BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

BTMOB RAT se propaga en Latinoamérica bajo el modelo Malware-as-a-Service

TLP:CLEAR
10.06.2026

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 Unified Communications Manager Server-Side Request Forgery Vulnerability

CVE-2026-20230

High (8.6)

Impacto: Escritura arbitraria de archivos y escalada de privilegios.

Resumen: Cisco identificó una vulnerabilidad crítica en Cisco Unified Communications Manager (Unified CM) y Unified CM SME que permite a un atacante remoto no autenticado realizar ataques SSRF y potencialmente obtener privilegios de administrador o root en los sistemas afectados cuando el servicio WebDialer está habilitado.

Producto Afectado

- Cisco Unified Communications Manager (WebDialer habilitado)
- Cisco Unified Communications Manager Session Management Edition (WebDialer habilitado)

Ver +INFO.

Solución:

Actualizar a las versiones corregidas publicadas por Cisco y, como medida temporal, deshabilitar el servicio WebDialer si no es necesario.

Ver + INFO.

Fecha de Publicación: 03/JUN/2026

Vulnerability in Oracle REST Data Services

CVE-2026-46840

Critical (10)

Impacto: Acceso no autorizado.

Resumen: Una vulnerabilidad crítica en Oracle REST Data Services (ORDS) permite a un atacante remoto no autenticado comprometer completamente el servicio mediante acceso HTTPS. La explotación exitosa puede resultar en la toma de control del sistema y afectar a otros productos relacionados.

Producto Afectado

Oracle REST Data Services (ORDS) – componente Backend-as-a-Service (BaaS), versiones 24.2.0 a 26.1.0.

Ver +INFO.

Solución:

Si estás en versiones 24.2.0–26.1.0 se recomienda aplicar:

- Oracle CPU May 2026 o posterior
- o versión ORDS posterior al build corregido del CPU.

Ver +INFO.

Fecha de Publicación: 29/MAY/2026

Windows Netlogon Remote Code Execution Vulnerability

CVE-2026-41089

Critical (9.8)

Impacto: Ejecución remota de código.

Resumen: Se ha detectado la explotación activa de una vulnerabilidad crítica en el servicio Windows Netlogon de los controladores de dominio de Windows Server. La falla permite a atacantes remotos no autenticados ejecutar código con privilegios elevados mediante solicitudes especialmente manipuladas, lo que podría derivar en el compromiso total de la infraestructura afectada.

Producto Afectado

- Windows Server Versiones soportadas desde 2012 en adelante

Ver +INFO.

Solución:

Aplicar las actualizaciones de seguridad publicadas en el Patch Tuesday de mayo 2026 para todas las versiones soporta das de Windows Server.

Ver +INFO.

Fecha de Publicación: 09/JUN/2026 INFO

GlobalProtect Authentication Bypass Vulnerabilities

CVE-2026-0257

High (7.8)

Impacto: Acceso no autorizado.

Resumen: Las vulnerabilidades de omisión de autenticación (Authentication Bypass) en el portal y gateway de GlobalProtect de los dispositivos Palo Alto Networks que ejecutan PAN-OS® permiten a un atacante eludir las restricciones de seguridad y establecer una conexión VPN no autorizada.

Producto Afectado

Firewalls de Palo Alto Networks que ejecutan PAN-OS, especialmente aquellos que usan los servicios de GlobalProtect (portal y gateway VPN)

Ver +INFO.

Solución:

Aplicar los parches de seguridad de PAN-OS proporcionadas por Palo Alto Network (versiones corregidas posteriores a las vulnerables).

Ver +INFO.

Fecha de Publicación: 03/JUN/2026 INFO

Google fixes one actively exploited Android zero-day, 124 flaws

CVE-2025-48595 – CVE-2025-65018
CVE-2026-0043

Google lanzó las actualizaciones de seguridad de Android de junio de 2026 para corregir 124 vulnerabilidades, incluida una falla de día cero que estaba siendo utilizada en ataques dirigidos. La compañía también solucionó varias vulnerabilidades críticas que podían permitir la ejecución de código o la escalada de privilegios en dispositivos sin actualizar.

Recomendación:
Actualizar Android e instalar los parches de seguridad más recientes lo antes posible.

Productos Afectados

Los productos afectados son:

Dispositivos con Android 14 y versiones posteriores.

Ver +INFO

Fecha de Publicación: 02/JUN/2026

INFO

Google chrome releases

CVE-2026-9872 – CVE-2026-9873
CVE-2026-9874 – CVE-2026-9875

Google lanzó una actualización de Chrome que corrige 151 vulnerabilidades, incluidas 22 críticas, en componentes clave del navegador, con riesgos de ejecución remota de código, corrupción de datos y escape del sandbox en múltiples sistemas operativos.

Recomendación:
Actualizar Google Chrome a la versión estable 148.0.7778.216/217 en Windows, 148.0.7778.215/216 en macOS y 148.0.7778.215 en Linux.

Productos Afectados:

Los productos afectados son:

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

Ver +INFO

Fecha de Publicación: 27/MAY/2026

INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
26/05/2026	CVE-2026-45659	Microsoft	8.8	La deserialización de datos no confiables en Microsoft Office SharePoint permite que un atacante autorizado ejecute código a través de una red.
03/06/2026	CVE-2026-49975	Apache	9.8	Permite a un atacante remoto no autenticado realizar un ataque de denegación de servicio (DoS) contra servidores web que utilizan HTTP/2, como nginx, Apache httpd, Microsoft IIS, Envoy y Cloudflare Pingora, provocando una sobrecarga de recursos que puede degradar el rendimiento del servicio o causar su caída completa.
04/06/2026	CVE-2026-46839	Oracle	9.0	Permite a un atacante con privilegios limitados y acceso a la red mediante HTTPS comprometer Oracle REST Data Services (Core) en versiones 24.2.0 a 26.1.0, explotando una vulnerabilidad fácilmente aprovechable que puede derivar en la toma de control total del servicio, con impacto crítico en la confidencialidad, integridad y disponibilidad.
04/06/2026	CVE-2026-50076	Apache	9.8	Permite a un atacante remoto explotar una vulnerabilidad de deserialización en Apache Fory (fory-core Java SDK) anterior a la versión 1.1.0, eludiendo mecanismos de validación como TypeChecker y listas de bloqueo, lo que puede derivar en la ejecución de código o el compromiso del sistema.

BTMOB RAT se propaga en Latinoamérica bajo el modelo Malware-as-a-Service

Investigadores de ESET detectaron la reaparición de BTMOB, un troyano de acceso remoto para Android que funciona bajo un modelo de malware como servicio (MaaS). Esta herramienta permite a ciberdelincuentes con escasos conocimientos técnicos crear y distribuir aplicaciones bancarias maliciosas mediante una interfaz sin necesidad de programación. La amenaza está siendo utilizada en campañas dirigidas principalmente a usuarios de Brasil y Latinoamérica, expandiéndose a través de técnicas de phishing y sitios que imitan servicios y tiendas de aplicaciones legítimas. Su facilidad de uso y bajo coste lo convierten en una herramienta accesible para múltiples actores maliciosos. Además, su enfoque modular permite adaptar rápidamente las campañas según la región o el objetivo.

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

El ATAQUE

Los atacantes distribuyen BTMOB mediante campañas de phishing que suplantan servicios conocidos como plataformas de streaming, aplicaciones de criptomonedas o tiendas oficiales de apps. Desde estos sitios falsos, las víctimas son inducidas a descargar archivos APK maliciosos generados automáticamente mediante la plataforma MaaS, lo que permite personalizar las aplicaciones según el país o el objetivo de la campaña. Una vez instalado, el malware solicita permisos elevados abusando de los Servicios de Accesibilidad de Android, lo que le permite obtener control total del dispositivo sin interacción adicional. A partir de ahí, puede registrar la actividad del usuario, capturar pantallas, robar credenciales bancarias y datos sensibles, y ejecutar acciones remotas como si fuera el propio usuario. También incorpora capacidades de control persistente que facilitan mantener el acceso incluso tras reinicios o cambios en el dispositivo, aumentando el impacto de la infección.

INFO

CONTEXT	INDICATOR	(MD5)
SHA256	a892f1ef2e530d67bf948a48c734da3f27718eb8b883ca0b686ddb0a81071731	dbd8934e2e80890a7067097079a40182
SHA256	e5a9fdff900dd502e8f3dce52d2d1b69aa9afafb5094a28f9037e8770db0e63b	7f493c8b8c3a1117c90e1f679c782d42
SHA256	75dd4fb011ed598374a46fc0d9c0d1d64a298341c34afc83a56a6983cfd27764	7881c012c247d29dbf43b05c8b042cc1
IPv4	191[.]96[.]78[.]172	N/A
IPv4	191[.]96[.]225[.]241	N/A
IPv4	200[.]9[.]155[.]153	N/A
IPv4	195[.]160[.]221[.]203	N/A
Dominio	Arbsniper[.]com	N/A

INFO

ÚLTIMAS NOTICIAS

Atacantes explotan FortiClient EMS para instalar EKZ Infostealer

Arctic Wolf detectó una campaña activa en entornos gestionados con FortiClient Endpoint Management Server (EMS), donde los atacantes distribuyen un falso parche de Fortinet que instala EKZ Infostealer. Este malware roba credenciales almacenadas en navegadores y las exfiltra a servidores remotos controlados por los atacantes. La campaña abusa de la consola de administración de EMS para ejecutar comandos de PowerShell de forma remota, lo que permite propagar la infección a múltiples endpoints dentro del entorno sin necesidad de acceso individual a cada dispositivo, aumentando el impacto del ataque.

INFO

MuddyWater realiza espionaje en 9 países usando carga lateral de DLL

MuddyWater, grupo de ciberespionaje vinculado a Irán, ha realizado una campaña global contra organizaciones de sectores como industria, educación, finanzas y administración pública, utilizando técnicas de carga lateral de DLL con binarios legítimos para ejecutar código malicioso de forma encubierta. La operación combina PowerShell y Node.js para reconocimiento, robo de credenciales, recopilación de información y movimiento lateral, además de herramientas para exfiltrar datos de navegadores y establecer túneles ocultos de comunicación.

INFO

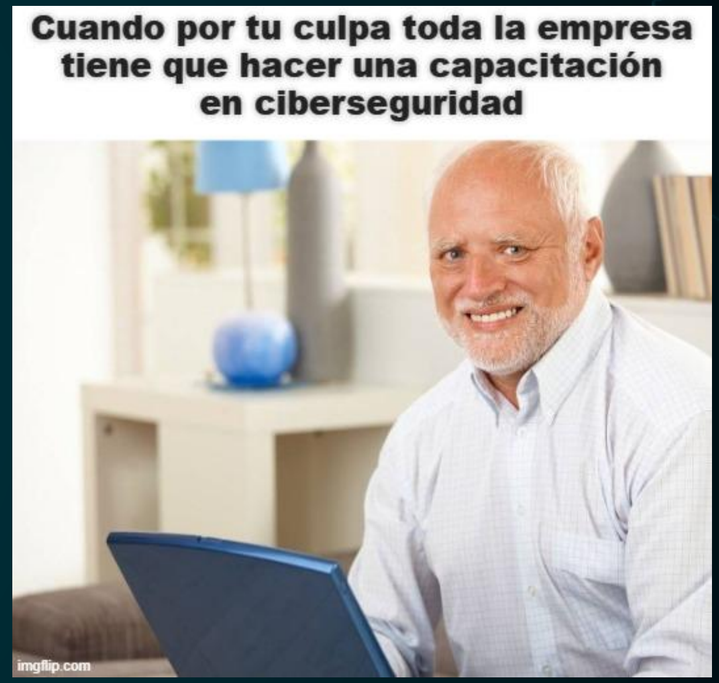
Malware en NuGet y npm roba credenciales bancarias y secretos en la nube.

Investigadores de seguridad descubrieron un paquete malicioso en NuGet que suplanta un SDK legítimo de Sicoob y roba información sensible como certificados PFX, credenciales y datos bancarios de clientes. Paralelamente, se identificó una campaña en npm con múltiples paquetes maliciosos diseñados para exfiltrar secretos en entornos de desarrollo, incluyendo credenciales de AWS, tokens de CI/CD y datos de infraestructura en la nube. Ambos casos forman parte de una ola de ataques a la cadena de suministro que utilizan repositorios de confianza para comprometer a desarrolladores y organizaciones.

INFO

Tus clics en internet: más consecuencias de las que crees

En ciberseguridad, los incidentes no siempre ocurren por ataques sofisticados. En muchas ocasiones, comienzan con acciones cotidianas como hacer clic en un enlace malicioso, descargar un archivo no verificado o ignorar una alerta de seguridad. Cuando sucede un incidente, el impacto puede extenderse más allá de una sola persona, afectando procesos, información y recursos de toda la organización. Por ello, fortalecer la cultura de seguridad es una tarea compartida.



🔍 Verifica dos veces antes de hacer clic en enlaces o abrir archivos adjuntos.
⏳ Tómate unos segundos para analizar correos inesperados o solicitudes urgentes.
📧 Confirma por otro medio cualquier solicitud inusual de información, dinero o credenciales.
🚨 Si algo parece sospechoso, repórtalo inmediatamente; es mejor una falsa alarma que un incidente real.
🧠 Mantente alerta: los ciberdelincuentes suelen aprovechar distracciones y rutinas.
🔐 Protege tu información y la de la organización siguiendo las políticas de seguridad establecidas.
👥 Comparte buenas prácticas con tu equipo y ayuda a fortalecer la cultura de ciberseguridad.

Si un error puede afectar a todos, una buena práctica también puede protegernos a todos.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4