BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Piratas informáticos usan videos de TikTok para distribuir el malware Vidar y StealC a través de la técnica ClickFix

TLP:CLEAR

03.06.2025

CLICK PARA EMPEZAR

En esta edición: → Piratas informáticos usan videos de TikTok para distribuir el malware Vidar y StealC a través de la técnica ClickFix

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 RADIUS Denial of Service Vulnerability

CVE-2025-20152

High (8.6)

Impacto: Denegación de servicio (DoS).

Resumen: Esta vulnerabilidad se debe a un manejo incorrecto de ciertas solicitudes RADIUS. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud de autenticación específica a un dispositivo de acceso a la red (NAD) que utiliza Cisco ISE para la autenticación, autorización y contabilidad (AAA). Un exploit exitoso podría permitir que el atacante haga que Cisco ISE se recargue.

Versiones Afectadas

Esta vulnerabilidad afecta a Cisco ISE si está configurado con servicios de autenticación RADIUS.(Los servicios RADIUS están habilitados de forma predeterminada).

Versión 3.4 afectada

Solución: Se recomienda a los clientes que actualicen a una versión de software fija adecuada.

Ver +INFO.

Fecha de Publicación: 21/MAY/2025 INFO

Cisco Unified Intelligence Center Privilege Escalation Vulnerabilities

CVE-2025-20113

High (7.1)

Impacto: Escalada de privilegios.

Resumen: Esta vulnerabilidad se debe a una validación insuficiente del lado del servidor de los parámetros proporcionados por el usuario en las solicitudes API o HTTP. Un atacante podría aprovechar esta vulnerabilidad enviando una API creada o una solicitud HTTP a un sistema afectado.

Versiones Afectadas

Estas vulnerabilidades afectan a Cisco Unified Intelligence Center, independientemente de la configuración del dispositivo, ambién afectan a Cisco Unified Contact Center Express (Unified CCX).

Solución: Cisco ha lanzado actualizaciones de software gratuitas que aborda la vulnerabilidad descrita en este boletín

Ver +INFO.

Fecha de Publicación: 21/MAY/2025 INFO

Vulnerabilities Let Attackers Escalate Privileges

CVE-2025-24916

High (7)

Impacto: Escalada de privilegios.

Resumen: Al instalar Tenable Network Monitor en una ubicación no predeterminada en un host de Windows, no aplicaban permisos seguros para los subdirectorios. Esto podría permitir la escalada de privilegios locales si los usuarios no han protegido los directorios en la ubicación de instalación no predeterminada.

Versiones Afectadas

Las versiones de Tenable Network Monitor anteriores a la 6.5.1

Solución: Tenable Network Monitor 6.5.1 actualiza OpenSSL a la versión 3.0.16, expat a la versión 2.7.0, curl a la versión 8.12.0, libpcap a la versión 1.10.5 y libxml2 a la versión 2.13.8

Ver +INFO.

Fecha de Publicación: 23/MAY/2025 INFO

Vulnerabilities Let Attackers Escalate Privileges

CVE-2025-24917

High (7.8)

Impacto: Escalada de privilegios.

Resumen: En las versiones de Tenable Network Monitor se descubrió que un usuario no administrativo podía preparar archivos en un directorio local para ejecutar código arbitrario con privilegios SYSTEM, lo que podría conducir a una escalada de privilegios locales.

Versiones Afectadas

Las versiones de Tenable Network Monitor anteriores a la 6.5.1

Solución: Tenable Network Monitor 6.5.1 actualiza OpenSSL a la versión 3.0.16, expat a la versión 2.7.0, curl a la versión 8.12.0, libpcap a la versión 1.10.5 y libxml2 a la versión 2.13.8

Ver +INFO.

Fecha de Publicación: 23/MAY/2025 INFO

Java SDK affect IBM WebSphere Application Server Liberty

CVE-2025-21587

High (7.4)

Impacto: Denegación de servicios.

Resumen: Una vulnerabilidad en el componente JSSE de Oracle Java SE y GraalVM (incluidas sus ediciones Enterprise), que afecta versiones como Java SE 8u441, 11.0.26, 17.0.14, 21.0.6 y 24, entre otras. La falla puede ser aprovechada remotamente sin autenticación mediante múltiples protocolos, permitiendo a un atacante comprometer completamente el sistema. Si se explota con éxito, podría permitir el acceso no autorizado a datos críticos, así como su modificación o eliminación.

Versiones Afectadas

- Servidor de aplicaciones IBM WebSphere 9.0
- Servidor de aplicaciones IBM WebSphere 8.5

Solución: Aplique el SDK de IBM Java suministrado con IBM WebSphere Application Server Fixpack 28 (8.5.5.28) o posterior.

Ver +INFO.

Fecha de Publicación: 9/MAY/2025

INFO

Java SDK affect IBM IBM WebSphere Application Server

CVE-2025-4447

High (7)

Impacto: Desbordamiento de búfer.

Resumen: En las versiones de Eclipse OpenJ9 hasta la 0.51, cuando se utiliza con la versión 8 de OpenJDK, se puede producir un desbordamiento de búfer basado en pila modificando un archivo en el disco que se lee cuando se inicia la JVM.

Versiones Afectadas

- Servidor de aplicaciones IBM WebSphere 9.0
- Servidor de aplicaciones IBM WebSphere 8.5

Solución: Aplique el SDK de IBM Java suministrado con IBM WebSphere Application Server Fixpack 28 (8.5.5.28) o posterior.

Ver +INFO.

Fecha de Publicación: 9/MAY/2025

INFO

Actualización de seguridad para Dell NetWorker

CVE-2024-10979, CVE-2024-45492, CVE-2024-45491

Se ha lanzado una actualización de seguridad para abordar múltiples vulnerabilidades en varios componentes de terceros de Dell NetWorker Management Console. Estas, si se explotan, podrían permitir a un actor malicioso comprometer el sistema afectado.

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

Versiones Afectadas

Consola de administración de NetWorker, versión 19.12
Consola de administración de NetWorker, versiones anteriores a 19.11.0.5

Fecha de Publicación: 27/MAY/2025

Actualización de seguridad de Microsoft Edge

CVE-2025-47181

Microsoft ha lanzado la última actualización de Edge para la corrección específica de una vulnerabilidad del proyecto Chromium. Esta podría permitir la elevación de privilegios en el sistema afectado.

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

Versiones Afectadas

Edge, versiones anteriores a 1.3.195.61

Fecha de Publicación: 22/MAY/2025

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
21/05/2025	CVE-2025-20242	CISCO	6.5	Esta vulnerabilidad se debe a la falta de controles de autenticación adecuados. Un atacante podría aprovechar esta vulnerabilidad enviando datos TCP creados a un puerto específico en un dispositivo afectado. Un exploit exitoso podría permitir al atacante leer o modificar datos en el dispositivo afectado.
21/05/2025	CVE-2025-20112	CISCO	5.1	Esta vulnerabilidad se debe a los permisos excesivos que se han asignado a los comandos del sistema. Un atacante podría explotar esta vulnerabilidad mediante la ejecución de comandos creados en el sistema operativo subyacente. Un exploit exitoso podría permitir al atacante escapar del shell restringido y obtener privilegios de root en el sistema operativo subyacente de un dispositivo afectado.
21/05/2025	CVE-2025-20246	CISCO	6.1	Estas vulnerabilidades se deben a un filtrado incorrecto de la entrada proporcionada por el usuario. Un atacante podría explotar estas vulnerabilidades persuadiendo a un usuario para que siga un enlace malicioso. Un exploit exitoso podría permitir al atacante llevar a cabo un ataque de scripting entre sitios contra el usuario objetivo.
21/05/2025	CVE-2025-20256	CISCO	6.5	Una vulnerabilidad en la interfaz de administración basada en web de Cisco Secure Network Analytics Manager y Cisco Secure Network Analytics Virtual Manager podría permitir que un atacante remoto autenticado con credenciales administrativas válidas ejecute comandos arbitrarios como root en el sistema operativo subyacente.
17/05/2025	CVE-2025-4919	Mozilla Firefox	8.8	Un atacante pudo realizar una lectura o escritura fuera de los límites en un objeto JavaScript confundiendo los tamaños de los índices de la matriz.
20/05/2025	CVE-2024-45641	IBM	6.5	IBM Security ReaQta podría permitir a un atacante realizar acciones no autorizadas debido a una validación incorrecta del certificado SSL.
20/05/2025	CVE-2023-33861	IBM	6.4	IBM Security ReaQta podría permitir a un atacante suplantar una entidad de confianza interfiriendo con la ruta de comunicación entre el host y el cliente.
22/05/2025	CVE-2025-33138	IBM	5.4	IBM Aspera Faspex 5.0.0 a 5.0.12 es vulnerable a la inyección de HTML. Un atacante remoto podría inyectar código HTML malicioso, que cuando se ve, se ejecutaría en el navegador web de la víctima dentro del contexto de seguridad del sitio de alojamiento.

Piratas informáticos usan videos de TikTok para distribuir el malware Vidar y StealC a través de la técnica ClickFix

El malware conocido como Latrodectus se ha convertido en el último en adoptar la técnica de ingeniería social ampliamente utilizada llamada ClickFix como vector de distribución.

"La técnica ClickFix es particularmente riesgosa porque permite que el malware se ejecute en la memoria en lugar de escribirse en el disco", dijo Expel en un informe compartido con The Hacker News. "Esto elimina muchas oportunidades para que los navegadores o las herramientas de seguridad detecten o bloqueen el malware". Por cierto, el malware es uno de los muchos programas maliciosos que han sufrido un revés operativo en el marco de la Operación Endgame, que derribó 300 servidores en todo el mundo y neutralizó 650 dominios relacionados con Bumblebee, Lactrodectus, QakBot, HijackLoader, DanaBot, TrickBot y WARMCOOKIE entre el 19 y el 22 de mayo de 2025.

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

El ATAQUE

La revelación se produce cuando Trend Micro reveló detalles de una nueva campaña de ingeniería social que, en lugar de depender de páginas falsas de CAPTCHA, emplea videos de TikTok probablemente generados con herramientas de inteligencia artificial (IA) para entregar los Stealers Vidar y StealC al instruir a los usuarios a ejecutar comandos maliciosos en sus sistemas para activar Windows, Microsoft Office, CapCut, y Spotify. Estos videos se han publicado desde varias cuentas de TikTok como @gitallowed, @zane.houghton, @allaivo2, @sysglow.wow, @alexfixpc y @digitaldreams771. Estas cuentas ya no están activas. Uno de los videos que afirma proporcionar instrucciones sobre cómo "mejorar su experiencia de Spotify al instante" ha acumulado casi 500,000 visitas, con más de 20,000 me gusta y más de 100 comentarios.

INFO

CONTEXT	INDICATOR	(MD5)
PEXE - PE32+ executable (GUI) x86-64	86ba63df301612c09821a8a410d1958f3e9447dd2e9d73bdbcbfe081d6f5b33b	00ba930075cfc22c6774928aa06ab79a
PEXE - PE32+ executable (GUI) x86-64	04ff626ceab63a9ebabda3df54dff36e36c44585df115f5b43e5802367689e49	0b2ebca8bff1e5cd9e43cfabc020a8c5
PEXE - PE32+ executable (GUI) x86-64	0b921636568ee3e1f8ce71ff9c931da5675089ba796b65a6b212440425d63c8c	0d40b55e1f552db81c2b8400e1f25558
IPv4	142.132.204.231	N/A
IPv4	5.75.188.83	N/A
IPv4	116.203.15.153	N/A
IPv4	195.201.46.226	N/A
URL	https://alexanderarthur.xyz/	N/A
URL	https://alexanderalbie.xyz/	N/A
URL	https://sares.xyz/	N/A
domain	sares.xyz	N/A
domain	stviw.xyz	N/A

INFO

Verifica el remitente: Asegúrate de que el correo provenga de una fuente confiable. Si no estás seguro, busca el contacto oficial en el sitio web de la empresa.

🎁 Regalos gratis en tu inbox: No caigas en la trampa de los correos fraudulentos ⚠️

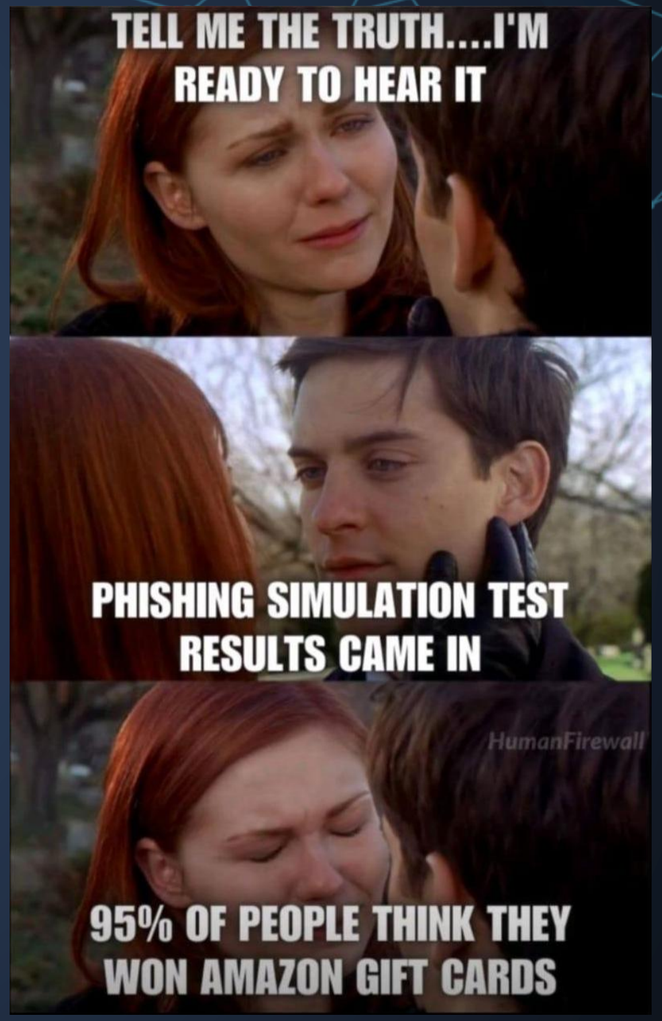
Hoy en día, los ciberdelincuentes usan tácticas cada vez más sofisticadas para engañarnos, y uno de sus métodos más comunes son los correos electrónicos que ofrecen “tarjetas de regalo” o “beneficios exclusivos”. Aunque la idea de obtener algo sin costo suena tentadora, la realidad es que la mayoría de estos correos son intentos de fraude.

🔐 Recomendaciones para protegerte:

🎯 No hagas clic en enlaces dudosos: Si un correo te ofrece algo "demasiado bueno para ser verdad", mejor ignóralo.

🛡️ Verifica el remitente: Asegúrate de que el correo provenga de una fuente confiable. Si no estás seguro, busca el contacto oficial en el sitio web de la empresa.

⚠️ No descargues archivos adjuntos desconocidos: Los archivos pueden contener malware.



DataSec

csirt_datasec@datasec.com.co

+57 310 285 8969