

Boletín de Ciberseguridad

Diciembre 12 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	dmontalvo1302@gmail.com
TLP:	BLANCO
Registro grafico relacionado con el Phishing	
Bogotá, Martes, 11 de marzo de 2025 Señor(a): Ciudad: Bogotá D.C Ref. CUI 7254178000020150023000 Respetado Señor(a):  PORTAFOLIO_JUDICIAL_ACUSE_PRIORITARIO_REFER... Se le notifica que el Secretaría General Tribunal Administrativo - Cundinamarca Con Función De Conocimiento programó diligencia de CONTINUACIÓN JUICIO ORAL para el día Miercoles 12 de marzo de 2025 a las 8:30:00 AM, actuación seguida en su contra , por el delito de perturbación a la posesión, esta audiencia se realizará de FORMA VIRTUAL. En el que usted figura como Imputado. OBSERVACIONES: Contáctese con el despacho al correo electrónico sectribant@cendoj.ramajudicial.gov.co para verificar la dirección donde debe asistir a la audiencia. Se recomienda visualizar este documento desde un ordenador o laptop, pulse "ejecutar" para garantizar la correcta comprensión de su contenido. Cordialmente, Reiner José Martínez Villegas SECRETARIO Carrera 28 A No. 18 A – 67 Complejo Judicial Paloque, Teléfono 4286242 Correo electrónico: planillascorreopq@cendoj.ramajudicial.gov.co AVISO DE CONFIDENCIALIDAD: Este correo electrónico contiene información de la Rama Judicial de Colombia. Si no es el destinatario de este correo y lo recibió por error comuníquelo de inmediato, respondiendo al remitente y eliminando cualquier copia que pueda tener del mismo. Si no es el destinatario, no podrá usar su contenido, de hacerlo podría tener consecuencias legales como las contenidas en la Ley 1273 del 5 de enero de 2009 y todas las que le apliquen. Si es el destinatario, le corresponde mantener reserva en general sobre la información de este mensaje, sus documentos y/o archivos adjuntos, a no ser que exista una autorización explícita. Antes de imprimir este correo, considere si es realmente necesario hacerlo, recuerde que puede guardarlo como un archivo digital.	

El CSIRT Académico UNAD informa acerca de un asunto de ciberseguridad que ha sido identificado y abordado por este Equipo. Se ha detectado un evento de phishing dirigido a miembros de nuestra comunidad. Es preciso indicar que la técnica de Phishing es un tipo de ataque cibernético en el cual los adversarios intentan engañar a los usuarios para que se revele información confidencial, como contraseñas, números de tarjetas de crédito o información personal.

Se ha realizado la respectiva indagación y se han identificado una serie de indicadores de compromiso (IoCs) asociados con este asunto.

Se realiza la verificación del archivo en mención, donde:

- 1. El archivo no cuenta con ninguna protección mediante contraseña:**
Para el usuario final, la ausencia de una contraseña en este tipo de archivos representa un alto riesgo. Al no estar protegido, el archivo puede ser abierto de manera inmediata, aumentando la probabilidad de que el usuario, sin sospechar de su naturaleza maliciosa, lo ejecute. Esto reduce significativamente el tiempo de reacción necesario para identificar la amenaza antes de que cause daño. Además, la facilidad de acceso elimina cualquier barrera

Boletín de Ciberseguridad

que pudiera obligar al usuario a detenerse y cuestionar la legitimidad del archivo, lo que incrementa el riesgo de infección y exposición de información sensible.

2. **El archivo descargado está comprimido y contiene un acceso directo malicioso:** Al extraer el archivo comprimido, se identificó un acceso directo que aparenta ser archivo legítimo, pero que, al analizar sus propiedades, se observa que es configurado para ejecutar acciones maliciosas. En la pestaña "Documento Web" del acceso directo, se encontró una URL con la siguiente dirección: file://\62.60.226.112@80\file\7309_9071.exe

Esta dirección apunta a un servidor remoto, desde el cual se intenta descargar y posiblemente ejecutar un archivo denominado build.exe. Este comportamiento indica un claro intento de los atacantes de explotar el acceso del usuario para conectarse a un recurso externo y ejecutar un archivo potencialmente malicioso.

Para el usuario final, este tipo de ataque representa un riesgo crítico porque:

- **Ejecución inadvertida de malware:** El acceso directo puede ser engañosamente presentado como un archivo legítimo, aumentando la probabilidad de que el usuario lo abra sin sospechar de su naturaleza maliciosa.
- **Exposición a servidores maliciosos:** Al intentar acceder a la dirección especificada, el sistema del usuario podría exponer información como la dirección IP o credenciales de red, facilitando un ataque más amplio.
- **Automatización del proceso malicioso:** La configuración del acceso directo permite que la descarga y ejecución del archivo se realice de manera rápida y silenciosa, sin intervención adicional del usuario, reduciendo las posibilidades de detección temprana.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	Documento judicial de cargos 11 de marzo - Orden de allanamiento No. 0077878.url
Veredicto:	Actividad sospechosa
Fecha del análisis:	Marzo 12, 2025 at 11:01:30
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	b2dead0f0563d77b54ae7fe99295a839
SHA1:	11d95f82815ade75d401df977474b9cdb90ca73b
SHA256:	5335603a304e42c6fef4d2fe76cbb92cf1b136d2ec9bea5a648fc002f392f2b1
SSDEEP:	6:JyXSvVG/FTVmJtOFJb5if5oeTckmrlSKdTQVciosv:cXaVWfmJtOFJQRzgrKd0VijT

Fuente. CSIRT Académico UNAD

Información de proceso



Boletín de Ciberseguridad

CMD	Ruta Comprometida	Proceso Padre
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

Correo electrónico: csirt@unad.edu.co

(+57 1) 344 37 00 Ext. 1042516