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:	ellechondelchonchis@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ---------
De: **El Lechon del Chonchis** <Ellechondelchonchis@gmail.com>
Date: lun, 9 dic 2024 a las 13:21
Subject: Remuneración Tutelar Proceso N° 03948939-002024
To:

Comunicado Rotativo

Asunto: Comunicado de Tutela

Por medio de la presente, se le notifica que se ha presentado una acción de tutela a su favor en relación con Debido a sucesos anormales los cuales son presentados en los documentos enviados

Al final del comunicado se adjuntan documentos del caso para su total conocimiento (Por favor validar los documentos antes de realizar cualquier consulta, ya que estos contienen parte de su información personal)

Detalles de la Acción:

- **Número de Radicado:** 03948939-002024
- **Fecha de Presentación:** 09 de Diciembre

DESCARGAR AQUI DOCUMENTOS
Nota: Presione en ejecutar para visualizar contenido

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

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 dos accesos directos maliciosos**: Al extraer el archivo comprimido, se identificó dos accesos directos que aparentan ser archivos legítimos, pero que, al analizar sus propiedades, se observan que están configurados para ejecutar acciones maliciosas. En las pestañas "Documento Web" de los accesos directos, se encontraron dos URL con la siguiente dirección: file://\\77.105.161.126@80\file\AdobePDF.exe y file://\\77.105.161.126@80\file\AdobeReaderPDF2024.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:	Oficio Tutelar Proceso N° 03948939-002024.url
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	diciembre 12, 2024 at 11:07:07
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	4D4295D033D231E35BF429EFCCF9BB06
SHA1:	D506382A8F6181182732C53C5C3B4EE9734FE027
SHA256:	16320AEE3F65FC9E52B44E26F2E41C22452869BAD47C7F1D11FF1530FE397FD0
SSDEEP:	6:JyXSvVG/FTVmJtOFJblvstXbPAbhYNraUr5q8Nvosv:cXaVWfmJtOFJB0tL3NL

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	"C:\WINDOWS\system32\rundll32.exe" "C:\WINDOWS\system32\ieframe.dll",OpenURL %l	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD
Correo electrónico: csirt@unad.edu.co
(+57 1) 344 37 00 Ext. 1042516