PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 02 de febrero de 2024

029-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°029	Fecha: 02-02-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Claro sufre ataque de ransomware que afecta su servicio celular en Centroamérica		
Tipo de Ataque	Ransonware	Abreviatura	Ransonware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES**:

   La operadora de telefonía Claro confirmó este viernes que las fallas en sus servicios a nivel de Centroamérica se deben a un "incidente de ransomware", un ataque cibernético para secuestrar los datos.

   Este ataque está afectando su servicio de telefonía móvil en países como Nicaragua, Costa Rica, Guatemala, Honduras y El Salvador.

   Un ransomware es un tipo de malware o software malicioso que impide acceder a su sistema o a determinados archivos y que normalmente exige el pago de un rescate para poder acceder de nuevo a ellos. Amenazan con quedarse con tu información y pueden tomar la decisión de guardarla para publicarla, o se la venden a otra organización que pueda interesarle esa base de datos.

2. **DETALLES:**

   En un comunicado, Claro señaló que el 25 de enero de 2024 identificaron la "existencia de una actividad anómala" en los sistemas por la infestación de un ransomware. Este tipo de malware impide el uso de los dispositivos hasta que la víctima pague por el rescate de la información a los ciberataques.

   "Como parte de nuestros protocolos, dichos equipos fueron aislados y decidimos apagar otros sistemas como medida precautoria. Hemos logrado dar continuidad a nuestra operación utilizando mecanismos alternos y estamos en proceso de restauración de los equipos afectados para regresarlos a su operación normal", añadió Claro.

   Entre las afectaciones reportadas en esa oportunidad por la empresa estaban problemas para los servicios de recarga de saldos e intermitencia en los de voz y datos.

   Igualmente, muchas personas usaron las redes sociales para indicar que no podían pagar sus facturas, que cortaron el servicio precisamente por estas situaciones y muchos solicitaron ajustes con sus facturas.

   El experto en seguridad digital recalca que el ransomware utilizado afectó el sistema de recargas de Claro, que solo en Nicaragua deja ganancias de unos 6 millones de córdobas, por lo que, sumando al resto de países centroamericanos, las pérdidas son "de proporciones gigantescas".

3. **RECOMENDACIONES:**

   - Mantener actualizados los programas, tanto en los dispositivos como en los servidores.
   - Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet.
   - Configurar copias de seguridad fuera de línea que los intrusos no puedan manipular y asegurarse de poder acceder a ellas rápidamente cuando sea necesario o en caso de emergencia.
   - Instalar soluciones anti-APT y EDR que permitan descubrir, detectar e investigar amenazas avanzadas y neutralizar rápidamente los incidentes.
   - Proporcionar a su equipo SOC acceso a la inteligencia de amenazas (TI) más reciente, pero con una biblioteca que además cubra amenazas antiguas.

Fuente de Información:	• hxxps://www.lamesaredonda.net/que-es-un-ransomware-el-virus-que-ataco-a-claro-en-toda-centroamerica/ • hxxps://gestion.pe/economia/empresas/claro-sufre-un-incidente-de-ransomware-que-afecta-su-servicio-celular-en-centroamerica-noticia/ • hxxps://www.revistaeyn.com/empresasymanagement/operacion-de-claro-en-centroamerica-fue-afectada-por-un-caso-de-ransomware-AB17340257

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°029**	**Fecha: 02-02-2024** **Página: 5 de 12**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en Gessler Web Master		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Felix Eberstaller y Nino Fürthauer, de Limes Security ha reportado dos vulnerabilidades de severidad **CRÍTICA y MEDIA** de tipo uso de credenciales débiles y uso de hash débil en Gessler Web Master. La explotación exitosa de estas vulnerabilidades podría permitir a un usuario tomar el control de la gestión web del dispositivo, así como extraer y romper los *hashes* de las contraseñas de todos los usuarios almacenados en el dispositivo (en caso de tener acceso al mismo).

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-1039 de tipo uso de credenciales débiles, podría permitir a un atacante controlar la gestión web del dispositivo. Esta vulnerabilidad, utiliza credenciales débiles (como una clave predeterminada o una contraseña codificada) que un atacante puede calcular, derivar, reutilizar o adivinar.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-1040 de tipo uso de hash débil, señala que un atacante puede restaurar las contraseñas rompiendo los hashes almacenados en el dispositivo.

Esta vulnerabilidad, utiliza un algoritmo que produce un resumen (valor de salida) que no cumple con las expectativas de seguridad para una función hash que permite a un adversario determinar razonablemente la entrada original (ataque de preimagen), encontrar otra entrada que pueda producir el mismo hash (segunda preimagen), o encontrar múltiples entradas que se evalúen con el mismo hash (ataque de cumpleaños).

A. Productos afectados:

- WEB-MASTER, versión 7.9.

3. RECOMENDACIÓN:

- Actualizar EZ2 a la versión 3.2 o superiores y Webmaster a la versión 4.4 o superiores para abordar estas vulnerabilidades.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-032-01

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°029**	**Fecha: 02-02-2024**
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en la herramienta de software HDD Health de PanteraSoft		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

Jorge Manuel Lozano Gómez ha reportado una vulnerabilidad de severidad **ALTA** de tipo ruta o elemento de búsqueda sin comillas en la herramienta de software HDD Health de PanteraSoft. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto escalar privilegios en el sistema.

2. **DETALLES:**

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-1201 de tipo ruta o elemento de búsqueda sin comillas, podría permitir a un atacante local almacenar un archivo ejecutable malicioso dentro de la ruta de búsqueda no entrecomillada, dando lugar a una escalada de privilegios.

Esta vulnerabilidad, utiliza una ruta de búsqueda que contiene un elemento sin comillas, en el que el elemento contiene espacios en blanco u otros separadores. Esto puede hacer que el producto acceda a recursos en una ruta principal.

A. Productos afectados:

- PanteraSoft HDD Health, versiones 4.2.0.112 y anteriores.

3. **RECOMENDACIÓN:**

- Actualizar el paquete afectado con la última versión de software disponible que el proveedor lance para abordar esta vulnerabilidad. A la fecha no se conoce ninguna solución oficial.

Fuente de Información:	• hxxps://download.cnet.com/hdd-health/3000-2086_4-10804806.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°029**	**Fecha: 02-02-2024** **Página: 7 de 12**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en IBM Operational Decision Manager		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA y MEDIA** de tipo neutralización inadecuada de elementos especiales utilizados en una consulta LDAP (Protocolo ligero de acceso a directorios), deserialización de datos que no son de confianza, error de validación de entrada y recorrido de camino en IBM Operational Decision Manager. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto eludir el proceso de autenticación, ejecutar código arbitrario en el sistema de destino, realizar un ataque de denegación de servicio y realizar ataques de cruce de directorio.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-22319 de tipo neutralización inadecuada de elementos especiales utilizados en una consulta LDAP, existe debido a una validación de entrada incorrecta al procesar consultas LDAP. Un atacante remoto no autenticado puede enviar una consulta LDAP especialmente diseñada a la aplicación, eludir el proceso de autenticación y obtener acceso no autorizado a la aplicación.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-22320 de tipo deserialización de datos que no son de confianza, existe debido a una validación de entrada insegura al procesar datos serializados. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar código arbitrario en el contexto de SYSTEM.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-34054 de tipo error de validación de entrada, existe debido a una validación insuficiente de la entrada proporcionada por el usuario. Un atacante remoto puede enviar solicitudes HTTP especialmente diseñadas a la aplicación y realizar un ataque de denegación de servicio (DoS).

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-34062 de tipo recorrido de camino, existe debido a un error de validación de entrada al procesar secuencias de recorrido de directorio. Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada y leer archivos arbitrarios en el sistema. La explotación exitosa de la vulnerabilidad requiere que el servidor HTTP Reactor Netty esté configurado para servir recursos estáticos.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-34055 de tipo error de validación de entrada, existe debido a una validación insuficiente de la entrada proporcionada por el usuario en Web Observations. Un atacante remoto puede enviar solicitudes HTTP especialmente diseñadas a la aplicación y realizar un ataque de denegación de servicio (DoS). La explotación exitosa de la vulnerabilidad requiere que la aplicación utilice Spring MVC o Spring WebFlux y que org.springframework.boot:spring-boot-actuator esté en el classpath.

A. Productos afectados:

- IBM Operational Decision Manager: antes de 8.12.0.1 Solución provisional 1.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión disponible para abordar estas vulnerabilidades.

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7112382

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°029**	**Fecha: 02-02-2024**
		Página: 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en la aplicación de servidor Moby		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

   Se ha reportado dos vulnerabilidades de severidad **ALTA y MEDIA** de tipo omisión de funciones de seguridad y verificación insuficiente de la autenticidad de los datos en la aplicación de servidor Moby. La explotación exitosa de estas vulnerabilidades permite que un atacante remoto comprometa el sistema afectado.

2. **DETALLES:**

   La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-21626 de tipo omisión de funciones de seguridad, existe debido a una fuga de descriptor de archivo interno que puede causar que un proceso contenedor recién generado (de runc exec) tenga un directorio de trabajo en el espacio de nombres del sistema de archivos del host o una imagen maliciosa para permitir que un proceso contenedor obtenga acceso al sistema de archivos del host. a través de runc run. Un atacante remoto puede engañar a la víctima para que cargue una imagen maliciosa para evitar las restricciones del sandbox y ejecutar código arbitrario en el sistema operativo host.

   La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-24557 de tipo verificación insuficiente de la autenticidad de los datos, existe debido a una verificación insuficiente de la autenticidad de los datos. Un atacante remoto puede envenenar el caché de la víctima haciéndole extraer una imagen especialmente diseñada que se consideraría como un candidato de caché válido para algunos pasos de compilación.

   A. Productos afectados:

   - Moby: 0.0.3 - 25.0.1.

3. **RECOMENDACIÓN:**

   - Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://github.com/moby/moby/releases/tag/v24.0.9

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°029	Fecha: 02-02-2024
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de identidad de la empresa de entretenimiento y plataforma de Streaming Netflix		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se vienen llevando a cabo una campaña de Phishing, quienes vienen suplantando la identidad de la empresa de entretenimiento y plataforma de Streaming Netflix, el supuesto sitio web cuenta con logos característicos al oficial, el cual tiene como finalidad robar sus credenciales de acceso y datos bancarios.

2. DETALLES:

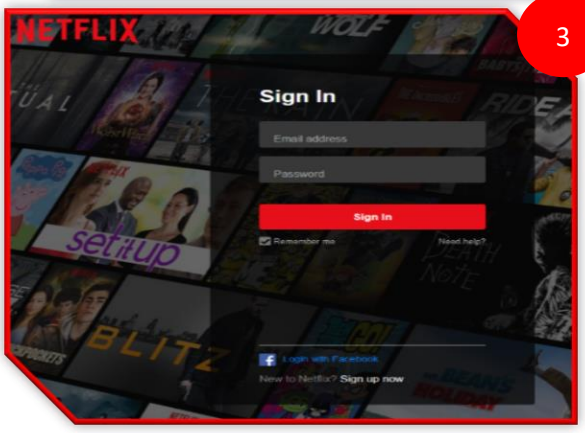
El proceso de estafa de Phishing es el siguiente:

1

Imagen 1
Sitio web fraudulento de Netflix, informa a la víctima que para crear o reiniciar su membresía tiene que registrarse en la plataforma a través de credenciales de acceso (correo electrónico y contraseña).

2

Imagen 2
Luego de darle clic en <empezar>, el atacante le solicita a la víctima registrar la contraseña para poder ingresar.

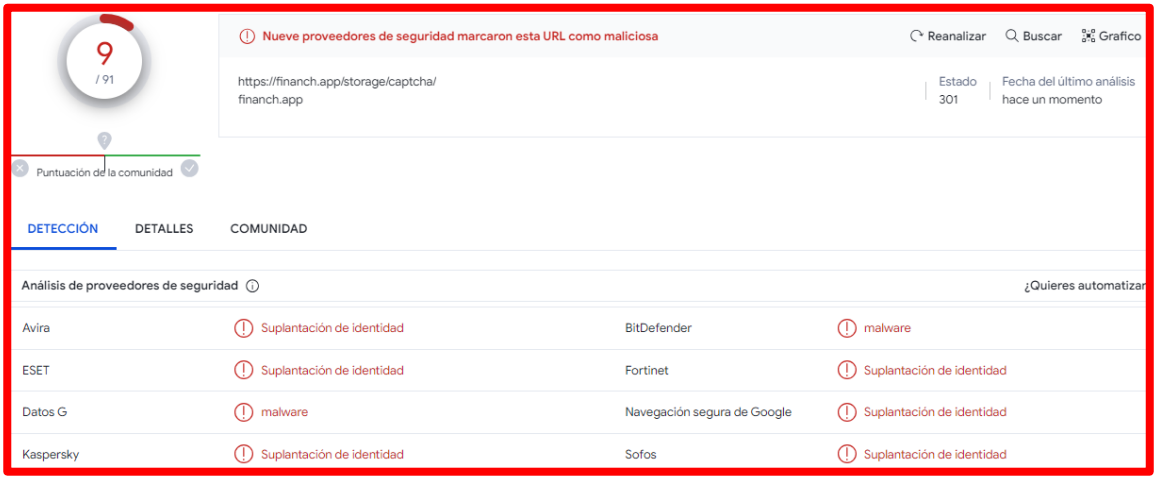


3

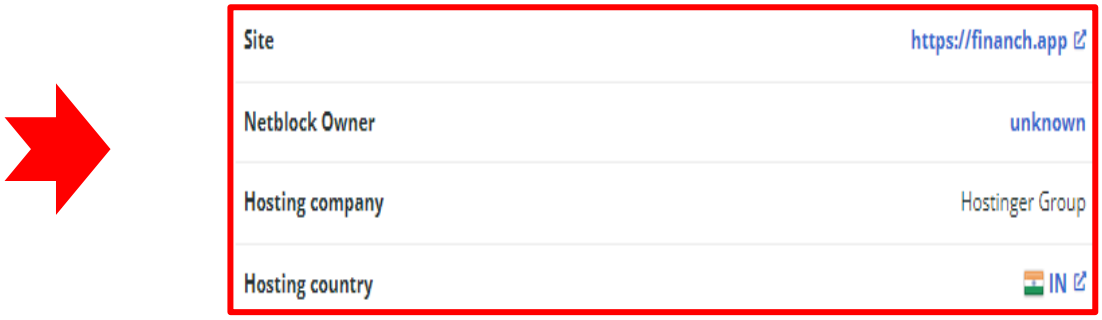
Imagen 3
Luego de completar los datos requeridos, le redirige a la víctima automáticamente a un supuesto sitio web de NETFLIX; sin embargo, los ciberdelincuentes obtuvieron los datos brindados por la víctima.

A. INDICADORES DE COMPROMISO:

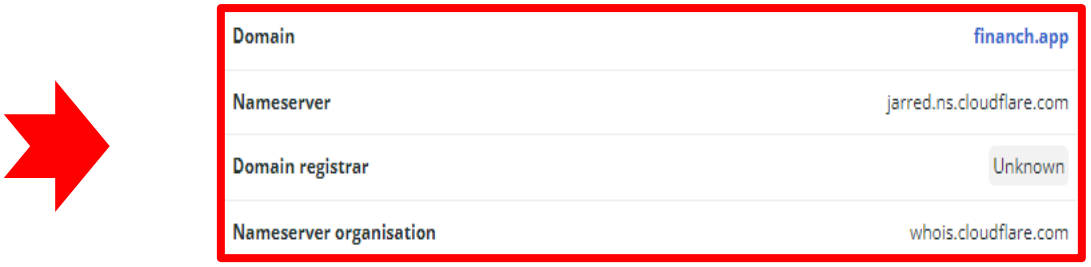
La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD**:



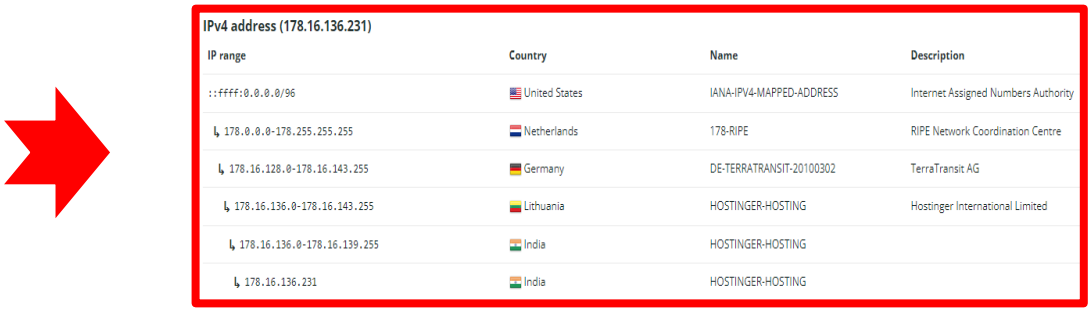
- **URL:** hxxps://financh[.]app/storage/captcha/



- **Dominio:** financh[.]app



- **IP:** 178[.]16[.]136[.]231



- **SHA-256:** 86196751fbfc8b0bfc58f572f2add5c4022c62f5c1dd04e991474b413882e4cc
- **Tipo de Contexto:** Text/html

B. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.).

C. Referencia:

- Phishing o suplantación de identidad, es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Verificar detalladamente la URL, que corresponda al sitio web oficial de Netflix.
- Evitar seguir las instrucciones de sitio web sospechoso o de dudosa procedencia.
- Mantener el antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.
- Ingresar desde fuentes oficiales (hxxps://www.netflix.com/browse).

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.

Índice alfabético