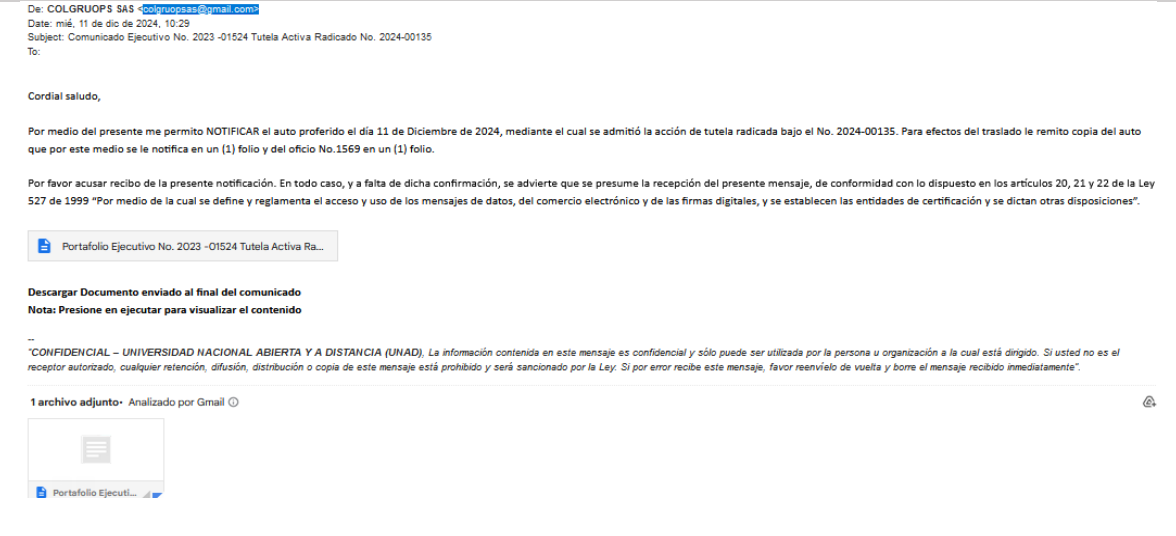
Diciembre 12 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	colgruopsas@gmail.com
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing


De: COLGRUOPS SAS <colgruopsas@gmail.com>
Date: mié, 11 de dic de 2024, 10:29
Subject: Comunicado Ejecutivo No. 2023 -01524 Tutela Activa Radicado No. 2024-00135
To:

Cordial saludo,

Por medio del presente me permito NOTIFICAR el auto proferido el día 11 de Diciembre de 2024, mediante el cual se admitió la acción de tutela radicada bajo el No. 2024-00135. Para efectos del traslado le remito copia del auto que por este medio se le notifica en un (1) folio y del oficio No.1569 en un (1) folio.

Por favor acusar recibo de la presente notificación. En todo caso, y a falta de dicha confirmación, se advierte que se presume la recepción del presente mensaje, de conformidad con lo dispuesto en los artículos 20, 21 y 22 de la Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

Portafolio Ejecutivo No. 2023 -01524 Tutela Activa Ra...

Descargar Documento enviado al final del comunicado
Nota: Presione en ejecutar para visualizar el contenido

--
"CONFIDENCIAL – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD). La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona u organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibido y será sancionado por la Ley. Si por error recibe este mensaje, favor reenvíelo de vuelta y borre el mensaje recibido inmediatamente".

1 archivo adjunto · Analizado por Gmail

Portafolio Ejecuti...

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 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://\\62.60.226.24@80\file\PDFReader.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:	Portafolio Ejecutivo No. 2023 -01524 Tutela Activa Radicado No. 2024-00135 (1).url
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	December 12, 2024 at 10:56:30
MIME:	application/x-wine-extension-ini
Información del archivo:	Generic INItialization configuration [InternetShortcut]
MD5:	FF05EADEB00D00F01BFBB29AB7B74B2E
SHA1:	2C64637BE98C0DEE4759A2BC6ED30D7AE7ABA8A7
SHA256:	A69C825854983C417970BAEA932318010672CB836C6F6721577657D1DDB530E7
SSDEEP:	6:JyXSvVG/FTVmJtOFJblvstXbPAbhYNrIEirQsv:cXaVWfmJtOFJB0tLjS

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