BeDisruptive™

It's an attitude

Evaluación de ciberamenazas en el panorama español

La primera mitad de 2023 ha traído consigo algunas de las tendencias que caracterizaron al 2022 y ha incorporado nuevas variables que han modificado el comportamiento de los atacantes y, por ende, el panorama de amenazas al que se enfrentan las empresas.

Tendencias emergentes

ChatGPT y sus variantes

La disrupción de 2023 es, sin duda alguna, la democratización de la inteligencia artificial desde la publicación de ChatGPT. Si bien el lanzamiento se produjo en diciembre de 2022, en el año 2023 los defensores y delincuentes están rentabilizando este recurso en su propio beneficio.

En la primera mitad de este año, se han puesto a prueba los límites y la seguridad de este nuevo recurso tecnológico y, además, se han creado versiones especializadas de ChatGPT para atacantes, como WormGPT, entre otros.

Esta nueva herramienta aumenta la eficiencia del uso de recursos de ciberseguridad, por lo que de nuevo se incrementa el nivel de exigencia y rapidez de las dinámicas de ataque y defensa.

Tendencias crecientes

MS SQL

Los ataques a los servidores MS SQL son una amenaza creciente para las organizaciones.
Se ha observado una marcada tendencia al alza en la detección de ataques dirigidos hacia sistemas MS SQL, que cada vez son más sofisticados y se detectan con mayor frecuencia.

En referencia a este tipo de ataque, se conoce que los intentos de ataque mediante RDP (Remote Desktop Protocol) y SQL (Structured Query Language) son los más comunes, mientras que los ataques a SMB (Server Message Block) durante 2022 y 2023 no han experimentado apenas detecciones.

Tendencias crecientes

Cambios en la entrega del *malware*

Hasta 2022, las macros de archivos Word o Excel adjuntos eran un método de infección muy efectivo. La víctima abría el documento y al habilitar la macro se infectaba con el *malware* correspondiente. Sin embargo, a mediados de 2022 Microsoft atajó ese problema, bloqueando de manera predeterminada las macros en archivos obtenidos desde Internet.

La respuesta criminal a esta limitación es la diversificación de la entrega del *malware* de dos formas principalmente:

Mediante archivos OneNote adjuntos

OneNote permite adjuntar archivos en sus blocs de notas y los delincuentes han aprovechado para mantener el *modus operandi* de adjuntar documentos maliciosos en los casos de *phishing*, cambiando únicamente el tipo de archivo adjunto.

Se conoce que los delincuentes han tratado de sustituir las macros por ficheros OneNote, por ello, se ha percibido una gran tendencia al respecto, habiendo detectado alrededor de 90.000 casos.

En febrero y a finales de marzo de 2023, se observó un mayor uso de esta plataforma bajo el contexto expresado previamente, siendo utilizado sobre todo por algunas de las siguientes amenazas:

- Emotet
- Qbot
- Redline Stealer
- Formbook
- AsyncRAT

Se han visto afectadas muchas extensiones, siendo algunas de estas las más relevantes:

- .asp
- .aspx
- .bat
- .com
- .iso

Mediante la distribución de *malware* por aplicaciones de mensajería

Algunas de las aplicaciones más utilizadas, como Discord o Telegram, están siendo usadas para distribuir *malware* de forma activa. Si bien esta tendencia no es actual y ya se llevaba a cabo anteriormente, la deshabilitación de las macros ha intensificado el uso de este recurso.

Tendencias crecientes

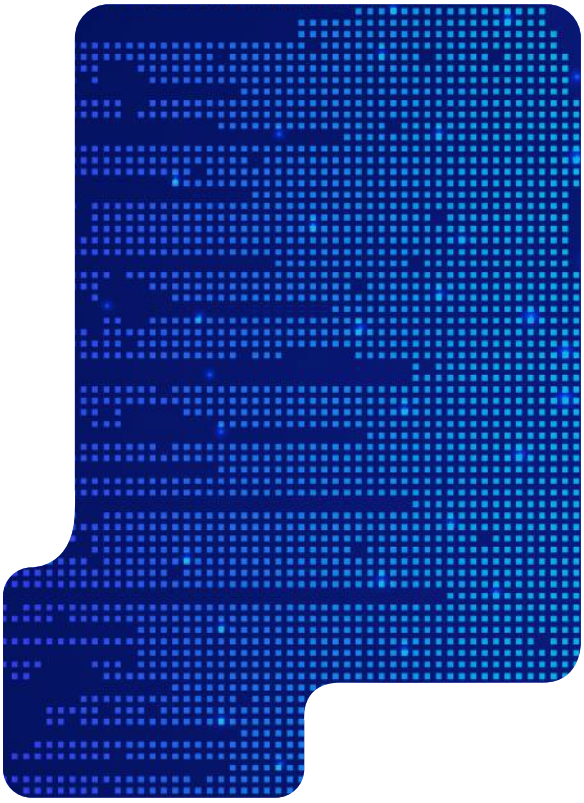
Nuevos dominios de Google y Log4Shell

Google

En el mes de mayo, Google lanzó ocho dominios TLP (Top Level Domains) nuevos.

Entre los dominios nuevos se encuentran dos que han preocupado especialmente a la comunidad de la seguridad informática: el .zip y el .mov.

Ambos dominios podrían confundirse con extensiones de archivos comprimidos o de vídeo y esta confusión puede ser aprovechada por los delincuentes para la propagación de *malware*.



Log4Shell

En correspondencia con Log4Shell (vulnerabilidad también conocida como CVE-2021-44228, que permite a los atacantes ejecutar código arbitrario en un sistema vulnerable mediante el envío de un mensaje especialmente diseñado a una aplicación que usa Log4j) y su uso en España, se ha observado una tendencia en las detecciones de estos ataques.

Conforme a los datos de ESET en el informe de Spain Threat Report H1 2023, el mayor aumento de explotación de esta vulnerabilidad fue en abril de 2023, lo que, en comparación con finales de 2022, supuso una diferencia de 10 millares de ataques.

Tendencias crecientes

Web *spoofing* y *Deepfakes*

En el vertiginoso mundo de la tecnología, donde la información fluye por la web, se conocen unas tendencias preocupantes que desafían la autenticidad de lo que se ve y se experimenta.

Es por ello, por lo que el web *spoofing* (suplantación de páginas web) y *deepfakes* (técnica de inteligencia artificial que falsifica contenido audiovisual) han aumentado. Haciendo alusión a los *deepfakes*, se conoce que la mayor tendencia es hacia perfiles públicos de gran repercusión social, mientras que el web *spoofing* tiene como mayor finalidad el robo de cuentas, ya sean de perfiles públicos o no.

Tendencias estables

Guerra, *hacktivismo* y *takedowns*

En febrero de 2023 fue el primer aniversario de la guerra en Ucrania. Su impacto en ciberseguridad salpica al panorama de amenazas a nivel global.

Los impactos más notorios son:

Aumento en la creación de nuevo *malware*.

Intensificación en el uso de *malware* de tipo *wiper*.

Mayor agresividad por parte de actores maliciosos apoyados por Rusia.

Despliegue de nuevas técnicas de desinformación a nivel nacional e internacional por parte del gobierno ruso.

Aumento de la actividad *hacktivista* y de las alianzas entre ellas.

Incremento de ciberataques a entidades gubernamentales.

Además, los actores maliciosos se han visto afectados en la primera mitad de 2023 por los *takedowns* de *markets* o recursos de ciberdelincuencia significativos, tales como Hive, Genesis y Chip Mixer.

Tendencias estables

Ataques a la cadena de suministro

Cada vez es más importante que las empresas protejan sus sistemas, no solo por su propia reputación, sino también por la seguridad de sus clientes.

Desde 2018 ha habido un aumento constante de ataques de cadena de suministro y 2023 no ha sido la excepción. Un ejemplo de ello es el ataque de Lazarus, un grupo de cibercrimen norcoreano, a la empresa de *software* 3CX en marzo.

Este primer ataque se debió originalmente a otro ataque de cadena de suministro, mediante la aplicación X_TRADER que estaba desactualizada y en desuso.

Las mayores consecuencias de estos ataques son también a nivel económico, puesto que se producen interrupciones en la producción y en la distribución.

Unido a la pérdida de datos y los costes de recuperación, estos ataques hacen, sin duda, un gran daño a las organizaciones.

Tendencias estables

Detección de *emails* maliciosos

Los ataques mediante correo electrónico son una de las amenazas más comunes en la seguridad de la información.

Cada año se envían miles de millones de *emails* maliciosos que logran evadir las defensas de las organizaciones.

Debido a una serie de factores, como el desarrollo de nuevos sistemas de detección, la cooperación entre organizaciones y Gobiernos y la concienciación de los usuarios genera una tendencia estable.

En enero de 2023, se detectó un descenso considerable en el uso de esta técnica.

En cambio, se ha visto una evolución conforme pasaba el tiempo y que constata el aumento de envío de *emails* maliciosos con ficheros adjuntos de extensiones tales como .vba, .zip y .iso, siendo estos los que más veces han sido bloqueados. Durante el resto del año, estas detecciones han evolucionado de forma creciente y se mantienen estables hoy en día.

Primer semestre de 2023 en España

La ciberseguridad en España ha sido víctima de numerosos ataques, siendo la región norte y, en concreto, el País Vasco, la zona que más ataques de *ransomware* ha sufrido, sobre todo en el sector público. Más de 100 ayuntamientos que dependían de la BiscayTIK se infectaron con *ransomware*.

LockBit es, sin duda, el actor de *ransomware* con mayor presencia en los ataques registrados.

Además de LockBit, en España se han identificado ataques de todos los grupos de *ransomware* activos, como en el caso del grupo RansomHouse que atacó el Hospital Clínic de Barcelona.

Asimismo, los periodos de mayor tendencia en referencia al *ransomware* durante 2023 se han producido en enero y principios de febrero, principios de abril y principios de mayo de 2023.

Win/Filecoder.STOP Trojan ha sido la amenaza de este tipo más detectada por ESET.

Este troyano cuenta con el 15,8% del total de familias de *ransomware* más utilizadas en el periodo de tiempo que comprende desde diciembre de 2022 hasta mayo de 2023.

Además de los ataques de *ransomware*, se han registrado 34 acciones cuya motivación era interrumpir los servicios de sus víctimas. El 79% de las interrupciones registradas corresponden a ataques de denegación de servicio, DDoS.

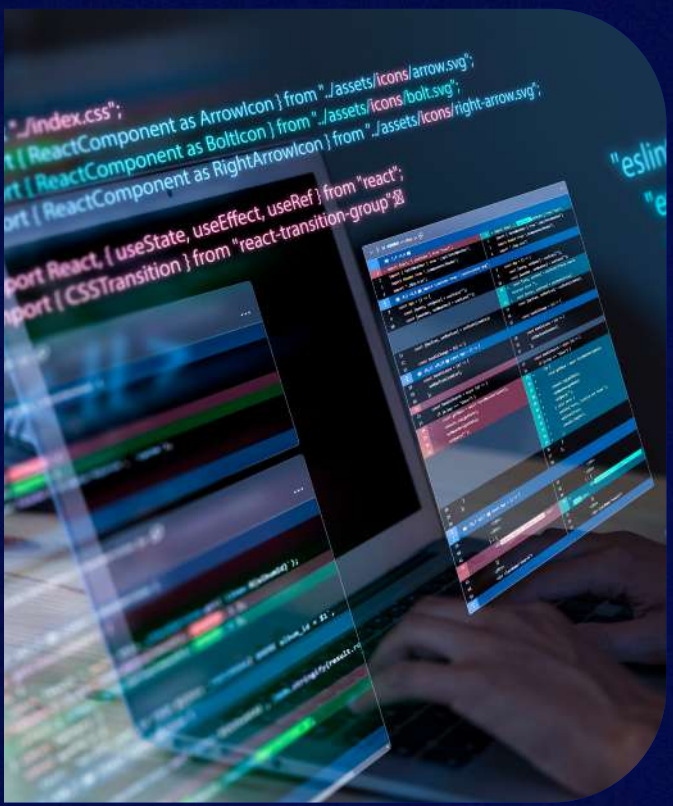
La mayoría de las víctimas pertenece al sector público, 11 de los 34 ataques fueron contra instituciones públicas, lo que representa un 32% de los ataques. El resto de los sectores con mayor número de ataques son del sector manufacturero y de servicios profesionales o del ámbito científico.

NoName057(16)

El actor de la amenaza destacado en este ámbito es NoName057(16). NoName057 es un grupo *hacktivista* prorruso observado por primera vez en marzo de 2022 y que opera desde esa fecha.

Este actor está claramente vinculado al conflicto entre Rusia y Ucrania. En su manifiesto afirman que sus acciones son una respuesta a quienes han adoptado una postura abiertamente hostil hacia Rusia, y tienen la fuerza y la experiencia necesarias para restablecer la justicia.

El grupo también señala que no trabaja para obtener beneficios económicos y que está dispuesto a cooperar con grupos de ideas afines.



El Gobierno de España se ha visto afectado por este actor, siendo el ataque más reciente al Ministerio del Interior el 23 de Julio de 2023, fecha en que se celebraron las elecciones generales.

También se han visto afectadas en diversas ocasiones mediante ataques DDoS las páginas web del Tribunal Constitucional, La Casa Real e, incluso, los Ministerios de Justicia y Política Territorial, entre otros.

A su vez, se ha percibido que las campañas de Emotet han recibido un fuerte golpe. Se utiliza un 94% menos que en el H2 de 2022, cuando se marcó una tendencia al alza muy importante de su uso en junio, julio y noviembre de dicho año.

Top 10 de detecciones de ciberamenazas en España

Fuente: Spain Threat Report H1 2023 - ESET

Referente a las detecciones globales, se ha distinguido el troyano HTML/Phishing.Agent con un 27,1% a nivel mundial, mientras que en España ha sido detectado un 25,4%, posicionándose como número uno en detecciones en ambos casos.

Durante 2023, ha disminuido la detección de amenazas, concretamente en enero y abril, siendo los meses con menos detecciones entre 2022 y 2023.

Posibles escenarios para el próximo semestre

El panorama global de amenazas ha evolucionado rápidamente en los últimos seis meses, con ataques cibernéticos que crecen en escala, complejidad e impacto.

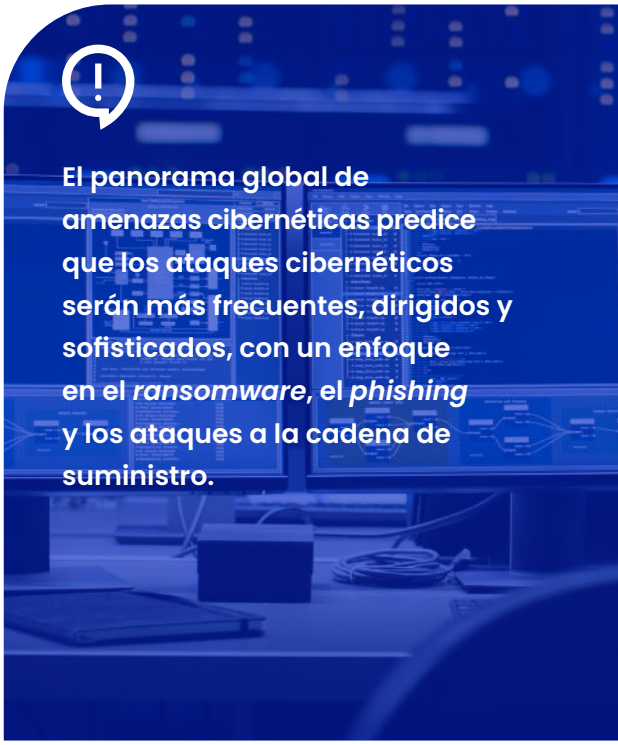
Las organizaciones deben priorizar las medidas de seguridad cibernética, incluidas las evaluaciones de seguridad periódicas, el intercambio de inteligencia sobre amenazas, la capacitación para la concienciación de los empleados y las estrategias de defensa proactiva para mitigar los riesgos asociados con las amenazas emergentes.

La colaboración entre los sectores público y privado, junto con la cooperación internacional, es crucial para combatir el panorama de amenazas globales cada vez más sofisticado.

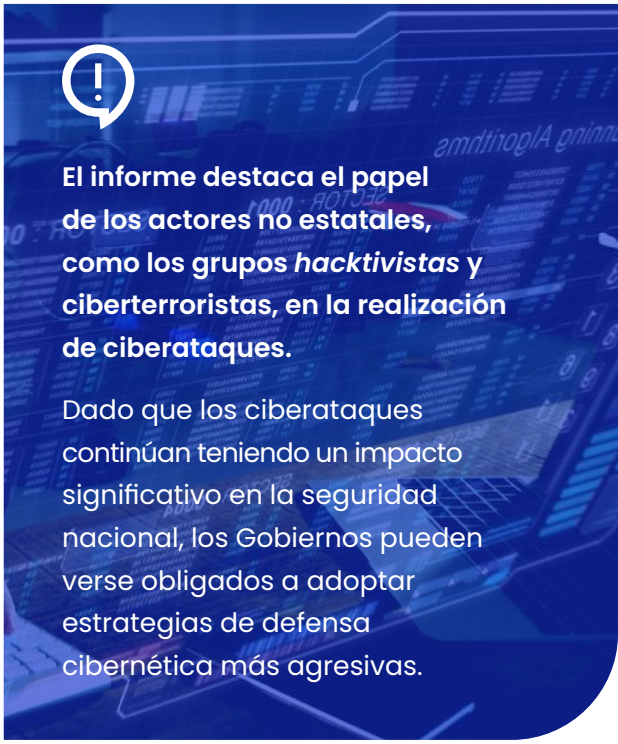
El informe advierte que estos ataques pueden causar interrupciones significativas en la infraestructura crítica, los sistemas financieros, la atención médica y otros servicios esenciales.

Tecnologías como las redes 5G y el Internet de las cosas (IoT) también brindan nuevas superficies de ataque y oportunidades para los ciberdelincuentes.

Una de las principales amenazas descrita en el informe son los ataques cibernéticos patrocinados por el Estado: países como China, Rusia, Irán y Corea del Norte continúan representando una grave amenaza para la ciberseguridad global.



El panorama global de amenazas cibernéticas predice que los ataques cibernéticos serán más frecuentes, dirigidos y sofisticados, con un enfoque en el *ransomware*, el *phishing* y los ataques a la cadena de suministro.



El informe destaca el papel de los actores no estatales, como los grupos *hacktivistas* y ciberterroristas, en la realización de ciberataques.

Dado que los ciberataques continúan teniendo un impacto significativo en la seguridad nacional, los Gobiernos pueden verse obligados a adoptar estrategias de defensa cibernética más agresivas.

Se espera que los ataques cibernéticos se vuelvan más complejos y que los atacantes dependan cada vez más de herramientas y técnicas avanzadas como la inteligencia artificial y el aprendizaje automático.

Los Gobiernos, las empresas y las personas deben permanecer alerta y tomar medidas proactivas para proteger sus sistemas frente a estas amenazas. Además, las partes interesadas en la industria de la ciberseguridad deben continuar invirtiendo en investigación y desarrollo para adelantarse a los ciberdelincuentes.

Dada la evolución de la seguridad cibernética y las tendencias mencionadas en el reporte, se evalúan algunos potenciales escenarios para el panorama de amenazas cibernéticas en los próximos meses:

Mayor frecuencia y sofisticación

Es probable que los ciberataques continúen aumentando en frecuencia, sofisticación y gravedad. Los actores de amenazas aprovecharán las herramientas y técnicas avanzadas, incluida la inteligencia artificial y el aprendizaje automático, para lanzar ataques más específicos y complejos.

Ransomware

Los ataques de *ransomware* seguirán siendo una amenaza importante. Los ciberdelincuentes continuarán apuntando a organizaciones en varios sectores, incluidas las infraestructuras críticas, la atención médica, las finanzas y el gobierno.

El impacto de estos ataques podría provocar importantes interrupciones, pérdidas financieras y, en los casos más peligrosos, fenómenos de injerencia política y procesos de desestabilización en las políticas de los Estados, para influenciar el proceso de toma de decisiones y la seguridad nacional de los mismos.

Ataques a la cadena de suministro

Esta tipología de ataque seguirá siendo un vector de amenaza prominente. Los ciberdelincuentes pueden explotar las vulnerabilidades en las cadenas de suministro de las organizaciones, comprometiendo el *software*, el *hardware* o los servicios para obtener acceso no autorizado o distribuir cargas maliciosas.

Phishing e ingeniería social

Los ataques de *phishing* persistirán como método favorito para obtener acceso no autorizado y recopilar información confidencial. Los ciberdelincuentes refinarán sus tácticas de ingeniería social, lo que hará que sea cada vez más difícil para las personas y las organizaciones detectar y prevenir estos ataques.

Tecnologías emergentes

La proliferación de tecnologías emergentes, como las redes 5G y el Internet de las cosas (IoT), ampliará la superficie de ataque de los ciberdelincuentes. Las vulnerabilidades en estas tecnologías pueden ser un objetivo, lo que podría generar interrupciones en la infraestructura crítica, los dispositivos IoT y los sistemas conectados.

Ataques patrocinados por Estados

Países como China, Rusia, Irán y Corea del Norte, seguirán representando amenazas significativas para la seguridad cibernética. Estos ataques patrocinados por el Estado pueden tener como objetivo infraestructuras críticas, entidades gubernamentales y organizaciones involucradas en sectores estratégicos.

Actores no estatales

Los actores no estatales, como los *hacktivistas* y las organizaciones terroristas, pueden emplear cada vez más los ataques cibernéticos para promover sus objetivos. Estos ataques pueden variar desde acciones disruptivas para robar información confidencial o desfigurar sitios web, hasta operaciones más sofisticadas dirigidas a infraestructuras críticas.

Mayores medidas de seguridad

En respuesta a las crecientes amenazas cibernéticas, los Gobiernos, las empresas y las personas probablemente invertirán más en medidas de seguridad cibernética. Esto puede implicar la adopción de estrategias de defensa proactivas, la mejora de las capacidades de respuesta a incidentes y la implementación de prácticas de seguridad más sólidas.

Infostealers

Los *infostealers* se están volviendo más sofisticados y difíciles de detectar. Están utilizando técnicas más avanzadas para robar información personal, como el uso de ingeniería social y el desarrollo de *malware* furtivo. Es por todo esto por lo que se espera una mayor madurez en las empresas para equiparar la pérdida de información.

Es importante tener en cuenta que el panorama real de amenazas cibernéticas puede desviarse de estas predicciones debido a eventos imprevistos, avances en tecnologías defensivas o cambios en el panorama geopolítico.

Por lo tanto, las organizaciones y las personas deben monitorizar y adaptar continuamente sus estrategias de ciberseguridad para abordar las amenazas emergentes.

BIBLIOGRAFÍA →

- https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/
- https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=15307
- https://www.deia.eus/bizkaia/2023/01/31/diputacion-deshabilita-servicio-sede-electronica-6385840.html
- https://www.lavanguardia.com/local/sevilla/20230203/8731115/eprinsa-trabaja-dar-respuesta-ciberataque-sistemas-informacion-diputacion.html
- https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
- https://www.elmundo.es/comunidad-valenciana/castellon/2023/02/20/63f389c3e4d4d84d118b45a1.html
- https://blog.sekoia.io/one-year-after-the-cyber-implications-of-the-russo-ukrainian-war/
- https://www.elnuevosiglo.com.co/articulos/03-30-2023-espana-desmantela-red-de-hackers-que-atacaron-empresas-en-16-paises
- https://www.diariodesevilla.es/sevilla/estafas-informaticas-denuncian-dia-Sevilla_0_1776422702.html
- https://cincodias.elpais.com/companias/2023-03-22/un-ciberataque-pone-en-jaque-al-cuarto-mayor-distribuidor-de-medicamentos-de-espana.html
- https://www.deia.eus/bizkaia/2023/03/08/ciberataque-haber-destapado-datos-getxotarras-6538971.html
- https://www.granadahoy.com/espana/Agencia-Tributaria-ataque-informatico_0_1771023659.html
- https://www.elespanol.com/omicrono/tecnologia/20230402/yoigo-sufre-ciberataque-consiguen-acceder-personales-clientes/753174684_0.html
- https://www.eldebate.com/espana/20230404/joven-hackeo-cgpj-presumia-haber-llamado-don-juan-carlos-tener-datos-toda-espana_105760.html
- https://computerhoy.com/ciberseguridad/noname-grupo-hackers-rusos-detras-ciberataques-jornada-electoral-1279940
- https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-14-3/
- https://www.elnacional.cat/es/politica/ayuntamiento-sils-sufre-ciberataque-puesto-riesgo-datos-personales_1018215_102.html
- https://www.lavanguardia.com/local/sevilla/20230421/8912243/sucesos-cae-malaga-trama-criminal-funcionaba-consultoria-cibercrimen.html
- https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

BeDisruptive™

Limiting threats
for an unlimited future

Paseo de la Castellana 259C, Plta.33, Madrid

Contáctanos en info@bedisruptive.com

Conoce nuestro manifiesto

Visítanos en

www.bedisruptive.com