BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Kimsuky lleva la IA al ataque: GitHub y AsyncRAT como armas cibernéticas

TLP:CLEAR
18.08.2026

CLICK PARA EMPEZAR

CYBERSOCDTS

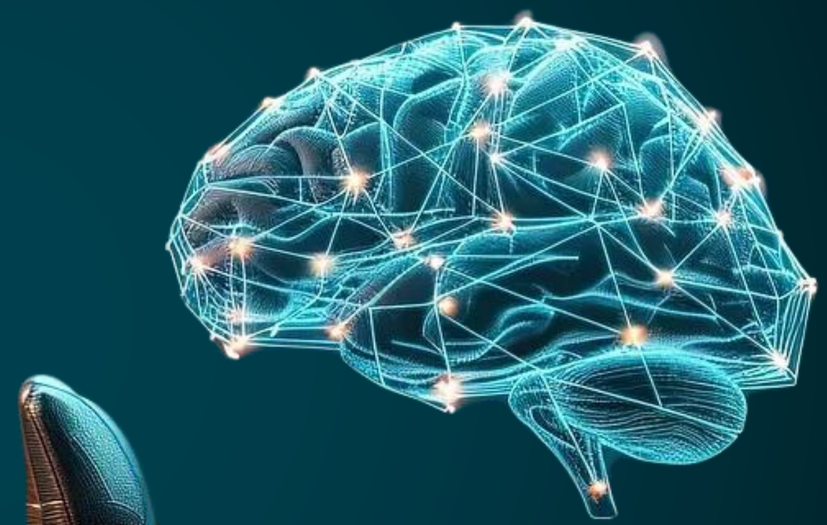
En esta edición:

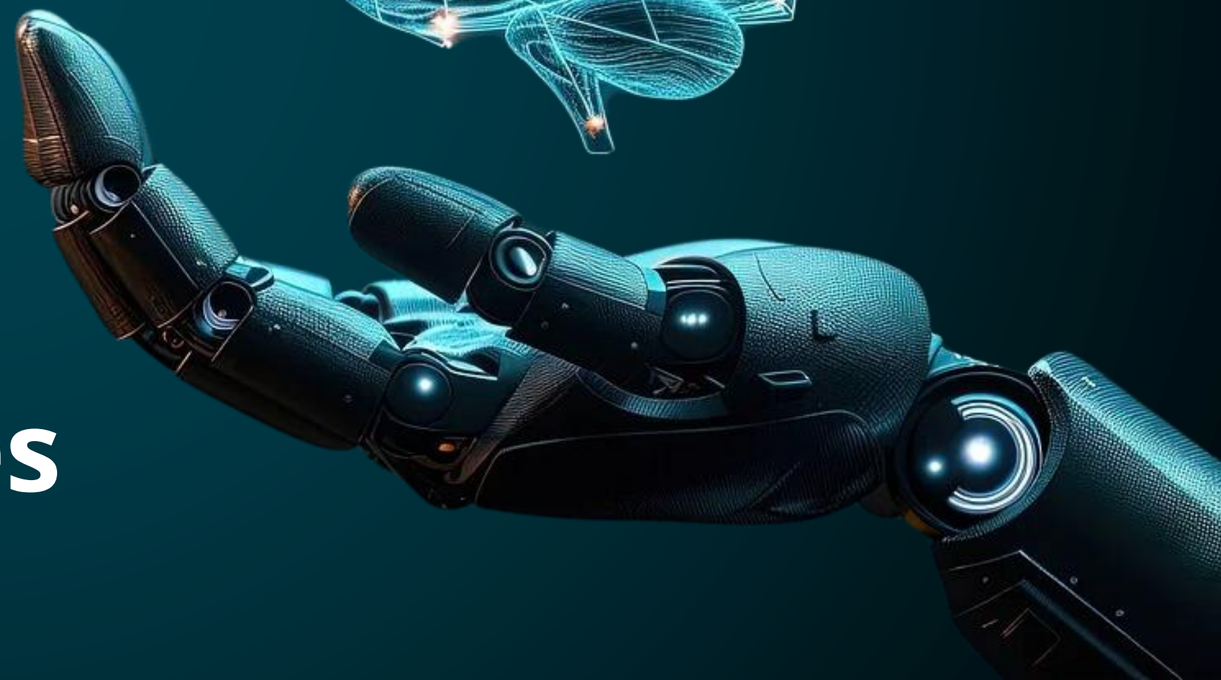
Kimsuky: IA y nuevas armas para sus ciberataques

CONTENIDO

DataSec

- Nuestra Esencia
- Vulnerabilidades
- Noticias
- Recomendaciones





NUESTRA ESENCIA

BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.

EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.

SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.

Adobe Campaign Classic (ACC) | Improper Neutralization of Special Elements Used in a Template Engine

CVE-2026-48323

Critical (10.0)

Impacto: Ejecución arbitraria de código.

Resumen: Se identificó una vulnerabilidad en Adobe Campaign Classic (ACC) relacionada con la neutralización incorrecta de elementos especiales utilizados en un motor de plantillas. La falla puede ser explotada sin requerir interacción del usuario y permite a un atacante lograr la ejecución arbitraria de código en el contexto del usuario actual, ampliando el alcance del impacto sobre el sistema comprometido.

Producto Afectado

- Adobe Campaign Classic ACC v7: 7.4.3 y versiones anteriores.

Ver +INFO.

Solución:

Actualizar Adobe Campaign Classic a la versión más reciente proporcionada por Adobe.

Ver + INFO.

Fecha de Publicación: 03/AGO/2026 INFO

Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability

CVE-2026-20079

Critical (10.0)

Impacto: Ejecución arbitraria de código.

Resumen: Se identificó una vulnerabilidad crítica de elusión de autenticación en Cisco Secure Firewall Management Center (FMC) que puede ser explotada remotamente sin autenticación. La falla permite a un atacante ejecutar scripts y comandos arbitrarios con privilegios root sobre el dispositivo afectado.

Producto Afectado

- Cisco Secure FMC Software.
- Cisco Security Cloud Control (SCC) Firewall Management.

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad publicadas por Cisco.

Ver +INFO.

Fecha de Publicación: 05/AGO/2026 INFO

Sensor Proxy Vulenarbility

CVE-2026-18667

Critical (9.3)

Impacto: Ejecución arbitraria de código.

Resumen: Se identificó una vulnerabilidad en Tenable Sensor Proxy que podría permitir a un atacante remoto ejecutar código arbitrario con privilegios elevados, mediante la conexión del sensor a un host controlado por el atacante.

Producto Afectado

- Sensor Proxy 1.4.1 y versiones anteriores.

Ver +INFO.

Solución:

Actualizar a Sensor Proxy 1.4.2.

Ver +INFO.

Fecha de Publicación: 03/AGO/2026 INFO

KVM: x86: Check for invalid/obsolete root *after* making MMU pages available

CVE-2026-64561

High (8.8)

Impacto: Posible corrupción del estado de memoria.

Resumen: Se identificó una vulnerabilidad en el kernel de Linux, específicamente en KVM para x86, relacionada con el manejo de raíces de memoria inválidas u obsoletas. La falla podría provocar un estado inconsistente en la gestión de memoria de las máquinas virtuales, afectando la estabilidad y seguridad del sistema.

Producto Afectado

- Linux Kernel – KVM (x86): afectado desde la versión 5.9.

Ver +INFO.

Solución:

Actualizar a la versión más reciente disponible de Linux Kernel.

Ver +INFO.

Fecha de Publicación: 09/AGO/2026 INFO

Microsoft security updates

CVE-2026-68820

Microsoft publicó las actualizaciones de seguridad de agosto de 2026 que corrigen 398 vulnerabilidades, incluyendo un fallo de día cero activamente explotado en Windows WinSock que podría permitir elevar privilegios hasta SYSTEM. También se corrigió una vulnerabilidad crítica en Windows DNS Server que podría permitir la ejecución remota de código sin autenticación.

Recomendación:

Aplicar oportunamente las actualizaciones de seguridad de Microsoft correspondientes a agosto de 2026.

Productos Afectados

Algunos de los productos afectados son:

- Windows 10
- Windows 11
- Windows Server

Ver +INFO

Fecha de Publicación: 11/AGO/2026

INFO

Google chrome releases

CVE-2026-19137 – CVE-2026-19149
CVE-2026-19154 – CVE-2026-19157

Se identificaron 41 vulnerabilidades de seguridad en Google Chrome 151, incluyendo fallas críticas de uso después de liberar (Use-After-Free) y escritura fuera de límites en componentes como WebGL, Aura, Skia, ANGLE y Views. Estas vulnerabilidades podrían provocar corrupción de memoria, fallos del navegador y ejecución arbitraria de código.

Recomendación:

- Actualizar Google Chrome a la versión más reciente disponible.

Productos Afectados:

Los productos afectados son:

- Google Chrome para Windows
- Google Chrome para MacOS
- Google Chrome para Linux

Ver +INFO

Fecha de Publicación: 06/AGO/2026

INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
05/08/2026	CVE-2026-20303	Cisco	9.9	Se identificaron múltiples vulnerabilidades críticas en Cisco Catalyst SD-WAN relacionadas con validación incorrecta de entradas, controles de acceso y manejo inadecuado de archivos e información sensible, que podrían permitir acciones no autorizadas y comprometer el sistema afectado.
10/08/2026	CVE-2026-20337	Cisco	7.5	Se identificaron múltiples vulnerabilidades de alta severidad en ClamAV que pueden permitir a un atacante remoto provocar una denegación de servicio (DoS) al interrumpir el proceso de escaneo.
03/08/2026	CVE-2026-18733	AWS	8.8	Se identificó una vulnerabilidad de inyección de prompts en Amazon Strands Agents Tools anteriores a la versión 0.8.0, que permite a un atacante remoto ejecutar comandos arbitrarios del sistema operativo al evadir el mecanismo de consentimiento humano.
09/08/2026	CVE-2026-64564	Linux	9.8	Se identificó una vulnerabilidad en el kernel de Linux, específicamente en SCTP, que podría provocar un use-after-free al procesar mensajes ASCONF maliciosos. La falla puede causar corrupción de memoria y afectar la estabilidad del sistema.
08/08/2026	CVE-2026-64566	Linux	9.8	Se identificó una vulnerabilidad en el kernel de Linux, específicamente en XFRM/IPTFS, que puede provocar corrupción de memoria al manejar fragmentos compartidos. La falla podría causar un pánico del kernel y afectar la estabilidad del sistema.

Kimsuky lleva la IA al ataque: GitHub y AsyncRAT como armas cibernéticas

Investigadores de Genians revelaron detalles sobre una campaña de Kimsuky, denominada Operación GitPower, que destaca por el uso de IA para generar documentos y señuelos de phishing más convincentes. La actividad está dirigida principalmente a organizaciones diplomáticas, militares, de seguridad, políticas, académicas y relacionadas con activos virtuales. Los investigadores también identificaron el uso de modelos de lenguaje locales, incluyendo Ollama, GPT4All y Msty, como parte de las capacidades empleadas por el grupo. La campaña evidencia cómo Kimsuky está incorporando herramientas de IA para mejorar sus operaciones y aumentar la efectividad de sus técnicas de ingeniería social.

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral. Ver *+INFO*.

El ATAQUE

La campaña de Kimsuky comienza con archivos ZIP que contienen accesos directos de Windows (LNK) que aparentan ser documentos legítimos. Al abrirlos, se ejecuta PowerShell de forma oculta mientras se muestra un PDF señuelo para reducir las sospechas. Posteriormente, los scripts descargados desde GitHub recopilan información del sistema, crean archivos en directorios temporales y de AppData, y establecen persistencia mediante tareas programadas. Las cargas maliciosas, disfrazadas como archivos de imagen, corresponden a versiones cifradas de AsyncRAT, permitiendo mantener el acceso remoto al equipo comprometido. La campaña también emplea ofuscación, codificación Base64 y manipulación de cabeceras para dificultar la detección.

INFO

CONTEXT	INDICATOR	(MD5)
IPv4	112.216.9[.]171	N/A
IPv4	170.205.30[.]227	N/A
IPv4	185.27.134[.]140	N/A
IPv4	27.102.137[.]126	N/A
IPv4	27.102.137[.]159	N/A
IPv4	27.102.138[.]44	N/A

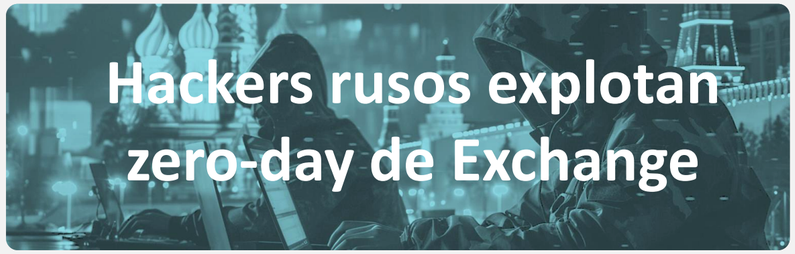
INFO

ÚLTIMAS NOTICIAS

Phishing suplanta a RingCentral

La plataforma Greatness, dedicada al phishing como servicio, ha evolucionado para atacar cuentas de Microsoft 365 mediante técnicas AiTM y códigos de dispositivo. Los atacantes suplantan servicios como RingCentral para evadir los filtros de correo y engañar a los usuarios. Tras comprometer las cuentas, pueden robar tokens de autenticación y acceder a Outlook, Teams, SharePoint y OneDrive, manteniendo el acceso durante semanas y obteniendo información corporativa sensible, credenciales y datos confidenciales de las organizaciones afectadas.

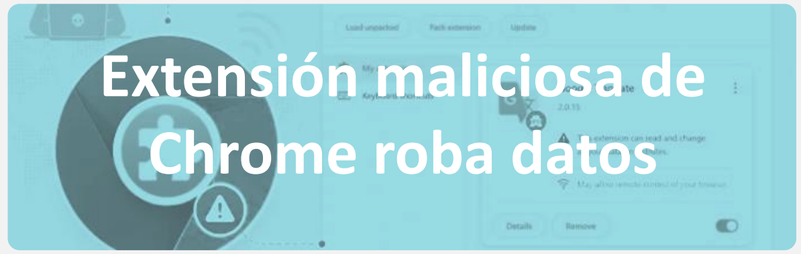
INFO



Hackers rusos explotan zero-day de Exchange

El grupo ruso Laundry Bear (Void Blizzard) explota la vulnerabilidad CVE-2026-42897 en Outlook Web Access para distribuir la puerta trasera OWAReaper. El ataque se activa al abrir un correo malicioso y permite ejecutar JavaScript, robar credenciales y tokens OAuth, acceder a buzones y mantener la persistencia incluso tras cambiar contraseñas o restaurar los sistemas afectados. La campaña está dirigida principalmente contra organizaciones gubernamentales y sectores estratégicos como telecomunicaciones, finanzas y aeroespacial.

INFO



Extensión maliciosa de Chrome roba datos

Una extensión maliciosa de Chrome que se hace pasar por Google Translate puede robar cookies, credenciales, historial y otros datos del navegador. Además, permite a los atacantes controlar remotamente las ventanas de Chrome, inyectar código y manipular sesiones sin que la víctima lo note. La campaña utiliza una cadena de infección que incluye Stealcv2, aumentando el riesgo de robo de cuentas, datos corporativos y fraude, además de facilitar ataques de phishing, secuestro de sesiones y acceso no autorizado a servicios empresariales.

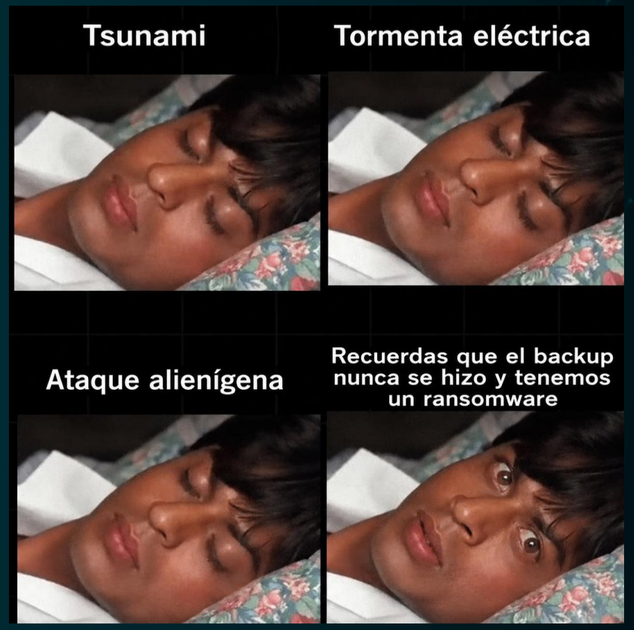
INFO

Prevenir hoy para recuperar mañana

La tranquilidad en ciberseguridad puede durar hasta que ocurre algo inesperado. Un ataque de ransomware, una falla del sistema o un error humano pueden provocar la pérdida de información importante. Por eso, contar con respaldos confiables no es una opción, sino una parte fundamental de la seguridad.

💾 Realiza copias de seguridad con frecuencia y evita depender de un único respaldo.
☁️ Guarda tus backups en diferentes ubicaciones para reducir el impacto de posibles incidentes.
🔐 Protege las copias de seguridad con contraseñas, cifrado y controles de acceso.
🧪 Comprueba que los respaldos funcionen antes de necesitarlos en una emergencia.
🚨 Considera el ransomware en tu plan de seguridad y asegúrate de que tus backups no sean accesibles para un atacante.
📋 Establece un plan de recuperación para saber cómo actuar ante una pérdida de información.

Porque tener un backup no significa estar protegido: también debes asegurarte de que esté disponible, protegido y listo para recuperarse cuando más lo necesites.



ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4