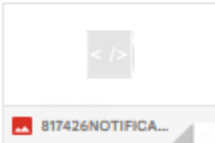


Boletín de Ciberseguridad

Mayo 23 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	HijackLoader, Loader
Cuenta de correo del remitente:	desarrollosocial@guasca-cundinamarca.gov.co
TLP:	BLANCO
Registro grafico relacionado con el Phishing	
ASUNTO: NOTIFICACIÓN DE DEMANDA CONTRASEÑA SEGURA PARA ABRIR ARCHIVO ADJUNTO: MI489T74Y FISCAL ACUSATORIO - JUZGADO NÚMERO 8  REPÚBLICA DE COLOMBIA TRIBUNAL SUPERIOR DEL DISTRITO DE LA RAMA JUDICIAL PALACIO DE JUSTICIA - CALLE 35 CARRERAS 11 Y 12 TELÉFONO 6520043 EXT.: 2201 CIRCULAR No. 07 1 archivo adjunto • Analizado por Gmail ⓘ 	

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.

Boletín de Ciberseguridad

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	01 PROCESO JUDICIAL.exe
Veredicto:	Actividad sospechosa
Fecha del análisis:	Mayo 23, 2024 at 17:20:12
MIME:	application/x-rar
Información del archivo:	RAR archive data, v5
MD5:	968CD58CD11C8C4367D36C0C6936AF6E
SHA1:	78E6482AA523A95EDB2B24967B0DD575A152E502
SHA256:	CBF8C97BB03BE7877390DDB7B133F666F808766C9F439724F37497948625C6BB
SSDEEP:	98304:iruqeySxwizlsd3xbmk+R5wuBeveYNw0x85PiSeybo27ODjurQKsVagvpL164P 2d:RPBFezzjvpe

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\Desktop\01 PROCESO JUDICIAL\01 PROCESO JUDICIAL.exe"	"C:\Users\admin\Desktop\01 PROCESO JUDICIAL\01 PROCESO 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