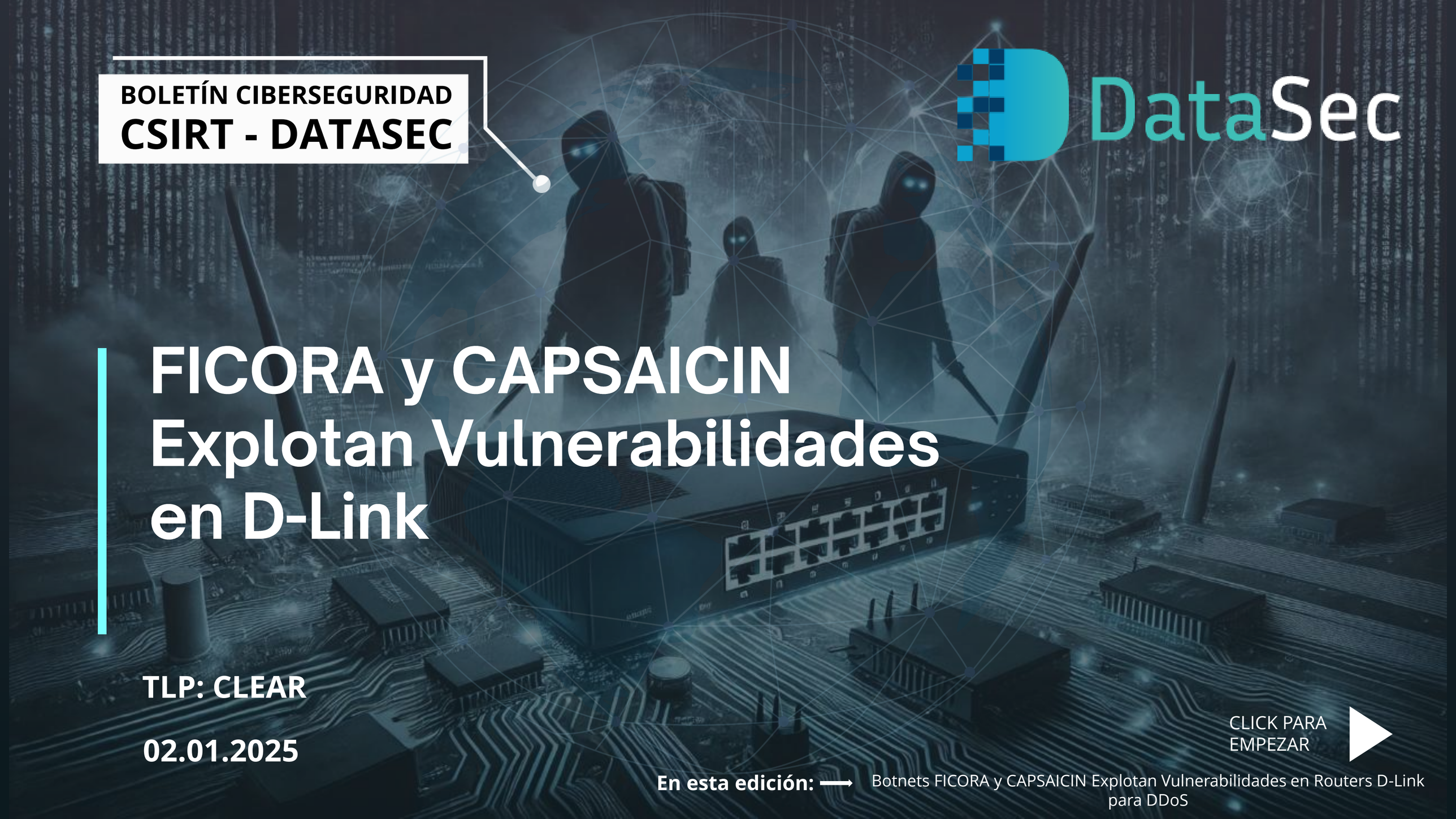


BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

FICORA y CAPSAICIN Explotan Vulnerabilidades en D-Link

TLP: CLEAR

02.01.2025

CLICK PARA EMPEZAR

En esta edición: Botnets FICORA y CAPSAICIN Explotan Vulnerabilidades en Routers D-Link para DDoS

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.

[FortiWLM] Unauthenticated limited file read vulnerability

CVE-2023-34990

Critical (9.6)

Impacto: Ejecución código o comandos no autorizados.

Resumen: Una vulnerabilidad de relative path traversal [CWE-23] en FortiWLM podría permitir a un atacante remoto no autenticado leer archivos sensibles.

Versiones Afectadas

- FortiWLM 8.6 8.6.0 through 8.6.5
- FortiWLM 8.5 8.5.0 through 8.5.4

Solución: Fortinet ha publicado actualizaciones de software que solucionan esta vulnerabilidad. Ver +INFO

Fecha de Publicación: 18/DIC/2024 INFO

OS command injection

CVE-2024-48889

High (7.2)

Impacto: Ejecución código o comandos no autorizados.

Resumen: Una vulnerabilidad de neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo (“OS Command Injection”) [CWE-78] en FortiManager podría permitir a un atacante remoto autenticado ejecutar código no autorizado a través de solicitudes FGFM manipuladas.

Versiones Afectadas

- FortiManager en múltiples versiones

Para más información, consulte + INFO.

Solución: Fortinet ha publicado actualizaciones de software que solucionan esta vulnerabilidad. Ver +INFO.

Fecha de Publicación: 18/DIC/2024 INFO

IBM Cognos Analytics expression language injection

CVE-2024-51466

Critical (9.0)

Impacto: Inyección de comandos.

Resumen: IBM Cognos Analytics es vulnerable a una inyección de Expression Language (EL). Un atacante remoto podría explotar esta vulnerabilidad para exponer información sensible, consumir recursos de memoria y/o provocar que el servidor se bloquee al utilizar una declaración EL especialmente diseñada.

Versiones Afectadas

IBM Cognos Analytics en las siguientes versiones:

- 12.0.0-12.0.4
- 11.2.0-11.2.4 FP4

Solución: Consultar la sección de *Remediation/Fixes* del fabricante para obtener más correcciones de las versiones de mantenimiento y más utilizadas. *Ver +INFO.*

Fecha de Publicación: 20/DIC/2024 +INFO

IBM Cognos Analytics file upload

CVE-2024-40695

High (8.8)

Impacto: Acceso no autorizado.

Resumen: IBM Cognos Analytics podría ser vulnerable a la carga de archivos maliciosos debido a la falta de validación del contenido de los archivos cargados en la interfaz web. Los atacantes podrían aprovechar esta vulnerabilidad para cargar archivos ejecutables maliciosos en el sistema y enviarlos a las víctimas para realizar ataques adicionales.

Versiones Afectadas

IBM Cognos Analytics en las siguientes versiones:

- 12.0.0-12.0.4
- 11.2.0-11.2.4 FP4

Solución: Consultar la sección de Remediation/Fixes del fabricante para obtener más correcciones de las versiones de mantenimiento y más utilizadas. Ver +INFO

Fecha de Publicación: 20/DIC/2024 +INFO

IBM Security Directory Integrator command execution

CVE-2024-45717

Medium (6.8)

Impacto: Ejecución remota de código.

Resumen: IBM Security Directory Integrator podría permitir que un atacante remoto autenticado ejecute comandos arbitrarios en el sistema mediante el envío de una solicitud especialmente diseñada.

Versiones Afectadas

- SDI - 7.2.0 - 7.2.0.13
- IBM Security Directory Integrator - 10.0.0 - 10.0.3

Solución: Actualizar los productos afectados a la última versión desde el sitio web oficial. *Ver +INFO.*

Fecha de Publicación: 20/DIC/2024 +INFO

IBM Security Guardium server-side request forgery

CVE-2024-49336

Medium (6.5)

Impacto: Acceso no autorizado a recursos internos.

Resumen: IBM Security Guardium es vulnerable a server-side request forgery (SSRF). Esto podría permitir a un atacante autenticado enviar solicitudes no autorizadas desde el sistema, lo que podría llevar a la enumeración de la red o facilitar otros ataques.

Versiones Afectadas

- IBM Security Guardium 11.5

Solución: Actualizar los productos afectados a la última versión desde el sitio web oficial. Ver +INFO.

Fecha de Publicación: 19/DIC/2024 +INFO

Stand-alone Security Patch Available for Tenable Security Center versions 6.3.0, 6.4.0 and 6.4.5: SC-202412.1

CVE-2024-53959

Security Center utiliza software de terceros, como OpenSSL y PHP, que contienen vulnerabilidades. Para mitigar los riesgos asociados, Tenable ha lanzado el parche Security Center Patch SC-202412.1, el cual actualiza OpenSSL a la versión 3.0.15 y PHP a la versión 8.2.26, en línea con las mejores prácticas de seguridad y con el fin de abordar las vulnerabilidades identificadas.

Recomendación:

Tenable ha lanzado el parche de Security Center SC-202412.1 para abordar estos problemas. Los archivos de instalación pueden obtenerse en el Portal de Descargas de Tenable. *Ver +INFO*

Versiones Afectadas

- El parche de Security Center SC-202412.1 actualiza OpenSSL a la versión 3.0.15 y PHP a la versión 8.2.26 para abordar las vulnerabilidades identificadas. *Ver +INFO.*

Fecha de Publicación: 20/DIC/2024 INFO

Security updates available for Adobe ColdFusion

CVE-2024-53961

Adobe ha lanzado actualizaciones de seguridad para las versiones 2023 y 2021 de ColdFusion. Estas actualizaciones resuelven una vulnerabilidad crítica que podría permitir la lectura arbitraria del sistema de archivos. Adobe está al tanto de que el CVE-2024-53961 tiene un proof-of-concept conocido que podría causar una lectura arbitraria del sistema de archivos.

Recomendación:

Para remediar la vulnerabilidad, se recomienda aplicar las actualizaciones y parches de seguridad disponibles en la página oficial del fabricante. Para más detalles, consulte directamente el sitio web. *Ver +INFO*

Versiones Afectadas

- ColdFusion 2023 Release Update 11 and earlier
- ColdFusion 2021 Release Update 17 and earlier

Fecha de Publicación: 20/DIC/2024 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	FABRICANTE	CVE / ACCESO	CVSSV3	DESCRIPCIÓN
18/12/2024	Apache Tomcat	CVE-2024-50378 CVE-2024-54677	9.8 5.3	Se han detectado vulnerabilidades de severidad crítica en Apache Tomcat, estas vulnerabilidades permitirían provocar condiciones de denegación de servicio y la ejecución remota de código en los sistemas afectados.
18/12/2024	Fortinet	CVE-2024-50570	4.9	Una vulnerabilidad de almacenamiento en texto claro de información sensible [CWE-312] en FortiClient para Windows podría permitir a un usuario local autenticado recuperar la contraseña de VPN a través de un volcado de memoria, debido al recolector de basura de JavaScript.
19/12/2024	IBM	CVE-2024-52896	6.2	La consola web de IBM MQ Appliance 9.3 LTS, 9.3 CD, 9.4 LTS y 9.4 CD podría permitir que un atacante remoto obtenga información confidencial cuando se devuelve un mensaje de error técnico detallado.
21/12/2024	IBM	CVE-2024-51464	4.3	Es vulnerable a la omisión de las restricciones de la interfaz de Navigator for i. Al enviar una solicitud especialmente manipulada, un atacante autenticado podría aprovechar esta vulnerabilidad para realizar de forma remota operaciones que el usuario no tiene permitido realizar cuando utiliza Navigator for i.
21/12/2024	IBM	CVE-2024-51463	5.4	Es vulnerable a server-side request forgery (SSRF). Esto puede permitir que un atacante autenticado envíe solicitudes no autorizadas desde el sistema, lo que podría provocar la enumeración de la red o facilitar otros ataques.
21/12/2024	WordPress	CVE-2024-12591	6.4	El complemento MagicPost para WordPress es vulnerable a Cross-Site Scripting almacenado a través del código corto wb_share_social del complemento en todas las versiones hasta la 1.2.1 incluida, debido a una desinfección de entrada insuficiente y al escape de salida en los atributos proporcionados por el usuario
19/12/2024	IBM	CVE-2024-52897	6.2	La consola web de IBM MQ Appliance 9.3 LTS, 9.3 CD y 9.4 LTS podría permitir que un atacante remoto obtenga información confidencial cuando se devuelve un mensaje de error técnico detallado.
23/12/2024	Cisco	CVE-2024-20397	5.2	Una vulnerabilidad en el cargador de arranque del software Cisco NX-OS podría permitir a un atacante no autenticado con acceso físico a un dispositivo afectado, o a un atacante local autenticado con credenciales administrativas, eludir la verificación de la firma de la imagen de NX-OS.
26/12/2024	Apache	CVE-2024-45387	9.9	Esta vulnerabilidad podría permitir que un usuario con privilegios «admin», «federation», «operations», «portal» o «steering» ejecute SQL arbitrario contra la base de datos enviando una solicitud PUT especialmente diseñada.

BOTNETS FICORA Y CAPSAICIN EXPLOTAN ANTIGUAS VULNERABILIDADES EN ROUTERS D-LINK PARA ATAQUES DDOS

Los investigadores en ciberseguridad han alertado sobre un aumento en la actividad maliciosa que involucra routers D-Link vulnerables, que están siendo incorporados a dos botnets: FICORA (una variante de Mirai) y CAPSAICIN (una variante de Kaiten).

Estos botnets explotan vulnerabilidades en el protocolo HNAP, que permite a los atacantes ejecutar comandos maliciosos remotamente.

FICORA ha afectado a varios países globalmente, mientras que CAPSAICIN se ha centrado en Asia, especialmente Japón y Taiwán, con una actividad destacada en octubre de 2024.

Los ataques se propagan aprovechando vulnerabilidades documentadas de D-Link.

El malware de FICORA incluye un script descargador que obtiene un payload para diferentes arquitecturas de Linux, además de capacidades para realizar ataques de fuerza bruta y DDoS utilizando protocolos UDP, TCP y DNS.

El ATAQUE

El ataque comienza con la descarga de un script de shell llamado "multi" que utiliza varios métodos, incluidos wget, ftpget, curl y tftp para descargar el malware real.

Este script de descarga primero elimina todos los procesos con la misma extensión de archivo que el malware “FICORA”. Luego descarga y ejecuta sus diversos programas maliciosos apuntando a diferentes arquitecturas de Linux, incluyendo “arc”, “arm”, “arm5”, “arm6”, “arm7”, “i486”, “i586”, “i686”, “m68k”, “mips”, “mipsel”, “powerpc”, “powerpc-440fp” y “sparc”.

INFO

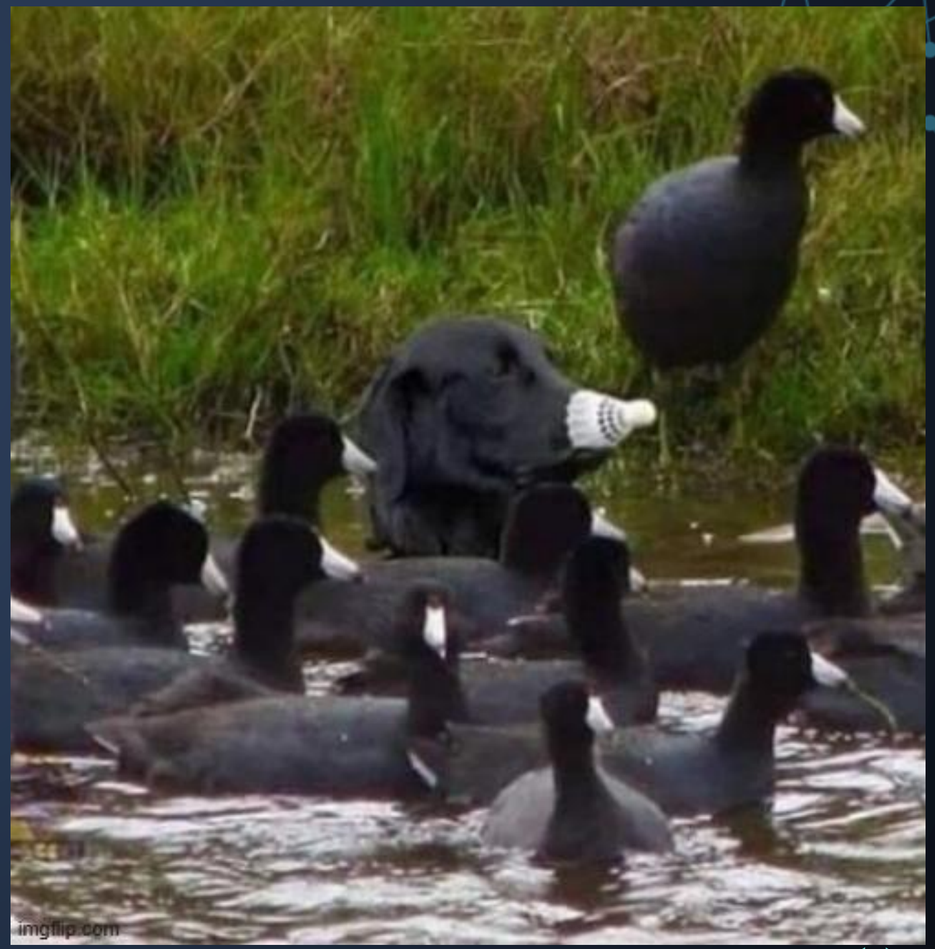
CONTEXT	INDICATOR	(MD5)
ELF - ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV)	4600703535e35b464f0198a1fa95e3668a0c956ab68ce7b719c28031d69b86ff	1b77238da15d598fe3877548b9b2197c
ELF - ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV)	7ab36a93f009058e60c8a45b900c1c7ae38c96005a43a39e45be9dc7af9d6da8	21f772d53fac58dd9020874ef8f1bfbb
SH - Bourne-Again shell script, ASCII text executable	48a04c7c33a787ef72f1a61aec9fad87d6bd9c49542f52af7e029ac83475f45d	42d36ae2eaf7090322d2638f5fb36a82
ELF - ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV)	d6a2a22000d68d79caeae482d8cf092c2d84d55dccee05e179a961c72f77b1ba	4b2bfa94425ea635064b9ed7c5ae58fe
ELF - ELF 32-bit MSB executable, SPARC, version 1 (SYSV)	540c00e6c0b53332128b605b0d5e0926db0560a541bb13448d094764844763df	4f972bcb14039a4fad62686929df5f9b
IPv4	103.149.87.69	N/A
IPv5	192.110.247.46	N/A
IPv6	194.110.247.46	N/A
URL	http:[/]/pirati[.].abuser[.]eu/yakuza[.]yak[.]sh	N/A
Domain	www[.]codingdrunk[.]in	N/A

INFO

INICIA EL 2025 DE FORMA CIBERSEGURA

Comienza 2025 reforzando tus prácticas de ciberseguridad para protegerte de las amenazas digitales, especialmente después de las festividades y promociones de fin de año que los ciberdelincuentes suelen aprovechar con tácticas como el envío de archivos maliciosos disfrazados de documentos legítimos en formatos como ZIP. Verifica siempre la autenticidad de los remitentes antes de abrir correos, evita descargar archivos no solicitados, utiliza herramientas antivirus confiables, mantén tus dispositivos actualizados y desconfía de enlaces abreviados o promociones demasiado buenas para ser verdad. Además, fomenta la capacitación en ciberseguridad entre familiares y colegas para construir un entorno digital más seguro y hacer de este año uno ciberseguro.

THAT MALICIOUS FILE IN ZIP FILE



DataSec

csirt_datasec@datasec.com.co

+57 310 285 8969