Junio 26 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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

---------- Forwarded message ---------
De: **Edna Lizeth Gutierrez Roa** <edna.gutierrez@florencia.edu.co>
Date: lun, 24 jun 2024 a la(s) 11:18 a.m.
Subject: COMUNICA ACTUACION PROCESAL RAD 2023-00136-00
To:

RADICACIÓN: 44001-33-40-005-2023-00136-00

NULIDAD Y RESTABLECIMIENTO DEL DERECHO - En general / Sin subclase

Para los fines pertinentes me permito informarle que en la fecha **24/06/2024** se emitió Auto ordena correr traslado para alegatos de conclusión en el asunto de la referencia.

VER AQUÍ PDF DE PROCESO DE AUDIENCIA JUDICIAL

CLAVE DE ACCESO AL PDF:6488

--

FLORENCIA BIODIVERSIDAD PARA Todos

EDNA LIZETH GUTIERREZ ROA
Técnico Administrativo
SEM Alcaldía de Florencia
(8) 4358100 Ext. 1307
Cll 15 Carrera 12 Esquina Piso 3
www.florencia.edu.co/portal/v4 edna.gutierrez@florencia.edu.co

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:	COMUNICA ACTUACION PROCESAL RAD 2023-00136-00d.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Junio 26, 2024 at 19:20:15

MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	9C13F9BD5206401FA51D1546C3938357
SHA1:	A2C93D591B791EE9208068FA6C5780B27A8FE73E
SHA256:	EEA6212509D6BEB5FA3514670FD0E697FA13BC894EF3F2D9D245453899BADEC9
SSDEEP:	49152:kkA1G4dnbibBlCDkTM+qnKK+tPNn4xKtuaJwT5z9ljTUEV2PXHL:r4dnbkTM+qnKK+tPlitaJQ72PXr

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
""C:\Users\admin\AppData\Local\Temp\COMUNICA ACTUACION PROCESAL RAD 2023-00136-00d.exe" "	""C:\Users\admin\AppData\Local\Temp\COMUNICA ACTUACION PROCESAL RAD 2023-00136-00d.exe" "	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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