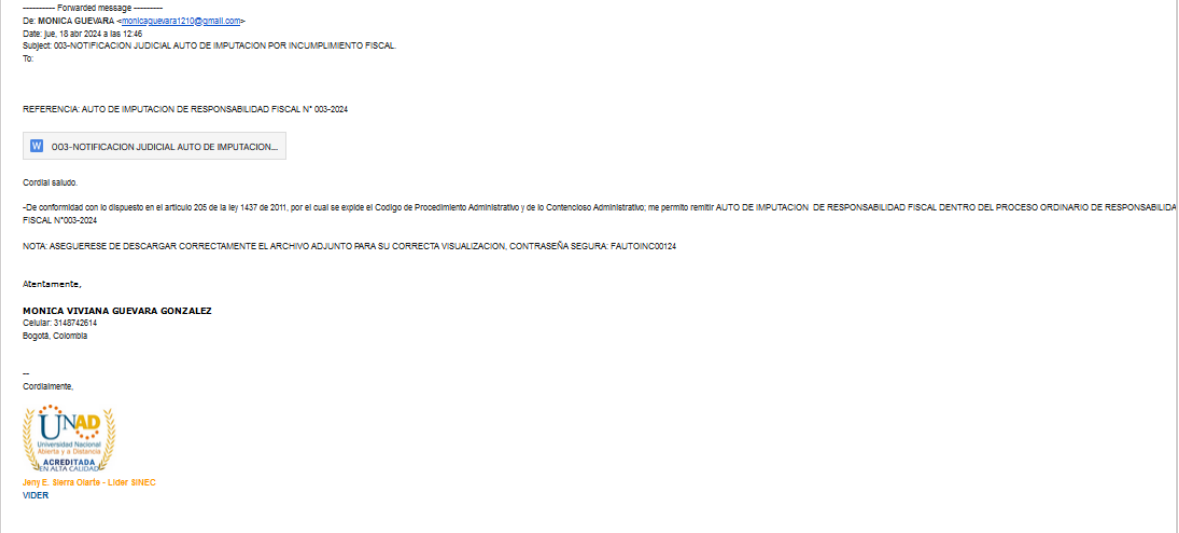
Abril 18 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.gvff
Cuenta de correo del remitente:	gestionsocial@nobsa-boyaca.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ----------
De: MONICA GUEVARA <monicaguevara1210@gmail.com>
Date: jue, 18 abr 2024 a las 12:46
Subject: 003-NOTIFICACION JUDICIAL AUTO DE IMPUTACION POR INCUMPLIMIENTO FISCAL
To:

REFERENCIA: AUTO DE IMPUTACION DE RESPONSABILIDAD FISCAL N° 003-2024

003-NOTIFICACION JUDICIAL AUTO DE IMPUTACION...

Cordial saludo.

-De conformidad con lo dispuesto en el articulo 205 de la ley 1437 de 2011, por el cual se expide el Codigo de Procedimiento Administrativo y de lo Contencioso Administrativo; me permito remitir AUTO DE IMPUTACION DE RESPONSABILIDAD FISCAL DENTRO DEL PROCESO ORDINARIO DE RESPONSABILIDA FISCAL N°003-2024

NOTA: ASEGUERESE DE DESCARGAR CORRECTAMENTE EL ARCHIVO ADJUNTO PARA SU CORRECTA VISUALIZACION, CONTRASEÑA SEGURA: FAUTOINC00124

Atentamente,

MONICA VIVIANA GUEVARA GONZALEZ
Celular: 3148742614
Bogotá, Colombia

--
Cordialmente,

Jeny E. Sierra Olarte - Líder SINEC
VIDER

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:	001-NOTIFICACION JUDICIAL.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	April 18, 2024 at 18:00:30
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	ae224c5e196ff381836c9e95deebb7d5
SHA1:	910446a2a0f4e53307b6fdeb1a3e236c929e2ef4
SHA256:	bf933ccf86c55fc328e343b55dbf2e8ebd528e8a0a54f8f659cd0d4b4f261f26

SSDEEP:	1536:Wio8DVyYs7JZT0uPXn8OS6sIe3ekT5Z240jSZk:WkhyYIJZT0uPXn8OdsIe3c4Ql

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\001-NOTIFICACION JUDICIAL.exe"	"C:\Users\admin\AppData\Local\Temp\001-NOTIFICACION JUDICIAL.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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