BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

ClickLock Stealer: el nuevo infostealer que deja inutilizable tu Mac

TLP:CLEAR
24.07.2026

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.

ColdFusion | Improper Limitation of a Pathname to a Restricted Directory

CVE-2026-48282

Critical (10.0)

Impacto: Ejecución arbitraria de código.

Resumen: Se identificó una vulnerabilidad crítica de tipo **Path Traversal** en Adobe ColdFusion que afecta las versiones 2025.9, 2023.20 y anteriores. 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 afectado, ampliando el alcance del impacto sobre el sistema comprometido.

Producto Afectado

- Adobe ColdFusion 2025 (versiones hasta la 2025.9).
- Adobe ColdFusion 2023 (versiones hasta la 2023.20).

Ver +INFO.

Solución:

Actualizar Adobe ColdFusion a la versión más reciente proporcionada por Adobe.

Ver + INFO.

Fecha de Publicación: 08/JUL/2026

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.

Resumen: Se identificaron múltiples vulnerabilidades en Cisco Identity Services Engine (ISE) y Cisco ISE Passive Identity Connector (ISE-PIC) que podrían ser explotadas remotamente por un atacante para ejecutar código arbitrario o divulgar información sensible en los dispositivos afectados.

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: 06/JUL/2026

LDAP authentication bypass in Agentless VPN and FSSO

CVE-2026-22153

High (7.5)

Impacto: Control de acceso inadecuado.

Resumen: Se identificó una vulnerabilidad de omisión de autenticación en el componente fnbamd de FortiOS que, bajo una configuración específica de servidor LDAP, podría permitir que un atacante no autenticado eluda la autenticación LDAP utilizada en políticas de VPN sin agente o FSSO.

Producto Afectado

- FortiOS 7.6 (versiones desde 7.6.0 a 7.6.4).

Ver +INFO.

Solución:

Actualizar a FortiOS 7.6.5 o superior.

Ver +INFO.

Fecha de Publicación: 04/JUL/2026 INFO

Unauthenticated VNC access exposed on all interfaces

CVE-2026-59835

High (7.7)

Impacto: Divulgación de información.

Resumen: Se identificó una vulnerabilidad de exposición de recursos en FortiSandbox que podría permitir que un atacante no autenticado acceda al servidor VNC de las máquinas virtuales utilizadas para realizar escaneos mediante solicitudes de red.

Producto Afectado

- FortiSandbox 5.0 (versiones desde 5.0.0 a 5.0.2).
- FortiSandbox 4.4 (versiones desde 4.4.3 a 4.4.8).

Ver +INFO.

Solución:

Actualizar a la versión mas reciente de FortiSandbox.

Ver +INFO.

Fecha de Publicación: 14/JUL/2026 INFO

Microsoft security updates

CVE-2026-50656

Microsoft publicó una actualización de seguridad para Microsoft Malware Protection Engine que corrige una falla de escalada de privilegios local en Windows Defender. Esta vulnerabilidad podría permitir que un atacante autenticado obtenga privilegios de sistema mediante un ataque de baja complejidad en sistemas Windows afectados.

Recomendación:

Actualizar Microsoft Malware Protection Engine a la versión corregida 1.1.26060.3008 y habilitar las actualizaciones automáticas de seguridad.

Productos Afectados

Los productos afectados son:

- Microsoft Malware Protection Engine
- Windows Defender en Windows 10 y Windows 11

Ver +INFO

Fecha de Publicación: 08/JUL/2026

INFO

Google chrome releases

CVE-2026-15112 – CVE-2026-15129
CVE-2026-15132 – CVE-2026-15108

Google publicó una actualización de seguridad para Google Chrome que corrige 27 vulnerabilidades, incluidas fallas críticas de corrupción de memoria que podrían permitir la ejecución remota de código al visitar un sitio web malicioso. Se recomienda actualizar el navegador a la versión más reciente.

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: 08/JUL/2026

INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
02/07/2026	CVE-2026-53917	Apache	7.5	Una vulnerabilidad de asignación incorrecta de memoria en Apache ActiveMQ podría permitir que un usuario autenticado provoque una denegación de servicio (DoS) mediante mensajes OpenWire especialmente manipulados.
01/07/2026	CVE-2026-20191	Cisco	7.5	Una vulnerabilidad en Cisco Catalyst Center podría permitir que un atacante remoto no autenticado lea archivos arbitrarios de un contenedor restringido mediante el envío de una solicitud HTTP especialmente diseñada.
08/07/2026	CVE-2026-0288	Palo alto	7.2	Múltiples vulnerabilidades de desbordamiento de búfer en el componente User-ID Terminal Server Agent (TSA) de PAN-OS podrían permitir que un atacante no autenticado provoque una denegación de servicio (DoS) o ejecute código arbitrario mediante tráfico de red especialmente diseñado.
08/07/2026	CVE-2026-43499	Linux	7.8	Una vulnerabilidad en el núcleo de Linux, en el componente `rtmutex`, podría provocar corrupción de memoria y condiciones de Use-After-Free (UAF) debido al manejo incorrecto de tareas durante la eliminación de un waiter, afectando la estabilidad del sistema.
07/07/2026	CVE-2026-57992	Microsoft	7.5	El uso gratuito en Microsoft Edge (basado en Chromium) permite a un atacante no autorizado ejecutar código a través de una red.
02/07/2026	CVE-2026-55957	Apache	7.3	Permite que atacantes se autentiquen sin proporcionar la contraseña correcta cuando JNDIRealm está configurado para usar GSSAPI, lo que puede derivar en acceso no autorizado a aplicaciones protegidas por Apache Tomcat.

ClickLock Stealer: el nuevo infostealer que deja inutilizable tu Mac

Investigadores de Group-IB revelaron detalles sobre ClickLock Stealer, un malware dirigido a usuarios de macOS que emplea ingeniería social y coerción para obtener credenciales. La amenaza utiliza campañas ClickFix para engañar a las víctimas, ejecutar comandos maliciosos e instalar mecanismos de persistencia que bloquean el entorno de trabajo hasta forzar la introducción de la contraseña del sistema. Una vez obtenida, permite extraer credenciales del navegador, cookies, datos del Llavero de macOS, carteras de criptomonedas y archivos de gestores de contraseñas. Su enfoque basado en la manipulación del usuario refleja una evolución de las técnicas de robo de información contra equipos macOS.

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

El ATAQUE

El ataque de ClickLock Stealer comienza con una campaña de ingeniería social basada en ClickFix, donde las víctimas son engañadas para copiar y ejecutar comandos maliciosos en Terminal bajo la apariencia de una verificación legítima. Tras la ejecución, el malware instala mecanismos de persistencia mediante LaunchAgents y, en el siguiente inicio de sesión, bloquea el entorno del usuario cerrando aplicaciones de forma repetitiva hasta forzar la introducción de la contraseña del sistema. Una vez obtiene las credenciales, ClickLock extrae información sensible como datos del Llavero de macOS, credenciales y cookies del navegador, archivos de gestores de contraseñas y monederos de criptomonedas. La combinación de automatización, persistencia y técnicas de presión psicológica permite a los atacantes evadir la interacción del usuario y maximizar el robo de información.

INFO

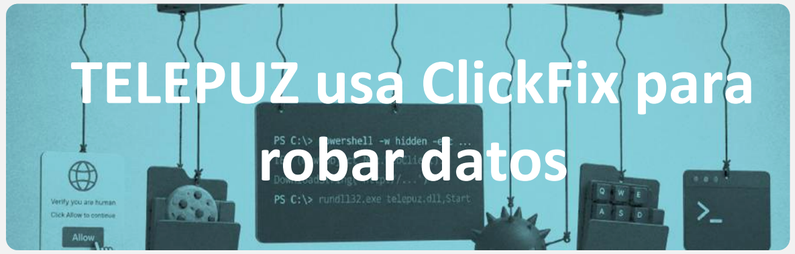
CONTEXT	INDICATOR	(MD5)
Dominio	update-check[.]com	N/A
Dominio	Panalobet[.]ph	N/A
Dominio	cottonbox.co[.]il	N/A
Dominio	store.grafsynergy[.]com	N/A
SHA1	8dda05168ea8610a2449419a47517bc32823d6ec	08ef1c04c21622901918f27e34589278
SHA1	b67aa4f598c0ea625a7409ea7884e10a7bc9c3ff	e53fdadff0516d34432b9d494da2eb62
SHA1	d9617710d4ed8e9b87f6fee0b7014c4101effba0	5d13cb18083fe73c85673618ad866f85

ÚLTIMAS NOTICIAS

RedWing spyware de Android como servicio

Investigadores de Zimperium zLabs identificaron RedWing, un spyware para Android distribuido como servicio mediante Telegram que permite crear aplicaciones maliciosas personalizadas sin conocimientos avanzados. La amenaza utiliza phishing y falsas aplicaciones legítimas para obtener permisos críticos, con los que puede robar credenciales, interceptar códigos 2FA, acceder a archivos, capturar pantalla, activar cámara y micrófono, y espiar la actividad del dispositivo. Su modelo Malware como Servicio (MaaS) evidencia cómo herramientas avanzadas de vigilancia están cada vez más disponibles para ciberdelincuentes.

INFO



TELEPUZ usa ClickFix para robar datos

Investigadores de Elastic Security Labs identificaron TELEPUZ, un malware modular distribuido mediante campañas ClickFix que engañan a las víctimas para ejecutar comandos maliciosos. La amenaza incorpora técnicas avanzadas de evasión, persistencia y comunicación con servidores de mando y control, permitiendo ejecutar comandos remotos, robar cookies, registrar pulsaciones, capturar pantallas e inyectar código en navegadores. Su desarrollo activo y posible modelo de Malware como Servicio (MaaS) apuntan a una amenaza en expansión.

INFO

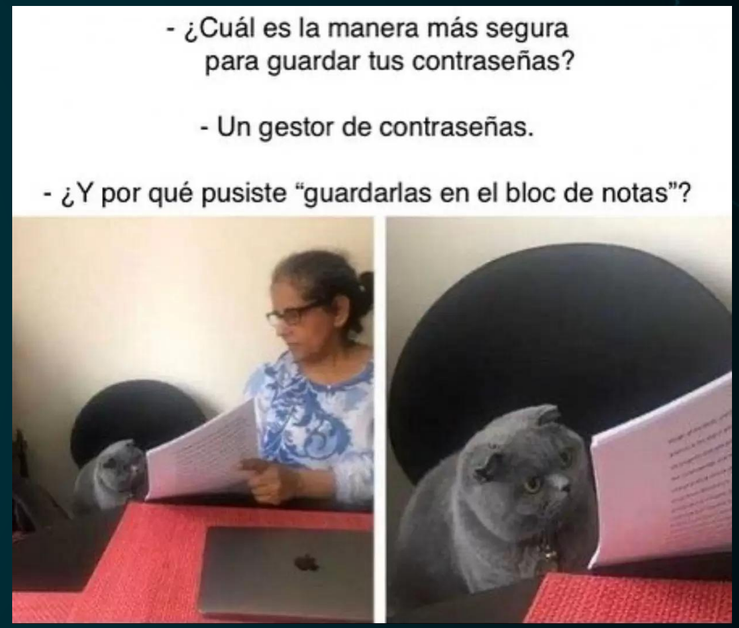
GodDamn renueva el ransomware Beast

Investigadores de Symantec Threat Hunter analizaron GodDamn, una nueva variante de ransomware vinculada a las familias Beast y Monster. En el ataque, los operadores utilizaron AnyDesk para acceso remoto, herramientas de robo de credenciales y el controlador PoisonX para desactivar las defensas del sistema antes de moverse lateralmente por la red y desplegar el ransomware. La campaña demuestra una operación bien organizada que combina acceso remoto, evasión de seguridad y robo de credenciales antes del cifrado de los equipos.

INFO

No es la contraseña, es cómo la administras

Crear una contraseña robusta es solo el primer paso. La forma en que administramos nuestras credenciales puede marcar la diferencia entre mantener nuestras cuentas protegidas o facilitar un acceso no autorizado. Pequeñas decisiones, como reutilizar contraseñas, almacenarlas en lugares inseguros o compartirlas sin protección, aumentan significativamente el riesgo.



🔍 Revisa si reutilizas contraseñas en diferentes plataformas.
🛡️ Almacena tus credenciales únicamente en herramientas diseñadas para ello.
🔢 Habilita MFA en los servicios más importantes.
🔑 Crea contraseñas largas y únicas en lugar de hacer pequeñas variaciones de una misma clave.
📧 Mantén actualizados tus métodos de recuperación de cuenta (correo y teléfono).
🚨 Activa las notificaciones de inicio de sesión para detectar accesos no autorizados.
🗑️ Elimina las cuentas que ya no utilizas para reducir tu superficie de exposición.

La fortaleza de una contraseña no solo se mide por cómo fue creada, sino también por cómo es administrada.

ISO 27001

ISO 20000

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4