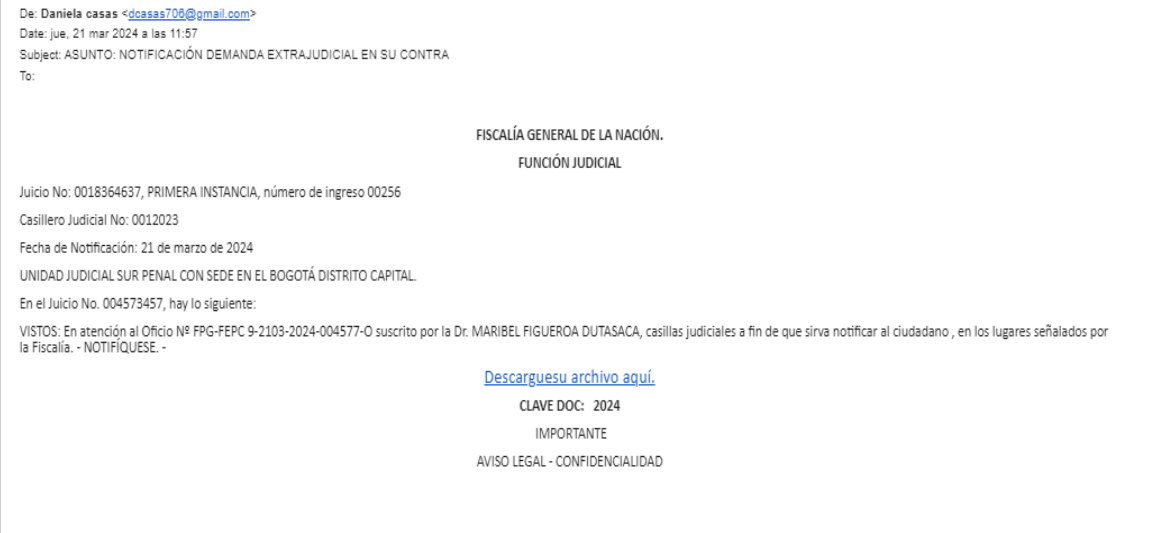
Marzo 24 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.lazy/remcos
Cuenta de correo del remitente:	dcasas706@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



De: **Daniela casas** <dcasas706@gmail.com>
Date: jue, 21 mar 2024 a las 11:57
Subject: ASUNTO: NOTIFICACIÓN DEMANDA EXTRAJUDICIAL EN SU CONTRA
To:

FISCALÍA GENERAL DE LA NACIÓN.
FUNCIÓN JUDICIAL

Juicio No: 0018364637, PRIMERA INSTANCIA, número de ingreso 00256
Casillero Judicial No: 0012023
Fecha de Notificación: 21 de marzo de 2024
UNIDAD JUDICIAL SUR PENAL CON SEDE EN EL BOGOTÁ DISTRITO CAPITAL.
En el Juicio No. 004573457, hay lo siguiente:
VISTOS: En atención al Oficio Nº FPG-FEPC 9-2103-2024-004577-O suscrito por la Dr. MARIBEL FIGUEROA DUTASACA, casillas judiciales a fin de que sirva notificar al ciudadano , en los lugares señalados por la Fiscalía. - NOTIFÍQUESE. -

Descarguesu archivo aquí.
CLAVE DOC: 2024
IMPORTANTE
AVISO LEGAL - CONFIDENCIALIDAD

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:	**wallpaper32.exe**
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Marzo 24, 2024 at 17:26:00
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	4882b39cbbfdb87fe32da4edb86a93f2
SHA1:	0bf9eee248df01a5d3ab794b0298a435c1516bfa
SHA256:	d2db2ce86fbf3b55e42cda816c500f7843f3ba02a8564e030b9305ef96716e2d

SSDEEP:	49152:WGczHI2l+Jl72+N/K4KfrsV5t9BU+4vPTb4YQtj1gkwnuGady/bg8F6jIIfrgqjp:rA+p/H9wwjOnuhdYbrcdxak44

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"%SAMPLEPATH%\wallpaper32.exe"	"%SAMPLEPATH%\wallpaper32.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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