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, 29 de enero de 2024

025-2024-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°025	Fecha: 29-01-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Otra variante de Phobos Ransomware lanza ataque – FAUST		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
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 familia de ransomware Phobos es un grupo notorio de software malicioso diseñado para cifrar archivos en la computadora de una víctima. Surgió en 2019 y desde entonces ha estado involucrado en numerosos ciberataques.

   Los atacantes utilizaron el servicio Gitea para almacenar varios archivos codificados en Base64, cada uno de los cuales llevaba un binario malicioso. Cuando estos archivos se inyectan en la memoria de un sistema, inician un ataque de cifrado de archivos.

2. **DETALLES:**

   La versión FAUST, una variante de Phobos, puede mantener la persistencia en un entorno determinado y genera múltiples subprocesos para una ejecución eficiente.

   El documento de Microsoft Excel (.XLAM) que descubrimos contiene un script VBA integrado. Al abrir el documento, el script activa PowerShell para la siguiente etapa usando la función “Workbook_Open()”. Luego descarga datos codificados en Base64 de Gitea, que se pueden decodificar en un archivo XLSX limpio. Luego, este archivo se guarda en la carpeta TEMP y se abre automáticamente, lo que induce a error a los usuarios al pensar que el proceso se ha completado y no supone ningún daño, ya que también se recupera sigilosamente un ejecutable que se hace pasar por un actualizador del software AVG AntiVirus ("AVG Updater. exe").

   El archivo ejecutable “AVG update.exe” funciona como descargador. Incorpora una gran cantidad de código extraño para evadir la detección y complicar el análisis. Al emplear una técnica de inyección de procesos, asigna memoria de lectura, escritura y ejecución (RWE) para inyectar el código malicioso en un proceso recién generado. Este binario busca e inicia otro ejecutable llamado "SmartScreen Defender Windows.exe" para iniciar su proceso de cifrado empleando un ataque sin archivos para implementar el código shell malicioso.

   La variante Faust exhibe la capacidad de mantener la persistencia en un entorno y crea múltiples subprocesos para una ejecución eficiente.

   El ransomware FAUST crea archivos info.txt e info.hta dentro de los directorios que contienen los archivos cifrados y agrega la extensión ".faust" a cada archivo cifrado. Estos archivos se utilizan como una forma de ponerse en contacto con los atacantes para iniciar negociaciones de rescate.

   “También inicia múltiples subprocesos para realizar diversas tareas. Estas tareas incluyen implementar cifrado, escanear unidades lógicas, buscar recursos de red/compartir, escanear archivos individualmente y buscar explícitamente archivos relacionados con bases de datos”, compartió Fortinet con Cyber Security News.

3. **RECOMENDACIONES:**

   - Abstenerse de abrir archivos de documentos de fuentes no confiables.
   - Normalizar la gestión de copias de seguridad.
   - Mantener siempre actualizado los programas, tanto en los dispositivos como en los servidores.
   - Procurar la gestión de un plan que incluya detección, investigación y respuesta a amenazas 24/7.
   - En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados.

Fuente de Información:	• hxxps://www.fortinet.com/blog/threat-research/phobos-ransomware-variant-launches-attack-faust • hxxps://gbhackers.com/phobos-ransomware-office-document/ • hxxps://thehackernews.com/2024/01/albabat-kasseika-kuiper-new-ransomware.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 29-01-2024
		Página: 5 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades críticas en productos TRUMPF		
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 **CRÍTICA** de tipo escritura fuera de límites e información insuficiente en productos TRUMPF. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante obtener acceso completo al servidor o estación de trabajo afectados.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2023-38545 de tipo escritura fuera de límites, en el que la variable local empleada para permitir al *host* resolver el nombre podría obtener el valor incorrecto durante un *handshake* SOCKS5 lento y copiar el nombre de *host* demasiado largo al búfer de destino.

La vulnerabilidad de severidad crítica, identificada por MITRE como CVE-2023-24540 de tipo información insuficiente, señala que no todos los caracteres de espacio en blanco válidos de JavaScript se consideran espacios en blanco. Es posible que las plantillas que contengan caracteres de espacio en blanco fuera del conjunto de caracteres "\t\n\f\r\u0020\u2028\u2029", en contextos JavaScript que también contengan acciones, no se desinfecten correctamente durante la ejecución.

A. Productos afectados:

- MonitoringAnalyzer, versiones 1.0 <= 1.3.
- Oseon, versiones 1.0.0 <= 3.0.24.
- ProgrammingTube, versiones 1.0.1 <= 4.11.0.
- TecZoneBend, versiones 18.02.R8 <= 23.11.
- Tops Unfold, versión 05.03.00.00.
- TrumpfLicenseExpert, versiones 1.5.2 <= 2.0.0.
- TruTops, versiones 08.00 <= 12.01.00.00.
- TruTopsBoost, versiones 06.00.23.00 <= 16.0.24.
- TruTopsCalculate, versiones 14.00 <= 23.00.00.
- TruTops Cell Classic, versiones <= 09.09.02.
- TruTops Cell SW48, versiones 01.00 <= 02.32.12.
- TruTopsFab (inkl.TruTops Monitor), versiones 15.00.23.00 <= 22.8.25.
- TruTopsFab Storage SmallStore, versiones 14.06.20 <= 20.04.20.00.
- TruTops Mark 3D, versiones 01.00 <= 06.2.
- TruTopsPrint, versiones 00.06.00 <= 01.00.
- TruTopsPrintMultilaserAssistant, versiones <= 01.02.
- TruTopsWeld, versiones 7.0.198.241 <= 9.0.28148.1.
- TubeDesign, versiones 08.00 <= 14.11.199.

3. RECOMENDACIONES:

- Actualizar el producto afectado a las versiones 2.1.0 o posteriores que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://cert.vde.com/de/advisories/VDE-2024-001/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 29-01-2024
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades críticas en productos de SE-elektrinic GmbH		
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 **CRÍTICA** de tipo consumo incontrolado de recursos y control inadecuado de la generación de código (inyección de código) en productos de SE-elektrinic GmbH. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-1014 de tipo consumo incontrolado de recursos, podría interrumpir la disponibilidad del panel de administración enviando múltiples paquetes ICMP. Esta vulnerabilidad, no controla adecuadamente la asignación y el mantenimiento de un recurso limitado, lo que permite que un actor influya en la cantidad de recursos consumidos, lo que eventualmente conduce al agotamiento de los recursos disponibles.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-1015 de tipo control inadecuado de la generación de código, señala que un atacante podría enviar diferentes comandos del sistema operativo al sistema a través de la funcionalidad de configuración web del dispositivo.

A. Productos afectados:

- E-DDC3.3, versiones 03.07.03 y posteriores.

3. RECOMENDACIONES:

- Actualizar el paquete afectado con la última versión de software disponible que el proveedor lance cuando esté listo para abordar estas vulnerabilidades. A la fecha no se conoce ninguna solución oficial que aborde estas vulnerabilidades.

Fuente de Información:	• hxxps://www.se-elektronic.de/en/products

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025**	**Fecha: 29-01-2024**
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en IBM Storage Fusion HCI		
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 una vulnerabilidad de severidad **ALTA** de tipo validación de entrada incorrecta y enlace duro UNIX en IBM Storage Fusion HCI. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y permitir a un usuario local sobrescribir archivos arbitrarios en el sistema.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-39017 de tipo validación de entrada incorrecta, existe debido a una validación de entrada incorrecta dentro del componente Operaciones (Quartz) en Oracle Retail Customer Management and Segmentation Foundation. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para ejecutar código arbitrario.

Esta vulnerabilidad, recibe entradas o datos, pero no valida o valida incorrectamente que la entrada tiene las propiedades necesarias para procesar los datos de forma segura y correcta.

A. Productos afectados:

- Storage Fusion: versiones anteriores a 2.7.1.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7104743

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025**	**Fecha: 29-01-2024**
		Página: 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en productos NetApp		
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 una vulnerabilidad de severidad **ALTA** de tipo escalada de privilegios en ONTAP 9 de NetApp. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario autenticado escalar privilegios y generar una denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-21985 de tipo escalada de privilegios en ONTAP 9 de NetApp, podría permitir a un usuario autenticado con múltiples cuentas remotas con diferentes roles realizar acciones a través de la API REST más allá de su privilegio pretendido. Las posibles acciones incluyen ver métricas y detalles de configuración limitados o modificar configuraciones limitadas, algunas de las cuales podrían resultar en una denegación de servicio.

La explotación exitosa de esta vulnerabilidad podría permitir que un usuario autenticado con una función fusionada escale sus privilegios en las versiones afectadas de ONTAP 9.

A. Productos afectados:

- ONTAP 9 anteriores a 9.9.1P18, 9.10.1P16, 9.11.1P13, 9.12.1P10 y 9.13.1P4.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://security.netapp.com/advisory/ntap-20240126-0001/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 29-01-2024
		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 plataforma de entretenimiento en línea 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		

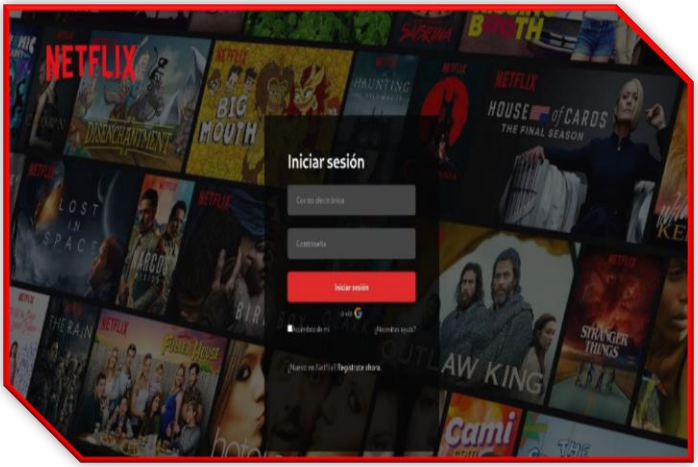
Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que ciberdelincuentes 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 del Phishing es el siguiente:



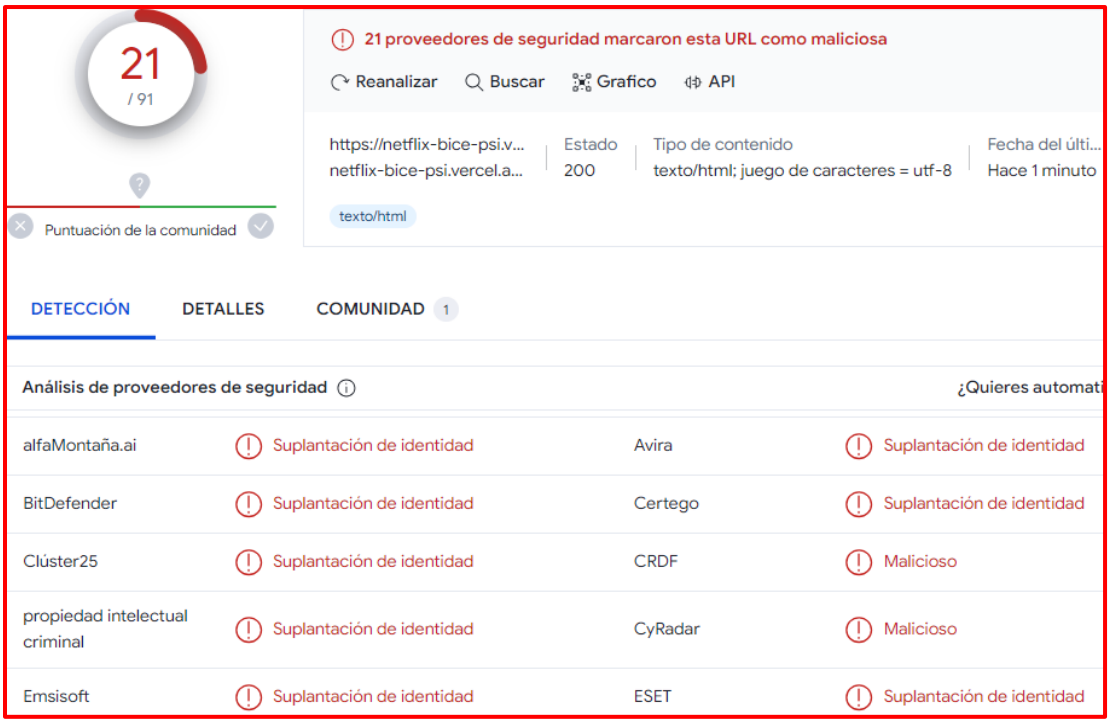
Paso N.º 01

Sitio web fraudulento de Netflix, solicita a la víctima registrar las credenciales de acceso (Correo electrónico y contraseña), para luego dar clic en <**Iniciar Sesión**>. Pero, pasados unos segundos, redirige al sitio web oficial de la plataforma de entretenimiento; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

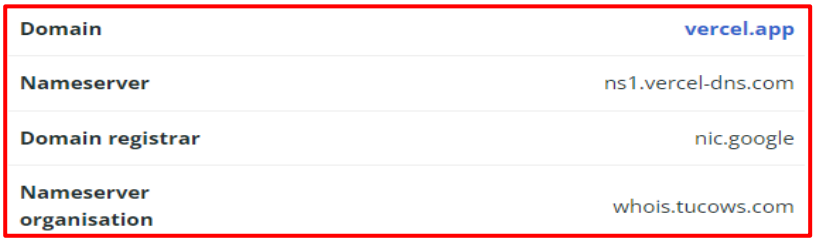
- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento POSEE protocolo de seguridad de red (https), sin embargo, es malicioso.
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. Proveedores de seguridad informática ALERTAN COMO SUPLANTACIÓN DE IDENTIDAD - PHISHING.

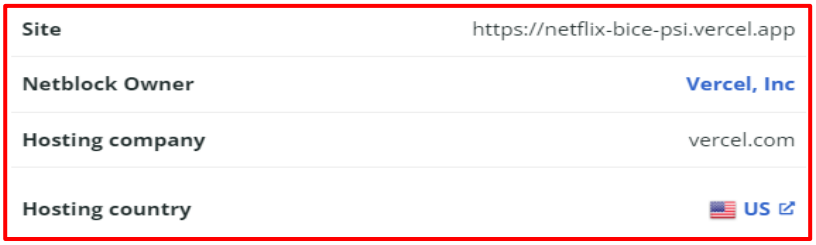


C. Indicadores de compromiso (IoC)

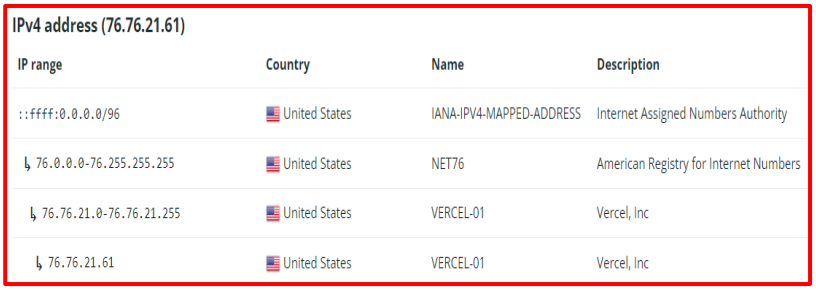
- Dominio : vercel[.]app



- URL : hxxps://netflix-bice-psi[.]vercel[.]app



- IP : 76[.]76[.]21[.]61



- Servidor : Vercel
- SHA-256 : 4573293eb1d01dfd0aef9d39eeb619b728157bb3f641ed12f035cd480e62b16c
- Tipo de tex. : Text/Html

D. 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.).

E. 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 las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).

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

Índice alfabético