BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

APT28 ruso implementa Backdoor «NotDoor» a través de Microsoft Outlook

TLP:CLEAR
16.09.2025

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: → APT28 ruso implementa Backdoor «NotDoor» a través de Microsoft Outlook

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 IOS XR ARP Broadcast Storm Denial of Service Vulnerability

CVE-2025-20340

High (7.4)

Impacto: Denegación de servicios (Dos)

Resumen: Una vulnerabilidad en la implementación del Protocolo de resolución de direcciones (ARP) del software Cisco IOS XR podría permitir que un atacante adyacente no autenticado genere una tormenta de broadcast, lo que lleva a una condición de denegación de servicio (DoS) en un dispositivo afectado.

Versiones Afectadas

Esta vulnerabilidad afecta a los dispositivos Cisco si ejecutan una versión vulnerable del software Cisco IOS XR y la interfaz de administración está configurada con una dirección IP en estado activo.

Solución:

Cisco ha publicado actualizaciones de software gratuitas que solucionan la vulnerabilidad descrita en este boletín.

Ver +INFO.

Fecha de Publicación: 10/SEP/2025 INFO

Vulnerability in IBM Concert Software

CVE-2025-25200

critical (9.2)

Impacto: Denegación de servicios (Dos).

Resumen: Koa es un middleware expresivo para Node.js que utiliza funciones asíncronas ES2017. En versiones anteriores a la 0.21.2, 1.7.1, 2.15.4 y 3.0.0-alpha.3, Koa utiliza una expresión regular maliciosa para analizar las cabeceras HTTP «X-Forwarded-Proto» y «X-Forwarded-Host». Esto puede aprovecharse para realizar un ataque de denegación de servicio.

Versiones Afectadas

En versiones anteriores a la 0.21.2, 1.7.1, 2.15.4 y 3.0.0-alpha.3

Solución:

Las versiones 0.21.2, 1.7.1, 2.15.4 y 3.0.0-alpha.3 solucionan el problema.

Ver +INFO.

Fecha de Publicación: 01/SEP/2025 INFO

IBM Transformation Advisor is affected by a vulnerability found in a container

CVE-2025-36193

High (8.4)

Impacto: Escalada de privilegios

Resumen: IBM Transformation Advisor asigna incorrectamente privilegios a archivos críticos de seguridad que podrían permitir una escalada de raíz local dentro de un contenedor que ejecuta la imagen del Catálogo de operadores de IBM Transformation Advisor.

Versiones Afectadas

IBM Transformation Advisor 2.0.1 a 4.3.1

Solución:

Instale v4.3.2 desde la página de OperatorHub en Red Hat OpenShift Container Platform

Ver +INFO.

Fecha de Publicación: 03/SEP/2025 INFO

IBM App Connect Enterprise Certified Container DesignerAuthoring operands are vulnerable to denial of service

CVE-2025-7338

High (7.5)

Impacto: Denegación de servicio (Dos).

Resumen: Multer es un middleware de Node.js para gestionar `multipart/form-data`. Una vulnerabilidad presente permite a un atacante activar una denegación de servicio (DoS) mediante el envío de una solicitud de carga malformada en formato multi-part. Esta solicitud provoca una excepción no controlada, lo que provoca un bloqueo del proceso.

Versiones Afectadas

A partir de la versión 1.4.4-lts.1 y anteriores a la 2.0.2

Solución:

Los usuarios deben actualizar a la versión 2.0.2 para recibir un parche.

Ver +INFO.

Fecha de Publicación: 01/SEP/2025 INFO

Actualización de seguridad para componentes de Dell VxRail

CVE-2025-41236, CVE-2025-41237, CVE-2025-41238

La corrección de Dell VxRail System for Azure Local está disponible para varias vulnerabilidades de seguridad que podrían ser explotadas por usuarios malintencionados para comprometer el sistema afectado.

Recomendación:
Actualizar a la última versión disponible a través del sitio web oficial del fabricante.

Versiones Afectadas

Dell VxRail Appliance, versiones 8.0.000 hasta 8.0.361

Ver +INFO

Fecha de Publicación: 04/SEP/2025 INFO

Actualización de seguridad para productos Acronis

CVE-2025-9578

Acronis ha lanzado una actualización de seguridad para remediar una vulnerabilidad de severidad alta en Cyber Protect Cloud Agent en Windows. La vulnerabilidad podría ser explotada para lograr la elevación de privilegios.

Recomendación:
Actualizar a la última versión disponible a través del sitio web oficial del fabricante.

Versiones Afectadas

Acronis Cyber Protect Cloud Agent (Windows), versiones anteriores a build 40734.

Ver +INFO

Fecha de Publicación: 04/SEP/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
3/09/2025	CVE-2025-20328	CISCO	5.4	Una vulnerabilidad en el componente de perfil de usuario de Cisco Webex Meetings podría haber permitido a un atacante remoto autenticado con privilegios bajos llevar a cabo un ataque de secuencias de comandos entre sitios
3/09/2025	CVE-2025-20270	CISCO	4.3	Una vulnerabilidad en la interfaz de administración basada en web de Cisco Evolved Programmable Network Manager (EPNM) y Cisco Prime Infrastructure podría permitir que un atacante remoto autenticado obtenga información confidencial de un sistema afectado.
4/09/2025	CVE-2025-54914	AZURE	10.0	Elevación de privilegios en Azure Networking
3/09/2025	CVE-2025-48384	GIT	8	En plataformas tipo Unix, si se usa git clone --recursive un repositorio no confiable, podría producirse una ejecución remota de código.
9/09/2025	CVE-2025-53609	FORTINET	4.7	Una vulnerabilidad de recorrido de ruta relativa en FortiWeb puede permitir que un atacante autenticado realice una lectura de archivo arbitraria en el sistema subyacente a través de solicitudes diseñadas.
9/09/2025	CVE-2024-45325	FORTINET	6.5	Una vulnerabilidad de neutralización incorrecta de elementos especiales utilizados en un comando del SO ('Inyección de comando del SO') en la CLI de FortiDDoS-F puede permitir que un atacante privilegiado ejecute código o comandos no autorizados a través de solicitudes CLI diseñadas.
3/09/2025	CVE-2025-20330	CISCO	6.1	Una vulnerabilidad en la interfaz de administración basada en web de Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) podría permitir que un atacante remoto no autenticado realice un ataque de secuencias de comandos entre sitios (XSS) contra un usuario de la interfaz.
3/09/2025	CVE-2025-20291	CISCO	4.3	Una vulnerabilidad en Cisco Webex Meetings podría haber permitido que un atacante remoto no autenticado redirigiera a un usuario de Webex Meetings objetivo a un sitio web no confiable. Cisco ha solucionado esta vulnerabilidad en el servicio Cisco Webex Meetings y no se requiere ninguna acción por parte del cliente.
3/09/2025	CVE-2025-20335	CISCO	5.3	Varias vulnerabilidades en los permisos de directorio de Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 y 8800 Series y Cisco Video Phone 8875 con software Cisco Session Initiation Protocol (SIP) podrían permitir que un atacante remoto no autenticado realice ataques arbitrarios de escritura de archivos y divulgación de información en un dispositivo afectado.

APT28 ruso implementa Backdoor «NotDoor» a través de Microsoft Outlook

APT28, el grupo de hackers ruso respaldado por el estado y vinculado desde hace tiempo a campañas de espionaje contra países de la OTAN, ha sido descubierto usando un nuevo truco dentro de Microsoft Outlook. Investigadores de Lab52, el equipo de inteligencia de amenazas de S2 Grupo, revelaron una backdoor personalizada llamada NotDoor que se ejecuta a través del cliente de correo electrónico de Outlook para robar datos y dar control remoto a los atacantes.

NotDoor funciona dentro de Outlook como una macro de Visual Basic para Aplicaciones (VBA). Funciona monitorizando los correos electrónicos entrantes en busca de una frase de activación especial, como "Informe diario", que activa sus funciones ocultas. Una vez activado, el malware puede enviar archivos robados, cargar nuevos en el equipo de la víctima y ejecutar comandos, todo ello mimetizándose con el flujo normal de correo electrónico.

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

Ver +INFO.

El ATAQUE

APT28 (también conocido como Fancy Bear, Sofacy, STRONTIUM —la designación de **Microsoft—, Sednit y Pawn Storm) lo despliega abusando del archivo firmado OneDrive.exe de Microsoft, el cual es vulnerable a una técnica de carga lateral de DLL (DLL sideloading).Los atacantes cargan una DLL maliciosa llamada SSPICLI.dll, que desactiva la seguridad de macros de Microsoft Outlook e instala la backdoor. A partir de ahí, el malware utiliza comandos de PowerShell codificados para copiarse en la carpeta de proyectos de macros de Outlook, verificar la infección mediante consultas DNS hacia webhook.site, y establecer persistencia mediante modificaciones en el Windows Registry. Una vez instalado, NotDoor está diseñado para ser difícil de detectar. El proyecto Visual Basic for Applications (VBA) está ofuscado, con nombres de variables desordenados y un método de codificación de cadenas que disfraza su código como si fueran datos aleatorios en Base64. Los archivos robados se cifran, se envían a través de Outlook y luego se eliminan de la máquina de la víctima. El malware incluso borra el correo electrónico de activación que lo desencadena, dejando muy pocos rastros para los equipos defensivos.

+ INFO

CONTEXT	INDICATOR	(MD5)
Dominio	dnshook[.]site	N\A
Dominio	webhook[.]site	N\A
Dominio	oast[.]fun	N\A
Hash de archivo	8f4bca3c62268fff0458322d111a511e0bcfba255d5ab78c45973bd293379901	f8d9b7c864fb7558e8bad4cfb5c8e6ff
Correo electrónico	a.matti444@proton.me	N\A
Nombre de host	run.mocky[.]io	N\A
Hash de archivo	5a88a15a1d764e635462f78a0cd958b17e6d22c716740febc114a408eef66705	15e9255a3e3401e5f6578d2ac45b7850

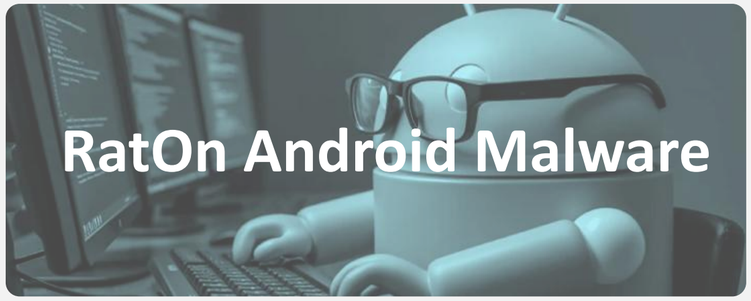
INFO

ÚLTIMAS NOTICIAS

Malware en archivos SVG

VirusTotal ha descubierto una campaña de phishing oculta en archivos SVG que crean portales convincentes que se hacen pasar por el sistema judicial de Colombia y distribuyen malware. VirusTotal detectó esta campaña después de agregar soporte para SVG a su plataforma AI Code Insight. La función AI Code Insight de VirusTotal analiza muestras de archivos cargados mediante aprendizaje automático para generar resúmenes de comportamiento sospechoso o malicioso encontrado en los archivos.

INFO



RatOn Android Malware

Un nuevo malware para Android llamado RatOn ha evolucionado desde una herramienta básica capaz de realizar ataques de retransmisión de comunicación de campo cercano (NFC) a un sofisticado troyano de acceso remoto con capacidades de sistema de transferencia automatizada (ATS) para realizar fraudes en dispositivos. RatOn combina los ataques tradicionales de superposición con transferencias automáticas de dinero y la funcionalidad de retransmisión NFC, lo que lo convierte en una amenaza excepcionalmente potente.

INFO

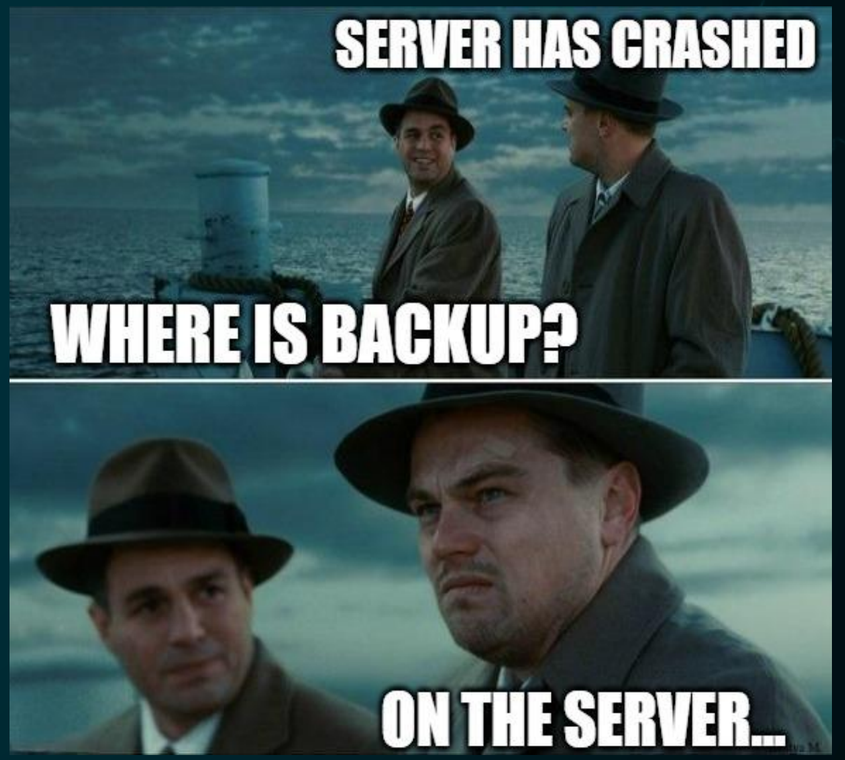
Phishing en Microsoft 365

Los actores de amenazas están abusando de herramientas de cliente HTTP como Axios junto con la función Direct Send de Microsoft para formar una "canalización de ataque altamente eficiente" en campañas de phishing recientes, según nuevos hallazgos de ReliaQuest. Se dice que la campaña observada por ReliaQuest comenzó en julio de 2025, inicialmente dirigida a ejecutivos y gerentes de los sectores de finanzas, atención médica y manufactura, antes de ampliar su enfoque para llegar a todos los usuarios.

INFO

🔐 Respaldos Seguros: Pilar de la Ciberresiliencia Organizacional

En el mundo digital actual, la protección de los datos es crucial para la continuidad operativa de cualquier organización. Confiar únicamente en el servidor principal para almacenar tanto los datos como las copias de seguridad es un riesgo significativo. En caso de un fallo del sistema o un ataque cibernético, todo se pierde de manera simultánea.



📌 Buenas Prácticas de Respaldo:

- Seguir la regla 3-2-1: Tener al menos 3 copias de los datos, almacenadas en 2 tipos de medios diferentes, y 1 ubicada fuera del entorno principal (off-site).
- Aislar las copias de seguridad: Usar almacenamiento externo, servicios en la nube confiables o soluciones inmutables.
- Probar periódicamente los respaldos: No basta con tenerlos; deben ser restaurables y actualizados.
- Automatizar el proceso de backup para reducir errores humanos y garantizar consistencia.

🔐 Invertir en una estrategia de respaldo sólida es fundamental para garantizar la continuidad del negocio ante cualquier eventualidad.

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 285 8969