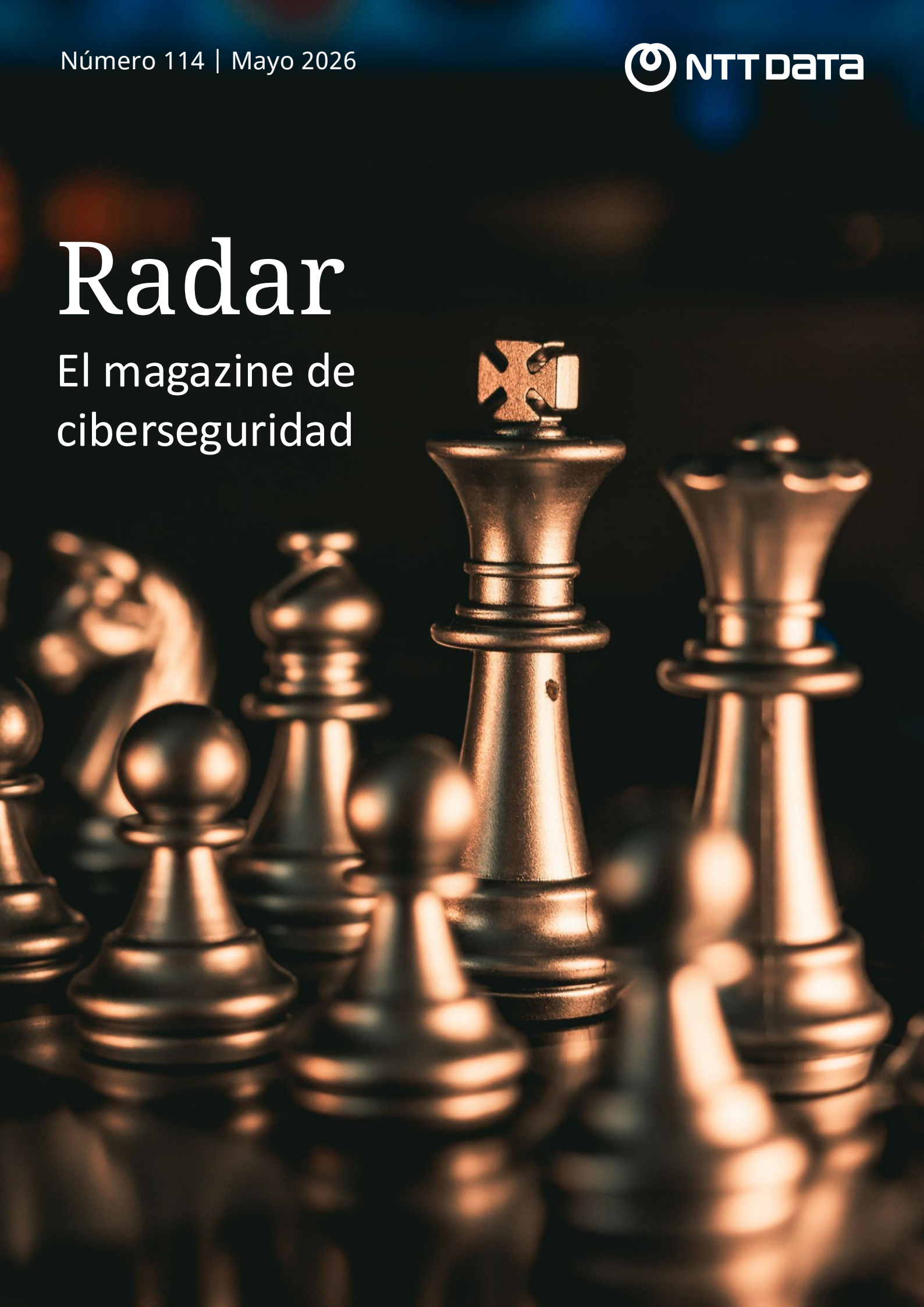
Número 114 | Mayo 2026

NTT DATA

Radar

El magazine de ciberseguridad



Más allá del Algoritmo: La Reinvención de CTI frente a la Democratización del Ataque

Por Alexis Martín García

Como responsables de inteligencia, solemos decir que nuestro trabajo consiste fundamentalmente en reducir la incertidumbre para facilitar la toma de decisiones. Sin embargo, en el último ciclo, esa incertidumbre no solo ha mutado, sino que ha adquirido una velocidad de crucero que desafía nuestros modelos tradicionales de defensa. Ya no nos enfrentamos únicamente a grupos estatales con recursos ilimitados o al oportunismo del cibercrimen convencional; estamos ante una democratización de la capacidad ofensiva que ha dinamitado las reglas de compromiso que conocíamos hasta hace apenas unos meses.

La realidad en las trincheras operativas es que la barrera de entrada para el adversario se ha desplomado. El auge de la automatización ofensiva y el uso de modelos de lenguaje aplicados al desarrollo de *malware* han transformado la economía del ataque: hoy, el coste de ejecución para el atacante tiende a cero, mientras que el coste de defensa para las organizaciones sigue siendo lineal y creciente. Cualquier actor con una intención clara puede ahora generar *payloads* polimórficos capaces de evadir soluciones de *endpoint* basadas en firmas, o diseñar campañas de ingeniería social tan quirúrgicas que el factor humano queda totalmente desarmado. Hemos pasado de detectar ataques "de manual" a gestionar una sinfonía de ruido automatizado que busca, con una persistencia algorítmica, ese único activo olvidado en nuestra superficie de exposición o esa vulnerabilidad de día cero recién publicada.

En este escenario de saturación, los indicadores de compromiso (IoCs) tradicionales, esas IPs, dominios y *hashes* que ayer eran nuestra base operativa, se han vuelto activos efímeros. Su vida útil en el ecosistema actual es tan corta que, para cuando llegan a nuestras listas de bloqueo, el adversario ya ha rotado su infraestructura de mando y control (C2). Por ello, el foco de la inteligencia moderna debe desplazarse irremediablemente hacia el análisis de las **TTPs (Tácticas, Técnicas y Procedimientos)**. Entender el *modus operandi* y los patrones de comportamiento no es ya una opción académica, sino la única forma real de anticiparnos a un vector de acceso antes de que se convierta en un incidente de impacto sistémico.

Pero esta carrera armamentista tecnológica no es unidireccional. Nosotros, como defensores, también hemos "aumentado" nuestra capacidad de respuesta a través de la misma tecnología que nos desafía. La integración de la inteligencia artificial y el aprendizaje automático en el flujo de CTI nos está permitiendo, por primera vez, procesar telemetría y fuentes de datos abiertos (OSINT) a una escala que hasta hace poco era puramente teórica. Estamos logrando conectar puntos dispersos entre un evento de red aparentemente trivial y una campaña dirigida que apenas está en fase de reconocimiento. La capacidad de filtrar el ruido y priorizar las amenazas en función del riesgo real es lo que permite que nuestros equipos de respuesta no sucumban a la fatiga por alertas.

Es ahí, en la detección de patrones invisibles y en la orquestación de la inteligencia, donde nuestra disciplina se convierte en el activo estratégico más crítico. Lo que encontraremos en las páginas de esta edición es un recorrido por esa tridimensionalidad que define el CTI actual: desde el peso de la realidad global y las tensiones que dictan los objetivos estratégicos, hasta la sofisticación técnica que permite el compromiso inicial, cerrando con las tendencias que están redefiniendo nuestra hoja de ruta operativa. No se trata solo de acumular datos, sino de transformarlos en conocimiento accionable que permita a la organización mantenerse un paso por delante en el tablero.

Al final, aunque la tecnología proporcione la velocidad y la fuerza bruta necesaria para navegar este nuevo entorno, el **criterio del analista,** esa capacidad única para interpretar la intención, el contexto geopolítico y la psicología detrás del dato, sigue siendo nuestro último y más sólido bastión. La IA puede automatizar la búsqueda, pero solo el analista humano puede dotarla de significado. Bienvenidos a un análisis profundo de nuestro presente más urgente, donde la inteligencia es, más que nunca, la diferencia entre la resiliencia y el compromiso.

Alexis Martín García
Project Manager of Cyber Threat Intelligence & Hacking Center

Cuando la confianza se convierte en perímetro: Anatomía de un mes de ataques

Cibercrónica Eduardo Gil Ciruelos

El mes que va de mediados de marzo a mediados de abril de 2026 no dejó un ataque histórico, pero sí algo más incómodo: una sucesión de incidentes que, leídos juntos, dibujan con precisión el escenario que anticipaba el artículo anterior. La barrera de entrada del adversario se ha desplomado, la automatización ha acelerado los ciclos y, en paralelo, las organizaciones han descubierto que sus perímetros ya no están donde creían. Esta es la crónica de esas semanas.

Todo empezó, o al menos se hizo visible, el **11 de marzo**. A las cinco de la mañana UTC, los empleados de **Stryker** repartidos por setenta y nueve países vieron sus dispositivos apagarse al mismo tiempo. Un **grupo vinculado a Irán** había comprometido una sola cuenta administrativa de **Microsoft Intune**, creando un nuevo administrador global y utilizado la herramienta legítima para borrar doscientos mil equipos. No hubo malware, no hubo *ransomware*, no hubo binario que analizar. El sistema no detectó un ataque porque, técnicamente, no lo estaba viendo: estaba viendo a un administrador haciendo su trabajo.

Pocos días después, el foco se desplazó a **Crunchyroll**, aunque el origen del incidente estaba mucho más lejos. Un agente de soporte de **Telus International**, trabajando desde un portátil en India, cayó en un correo de phishing. Las credenciales capturadas abrían, vía SSO de Okta, Zendesk, Slack, Workspace y Jira. En menos de veinticuatro horas **se exfiltraron cien gigabytes de datos y casi siete millones de direcciones de correo**. Cuando el equipo de seguridad logró revocar el acceso, la operación ya había terminado. El perímetro atacado no estaba en Tokio ni en California, sino en un contrato de externalización.

Mientras esos casos ocupaban titulares, otro salió a la superficie con retraso. **Marquis Software Solutions,** proveedor de servicios a cientos de entidades financieras en USA, comunicó en marzo un incidente ocurrido siete meses antes. Un *firewall* **SonicWall** comprometido había permitido desplegar *ransomware* que terminó afectando a setecientas mil personas y a setenta y cuatro bancos. Durante más de medio año, las víctimas no supieron que debían protegerse.

Casi en paralelo, la **Universidad Sapienza de Roma**, con sus ciento veinte mil estudiantes, amaneció sin servicios digitales. Exámenes, correo, trámites administrativos. Todo detenido durante varios días. No hubo reivindicación inmediata ni grandes exigencias públicas; solo la constatación de que una única puerta comprometida bastaba para parar una institución entera.

La primera semana de abril trajo un giro distinto. El día 7, el plugin **Smart Slider 3 Pro,** presente en más de ochocientas mil instalaciones de **WordPress**, publicó una nueva versión a través de su canal oficial. Durante seis horas, esa versión fue, en realidad, una puerta trasera completa escrita por un atacante que había tomado el control de la infraestructura de actualizaciones. Cada sitio que actualizó en ese intervalo se convirtió automáticamente en un punto de acceso remoto.

Dos días más tarde, la escena se repitió con otra firma. El **9 de abril**, los enlaces de descarga oficiales de **CPU-Z y HWMonitor**, en el sitio de CPUID, empezaron a redirigir a dominios maliciosos. La alteración duró alrededor de diecinueve horas. Los binarios firmados seguían siendo legítimos, pero la web que los distribuía ya no lo era. El usuario que hacía exactamente lo correcto, descargar desde la fuente, terminaba comprometido igual.

En esos mismos días, el foco se trasladó al sector público latinoamericano. En **México**, la filtración en el sistema **Safe Smart Port** de la Secretaría de Marina expuso casi cuarenta *gigabytes* de información sobre seiscientos cuarenta mil trabajadores portuarios, incluyendo rasgos biométricos, tipo de sangre y ubicación laboral. La brecha no comprometía solo datos personales, sino la trazabilidad operativa de infraestructura crítica logística.

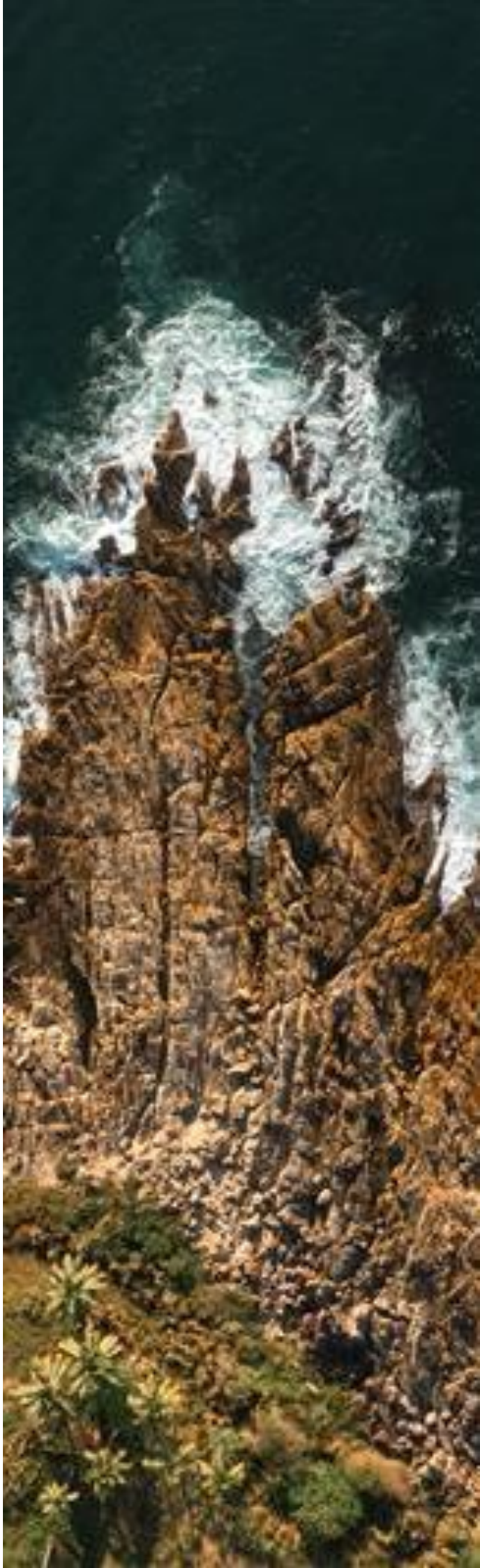
En Argentina, el grupo Chronus Team había anunciado días antes, en redes sociales, que iba a atacar. Y atacó. Veintiocho filtraciones simultáneas contra organismos gubernamentales nacionales y provinciales, dependencias de salud, finanzas y Fuerzas de Seguridad. El aviso previo no activó ninguna respuesta coordinada visible.

El cierre del mes lo marcaron incidentes en el sector privado. **Adobe** confirmó la exposición de trece millones de tickets de soporte, quince mil registros de empleados, documentos internos y envíos completos de su programa de *bug bounty*. La sensibilidad del conjunto no estaba en cada pieza, sino en lo que podía reconstruirse correlacionándolas.

Y el 11 de abril, el grupo ShinyHunters reivindicó dos operaciones casi consecutivas: en Rockstar Games, el compromiso de métricas de instancias Snowflake a través de la integración con Anodot; en Abrigo, la exfiltración de más de un millón setecientos mil registros de Salesforce. En ninguno de los dos casos el acceso vino desde el objetivo final, sino desde un servicio conectado.

Mirando el mes en conjunto, el hilo que une todos estos incidentes no es técnico. Ninguno exigió capacidades extraordinarias. Lo que los conecta es la forma en que cada atacante encontró una relación de confianza, una credencial, un proveedor, una actualización firmada, una integración SaaS, que la organización había dejado de cuestionar hace tiempo. Ninguno rompió una puerta. Todos tenían llave.

Eduardo Gil Ciruelos
Junior Cyber Threat Intelligence Analyst



Cuando el conflicto no se declara: el ciberespacio como herramienta de poder geopolítico

Artículo por Sandra Somastre

El ciberespacio se ha consolidado como un espacio de competencia geopolítica donde los Estados proyectan poder sin necesidad de confrontación directa. En este entorno, las ciberoperaciones no son eventos aislados, sino parte de estrategias más amplias orientadas a la persistencia, la influencia y la obtención de ventaja.

Comprender las amenazas actuales exige ir más allá del dato técnico y analizar el contexto estratégico en el que se desarrollan.

El contexto geopolítico actual se caracteriza por una competencia constante entre estados con intereses estratégicos cada vez más definidos.

Lejos de los modelos tradicionales de confrontación, los conflictos ya no se desarrollan únicamente en el plano físico, sino que se extienden a otros lugares donde la presión puede ejercerse de forma sostenida y con un menor riesgo de escalada.

En este contexto, el ciberespacio se ha establecido como un vector esencial para proyectar poder. No es un ambiente autónomo, sino más bien un espacio en el que muchas de las dinámicas geopolíticas actuales se definen: presión económica, rivalidad tecnológica, operaciones de influencia y obtención de inteligencia.

El ciberespacio ya no acompaña al conflicto: forma parte de él desde su diseño.

Un entorno de competencia persistente

El equilibrio internacional ha evolucionado hacia un modelo más fragmentado, donde múltiples actores estatales compiten sin que exista una separación clara entre periodos de paz y conflicto.

Esta situación favorece una actividad continua en la que las operaciones no buscan necesariamente un impacto inmediato, sino posicionarse de manera estratégica. Esta lógica se aplica de manera ideal a la actividad en el ciberespacio, lo que posibilita actuar de manera sostenida sin tener que recurrir a métodos tradicionales de enfrentamiento.

Conflictos como la guerra entre Rusia y Ucrania, las tensiones en Oriente Medio o la competencia tecnológica entre China y Occidente reflejan esta evolución. En todos ellos, el componente cibernético forma parte estructural del conflicto, complementando otras formas de presión.

Además, este modelo introduce una característica clave**: la asincronía.** Mientras que los conflictos tradicionales tienen fases más o menos identificables, la actividad en el ciberespacio no se detiene. Incluso en momentos de aparente estabilidad, las operaciones continúan, acumulando acceso, información y capacidad de influencia.

El ciberespacio como herramienta de presión estratégica

El valor del ciberespacio en el contexto actual se basa en su capacidad para operar en lo que se conoce **como zonas grises del conflicto**. Es decir, permite ejecutar acciones que generan impacto sin cruzar límites que obliguen a una respuesta directa, lo cual lo hace particularmente efectivo en un entorno geopolítico donde la escalada abierta supone un alto coste.

Esta lógica no se queda en lo teórico, sino que se manifiesta directamente en escenarios internacionales importantes, donde esta actividad acompaña, aumenta e incluso previene conflictos.

En este sentido, es posible identificar distintos patrones de uso del ciberespacio en función del contexto geopolítico:

- **Rusia – Ucrania:** La actividad cibernética ha sido incorporada de manera estructural en el conflicto, fusionando operaciones de influencia, campañas enfocadas a naciones ajenas y la interrupción de servicios. El ciberespacio posibilita ampliar el alcance del conflicto sin necesidad de una escalada tradicional, generando impacto en aliados, cadenas de suministro y opinión pública.
- **Oriente Medio (Israel y actores regionales):** En este escenario, el ciberespacio actúa como un medio de confrontación indirecta. Campañas de desinformación, filtraciones y ataques coordinados se combinan con operaciones de *hacktivismo* alineadas ideológicamente. El objetivo no es solo técnico, sino también influir en la percepción pública y aumentar la presión durante los momentos de tensión.

- **China – Occidente:** La acción se enfoca en campañas de ciberespionaje dirigidas a sectores críticos como tecnología, energía o manufactura avanzada. Este enfoque refleja una estrategia sostenida en el tiempo, donde la obtención de información y el establecerse tecnológicamente resultan prioritarios frente a la disrupción inmediata.
- **Estados Unidos:** Su rol en la economía digital y su peso geopolítico. La manera en que se emplea el ciberespacio para influir directamente en áreas donde se determina la ventaja global, desde la estabilidad económica hasta la innovación, queda demostrada por la concentración de actividad en sectores estratégicos.
- **Irán y Corea del Norte:** Estos actores combinan operaciones de influencia, espionaje y actividades orientadas a la obtención de recursos. El ciberespacio se transforma en un instrumento para superar restricciones estructurales, sobre todo en el sector económico, y extender la capacidad más allá de las fronteras.

En resumen, estos escenarios muestran una tendencia evidente: las operaciones cibernéticas no son sucesos aislados, sino que forman parte de **estrategias permanentes orientadas a ejercer influencia, desgastar y situar a los actores en un ambiente de competencia constante**. El impacto no se mide solamente en términos técnicos, sino también por su habilidad de integrarse en procesos más extensos y producir efectos acumulativos a lo largo del tiempo.

La evolución técnica como reflejo del contexto

El auge de técnicas basadas en la explotación de identidades, el uso de herramientas legítimas o la disminución del *malware* convencional responde no solo a una evolución operativa, sino a una adaptación al entorno geopolítico. En un contexto en el que la atribución tiene efectos estratégicos, la habilidad de operar con discreción se vuelve un factor distintivo.

Esto explica por qué muchas campañas actuales priorizan el acceso silencioso en lugar de la explotación visible. El objetivo no es únicamente entrar, sino permanecer.

En este sentido, la técnica deja de ser un objetivo en sí mismo y pasa a ser un medio que sirve a una estrategia más amplia. La elección de herramientas, vectores y objetivos se basa en una lógica que va más allá de lo técnico.

Un ecosistema de actores cada vez más complejo

El entorno actual también se caracteriza por una creciente conexión entre actores estatales y no estatales.

El trabajo conjunto entre grupos de hacktivismo, cibercrimen y estructuras asociadas a Estados crea un ecosistema más adaptable, en el que se intercambian capacidades y se desdibujan los motivos. Este modelo no solo complica la atribución, sino que además permite a los Estados mantener un margen de ambigüedad sobre su verdadera implicación.

Además, la expansión de herramientas accesibles, servicios criminales y modelos "*as-a-service*" ha reducido las barreras de entrada, ampliando el número de actores que pueden participar en estas operaciones.

Desde una perspectiva criminológica, esto introduce dinámicas propias de entornos organizados: especialización, externalización de funciones y adaptación constante en función del riesgo y el beneficio.

El papel de la Ciberinteligencia en un entorno de ambigüedad

En este contexto, el principal reto para la Ciberinteligencia de Amenazas no es únicamente la detección, sino **la interpretación de la actividad.**

El volumen de información disponible es cada vez mayor, pero su valor depende de la capacidad para contextualizarla. Entender una campaña implica analizar no solo cómo se ejecuta, sino **por qué ocurre, en qué momento y con qué objetivo estratégico.**

Esto supone un cambio en la forma de abordar el análisis. Las investigaciones ya no pueden limitarse a la identificación de indicadores técnicos o patrones conocidos, sino que requieren integrar variables externas como el contexto geopolítico, la evolución de los conflictos o los intereses de los actores implicados.

Desde esta perspectiva, la Ciberinteligencia se aproxima cada vez más a disciplinas centradas en el análisis del comportamiento y del entorno, donde la interpretación resulta tan relevante como la evidencia técnica. La capacidad de anticipar movimientos ya no depende únicamente de la detección, sino de la **comprensión del escenario en el que se opera**.

Así el ciberespacio se ha consolidado como una extensión directa de la competencia geopolítica. Las operaciones ya no son incidentes aislados, sino parte de estrategias continuas donde la persistencia, la ambigüedad y la presión indirecta marcan el ritmo del conflicto.

Es por ello que en un entorno donde el conflicto no siempre se declara, la diferencia no está en detectar más, sino en interpretar mejor.

Sandra Somastre
Cyber Threat Intelligence Analyst

Del acceso a la intención: visión CTI cuando el atacante es un usuario

Artículo por Raquel Gálvez Huertas

Cada vez más ciberataques comienzan con un acceso aparentemente legítimo, en lugar de una intrusión visible. El atacante no necesita vulnerar sistemas: le basta con que el sistema confíe en él.
Este cambio no es solo operativo, es estructural. La seguridad tradicional se ha construido para detectar accesos no autorizados. Sin embargo, cada vez más ataques utilizan accesos válidos, lo que difumina la frontera entre actividad legítima y comportamiento malicioso.
En este contexto, la Inteligencia de Ciberamenazas se enfrenta a un reto distinto: ya no basta con identificar amenazas externas, sino entender cómo se comportan los atacantes cuando ya parecen usuarios.

El cambio de paradigma se explica mejor a través de las técnicas que han ganado protagonismo recientemente. Todas ellas comparten un elemento común: el atacante no "rompe" el sistema, lo utiliza.

Cuando el acceso ya no es una señal de legitimidad

Una de las más representativas es el *phishing* tipo ***Adversary-in-the-Middle*** **(AiTM)**, que se ha consolidado como uno de los principales vectores en campañas dirigidas. A diferencia del *phishing* tradicional, este enfoque permite interceptar en tiempo real las credenciales y las sesiones del usuario, incluso en entornos protegidos con autenticación *multifactor* (MFA). El resultado no es solo el robo de contraseñas, sino de sesiones activas completamente válidas.
Este modelo ha alcanzado un nivel de industrialización significativo. En marzo de 2026, Europol y Microsoft desmantelaron la plataforma **Tycoon 2FA**, un servicio de *phishing-as-a-service* basado en AiTM que permitió comprometer cuentas en cerca de 100.000 organizaciones, generando campañas masivas capaces de eludir MFA y operar con accesos legítimos a gran escala.
A esto se suma el crecimiento del ***session hijacking***, especialmente en entornos *cloud* y SaaS, donde los atacantes reutilizan *cookies* o *tokens* de autenticación para acceder a los servicios sin necesidad de volver a autenticarse.
Este tipo de técnicas se ha observado en incidentes recientes en entornos Microsoft 365, donde actores avanzados como **Storm-2755** accedieron a cuentas institucionales mediante el uso de *tokens* de autenticación válidos, sin credenciales ni nuevos procesos de *login*. El acceso se realizaba sobre sesiones legítimas ya emitidas, lo que dificultó su detección al no existir irregularidades evidentes en el proceso de autenticación.

Persistencia sin credenciales: el abuso de OAuth (*Open Authorization*)

Otra técnica emergente, especialmente relevante en entornos corporativos, es el abuso de aplicaciones **OAuth**. En estos casos, el atacante consigue que el usuario autorice una aplicación maliciosa que obtiene permisos sobre su cuenta (correo, archivos, etc.). A partir de ahí, el acceso se mantiene sin necesidad de credenciales adicionales.
En marzo de 2026, una campaña activa sin atribución que abusaba de flujos legítimos de OAuth comprometió más de 340 organizaciones al inducir a los usuarios a introducir códigos en páginas legítimas de autenticación, autorizando sin saberlo el acceso de los atacantes y generando *tokens* válidos sin necesidad de robo de credenciales.
Estas prácticas introducen un nuevo reto: la persistencia ya no depende de credenciales comprometidas, sino de permisos concedidos.

Ataques sin *malware*: invisibilidad operativa

Por otro lado, se consolida el uso de enfoques conocidos como ***Living-off-the-Land*** **(LotL)**, donde los atacantes utilizan herramientas legítimas del propio entorno (*scripts*, APIs, funcionalidades *cloud*) para ejecutar sus acciones.
Campañas actuales de actores APT, como **APT29** y **APT28**, motivados por el conflicto geopolítico reflejan estos métodos, donde los atacantes se infiltran en los sistemas de infraestructuras críticas del enemigo haciendo uso de herramientas nativas, permaneciendo sin ser detectados mientras se extrae información con fines estratégicos.
Así, cuando la actividad se apoya en LotL, uno de los principales indicadores de compromiso tradicionales, el *malware*, pasa a un segundo plano o incluso desaparece.
El resultado es una operativa difícil de distinguir de la de un usuario real, integrada, sin alertas evidentes ni comportamientos inesperados.
Si el acceso ya no es una barrera, el siguiente punto de control pasa a ser el propio usuario.

El usuario como vector de *bypass*

Otra tendencia relevante es el uso de técnicas que explotan directamente al usuario como mecanismo de evasión.
El **MFA *fatigue***, también conocido como *push bombing*, consiste en bombardear al usuario con solicitudes de autenticación hasta que, por error o fatiga, acepta una de ellas. En este punto, el atacante obtiene acceso sin tener que vulnerar ninguna medida técnica.
En paralelo, se ha observado un incremento de **ataques dirigidos a servicios de soporte IT o *helpdesk***, donde los atacantes suplantan identidades para solicitar reseteos de credenciales o cambios en los factores de autenticación. Aquí, el vector no es tecnológico, sino procedimental.
Estos mecanismos reflejan un cambio claro: el foco del atacante se desplaza de las debilidades en los sistemas a los procesos y las personas.
Este enfoque ha sido utilizado de forma recurrente por grupos como **Scattered Spider**, que en campañas activas en 2025/26 han combinado el envío masivo de notificaciones MFA con ingeniería social contra servicios de soporte IT para lograr accesos legítimos en entornos corporativos.
Una vez dentro, el objetivo ya no es ocultarse, sino operar sin levantar sospechas.

Implicaciones para CTI: cuando la confianza genera incertidumbre

Todas estas técnicas, aun diferentes en su ejecución, comparten un patrón claro: operan dentro de los límites de lo que el sistema considera normal.

- Accesos válidos,
- Herramientas legítimas,
- Procesos autorizados,
- Comportamientos creíbles.

La integración de estos factores como parte del propio ataque no solo reduce la visibilidad técnica, sino que cambia el tipo de problema al que se enfrenta la seguridad.
Cuando no hay *malware*, ni explotación evidente, ni eventos sospechosos, los mecanismos tradicionales pierden capacidad para interpretar lo que está ocurriendo.
Ahora el juego no va de evadir los controles si no de encajar en ellos.
De esta manera, el valor de los equipos de CTI no se limita a la detección de señales evidentes, sino que evoluciona para interpretar lo que ocurre dentro de esa aparente normalidad. Identificar patrones de uso que no encajan, correlacionar pequeñas anomalías y entender las técnicas del atacante permite dar sentido a actividades que, de forma aislada, parecen normales.
En un entorno donde el acceso deja de ser un indicador fiable, la capacidad de interpretar el comportamiento se convierte en el elemento clave para reducir la incertidumbre y apoyar la toma de decisiones.

Raquel Gálvez Huertas
Cyber Threat Intelligence Analyst

El Nuevo Orden de Amenazas: Las tendencias que están redefiniendo nuestra hoja de ruta

Tendencias por Alberto Herrera García

El primer cuatrimestre de 2026 ha confirmado lo que ya intuíamos: la amenaza no sólo ha crecido en volumen, ha cambiado de naturaleza. La identidad ha desplazado al perímetro como campo principal de batalla, la cadena de suministro se ha convertido en una vulnerabilidad estructural y la IA ha dejado de ser una ventaja exclusiva del defensor para convertirse en compañera de campaña del adversario. A todo esto, se le suma una geopolítica que dicta objetivos con más precisión que nunca y una exigencia creciente de que el analista deje de informar para empezar a decidir.

Estas son las tendencias que están redefiniendo nuestra hoja de ruta.

La Identidad como el Nuevo Perímetro de Combate

La conclusión más contundente que emerge de los principales informes de inteligencia publicados en lo que llevamos de año es, a la vez, la más incómoda de asumir: la identidad se ha convertido en la puerta de entrada primaria a los entornos empresariales modernos. A medida que las organizaciones se expanden hacia plataformas *cloud*, ecosistemas SaaS y modelos de acceso remoto, las tradicionales fronteras de red se han difuminado. La identidad define ahora el acceso, la exposición y el compromiso. Por ello, los actores de amenazas han adaptado su operativa en consecuencia y han optado de forma masiva por aprovechar credenciales válidas obtenidas mediante malware *infostealer*, registros y mercados ilícitos para iniciar sesión en lugar de forzar entradas y explotar sistemas. Lo que en la comunidad se denomina ya: "*log in, don't break in*".

Durante el 2025, cientos de miles credenciales de plataformas de IA aparecieron en mercados clandestinos, lo que confirma que las herramientas de productividad corporativa se han convertido en un vector de exposición de primer nivel. Para el CTI operativo, esta nueva tendencia ha implicado redefinir qué acciones constituyen la monitorización de exposición: desde vigilar la *dark web* hasta rastrear *tokens*, *API keys* y sesiones activas.

La Cadena de Suministro: de Vector de Ataque a Condición Sistémica

Atrás quedaron los días en que los ataques de cadena de suministro eran incidentes puntuales protagonizados por actores sofisticados. En los últimos 5 años, los compromisos de terceros se han cuadruplicado y, lo que antes era una categoría de ataque diferenciada, se ha convertido en una condición permanente del ecosistema. Los adversarios ya no atacan el endpoint de la organización objetivo, atacan directamente a los entornos donde su software es construido y desplegado.

Una clara tendencia al alza, impulsada por la fragilidad de las cadenas de dependencia, es la explotación de aplicaciones públicas. Un único repositorio comprometido puede distribuir actualizaciones maliciosas a miles de proyectos relacionados antes de que ningún sistema de detección haya generado la primera alerta. Para nuestra disciplina, esto implica una ampliación forzosa del modelo de recolección: la inteligencia útil tiene que incluir visibilidad sobre la postura de seguridad de nuestros proveedores, sus dependencias de código abierto y los accesos que tienen sobre nuestra infraestructura. El mapa de riesgo de cadena de suministro enriquecido con telemetría de amenazas ya no es una aspiración de madurez, es el estándar mínimo exigible.

La IA Adversarial: de Herramienta a Compañero de Campaña

El uso de inteligencia artificial por parte de los adversarios ha dejado de ser un argumento de futuro próximo. Familias de malware como *Promptflux* y *Promptsteal* consultan activamente modelos de lenguaje durante su propia ejecución para adaptar su comportamiento y evadir la detección en tiempo real. Nos encontramos ante malware que es capaz de razonar sobre su entorno. Paralelamente, han cobrado relevancia los llamados ataques de destilación (*distillation attacks)* que permiten extraer la lógica propietaria de modelos de alto valor, convirtiendo los activos de IA de la organización en un objetivo de exfiltración tan crítico como cualquier base de datos.

El incremento en ataques perpetrados por adversarios con capacidades habilitadas por IA confirma que ya no se trata sólo del patrimonio de actores de élite. En particular, la ingeniería social también ha experimentado una transformación cualitativa: *deepfakes* generados con precisión contextual, suplantación de servicios de soporte técnico y campañas de phishing multifase que son capaces de desactivar el factor humano antes de que el objetivo haya identificado la amenaza.

La Geopolítica como variable de Inteligencia Estratégica

Ningún análisis del panorama de 2026 estaría completo sin reconocer el peso de la geopolítica como variable de primer orden. Los conflictos activos, las disputas comerciales y la redefinición de alianzas siguen moldeando los objetivos y el ritmo de los actores de amenazas de forma tan determinante como cualquier vulnerabilidad técnica. Por estos motivos, la línea que separaba el cibercrimen con la motivación financiera de las operaciones de espionaje patrocinadas por estados se ha desdibujado hasta hacer prácticamente imposible la consecución de una atribución limpia en gran parte de los escenarios. Los grupos de *ransomware*, por ejemplo, están sirviendo de manera simultánea como fuentes de financiación y como agentes de perturbación geopolítica.

Al mismo tiempo, la convergencia de herramientas compartidas, programas de afiliados e infraestructura solapada ha generado un ecosistema adversarial dinámico en el que los modelos de atribución tradicionales (basados en TTPs o actores concretos) resultan insuficientes. Desde el punto de vista estratégico, esta situación exige a los analistas incorporar la geopolítica como capa permanente del ciclo de inteligencia y como variable predictiva, tratando de anticipar quién va a ser el próximo objetivo, cuándo y con qué intensidad.

La Inteligencia como Decisión, No como Dato

Este recorrido por las principales tendencias de los primeros cinco meses del año nos deja con una certeza que no requiere datos adicionales para su sustento: la complejidad del entorno actual no se resuelve ni con más herramientas ni con más *feeds*.

Se resuelve con mejor criterio analítico, con estructuras que permitan que la inteligencia fluya hacia la acción y con la capacidad de mantener la mirada estratégica, precisamente en el momento en el que el ruido operativo está en su máximo esplendor.

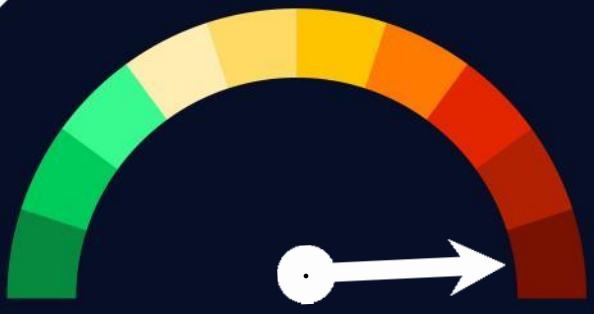
Cuando las amenazas se mueven a velocidad de máquina, la defensa centrada exclusivamente en el ser humano deja de ser suficiente. Pero la autonomía defensiva no implica la irrelevancia del analista, implica su elevación. Alguien tiene que diseñar los modelos, calibrar los umbrales e interpretar las anomalías que ningún sistema ha visto antes. Esa función no es delegable. Lo que las tendencias confirman es que la inteligencia ha completado su transición de disciplina técnica especializada a función estratégica de primer nivel. Hemos pasado de recopilar indicadores a modelar adversarios, de monitorizar amenazas a gestionar exposiciones, de informar, a ser parte activa del ciclo de decisión. Es una responsabilidad mayor pero también es el reconocimiento de que, en un entorno donde los adversarios operan con una velocidad algorítmica y una eficiencia industrial, la única respuesta que tenemos es la inteligencia: construida con rigor y aplicada con el juicio que sólo el analista humano puede aportar.

Alberto Herrera García
Junior Cyber Threat Intelligence Analyst

Vulnerabilidades

Vulnerabilidad de Bypass en productos Cisco

Fecha: 1 de abril de 2026
CVE: CVE-2026-20093



CVSS: 9.8

CRÍTICA

Descripción

Se ha identificado una vulnerabilidad crítica de tipo *bypass* contra la autenticación del controlador de gestión integrado de Cisco.

Esta vulnerabilidad se encuentra en la función de cambio de contraseña de Cisco IMC, donde un atacante puede enviar una solicitud HTTP especialmente diseñada a un dispositivo vulnerable.

La explotación exitosa podría permitir al atacante omitir el proceso de autenticación, modificar las contraseñas de cualquier usuario existente y obtener acceso a dicho usuario al sistema.

Cisco ha publicado actualizaciones que solventan esta vulnerabilidad, no se tiene constancia que existan otras remediaciones.

Solución

Se recomienda:

- Instalar la actualización correspondiente al nivel de parche 2026-04-01 o posterior, según el producto afectado.

Productos afectados

Algunos de los productos afectados son:

- 5000 Series Enterprise Network Compute Systems (ENCS) (CSCwq55648)
- Catalyst 8300 Series Edge uCPE (CSCwq68912)
- UCS C-Series M5 and M6 Rack Servers in standalone mode (CSCwq55659)
- UCS E-Series Servers M3 (CSCwq55648)

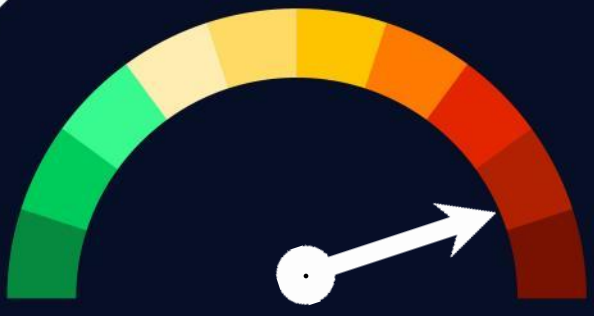
Referencias

- sec.cloudapps.cisco.com
- socradar.io
- thehackernews.com

Vulnerabilidades

Vulnerabilidad en Docker permite accesos sin autorización

Fecha: 30 de marzo de 2026
CVE: CVE-2026-34040



CVSS: 8.8

ALTA

Descripción

Se ha descubierto una vulnerabilidad alta en Docker Engine que permite a los atacantes eludir los *plugins* de autorización (AuthZ) y obtener acceso al *host*.

El fallo se debe a una corrección incompleta de una vulnerabilidad previa que permite enviar peticiones API manipuladas cuyo contenido no es analizado por los mecanismos de control. Como resultado, se pueden crear contenedores privilegiados con acceso al sistema anfitrión, exponiendo credenciales y claves SSH.

La vulnerabilidad ya ha sido corregida en la versión 29.3.1, y se recomienda actualizar de inmediato o aplicar medidas de mitigación como restringir el acceso a la API.

Solución

- La vulnerabilidad fue corregida en Docker Engine versión 29.3.1.
- Se recomienda actualizar lo antes posible a esta versión.

Productos afectados

- Productos que utilizan Docker Engine con versiones anteriores a 29.3.1 y que además hagan uso de plugins de autorización (AuthZ).
- Algunos ejemplos: Docker Desktop (Windows / macOS), Docker CE (Community Edition), Docker EE / Mirantis Container Runtime, Servidores Linux con Docker Engine instalado manualmente, etc.

Referencias

- thehackernews.com
- cybersecuritynews.com

TLP:WHITE

Actualización urgente por vulnerabilidad crítica en FortiClient EMS

Fecha: 5 de abril de 2026
CVE: CVE-2026-35616

Crítica

Descripción

Fortinet ha publicado un parche de emergencia para una vulnerabilidad crítica en FortiClient EMS (CVE-2026-35616), que ya está siendo explotada activamente.

El fallo se debe a un problema de control de acceso que permite a los atacantes eludir la autenticación de la API y ejecutar código o comandos mediante peticiones manipuladas.

Afecta a las versiones 7.4.5 y 7.4.6, para las que ya se han publicado *hotfixes*, mientras que la solución definitiva llegará en la versión 7.4.7.

Los investigadores detectaron su explotación como zero-day antes de su divulgación e identificaron más de 2.000 instancias expuestas a internet.

Productos afectados

- La vulnerabilidad afecta a las versiones 7.4.5 y 7.4.6 de FortiClient EMS.
- También se corregirá en la futura versión 7.4.7.
- La versión 7.2 no se ve afectada.

Solución

- Se recomienda aplicar los parches de inmediato para evitar compromisos.
- Enlaces de instalación de los parches:
  - FortiClient 7.4.5
  - FortiClient 7.4.6

Referencias

- bleepingcomputer.com
- thehackernews.com

Google corrige una vulnerabilidad de tipo Zero-Day

Fecha: 1 de abril de 2026
CVE: CVE-2026-5281

Alta

Descripción

Google ha lanzado un parche de seguridad urgente para Chrome con el fin de solventar una vulnerabilidad de tipo *Zero Day.*

La descripción oficial del proveedor menciona que se trata de una vulnerabilidad de tipo UAF (*use after free),* implementación de código abierto del estanda WebGPU, que es utilizado en los navegadores Chronium.

Esta vulnerabilidad permitiría a un atacante remoto que haya comprometido el proceso de renderizador, usado en estos navegadores, ejecutar código arbitrario en una página HTML previamente elaborada.

Esta vulnerabilidad fue notificada por un *bug bounty*, el cual informó previamente de otras dos vulnerabilidades corregidas en otra actualización de Chrome del pasado 23 de marzo.

Productos afectados

Los productos afectados por esta vulnerabilidad incluyen todas las versiones de Google Chrome anteriores a la versión:

- 146.0.7680.177/178 para Windows/Mac
- v146.0.7680.177 para Linux.

Solución

Se recomienda:

- Actualizar a las últimas versiones del software.

Referencias

- helpnetsecurity.com/
- app.opencve.io

Eventos

International Conference on Data Privacy and Protection – ICDPP
2 de mayo

La ICDPP reúne a investigadores, profesionales y responsables de cumplimiento en torno a los retos actuales de la privacidad y la protección de datos. Con especial atención al marco regulatorio europeo, incluyendo el RGPD, el congreso ofrece una visión integral que conecta la investigación académica con su aplicación en entornos empresariales. Se trata de un foro clave para analizar tendencias en gobernanza del dato, ética digital y cumplimiento normativo en un escenario donde la gestión responsable de la información es cada vez más crítica.

Enlace

CyberWiseCon Europe 2026
19 – 22 de mayo

CyberWiseCon es una conferencia de primer nivel en seguridad informática que reúne a expertos en ciberseguridad, líderes del sector y profesionales de TI de toda Europa.En un entorno digital en constante evolución, el conocimiento por sí solo no es suficiente para protegerse frente a las amenazas cibernéticas. La sabiduría, adquirida a través de la experiencia y el entendimiento colectivo, nos permite mantenernos un paso por delante de los actores maliciosos.En CyberWiseCon celebramos la unión entre conocimiento y sabiduría, ofreciendo una plataforma para intercambiar ideas, compartir buenas prácticas y explorar enfoques innovadores en ciberseguridad.

Enlace

Cybersec Europe
20 - 21 de mayo

Cybersec Europe se consolida como uno de los principales puntos de encuentro de la ciberseguridad en Europa, reuniendo a expertos, empresas tecnológicas y responsables de negocio en torno a los desafíos más actuales del sector. La edición de 2026 pondrá el foco en áreas como la seguridad en la nube, la gestión de identidades (IAM) y la resiliencia digital, combinando innovación tecnológica con una clara orientación estratégica. Con una fuerte presencia de partners y líderes del mercado, el evento destaca también por su capacidad para generar networking de alto nivel y oportunidades de colaboración.

Enlace

CYSAT Europe 2026
20 - 21 de mayo

CYSAT Europe representa una de las propuestas más innovadoras dentro del panorama actual, centrada en la ciberseguridad aplicada al ámbito espacial y satelital. En un contexto donde las infraestructuras críticas trascienden el entorno terrestre, este evento aborda los riesgos emergentes en comunicaciones espaciales, satélites y sistemas asociados. Con un enfoque que combina industria, defensa y tecnología, CYSAT pone sobre la mesa la necesidad de anticiparse a amenazas cada vez más sofisticadas en un dominio estratégico en plena expansión

Enlace

Recursos

➢ Cyber Threat Monitor & Sector Reports

Cyble ha publicado en abril de 2026 nuevos informes sectoriales, incluyendo el *Healthcare Threat Landscape Report 2026*, donde analiza amenazas reales activas en sectores críticos. Este tipo de reportes ofrece inteligencia directamente accionable sobre ransomware, actividad en la *dark web* y campañas dirigidas. Es especialmente útil para entender cómo los atacantes están adaptando sus tácticas por industria en tiempo casi real.

Enlace

➢ Weekly Vulnerability Digest – CVE Watchtower

Este briefing semanal es oro para equipos de seguridad: solo en una semana reciente se registraron más de 1.300 nuevas vulnerabilidades, incluyendo *zero-days* críticos que requieren acción inmediata. El informe filtra el ruido y prioriza lo realmente explotable, ayudando a equipos SOC y de gestión de vulnerabilidades a tomar decisiones rápidas y basadas en riesgo.

Enlace

➢ Vulnerability Statistics 2026

Un recurso brutalmente actual: a abril de 2026 ya se han publicado más de 17.000 vulnerabilidades, lo que supone un incremento del 26% respecto al año anterior. Este *dashboard* actualizado diariamente permite entender la velocidad real del riesgo y dimensionar el reto operativo al que se enfrentan los equipos de ciberseguridad.

Enlace

NTT DATA

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com