GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

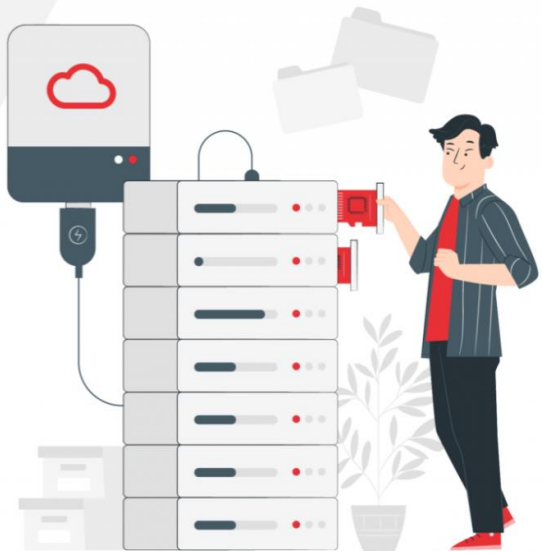
incibe_ ES-ISAC TIC

Informe de situación de ciberseguridad (2024)

Sectores Estratégicos: Sector TIC

TLP:AMBER

ES-ISAC
TIC



La información contenida en este documento está clasificada como sensible de nivel **TLP:AMBER**, lo que significa que los receptores pueden compartirla únicamente con miembros de su propia organización que necesiten conocerla, y con clientes, proveedores o asociados que deban estar al tanto para protegerse a sí mismos o evitar daños.

Puede encontrar más información al respecto en este enlace: https://www.incibe.es/incibe-cert/sobre-incibe-cert/TLP

Por otro lado, este informe se basa en información obtenida a través de diversas fuentes. El contenido de este informe debe considerarse solo de referencia. Por lo tanto, los usuarios son totalmente responsables de confiar o no en dicho contenido. Ni ES-ISAC TIC, ni las entidades que lo conforman asumen ninguna responsabilidad por la exactitud ni las consecuencias del uso de esta información.

ÍNDICE

ÍNDICE DE FIGURAS

1. Introducción

ES-ISAC TIC

El 22 de octubre de 2024 se constituyó el ES-ISAC TIC [1]. Se trata de una colaboración público privada, voluntaria y gratuita, impulsada por INCIBE (Instituto Nacional de Ciberseguridad). Está constituida inicialmente además por CONETIC (confederación española de empresas de tecnologías de la información, comunicaciones y electrónica) y AMETIC (asociación multisectorial de empresas de la electrónica, las tecnologías de la información y la comunicación, de las telecomunicaciones y de los contenidos digitales).

Sobre este informe

La última versión editada de este informe es de septiembre de 2025 y la información incluida en él se circunscribe específicamente al año 2024.

Este documento da respuesta a uno de los compromisos adquiridos por INCIBE y las asociaciones que conforman el ES-ISAC TIC, en su plan de trabajo para el año 2025. En concreto, se trata del **Objetivo 3: Informe periódico de situación del sector**.

Tener un conocimiento detallado de la ciberseguridad en el sector TIC es necesario para orientar adecuadamente las acciones futuras a llevar a cabo en el marco del ES-ISAC TIC.

Por último, cabe destacar que el término "sector TIC" empleado en este informe incluye los siguientes sectores que aparecen en la Directiva NIS2:

- **Infraestructura digital**. Señalado en el Anexo I: Sectores de Alta Criticidad.
- **Gestión de servicios de TIC (de empresa a empresa)**. Señalado en el Anexo I: Sectores de Alta Criticidad.
- **Proveedores de servicios digitales**. Señalado en el Anexo II: Otros sectores críticos.

Metodología

Para elaborar este contenido, se ha empleado una **metodología** que combina **fuentes abiertas de terceros** (noticias, reportes, análisis técnicos, etc.) y **fuentes propias de INCIBE** de dominio público.

Objetivo

El presente informe persigue proporcionar una visión global de la información de inteligencia en ciberseguridad más relevante para el sector TIC, durante el año 2024, desarrollándose en los siguientes apartados específicos:

- Principales **vulnerabilidades** de las tecnologías utilizadas por el sector.
- **Ciberincidentes** más importantes de los que se ha tenido conocimiento.
- **Ciberamenazas** más relevantes.
- **Buenas prácticas** y **cumplimiento normativo**.
- **Tendencias** en ciberseguridad.

Contacto

Ante cualquier duda o cuestión relacionada con este informe, el punto de contacto es el siguiente buzón de correo electrónico:

es-isac-tic@incibe.es

Ilustración 1: correo electrónico de contacto de ES-ISAC TIC

2. Vulnerabilidades

El termino CVE (*Common Vulnerabilities and Exposures*) es el estándar internacional para la identificación de vulnerabilidades existentes en un determinado dispositivo informático. Al descubrirse un problema de seguridad en un dispositivo, se analiza si el error ha sido descubierto con anterioridad y, si no es así, se le asigna un identificador.

El método más comúnmente utilizado para la puntuación CVE es el sistema de puntuación de vulnerabilidad común o CVSS (*Common Vulnerability Scoring System*). CVSS es considerado el mecanismo estándar para medir la gravedad de las vulnerabilidades de seguridad, lo que facilita que las organizaciones prioricen cuáles resolver primero.

En concreto, puntúa las vulnerabilidades en una escala de 0 a 10, donde 0 representa la ausencia de riesgo y 10 el nivel de severidad más alto. Internamente la puntuación se basa en cuatro grupos de métricas adicionales. A continuación, se pueden ver las diferentes categorías de severidad en base a dicha puntuación:

Puntuación	Severidad
0	Nula
0,1 - 3,9	Baja
4,0 - 6,9	Media
7,0 - 8,9	Alta
9,0 - 10	Crítica

Ilustración 2: categorías de severidad en base a la puntuación CVSS (versiones 3.x y 4.0)

En base al registro de CVE publicados durante el 2024, se han identificado un total de 149 vulnerabilidades conocidas que se haya evidenciado de alguna manera haber sido explotadas, lo que supone que al menos el 0.37% de vulnerabilidades publicadas de una forma controlada han acabado aun así provocando un ciberincidente.

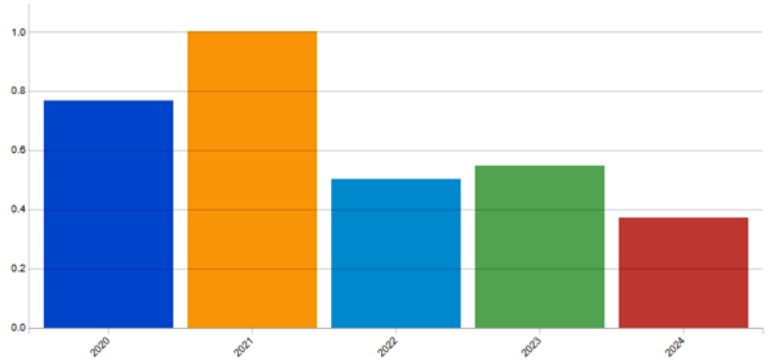


Ilustración 3: evolución temporal del porcentaje de CVE explotados [https://nvd.nist.gov/]

A continuación, se exponen algunas vulnerabilidades relevantes que han afectado durante 2024 al sector TIC, principalmente publicadas por CISA, ordenadas en función de su severidad:

01

EcoStruxure IT Gateway

Schneider Electric

Descripción: existe una vulnerabilidad de autorización faltante que podría causar acceso no autorizado a los dispositivos de la infraestructura TIC cuando se habilita en la red y, potencialmente, afectar los dispositivos conectados.

CVE-2024-10575
ICSA-24-326-05

Solución: actualizar el software a la última versión publicada.

Recomendaciones: ubicar el software en una red con control de acceso. Minimizar la exposición de la plataforma, ubicándola detrás de un *firewall* y denegando el acceso remoto a la API. Habilitar la actualización automática del software.

Tipo de vulnerabilidad: falta de autorización (CWE-862)

Publicación: 13/11/2024

Fuentes: CISA, NVD, INCIBE

Critica

9,8 CVSS v3

10 CVSS v4

02

Controladores de la serie DDC4000

Kieback & Peter

Descripción: la serie DDC4000 de Kieback & Peter es vulnerable a una vulnerabilidad de *path traversal* que puede permitir que un atacante no autenticado lea archivos en el sistema y consiga permisos de administración.

CVE-2024-41717
ICSA-24-291-05

Solución: para los controladores que han llegado al final de su ciclo de vida, actualizar a otros controladores con soporte. Para los controladores con soporte, actualizar el software a la última versión publicada.

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall*, evitando que esté expuesta a Internet y aislando estos dispositivos de otras redes de la organización. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: *path traversal* (CWE-22)

Publicación: 22/10/2024

Fuentes: CISA, NVD, INCIBE

Critica

9,8 CVSS v3

9,3 CVSS v4

03

Reyee OS

Ruijie

Descripción: Las versiones del sistema operativo Ruijie Reyee 2.206.x hasta la 2.320.x, pero no incluida, utilizan una función inherentemente peligrosa que podría permitir a un atacante enviar un mensaje MQTT malicioso que resulte en que los dispositivos ejecuten comandos arbitrarios del sistema operativo.

CVE-2024-52324
ICSA-24-338-01

Solución: Ruijie informó que los problemas se solucionaron en la nube y que los usuarios finales no necesitan realizar ninguna acción.

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall*, evitando que esté expuesta a Internet y aislando estos dispositivos de otras redes de la organización. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: *Use of Inherently Dangerous Function* (CWE-242)

Publicación: 22/10/2024

Fuentes: CISA, NVD, INCIBE

Critica

9,8 CVSS v3

9,2 CVSS v4

04

CVE-2024-41988
ICSA-24-277-01

Opera Plus FM Family Transmitter

TEM SRL

Descripción: TEM Opera Plus FM Family Transmitter permite el acceso a un *endpoint* desprotegido que permite la carga de imágenes binarias del sistema de archivos MPFS sin autenticación. Este sistema de archivos sirve como base para el módulo de servidor web HTTP2, pero también lo utiliza el módulo SNMP y está disponible para otras aplicaciones que requieren capacidades básicas de almacenamiento de solo lectura. Esto se puede aprovechar para sobrescribir la memoria flash del programa que contiene las interfaces principales del servidor web y ejecutar código arbitrario.

Solución: TEM no ha respondido a las solicitudes de colaboración con CISA para mitigar estas vulnerabilidades. Se recomienda a los usuarios de los productos afectados que se pongan en contacto con TEM para obtener más información.

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall*, evitando que esté expuesta a Internet y aislando estos dispositivos de otras redes de la organización. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: ausencia de autenticación para una función crítica (CWE-306)

Publicación: 03/10/2024

Fuentes: CISA, NVD, INCIBE

Critica

N/A
CVSS v3

9,3
CVSS v4

05

CVE-2024-9166
ICSA-24-270-03

Atemio AM 520 HD Full HD Satellite Receiver

Atelmo

Descripción: El dispositivo permite que un atacante no autorizado ejecute comandos del sistema con privilegios elevados. Esta vulnerabilidad se facilita mediante el uso de la consulta 'getcommand' dentro de la aplicación, lo que permite al atacante obtener acceso superusuario.

Solución: Atelmo ha declarado que este producto ha sido descontinuado. No hay direcciones de servicio ni soporte disponibles.

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall*, evitando que esté expuesta a Internet y aislando estos dispositivos de otras redes de la organización. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: neutralización incorrecta de elementos especiales usados en un comando de sistema operativo (Inyección de comando de sistema operativo) (CWE-78)

Publicación: 26/09/2024

Fuentes: CISA, NVD, INCIBE

Critica

N/A
CVSS v3

9,3
CVSS v4

06

CVE-2024-50557
ICSA-24-319-06

SCALANCE M-800 Family

Siemens AG

Descripción: esta vulnerabilidad afecta a varios dispositivos de red de Siemens, incluyendo los modelos RUGGEDCOM RM1224 LTE (4G) y varios modelos de la serie SCALANCE. Este fallo se debe a que los dispositivos afectados no validan correctamente la entrada en los campos de configuración de la funcionalidad iperf,

Critica

9,8
CVSS v3

lo que permite a un atacante remoto no autenticado ejecutar código arbitrario en el dispositivo

Solución: actualizar a la versión V8.2 o superior.

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall*, evitando que esté expuesta a Internet y aislando estos dispositivos de otras redes de la organización. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: *Improper Input Validation* (CWE-20)

Publicación: 12/11/2024

Fuentes: CISA, NVD, INCIBE

8,6 CVSS v4

07

CVE-2024-34102

Adobe Commerce y Magento Open Source

Adobe Systems Incorporated

Descripción: problema de restricción incorrecta de la referencia a una entidad externa XML (CWE-611) que afecta a Adobe Commerce y Magento Open Source, en versiones 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 y anteriores.

Solución: actualizar el software a la última versión publicada.

Recomendaciones: implementar medidas de seguridad adicionales, como la validación estricta de entradas y la configuración adecuada de las políticas de seguridad XML.

Tipo de vulnerabilidad: restricción incorrecta de la referencia a entidad externa XML (CWE-611)

Publicación: 13/06/2024

Fuentes: NVD, INCIBE

Critica

9,8 CVSS v3

N/A CVSS v4

08

CVE-2024-42355

Shopware

Shopware AG

Descripción: Shopware, una plataforma de comercio electrónico abierta, tiene una nueva etiqueta Twig `sw_silent_feature_call` que silencia los mensajes de obsolescencia mientras se activa en esta etiqueta. Antes de las versiones 6.6.5.1 y 6.5.8.13, acepta como parámetro una cadena con el nombre del indicador de característica a silenciar, pero este parámetro no se escapa correctamente y permite la ejecución de código.

Solución: actualizar a Shopware 6.6.5.1 o 6.5.8.13 para recibir un parche. Para las versiones anteriores 6.2, 6.3 y 6.4 también están disponibles las medidas de seguridad correspondientes a través de un complemento.

Tipo de vulnerabilidad: control incorrecto de generación de código (Inyección de código) (CWE-94)

Publicación: 08/08/2024

Fuentes: NVD, INCIBE

Critica

9,8 CVSS v3

N/A CVSS v4

09

CVE-2024-24308

Módulo Boostmyshop para PrestaShop

Boostmyshop France SAS

Descripción: vulnerabilidad de inyección SQL en el módulo Boostmyshop (boostmyshopagent) para las versiones de Prestashop 1.1.9 y anteriores, permite

Critica

9,8

	a atacantes remotos escalar privilegios y obtener información confidencial a través de changeOrderCarrier.php, RelayPoint.php y ShippingConfirmation.php. Solución: aplicar el parche de la versión 1.1.9 o actualizar el software a la última versión publicada. Recomendaciones: https://security.friendsofpresta.org/modules/2024/02/08/boostmyshopagent.html Tipo de vulnerabilidad: neutralización incorrecta de elementos especiales usados en un comando SQL (Inyección SQL) (CWE-89) Publicación: 09/02/2024 Fuentes: NVD, INCIBE	CVSS v3 N/A CVSS v4

10 CVE-2024-36678	**Módulo "Configuración del tema" para PrestaShop** Promokit.eu Descripción: en el módulo "Configuración del tema" (pk_themesettings) <= 1.8.8 de Promokit.eu para PrestaShop, un invitado puede realizar una inyección SQL. El script ajax.php tiene una llamada SQL sensible que puede ejecutarse con una llamada http trivial y explotarse para falsificar una inyección SQL. Solución: N/A Recomendaciones: https://security.friendsofpresta.org/modules/2024/06/18/pk_themesettings.html Tipo de vulnerabilidad: neutralización incorrecta de elementos especiales usados en un comando SQL (Inyección SQL) (CWE-89) Publicación: 19/06/2024 Fuentes: NVD, INCIBE	Critica 9,8 CVSS v3 N/A CVSS v4

11 CVE-2024-45115	**Adobe Commerce** Adobe Inc. Descripción: las versiones 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 y anteriores de Adobe Commerce se ven afectadas por una vulnerabilidad de autenticación incorrecta que podría provocar una escalada de privilegios. Un atacante podría aprovechar esta vulnerabilidad para obtener acceso no autorizado o privilegios elevados dentro de la aplicación. La explotación de este problema no requiere la interacción del usuario. Solución: actualizar el software a la última versión publicada. Tipo de vulnerabilidad: autenticación incorrecta (CWE-287) Publicación: 10/10/2024 Fuentes: NVD, INCIBE	Critica 9,8 CVSS v3 N/A CVSS v4

12 CVE-2024-11281	**WooCommerce Point of Sale para WordPress** WooCommerce Inc. Descripción: el complemento WooCommerce Point of Sale para WordPress es vulnerable a la escalada de privilegios en todas las versiones hasta la 6.1.0 incluida. Esto se debe a una validación insuficiente del valor 'logged_in_user_id' cuando los valores de las opciones están vacíos y a la capacidad de los atacantes de cambiar el correo electrónico de cuentas de usuario arbitrarias. Esto hace posible que	Critica 9,8 CVSS v3

atacantes no autenticados cambien el correo electrónico de cuentas de usuario arbitrarias, incluidos los administradores, y restablezcan su contraseña para obtener acceso a la cuenta.

Solución: actualizar el software a la última versión publicada.

Tipo de vulnerabilidad: falta de autorización (CWE-862)

Publicación: 25/12/2024

Fuentes: NVD, INCIBE

N/A

CVSS v4

13

CVE-2024-23832

Mastodon

Mastodon gGmbH

Descripción: Mastodon es un servidor de red social gratuito y de código abierto basado en ActivityPub. Mastodon permite la configuración de LDAP para la autenticación. Debido a una validación de origen insuficiente en todos los Mastodon, los atacantes pueden hacerse pasar por cualquier cuenta remota y apoderarse de ella. Todas las versiones de Mastodon anteriores a la 3.5.17 son vulnerables, así como las versiones 4.0.x anteriores a la 4.0.13, la versión 4.1.x anteriores a la 4.1.13 y las versiones 4.2.x anteriores a la 4.2.5.

Solución: actualizar el software a alguna de las versiones parcheadas (3.5.17, 4.0.13, 4.1.13, 4.2.5).

Tipo de vulnerabilidad: *Authentication Bypass by Spoofing* (CWE-290)

Publicación: 01/02/2024

Fuentes: NVD, INCIBE

Critica

9,8 CVSS v3

N/A

CVSS v4

14

CVE-2024-39703

ICSA-24-352-01

ThreatQ Platform

ThreatQuotient Inc.

Descripción: en las versiones de ThreatQ Platform anteriores a la 5.29.3, existe una vulnerabilidad de inyección de comandos en el *endpoint* de su API, que podría permitir a un atacante la ejecución remota de código.

Solución: actualizar el software a la última versión publicada.

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall* y evitando que esté expuesta a Internet. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: inyección de comandos (CWE-77)

Publicación: 18/12/2024

Fuentes: CISA, NVD, INCIBE

Alta

8,8 CVSS v3

8,7 CVSS v4

15

CVE-2024-12700

ICSA-24-354-05

Tibbo AggreGate Network Manager

Tibbo Technology Inc.

Descripción: vulnerabilidad de carga de archivos sin restricciones donde es posible que un usuario autenticado (con poco nivel de privilegios) cargue un shell jsp y ejecute código con los privilegios del usuario que ejecuta el servidor web.

Solución: actualizar el software a la versión 6.40.02, 6.34.03, o a la última versión publicada.

Alta

8,8 CVSS v3

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall* y evitando que esté expuesta a Internet. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: *Unrestricted Upload of File with Dangerous Type* (CWE-434)

Publicación: 19/12/2024

Fuentes: CISA, NVD, INCIBE

8,7 CVSS v4

16

CVE-2024-47130
ICSA-24-270-04

goTenna Pro App

goTenna Inc.

Descripción: la serie goTenna Pro permite a atacantes no autenticados actualizar de forma remota las claves públicas locales utilizadas para mensajes P2P y grupales.

Solución: actualizar Android Pro: v2.0.3 o superior o iOS Pro: v2.0.3 o superior.

Recomendaciones: al compartir claves de cifrado mediante código QR utilizar códigos QR similares a ATAK, para el intercambio seguro de claves de cifrado.

Transmisión segura: al transmitir hay que asegurarse de estar en una zona segura y transmitir la clave a una potencia reducida de 0,5 Watts para limitar la exposición.

Aprovechar el cifrado por capas: implementar claves de cifrado por capas para gestionar las comunicaciones de forma segura, ya sea interactuando con personas o equipos.

Tipo de vulnerabilidad: ausencia de autenticación para una función crítica (CWE-306)

Publicación: 26/09/2024

Fuentes: CISA, NVD, INCIBE

Alta

8,8 CVSS v3

8,7 CVSS v4

17

CVE-2024-11205

WPForms para WordPress

WPForms LLC

Descripción: problema de falta de autorización que afecta al complemento WPForms para WordPress en las versiones desde la 1.8.4 hasta la 1.9.2.1 inclusive. Esto permite que atacantes autenticados, con acceso de nivel de suscriptor o superior, reembolsen pagos y cancelen suscripciones.

Solución: actualizar el software a la versión 1.9.2.2.

Tipo de vulnerabilidad: falta de autorización (CWE-862)

Publicación: 10/12/2024

Fuentes: NVD, INCIBE

Alta

8,5 CVSS v3

N/A CVSS v4

18

CVE-2024-21514

OpenCart

OpenCart Limited

Descripción: vulnerabilidad que afecta a las versiones del paquete opencart/opencart desde 0.0.0. Se identificó un problema de inyección SQL en la extensión de pago Divido para OpenCart, que se incluye de forma predeterminada en la versión 3.0.3.9. Como usuario anónimo no autenticado, si el módulo de pago Divido está instalado (no es necesario habilitarlo), es posible aprovechar la inyección SQL para obtener

Alta

8,1 CVSS v3

acceso no autorizado a la base de datos backend. Para cualquier sitio que sea vulnerable, cualquier usuario no autenticado podría aprovechar esto para volcar toda la base de datos de OpenCart, incluidos los datos de PII del cliente.

Solución: actualizar el software a la versión 3.0.4.0 o superior.

Tipo de vulnerabilidad: inyección SQL (CWE-89)

Publicación: 22/06/2024

Fuentes: NVD, INCIBE

N/A

CVSS v4

19

CVE-2024-10494

ICSA-24-345-04

LabVIEW

National Instruments

Descripción: una lectura fuera de los límites en LabVIEW, debido a una validación de entrada incorrecta, puede revelar información sensible o provocar la ejecución de código arbitrario. Para explotarla con éxito, es necesario que un atacante proporcione a un usuario un vector de inicialización especialmente manipulado. Esta vulnerabilidad afecta a LabVIEW 2024 Q3 y versiones anteriores.

Solución: actualizar el software a la última versión publicada.

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall*, evitando que esté expuesta a Internet y aislando estos dispositivos de otras redes de la organización. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: lectura fuera de rango (CWE-125)

Publicación: 10/12/2024

Fuentes: CISA, NVD, INCIBE

Otras vulnerabilidades relacionadas: CVE-2024-10495, CVE-2024-10496

Alta

7,8

CVSS v3

8,4

CVSS v4

20

CVE-2024-47253

ICSA-24-319-17

Access Commander

2N

Descripción: en las versiones 3.1.1.2 y anteriores de 2N Access Commander, una vulnerabilidad de *path traversal* podría permitir a un atacante escribir archivos en el sistema de archivos para lograr la ejecución remota de código arbitrario.

Solución: actualizar el software a la última versión publicada.

Recomendaciones: minimizar la exposición de la plataforma, ubicándola detrás de un *firewall*, evitando que esté expuesta a Internet y aislando estos dispositivos de otras redes de la organización. Utilizar una VPN segura y actualizada en caso de necesidad de acceso remoto.

Tipo de vulnerabilidad: *path traversal* (CWE-22)

Publicación: 05/11/2024

Fuentes: CISA, NVD, INCIBE

Otras vulnerabilidades relacionadas: CVE-2024-47254, CVE-2024-47255, CVE-2024-47256

Alta

7,2

CVSS v3

8,6

CVSS v4

Recomendaciones

Se recogen a continuación una serie de pautas que pueden ayudar a los responsables de gestionar los activos TIC (software y hardware) de una organización:

- Mantenerse informado de las nuevas vulnerabilidades, suscribiéndose a los boletines de los propios fabricantes. Adicionalmente INCIBE dispone de un servicio gratuito al que suscribirse: Servicio Boletines de INCIBE.
- Disponer de un procedimiento de gestión de parches y actualizaciones de ciberseguridad de parches. Es muy importante que dicho procedimiento establezca bien la prioridad a la hora de abordar cada actualización. Algunas cuestiones a tener en cuenta podrían ser las siguientes:
  - **Nivel de severidad de la vulnerabilidad**. El valor CVSS indica el nivel de criticidad de la misma.
  - **Probabilidad de que la vulnerabilidad sea explotada**. La iniciativa EPSS (*Exploit Prediction Scoring System*) persigue predecir la probabilidad de que una vulnerabilidad sea explotada, basado en datos reales del ecosistema de amenazas.
  - **Contrastar si la vulnerabilidad está ya siendo explotada**. Diferentes fuentes o listas como KEV (*Known Exploited Vulnerabilities*), que es una lista oficial del gobierno de EEUU (CISA) con vulnerabilidades que ya están siendo explotadas activamente, puede facilitar la toma de decisiones a la hora de abordar una vulnerabilidad.

  Adicionalmente se puede consultar en la web de INCIBE un *checklist* de buenas prácticas en las actualizaciones de software, destinado a personal técnico.
- Como principio básico, llevar a cabo una **correcta gestión de riesgos de ciberseguridad** en la organización es fundamental para que el personal encargado de manejar las vulnerabilidades conozca no solo la probabilidad de ocurrencia de una vulnerabilidad, sino también el posible impacto en caso de materializarse.

3. Ciberincidentes

3.1. Ciberincidentes a nivel nacional

Según el último **balance de ciberseguridad publicado por INCIBE** [2], a lo largo del año 2024, a través de su CERT (equipo de respuesta a incidentes de ciberseguridad), gestionó un total de **97.348 incidentes** de ciberseguridad, lo que representa un aumento del 16,6% en comparación con el año anterior. Además, como medida proactiva, se detectaron y notificaron 183.851 sistemas vulnerables relevantes, susceptibles de ser explotados por ciberdelincuentes para acceder a redes o provocar incidentes.

En el ámbito de los operadores esenciales e importantes, alineados con la directiva NIS2, y vitales para el funcionamiento de la sociedad, se atendieron en concreto 341 incidentes. Estos se distribuyeron por sectores clave. De estos incidentes, el 14,1% corresponden al **sector TIC**.

Ilustración 4: sectores más afectados por ciberincidentes

Es importante destacar que, a partir de los datos anteriores, 4 de cada 10 ciberincidentes del total gestionado, estaban relacionados con *malware*, de los que 357 eran *ransomware*, un tipo de *malware* caracterizado porque los ciberdelincuentes bloquean el acceso a los archivos o los sistemas, pidiendo luego un rescate para devolvérselos a las víctimas.

También se han detectado incidentes relacionados con ataques de denegación de servicio distribuidos (DDoS) y accesos no autorizados a sistemas de información que han provocado fugas de información de las organizaciones afectadas.

3.2. Ciberincidentes a nivel internacional

A continuación, se muestra información de algunos de los ciberincidentes más relevantes sufridos por entidades del sector TIC, a nivel internacional, durante el año 2024. En concreto, se han priorizado aquellos ataques dirigidos contra entidades de especial importancia en el sector TIC. Por cada incidente referenciado se aportan datos clave para poder contextualizarlo, los cuales son los siguientes:

- El actor involucrado.
- La víctima del ciberataque.
- El país donde se ha materializado.

- Fecha relacionada con el ciberincidente, bien cuando se detecta, bien cuando se publica.
- Breve descripción del ciberincidente.
- Impacto, en caso de ser conocido.
- Mitigación, también en el supuesto que haya trascendido.
- Fuente pública o propia utilizada para documentar cada caso.

01	Ciberataque a *Societe Francaise Du Radiotelephone*
Actor	APT73
Víctima	Empresa de telecomunicaciones *Societe Francaise Du Radiotelephone - SFR*
Países	Francia
Fecha	Noviembre de 2024
Descripción	En noviembre de 2024, la empresa francesa de telecomunicaciones SFR fue objeto de un ataque de ransomware por parte del grupo conocido como APT73 o Bashe.
Impacto	Los atacantes afirmaron haber exfiltrado 1.445.684 registros que contenían información sensible de clientes, incluyendo nombres, números de teléfono, direcciones, datos de geolocalización y detalles de suscripciones entre otra información.
Mitigación	No han trascendido más detalles acerca de las medidas de mitigación concretas llevadas a cabo por la empresa.
Fuentes	x.com

02	Campaña de ataques a empresas de telecomunicaciones
Actor	Salt Typhoon
Víctima	Al menos nueve empresas de telecomunicaciones fueron comprometidas, incluyendo AT&T, Verizon, Lumen Technologies y T-Mobile.
Países	Estados Unidos
Fecha	2024
Descripción	Se observaron ataques dirigidos a individuos de alto perfil, incluyendo miembros de campañas presidenciales y funcionarios gubernamentales. Durante la campaña, los actores maliciosos aprovecharon vulnerabilidades en dispositivos de red, como enrutadores y “switches”, para infiltrarse en las infraestructuras de telecomunicaciones. Además, comprometieron sistemas utilizados para intervenciones legales, accediendo a información sobre números telefónicos bajo vigilancia y, potencialmente, al contenido de dichas comunicaciones.

Impacto	Los atacantes accedieron a metadatos de llamadas y mensajes de texto, como fechas, horas, números de teléfono y direcciones IP de origen y destino. En ciertos casos, también lograron interceptar el contenido de las comunicaciones.
Mitigación	Como respuesta a esta campaña de ataques, CISA en colaboración con la NSA, el FBI y socios internacionales, se vio obligada a publicar una guía para mitigar ciberataques. Esta recomienda aplicar parches, desactivar protocolos inseguros, usar contraseñas fuertes y configurar alertas para cambios sospechosos, entre otras acciones, como limitar el acceso a dispositivos de gestión, monitorear tráfico de socios de confianza y reforzar la segmentación de redes. También se destaca la importancia de una alta visibilidad en las redes para detectar actividades anómalas y proteger infraestructuras críticas.
Fuentes	wsj.com, wsj.com, wsj.com, lumen.com, cisa.gov

03 Ciberataque a América Móvil

Actor	Trigona
Víctima	Empresa de telecomunicaciones América Móvil, S.A.B. de C.V.
Países	Guatemala, Honduras, El Salvador y Costa Rica
Fecha	Enero de 2024
Descripción	El grupo de ransomware Trigona se atribuyó un ataque contra América Móvil, matriz de Claro, a finales de enero de 2024, afectando los servicios de telefonía en Guatemala, Honduras, El Salvador y Costa Rica. Trigona exigió un rescate de 10 millones de dólares, con fecha límite el 24 de febrero.
Impacto	Claro dio a conocer a través de redes sociales y su sitio web, este ataque que impactó a múltiples empresas subsidiarias, destacando el amplio alcance del incidente en toda la región.
Mitigación	No han trascendido más detalles acerca de las medidas de mitigación concretas llevadas a cabo por la empresa.
Fuentes	cyberKendra.com, x.com

04 Ciberataque a Shopify

Actor	Usuario autoidentificado como 888 en el foro BreachForums
Víctima	Shopify Inc., empresa que ofrece una plataforma de comercio electrónico
Países	Canadá
Fecha	Julio de 2024
Descripción	El usuario 888 del foro BreachForums puso a la venta una base de datos exfiltrada, supuestamente, a la plataforma de comercio digital Shopify. Según el actor malicioso el archivo contenía 179.873 líneas de datos de clientes que incluían nombre, dirección y teléfono entre otros, aunque no se hace mención a datos bancarios. Sin embargo, Shopify negó que sus sistemas hubieran sido comprometidos, vinculando el incidente a un problema en un proveedor externo.

Impacto	Exfiltración de 179.873 líneas de datos de clientes que incluían nombre, dirección y teléfono.
Mitigación	No han trascendido más detalles acerca de las medidas de mitigación concretas llevadas a cabo por la empresa.
Fuentes	Shopify.com, cyberpress.org, x.com, bleepingcomputer.com

05 Ciberataque a PandaBuy

Actor	Desconocido
Víctima	Plataforma de compras en línea PanDa (HongKong) Technology Co. (PandaBuy)
Países	China (Hong Kong)
Fecha	Abril de 2024
Descripción	La plataforma de compras en línea PandaBuy sufrió una brecha de datos que afectó a 1,3 millones de clientes. El incidente fue resultado de la explotación de múltiples vulnerabilidades críticas en la API de la plataforma. Tras el pago inicial de un rescate, la empresa fue objeto de un segundo intento de extorsión.
Impacto	Brecha de datos que afectó a la información 1,3 millones de clientes incluyendo nombres completos, datos de contacto, direcciones, detalles de pedidos e IPs de inicio de sesión de los usuarios.
Mitigación	No han trascendido más detalles acerca de las medidas de mitigación concretas llevadas a cabo por la empresa.
Fuentes	bitdefender.com, bleepingcomputer.com

06 Ciberataque a Horsa Blue

Actor	Hunters International
Víctima	Empresa del grupo Horsa (grupo italiano especializado en soluciones TIC corporativas)
Países	Italia
Fecha	Noviembre de 2024
Descripción	Según declara el actor, fueron exfiltrados 57,3 GB de datos de la víctima.
Impacto	Brecha de datos que supuestamente incluía información financiera y datos de clientes. La propia empresa matriz ha desmentido la versión del atacante, aclarando que el incidente afectó exclusivamente a Horsa Blue, una pequeña compañía satélite que representa menos del 0,5 % de los activos del grupo y opera con sistemas completamente independientes.
Mitigación	La empresa matriz informa de que, gracias a la rápida intervención de sus expertos en seguridad, el ataque fue contenido rápidamente, adoptando medidas para evitar cualquier riesgo de contagio a otras empresas del grupo
Fuentes	x.com, horsa.com

07	Ciberataque a Ticketmaster
Actor	ShinyHunters
Víctima	Ticketmaster LLC, empresa estadounidense de venta y distribución de entradas
Países	Estados Unidos
Fecha	Mayo de 2024
Descripción	Ticketmaster sufrió una brecha de datos masiva que afectó a millones de usuarios. El actor malicioso ShinyHunters puso a la venta a cambio de 500.000 dólares una base de datos que, según sus afirmaciones, contenía 1,3 TB de datos pertenecientes a Ticketmaster. En el archivo se muestran datos personales confidenciales de 560 millones de usuarios incluidos datos parciales de medios de pago. Ticketmaster reconoció el incidente y poco tiempo después ShinyHunters valoró la información exfiltrada en 22.000 millones de dólares y exigió 8 millones de dólares a LiveNation, empresa matriz de Ticketmaster.
Impacto	1.3 TB de datos de información de clientes de Ticketmaster
Mitigación	No han trascendido más detalles acerca de las medidas de mitigación concretas llevadas a cabo por la empresa.
Fuentes	hackread.com, sec.gov, hackread.com

Recomendaciones

La mayoría de los ciberincidentes mencionados están provocados por *ransomware*. Este tipo de ataque está creciendo de forma exponencial debido a que es muy rentable para los ciberdelincuentes. A continuación, se muestra algunas referencias de interés:

- INCIBE ha publicado una guía denominada **Ransomware: una guía de aproximación para el empresario**. Se trata de una guía que pretende ayudar a evitar un grave incidente por *ransomware* mediante unas prácticas recomendaciones de ciberseguridad [3].
- También existen otros recursos como **entradas de blog**, de lectura más ágil, que pueden ayudar para tener una primera aproximación de cómo actuar en caso de un ataque de *ransomware* [4].

4. Ciberamenazas

El informe ENISA THREAT LANDSCAPE 2024 [5] identifica a los actores de amenazas de ciberseguridad más activos en el año 2024.

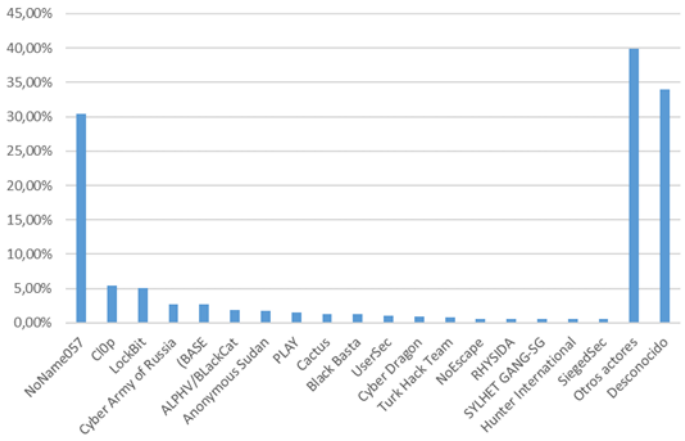


Ilustración 5: grupos con mayor actividad [ENISA]

Según este informe, la gran mayoría de los eventos recopilados no se atribuyeron a ningún actor de amenazas específico, lo que pone de relieve las dificultades asociadas con una atribución precisa. Por otra parte, el grupo *hacktivista* **NoName057** evidencia una alta actividad durante el período de estudio.

En los siguientes apartados se describen una serie de amenazas que han afectado al sector TIC durante 2024.

01 NoName057(16)

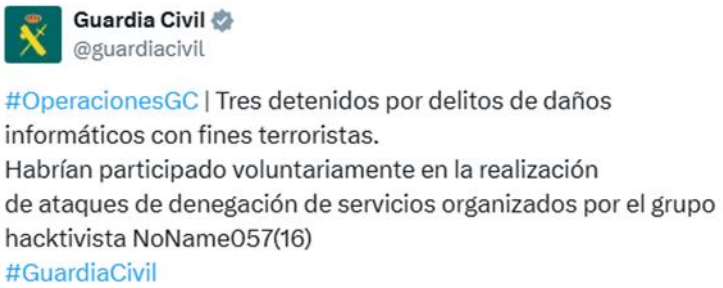


Ilustración 6: notificación de la Guardia Civil en x [@guardiacivil]

Grupo *hacktivista* surgido en marzo de 2022 cuyas actividades, principalmente ataques de denegación de servicio distribuido (DDoS), tienen un componente ideológico de carácter político antiucraniano, por lo que sus objetivos van más allá de la búsqueda del beneficio económico.

Aunque dirige sus ataques contra múltiples países europeos y pertenecientes a la OTAN, el país más atacado sería Ucrania, seguido de República Checa e Italia. Este actor habría llevado a cabo múltiples campañas contra España, el cuarto país más atacado por el grupo, con motivo de la detención de dos de sus presuntos miembros en España en julio de 2024, como represalia por el envío de ayuda o entrenamiento militar a Ucrania, o durante las elecciones generales de julio de 2023.

Con respecto al **sector TIC**, en 2024 llevó a cabo numerosos ataques contra entidades de dicho sector en diversos países europeos, incluyendo Polonia, Rumanía, Letonia, Bélgica y España, entre otros, siendo el actor con más ataques registrados al sector durante dicho periodo.

Entre las técnicas más relevantes a nivel de impacto empleadas por este actor, se encuentra la realización de ataques *DDoS*, *defacement* o *Endpoint Denial of Service*. Destaca la creación de un proyecto denominado DDosia, herramienta que da soporte para la organización y realización de ataques de DDoS de manera coordinada.

Fuentes: @guardiacivil, tgstat.com, tgstat.com, elconfidencial.com, sentinelone.com, INCIBE

02 RansomHub


JOINT CYBERSECURITY ADVISORY
TLP:CLEAR
MS-ISAC
#StopRansomware: RansomHub Ransomware
Summary

Ilustración 7: recomendaciones específicas contra RansomHub [CISA]

Este grupo surge en febrero de 2024 y se ha convertido rápidamente en una amenaza significativa, afectando a una amplia gama de sectores, incluyendo infraestructuras críticas y servicios gubernamentales.

RansomHub utiliza un modelo de doble extorsión: cifra datos y los exfiltra para exigir rescates. Las víctimas deben pagar no solo para recuperar el acceso a sus datos cifrados, sino también para evitar la divulgación pública de la información robada.

Emplea técnicas sofisticadas, como la explotación de vulnerabilidades de día cero como Zerologon y el uso de métodos avanzados de exfiltración de datos. Utiliza herramientas para escanear redes, mapear objetivos potenciales y evadir la detección.

RansomHub ha afectado a diversas industrias en todo el mundo, lo que pone de manifiesto la naturaleza indiscriminada y el amplio alcance de las amenazas modernas de *ransomware*.

Fuentes: cyble.com, CISA, INCIBE

03 Medusa

Ilustración 8: sitio web del ransomware Medusa [WeLiveSecurity]

Los actores que se encuentran detrás de este *ransomware* utilizan un modelo de doble extorsión reclamando una cuantiosa suma de dinero a cambio de descifrar la información bajo la amenaza de filtrar o vender los datos robados si la víctima se niega a pagar. A comienzos del año 2023, el grupo incrementa su actividad y crea el sitio web "Medusa Blog" en la red Tor, donde publican los datos de las organizaciones extorsionadas.

Este grupo criminal no tiene código ético y entre las víctimas se encuentran instituciones de todos los sectores críticos, incluido el sector TIC.

Fuentes: [ciberseguridad.euskadi.eus](), [welivesecurity.com]()

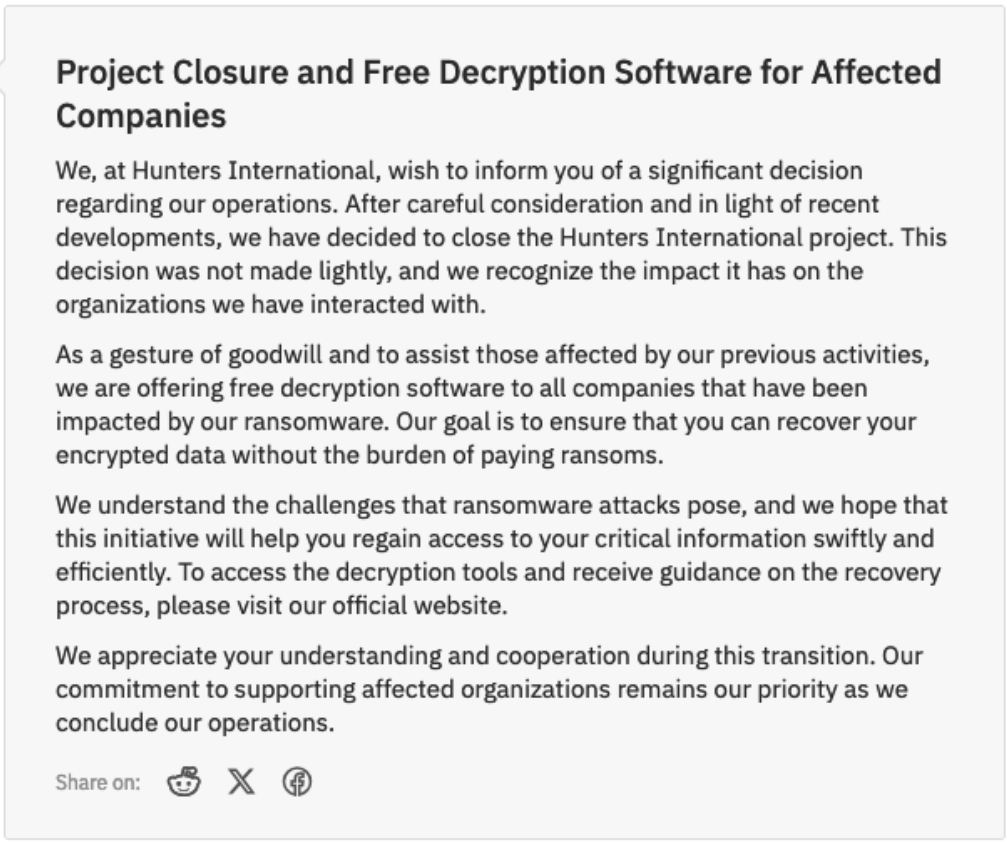
04 LockBit3

Ilustración 9: sitio web en Tor de LockBit clausurado por parte de fuerzas y cuerpos de seguridad [TrendMicro]

LockBit 3.0, también conocido como LockBit Black, es una variante del ransomware LockBit que lleva activa desde al menos julio de 2022. En febrero de 2024, una operación internacional liderada por la Agencia Nacional contra el Crimen del Reino Unido, en colaboración con el FBI y Europol, logró incautar 34 servidores asociados al grupo y tomar el control de su sitio web, interrumpiendo significativamente sus actividades. A pesar de estos esfuerzos, LockBit 3.0 ha continuado sus operaciones maliciosas, afectando a múltiples sectores y, en particular, al sector TIC.

Fuentes: trendmicro.com, INCIBE, INCIBE, INCIBE, INCIBE

05 Hunters



Project Closure and Free Decryption Software for Affected Companies

We, at Hunters International, wish to inform you of a significant decision regarding our operations. After careful consideration and in light of recent developments, we have decided to close the Hunters International project. This decision was not made lightly, and we recognize the impact it has on the organizations we have interacted with.

As a gesture of goodwill and to assist those affected by our previous activities, we are offering free decryption software to all companies that have been impacted by our ransomware. Our goal is to ensure that you can recover your encrypted data without the burden of paying ransoms.

We understand the challenges that ransomware attacks pose, and we hope that this initiative will help you regain access to your critical information swiftly and efficiently. To access the decryption tools and receive guidance on the recovery process, please visit our official website.

We appreciate your understanding and cooperation during this transition. Our commitment to supporting affected organizations remains our priority as we conclude our operations.

Share on:

Ilustración 10: anuncio de cierre del proyecto [Hunters International]

Hunters, también conocido como Hunters International, es un *Ransomware-as-a-Service* que lleva activo desde al menos 2023. Debido a que el código fuente del malware presenta un 60% de similitudes con una versión del ransomware Hive, se considera probable que sea una variante de este o que haya sido desarrollado por los operadores de Hive, aunque los actores maliciosos detrás de Hunters han negado cualquier relación con los desarrolladores de dicho malware.

Cabe destacar que el grupo ha anunciado en julio de 2025 el cese de su actividad, indicando que ofrecen software de descifrado de la información cifrada por su *ransomware* (información sin confirmar). Se desconoce la motivación real tras este anuncio de cierre, ya que otros grupos de este tipo han realizado movimientos similares en el pasado, para luego reanudar su actividad bajo otro nombre.

Fuentes: quorumcyber.com, techcrunch.com, INCIBE

06 Play

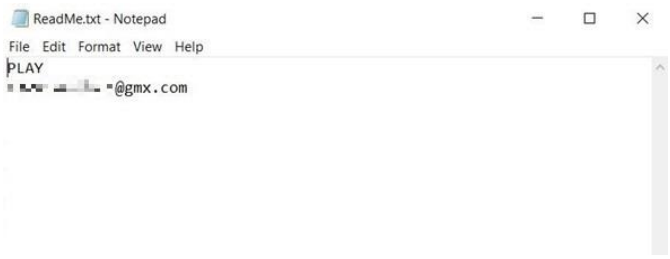


Ilustración 11: ejemplo de nota de rescate de Play [TrendMicro]

Grupo de *ransomware* que aplica la técnica de doble extorsión (cifrado y exposición de información), activo desde al menos junio de 2022. En noviembre de 2023 se detectó que estaba siendo vendido como *Ransomware-as-a-Service* (RaaS). Algunos investigadores afirman que las TTP (Tácticas, Técnicas y Procedimientos) de Play coincidirían con las de Hive y Nokoyawa, dos familias de *ransomware* vinculadas a la "Hive Gang". Asimismo, se ha establecido una relación entre Play y Quantum debido a la similitud entre la infraestructura utilizada.

Fuentes: adlumin.com, trendmicro.com

07 Cactus

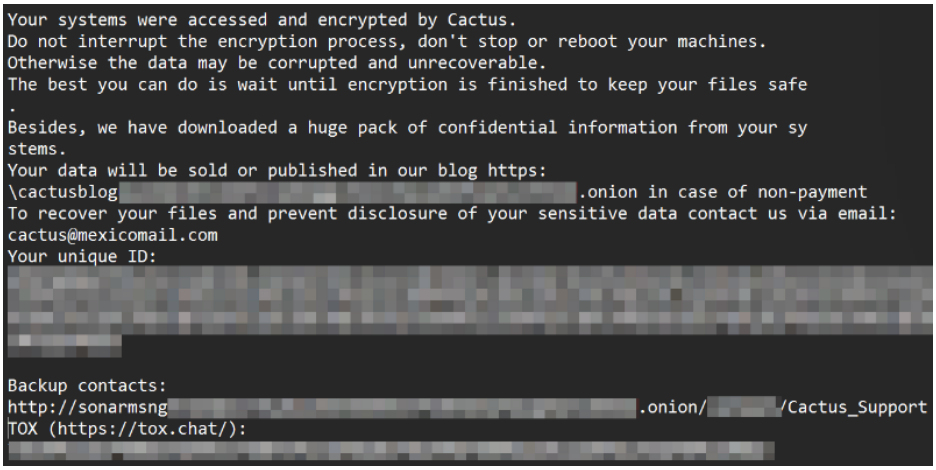


Ilustración 12: ejemplo de nota de rescate de Cactus [SOCRadar]

El grupo de *ransomware* Cactus fue detectado por primera vez en marzo de 2023. Actuando como *Ransomware-as-a-Service*, el grupo emplea la técnica de doble extorsión, cifrando los archivos de las víctimas y amenazando con publicarlos si no se efectúa el pago del rescate. Su motivación principal parece ser la obtención de ganancias económicas, dirigiendo sus ataques hacia múltiples sectores, especialmente el sector industrial.

Fuentes: socradar.io, INCIBE

08 Black Basta

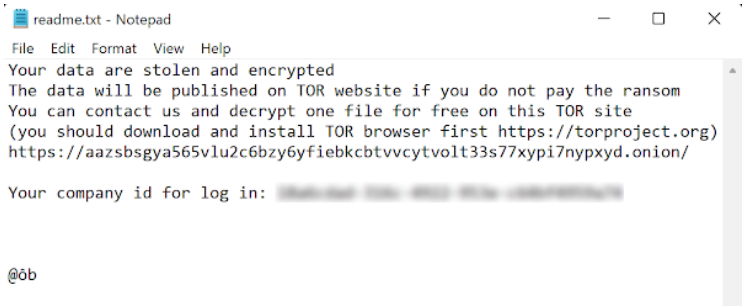


Ilustración 13: ejemplo de nota de rescate de Black Basta [INCIBE]

El grupo organizado de ciberdelincuentes conocido como Black Basta, nombre por el que se conoce también a su propio *ransomware*, emergió por primera vez en la primavera de 2022, operando bajo el modelo de *ransomware* como servicio (RaaS). Esta organización rápidamente se estableció como uno de los actores de amenaza más destacados en el ámbito del RaaS a nivel mundial.

Adoptó la táctica de la doble extorsión. Se observó que el grupo operaba mediante dos portales en la red Tor, uno dedicado a la difusión de información sustraída y otro para facilitar la comunicación con las víctimas.

Fuentes: CISA, INCIBE

09 NetForceZ

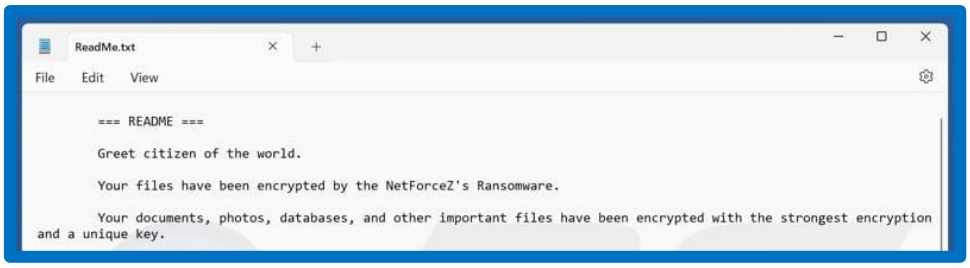


Ilustración 14: captura de pantalla del archivo de texto de NetForceZ [PcRisk]

Grupo hacktivista prorruso activo desde junio de 2024 que lleva a cabo ataques, iniciados por sí mismo o por otros grupos con la misma ideología, contra lo que considera aliados de Ucrania en el contexto de la guerra entre Ucrania y Rusia. Además, el actor de amenazas también ataca a Israel. Su principal actividad es la realización de ataques DDoS.

A finales de julio NetForceZ participó en una campaña de ataques contra activos españoles lanzada por el grupo prorruso NoName057 como respuesta a la detención de tres supuestos miembros de su equipo en España. Así, NetForceZ atacó páginas web de entidades como la Agencia Española de Meteorología, el Museo del Prado o los ministerios de Interior y Exteriores, además del ataque a la tienda en línea de Consum.

Por último, merece la pena destacar que NetForceZ anunció que buscaban un desarrollador de ransomware para colaborar, lo que sugiere un posible cambio en sus estrategias.

Fuentes: cybernews.com

10 Sabotajes a cables submarinos

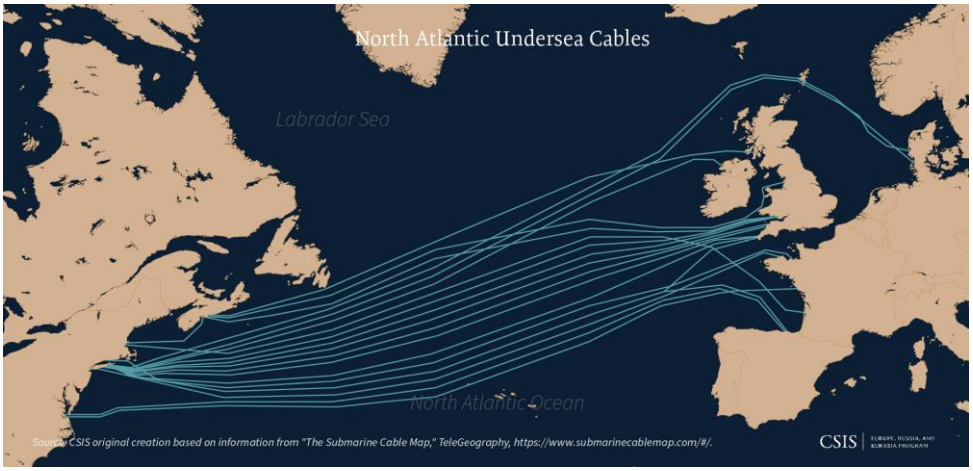


Ilustración 15: creación del CSIS basada en el mapa de cables submarinos de TeleGeography [Center for Strategic & International Studies]

Según Naciones Unidas, se registran entre 150 y 200 cortes de cables submarinos cada año. Dos tercios de estos incidentes son causados por accidentes (Pesca de arrastre, dragado, anclas, etc.), y el tercio restante es causado de forma deliberada. Al respecto, merece la pena mencionar que la relativa facilidad para cortar un cable submarino en proporción al daño efectivo, reputacional, operativo y económico es un factor que lo convierte en un tipo de ataque muy atractivo para actores de amenazas internacionales, pues, no en vano, los cables submarinos son los encargados de transportar en torno al 95% de los datos entre países, fluyendo a través de ellos los más de 9 billones de euros en transacciones financieras diarias. Actualmente, se tiene constancia de más de 600 cables submarinos entre los que están en servicio y los previstos.

Así, en 2024 se han producido diversos incidentes destacables relacionados con cables submarinos. En marzo de 2024, al menos cuatro cables submarinos en el Mar Rojo (Seacom, TGN, AAE-1 y EIG) resultaron cortados, afectando aproximadamente al 25% del tráfico mundial de Internet. Aunque las causas exactas no fueron esclarecidas, se sospechó de posibles ataques en medio de las tensiones regionales.

Los problemas en este tipo de infraestructuras persistieron en 2024, ya que el 18 de noviembre de 2024, se reportaron daños en dos cables submarinos de telecomunicaciones en el Mar Báltico: el BCS East-West Interlink entre Lituania y Suecia, y el C-Lion1 entre Finlandia y Alemania. Ambos incidentes ocurrieron casi simultáneamente y en proximidad geográfica, lo que llevó a sospechas de sabotaje. Las investigaciones se centraron en un buque de carga chino llamado Yi Peng 3 presente en la zona durante los incidentes. Aunque no se haya esclarecido el incidente de forma oficial, los investigadores sospechan que los marineros del Yi Peng 3 soltaron el ancla del barco a propósito para que ésta rompiera los citados cables submarinos. Según informó Wall Street Journal, la investigación trata de aclarar si el capitán del Yi Peng 3, que iba cargado de fertilizantes rusos y había zarpado del puerto ruso Ust-Luga, tomó la decisión de soltar el ancla inducido por agentes de la inteligencia rusa.

Fuentes: csis.org, internetsociety.org, elconfidencial.com, efe.com, wikipedia.org, wsj.com

11 Akira

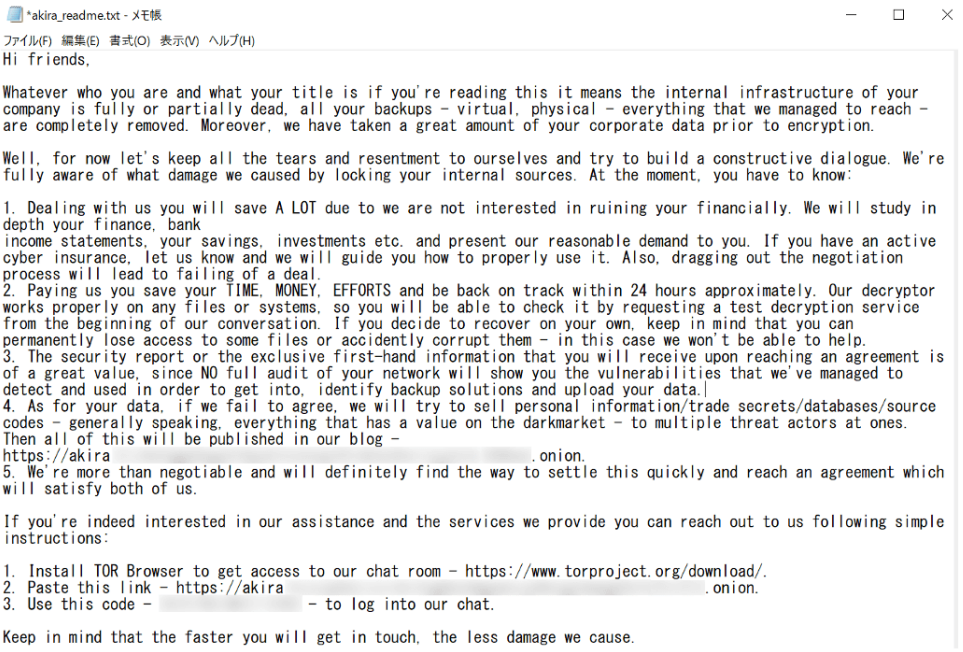


Ilustración 16: ejemplo de nota de rescate de AKIRA [FORTINET]

El grupo de ransomware Akira surgió en marzo de 2023 y presenta similitudes con las técnicas y el modus operandi de Conti, otro grupo de ransomware. Akira implementa la técnica de doble extorsión, encriptando los datos de la víctima y solicitando un pago de rescate, mientras amenaza con publicar o vender dicha información a través de su sitio web en la red Tor.

Fuentes: cisa.gov, socradar.io, INCIBE

12 Funksec

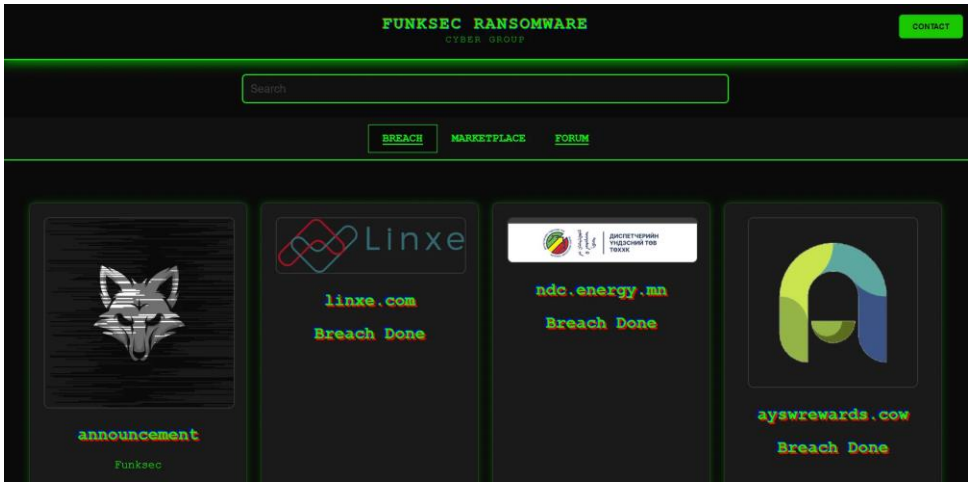


Ilustración 17: FunkSec Ransomware's DLS [SOCRadar]

Funksec es un grupo de ransomware que opera bajo el modelo Ransomware-as-a-Service (RaaS), conocido por emplear tácticas de doble y triple extorsión. Activo desde diciembre de 2024, Funksec ha sido vinculado con el grupo hacktivista GhostSec y su foro Darkzone, además de la posible participación de actores de origen brasileño y argelino, aunque su principal motivación declarada es financiera.

Fuentes: PortalERP

13 KillSecurity

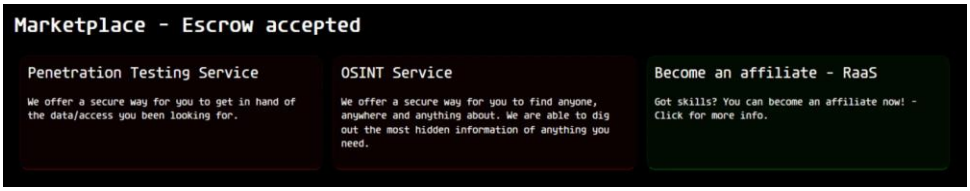


Ilustración 18: servicios ofrecidos por KillSec [SOCRadar]

KillSecurity, también conocido como KillSec, es un actor de amenazas que opera bajo un modelo de *ransomware as a service* (RaaS). Este grupo permite a sus afiliados ejecutar ataques utilizando su infraestructura de malware. Emplea métodos de extorsión directa y doble extorsión, donde no solo cifran los datos, sino que también amenazan con publicar la información robada si no se paga el rescate.

Fuentes: blackfog.com, watchguard.com

14 Ataques de LightBasin explotando el protocolo GPRS

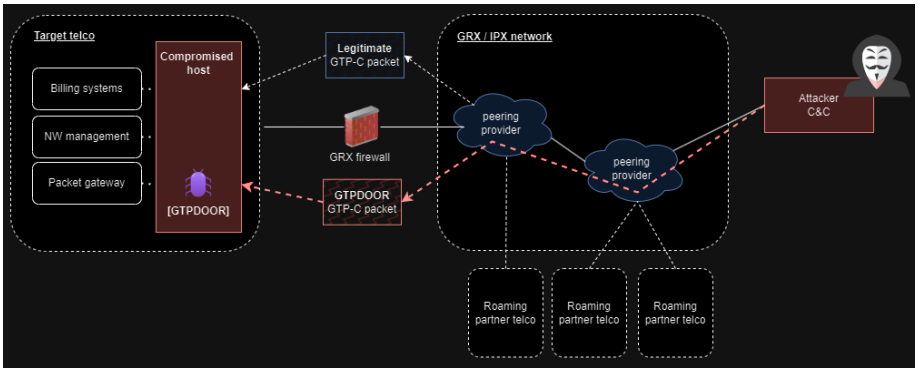


Ilustración 19: ataque GTPDOOR [doubleagent.net, haxrob.net]

GTPDOOR es un malware para Linux que tiene como objetivo las redes de telecomunicaciones que utilizan itinerancia GPRS, explotando el protocolo de túnel GPRS (GTP) para su comunicación con el servidor de comando y control (C2). Al ejecutarse, GTPDOOR cambia su nombre de proceso y abre un conector para recibir mensajes UDP. Además, permite que el actor amenaza se comunique con hosts comprometidos enviando mensajes maliciosos a través

de solicitudes GTP-C Echo; lo cual actúa como un conducto para ejecutar comandos en la máquina infectada. Asimismo, GTPDOOR puede ser sondeado desde una red externa, devolviendo información sobre la disponibilidad de puertos en el host infectado. Este malware parece dirigirse específicamente a hosts comprometidos que están conectados directamente a la red GRX, utilizada para la itinerancia entre operadores de telecomunicaciones.

Fuentes: haxrob.net

15 Campaña de UNC3886

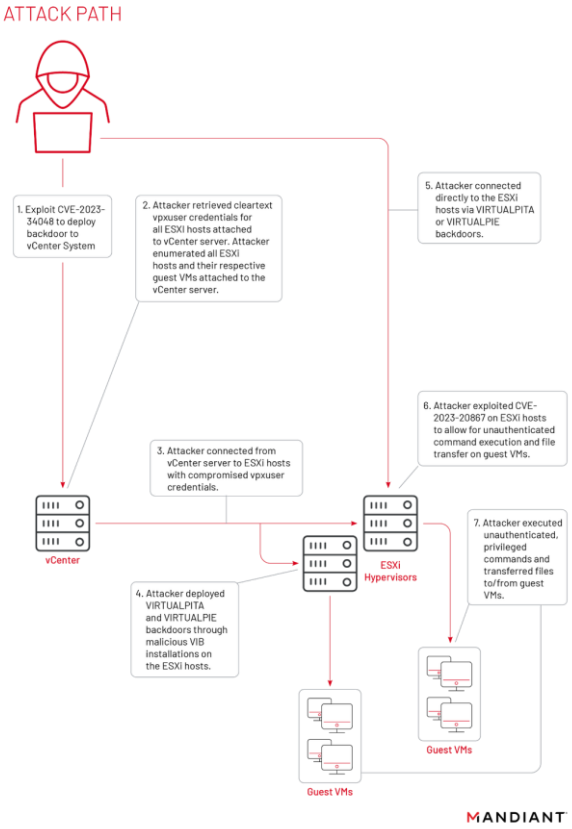


Ilustración 20: secuencia de ataques de UNC3886 [Mandiant]

El equipo de investigación de Mandiant reveló que UNC3886 ha estado explotando la vulnerabilidad CVE-2023-34048 (CVSSv3 9.8), desde finales de 2021, dirigiéndose principalmente a organizaciones en sectores como defensa, gobierno, telecomunicaciones y tecnología. UNC3886 aprovecha el fallo de seguridad para comprometer servidores vCenter, implementando puertas traseras en hosts ESXi. Luego, explotan CVE-2023-20867 (CVSSv3 3.9), una falla de omisión de autenticación de VMware Tools para escalar privilegios y extraer archivos de máquinas virtuales. Aunque la vulnerabilidad fue corregida en octubre de 2023, y a pesar de que no parece existir una PoC publica, los detalles técnicos están disponibles desde principios de diciembre de 2023. Además, VMware confirmó la explotación activa por parte del mencionado grupo de ciberespionaje.

Fuentes: cloud.google.com

5. Buenas prácticas y cumplimiento normativo

5.1. Buenas prácticas

En el sector TIC, la protección en materia de ciberseguridad se centra principalmente en los sistemas de tecnología de la información (IT), dado que las empresas de este sector proporcionan infraestructura, plataformas y servicios digitales esenciales para otras organizaciones. Estos sistemas incluyen servidores, centros de datos, servicios en la nube y soluciones de ciberseguridad gestionada, entre otros.

A diferencia de sectores industriales que dependen de la tecnología operativa (OT) para el control de procesos físicos, en el ámbito de los servicios TIC las buenas prácticas se focalizan en la seguridad de las infraestructuras IT.

En esta sección se mencionará por lo tanto el principal estándar internacional enfocado a la protección de los sistemas IT en una organización típica del sector TIC.

ISO/IEC 27001:2022. Gestión de la seguridad de la Información

Es una norma internacional que proporciona un marco general para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI). Es decir, un marco de este tipo ayuda a la implementación de los medios necesarios para mejorar la seguridad y reducir los riesgos de los sistemas de información de una organización.

En una empresa del sector TIC, la ciberseguridad ayuda a proteger la información crítica operativa y administrativa, como bases de datos con información de clientes, contratos y configuraciones de infraestructura digital. Asimismo, contribuye a la protección y reducción de la exposición ante amenazas en los sistemas IT, incluyendo servidores, redes, plataformas en la nube y software empresarial.

Además de esta certificación, se han establecido extensiones de la norma que han ayudado a completar con mayor nivel de detalle lo establecido en ella. Por ejemplo:

- **ISO/IEC 27701:2021. Sistema de Gestión de Información de Privacidad**.
- **ISO/IEC 27017:2015. Seguridad para servicios en Nube**.

Dichas extensiones cubren aspectos que no se tuvieron en cuenta en la definición de la 27001. Una vez que se cumple esta, obtener estas nuevas certificaciones no supone grandes cambios en la operativa de una organización.

5.2. Cumplimiento normativo

En esta sección se documentan las principales normativas y estándares, tanto nacionales como internacionales, que establecen las directrices fundamentales para mitigar riesgos y proteger los activos digitales de las empresas del sector TIC.

- **Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas**. Esta normativa reconoce el papel fundamental de algunos tipos de organizaciones en la sociedad actual, refiriéndose a entidades que, de quedar comprometidas por un ciberataque, pueden poner en peligro la vida de ciudadanos, tener graves consecuencias en la seguridad nacional o tener un impacto importante en la economía y en la sociedad.

- **Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.** Transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, y tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes y un marco institucional para la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario.
- **Real Decreto 43/2021**. Desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información desarrolla esta disposición y define, entre otras cuestiones, la cooperación y coordinación de los CSIRT de referencia: CCN-CERT, MCCE e INCIBE-CERT, así como las tareas y apoyo de los CSIRT de referencia a los operadores críticos, operadores de servicios esenciales, proveedores de servicios digitales, las autoridades competentes, la Oficina de Coordinación de Ciberseguridad, entre otros.
- **Directiva (UE) 2022/2555, de 14 de diciembre de 2022 (Directiva NIS2)**. Actualizará y derogará la Directiva (UE) 2016/1148 del 6 de julio de 2016, conocida como Directiva NIS1. Propone seguir mejorando el trabajo iniciado en la Directiva NIS para crear un alto nivel común de ciberseguridad en toda la Unión Europea, imponiendo obligaciones a los Estados miembros y a las entidades públicas y privadas de sectores críticos. Entre los sujetos obligados están las entidades del sector TIC. El 14/02/2025 el anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad fue aprobado por el Consejo de Ministros [6].
- **Reglamento de Ejecución (UE) 2024/2690**

  Directamente relacionado con NIS2 está el Reglamento de Ejecución (UE) 2024/2690 de la Comisión Europea, adoptado el 17 de octubre de 2024. Este reglamento establece las disposiciones de aplicación de NIS2, especificando los requisitos técnicos y metodológicos para la gestión de riesgos de ciberseguridad. En particular, el reglamento detalla los criterios para determinar cuándo un incidente de ciberseguridad se considera significativo y debe ser reportado a las autoridades. Esto incluye a proveedores de servicios como DNS, computación en la nube, centros de datos, plataformas de redes sociales, los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados, entre otros [7].
- **Reglamento General de Protección de Datos**. Normativa de la Unión Europea, adoptada en 2016 y aplicable desde el 25 de mayo de 2018 donde su objetivo es regular la protección de los datos personales de los ciudadanos de todos los Estados miembros pertenecientes. El reglamento se aplica a cualquier organización, dentro o fuera de la Unión Europea, que procese datos personales de ciudadanos residentes. En España, la Agencia Española de Protección de Datos (AEPD) es el organismo encargado de garantizar el cumplimiento de la GDPR a nivel nacional. La AEPD proporciona directrices, resuelve consultas legales y técnicas, y gestiona las denuncias relacionadas con posibles incumplimientos. Además, es responsable de imponer sanciones en caso de infracciones.

- **ENS (Esquema Nacional de Seguridad).** El ENS, regulado a través del Real Decreto 311/2022, de 3 de mayo, sustituye a la normativa anterior, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- ***Cyber Resilience Act* (CRA).** Tiene como objetivo proteger a los consumidores y las empresas que compran productos de software o hardware con un componente digital.

Recomendaciones

INCIBE, como organismo de referencia en materia de ciberseguridad, ofrece en su portal web multitud de recursos orientados a elevar el nivel de ciberseguridad de las entidades e infraestructuras del sector TIC.

6. Tendencias de ciberseguridad

El sector TIC se enfrenta un panorama de ciberseguridad cada vez más complejo. En este contexto, se presentan a continuación una serie de tendencias en relación a las principales vulnerabilidades, ciberincidentes, ciberamenazas, buenas prácticas y cumplimiento normativo que afectan al sector TIC.

Vulnerabilidades

El año 2024 finalizó con 40.009 CVE publicados, un aumento de más del 38% respecto de los 28.818 CVE publicados en 2023.

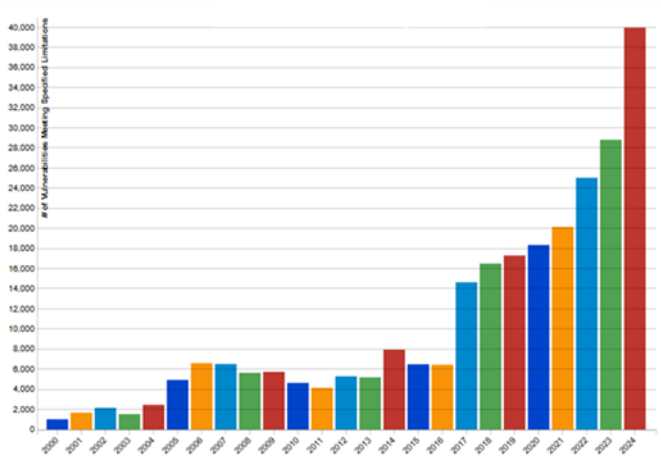


Ilustración 21: evolución temporal del número de CVE publicados anualmente [NVD]

Todo parece indicar que la tendencia, lejos de retroceder, seguirá en aumento. Algunos de los motivos son los que se indican a continuación:

- El crecimiento sostenido del sector TIC, tanto a nivel nacional como internacional, hace que cada vez haya más productos y servicios IT, lo cual incrementa la superficie de exposición y, por lo tanto, la probabilidad de aparición de nuevas vulnerabilidades en los mismos.
- Cada vez se invierten más recursos y hay más concienciación en materia de ciberseguridad, siendo los propios fabricantes e investigadores de ciberseguridad los que trabajan, de forma cada vez más frecuente, en la publicación responsable de vulnerabilidades y en la actualización de sus productos para corregir problemas de seguridad.
    - La aplicación de nuevas regulaciones como la Directiva NIS2 (artículo 12) favorece la divulgación coordinada de las vulnerabilidades.
    - INCIBE, como CNA (Autoridad de Numeración de CVE), ha publicado en su página web aproximadamente el doble de vulnerabilidades en 2024 que en 2023.
- Además, la dependencia de proveedores externos para servicios y tecnologías esenciales introduce riesgos adicionales debido a que las **vulnerabilidades en la cadena de suministro** pueden ser explotadas para infiltrarse en las redes de las organizaciones, subrayando la necesidad de una gestión rigurosa de terceros colaboradores.

Ciberincidentes

El análisis de ciberincidentes recientes revela patrones relevantes en el sector TIC. La previsión en este sentido se basará en lo siguiente:

- **Ciberataques de *ransomware* y DDoS** guiados bien por motivos económicos (como es el caso de *ransomware*) o por causas ideológicas (como son los ataques *hacktivistas* de tipo DDoS, *defacement*, etc.).
- Por otro lado, las **campañas de *phishing*** personalizadas y dirigidas seguirán aumentando en sofisticación, especialmente ante la creciente democratización en el uso de las nuevas tecnologías y herramientas de inteligencia artificial.
- Adicionalmente, debido a su papel transversal y a las actuales tensiones geopolíticas, el sector TIC debería aumentar su vigilancia ante posibles **ciberataques que puedan llevar a cabo otras naciones**.

Por último, teniendo en cuenta las consultas recibidas durante el 2024 en la Línea de Ayuda de INCIBE (98.546), todo parece indicar que las empresas, en general, seguirán estando preocupadas por la suplantación de identidad, *phishing* y fraude del tipo *Business Email Compromise* (*BEC*).

Ilustración 22: consultas de empresas en el servicio de la Línea de Ayuda [INCIBE]

Sobre esta fuente de información, es importante destacar que el 46% de dichas consultas se hicieron cuando ya se había materializado el ciberincidente.

Ciberamenazas

El sector TIC, al tratarse de un sector transversal que provee de servicios y tecnologías a otros sectores, ha sido históricamente más afectado por ciberamenazas que otros sectores críticos. Por ello, su importancia estratégica y su elevada superficie de exposición lo convierte en un objetivo clave.

La previsión en este aspecto se prevé que sea la siguiente:

- La combinación del ***ransomware*** con la **doble extorsión**, donde además de cifrar los datos se amenaza con su divulgación, incrementará aún más la presión sobre las organizaciones afectadas.
- **Filtración de datos en foros** clandestinos. Se prevé un aumento en los intentos de intrusión con el objetivo de robar información sensible de las organizaciones.
- Además, los **ataques de denegación de servicio distribuido (DDoS)** experimentarán un aumentado en frecuencia y sofisticación.

Buenas prácticas y cumplimiento normativo

El cumplimiento de regulaciones nacionales e internacionales, como la Directiva NIS2 en Europa, promoverá que las empresas del sector sigan estándares robustos de seguridad.

A fecha de elaboración del presente informe, según el portal de ECSO (*NIS2 Directive Transposition Tracker*), son 14 los estados miembros que ya han traspuesto la Directiva NIS2 a su ordenamiento jurídico nacional.

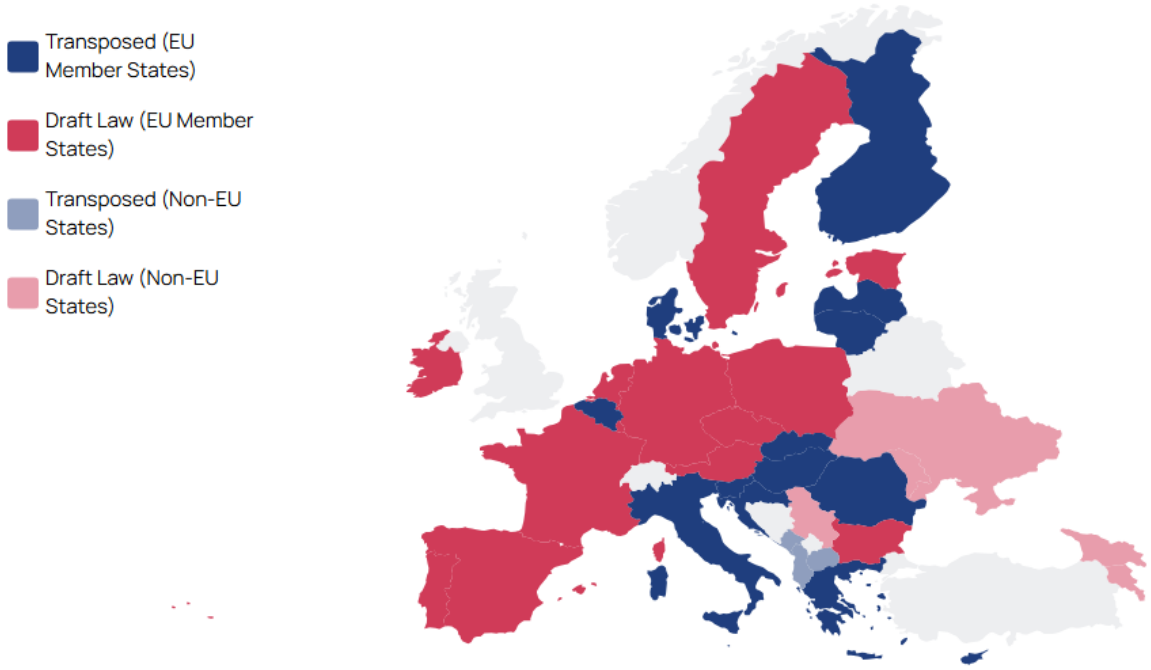


Ilustración 23: seguimiento de la transposición de la directiva NIS2 [ENISA]

Glosario

APT	Amenaza avanzada persistente. Consiste en un tipo de ataque informático que se caracteriza por realizarse con sigilo, permaneciendo activo y oculto durante mucho tiempo, utilizando diferentes formas de ataque. Suelen estar patrocinados por compañías, mafias o estados.
DDoS	Denegación de servicio distribuida. Es una denegación de servicio, solo que las peticiones se hacen desde diversos orígenes, de esta forma es más efectivo y complicado de detener, así como determinar su origen.
Defacement	Tipo de ataque contra un sitio web en el que se modifica la apariencia visual de una página web. Normalmente son producidos por ciberdelincuentes que obtuvieron algún tipo de acceso a la página, bien por algún error de programación de la página, algún bug en el propio servidor o una mala administración por parte de los gestores de la web.
Firewall	Cortafuegos. Sistema de seguridad compuesto o bien de programas (software), o de dispositivos hardware, situados en los puntos limítrofes de una red. Tiene como objetivo permitir y limitar el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red interna e Internet se realicen conforme a las políticas de seguridad de una organización. Estos sistemas suelen poseer características de privacidad y autentificación.
ISAC	Los ISAC son asociaciones público-privadas expuestas a vulnerabilidades y amenazas de ciberseguridad similares y suelen estar formadas por iniciativa del sector privado, en particular operadores de servicios esenciales de los sectores críticos. Los ISAC recopilan, analizan y difunden información procesable sobre amenazas a sus miembros y les brindan herramientas para mitigar los riesgos y mejorar la resiliencia en el sector correspondiente.
Ransomware	Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene, de tal forma que, si la víctima no paga el rescate, no podrá acceder a ella.
VPN	Una red privada virtual, también conocida por sus siglas VPN (*Virtual Private Network*), es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada, como por ejemplo Internet. De esta manera la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Se trata realmente de una conexión virtual punto a punto entre dos redes LAN, usando para la conexión una red pública como Internet, de tal forma que conexión se mantiene segura gracias al cifrado de la comunicación.

Nota: INCIBE dispone en su web de un completo glosario de términos de ciberseguridad.

Bibliografía

[1] INCIBE, «Sitio web de ES-ISAC TIC» [En línea]. Disponible: https://www.incibe.es/incibe-cert/sectores-estrategicos/ES-ISAC/TIC.

[2] INCIBE, «Balance de ciberseguridad 2024» [En línea]. Disponible: https://www.incibe.es/sites/default/files/Comunicaci%C3%B3n_2025/Infograf%C3%ADa_BalanceCiberseguridad_INCIBE_2024_web.pdf.

[3] INCIBE, «Ransomware: una guía de aproximación para el empresario» [En línea]. Disponible: https://www.incibe.es/empresas/guias/ransomware-guia-aproximacion-el-empresario.

[4] INCIBE, «Cómo actuar en caso de un ataque de ransomware» [En línea]. Disponible: https://www.incibe.es/ciudadania/ayuda/ransomware.

[5] ENISA, «ENISA THREAT LANDSCAPE 2024» [En línea]. Disponible: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[6] «Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad» [En línea]. Disponible: https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf.

[7] «Reglamento de Ejecución (UE) 2024/2690» [En línea]. Disponible: https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81540.


incibe_
ES-ISAC TIC