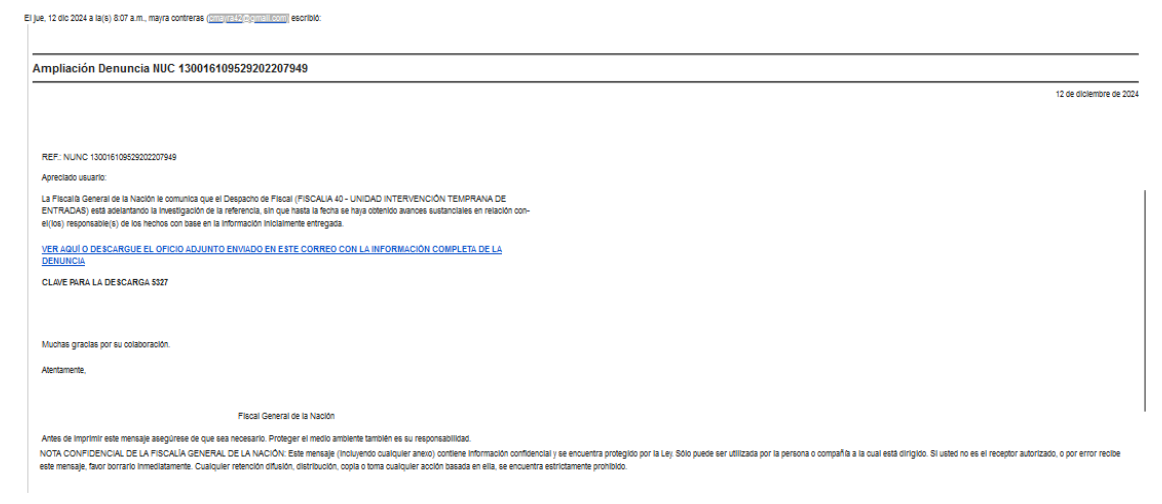
Diciembre 13 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	downloader.
Cuenta de correo del remitente:	cmayra42@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



El jue, 12 dic 2024 a la(s) 8:07 a.m., mayra contreras (cmayra42@gmail.com) escribió:

Ampliación Denuncia NUC 130016109529202207949

12 de diciembre de 2024

REF: NUNC 130016109529202207949

Apreciado usuario:

La Fiscalía General de la Nación le comunica que el Despacho de Fiscal (FISCALIA 40 - UNIDAD INTERVENCIÓN TEMPRANA DE ENTRADAS) está adelantando la investigación de la referencia, sin que hasta la fecha se haya obtenido avances sustanciales en relación con-el(los) responsable(s) de los hechos con base en la información inicialmente entregada.

VER AQUÍ O DESCARGUE EL OFICIO ADJUNTO ENVIADO EN ESTE CORREO CON LA INFORMACIÓN COMPLETA DE LA DENUNCIA

CLAVE PARA LA DE$CARGA 5327

Muchas gracias por su colaboración.

Atentamente,

Fiscal General de la Nación

Antes de imprimir este mensaje asegúrese de que sea necesario. Proteger el medio ambiente también es su responsabilidad.
NOTA CONFIDENCIAL DE LA FISCALÍA GENERAL DE LA NACIÓN: Este mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley. Sólo puede ser utilizada por la persona o compañía a la cual está dirigido. Si usted no es el receptor autorizado, o por error recibe este mensaje, favor borrarlo inmediatamente. Cualquier retención difusión, distribución, copia o toma cualquier acción basada en ella, se encuentra estrictamente prohibido.

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.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	OFICIO DE NUC 130016109529202207949 DICIEMBRE 12 DE 2024.wsf
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	November 13, 2024 at 10:07:51
MIME:	text/html
Información del archivo:	HTML document, Unicode text, UTF-16, little-endian text, with very long lines (566), with CRLF line terminators
MD5:	EBD2634C82FA75460E28EE20E27C6970
SHA1:	DEA94132DD5A0772F2908F181BF2D756294F381D

SHA256:	B168267ED0C650F42E9A2E3CC4D702E0CA8946E0F1D8B5E624DDC8B239C87CD8
SSDEEP:	48:aTyUeHeHeTe8eJeoeoeTeme8eHeqeA+eRe8eoeQeoeFe2exfec/6q28f409:Wyj+ +6bUHH65b+9AhsbHfHQJxms6q28R

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\<USER>\Desktop\98978676465879 8789 TRANSACCION ACH DICIEMBRE 12 DE 2024.wsf"	"C:\Users\<USER>\Desktop\98978676465879 8789 TRANSACCION ACH DICIEMBRE 12 DE 2024.wsf"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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