BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Scatter Spider lanza Ransomware en sistemas VMware secuestrados

TLP:CLEAR
4.08.2025

CLICK PARA EMPEZAR

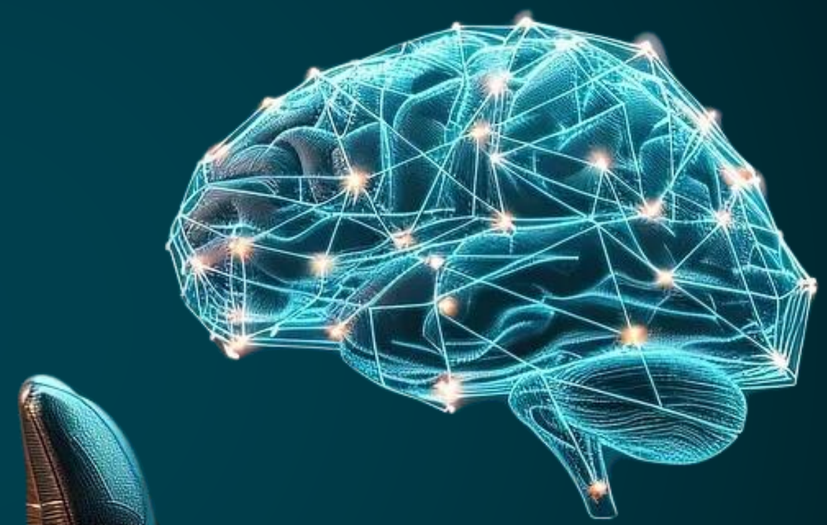
CYBERSOCDTS

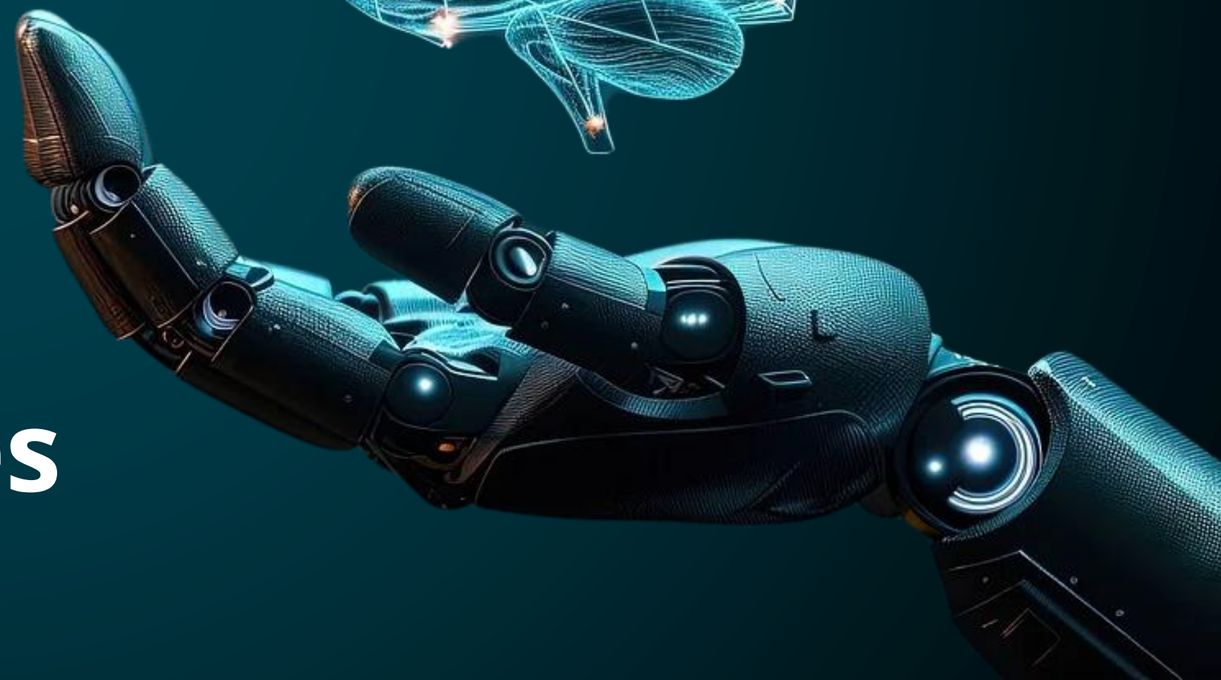
En esta edición: → Scatter Spider lanza Ransomware en sistemas VMware secuestrados

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 Unauthenticated Remote Code Execution Vulnerabilities

CVE-2025-20281

Critical (10)

Impacto: Ejecución de código no autorizado.

Resumen: Múltiples vulnerabilidades en Cisco Identity Services Engine (ISE) y Cisco ISE Passive Identity Connector (ISE-PIC) podrían permitir que un atacante remoto no autenticado emita comandos en el sistema operativo subyacente como usuario root.

Versiones Afectadas

Versiones 3.3 y 3.4 de Cisco ISE e ISE-PIC, independientemente de la configuración del dispositivo. Estas vulnerabilidades no afectan a Cisco ISE e ISE-PIC versión 3.2 o anterior.

Solución:

Cisco ha lanzado actualizaciones de software gratuitas que aborda la vulnerabilidad descrita en este boletín *Ver +INFO.*

Fecha de Publicación: 24/JUL/2025 INFO

Microsoft SharePoint Server Remote Code Execution Vulnerability

CVE-2025-53770

Critical (9.8)

Impacto: Ejecución de código no autorizado.

Resumen: La deserialización de datos que no son de confianza en Microsoft SharePoint Server local permite a un atacante no autorizado ejecutar código a través de una red.

Versiones Afectadas

- Edición de suscripción de Microsoft SharePoint Server
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server 2016

Solución:

Se ha publicado un blog de inteligencia de amenazas para proporcionar actualizaciones, tácticas, técnicas y procedimientos de actores de amenazas, indicadores de compromiso y orientación para la búsqueda de amenazas en su propio entorno. *Ver +INFO.*

Fecha de Publicación: 19/JUL/2025 INFO

SNMP Remote Code Execution Vulnerabilities in Cisco IOS and IOS XE Software

CVE-2017-6736

High (8.8)

Impacto: Acceso no autorizado.

Resumen: El subsistema SNMP de Cisco IOS e IOS XE presenta vulnerabilidades que permiten a un atacante remoto autenticado ejecutar código (remote code execution) o forzar un reinicio (reload) del sistema. El fallo se debe a una condición de buffer overflow y afecta a SNMP v1, v2c y v3. Para explotarlo, se requiere conocer la community string (v1/v2c) o tener credenciales válidas (v3). El ataque se realiza mediante paquetes SNMP manipulados enviados por IPv4 o IPv6.

Versiones Afectadas

Cisco IOS o IOS XE y aplica a todas las versiones de SNMP, versiones 1, 2c y 3.

Solución:

se recomienda a los administradores que supervisen los sistemas afectados mediante el comando show snmp host en la CLI. *Ver +INFO.*

Fecha de Publicación: 30/JUL/2025 INFO

AWS Client VPN Windows Client Local Privilege Escalation

CVE-2025-8069

High (7.8)

Impacto: Escalada de privilegios.

Resumen: Se identificó una vulnerabilidad en AWS Client VPN para sistemas Windows, la cual permite que un usuario sin privilegios modifique el archivo de configuración de OpenSSL. Esta modificación puede conducir a la ejecución de código arbitrario en el momento en que un administrador instala el cliente, lo que potencialmente podría derivar en una ejecución con privilegios elevados.

Versiones Afectadas

Versiones 4.1.0, 5.0.0, 5.0.1, 5.0.2, 5.1.0, 5.2.0, 5.2.1.

Solución:

Este problema se ha solucionado en la versión del cliente VPN de AWS Client 5.2.2. Recomendamos a los usuarios que interrumpan cualquier instalación nueva de AWS Client VPN en Windows anterior a la versión 5.2.2. *Ver +INFO.*

Fecha de Publicación: 23/JUL/2025 INFO

Oracle Critical Patch Update Advisory

CVE-2025-30751, CVE-2025-50069, CVE-2025-27363, CVE-2025-50070

Una actualización de parches críticos es un conjunto de correcciones diseñadas para abordar múltiples vulnerabilidades de seguridad. Estos parches corrigen fallos tanto en el código de Oracle como en componentes de terceros integrados en sus productos.

Recomendación:
Hasta que aplique los parches de actualización de parches críticos, es posible reducir el riesgo de un ataque exitoso bloqueando los protocolos de red requeridos por un ataque.

Versiones Afectadas

- MySQL Enterprise Backup, versiones 8.0.0-8.0.42, 8.4.0-8.4.5, 9.0.0-9.3.0
- MySQL Server, versiones 8.0.0-8.0.42, 8.4.0-8.4.5, 9.0.0-9.3.0
- Oracle Agile Engineering Data Management, versión 6.2.1
- Oracle Application Express, versiones 24.2.4, 24.2.5 entre otras.*Ver +INFO*

Fecha de Publicación: 21/JUL/2025 INFO

Third-Party Package Updates in Splunk SOAR

CVE-2024-32002, CVE-2024-45230, CVE-2024-21538

Splunk ha lanzado actualizaciones de seguridad para corregir múltiples vulnerabilidades en paquetes de terceros para SOAR. Un actor malicioso remoto podría explotar estas vulnerabilidades para el acceso no autorizado, la ejecución de código o la manipulación de datos en la infraestructura principal.

Recomendación:
Actualice Splunk SOAR a la versión 6.4.1 o superior.

Versiones Afectadas

Splunk SOAR por debajo de 6.4.1

Fecha de Publicación: 7/JUL/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
15/07/2025	CVE-2025-41236	VMWARE	9.3	Un actor malintencionado con privilegios administrativos locales en una máquina virtual con VMXNET3 adaptador de red virtual puede aprovechar este problema para ejecutar código en el host. Los adaptadores virtuales que no son VMXNET3 no se ven afectados por este problema.
15/07/2025	CVE-2025-41237	VMWARE	9.3	Un actor malintencionado con privilegios administrativos locales en una máquina virtual puede aprovechar este problema para ejecutar código como el proceso VMX de la máquina virtual que se ejecuta en el host. En ESXi, la explotación está contenida en el entorno limitado de VMX, mientras que, en Workstation y Fusion, esto puede provocar la ejecución de código en el equipo donde está instalado Workstation o Fusion.
16/07/2025	CVE-2025-20274	CISCO	6.3	Una vulnerabilidad en la interfaz de administración basada en web de Cisco Unified Intelligence Center podría permitir que un atacante remoto autenticado cargue archivos arbitrarios en un dispositivo afectado.
16/07/2025	CVE-2025-20272	CISCO	4.3	Una vulnerabilidad en un subconjunto de API REST de Cisco Prime Infrastructure y Cisco Evolved Programmable Network Manager (EPNM) podría permitir que un atacante remoto autenticado y con pocos privilegios realice un ataque de inyección SQL ciego.
22/07/2025	CVE-2025-8028	FIREFOX	9.8	Existe una vulnerabilidad en la instrucción WASM `br_table`. Esto podría permitir a un actor malicioso generar una tabla con muchas entradas, provocando que la etiqueta se aleje demasiado de la instrucción, lo que podría causar truncamiento y un cálculo incorrecto de la dirección de la rama.
22/07/2025	CVE-2025-8040	FIREFOX	8.8	Existe una vulnerabilidad de seguridad de memoria. Esto podría permitir a un actor malicioso provocar una corrupción de memoria que potencialmente resulte en la ejecución de código arbitrario.
23/07/2025	CVE-2025-33076	IBM	8.8	IBM Engineering Systems Design Rhapsody era vulnerable a un desbordamiento de búfer basado en pila, causado por una comprobación incorrecta de los límites. Un usuario local podría desbordar el búfer y ejecutar código arbitrario en el sistema.

Scatter Spider lanza Ransomware en sistemas VMware secuestrados

Una campaña cibernética altamente "agresiva", identificada a mediados de 2025 por el Grupo de Inteligencia de Amenazas (GTIG) de Google, representa una grave amenaza para las principales industrias, incluidas las minoristas, las aerolíneas y los seguros. Esta sofisticada operación se atribuye a Scatter Spider, un grupo de piratería con motivación financiera también conocido como 0ktapus y UNC3944.

En su última campaña, según lo informado por GTIG, el grupo está considerando cuentas de Active Directory comprometidas para obtener el control total de los entornos VMware vSphere para robar datos confidenciales e implementar Ransomware directamente desde el hipervisor.

Este método es particularmente peligroso, ya que a menudo pasa por alto las herramientas de seguridad tradicionales como Endpoint Detection and Response (EDR), que carecen de visibilidad del hipervisor ESXi subyacente y vCenter Server Appliance (VCSA).

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral.

Ver +INFO.

El ATAQUE

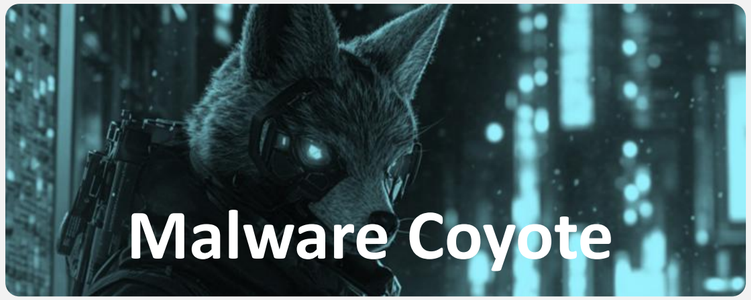
GTIG describe como UNC3944 pasa de un punto de apoyo inicial de bajo nivel al control completo del hipervisor en cinco fases metódicas. El punto de entrada crítico involucra la ingeniería social basada en el teléfono, donde los atacantes se hacen pasar por un empleado regular, haciendo llamadas telefónicas a la mesa de ayuda de TI. Mediante el uso de información personal disponible públicamente y tácticas persuasivas, engañan a los agentes de la mesa de ayuda para que restablezcan las contraseñas de Active Directory. Este acceso inicial les permite realizar un reconocimiento interno, buscando objetivos de alto valor como administradores de vSphere o grupos potentes de Active Directory. Luego hacen una segunda llamada más informada, haciéndose pasar por un administrador privilegiado para hacerse cargo de su cuenta. Este astuto proceso de dos pasos elude las protecciones técnicas estándar al explotar las vulnerabilidades en los procedimientos de verificación de identidad de la mesa de ayuda.

INFO

CONTEXT	INDICATOR	(MD5)
domain	oktalogin-targetcompany[.]com	N/A
domain	targetsname-cms[.]com	N/A
domain	targetsname-helpdesk[.]com	N/A
domain	targetsname-okta[.]com	N/A
domain	targetsname-servicedesk[.]com	N/A
domain	targetsname-sso[.]com	N/A
domain	chipotle-sso[.]com	N/A
domain	gemini-servicedesk[.]com	N/A
domain	hubspot-okta[.]com	N/A
domain	victimname-okta[.]com	N/A
domain	victimname-servicedesk[.]com	N/A
domain	victimname-sso[.]com	N/A

INFO

ÚLTIMAS NOTICIAS



Malware Coyote

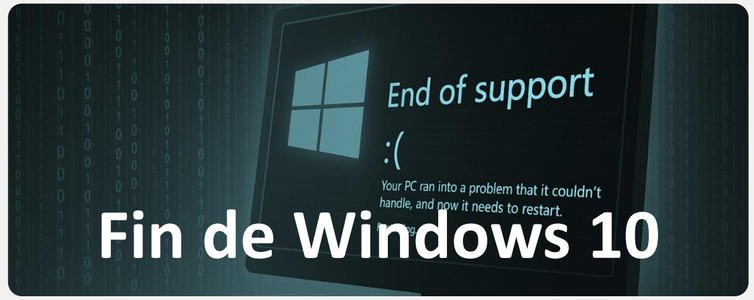
Una nueva variante del troyano bancario 'Coyote' ha comenzado a abusar de una función de accesibilidad de Windows, el marco de automatización de la interfaz de usuario de Microsoft, para identificar a qué sitios bancarios y de intercambio de criptomonedas se accede en el dispositivo para un posible robo de credenciales.

INFO

Malware Matanbuchus

Se ha visto que el cargador de malware Matanbuchus se distribuye a través de la ingeniería social a través de llamadas de Microsoft Teams que se hacen pasar por el servicio de asistencia de TI. Matanbuchus es una operación de malware como servicio que se promocionó por primera vez en la web oscura a principios de 2021.

INFO



Fin de Windows 10

A partir del 14 de octubre de 2025, Microsoft finalizará el soporte extendido para Windows 10 Home y Pro. Esta finalización suspende de forma permanente la publicación de actualizaciones de seguridad, lo que convierte a cualquier sistema que continúe operando con esta versión en un objetivo de alto riesgo.

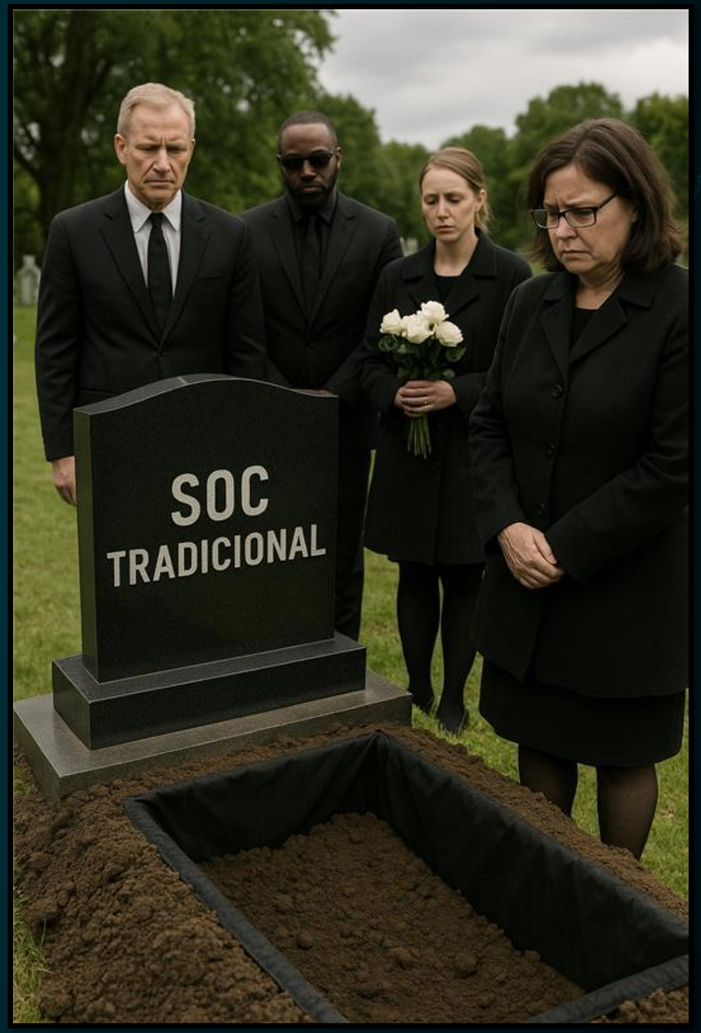
INFO

Aquí yace el SOC Tradicional

El que detectaba… pero no aportaba valor.
El que generaba alertas… pero no entendía el contexto.
El que escalaba… pero dejaba al cliente con más dudas que certezas.

Durante años, el modelo clásico funcionó. Pero el mundo cambió. Las amenazas ya no esperan: se mueven con velocidad, automatización e inteligencia artificial. Hoy, el negocio no necesita un observador pasivo. Necesita un aliado que analice, oriente y guíe con estrategia. Se trata de enterrar el conformismo. De dejar atrás la vigilancia sin inteligencia, la acumulación de herramientas sin sentido y la información que no lleva a la acción.

En el SOC de DataSec no nos limitamos a mirar pantallas. Acompañamos, recomendamos y orientamos a nuestros clientes para que tomen decisiones rápidas y acertadas. Porque un verdadero SOC no es solo tecnología: es conocimiento, contexto y compromiso.



DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 285 8969