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, 24 de enero de 2023

021-2023-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° 021	Fecha: 24-01-2023 Página 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Hackers promocionan malware a través de anuncios de búsqueda de Google para OBS, VLC, 7-Zip, CCleaner		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Internet, Correo Electrónico, Redes Sociales		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código malicioso		

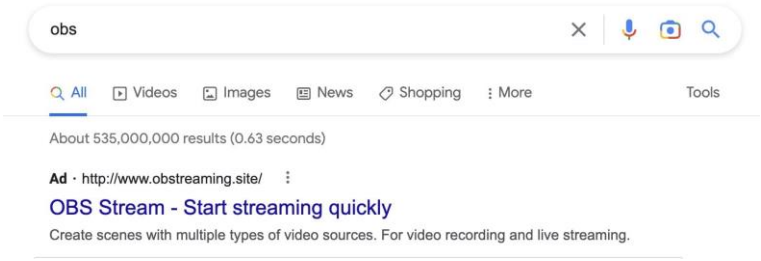
Descripción

Basándose en la creación de sitios falsos y pautando para que la página salga en los primeros resultados de búsqueda de Google, los atacantes pretenden engañar a los usuarios.

DETALLES:

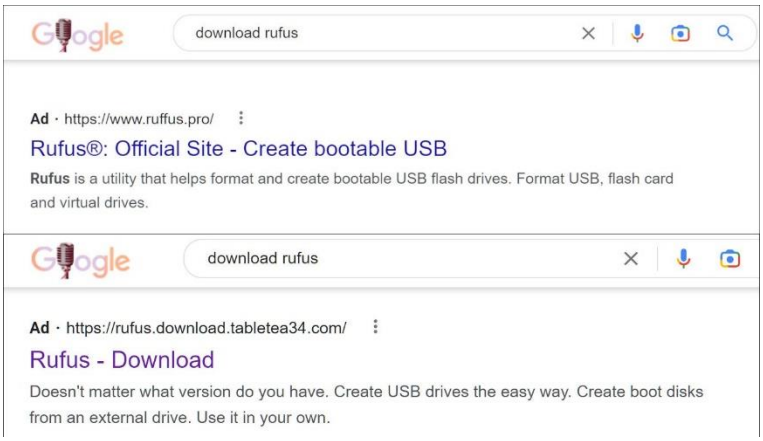
Ya son varios los casos que se conocen sobre esta modalidad de ciberataque, con la que los delincuentes quieren que la persona acceda a la página y descargue un software, que en realidad es un virus.

Uno de ellos es promocionando OBS (Open Broadcaster Software), que es un programa para transmitir directos en plataformas digitales como Twitch, Facebook y YouTube. Cuando los usuarios buscan en Google la aplicación les puede salir como primer resultado un anuncio de una página falsa.



Pero este no es el único caso que se ha conocido hasta el momento. Según reportaron usuarios en Reddit, al buscar los controladores gráficos de AMD para descargarlos en Google, les apareció un anuncio de una página falsa en el primer resultado.

Una situación que también sucedió con VLC, el reproductor multimedia gratuito desarrollado por la fundación VideoLAN, que fue incorporado en una web falsa, según detectó Trend Micro, denominando este tipo de ataque como "envenenamiento de la optimización de motores de búsqueda (SEO)".



Los resultados del motor de búsqueda pueden estar contaminados para descargar archivos maliciosos por envenenamiento de SEO y las herramientas legítimas pueden realizar un comportamiento malicioso porque se abusó de ellas, comentaron los investigadores.

Al ser un contenido pago, el buscador posiciona el sitio fraudulento por encima de los oficiales, que son los que brindan las garantías para que los usuarios descarguen los programas sin ningún problema

RECOMENDACIONES:

- Evite ingresar a los enlaces de mensajes de spam/phishing o ingresar a sitios web desconocidos.
- Evite ingresar a los anuncios publicitarios.
- Evite revelar información personal mediante un mensaje de texto o un correo electrónico de una fuente que no sea de confianza en donde se le solicita información personal.
- Evite abrir archivos adjuntos de correos electrónicos sospechosos.
- Buscar y descargar los programas que necesita desde sus sitios oficiales.
- Mantenga sus programas, antivirus y sistema operativo actualizados.

Fuentes de información	▪ hxxps://blog.segu-info.com.ar/2023/01/delincuentes-promocionan-malware-traves.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 021**	**Fecha: 24-01-2023**
		Página 6 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de ejecución remota de comandos en Apache Airflow MySQL Provider		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo inyección de comando de sistema operativo en Apache Airflow MySQL Provider. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos de shell arbitrarios en el sistema de destino.

2. **Detalles:**

- La vulnerabilidad de severidad **alta** identificada como CVE-2023-22884 de inyección de comando de sistema operativo podría permitir a un atacante remoto ejecutar comandos de shell arbitrarios en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable.
- La vulnerabilidad de tipo inyección de comando de sistema operativo, se debe a que el software construye la totalidad o parte de un comando del sistema operativo utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente los elementos especiales que podrían modificar el comando previsto del sistema operativo cuando se envía a un componente descendente.

3. **Productos afectados:**

- Apache Airflow: 0.1 - 2.5.0;
- Apache Airflow MySQL Provider: 1.0.0 - 4.0.0 rc1.

4. **Solución:**

- Se recomienda actualizar los productos afectados con la última versión de software disponible que corrige esta vulnerabilidad.

Fuentes de información	▪ hxxp://github.com/apache/airflow/pull/28811 ▪ hxxp://lists.apache.org/thread/0l0j3nt0t7fzrcjl2ch0jgj6c58kxs5h

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 021**	**Fecha: 24-01-2023** **Página 7 de 10**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de escalada de privilegios en Dell EMC PV ME5		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo permisos, privilegios y controles de acceso en Dell EMC PV ME5. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto elevar privilegios en un sistema afectado.

2. Detalles:

- La vulnerabilidad de severidad **alta** identificada como CVE-2023-23691 de permisos, privilegios y controles de acceso en Dell EMC PV ME5, podría permitir a un atacante remoto aumentar los privilegios en el sistema. La vulnerabilidad existe debido a un problema de desincronización del lado del cliente. Un atacante remoto puede obligar al navegador de la víctima a desincronizar su conexión con el sitio web.
- La vulnerabilidad de tipo permisos, privilegios y controles de acceso en los puntos débiles de esta categoría, están relacionados con la gestión de permisos, privilegios y otras características de seguridad que se utilizan para realizar el control de acceso.

3. Productos afectados:

- DELL VP ME5012: 5.1.0.0.0 - 5.1.0.1.0;
- DELL VP ME5024: 5.1.0.0.0 - 5.1.0.1.0;
- DELL PV ME5084: 5.1.0.0.0 - 5.1.0.1.0.

4. Solución:

- Se recomienda actualizar los productos afectados con la última versión de software disponible que corrige esta vulnerabilidad.

Fuentes de información	▪ hxxp://www.dell.com/support/kbdoc/en-us/000207533/dsa-2023-018-dell-emc-powervault-me5-security-update-for-a-client-desync-attack-vulnerability

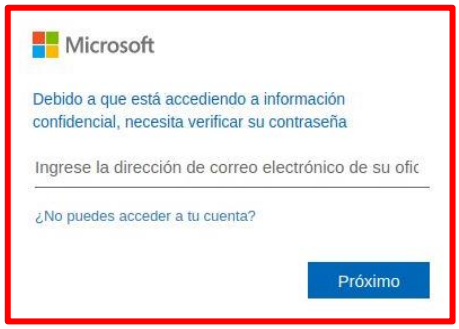
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 021	Fecha: 24-01-2023
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección falso servicio del correo electrónico de Microsoft.		
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 subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que los ciberdelincuentes vienen llevando a cabo una campaña de Phishing dirigidos a usuarios del servicio de correo electrónico proporcionados por Microsoft, por medio de la creación de un sitio web falso similar al oficial Microsoft Office, con el objetivo de robar credenciales de acceso (correo electrónico y contraseña) de los usuarios de la compañía tecnológica.

2. Detalles del proceso de Phishing



01

Paso N.º 01

Sitio web falso que suplanta la identidad de Microsoft Office, solicita a la víctima, registrar el usuario (correo electrónico, teléfono o Skype) al momento de abrir un archivo confidencial.

Paso N.º 02

Una vez registrado el usuario y hecho clic en <Próximo>, requiere ingresar la contraseña para continuar con el acceso.

02

03

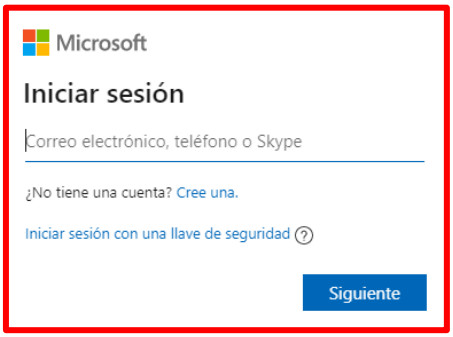
Paso N.º 03

Luego de completar las credenciales de acceso y darle clic en <Próximo>, el atacante le informa a la víctima que no puede mostrar el mensaje por el momento y vuelva intentarlo.

Paso N.º 03

Al darle clic en intentar otra vez, es redirigido al sitio oficial de Microsoft, aludiendo un aparente error de autenticación; sin embargo, los datos ya fueron capturados.

04



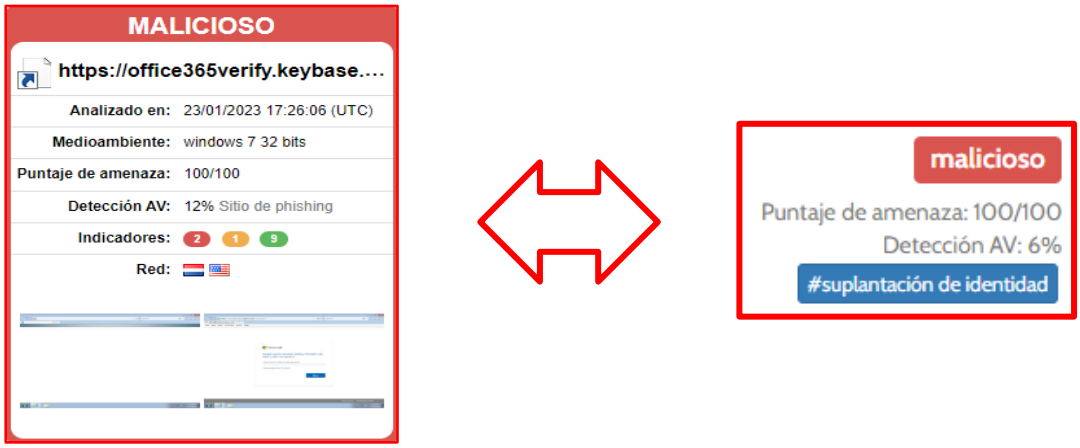
3. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que ONCE (11) proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING**.

CRDF	Malicioso	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	CASO	Suplantación de identidad
Fortinet	Suplantación de identidad	kaspersky	Suplantación de identidad
netcraft	Malicioso	OpenPhish	Suplantación de identidad
Base de datos de phishing	Suplantación de identidad	Sophos	Suplantación de identidad

4. INDICADORES DE COMPROMISO

- **URL** : hxxps://office365verify.keybase.pub/iverify.html
- **SHA-256** : bee4110a05ebe555395ed0ee5fc8e6cdc0f6f625c09d5b4682b660dd415a2057
- **IP** : 3[.]95[.]91[.]171
- **Servidor** : nginx/1.18.0 (Ubuntu)
- **Dominio** : keybase.pub
- **Tipo** : texto/html

5. OTRAS DETENCIONES



6. Que es un Phishing:

- Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

7. Algunas Recomendaciones:

- Verificar detalladamente las URL de los sitios web
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético