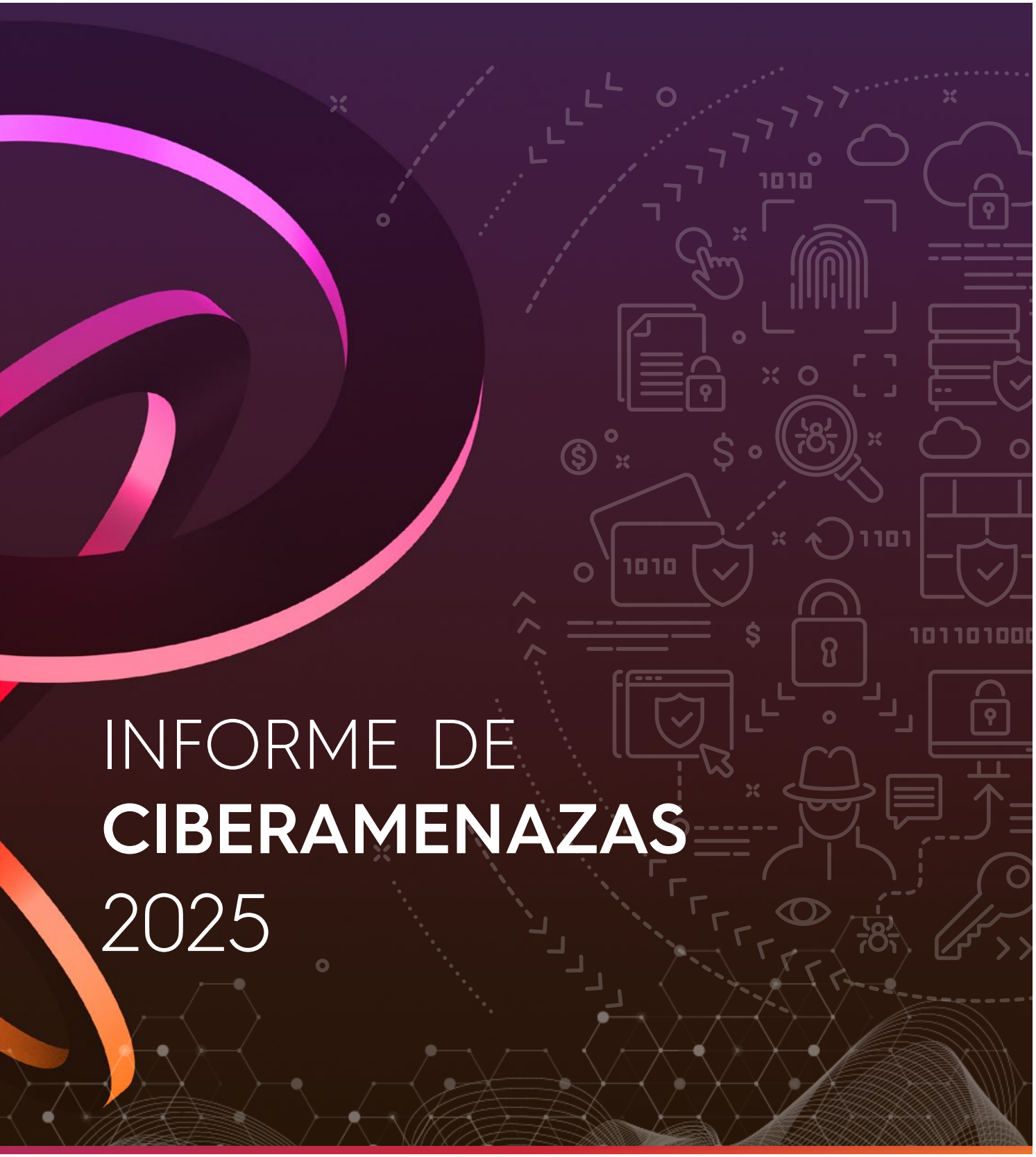
Security Operations Center



INFORME DE **CIBERAMENAZAS** 2025

sopra steria

CIBERSEGURIDAD SOPRA STERIA

La perspectiva estratégica de un líder europeo sobre las amenazas de ciberseguridad

En Sopra Steria hemos establecido la **línea de negocio de Ciberseguridad del Grupo** como un **pilar estratégico** de la transformación de la Compañía con la ambición de situarnos como **uno de los cinco principales líderes europeos en ciberseguridad para 2028.**

Estamos firmemente establecidos en Europa, con una fuerte presencia en Francia, los países nórdicos, Alemania, Benelux, Reino Unido y España. Además, hemos consolidado nuestra expansión internacional con la incorporación de Italia, Suiza, Singapur y América del Norte.

CIBERSEGURIDAD SOPRA STERIA

Fuerza global, cercanía local

Nuestro modelo *'Follow-the-Sun'* y las capacidades de *X-shore* en India, Polonia y España nos permiten ofrecer servicios continuos y de alto impacto a nuestros clientes. Esta base europea no es solo geográfica, sino que refleja nuestro compromiso con la soberanía, la confianza y la alineación regulatoria.

Estamos orgullosos de ser reconocidos como líderes en servicios de ciberresiliencia y de formar parte del reducido grupo de compañías que trabajan conforme a los principales marcos normativos en España y Europa, incluyendo el Esquema Nacional de Seguridad (ENS, RD 311/2022), la ISO/IEC 27001:2022, así como la Directiva NIS2 (UE 2022/2555) y el Reglamento DORA (UE 2022/2554). Estas acreditaciones y marcos de referencia avalan nuestra capacidad para actuar como socio de confianza tanto para los clientes del sector público como del privado, ayudándoles a desenvolverse en un panorama de amenazas complejo y en constante evolución.

Actuando como un solo equipo y aprovechando nuestra experiencia colectiva, aceleramos nuestro crecimiento, invirtiendo en plataformas de nueva generación impulsadas por IA y apoyando a nuestros clientes con un ecosistema de ciberseguridad resiliente y 100% europeo.

***FOLLOW THE SUN* – El modelo**

14 oficinas en **4** continentes

2.300 consultores y expertos en ciberseguridad

230M€ de facturación

Capacidades de nearshoring y offshoring

Reconocimiento en el mercado:

- Nelson Hall
- Sellos de la UE y del Gobierno para infraestructuras críticas

CIBERSEGURIDAD SOPRA STERIA

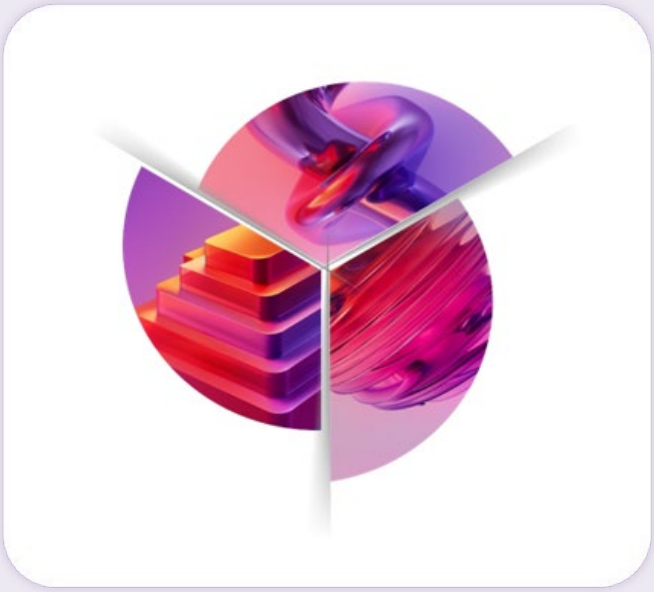
Una amplia gama de servicios y soluciones

PREVENCIÓN

Estrategia
Gobierno
Riesgos
Compliance
Auditorías técnicas
Pentest
Formación y sensibilización
Gestión de crisis

SOLUCIONES SOBERANAS

CAPITAL RIESGO



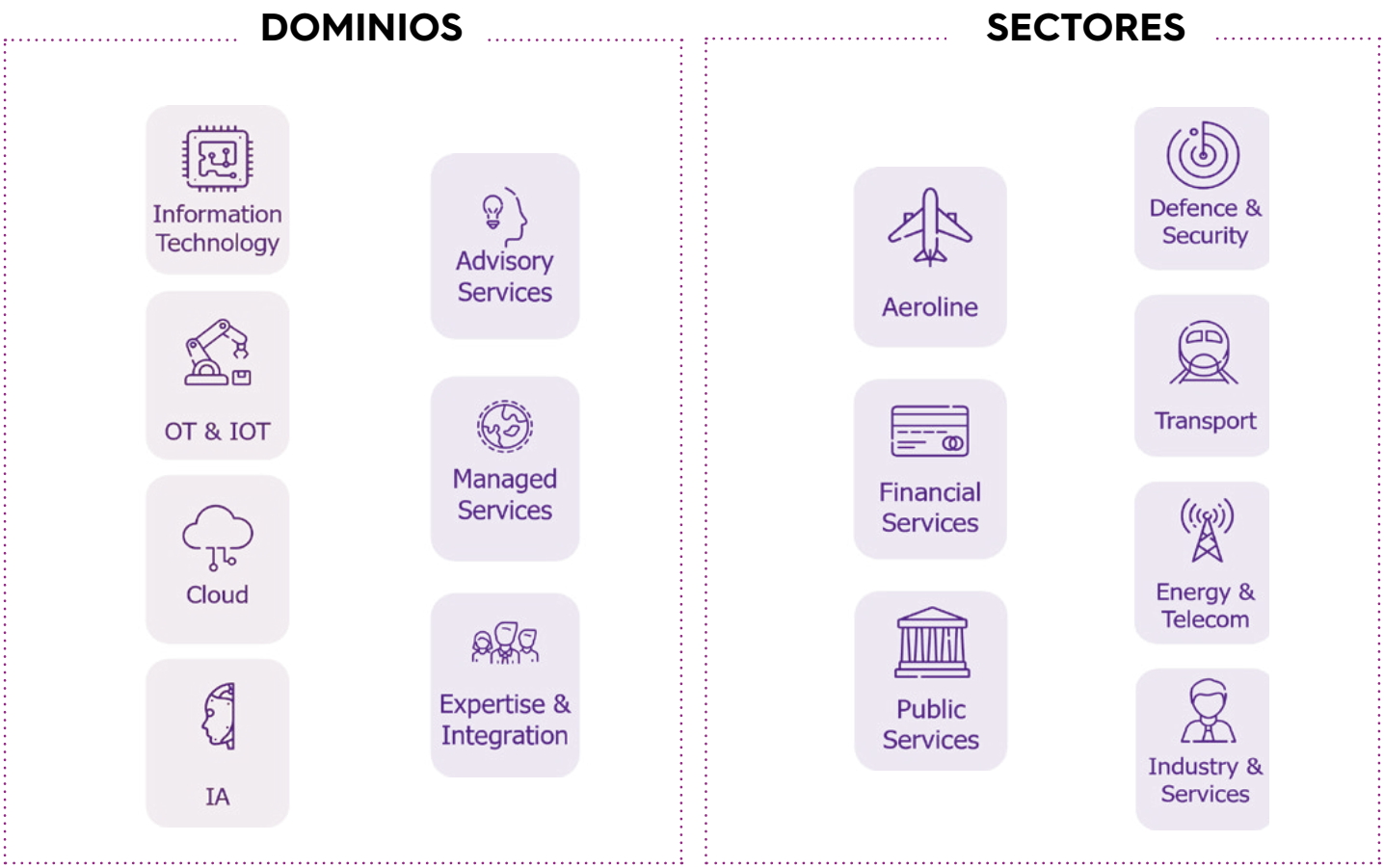
DETECCIÓN Y RESPUESTA GESTIONADAS

Detección
Investigación
Respuesta
Inteligencia sobre amenazas
Gestión de vulnerabilidades

PROTECCIÓN

Protección por diseño
Protección de dispositivos
Protección de datos
Protección de aplicaciones
Protección de la conectividad
Protección de la identidad
Protección de la confianza

Nuestra oferta es completa e integrada, abarcando todo el ciclo de vida de la ciberseguridad: desde la prevención y la protección, hasta la detección y respuesta. Todo ello, se complementa con soluciones soberanas desarrolladas por entidades de confianza como CS Group y la Unidad de Negocio de Defensa y Seguridad.



Para reforzar aún más esta oferta y acelerar la innovación, nuestra línea de negocio de Ciberseguridad cuenta con el apoyo estratégico de Sopra Steria Ventures.

Sopra Steria Ventures (SSV) es la división de inversión y alianzas estratégicas de Sopra Steria. Especializada en tecnologías de próxima generación como la inteligencia artificial y la computación cuántica, apoya a sectores europeos críticos como el aeroespacial, la defensa, la seguridad, los servicios financieros, los sectores públicos y el transporte.

Entre sus últimas inversiones destacan nuevas empresas de referencia como Egerie y Alice & Bob, así como fondos reconocidos como Tikehau Capital y Quantonation.

El equipo trabaja en estrecha colaboración con *startups* para potenciar su madurez tecnológica y generar sinergias con los clientes, talentos y socios de Sopra Steria. Esto nos permite no solo impulsar la innovación, sino también consolidarnos como socio estratégico para los principales líderes mundiales de seguridad y de los grandes *hyperscalers*.

CONTENIDO

ESTADO DE LA **CIBERSEGURIDAD** 2025

RESUMEN EJECUTIVO

El informe Estado de la Ciberseguridad 2025 ofrece un análisis exhaustivo del panorama actual de la ciberseguridad, destacando las principales tendencias, amenazas y desarrollos regulatorios. Su objetivo es informar a los responsables de la toma de decisiones sobre la evolución del entorno de ciberseguridad y brindar recomendaciones prácticas para fortalecer la seguridad organizacional.

España cuenta ya con un marco regulatorio consolidado en materia de ciberseguridad, sustentado en el Esquema Nacional de Seguridad (ENS, RD 311/2022) y en la futura transposición de la Directiva NIS2 (UE 2022/2555). Además, con el Reglamento DORA (UE 2022/2554), de aplicación directa desde enero de 2025, se refuerza la resiliencia operativa del sector financiero frente a amenazas avanzadas. Esta agrupación de marcos normativos, junto con las directrices del CCN-CERT y el impulso de INCIBE, buscan instar a las organizaciones a integrar la ciberseguridad y la resiliencia en el núcleo de sus operaciones.

En 2024, los ciberdelincuentes emplearon diversas tácticas como el uso de herramientas ilegítimas de monitoreo y administración remota (RMM), empleadas con fines maliciosos. Se observó una creciente especialización entre los grupos de ciberdelincuentes, así como una mayor explotación de entornos híbridos. Entre los métodos más utilizados para obtener acceso inicial figuran el *phishing*, el uso de credenciales válidas y la explotación de vulnerabilidades conocidas. Las técnicas de recopilación de datos y los objetivos destructivos, como el cifrado de información y la interrupción de la recuperación del sistema, se mantuvieron como tácticas habituales.

El creciente uso de herramientas legítimas de administración, *malware*, softwares para el robo de datos y herramientas diseñadas para evadir redes plantean importantes desafíos para la detección y mitigación de amenazas. El informe destaca la sofisticación de estos métodos y la necesidad urgente de estrategias avanzadas de detección y respuesta.

Se identificaron vulnerabilidades críticas en redes privadas virtuales (VPN), interfaces de programación de aplicaciones (API) y otros componentes esenciales de la infraestructura digital. La explotación activa de estas vulnerabilidades y el uso de servicios de túneles para exfiltrar datos representan una preocupación clave. El tiempo promedio de explotación (TTE), que mide cuánto tarda una vulnerabilidad en ser explotada tras su divulgación, se

ha reducido notablemente en los últimos años, situándose actualmente en apenas cinco días. Ante esta situación, las organizaciones deben priorizar la aplicación oportuna y frecuente de parches y actualizaciones.

El *phishing* continúa siendo uno de los vectores de ataque más comunes, con el auge de tendencias emergentes como el *phishing* multicanal, los ataques del tipo '*Adversary-in-the-middle*' (AiTM) y el auge de las plataformas de '*Phishing-as-a-Service*' (PhaaS). El informe detalla estas tácticas y recomienda estrategias de mitigación, poniendo especial énfasis en la autenticación multifactor (MFA) y la formación continua de los usuarios.

El resurgimiento del *malware*, en particular los stealers como Lumma Stealer, confirman el papel crucial de este tipo de softwares en las fases iniciales de los ataques y los desafíos que enfrentan los defensores ante adversarios que emplean técnicas del tipo *living-off-the-land* (LotL). El informe destaca la importancia de soluciones sólidas de detección y respuesta en endpoints (EDR) para hacer frente a estas amenazas.

Asimismo, se analiza la evolución del modelo *Ransomware-as-a-Service* (RaaS) y la volatilidad de los grupos de *ransomware*, con un incremento notable de ataques y el uso de técnicas cada vez más sofisticadas por parte de sus operadores. Entre las medidas de mitigación de estos riesgos se encuentran la segmentación de redes y la detección de amenazas en tiempo real.

INTRODUCCIÓN

Este informe está diseñado para una audiencia amplia: desde líderes en seguridad y profesionales del sector, hasta cualquier persona interesada en comprender mejor el mundo de la ciberseguridad. En un contexto donde los titulares sobre amenazas de ciberdelincuentes y nuevas vulnerabilidades aparecen a diario, resulta cada vez más complejo saber qué riesgos merecen realmente nuestra atención. Para ayudar a esta tarea, el informe recopila datos reales obtenidos por Sopra Steria a partir de una amplia variedad de organizaciones de distintos sectores. Los lectores tendrán la oportunidad de explorar análisis detallados sobre las metodologías de los atacantes, sus movimientos tras obtener el acceso y consejos prácticos de expertos en respuesta a incidentes, con el fin de ayudar a prevenir este tipo de ataques.

Aunque a veces la ciberseguridad pueda parecer una batalla interminable, este informe parte de la convicción de que, con inteligencia, conocimiento y una buena preparación, los defensores pueden mantenerse un paso por delante.

> "En última instancia, el informe pretende informar y concienciar a las partes interesadas sobre un panorama de amenazas en constante evolución.

DIRECTIVAS DE DEFENSA DIGITAL

El Gobierno de España, consciente de la necesidad de establecer un marco sólido en materia de ciberseguridad, dio un primer paso con la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, que ya introducía obligaciones de seguridad en los servicios digitales. Como desarrollo de esta norma, en 2010 se aprobó el Esquema Nacional de Seguridad (ENS), posteriormente actualizado en 2022 mediante el Real Decreto 311/2022, con el fin de garantizar la correcta aplicación de las medidas de seguridad en el sector público y en sus proveedores, así como de sentar una base robusta para su evolución futura.

Desde la aprobación del primer Esquema en 2010, España ha venido reforzando progresivamente su marco regulatorio en materia de ciberseguridad. A la actualización del ENS en 2022 (RD 311/2022) se suma la transposición de la Directiva NIS1 mediante el Real Decreto-ley 12/2018, que estableció obligaciones de seguridad para operadores de servicios esenciales y proveedores digitales.

Actualmente, España se encuentra en proceso de transposición de la Directiva NIS2 (UE 2022/2555), que amplía los sectores obligados y endurece los requisitos de gobernanza y notificación de incidentes. Esta evolución normativa también responde a un panorama en el que las infraestructuras críticas están cada vez más interconectadas y dependen de sistemas digitales, lo que multiplica tanto las vulnerabilidades como los posibles impactos. En este contexto, contar con marcos regulatorios que no solo respondan a los riesgos actuales, sino que preparen a las organizaciones para los desafíos futuros, resulta esencial. El enfoque intersectorial de la nueva regulación refleja una realidad clave: las amenazas en ciberseguridad no entienden de fronteras entre industrias y, por ello, la protección de la infraestructura nacional requiere estrategias coordinadas y transversales.

Paralelamente, otras normativas refuerzan este marco, como el Reglamento General de Protección de Datos (RGPD, UE 2016/679) y la LOPDGDD (LO 3/2018) en materia de privacidad y seguridad de la información, así como el Reglamento DORA (UE 2022/2554). Este último, en vigor desde enero de 2023 y de aplicación directa a partir del 17 de enero de 2025, supone un punto de inflexión en la regulación europea al abordar de forma integral la resiliencia operativa digital en el sector financiero. DORA introduce avances relevantes, como pruebas basadas en amenazas reales y requisitos más exigentes de gestión y respuesta ante incidentes. Su carácter exhaustivo marca una diferencia significativa respecto al Real Decreto-ley 12/2018, que transpuso la Directiva NIS1 en España. Mientras NIS1 planteaba un marco general de seguridad y gestión de riesgos para operadores de servicios esenciales y proveedores digitales, DORA pone el foco en garantizar que las instituciones financieras puedan mantener su funcionalidad incluso en condiciones

> El enfoque intersectorial de la nueva regulación refleja una realidad clave: las amenazas en ciberseguridad no entienden de fronteras entre industrias.

adversas. Este refuerzo normativo busca minimizar la posibilidad de perturbaciones generalizadas en un sector de importancia sistémica y alta exposición a amenazas avanzadas.

En conjunto, estas normativas reflejan un cambio de paradigma ya que la ciberseguridad ha pasado de ser un ejercicio voluntario a convertirse en un requisito estratégico y legal de obligado cumplimiento para las organizaciones públicas y privadas. Para cumplir con este nuevo marco, las entidades deben asumir que la seguridad digital constituye la base de su actividad y que el riesgo al que se enfrentan está estrechamente ligado a los actores que representan una amenaza para ellas. Además, la gestión de riesgos no puede entenderse como un proceso estático, sino como un sistema dinámico que debe adaptarse de forma continua a la evolución de las amenazas y a la aparición de nuevos vectores de ataque. De esta manera, las organizaciones no solo podrán cumplir con la normativa, sino también fortalecer su resiliencia y capacidad de respuesta frente a un entorno digital cambiante.

En España, la transposición de la Directiva NIS2 (UE 2022/2555) se encuentra actualmente en desarrollo y se espera que quede plenamente incorporada al ordenamiento jurídico durante 2025. Esta directiva pondrá un mayor énfasis en aspectos críticos como la continuidad de negocio, la gestión de incidentes y la gobernanza de la ciberseguridad a nivel directivo. Aunque el alcance exacto y los mecanismos de supervisión nacional aún están en proceso de definición, la tendencia es clara: avanzar hacia un marco más detallado, exigente y aplicable. Esto obligará a las organizaciones a adoptar un enfoque holístico en su gestión de la seguridad, donde el incumplimiento podrá derivar en responsabilidades directas, incluidas sanciones administrativas. La introducción de estos marcos regulatorios refleja un cambio general hacia la incorporación de la resiliencia como parte esencial de las estructuras operativas básicas, asegurando que las entidades estén mejor preparadas para afrontar los retos de un panorama digital en constante transformación.

01. **CIBERDELINCUENCIA** Y MÉTODOS

En 2024, los ciberdelincuentes emplearon una amplia gama de tácticas, técnicas y procedimientos (TTP) que abarcan múltiples etapas de la *Kill Chain*. La explotación de numerosas herramientas, y métodos para avanzar en sus ataques, ilustra tendencias significativas en la evolución de las ciberamenazas.
Estas tendencias reflejan los esfuerzos de los atacantes para evadir los sistemas de detección tradicionales y aprovechar las complejidades de los entornos híbridos. En particular, se ha registrado un mayor uso de herramientas de monitoreo y administración remotas (RMM), que, debido a sus amplias capacidades e integración en algunos entornos corporativos, permiten a los atacantes desplegar una gran variedad de técnicas mientras se camuflan dentro del tráfico legítimo.

El análisis de las herramientas y el *malware* predominantes revelan una

diversificación en los métodos y una mayor explotación del software legítimo con fines maliciosos. En el año 2024 se observó una especialización entre los ciberdelincuentes con más grupos centrados en etapas concretas de la cadena de ataque en lugar de cubrir el ataque completo. Por ejemplo, grupos especializados en acceso inicial, vulnerabilidades de seguridad o desarrollo de *malware*. Los criminales innovan con técnicas de evasión y cifrado mejorado para eludir las soluciones de seguridad. La persistencia de estos actores demuestra el interés lucrativo de la ciberdelincuencia en este método de extorsión, especialmente a través de ataques de doble extorsión.

Cada vez más adaptados, los ciberdelincuentes están dirigiendo sus ataques a infraestructuras de red y plataformas SaaS, centrándose en los cimientos de los entornos en la nube y el trabajo remoto. Esta transición no solo ilustra su capacidad para explotar debilidades organizativas, como la gestión de parches, sino también su estrategia para maximizar el impacto en un mundo interconectado.

ETAPAS DE LA INTRUSIÓN

Acceso inicial

Las propias observaciones de Sopra Steria indican que los ciberdelincuentes explotaron principalmente las siguientes técnicas del marco MITRE ATT&CK[1] para obtener acceso a los sistemas a lo largo de 2024:

- *Phishing* (T1566): Las ciberamenazas continúan introduciendo innovaciones en las campañas de *phishing*.
- Cuentas válidas (T1078): La prevalencia de *stealers* en 2024 influyó significativamente en la forma en que los criminales obtuvieron su acceso inicial a los sistemas objetivo.
- Explotación de vulnerabilidades públicas (T1190): La explotación de vulnerabilidades en sistemas expuestos a Internet sigue siendo un método utilizado de forma marginal en la esfera cibercriminal.
- Cada vez más, los métodos empleados por los ciberdelincuentes para obtener acceso inicial a los sistemas comprometidos implican el uso de cuentas válidas previamente adquiridas por ellos. A través de un incidente inicial por parte de un *stealer* (RDP, SSH u otro), las credenciales se compran en la *darknet* y luego se reutilizan para otros fines.

Recogida de datos

Los atacantes han diversificado e intensificado su búsqueda de información confidencial en sistemas comprometidos.

Esto explica la presencia de las siguientes técnicas entre las mejores metodologías de 2024:

- Volcado de credenciales del sistema operativo (T1003)
- Datos del sistema local (T1005)
- Exfiltración a través del canal C2 (T1041)

Impacto y objetivos destructivos

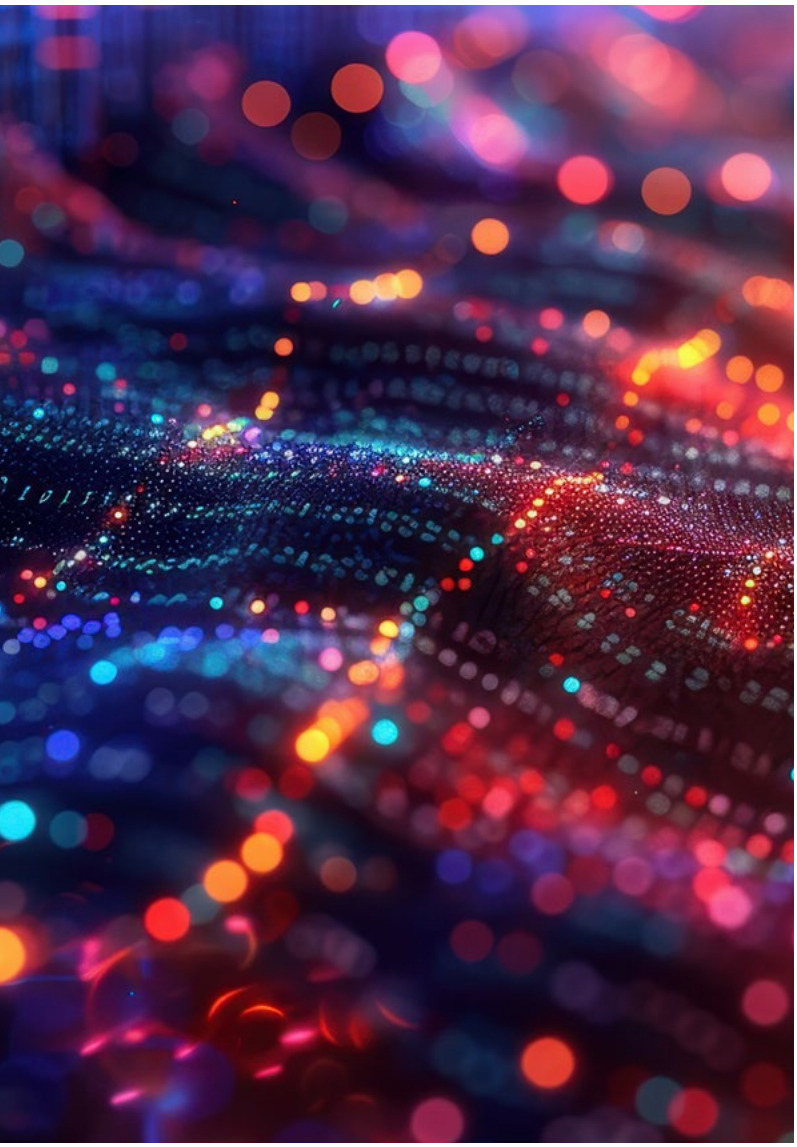
- Cifrado de datos (T1486): Se utiliza principalmente en ataques de *ransomware* para hacer que los datos sean inaccesibles para las víctimas.
- Inhibir la recuperación del sistema (T1490): Impide que las víctimas restauren los sistemas a partir de copias de seguridad, lo que aumenta el impacto del ataque.

Estos métodos evidencian un objetivo final destructivo junto con impactos significativos en los sistemas comprometidos.

[1] https://attack.mitre.org/techniques/enterprise/

HERRAMIENTAS Y TÉCNICAS

El uso creciente de servicios y plataformas legítimas por parte de los ciberdelincuentes marca un cambio significativo en sus tácticas. Ya no se limitan a emplear las herramientas maliciosas tradicionales, ahora adoptan un enfoque de *"Living off the Land"*, utilizando herramientas existentes ya instaladas en el sistema de destino. Esta evolución refleja una experiencia avanzada y profundo conocimiento de los entornos a los que se dirigen, mostrando un nuevo nivel de madurez tecnológica.



Mayor uso de herramientas de administración legítimas:

Herramientas como **ADExplorer, AnyDesk, Advanced IP Scanner y PsExec** se reutilizan con frecuencia para intrusiones en sistemas corporativos. Éstas herramientas permiten a los atacantes explorar la infraestructura, mantener el acceso persistente y ampliar sus ataques en tiempo mientras reducen el riesgo de detección al simular operaciones legítimas.

- Por ejemplo, **AnyDesk** y **TeamViewer** facilitan el control remoto.
- Los comandos **ADExplorer** y **PowerShell** permiten la asignación de *Active Directory.*

Proliferación de *malware* y herramientas de robo de datos

Las herramientas de robo de datos como **Mimikatz**, **LaZagne**. entre otras, así como el *malware* dirigido como **Lumma Stealer**, **Redline** y **Raccoon Stealer**, se han utilizado ampliamente para extraer credenciales. Estas permiten a los atacantes filtrar contraseñas e información confidencial, lo que facilita el acceso no autorizado y el movimiento lateral dentro de las redes empresariales.

Los ciberdelincuentes actualizan con frecuencia sus herramientas para evitar la detección. Por ejemplo:

- **Lumma Stealer** recibe actualizaciones semanales de código y servidores, lo que dificulta su detección y lo hace más atractivo para los delincuentes. Este ciclo rápido de actualización permite mantenerse a la vanguardia de las funciones de seguridad aplicadas en el navegador web.
- Del mismo modo, **Latrodectus**, el sucesor de **IcedID**, elimina características en sus actualizaciones para evadir controles de seguridad.

Explotación de servicios de tunelización y herramientas de evasión de red

Los ciberdelincuentes utilizan servicios de *tunneling* como **Ngrok** y **Cloudflare Tunnel** para eludir las medidas de seguridad. Estas herramientas dificultan la detección y el bloqueo de conexiones maliciosas, lo que refleja la creciente sofisticación de los atacantes en la evasión de defensas de la red.

Uso de herramientas de explotación de vulnerabilidades

Se emplean herramientas y técnicas como **Metasploit**, **Nmap** y **Kerberoasting** para identificar y explotar vulnerabilidades dentro de los sistemas de red y los servicios de autenticación. Al detectar configuraciones incorrectas de seguridad, estos enfoques permiten a los atacantes infiltrarse y potencialmente comprometer infraestructuras completas.

Uso de servicios legítimos para la exfiltración de datos

Los ciberdelincuentes recurren a plataformas de intercambio de archivos como **Dropbox** y **MEGA** para exfiltrar en secreto los datos robados. Al apoyarse en servicios confiables, dificultan la detección por parte de los equipos de seguridad, demostrando su habilidad para eludir las defensas tradicionales y aprovechar las debilidades de los servicios externos.

Herramientas de evasión y persistencia

Los atacantes utilizan herramientas como **SystemBC** y **SocGholish** para ocultar su presencia y mantener acceso a sistemas infectados. También emplean **BITSAdmin** y **PowerShell** para automatizar tareas maliciosas. Esta combinación de herramientas legítimas y *malware* avanzado hace que sus acciones sean más difíciles de detectar y más efectivas.

Canales múltiples C2 para evitar la detección

Los atacantes se comunican con las máquinas infectadas mediante canales como **Discord**, **Telegram**, **IRC** y **SMTP**. Esta diversidad muestra su habilidad técnica para mantener sistemas de *command & control* (C2) flexibles y resistentes. Al utilizar múltiples servicios, reducen el riesgo de interrupción si uno de los canales es bloqueado, lo que evidencia su adaptabilidad.

INFRAESTRUCTURA

Explotación de APIs y tecnologías de *streaming*

Los atacantes aprovechan APIs de servicios como **GitHub**, **GitLab**, **GoFile** y **Vimeo** para integrarlos en sus procesos C2. Esta automatización incrementa la resiliencia y eficiencia de sus operaciones. El uso de tecnologías como **WebSockets** y **WatsonTCP** refleja su experiencia en protocolos de comunicación avanzados.

Confusión a través de algoritmos de destino generados aleatoriamente

Al utilizar algoritmos que generan destinos aleatorios para la transferencia de datos, los ciberdelincuentes dificultan la detección de los flujos de exfiltración. Esta técnica demuestra una comprensión profunda de los métodos de análisis del tráfico de red y las formas de eludir las medidas de detección basadas en modelos de comportamiento.

Uso de soluciones de nube pública

Los atacantes emplean servicios como **CloudFlare**, **Amazon Web Services** y **Firebase** para ocultar sus actividades detrás de una infraestructura legítima en la nube. Esto complica la labor de los analistas de seguridad a la hora de distinguir entre tráfico normal y malicioso, lo que refleja la madurez y el conocimiento de los atacantes sobre las prácticas de seguridad en entornos Cloud.

MONITOREO REMOTO Y ADMINISTRACIÓN

Una herramienta de supervisión y gestión remota (RMM) es un tipo de software diseñado para ayudar a los proveedores de servicios gestionados (MSP) y a los profesionales de IT a supervisar y administrar de forma remota los *endpoints*, las redes y los ordenadores de los clientes cuando el acceso físico es limitado. Estas herramientas suelen ofrecer una variedad de funciones como el acceso remoto, el monitoreo, la automatización, las alertas, los informes o la gestión de seguridad.

Aunque están diseñadas para fines legítimos, los atacantes las aprovechan cada vez más por sus amplias capacidades. Los ciberdelincuentes utilizan herramientas RMM para controlar de forma remota los ordenadores de las víctimas, realizar tareas de reconocimientos, desplegar *malware* y mantener un acceso persistente, a menudo eludiendo las medidas de seguridad tradicionales gracias a su naturaleza legítima.

Esto se observó en una campaña en **agosto de 2024**, donde los atacantes emplearon ingeniería social, como *phishing* y llamadas telefónicas, para engañar a las víctimas e inducirlas a que instalaran el software RMM **AnyDesk**. Tanto los **ciberdelincuentes patrocinados por el Estado** como los **grupos de *ransomware*** utilizan herramientas RMM para obtener acceso no autorizado, mantener la persistencia, ejecutar comandos y exfiltrar datos.

En particular, entre **julio y agosto de 2024**, se registraron ataques de *ransomware* que involucraron a **AnyDesk** y alteraron la **configuración de RDP** para implementar *ransomware* y exfiltrar datos.

Los delincuentes suelen usar ingeniería social, como ventanas emergentes amenazantes, campañas de phishing o llamadas dirigidas, para engañar a las víctimas para que instalen el software RMM.

Acceso inicial:

Bombardeo de correos electrónicos y llamadas telefónicas persuasivas.

Suplantación de bancos del Reino Unido mediante sitios web falsificados y técnicas de *phishing*.

Post-instalación: *malware*

Entrega de diferentes *payloads*, como **SystemBC** y **túneles SSH inversos**, **para elevar privilegios y ejecutar actividades maliciosas en sistemas comprometidos.**

Acceso a las cuentas bancarias de las víctimas y exfiltración de datos.

Insight

Las herramientas RMM son frecuentemente utilizadas por grupos de ransomware, ya que permiten establecer persistencia y control remoto. También facilitan el despliegue de ransomware y la exfiltración de datos. Algunos ejemplos como los ataques de ransomware, ocurridos entre julio y agosto de 2024, aprovecharon AnyDesk o alteraron la configuración del Protocolo de Escritorio Remoto (RDP):

Acceso inicial:

Explotación de sistemas conectados a Internet y credenciales comprometidas para acceder a sistemas de servidores RDP y Exchange expuestos.

INC Ransomware utilizó infecciones de Gootloader en una campaña dirigida a hospitales de EE. UU.

Mad Liberator atacó a las víctimas que ya usaban AnyDesk, enviando solicitudes de conexión no solicitadas para obtener acceso no autorizado.

Akira explotó un servidor de copias de seguridad de Veeam sin parches a través del CVE-2023-27532.

Post-instalación:

Las herramientas de RMM se utilizaron para mantener la persistencia, exfiltrar datos y, en última instancia, implementar *ransomware*.

Deshabilitar la entrada del usuario.

Protege tu organización de las amenazas de supervisión y gestión remotas

Para poder detectar la actividad maliciosa de RMM se requiere una combinación de medidas técnicas y análisis, como:

- Detección y respuesta de *Endpoints* (EDR): Implementar soluciones EDR que monitoreen las actividades de los *endpoints* y detecten comportamientos sospechosos. Estas herramientas EDR pueden identificar el uso de RMM no autorizadas a partir de sus patrones de comportamiento y comunicación.
- Auditorías periódicas: Realizar auditorías de seguridad y escaneos de vulnerabilidades de forma periódica para identificar y mitigar riesgos potenciales. Estas auditorías ayudan a descubrir instalaciones o configuraciones de software no autorizadas.
- *Whitelist* de aplicaciones: Asegurarse de que solo el software aprobado pueda ejecutarse en la red, evitando así que la instalación y ejecución de herramientas RMM no autorizadas.

02.
INCIDENTE
INICIAL

El incidente inicial es la fase en la que los atacantes buscan establecer su primer punto de apoyo dentro de una red. En 2024, Sopra Steria observó que los ciberdelincuentes se basaban principalmente en tres técnicas para infiltrarse en los sistemas: *Phishing*, uso de cuentas válidas y explotación de vulnerabilidades públicas

Esta sección analiza las tendencias de *phishing* de 2024, junto con las vulnerabilidades observadas durante el mismo año.

PHISHING

El *phishing* ha pasado de ser una simple molestia a convertirse en una piedra angular del cibercrimen moderno, explotando vulnerabilidades humanas y técnicas. Es el principal vector de ataque inicial, y tanto la frecuencia de los ataques como la sofisticación de las tácticas aumentan cada año.

En 2024, Sopra Steria observó que el 59,9% de todos los incidentes dentro de las redes de sus clientes estaban relacionados con el *phishing*. El aumento de los incidentes de *phishing* observado por Sopra Steria en 2023 se han mantenido a lo largo de 2024.

TENDENCIAS OBSERVADAS DE *PHISHING* EN 2024

Las tendencias de *phishing* en 2024 muestran similitudes con años anteriores, pero han evolucionado con nuevas técnicas emergentes que se adaptan a entornos cambiantes. A continuación, se proporciona un análisis de las tácticas de *phishing* más frecuentes observadas por Sopra Steria a lo largo del año.

Recolección de credenciales

Una de las tendencias más significativas y en continuo aumento es la recolección de credenciales. Más allá de la explotación inmediata, estas credenciales a menudo se venden o intercambian para su uso en ataques posteriores, como: apropiaciones de cuentas, fraude financiero y robo de identidad.

El robo de credenciales alimenta un mercado clandestino amplio y muy activo.

Ataques de *phishing* multicanal

En 2024, los ataques de *phishing* multicanal han aumentado y los ciberdelincuentes utilizan: SMS, llamadas telefónicas, apps de mensajería y emails. A menudo, estos atacantes se hacen pasar por personal de soporte de IT para engañar a los usuarios para que descarguen software malicioso u otorguen acceso.

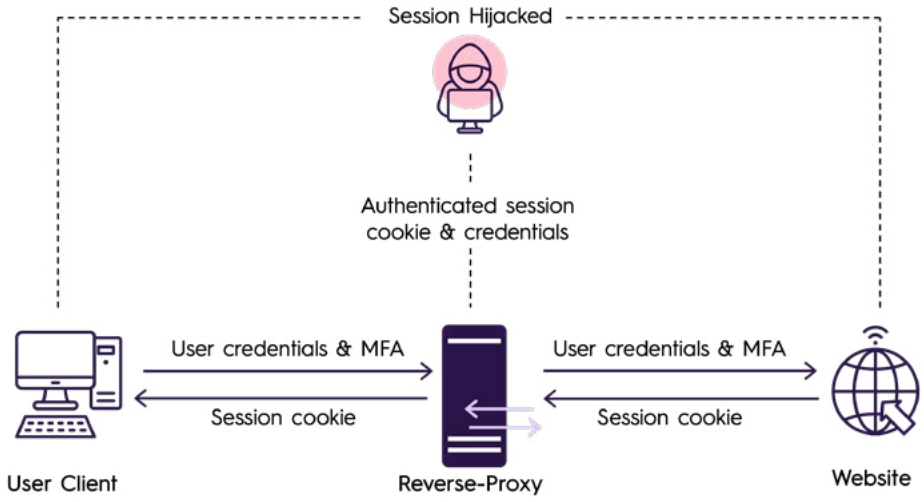
Según diferentes proveedores de telecomunicaciones, la introducción de filtros de suplantación de identidad más eficaces para bloquear llamadas falsas han llevado a que los criminales usen cada vez más números de distintos países para eludir las defensas.

Adversary-in-the-Middle

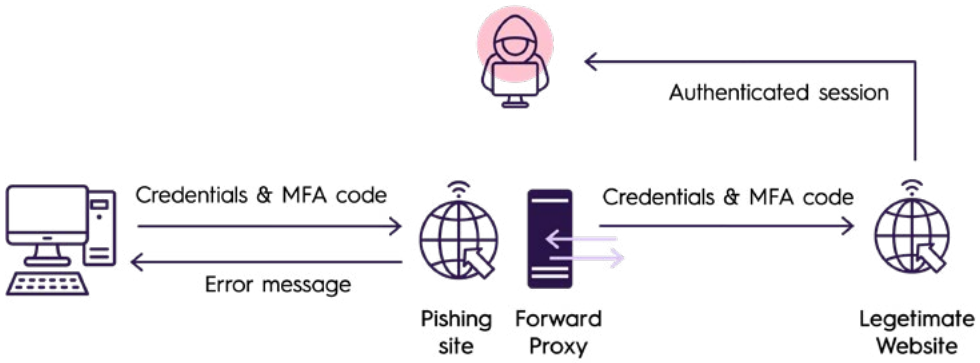
Sopra Steria ha observado una alta incidencia de ataques AiTM en nuestra base de clientes a lo largo de 2024. La disponibilidad de plataformas PhaaS como Tycoon y Evilginx ha contribuido a la creciente popularidad de los ataques AiTM, haciéndolos más accesibles para los grupos de delincuentes, independientemente de su capacidad técnica. Estos ataques utilizan *proxies* para interceptar la comunicación entre los usuarios y los sitios web legítimos, capturando credenciales y *cookies* de sesión para eludir la autenticación multifactorial (MFA).

Entre las técnicas observadas se incluyen los ataques AiTM de *proxy* inverso, que se dirigen a cuentas específicas interceptando el tráfico hacia sitios legítimos, y los ataques AiTM de *proxy* directo, que imitan las páginas de inicio de sesión para robar credenciales y *tokens* MFA sin *proxy* directo del tráfico.

AITM DE PROXY INVERSO



AITM DE PROXY DIRECTO



Ejemplo

El 18 de abril de 2024, la Policía Metropolitana de Reino Unido, junto con agencias internacionales de seguridad y socios del sector privado, lograron desmantelar LabHost, un proveedor de *Phishing-as-a-Service* (PhaaS), también conocido como LabRat. Surgido a finales de 2021, ofrecía diversos servicios de *phishing* dirigidos a bancos y otras organizaciones, principalmente en Canadá, Estados Unidos y Reino Unido. En el momento de su desmantelamiento: LabHost contaba con más de 2.000 usuarios criminales, se habían desplegado más de 40.000 sitios fraudulentos y la plataforma había afectado a cientos de miles de víctimas en todo el mundo. LabHost proporcionaba herramientas para: Obtener códigos de autenticación de dos factores (2FA), plantillas de *phishing* personalizables y un componente de smishing por SMS muy popular.

Sopra Steria ha observado varios incidentes que implican el uso de Tycoon y Evilginx. Tras obtener el acceso inicial, estos incidentes suelen incluir: Añadir dispositivos de autenticación adicionales a la cuenta del usuario para mantener la persistencia, solicitar o buscar documentos sensibles y crear reglas de bandeja de entrada en los buzones para manipular el flujo del correo electrónico y ocultar la actividad maliciosa.

Ejemplo

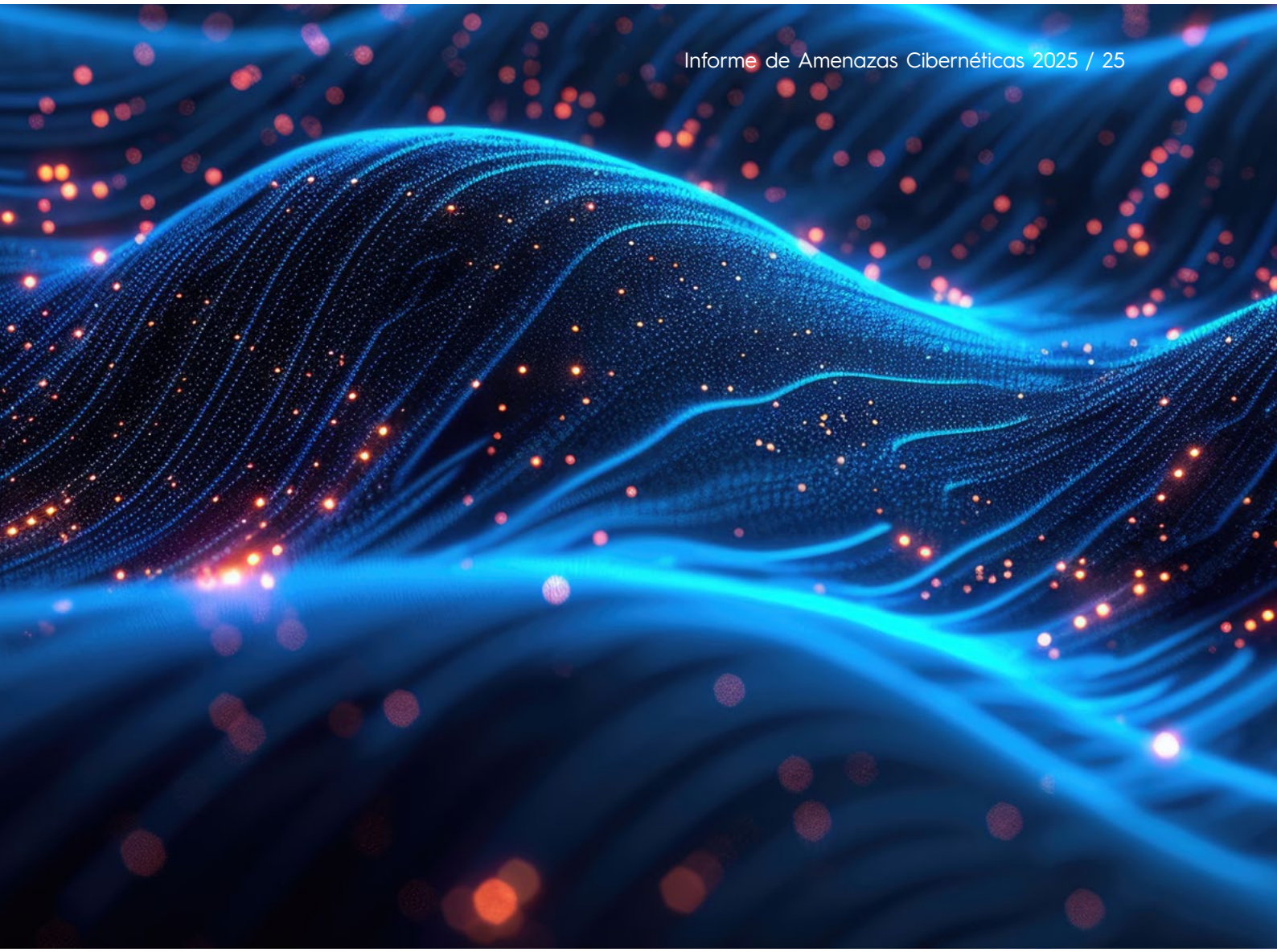
Phishing-as-a-Service **(PhaaS)**

El PhaaS se ha consolidado como un actor significativo en el panorama global del *phishing* al ofrecer soluciones llave en mano que simplifican y optimizan las operaciones. En 2024, la mayoría de los correos electrónicos de *phishing* se originaron en estas plataformas, que proporcionan: Kits de *phishing* prediseñados, dominios falsificados y servicios de soporte integrales.

El PhaaS reduce la barrera de entrada para los ciberdelincuentes, lo que permite ataques de *phishing* más generalizados y sofisticados. Plataformas como Darcula, Tycoon y Caffeine (ahora ONNX) permiten que incluso atacantes con escasa capacitación técnica puedan lanzar campañas sofisticadas, a menudo dirigidas contra cuentas protegidas con MFA mediante *Adversary-in-the-Middle* (AiTM).

Sopra Steria ha observado varios incidentes que implican el uso de Tycoon y Evilginx. Tras el acceso inicial, estos incidentes suelen incluir: alta de dispositivos de autenticación adicionales a la cuenta del usuario para mantener la persistencia, consulta de documentos sensibles y reglas de bandeja de entrada en los buzones para manipular el flujo del correo electrónico y mantener el acceso.

La adaptabilidad de las plataformas PhaaS incluye tácticas como incrustar URLs de *phishing* en archivos HTML, PDFs o ZIP para evadir los mecanismos de detección. Esto condujo a un aumento notable en el robo de credenciales en 2024. Durante ese año, los principales proveedores de PhaaS enviaron millones de correos de *phishing* cada mes, amplificando significativamente su impacto.



REDES SOCIALES

El uso de redes sociales y perfiles falsos en campañas de *phishing* creció significativamente en 2024. Los atacantes monitorizan en tiempo real plataformas como LinkedIn, explotando actualizaciones —como cambios en títulos de trabajo— para lanzar ataques de ingeniería social (*social engineering attacks*) poco después de que se produzcan dichas modificaciones. Sopra Steria ha observado casos en los que esta táctica se utilizó para obtener acceso inicial a los sistemas de las víctimas.

Además, se ha percibido que actores estatales llevan a cabo campañas de *phishing* en las que se hacen pasar por reclutadores o candidatos. Con herramientas de IA crean perfiles y currículums convincentes para atraer a las víctimas a reuniones falsas, redirigirlas a portales infectados con *malware* o comprometer credenciales a través de evaluaciones de habilidades fraudulentas. En algunos casos, llegan a asegurar puestos de trabajo remotos para abusar de accesos legítimos y robar datos, propiedad intelectual y fondos.

DENTRO DE LA BANDEJA DE ENTRADA

En 2024, Sopra Steria registró un total de 824 millones de correos electrónicos procesados en su base de clientes, con un promedio de 4,6 URLs y 1,7 archivos adjuntos por cada correo recibido en bandeja de entrada. Esta prevalencia de enlaces y ficheros incrustados subraya el desafío de distinguir los correos legítimos de las posibles amenazas, elevando el riesgo de ataques de *phishing*.

Esta sección abordará específicamente nuestras observaciones sobre correos en cuarentena, archivos adjuntos y amenazas relacionadas con dominios observados en la base de clientes de Sopra Steria.

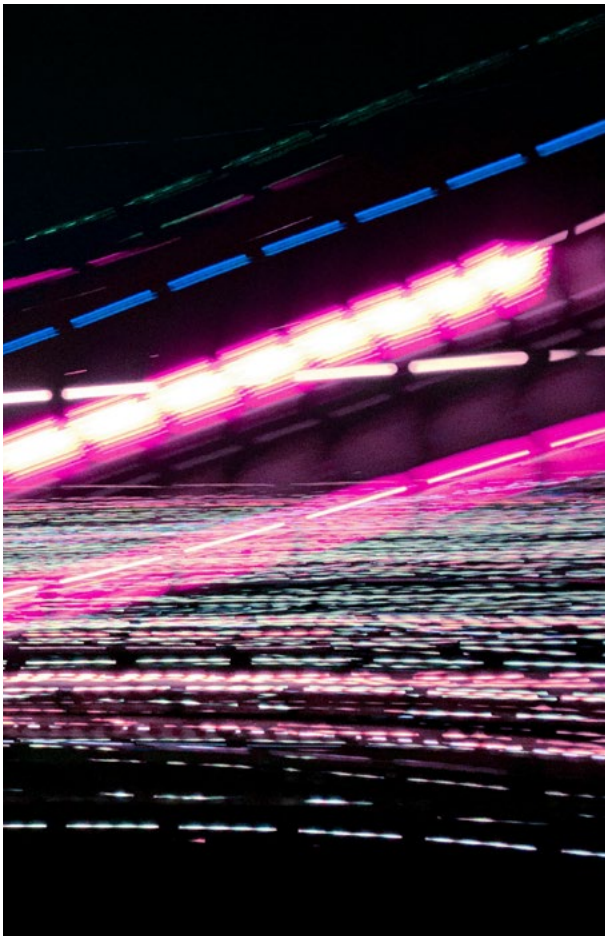
Archivos adjuntos

El análisis de datos de clientes realizado por Sopra Steria revela que los tipos de archivo más comunes encontrados en las carpetas de cuarentena, excluyendo imágenes y archivos de texto, son: RAR, HTML, ZIP, PDF y DOCX. Esto coincide con los patrones globales de ficheros usados comúnmente en campañas de *phishing* y otros ciberataques.

A nivel global, hemos observado técnicas de *phishing* interesantes. Ejemplos incluyen: Archivos SVG, documentos de OneNote con URLs maliciosas incrustadas y archivos RDP como adjuntos. Estos casos son relativamente poco frecuentes en nuestros clientes de Sopra Steria, probablemente debido a nuestras medidas proactivas de bloqueo y porque dichos métodos suelen ser empleados por grupos pequeños y especializados con objetivos específicos.

Emails en cuarentena

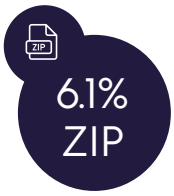
El análisis de los datos de clientes de Sopra Steria en 2024 reveló que más de 29 millones de correos electrónicos —aproximadamente el 3,6 % de todos los emails— fueron puestos en cuarentena o marcados como *spam*. Si bien no todos los correos en cuarentena o *spam* son intentos de *phishing*, a menudo indican patrones sospechosos, lo que los convierte en una fuente valiosa para el análisis de amenazas.



Top 5 de tipos de archivos en cuarentena

Los archivos RAR son usados con frecuencia en las campañas de *phishing* debido a su capacidad para agrupar múltiples componentes maliciosos. Los archivos RAR cifrados o protegidos con contraseña pueden eludir los filtros de correo electrónico, ocultando su contenido frente a los análisis automatizados y entregando *malware* como *ransomware* o troyanos.

Los archivos HTML se utilizan habitualmente en ataques de *phishing* debido a su versatilidad. A menudo contienen URLs que conducen a sitios de *phishing* o se conectan a servidores controlados por atacantes para desplegar contenido malicioso. Para evadir la detección, los archivos HTML se incrustan con frecuencia en archivos ZIP, documentos de Microsoft Office u otros tipos de ficheros. Técnicas como HTML *smuggling* permiten que el código malicioso se oculte dentro del HTML y permita a los atacantes eludir filtros de seguridad para entregar *malware* o esquemas de robo de credenciales.



Los archivos ZIP son una herramienta habitual en el *phishing* por su capacidad para comprimir y ocultar *payloads* maliciosas. Los atacantes los utilizan para agrupar componentes dañinos y eludir filtros de seguridad, especialmente cuando están cifrados o protegidos con contraseña. Sin embargo, los archivos RAR suelen ser más utilizados frente al uso ZIP, ya que permiten empaquetar estructuras más complejas, lo que los hace más efectivos en campañas de *phishing* sofisticadas.

Los archivos PDF siguen siendo un vector de *phishing* popular, a menudo conteniendo URLs que redirigen a sitios de *phishing* mediante varios pasos de redirección. Estos pueden implicar servicios legítimos, desafíos CAPTCHA o enlaces directos a dominios corruptos. Con frecuencia, los atacantes ocultan PDFs dentro de otras capas de tipos de archivo, como ZIP, o los alojan en plataformas legítimas para evadir la detección. Este enfoque refleja las tácticas de *phishing* basadas en HTML y subraya la adaptabilidad de los atacantes al aprovechar formatos de confianza con fines maliciosos.

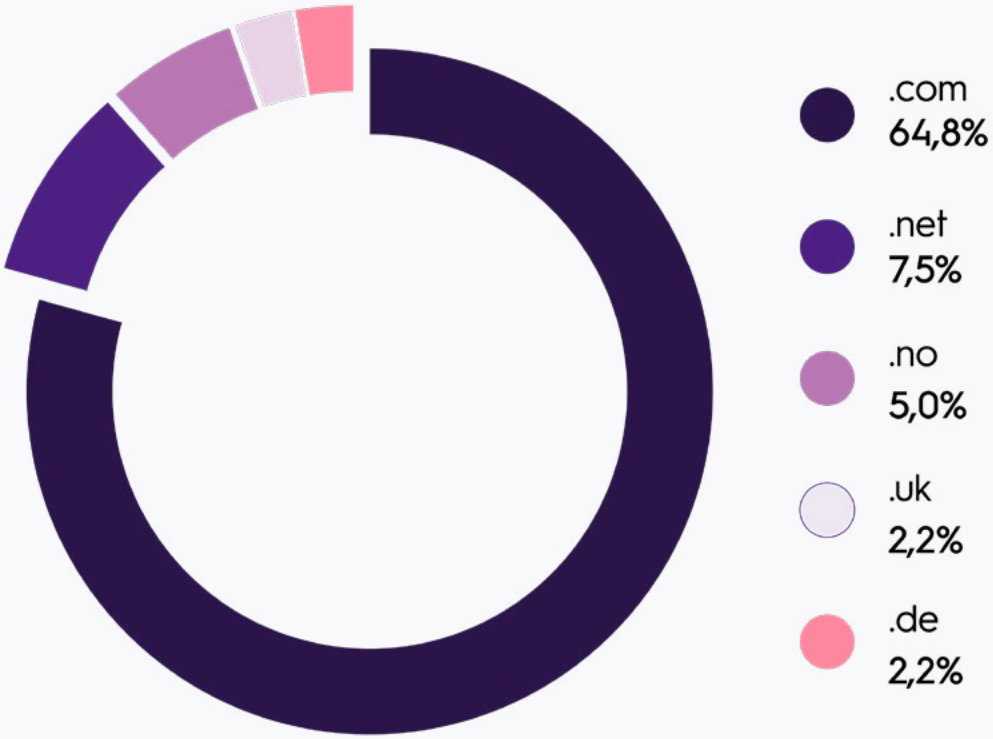
Los archivos DOCX, con menor presencia en cuarentena, siguen representando una amenaza. Aunque las macros están bloqueadas por defecto en las instalaciones modernas de Office, los ciberdelincuentes utilizan métodos alternativos de explotación como la inyección de plantillas (*template injection*). En 2024, se observó una tendencia destacada en el uso de archivos DOCX corruptos dentro de campañas de *phishing*. Estos archivos dañados pueden evadir los filtros de seguridad y, cuando los destinatarios los abren, la función de recuperación de Word restaura el documento, incitando a la interacción con el contenido malicioso incrustado.

Dominios

Los dominios de primer nivel (TLD) identificados con mayor frecuencia en las carpetas de cuarentena de la base de clientes de Sopra Steria en 2024 fueron: **.com**, **.net**, **.no**, **.uk** y **.de**.

Cabe destacar que una parte de todos los TLDs presentes en estas carpetas proviene de **.ru** (Rusia) y **.cn** (China). Estos TLDs rara vez se asocian a comunicaciones legítimas por correo electrónico para nuestros clientes, por lo que su presencia resulta especialmente relevante.

Top 5 de TLDs en correos en cuarentena



Los cinco TLDs principales encontrados en correos electrónicos en cuarentena reflejan una mezcla de dominios globales y regionales de confianza. Aunque son esperables en las redes de Sopra Steria, su uso generalizado y su credibilidad los convierten en objetivos propicios para el abuso.
Las campañas de *phishing* suelen explotar TLDs populares como: .com, .net, .no, .uk, .de... para parecer legítimas. Con frecuencia, estos dominios se combinan con **servicios de alojamiento 'a prueba de derribos' (*bulletproof hosting*)** que resisten intentos de cierre y acciones legales, proporcionando a los atacantes una infraestructura estable para actividades maliciosas.

Los atacantes integran cada vez más estos TLDs con **plataformas en la nube** como **AWS** y **Google Cloud** para alojar páginas de *phishing*, mezclando tráfico malicioso con uso legítimo. También se emplean servicios de confianza como **Dropbox** y **OneDrive** para alojar *payloads*, mientras que los **certificados gratuitos** (p. ej., ***Let's Encrypt***) facilitan la creación de sitios de *phishing* convincentes con seguridad HTTPS.

Las URLs de *phishing* combinan estos elementos con tácticas como: ***Typosquatting*, cadenas de redirecciones y parámetros codificados** enmascarando así su propósito mientras imitan a marcas de confianza.

El *Business Email Compromise* (BEC, Compromiso del Correo Electrónico Empresarial) es una forma sofisticada de ciberdelito en la que los atacantes usan el correo electrónico para engañar a las empresas y lograr transferencias de dinero o la obtención de información sensible. A menudo estos atacantes se hacen pasar por altos ejecutivos o socios de confianza, utilizando tácticas como facturas falsas o solicitudes urgentes para manipular a sus destinatarios. El objetivo es explotar la confianza y la autoridad asociadas a las cuentas de correo suplantadas para llevar a cabo actividades fraudulentas.

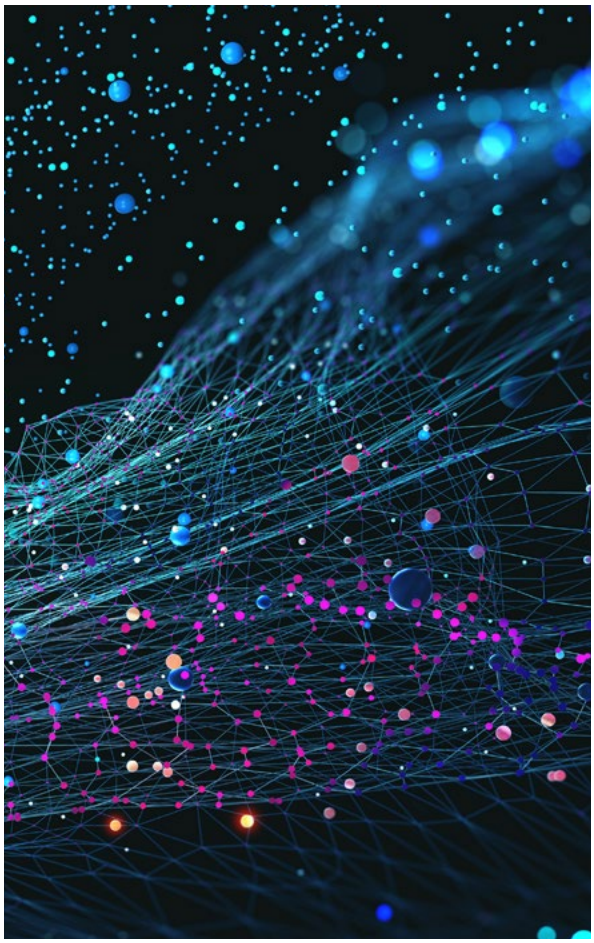
El BEC ha evolucionado con la integración de herramientas de IA generativa, lo que ha derivado en ataques más sofisticados y difíciles de detectar. Las medidas tradicionales de ciberseguridad tienen dificultades para mantenerse al día, lo que hace necesaria una estrategia de defensa en múltiples capas.

Las estafas BEC pueden implicar: Suplantación de cuentas de correo electrónico (*spoofing*), *spear phishing* y el uso de *malware* para infiltrarse en redes y lanzar solicitudes fraudulentas en el momento oportuno.

Los atacantes a menudo manipulan las reglas de bandeja de entrada para ocultar su actividad, se mueven de manera lateral dentro de las organizaciones, secuestran conversaciones ya iniciadas, alteran la autenticación multifactor (MFA) para mantener el acceso, explotan aplicaciones legítimas para exfiltrar buzones y ejecutan ataques discretos para evadir la detección.

En 2024, Sopra Steria gestionó varios casos significativos de *Business Email Compromise*. En una táctica observada se utilizaron **cuentas comprometidas de organizaciones externas del mismo sector** para enviar correos electrónicos de *phishing*. Al proceder de proveedores o socios conocidos, lograron eludir los filtros de correo de la empresa objetivo y explotaron la confianza inherente de los destinatarios.

En algunos incidentes observados por Sopra Steria, los atacantes utilizaron estas cuentas comprometidas para enviar correos electrónicos de *phishing* adicionales, ampliando aún más la propagación del ataque dentro de la organización.



> *Business Email Compromise* (BEC) ha evolucionado con la integración de herramientas de IA generativa, lo que ha derivado en ataques más sofisticados y difíciles de detectar.

VULNERABILIDADES

El año 2024 registró avances significativos en el panorama de las vulnerabilidades de ciberseguridad. Diversas fuentes[3]-[4] informaron de un aumento notable del número total de vulnerabilidades descubiertas respecto a 2023. Además, el número de vulnerabilidades explotadas creció aproximadamente un 20 %[5].

Entre las categorías de vulnerabilidades más destacadas se encuentra ***Cross-Site Scripting*** **(XSS)**, clasificada como la vulnerabilidad de software más crítica de 2024 por **MITRE** y la ***Cybersecurity and Infrastructure Security Agency*** **(CISA)**, superando a 2023 en un 10,2 %. Las vulnerabilidades de tipo ***Out-of-Bounds Write*** y ***SQL Injection*** también continuaron dominando el panorama de amenazas.

Estas categorías, incluidas en la lista ***MITRE 2024 CWE Top 25***, evidencian debilidades persistentes en los sistemas de software que los adversarios explotan con frecuencia para comprometer datos e interrumpir servicios.

---

[3] https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

[4] https://www.secpod.com/blog/the-cybersecurity-landscape-of-2024-key-insights-from-the-annual-vulnerability-report/

[5] https://vulncheck.com/blog/2024-exploitation-trends

Número de alertas de vulnerabilidad creadas por el SOC de Sopra Steria

Enero
- GitLabEE/CE
- Cisco Unified Communications
- Ivanti
- Citrix Netscaler
- Jenkins

Febrero
- Ivanti
- Fortnet

Marzo
- Cisco Secure Client

Abril
- xz/liblzma
- Palo Alto
- GlobalProtect
- Oracle
- Cisco
- ArcaneDoor

Mayo
- Checkpoint Security Gateway

Junio
- MOVEit Gateway/ Transfer
- GitLab pipeline

Julio
- Cisco Smart software
- Oracle
- Cisco Email Gateway
- OpenSSH
- Git cloning repositories
- Cisco Nexus Switch
- Citrix Netscaler
- GitLab

Agosto
- Windows TCP IP
- Apache HTTP Server

Septiembre
- GitLab CEÆE
- VMware Vcenter
- SolarWinds
- GitLab
- Cisco Smart Licensing
- Veeam
- Linux CUPS

Octubre
- Firefox
- WhatsUp Gold
- WatchGuard
- GitLab
- Junos
- Cisco ASA, FMC & FTD

Noviembre
- Palo Alto
- FortiOS SSLVPN
- Citrix Virtual Apps & Desktops
- Ivanti

Diciembre
- Apache Struts
- Cisco ASA
- Ivanti Cloud Services Application
- Privileged Remote Access (PRA) and Remote Support (RS) products
- Palo Alto PAN-OS
- Apache MINA framework

Abordar regularmente las vulnerabilidades de Windows a través de las actualizaciones de Patch Tuesday de Microsoft resulta beneficioso, ya que reduce la vida útil de dichas vulnerabilidades. En consecuencia, las empresas que programan sus actualizaciones de Windows en torno a estos lanzamientos se ven menos afectadas por fallos en productos de Microsoft.

Sin embargo, las vulnerabilidades en plataformas fuera del calendario de lanzamientos de Microsoft, como Fortinet, Cisco, Citrix y VMware, se han convertido en objetivos atractivos para actores maliciosos, con varios grupos criminales y patrocinados por Estados aprovechando estos *exploits* para llevar a cabo ataques de *ransomware* y operaciones de espionaje.

ENFOQUE EN LAS REDES PRIVADAS VIRTUALES

Durante 2024, los operadores de *ransomware* mantuvieron su foco en las soluciones VPN, tanto para explotarlas como para utilizarlas como punto de acceso con credenciales comprometidas. El enfásis de los ataques de *ransomware* se desplazó hacia la explotación de vulnerabilidades en tecnologías del perímetro de red, como VPNs e infraestructura de escritorio virtual, con frecuencia debido a la ausencia o a la falta de aplicación de la autenticación multifactor (MFA).

Fueron especialmente atacadas las soluciones de VPN basadas en *Secure Socket Layer/Transport Layer Security* (SSL/TLS), comúnmente conocidas como SSLVPN, WebVPN o VPN sin cliente (*clientless VPN*). Estas soluciones son objetivo frecuente de actores de amenazas debido a su alta exposición en internet público, lo que las hace visibles y accesibles para los atacantes.

La dependencia de prácticas y algoritmos de seguridad obsoletos agravó aún más el problema, haciendo que estas soluciones fueran vulnerables a ataques de fuerza bruta y otras técnicas. Además, muchas implementaciones genéricas de estas soluciones suelen carecer de mecanismos de autenticación robustos, confiando a menudo en autenticación de un solo factor fácilmente comprometible.

Por ello, el CCN-CERT, a través de su guía CCN-STIC 836 sobre seguridad en VPN, y el INCIBE, mediante sus artículos “Recomendaciones de seguridad en el empleo de redes VPN” y la publicación “Teletrabajo: VPN y otras recomendaciones” de INCIBE-CERT, recomiendan reforzar los mecanismos de acceso remoto con autenticación multifactor y sustituir soluciones de VPN basadas en SSL/TLS por alternativas más seguras.

Ejemplo

Vulnerabilidades notables, como aquellas que explotan Windows SmartScreen, recibieron especial atención debido a su explotación recurrente por parte de agentes maliciosos que buscaban eludir las medidas de seguridad integradas en Windows Defender. En particular, **CVE-2023-36025** fue aprovechada por grupos de ciberdelincuentes como **TA544** para desplegar el troyano de acceso remoto **Remcos** en ataques sofisticados dirigidos principalmente a instituciones en Europa.

La vulnerabilidad de omisión de la función de seguridad Windows SmartScreen (**CVE-2024-21351**) fue explotada activamente por numerosos grupos de *hacking*, quienes la utilizaron para infiltrarse en instituciones financieras y desplegar *malware* como **DarkGate** y **Phemedrone Stealer**.

Los productos **Connect Secure y Policy Secure de Ivanti** han recibido una atención significativa debido a varias vulnerabilidades críticas detectadas, beneficiarias para ciberdelincuentes, incluidos sofisticados grupos patrocinados por Estados.

«El enfoque de los ataques de *ransomware* se desplazó hacia la explotación de vulnerabilidades en tecnologías del perímetro de red, como las VPNs y la infraestructura de escritorio virtual, a menudo debido a la ausencia o a la falta de aplicación de la autenticación multifactor (MFA).»

Ejemplo

EXPLOTACIÓN DE LAS VULNERABILIDADES

A lo largo del año, los grupos de *ransomware* continuaron enfocándose en la explotación de vulnerabilidades de sistemas, una tendencia repetida en los últimos años. Se produjo un cambio notable con la disrupción de actores consolidados como **LockBit**, lo que llevó a la aparición de nuevas variantes de *ransomware* como **RansomHub, Fog y 3AM**. A diferencia de sus predecesores, estas nuevas cepas explotan vulnerabilidades a nivel de ejecución, en lugar de hacerlo a nivel de red o aplicación. Este cambio ha venido acompañado de medidas avanzadas de anti-detección, incluyendo el uso de contraseñas para bloquear el acceso a sistemas embebidos, lo que protege sus *payloads* y complica los esfuerzos de ingeniería inversa. Como consecuencia, estas medidas han obstaculizado de manera significativa los esfuerzos de detección y mitigación.

Un área significativa de explotación de vulnerabilidades se observó en la evolución de las técnicas de evasión utilizadas por ***stealers***, **troyanos** y ***loaders*** de *malware*. Además, *malware* como **Raspberry Robin** explotó vulnerabilidades en emuladores y entornos *sandbox* mediante el uso de librerías dinámicas virtuales (VDLLs). Al identificar y aprovechar vulnerabilidades en entornos *sandbox,* este *malware* logró evadir la detección de manera efectiva. De forma similar, **RedLine** aprovechó vulnerabilidades relacionadas con el análisis de lenguajes de programación menos comunes, como **Lua**, evadiendo los sistemas tradicionales de detección de *malware*, que no estaban preparados para procesar dichos lenguajes.

Otra tendencia observada durante 2024, fue un incremento de la explotación de vulnerabilidades más simples y accesibles. Los problemas de **inyección de comandos y de autenticación incorrecta** (*Improper Authentication*) fueron atacados con frecuencia, lo que refleja una tendencia de los ciberdelincuentes a preferir *exploits* de baja complejidad, pero de alto impacto. Un ejemplo de ello fue la vulnerabilidad de omisión de **autenticación en la interfaz web de gestión de Palo Alto Networks PAN-OS (CVE-2024-0012)**. Este hecho también fue evidente en el incremento de la explotación de vulnerabilidades de **inyección de comandos (CWE-77)**, como la vulnerabilidad en el **software Cisco NX-OS (CVE-2024-20399)** con una **puntuación CVSS de 6.7**. Esto ha derivado en un aumento de los ataques exitosos y en un mayor riesgo de filtraciones de datos y disrupciones en los sistemas.

OBJETIVO: INTERFACES DE PROGRAMACIÓN DE APLICACIONES

La adopción de APIs (Interfaces de Programación de Aplicaciones) se ha disparado, siendo esenciales para los microservicios, la proliferación de la IA y las arquitecturas impulsadas por contenedores, convirtiéndolas en un pilar clave de la innovación. Esta rápida adopción también ha ampliado la superficie de ataque para los grupos maliciosos, como lo demuestra un aumento del 80 % en las filtraciones de datos relacionadas con APIs en el último año. Estas brechas han expuesto más de 1.600 millones de registros, lo que subraya la urgencia de reforzar la seguridad de las APIs[6].

Las APIs son vulnerables a una amplia gama de amenazas, a menudo agravadas por su apertura. Estos riesgos incluyen filtraciones de datos y acceso no autorizado debido a configuraciones incorrectas o a una validación perimetral insuficiente. La facilidad para explotar APIs ha crecido, en particular con los avances en las capacidades de llamadas a APIs mediante IA, lo que ha democratizado el acceso, permitiendo que atacantes —independientemente de su nivel de experiencia— puedan analizar y explotar APIs de manera extensa y eficiente.

Ejemplo

Tanto los *malware loaders* como el *ransomware* se aprovecharon de las vulnerabilidades en las defensas de los sistemas. Las operaciones que involucraron a **GuLoader** y **Remcos** explotaron vulnerabilidades a partir de vectores de *phishing* por correo electrónico. GuLoader empleó técnicas complejas de evasión para manipular y eludir las defensas del sistema, mientras que Remcos explotó vulnerabilidades del sistema para mantener el control remoto, permitiendo posteriormente el despliegue de *ransomware*.

Ejemplo

La **fuga de secretos en un repositorio de GitHub**, que expuso 13 millones de secretos de API, demuestra que los atacantes valoran altamente estos secretos de API para utilizarlos en incidentes posteriores. Esto refleja los mismos patrones observados con las credenciales de usuario habituales.

[6] https://www.firetail.io/reports/the-state-of-api-security-2024

Insight

CIBERSEGURIDAD OT EN 2024

En 2024, vimos un aumento significativo del interés en la ciberseguridad OT en Europa, impulsado por el incremento de incidentes internacionales y el endurecimiento de las exigencias regulatorias. El *ransomware* continúa dominando como la amenaza más prevalente, dirigiéndose a industrias de todo tipo, desde la energía y la manufactura, hasta los servicios públicos. Mientras tanto, la creciente frecuencia de las explotaciones de vulnerabilidades *zero-day* y la reciente detección de herramientas avanzadas como **PipeDream** ponen de relieve el creciente estado de vulnerabilidad de los **sistemas de control industrial (ICS)**, que son críticos para la infraestructura moderna.

Los acontecimientos internacionales, como las repercusiones del ataque a la cadena de suministro de **SolarWinds** y las **resoluciones de responsabilidad de la SEC**, han intensificado aún más la atención sobre la seguridad en la cadena de suministro. Las organizaciones están adoptando cada vez más medidas como los controles de **lista de materiales de software** (SBOM, *Software Bill of Materials*) y los sistemas de inventario para abordar estos riesgos y garantizar el cumplimiento normativo.

Las presiones regulatorias también se han intensificado. Actualizaciones como la **Directiva NIS2**, el **Cyber Resilience Act (CRA)** y varias regulaciones sectoriales específicas han impulsado requisitos de cumplimiento más estrictos. Los operadores de infraestructuras críticas se enfrentan ahora a una mayor presión para implementar marcos de seguridad sólidos como la norma **IEC 62443**, identificar y gestionar los riesgos de ciberseguridad en su entorno OT (tecnología operacional) y desarrollar una mayor resiliencia en sus operaciones.

En medio de estos desafíos, está surgiendo un movimiento creciente hacia estrategias proactivas de ciberseguridad. Las organizaciones están adoptando medidas como la segmentación de redes, la detección de amenazas en tiempo real, los servicios SOC adaptados a entornos OT y programas integrales de formación para empleados. Estos esfuerzos sumados al cumplimiento normativo no solo abordan las amenazas inmediatas, sino que también sientan las bases para un enfoque más sólido y resiliente en la protección de infraestructuras críticas frente a un panorama de amenazas cada vez más sofisticado.

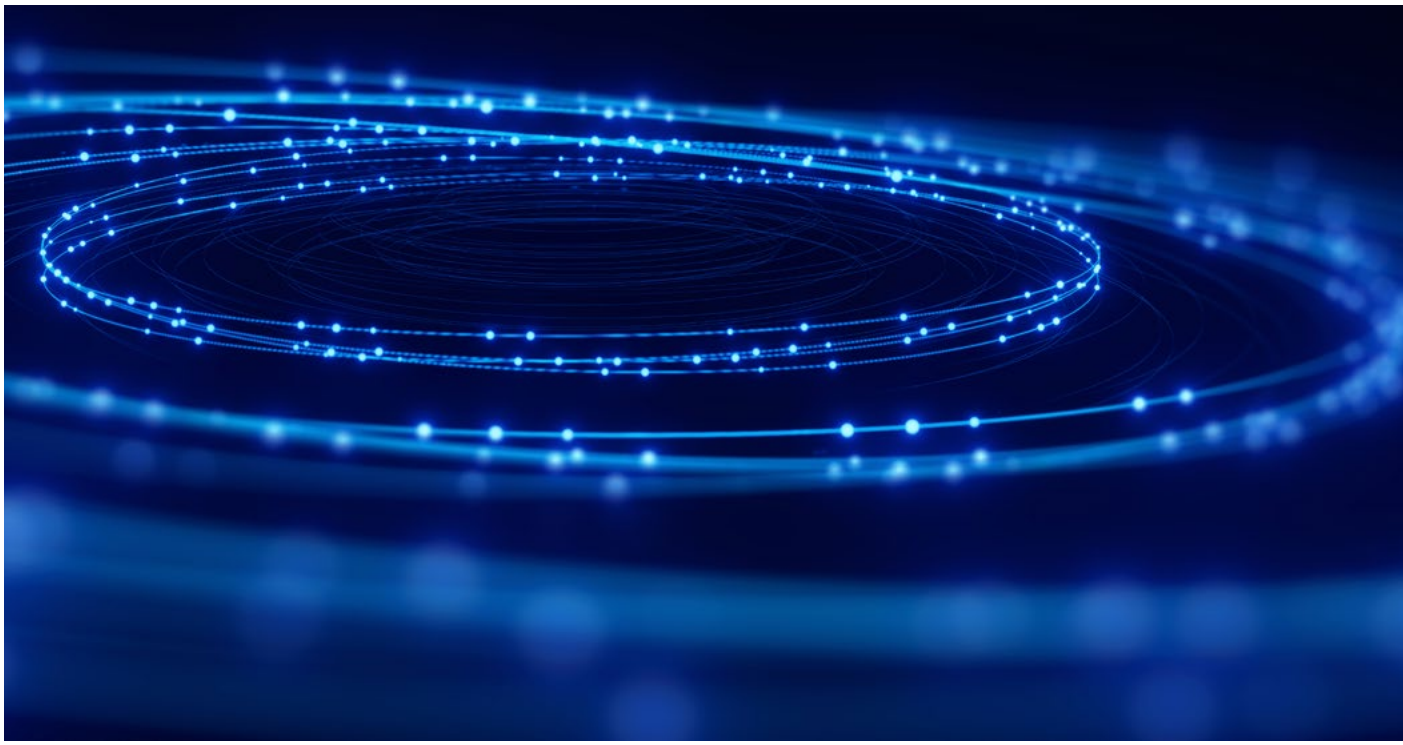
Dicho esto, la evolución hacia una protección y resiliencia adecuadas en las infraestructuras críticas, proporcionales a las posibles consecuencias de los incidentes, está lejos de terminar. Muchas organizaciones aún se encuentran en las etapas iniciales de implementación de las medidas de seguridad necesarias, y el camino por delante requerirá un enfoque sostenido, inversiones e innovación. Afortunadamente, observamos que algunos de nuestros clientes están estableciendo un estándar global en ciberseguridad OT, demostrando que la seguridad de primer nivel es alcanzable. Estos pioneros ofrecen una visión de lo que es posible, incluso mientras el panorama general sigue evolucionando y adaptándose a las amenazas emergentes.

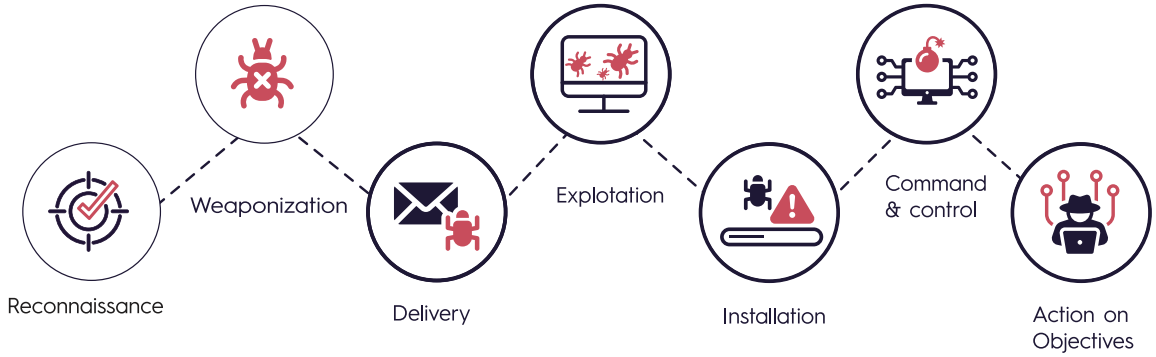
03. **Tras el** incidente

En 2024, los ciberdelincuentes siguieron utilizando una amplia gama de herramientas, *malware* y técnicas para llevar a cabo sus ataques, revelando tendencias en la evolución de las ciberamenazas. Ha habido una diversificación de métodos y un mayor aprovechamiento de software legítimo con fines maliciosos. Esta sección revela las tendencias de 2024 relacionadas con el *malware*, *stealers* y las herramientas de *hacking*.

Las observaciones de **Sopra Steria**, respaldadas por otros servicios de seguridad como **ENISA (Agencia de la Unión Europea para la Ciberseguridad)**, muestran que el *malware* ha experimentado un resurgimiento, especialmente a través del uso de *infostealers*. Algunos ejemplos son **RedLine, Raccoon Stealer, Vidar, Agent Tesla, FormBook y Lumma Stealer**. Cabe destacar que **Lumma Stealer** se ha observado de forma masiva en la base de clientes de Sopra Steria durante la segunda mitad de 2024.

> "Otro desafío para las defensas de ciberseguridad es el mayor uso de las tácticas *"Living-off-the-Land"*, en las que los atacantes utilizan herramientas y funciones legítimas de la infraestructura que están atacando, manipulando su funcionalidad para adaptarla a sus necesidades maliciosas.





MALWARE Y STEALERS

El *malware*, incluidos los virus, gusanos y troyanos, es un software diseñado para causar daño a un ordenador, servidor, cliente o red informática. Puede permitir el control sobre sistemas (p. ej., *botnets*), robar datos, otorgar acceso remoto (p. ej., troyanos de acceso remoto) o instalar software malicioso adicional (p. ej., *downloaders*), dependiendo del objetivo del atacante.

Los ciberdelincuentes crean o acceden a *malware* para llevar a cabo campañas cibernéticas, evadiendo defensas y controlando activos. A diferencia del *ransomware*, el *malware* es una amenaza distinta y persistente, con tácticas en evolución que ponen a prueba las defensas de ciberseguridad.

Otro desafío para las defensas de ciberseguridad es el creciente uso de tácticas ***"Living-off-the-Land"***, en las que los atacantes emplean herramientas y funciones legítimas de la infraestructura que están atacando, manipulando su funcionalidad para adaptarla a sus fines maliciosos. Aunque no se clasifican como *malware*, los atacantes pueden aprovechar estas herramientas con fines maliciosos, para ejecutar comandos no autorizados, descargar archivos maliciosos o evadir las medidas de seguridad.[7]

En la ***cyber kill chain***, el *malware* suele desempeñar un papel crucial en las fases de "entrega", "explotación" e "instalación". Durante la fase de entrega, el *malware* se introduce en el sistema objetivo, a menudo a través de archivos adjuntos en correos electrónicos, enlaces maliciosos u otros vectores. En la fase de explotación, aprovecha vulnerabilidades para ejecutar su carga útil en el destinatario. A continuación, en la fase de instalación, el *malware* se instala en el sistema para establecer una base que permita actividades maliciosas posteriores.

Dependiendo de sus capacidades, el *malware* también puede intervenir en fases posteriores, como "*Command and Control*" y "*Actions on Objectives*", permitiendo un control continuo y la consecución de los objetivos de los atacantes.

---

[7] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

DENTRO DE LOS SISTEMAS

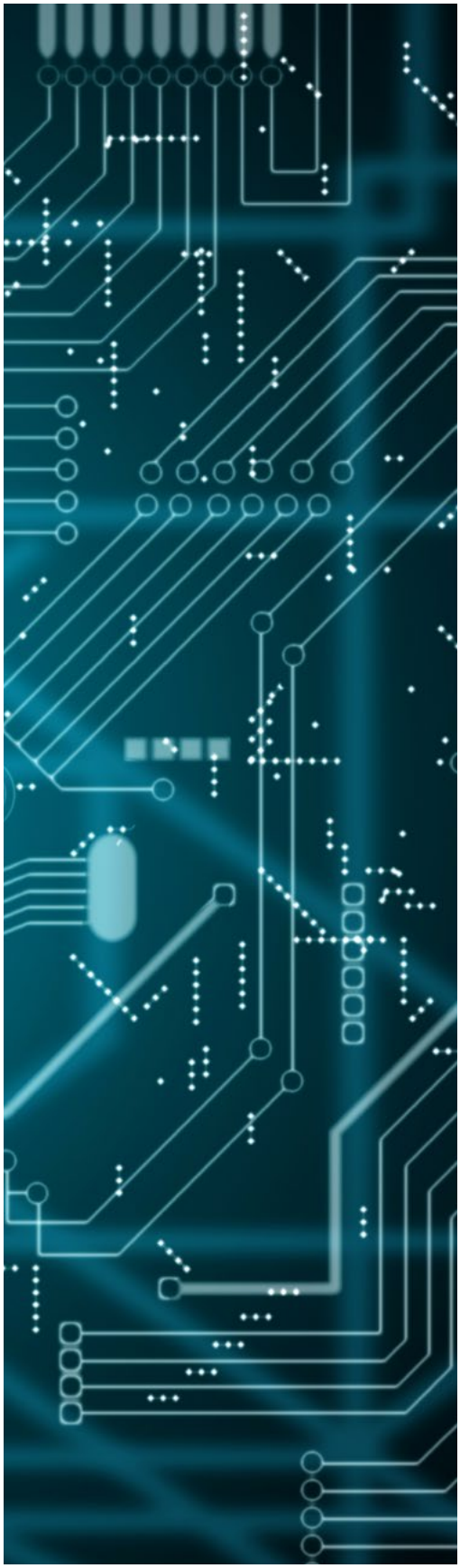
Sopra Steria detectó y bloqueó varias amenazas de *malware* destacadas dirigidas a clientes de Sopra Steria en 2024. El *malware* se asocia principalmente con la fase de **instalación** de la ***Cyber Kill Chain***. A menudo está diseñado para asegurar un punto de acceso inicial, facilitar la descarga de herramientas maliciosas adicionales o conceder a los atacantes un mayor acceso para posteriores intrusiones.

Los casos de *malware* representaron una proporción relativamente pequeña de todos los casos positivos reales gestionados por nuestro SOC. La mayor cantidad se registró durante la primera mitad de 2024. En promedio, el **10,1%** de todos los casos positivos reales gestionados por nuestro SOC estuvieron relacionados con *malware* en 2024. Esto excluye las instancias de *malware* que fueron bloqueadas automáticamente por el antivirus.

El **MaaS (*Malware-as-a-Service*)** es el modelo de negocio en el que los ciberdelincuentes ofrecen acceso a software malicioso e infraestructura relacionada a cambio de una tarifa, de forma similar al modelo legítimo de **SaaS (*Software-as-a-Service*)**. El MaaS, como los *infostealers* **Vidar y Lumma Stealer**, ha sido especialmente explotado por grupos de atacantes motivados por beneficios económicos, que también despliegan otras variantes de ladrones de información.

Los *infostealers* representan una amenaza en el panorama de la ciberseguridad, ya que los atacantes los utilizan habitualmente para recolectar credenciales de inicio de sesión e información sensible de sistemas comprometidos, lo que puede derivar en nuevas brechas, fraudes financieros o movimientos laterales dentro de una organización. Las credenciales suelen venderse en mercados clandestinos y desempeñan un papel crucial en las operaciones de acceso inicial, siendo a menudo el primer paso en intrusiones de múltiples etapas.

El aumento en el uso de *infostealers* está correlacionado con la mayor actividad de los **IABs (*Initial Access Brokers*)**, la expansión de las redes de distribución y la creciente sofisticación de las técnicas de evasión.



OBSERVADO Y BLOQUEADO

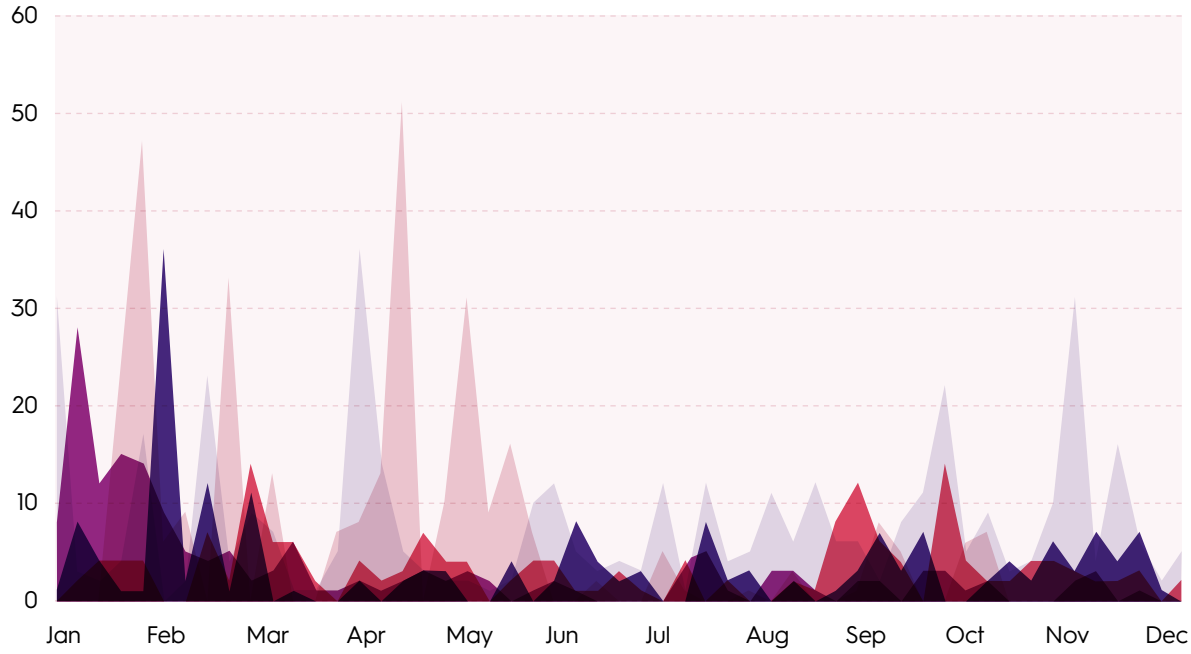
Hemos observado y bloqueado *malware* de uso común a lo largo de 2024, siendo los tipos Bearfoos, MediaArena, Phonzy, Plasti y Wacatac (denominación de Microsoft) los más destacados.

Estas fueron las cinco familias de *malware* más relevantes observadas en 2024:

Top 5 familias de *malware*

- Plasti
- Wacatac
- MediaArena
- Bearfoos
- Phonzy

Familias de *malware*



El *malware* más detectado por Sopra Steria durante 2024 corresponde a tipos que representan amenazas significativas para los sistemas informáticos y que comparten gran parte de su funcionalidad. Estas familias de *malware* se engloban en la categoría de ***commodity malware*** y comparten métodos de distribución muy similares. La infección suele producirse a través de archivos adjuntos maliciosos en correos electrónicos, sitios web infectados, descargas de software pirata o el uso de memorias USB comprometidas.

!

El *malware* de uso común (*commodity malware*) se refiere al software malicioso que está fácilmente disponible para su compra o descarga en la *dark web* u otras plataformas ilícitas. A diferencia del *malware* creado a medida para objetivos específicos, el *malware* de uso común se produce en masa y se vende a una amplia variedad de ciberdelincuentes. Este tipo de *malware* suele utilizarse en ataques amplios y oportunistas en lugar de en campañas dirigidas.

Wacatac, también conocido como **DeathRansom**, comenzó como un troyano y evolucionó a *ransomware*, cifrando archivos y exigiendo un rescate. Evita infectar sistemas en países de Europa del Este y está vinculado al *malware* **Vidar**. De forma similar, **Bearfoos** es un troyano que ataca a Windows, ejecutando comandos para robar datos, instalar *malware* y proporcionar acceso remoto a los atacantes. Esto pone de relieve la creciente sofisticación de las ciberamenazas.

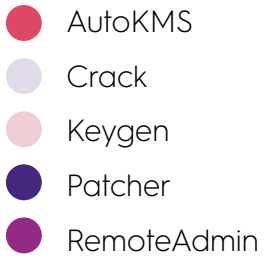
Además de los troyanos, **MediaArena** es un *browser hijacker* (secuestrador de navegador) que modifica la página de inicio y el motor de búsqueda, inyecta anuncios y redirige las búsquedas. También puede abrir pestañas con publicidad, forzar actualizaciones falsas y promover estafas, lo que agrava el panorama de las amenazas digitales.

Phonzy, conocido como **Trojan:Script/ Phonzy.A!ml**, roba datos, instala *malware* y permite el control remoto por parte de los atacantes. Esto subraya la necesidad de contar con medidas de ciberseguridad sólidas. De manera similar, **Plasti**, conocido como **TROJ_ PLASTI.A**, lleva a cabo acciones dañinas como el robo de datos, la instalación de *malware* y el acceso remoto a los atacantes.

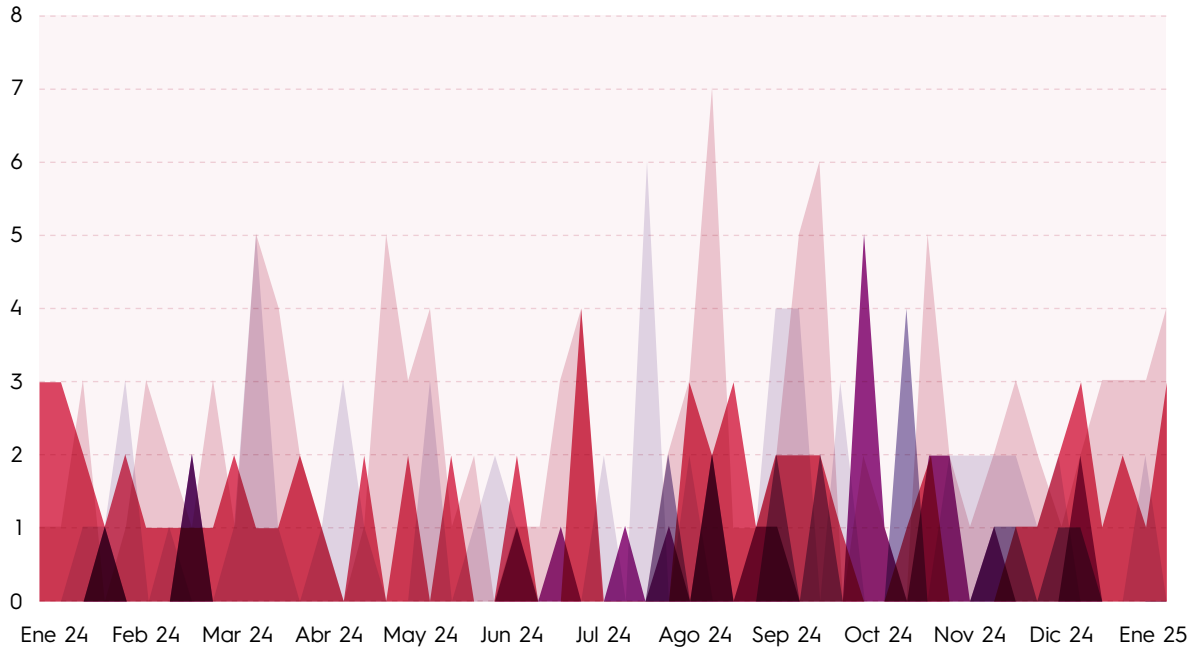
Otro tipo de software malicioso que Sopra Steria observa y bloquea son los ***hacktools***, que son programas o utilidades diseñados para ayudar a los atacantes en actividades de intrusión. Estas herramientas abarcan una gran variedad de aplicaciones y se utilizan habitualmente para obtener acceso no autorizado a un PC con el fin de insertar gusanos, virus y troyanos.

Esta sección se basa en la definición de ***hacktools* de Microsoft.** La compañía clasifica muchos **programas de *cracking* y *bypass* de licencias** como *hacktools*, los cuales son más frecuentes que las herramientas de *hacking* tradicionales como **Metasploit, Cobalt Strike, Brute Ratel y BloodHound.** Aunque sí encontramos instancias de estas herramientas en la base de clientes de Sopra Steria, no son tan comunes como los distintos tipos de software de *cracking* y *bypass* de licencias.

Top 5 familias de *Hacktool*



Familias de *Hacktool*

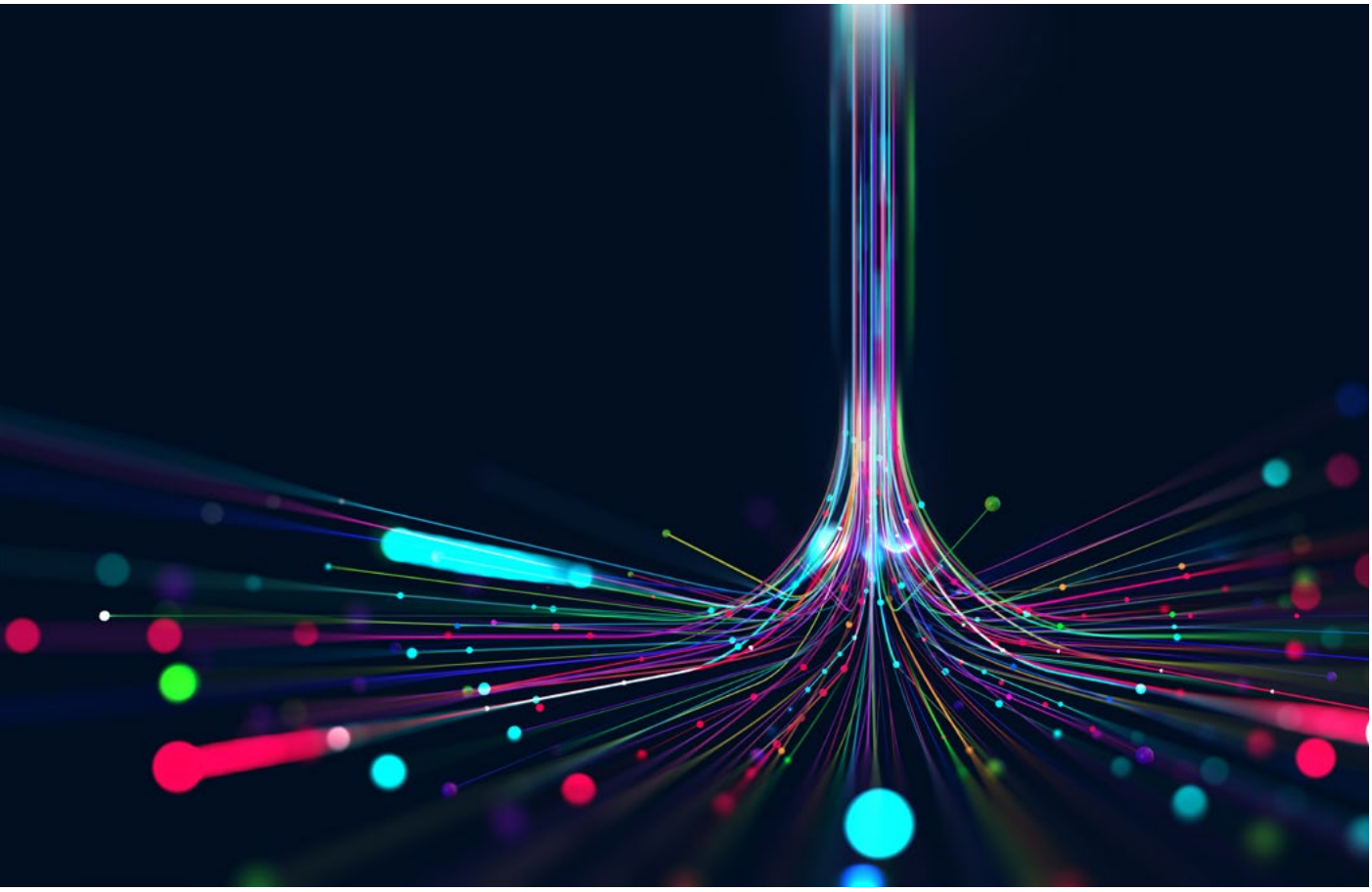


Los más destacados observados por **Sopra Steria** son los *hacktools* **AutoKMS, Crack, Keygen, Patcher y RemoteAdmin**. La mayoría de ellos son herramientas diseñadas para eludir los mecanismos de licencia de software, lo que implica riesgos tanto para la seguridad del sistema como para la legalidad.

AutoKMS, Crack y Keygen son *hacktools* utilizados para activar ilegalmente software no registrado o pirata mediante la evasión de los mecanismos de licencia. Aunque no son inherentemente maliciosos, a menudo vienen acompañados de *malware*, lo que genera vulnerabilidades de seguridad. **Patcher**, de forma similar, modifica el software para eludir las restricciones de licencia, con riesgos como la asociación con *malware* y vulnerabilidades de seguridad. El uso de estas herramientas infringe los acuerdos de licencia de software y las leyes de derechos de autor.

Por otro lado, ***RemoteAdmin*** está diseñado para proporcionar acceso remoto a un ordenador, permitiendo a un usuario controlar el sistema desde una ubicación diferente. Si bien las herramientas de administración remota pueden usarse con fines legítimos, como el soporte y la gestión de IT, también pueden ser explotadas por actores maliciosos para obtener acceso no autorizado a los sistemas. *RemoteAdmin* permite a los atacantes controlar un dispositivo como si estuvieran físicamente presentes, incluyendo el acceso a archivos, la ejecución de programas y la gestión de configuraciones del sistema.

> "En la *cyber kill chain*, el *malware* suele desempeñar un papel crucial en las fases de 'entrega', 'explotación' e 'instalación'."



ENVENENAMIENTO DE REPOSITORIO

En 2024, el panorama del ***malware* de código abierto** se expandió a un ritmo alarmante, planteando desafíos a la integridad de las cadenas de suministro de software. El año estuvo marcado por un aumento en la identificación de paquetes maliciosos, según los reportes de *OSINT*. A diferencia de los errores de codificación accidentales que derivan en vulnerabilidades, este *malware* de código abierto está diseñado intencionadamente para infiltrarse y explotar las cadenas de suministro haciéndose pasar por componentes legítimos.

Durante 2024, las **descargas en la sombra** (*shadow downloads*) se convirtieron también en una gran preocupación. Éstas ocurren cuando los paquetes maliciosos eluden a los gestores de repositorios y llegan directamente al ordenador del desarrollador o a la infraestructura compartida de *build*. Este proceso introduce dependencias no verificadas en los proyectos, debilitando los controles de seguridad establecidos e incrementando el riesgo de introducción de *malware*. Esto ha incrementado significativamente el riesgo, ya que los controles de seguridad se eluden con frecuencia, dejando a los sistemas expuestos frente a software no verificado. El volumen de estas descargas en la sombra se ha disparado, alcanzando **billones mensuales**, lo que pone de manifiesto una profunda brecha de gobernanza en las cadenas de suministro de software.

La naturaleza sigilosa del *malware* de código abierto y su capacidad de infiltrarse a través de repositorios aparentemente benignos lo hacen especialmente difícil de detectar. Los ecosistemas que alojan estos repositorios, como ***npm***, ***GitHub*** y ***PyPI***, se han convertido en puntos críticos por sus bajas barreras de entrada y la falta de verificaciones estrictas de identidad de los autores. Esto ha permitido a los atacantes introducir con facilidad diversos componentes maliciosos, explotando las brechas en la gestión de dependencias y en las canalizaciones de compilación para propagar su código malicioso.

Las organizaciones deben implementar medidas de seguridad estrictas para proteger sus cadenas de suministro de software. Esto incluye realizar revisiones de seguridad exhaustivas de los componentes de código abierto, emplear herramientas automatizadas para detectar paquetes maliciosos y mantener un plan de respuesta ante incidentes sólido para abordar posibles amenazas.

Ejemplo

Se ha observado a actores estatales utilizando repositorios de código para dirigirse principalmente a desarrolladores y obtener acceso, como el caso del **agente norcoreano *Moonstone Sleet*** que distribuyó *malware* a través de **repositorios de *npm*** para exfiltrar datos sensibles de monederos de criptomonedas.

En **marzo de 2024** se descubrió una puerta trasera en ***xz-utils***, un paquete de software que proporciona compresión sin pérdida para los desarrolladores. El código malicioso añadido a las **versiones 5.6.0 y 5.6.1 de *xz-utils*** modificaba su funcionamiento. La puerta trasera manipulaba ***sshd***, el archivo ejecutable utilizado para establecer conexiones remotas *SSH*. Cualquiera que dispusiera de una clave de cifrado predeterminada podía incrustar cualquier código de su elección en un certificado de inicio de sesión *SSH*, cargarlo y ejecutarlo en el dispositivo comprometido. El **incidente de la puerta trasera de *xz-utils*** generó un amplio debate dentro de la comunidad de seguridad. Una de las principales preocupaciones fue cómo el atacante que introdujo la puerta trasera logró pasar desapercibido durante tanto tiempo, evidenciando las posibles debilidades en los procesos de seguridad actuales.

Ejemplo

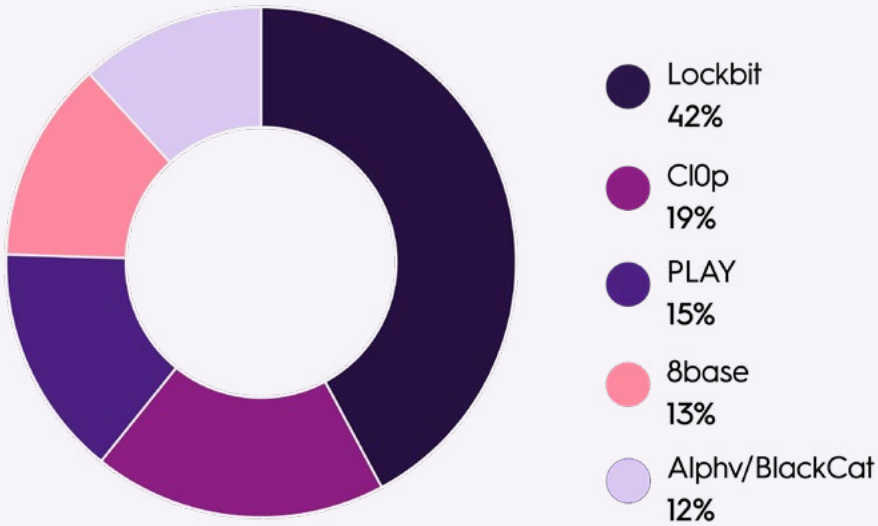
ECOSISTEMA *RANSOMWARE*

El modelo de ***RaaS, (Ransomware-as-a-Service)*** continuó desarrollándose durante 2024, permitiendo a los ciberdelincuentes delegar las operaciones de extorsión en operadores de *ransomware* a cambio de una parte de los beneficios o de un pago fijo. Este enfoque ha democratizado los ataques de *ransomware* al proporcionar herramientas listas para usar a afiliados sin experiencia.

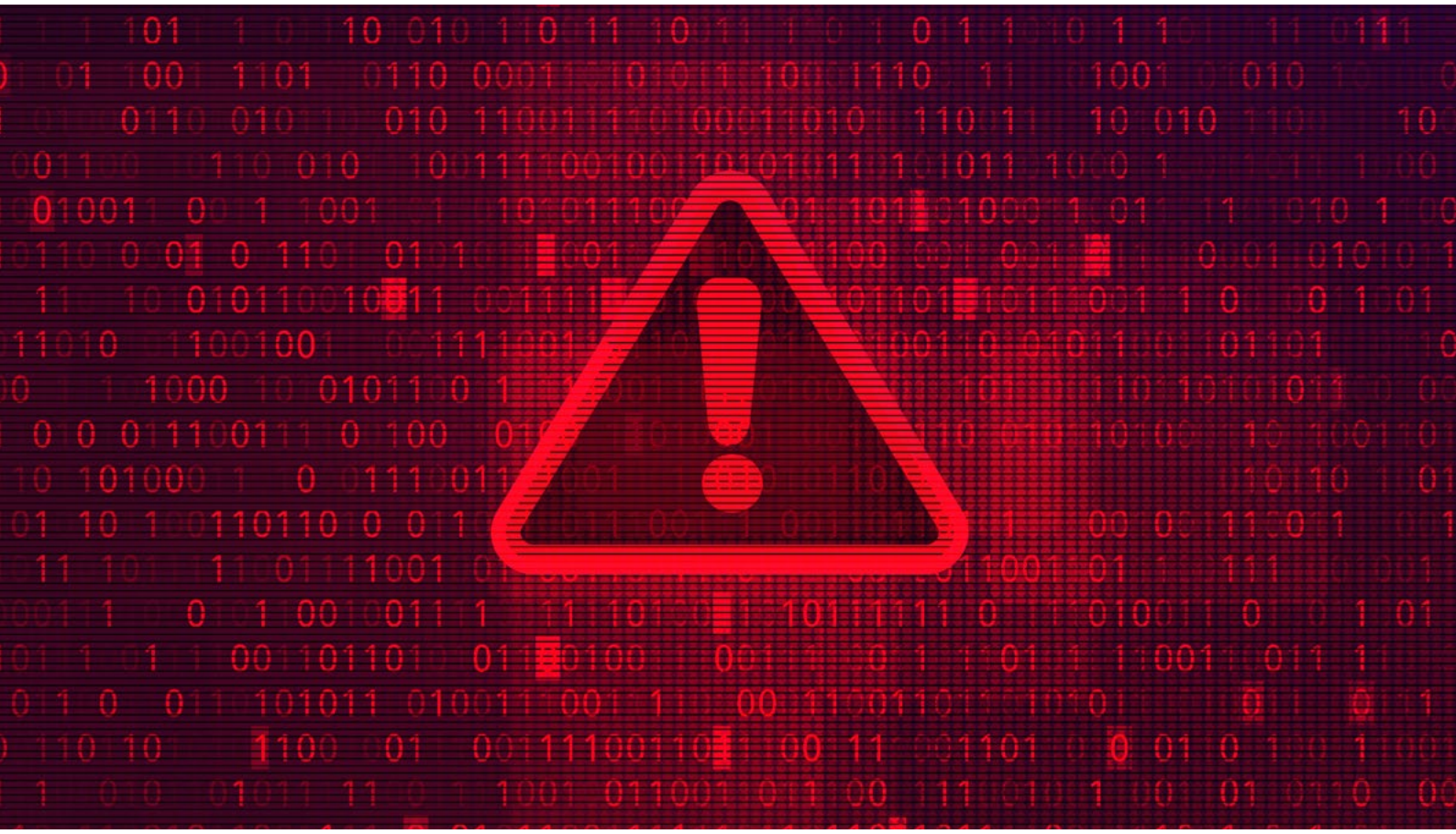
Los operadores RaaS desarrollan y mantienen la infraestructura, mientras que los afiliados ejecutan los ataques. Este modelo dificulta la atribución de los ataques y refuerza su resiliencia: el arresto de afiliados no afecta a los operadores, y los afiliados pueden cambiar de *kit* si es necesario. Entre los grupos de atacantes que explotan este modelo se encuentran ***Lockbit, DarkSide, REvil, Dharma y Akira.***

Los atacantes utilizan una combinación de herramientas nativas y descargadas para alcanzar sus objetivos finales, con un enfoque en el **robo y la exfiltración de datos**. Se observó a un afiliado de **Cactus**, usando una herramienta que exfiltraba automáticamente archivos a la nube durante una brecha de seguridad, posteriormente éstos fueron publicados en su sitio de filtraciones. Después, amenazaron con divulgar más información para ejercer presión sobre su víctima.

Los cinco grupos más activos de *ransomware* en 2024



Fuente: ENISA



04. PANORAMA DE AMENAZAS

En 2024, los objetivos de los actores de ciberamenazas, incluidos tanto los ciberdelincuentes como los grupos patrocinados por Estados, están evolucionando rápidamente, con cambios notables en sus **tácticas, técnicas y procedimientos (TTPs)**, tal y como se analizó anteriormente en este informe.

El cambiante panorama de amenazas plantea importantes desafíos, ya que los ciberdelincuentes son cada vez más sofisticados y efectivos, en gran medida debido a la **reducción de las barreras de entrada**. Su objetivo principal es acceder sin autorización a información sensible y sistemas, generalmente **con fines económicos**, empleando diversas técnicas de ataque avanzadas.

Con la transformación digital en curso, los ciberdelincuentes se han adaptado enfocándose cada vez más en las infraestructuras de red, los servicios de almacenamiento en la nube y las plataformas de *Software-as-a-Service* (*SaaS*), explotando una variedad de vulnerabilidades como la gestión inadecuada de parches, las configuraciones incorrectas, las *APIs* no seguras y el software obsoleto.
Se observa una tendencia creciente de paquetes de software malicioso diseñados para infiltrarse y explotar las cadenas de suministro haciéndose pasar por componentes legítimos.
Además, el *hacktivismo* está fuertemente influenciado por los conflictos geopolíticos, en particular los relacionados con Gaza, Israel-Irán y Ucrania.

Los actores estatales son contribuyentes clave al panorama de amenazas, utilizando recursos significativos para el espionaje y el robo de propiedad intelectual.
Llevan a cabo una labor exhaustiva de reconocimiento para preparar, y en ocasiones interrumpir, infraestructuras críticas, lo que subraya la complejidad y la gravedad de estas amenazas.
Actores destacados como el grupo chino patrocinado por el Estado Volt Typhoon, infiltraron redes de IT en Estados Unidos, con posibles intenciones de interrumpir infraestructuras críticas. De modo similar, Salt Typhoon vulneró a compañías de telecomunicaciones en varios países.
Es probable que esto se hiciera para acceder a gran escala a datos de tráfico telefónico en forma de registros de detalle de llamadas y, posiblemente, también al contenido de las comunicaciones de un conjunto más amplio de llamadas telefónicas. Ambos tipos de información pueden tener un alto valor para el atacante de cara a su explotación posterior.

Sus métodos no convencionales evidencian un entorno de amenazas en alza, con entornos comprometidos en sectores clave como las telecomunicaciones y la energía.

VOLATILIDAD DE LOS GRUPOS DE *RANSOMWARE*

En 2024, varios grupos de *ransomware* fueron creados y disueltos. Este hecho no es exclusivo de ese año, pero se observaron cambios significativos causados por acciones judiciales que involucraron a múltiples países, como la operación de febrero contra el grupo LockBit gracias a una vulnerabilidad de *PHP* sin parchear en su sitio web.

Aunque no eliminó a LockBit, sí redujo significativamente su nivel de amenaza. Como resultado de la operación, se disolvieron claves de cifrado y se entregaron a sus víctimas, mostrando cómo los esfuerzos y la coordinación internacional marcan la diferencia.

Sin embargo, la desaparición de un grupo de *ransomware* no implica necesariamente una disminución de la actividad general de *ransomware*. De hecho, los grupos pueden cambiar de nombre con el tiempo, pero muchos de los actores implicados suelen seguir siendo los mismos. Por ejemplo, la operación *RansomHub*, activa desde principios de 2024, ha atraído a una oleada de afiliados que abandonaron las operaciones de LockBit (y BlackCat).

> "La proliferación de *infostealers* ha provocado un aumento de los incidentes de filtración de datos, a menudo facilitados por el uso de credenciales robadas."

OBSERVACIONES CLAVE

La proliferación de *infostealers* ha provocado un aumento de los incidentes de filtración de datos, a menudo facilitados por el uso de credenciales robadas. Los ciberdelincuentes utilizan con frecuencia infraestructuras maliciosas y servicios públicos en la nube para alojar *malware* y exfiltrar información.

Mientras tanto, las campañas de *ransomware* y destructivas siguen siendo dominantes, con operadores que emplean modelos de *Ransomware-as-a-Service* (*RaaS*) para ampliar sus capacidades de ataque y dirigirse a un espectro más amplio de víctimas. Estos actores no sólo cifran y roban datos, sino que también utilizan la amenaza de la exposición pública para extorsionar pagos, aprovechando a menudo el almacenamiento en la nube para las transferencias de datos.

Además, los grupos de *ransomware* sofisticados son utilizados cada vez más por actores estatales para obtener información sobre los datos de otras naciones, infraestructuras críticas u otra información de valor.

Las observaciones indican un mayor nivel de sofisticación en los métodos de exfiltración para evadir las medidas de seguridad. En respuesta al desarrollo, por parte de la industria de la ciberseguridad, de métodos de detección diseñados específicamente para defenderse de la amenaza latente de los *infostealers*, los ciberdelincuentes están intentando eludir la detección innovando con herramientas de archivado o protocolos de exfiltración alternativos.

También se ha producido un aumento en el uso de técnicas de exfiltración, como la exfiltración hacia almacenamiento en la nube y el uso de canales cifrados. Esto refleja la adaptación de los atacantes al creciente uso de soluciones en la nube para llevarlo a cabo, al mismo tiempo que protegen su comunicación.

Además, este método de exfiltración basado en la nube busca camuflarse en el ruido del tráfico de datos, considerando que muchas empresas almacenan su información en nubes de terceros.

Herramientas como Cobalt Strike, Mimikatz, PsExec, RClone y PowerShell siguen siendo ampliamente utilizadas por los atacantes, lo que refleja tanto su efectividad como su versatilidad en los ataques —ya sea para movimientos laterales, exfiltración o la recopilación de datos sensibles—.

Esto subraya la necesidad crítica de contar con reglas de detección específicas que permitan identificar tanto el uso extendido de herramientas de *hacking* como el uso malicioso de herramientas legítimas.

INTELIGENCIA ARTIFICIAL

En 2024, vimos un progreso notable en el ámbito de la inteligencia artificial (IA), particularmente en el campo de la IA generativa, con nuevos modelos más potentes disponibles casi semanalmente, mostrando mejoras significativas en calidad, precisión y capacidad de procesamiento de información. Muchos modelos también introdujeron la multimodalidad completa, donde la entrada y la salida ya no se limitaban únicamente al texto, sino que también incluían imágenes, audio y video, otorgando a los modelos la capacidad de ver y escuchar. Si bien el mercado sigue estando en gran medida dominado por OpenAI, Microsoft, Google, Meta y Amazon, también se observa un auge de modelos open-source y de terceros desarrollados por empresas más pequeñas que rivalizan con los modelos de mayor tamaño. Asimismo, se han introducido nuevas capacidades que permiten ejecutar los modelos en *hardware* local, lo que posibilita procesar imágenes, video, audio y texto dentro de la propia infraestructura o en el *edge*.

Este año, muchas organizaciones comenzaron a utilizar IA generativa para el desarrollo de aplicaciones (GitHub Copilot) y la colaboración (Microsoft 365 Copilot), y otras están en fases iniciales de evaluación del uso de IA generativa para la automatización de procesos empresariales.

Un riesgo al que muchas empresas se han enfrentado este año es el de la **Shadow GenAI**, donde los empleados comenzaron a utilizar alguna de las miles de herramientas y servicios de GenAI disponibles en el mercado con datos corporativos, sin conocer cómo los diferentes servicios procesan la información. Esta falta de visibilidad y control genera posibles vulnerabilidades de seguridad, problemas de cumplimiento normativo y la posibilidad de filtraciones de datos sensibles.

También ha habido un aumento de ciberdelincuentes e incluso agentes estatales que utilizan IA generativa para:

- **Generar contenido *deepfake*** con la intención de llevar a cabo ataques de ingeniería social o manipular la opinión pública mediante información falsa, particularmente en relación con asuntos políticos o conflictos internacionales en curso.
- **Nuevos métodos de ingeniería social** mediante IA generativa para replicar la voz o el rostro de una persona. Las mejoras en los modelos y el hardware han hecho posible generar vídeos *deepfake* en tiempo real, incluso en llamadas de Microsoft Teams.
- **Generar nuevo código malicioso**, como *malware*, virus o troyanos. Aunque la calidad del *malware* generado por la IA generativa es actualmente bastante baja, se espera que, con las mejoras en los modelos, esto se convierta en un riesgo mayor en los próximos años.

Afortunadamente, muchos proveedores de IA han añadido más garantías en sus modelos para prohibir este tipo de abusos. Sin embargo, lo que estamos observando ahora es que los ciberdelincuentes están encontrando nuevos métodos para evadir estas

> Un riesgo al que muchas empresas se han enfrentado este año es el de la Shadow GenAI, donde los empleados comenzaron a usar alguna de las miles de herramientas y servicios de GenAI en el mercado con datos corporativos, sin conocer cómo los distintos servicios procesan la información."

protecciones mediante una técnica llamada **inyección de *prompts***.

Otra tendencia emergente es el uso de agentes virtuales, donde se combina la IA generativa con un agente virtual que dispone de un conjunto de integraciones predefinidas y un conjunto de instrucciones. Estos agentes pueden asumir una variedad de tareas, como recopilar información o realizar labores de reconocimiento mediante herramientas como AutoGPT, Autogen o MetaGPT. También pueden gestionar pruebas de seguridad automatizadas utilizando marcos como PentestGPT. Estos entornos de agentes se están volviendo tan potentes que ya pueden emplearse para realizar ataques automatizados, e incluso interactuar localmente con ordenadores mediante funciones como las APIs de Anthropic Compute Use, o ejecutarse en un entorno virtualizado.

Si bien no prevemos que los ciberataques impulsados por IA se conviertan en la norma a corto plazo, sí observamos que los ciberdelincuentes están utilizando la IA generativa como apoyo. Es probable que la IA asista en el desarrollo de *malware* y *exploits*, en la investigación de vulnerabilidades y en el movimiento lateral, haciendo que las técnicas existentes sean más eficientes. Sin embargo, a corto plazo, estas áreas seguirán dependiendo de la experiencia humana.

La IA también reducirá las barreras para que ciberdelincuentes novatos y *hacktivistas* lleven a cabo operaciones de acceso y recopilación de información.

La IA generativa se convertirá en un tema aún más importante en los próximos años, con cada vez más empresas buscando aprovechar esta tecnología en múltiples áreas de negocio.

05. RECOMENDACIONES **PARA LA DEFENSA**

Las organizaciones deben adoptar un enfoque integral de la seguridad, incorporando la resiliencia en el núcleo de sus operaciones para gestionar con eficacia un entorno digital en rápida evolución. Es importante implementar pruebas basadas en amenazas y reforzar la capacidad de respuesta ante incidentes. Los esfuerzos de seguridad deben ser dinámicos y adaptarse continuamente al cambiante panorama de amenazas.

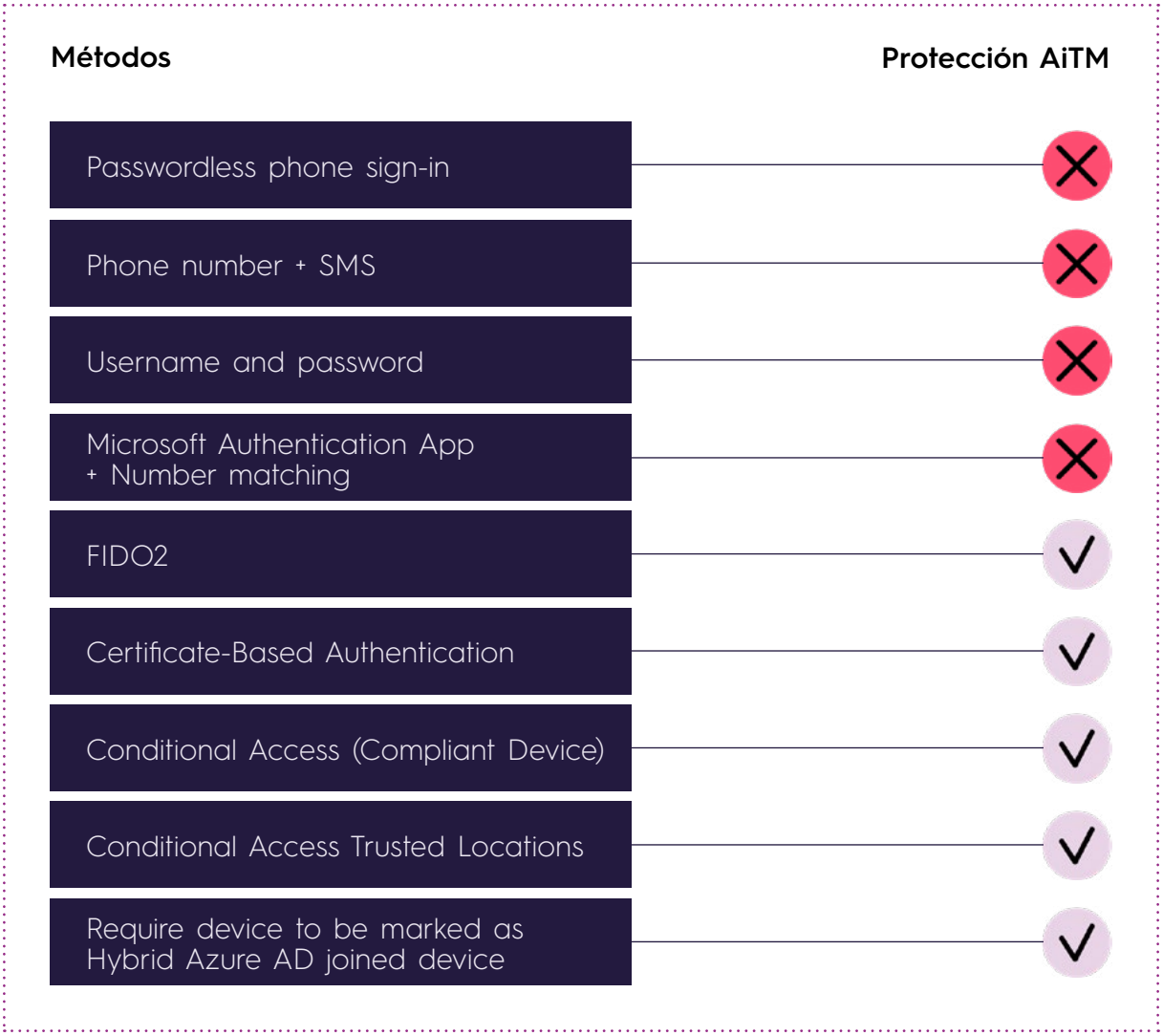
Muchas de las tendencias de la ciberdelincuencia reportadas globalmente en 2024 reflejan las observaciones e incidentes registrados por Sopra Steria. El *phishing*, con sus nuevos métodos, constituye la mayor categoría de incidentes de seguridad gestionados por nuestro *Security Operation Center* (SOC) en 2024. La cobertura de las herramientas EDR (*Endpoint Detection and Response*) es crucial para detectar y responder ante actividad maliciosa. Recomendamos que todas las organizaciones adopten los principios fundamentales de NSM para la seguridad TIC. Aquellas organizaciones que han desarrollado un mayor nivel de madurez de seguridad —incluyendo una buena política de parches, un inventario de activos y control sobre los puntos de acceso expuestos— tienen más facilidad para proteger su infraestructura y experimentan menos incidentes.

PHISHING

Defenderse contra la suplantación de identidad requiere un enfoque en múltiples capas para protegerse eficazmente de estos ataques engañosos. La autenticación multifactor (MFA) para todas las cuentas de usuario es una necesidad. Con el aumento del *phishing* AiTM (Adversary-in-the-Middle), se debe optar por MFA resistente al *phishing*. Es fundamental formar regularmente a los empleados sobre cómo reconocer y reportar intentos de *phishing*, ya que la vigilancia humana constituye una línea de defensa crucial. También se deben utilizar herramientas y servicios avanzados anti-*phishing* que puedan monitorizar, bloquear y filtrar intentos en tiempo real, reduciendo así las posibilidades de que los correos maliciosos lleguen a la bandeja de entrada.

- **Habilitar una autenticación multifactor (MFA) sólida**: Implementar MFA en todas las cuentas de usuario para protegerse contra técnicas avanzadas de *phishing*. Idealmente, utilizar MFA resistente al *phishing*.
- **Formación en concienciación de usuarios**: Formar regularmente a los empleados para identificar y reportar intentos de *phishing*.
- **Herramientas y servicios anti-*phishing***: Utilizar herramientas que supervisen, bloqueen y filtren intentos de *phishing* en tiempo real.

Métodos de autentificación



VULNERABILIDADES

Las organizaciones deben priorizar la seguridad de sus APIs implementando mecanismos sólidos de autenticación y autorización, pruebas de seguridad regulares y monitorización continua, garantizando al mismo tiempo una configuración y validación adecuadas para mitigar los riesgos asociados.

Además, es crucial actualizar las soluciones VPN a alternativas más seguras y aplicar la autenticación multifactor (MFA) para controlar y proteger todos los puntos de acceso expuestos, asegurando que solo haya accesos autorizados. La actualización y el parcheo regular del software VPN, combinados con mecanismos de autenticación robustos, pueden reducir significativamente los riesgos.

Asimismo, las organizaciones deben priorizar el parcheo y las actualizaciones regulares en todos los aspectos de su infraestructura, incluidos los dispositivos de red, los sistemas de virtualización y las aplicaciones independientes. Con tiempos de explotación de vulnerabilidades cada vez más reducidos —los adversarios ahora pueden explotarlas en un promedio de apenas cinco días—, el parcheo a tiempo es más crítico que nunca.

- **Parcheo y actualizaciones regulares:** Priorizar el parcheo y las actualizaciones regulares para mitigar los riesgos asociados a vulnerabilidades.
- **APIs y tecnologías de *streaming* seguras:** Implementar mecanismos sólidos de autenticación y autorización, pruebas de seguridad regulares y monitorización continua.

[8] https://socradar.io/top-10-exploited-vulnerabilities-of-2024/

MALWARE

Defenderse contra el *malware* exige de una combinación de medidas preventivas y de monitorización. Es fundamental asegurarse de que el software antivirus esté instalado en todos los dispositivos y se mantenga actualizado para detectar y eliminar cualquier software malicioso.

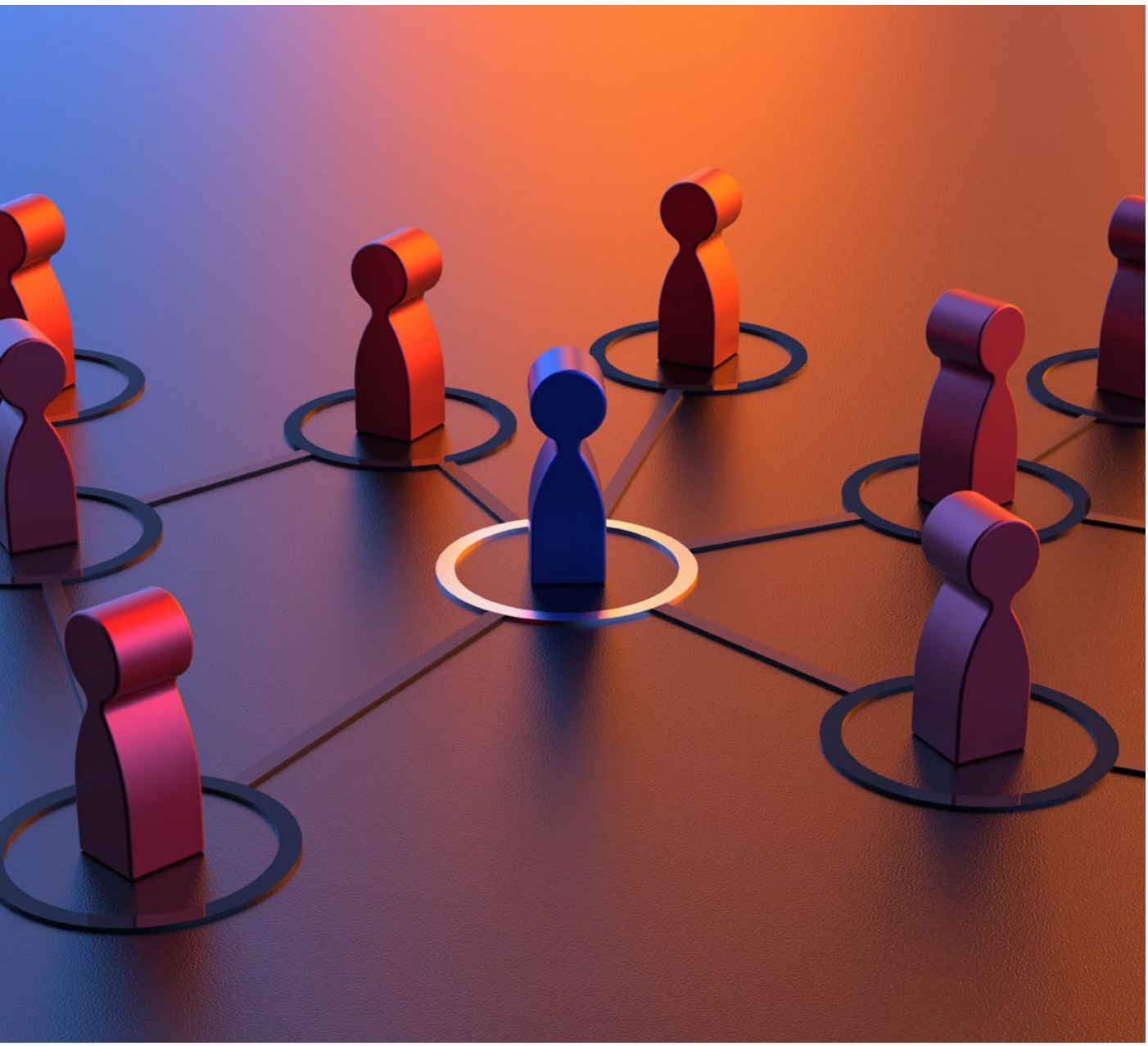
Implementar herramientas de monitorización de red ayuda a detectar actividades inusuales que puedan indicar la presencia de *malware*. Además, es importante formar a los empleados sobre los riesgos de descargar y abrir archivos sospechosos o hacer clic en enlaces desconocidos no verificados, ya que éstos son métodos comunes de distribución de infección.

Asimismo, se recomienda emplear soluciones de *Endpoint Detection and Response* (EDR) para monitorizar la actividad de los *endpoints* y responder rápidamente a posibles amenazas:

- **Visibilidad de dispositivos e inteligencia de amenazas en tiempo real:** Supervisar el tráfico de red con analítica avanzada y mantenerse informado sobre amenazas emergentes.

- **Instalar y actualizar el software antivirus:** Garantizar que el antivirus esté instalado y se actualice regularmente.

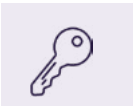
- **Fortalecer la detección de exfiltración de datos:** Implementar reglas de detección específicas para identificar el uso extendido de herramientas de *hacking* y el uso malicioso de herramientas legítimas.



PERSPECTIVA DEL *PEN-TESTER*

Durante el último año, el equipo de pruebas de penetración (*penetration testing*) ha identificado varias vulnerabilidades y debilidades recurrentes entre los clientes. Muchos problemas fundamentales y han persistido con los años, lo que mantiene su relevancia.

Estas vulnerabilidades continúan brindando a los atacantes de oportunidades escalar privilegios y lograr un impacto significativo, lo que subraya la importancia de abordarlas de manera eficaz.



Principales hallazgos de las pruebas de penetración

- **Mala elección de contraseñas:** La mala gestión de contraseñas sigue siendo algo que se explota con frecuencia para obtener acceso a dominios. Mediante ataques de *password spraying*, utilizando contraseñas simples y predecibles, a menudo se logra acceso no autorizado a cuentas de usuario, servicio y administrador.

- **Archivos sensibles en recursos compartidos:** Con frecuencia se encuentran archivos de configuración que contienen cadenas de conexión en texto plano, *tokens,* contraseñas y otros datos sensibles en recursos compartidos. Esto proporciona a los atacantes oportunidades directas para la escalada horizontal y la exposición de información crítica. La falta de controles de acceso adecuados y de registros agrava aún más este problema.

- **Plantillas de certificados vulnerables:** Las plantillas de certificados mal configuradas son un problema recurrente, ya que permiten la escalada de privilegios. Se han dado casos en los que usuarios comunes han podido obtener derechos de administrador del dominio debido a configuraciones incorrectas en las plantillas de certificados.

- **Mala configuración:** Las configuraciones incorrectas siguen siendo un problema habitual, Con ejemplos que incluyen:
  - Configuraciones débiles en plataformas en la nube, lo que conduce a accesos no deseados a datos o recursos sensibles.
  - Segmentación de red mal implementada, que facilita el movimiento lateral de los atacantes dentro del entorno.

- **Problemas de autorización y Cross-Site Scripting en aplicaciones web:** Con frecuencia encontramos implementaciones de autorización débiles o ausentes en APIs y aplicaciones web. Estas vulnerabilidades han dado lugar a accesos no autorizados a datos y sistemas sensibles, así como a la posibilidad de realizar acciones indebidas. En algunos casos, esto ha permitido escalar privilegios tanto verticalmente (obteniendo permisos de mayor nivel) como horizontalmente (accediendo a datos de otros usuarios).

  Además, se indentifican a menudo vulnerabilidades de *Cross-Site Scripting* (XSS) en aplicaciones web. Estos fallos permiten inyectar *scripts* maliciosos que pueden comprometer sesiones de usuario, modificar sitios web o robar información sensible.

> // El uso de contraseñas inseguras o mal gestionadas sigue siendo algo que se explota con frecuencia para obtener acceso a dominios.

Recomendación para mejorar la seguridad

- **Fortalecer las prácticas de contraseñas:** Aplicar políticas de contraseñas robustas y MFA obligatoria en todos los sistemas críticos. Bloquear el uso de contraseñas simples o comúnmente utilizadas.
- **Revisar los permisos de acceso:** Auditar regularmente las áreas de archivos compartidos y asegurarse de que la información sensible no se almacene sin las protecciones adecuadas.
- **Endurecer las configuraciones:** Revisar y actualizar las configuraciones, incluidas las plantillas de certificados, para alinearlas con las mejores prácticas.
- **Probar los mecanismos de autorización:** Realizar *testing* periódico en aplicaciones web para garantizar que la autorización esté correctamente implementada y evitar el acceso a datos sensibles sin permisos válidos.

OUTLOOK **2025**

En 2025, es muy probable que el uso de la inteligencia artificial (IA) en los ciberataques sea aún más sofisticado y fácil de llevar a cabo. Los ciberdelincuentes emplearán cada vez más la IA para crear correos de *phishing* y ataques de ingeniería social altamente convincentes, imitando el comportamiento y los patrones de lenguaje humano con mayor precisión, lo dificultará su detección.

La tecnología *deepfake* también será utilizada por muchos ciberdelincuentes para generar vídeos y grabaciones de audio realistas con fines de robo de identidad, fraude y evasión de medidas de seguridad, permitiendo a los atacantes suplantar la identidad de usuarios con acceso legítimo y obtener acceso no autorizado a información sensible.

Además, en el ámbito de las operaciones de la información, la IA se aprovechará para acelerar la creación de contenidos fraudulentos, produciendo personas ficticias más persuasivas. Esto aumentará la capacidad de los ciberdelincuentes para influir en la opinión pública y llevar a cabo campañas de desinformación.

En general, la integración de la IA hará que los ciberataques sean más sofisticados, escalables y difíciles de defender, por lo que las organizaciones deberán invertir en medidas de seguridad avanzadas y en una monitorización continua para mantenerse a la vanguardia de estas amenazas en constante evolución.

En paralelo, el valor que los ciberdelincuentes otorgan a las credenciales robadas seguirá siendo alto, tal y como se observa en varias tendencias clave de 2024. A lo largo de este año, hubo un aumento significativo en el uso de credenciales legítimas para el acceso inicial en ciberataques. El mercado de credenciales comprometidas, a menudo obtenidas con *infostealers*, continuó prosperando.

Los atacantes reconocieron que incluso con una sola credencial de empleado —que podía obtenerse por tan solo 10 dólares— podía desencadenar incidentes de seguridad de gran impacto. Es muy probable que esta tendencia persista en 2025, ya que la demanda de dichas credenciales sigue siendo alta debido a su efectividad para obtener acceso no autorizado a sistemas.

Las organizaciones deberán priorizar la seguridad de las credenciales, incluyendo métodos seguros de autenticación y monitorización continua, para mitigar los riesgos asociados al robo de credenciales.

A medida que los grupos criminales continúen especializándose, es probable que esta tendencia se mantenga o incluso se intensifique en 2025, para responder a las crecientes demandas del mercado del cibercrimen. Es probable que veamos grupos enfocados exclusivamente a un área muy específica, como la exfiltración o la explotación de infraestructuras en la nube.

Además, las colaboraciones entre estos grupos podrían volverse cada vez más frecuentes, con alianzas temporales creadas para campañas específicas o para compartir recursos, como vulnerabilidades e infraestructuras.

Los grupos de APT (Amenazas Persistentes Avanzadas) alineados con Estados están colaborando cada vez más con ciberdelincuentes, particularmente en el uso de *ransomware*, IABs (*brokers* de acceso inicial) y ataques destructivos. Esta colaboración difumina la línea entre el cibercrimen y los ataques patrocinados por Estados, lo que impacta de manera significativa en la atribución y en la gestión de la seguridad en general.

Además, la Directiva NIS2, aprobada recientemente por la Unión Europea, tiene como objetivo mejorar significativamente la colaboración entre los Estados miembros de la UE en la lucha contra la ciberdelincuencia. Además de contribuir a una mayor protección de los sistemas, probablemente influirá en los esfuerzos preventivos y operativos de las fuerzas del orden, las agencias de inteligencia y los distintos CSIRTs (*Computer Security Incident Response Teams*) de cada país.

La directiva promueve un aumento y estandarización en la notificación de incidentes, una mejora en el intercambio de información, el refuerzo de los mecanismos de cooperación y un marco legal más armonizado.

Probability Matrix				
Highly Unlikely	Unlikely	Even Chance	Likely	Highly Likely
<10%	**10-40%**	**40-60%**	**60-90%**	**>90%**

" Los grupos de APT (Amenazas Persistentes Avanzadas o *Advanced Persistent Threat*) alineados con Estados están colaborando cada vez más con ciberdelincuentes, en particular en el uso de *ransomware*, IABs (*brokers* de acceso inicial) y ataques destructivos.

CÓMO TE PUEDE AYUDAR **SOPRA STERIA**

Basándonos en nuestras observaciones a lo largo de 2024, queda mucho por abordar para alcanzar un nivel de seguridad aceptable. La amenaza en el ámbito cibernético sigue creciendo, y su ritmo va en aumento.

En Sopra Steria contamos con más de 300 expertos que ayudan a las organizaciones a reducir la probabilidad de éxito en un ciberataque mediante la reducción sistemática del riesgo y el incremento medible de la madurez en seguridad.

Si en 2025 solo va a enfocarse en "tres aspectos", es importante que sea en estas áreas clave para maximizar el impacto en seguridad:

Mejor gestión del *phishing*

- Formar y sensibilizar a los empleados sobre *phishing* a través de correo electrónico, chat y teléfono.
- Implementar herramientas anti-*phishing* que ayuden a los empleados a evaluar al instante el riesgo de los correos electrónicos.
- Establecer rutinas de reporte y alertas para notificar riesgos de seguridad o comportamientos sospechosos.

Reducción de la superficie de ataque

- Corregir vulnerabilidades, priorizando aquellas conocidas y explotadas o expuestas a Internet.
- Medir la calidad de los sistemas IT frente a marcos de referencia reconocidos y fijar requisitos claros de cumplimiento.
- Utilizar MFA (autenticación multifactor) resistente al *phishing*.

Comprender el panorama de amenazas

- Asegurarse de que la empresa tenga una visión actualizada del panorama de amenazas que le afecta.
- Identificar activos e información críticos de la empresa valiosos para un atacante.
- Comprender cómo la inteligencia artificial y las nuevas regulaciones influyen en el panorama de amenazas.

En ciberseguridad siempre existirá una batalla en la que los delincuentes se beneficien de forma rápida y oportunista de un espacio digital creciente. Puede resultar difícil priorizar y saber dónde enfocar los esfuerzos de seguridad.

- ¿Cómo se puede establecer un proyecto que nos proteja mejor contra el *phishing*?
- ¿Cómo se puede reducir de manera sistemática la superficie de ataque?

Este tipo de preguntas surgen a menudo cuando estamos expuestos diariamente a ciberamenazas y nuevas tecnologías.

En Sopra Steria podemos ayudar a tu empresa en todo el ciclo de la ciberseguridad: desde evaluaciones de madurez y pruebas de seguridad, hasta la definición de estrategias, diseño de arquitecturas seguras y cumplimiento normativo. También apoyamos en la mejora continua, la monitorización y la capacidad de respuesta ante incidentes, adaptándonos a cada necesidad.

Nuestros clientes ofrecen servicios críticos para la sociedad, y trabajamos a tiempo completo para ayudarles a proteger y salvaguardar sus funciones esenciales.

Queremos ayudar, y podemos ayudar.

NUESTROS LÍDERES

CEO Cybersecurity Business Line Group FRANCIA
Fabien LECOQ

BELUX
Karim AZER NESSIM

NÓRDICOS
Jorgen RORVIK

PAÍSES BAJOS
Gijs VAN DEN ELSHOUT

REINO UNIDO
Craig SHAW

INDIA
Yogesh KHETERPAL

ESPAÑA
Arsenio PEREZ GAVIRA

ITALIA
Stefano MEREGHETTI

CS GROUP
Laurent PORRACCHIA

SUIZA
Ales KUPSKY

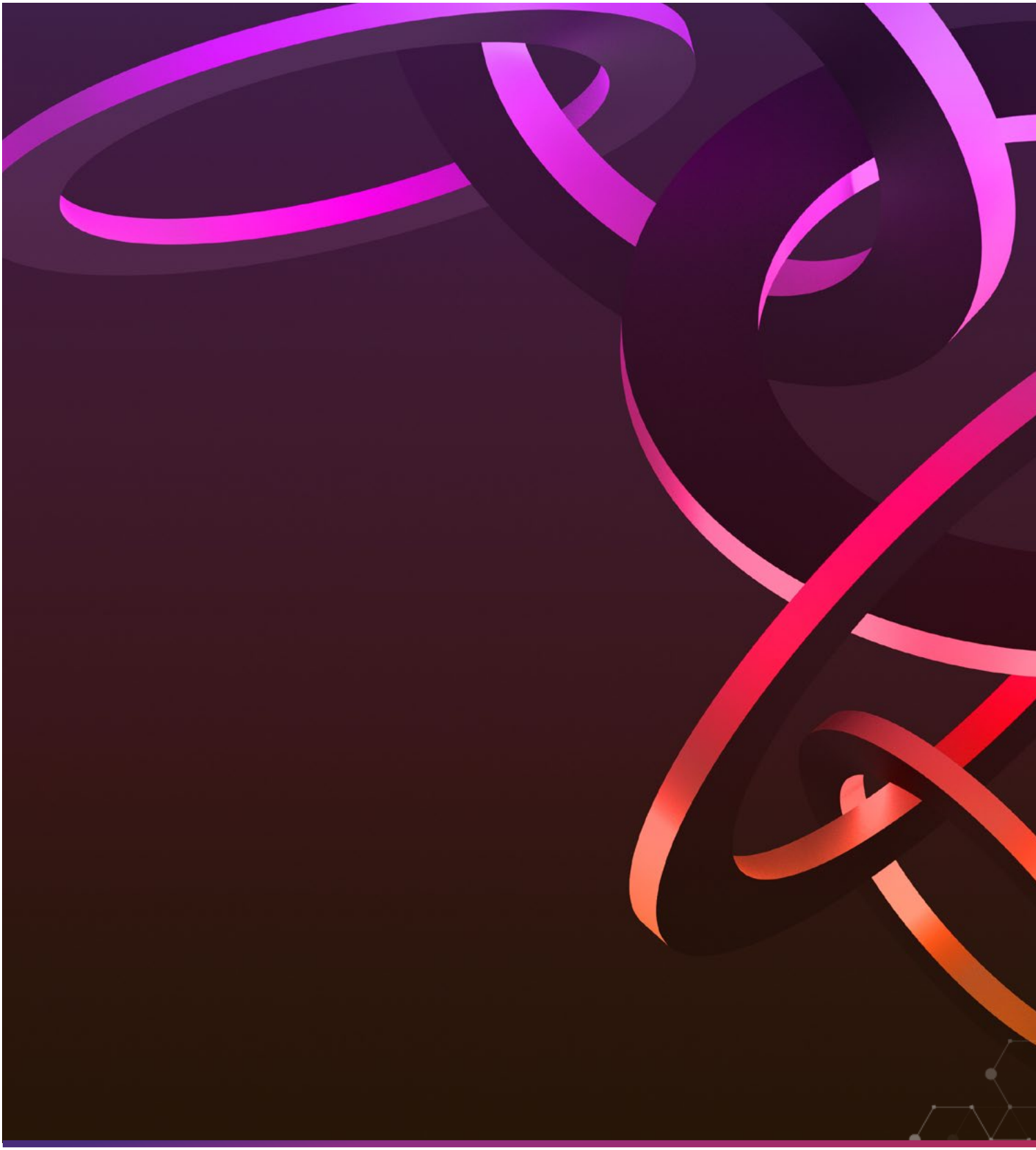
ALEMANIA
Olaf JANSSEN

EE.UU.-CANADA
Thomas CURUTCHET

PONTE EN CONTACTO:

cybersecurity-group-bl@soprasteria.com

SINGAPUR/HONG KONG
Cyril AYOUB



sopra steria

The world is how we shape it.

www.soprasteria.com