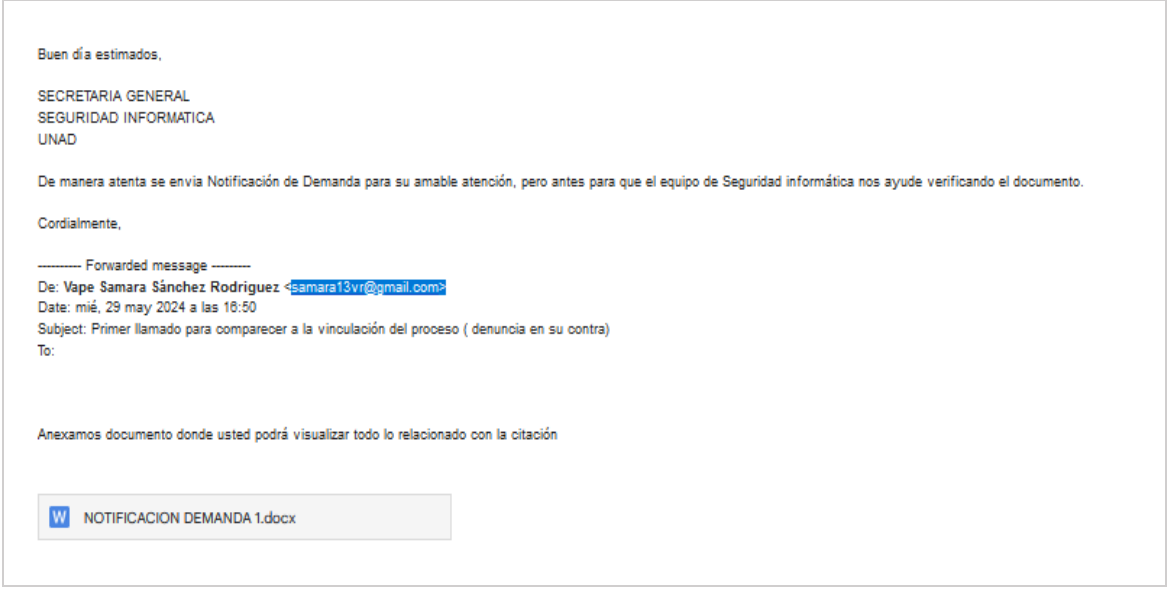
Mayo 30 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	W64.AIDetectMalware
Cuenta de correo del remitente:	samara13vr@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



Buen día estimados,

SECRETARIA GENERAL
SEGURIDAD INFORMATICA
UNAD

De manera atenta se envia Notificación de Demanda para su amable atención, pero antes para que el equipo de Seguridad informática nos ayude verificando el documento.

Cordialmente,

---------- Forwarded message ---------
De: **Vape Samara Sánchez Rodriguez** <samara13vr@gmail.com>
Date: mié, 29 may 2024 a las 16:50
Subject: Primer llamado para compareoer a la vinculación del proceso (denuncia en su contra)
To:

Anexamos documento donde usted podrá visualizar todo lo relacionado con la citación

NOTIFICACION DEMANDA 1.docx

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:	05 PROCESO JUDICIAL JUZGADO CIVIL 05 DEL CIRCUITO.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Mayo 30, 2024 at 15:49:12
MIME:	application/x-dosexec
Información del archivo:	Win32 EXE
MD5:	41a41b33ea2567251b5f43f792cf8d39

SHA1:	2fca6e8207addc8c16395e68b9583920d889b185
SHA256:	d87b9e3357deb4a65a4fffc7db078a5d2dbfccad834080f507e32af551057b07
SSDEEP:	196608:j3G5DyJF9SC3Vde4g9SoEeDcSozefxyVENBx:quJF9n2/ncZUy+h

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\user\Desktop\05 PROCESO JUDICIAL JUZGADO CIVIL 05 DEL CIRCUITO.exe"	"C:\Users\user\Desktop\05 PROCESO JUDICIAL JUZGADO CIVIL 05 DEL CIRCUITO.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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