BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

OnyxC2 Stealer: el negocio del robo de credenciales por suscripción.

TLP:CLEAR
01.07.2026

CLICK PARA EMPEZAR

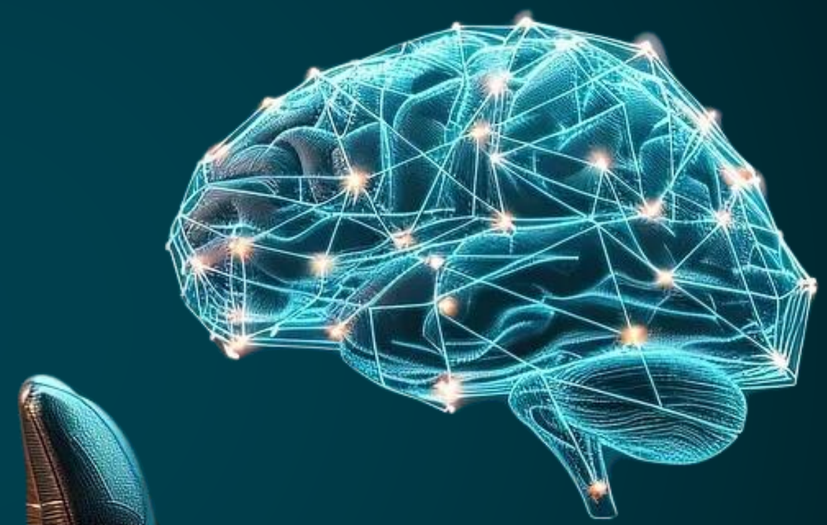
CYBERSOCDTS

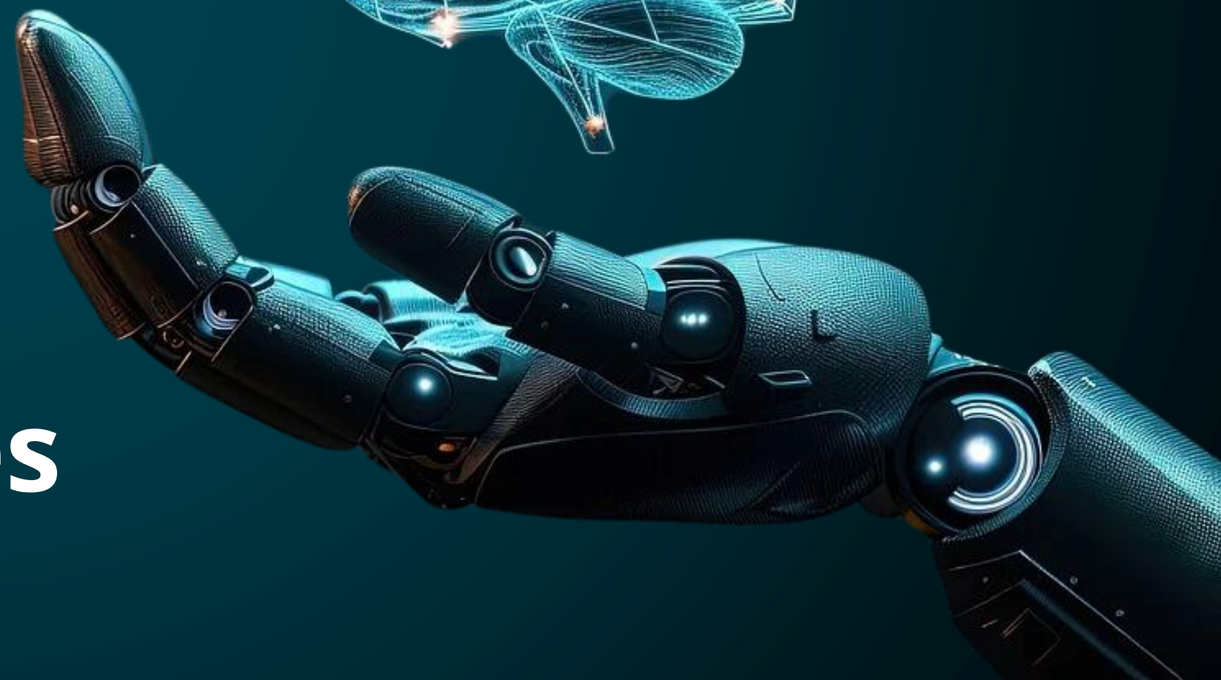
En esta edición:

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.

Cisco Identity Services Engine Remote Code Execution and Information Disclosure Vulnerabilities

CVE-2026-20181 – CVE-2026-20190

Critical (9.1)

Impacto: Ejecución remota de código y acceso no autorizado.

Resumen: Se identificaron múltiples vulnerabilidades en Cisco ISE e ISE-PIC que podrían ser explotadas por atacantes remotos para ejecutar código malicioso o acceder a información sensible en los dispositivos afectados. Cisco ha publicado actualizaciones de seguridad para corregir estas fallas y recomienda su pronta instalación, ya que no existen soluciones alternativas disponibles.

Producto Afectado

- Cisco Identity Services Engine (ISE)
- Cisco ISE Passive Identity Connector (ISE-PIC)

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad publicadas por Cisco.

Ver + INFO.

Fecha de Publicación: 19/JUN/2026 INFO

Remote Code Execution in Oracle PeopleSoft PeopleTools

CVE-2026-35273

Critical (9.8)

Impacto: Ejecución remota de código.

Resumen: Se identificó una vulnerabilidad crítica en el componente Update Environment Management de Oracle PeopleSoft Enterprise PeopleTools que afecta las versiones 8.61 y 8.62. La falla puede ser explotada remotamente por un atacante no autenticado a través de HTTP, permitiendo el compromiso completo del sistema afectado.

Producto Afectado

- Herramientas PeopleSoft Enterprise 8.61
- Herramientas PeopleSoft Enterprise 8.62

Ver +INFO.

Solución:

aplicar de inmediato los parches de seguridad oficiales proporcionados por Oracle (Critical Patch Updates)

Ver +INFO.

Fecha de Publicación: 11/JUN/2026 INFO

Apache HTTP Server: mod_http2 denial of service

CVE-2026-49975

High (7.5)

Impacto: Denegación de servicio (DoS).

Resumen: La vulnerabilidad de asignación de memoria con tamaños excesivos en el módulo mod_http del servidor Apache HTTP Server puede ser explotada mediante solicitudes HTTP maliciosas especialmente diseñadas. Esto provoca un consumo elevado de memoria que deriva en una denegación de servicio (DoS).

Producto Afectado

- Apache HTTP Server versiones 2.4.17 hasta 2.4.67.

Ver +INFO.

Solución:

Actualizar Apache HTTP Server a la versión 2.4.68, donde se corrige la vulnerabilidad.

Ver +INFO.

Fecha de Publicación: 25/JUN/2026 INFO

KVM: arm64: vgic-its: Drop the translation cache reference only for the erased entry

CVE-2026-46316

Critical (9.3)

Impacto: Corrupción de memoria e inestabilidad del sistema..

Resumen: Se identificó una vulnerabilidad en el núcleo de Linux, específicamente en el subsistema KVM para arquitectura ARM64 (vgic-its), relacionada con una gestión incorrecta de la caché de traducción. Esta condición de concurrencia permite inconsistencias al eliminar entradas de la caché, lo que puede derivar en corrupción de memoria o comportamiento inesperado del sistema.

Producto Afectado

Kernel de Linux en arquitecturas ARM64 con KVM (vgic-its) habilitado.

Ver +INFO.

Solución:

Aplicar las actualizaciones del kernel de Linux que corrigen el manejo de la caché en KVM (ARM64 vgic-its)

Ver +INFO.

Fecha de Publicación: 17/JUN/2026 INFO

Mozilla Foundation Security Advisory 2026-57

CVE-2026-12289 – CVE-2026-12290
CVE-2026-12291 – CVE-2026-12292

Mozilla publicó Firefox versión 152 para corregir múltiples vulnerabilidades de alta severidad que podían permitir ejecución de código remoto y escape de sandbox. Las fallas afectaban componentes como WebRender, HTTP networking y WebGPU, y podían ser explotadas mediante contenido web malicioso, incluyendo errores de memoria como use-after-free y fallos de escalada de privilegios.

Recomendación:
Actualizar Mozilla Firefox a la versión 152 o superior para corregir vulnerabilidades críticas de ejecución remota de código y escape de sandbox.

Productos Afectados

Los productos afectados son:

Mozilla Firefox versiones anteriores a 152.

Ver +INFO

Fecha de Publicación: 16/JUN/2026

INFO

Google chrome releases

CVE-2026-12437 – CVE-2026-12438
CVE-2026-12439 – CVE-2026-12440

Google publicó una actualización de seguridad para Google Chrome que corrige 33 vulnerabilidades, incluidas fallas críticas de tipo use-after-free que podrían permitir ejecución remota de código. Estas vulnerabilidades afectan varios componentes del navegador y pueden ser explotadas al visitar sitios web maliciosos sin interacción adicional del usuario.

Recomendación:

- Actualizar Google Chrome a la versión 149.0.7827.155 o 149.0.7827.156 para Windows y macOS.
- 149.0.7827.155 para Linux.

Productos Afectados:

Los productos afectados son:

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

Ver +INFO

Fecha de Publicación: 16/JUN/2026

INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
10/06/2026	CVE-2026-0274	Paloalto	8.1	Una validación incorrecta de la vulnerabilidad de credenciales en la integración CommvaultSecurityIQ para Cortex XSOAR y Cortex XSIAM permite que un atacante no autenticado acceda y modifique recursos protegidos.
17/06/2026	CVE-2026-44815	Microsoft	9.8	El desbordamiento de búfer basado en pila en el cliente DHCP de Windows permite que un atacante no autorizado ejecute código a través de una red.
23/06/2026	CVE-2026-50656	Microsoft	7.8	Microsoft ha identificado una vulnerabilidad de elevación de privilegios en el motor de protección de Microsoft Defender y está trabajando en una actualización de seguridad para corregirla.
23/06/2026	CVE-2026-45586	Microsoft	7.8	Una resolución incorrecta de enlaces antes del acceso a archivos ('seguimiento de enlace') en el Marco de Traducción Colaborativa de Windows permite a un atacante autorizado elevar privilegios localmente.
25/06/2026	CVE-2026-20175	Cisco	6.1	La vulnerabilidad en Cisco Finesse permite a un atacante remoto inyectar código o cargar contenido malicioso en sesiones activas mediante un enlace manipulado, lo que puede derivar en ataques en el navegador y exposición de información sensible.
23/06/2026	CVE-2026-13007	Tenable	7.5	Permite que usuarios no autenticados accedan a endpoints de la API y expongan información sensible como credenciales LDAP y configuraciones SAML, que pueden ser almacenadas en cachés mal configuradas y reutilizadas, provocando fuga de datos.

OnyxC2 Stealer: el negocio del robo de credenciales por suscripción.

Investigadores de BlackFog revelaron detalles sobre OnyxC2, una plataforma de malware especializada en el robo de información que se comercializa como un servicio listo para usar. La herramienta ofrece amplias capacidades para comprometer sistemas, extraer credenciales, cookies, datos financieros y otra información sensible de navegadores, aplicaciones empresariales y monederos de criptomonedas. Además del robo de datos, incorpora funciones de acceso remoto y persistencia que permiten a los atacantes mantener el control de los equipos comprometidos durante largos periodos. Su capacidad para evadir soluciones de seguridad y su disponibilidad comercial evidencian una evolución del malware hacia modelos cada vez más sofisticados y accesibles para los ciberdelincuentes.

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

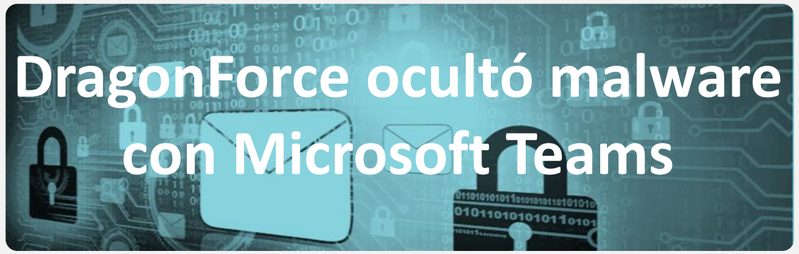
El ATAQUE

El ataque se lleva a cabo mediante instaladores o aplicaciones aparentemente legítimas que contienen una DLL maliciosa disfrazada de componente confiable. Al ejecutar el archivo, la carga útil se descifra y ejecuta en memoria, evadiendo la detección de herramientas de seguridad. Una vez activo, OnyxC2 recopila credenciales, cookies, datos de autocompletado, información de gestores de contraseñas, extensiones de autenticación multifactor y monederos de criptomonedas, además de habilitar capacidades de acceso remoto como captura de pantalla, registro de pulsaciones de teclado, gestión de archivos y ejecución de comandos. Estas funciones, combinadas con mecanismos de persistencia y evasión, permiten a los atacantes mantener acceso prolongado al sistema comprometido y ampliar el alcance del ataque hacia otros servicios o entornos corporativos.

INFO

CONTEXT	INDICATOR	(MD5)
Dominio	Akmuniverstall[.]top	N/A
SHA1	c333a821f1764abe2aed2c1ab27d2349f64e4264	N/A
SHA1	04ccc8f9f5e343f94ad9f41f08439b545d4b8486	N/A
SHA256	41999a3d0da035ff8068905c90235ea50121329cb0661e38d745974ebf5e3ae2	cf64c7e2e3897ae5fce3d5414e3d1d27
SHA256	f6e4b09ef788adef3f65fd2b99da8f5be5391be29471676dc07040a56c8fdfab	b5b603ff57142a454c3b0fb12eb8a4eb
SHA256	78945c844fc23dd3446cf17987edeeb6cc21986820c92df82a126af24a5a38d1	N/A
SHA256	d89bb4b23a67814ef511e4e9dda7ad36fa519a322fa7c25ea451c7dd7ef61e54	N/A

ÚLTIMAS NOTICIAS



DragonForce ocultó malware con Microsoft Teams

Investigadores de Broadcom informan que el grupo de ransomware DragonForce comprometió una empresa estadounidense de servicios utilizando técnicas avanzadas de evasión. Los atacantes emplearon una puerta trasera personalizada para ocultar su tráfico malicioso a través de la infraestructura de Microsoft Teams, haciendo que las comunicaciones parecieran tráfico legítimo de la plataforma. Esta técnica les permitió mantener acceso persistente en la red, evadir herramientas de seguridad y finalmente desplegar ransomware para el robo y cifrado de información sensible.

INFO

Falsos códigos de Claude distribuyen AsyncRAT

Investigadores de FortiGuard Labs detectaron una campaña que aprovecha el interés por la inteligencia artificial para distribuir malware en sistemas Windows mediante archivos comprimidos disfrazados de guías técnicas. La cadena de ataque ejecuta múltiples etapas usando scripts de PowerShell, técnicas de ofuscación, exclusión de antivirus y procesos legítimos de Windows para evadir la detección. Finalmente, el ataque despliega troyanos de acceso remoto como AsyncRAT, permitiendo a los atacantes controlar los equipos, monitorear la actividad del usuario y exfiltrar información sensible.

INFO

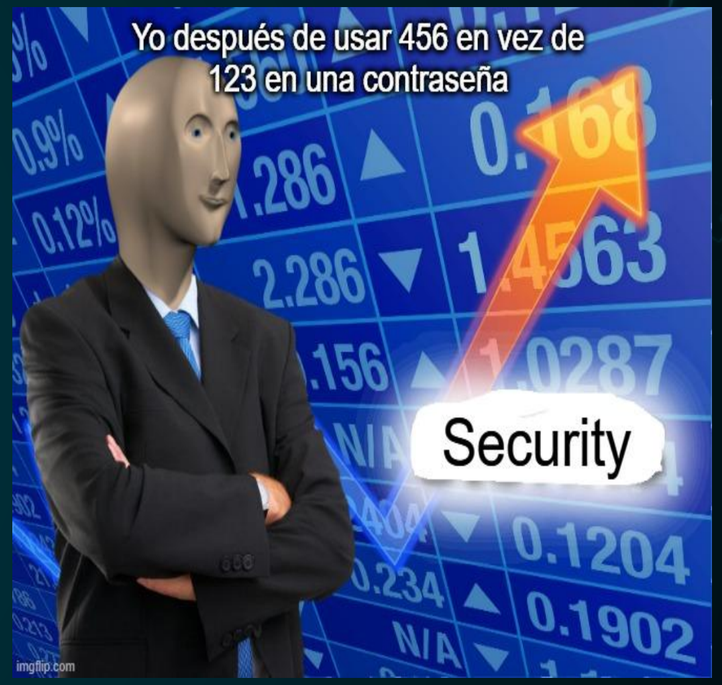
ShinyHunters explota un zero-day de Oracle.

El grupo de extorsión ShinyHunters explotó una vulnerabilidad zero-day crítica (CVE-2026-35273) en Oracle PeopleSoft Enterprise PeopleTools, específicamente en el componente EMHub, permitiendo ejecución remota de código sin autenticación. La campaña, activa entre mayo y junio de 2026, afectó a más de 100 organizaciones, principalmente universidades, donde se exfiltraron grandes volúmenes de datos mediante herramientas de acceso remoto y técnicas de evasión. Oracle ya corrigió la falla y recomendó aplicar parches de seguridad de forma urgente.

INFO

La seguridad de acceso: más allá de cambiar unos números

En ciberseguridad, uno de los errores más frecuentes es asumir que pequeñas acciones son suficientes para estar protegidos. Cambiar algunos números en una contraseña, ignorar una actualización porque "nunca ha pasado nada" o confiar en hábitos conocidos puede generar una sensación de seguridad que no siempre corresponde con la realidad. Los atacantes suelen aprovechar precisamente estas percepciones erróneas para comprometer cuentas, sistemas e información.



🔍 Cuestiona periódicamente tus hábitos de seguridad y evita asumir que son suficientes.
🔐 Utiliza medidas de protección que realmente reduzcan el riesgo, como contraseñas robustas y MFA.
🧮 No confundas comodidad con seguridad; lo más fácil suele ser también lo más predecible.
⚠️ Evita confiar en que la ausencia de incidentes significa que no existen vulnerabilidades.
🧠 Recuerda que la seguridad es un proceso continuo, no una acción puntual.
👥 Comparte una cultura de prevención basada en hechos y no en percepciones.

El mayor riesgo no siempre es una vulnerabilidad técnica; a veces es creer que estamos protegidos cuando no lo estamos.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4