticos a los reales, lo que dificulta a simple vista sobre si es un enlace legitimo.

Si la víctima hace clic en uno de estos enlaces, se le lleva a una página falsa que parece Google Meet, donde rápidamente aparece un mensaje diciendo que hay un problema técnico, como un fallo con el micrófono o los auriculares.

Cuando el usuario hace clic en "Probar solución", el sitio copia un código de PowerShell en su portapapeles y le indica que lo pegue en la terminal de Windows. Si lo hacen, su computadora se infecta con malware que se descarga desde el dominio malicioso googiedrivers[.]com.

Más Información

¿Cómo protegerse de las estafas en época decembrina?

La temporada navideña es una época de alegría, compras y celebraciones, pero también un momento en que los ciberdelincuentes intensifican sus esfuerzos.

En el segundo semestre de 2023, los fraudes con tarjetas regalo aumentaron un 110%, mientras que los ataques relacionados con scraping, tarjetas de fidelización y tarjetas de pago crecieron más del 700%.

Este entorno es un caldo de cultivo para fraudes como el typosquatting y las falsificaciones de tiendas en línea, que engañan a los consumidores para que compartan datos sensibles o realicen compras en sitios falsos.

El phishing impulsado por IA y los ataques de credenciales obligaron a empresas como 23andMe.com a fortalecer sus defensas tras la exposición de 14.000 cuentas.

En 2023, Amazon reportó que los incidentes de phishing se duplicaron en la segunda mitad del año.

Recomendaciones:

- Actualizar regularmente las aplicaciones y software.
- Usar contraseñas fuertes y seguras.
- Evitar compartir información personal.
- Realizar copias de seguridad constantemente.
- Habilitar el doble factor de autenticación.
- Evitar conectarse a redes públicas

Vulnerabilidades destacadas

Microsoft ha corregido 89 vulnerabilidades en sus productos, dos de las cuales están siendo explotadas activamente.
Una de ellas, CVE-2024-43451 , es especialmente alarmante ya que permite a los atacantes obtener acceso al hash NTLMv2 de la víctima.

CVE-2024-43451

Microsoft - Windows

Versiones afectadas

Todas las versiones.

CVE-2024-20418

Cisco

Versiones afectadas

Cisco Catalyst

Una vulnerabilidad en la interfaz de administración basada en web de Cisco podría permitir que un atacante remoto no autenticado realice ataques de inyección de comandos con privilegios de root en el sistema operativo.

CVE-2024-0012

Paloalto

Versiones afectadas

PAN-OS

Una omisión de autenticación en el software PAN-OS de Palo Alto Networks permite que un atacante no autenticado con acceso de red a la interfaz web obtenga privilegios de administrador de PAN-OS.

Ciber incidentes en Colombia y en el mundo

Colombia fue víctima de 36 mil millones de intentos de ciberataques en 2024

Entre enero y noviembre de 2024, Colombia fue blanco de 36 mil millones de intentos de ciberataques, de acuerdo con un informe de Fortinet.

Los ataques más comunes fueron: Phishing, Ataque de denegación de servicios (DoS) y Ransomware.

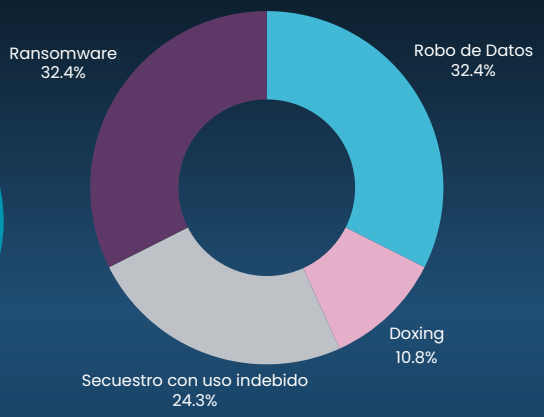
Más información

El mundo

37

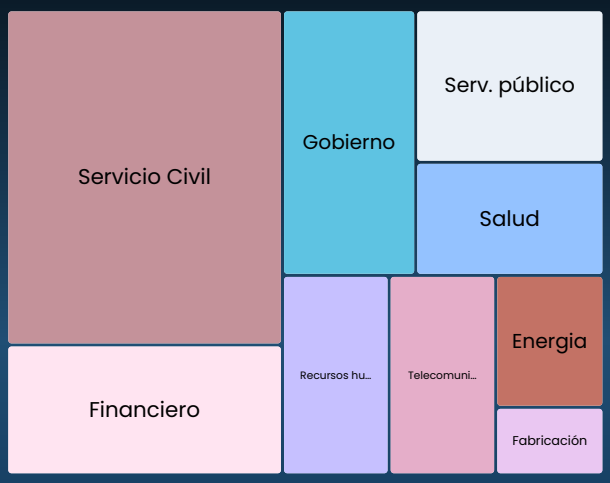
Ciber incidentes

TIPO DE INCIDENTE

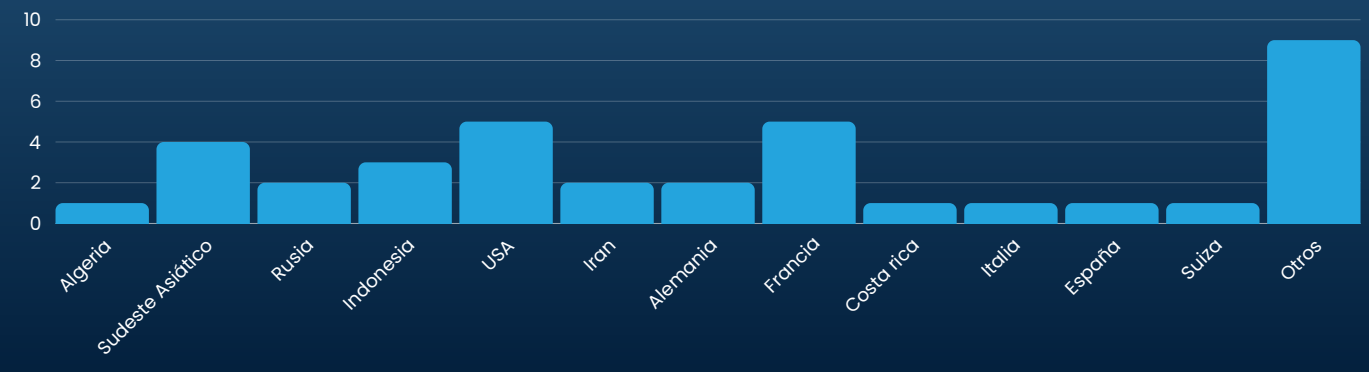


SECTORES AFECTADOS

Más información



PAISES ATACADOS



CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

www.e-dea.co