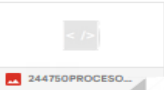


Boletín de Ciberseguridad

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:	martha52325@gmail.com
TLP:	BLANCO
Registro grafico relacionado con el Phishing	
ASUNTO: NOTIFICACIÓN DE DEMANDA CONTRASEÑA SEGURA PARA ABRIR ARCHIVO ADJUNTO: MITY4Y84T FISCAL ACUSATORIO - JUZGADO NÚMERO 13  REPÚBLICA DE COLOMBIA TRIBUNAL SUPERIOR DEL DISTRITO DE LA RAMA JUDICIAL PALACIO DE JUSTICIA - CALLE 35 CARRERAS 11 Y 12 TELÉFONO 65200043 EXT.: 2204 CIRCULAR NO. 09 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.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	01 PROCESO JUDICIAL EN SU CONTRA.exe
Veredicto:	Actividad sospechosa
Fecha del análisis:	Mayo 30, 2024 at 16:15:20



Boletín de Ciberseguridad

MIME:	application/x-dosexec
Información del archivo:	PE32+ executable (GUI) x86-64, for MS Windows
MD5:	9d2d82ab50fb044e5aeaa37bbc70aa16
SHA1:	328c1833748c0d17fec5970270ff4fc44323cc52
SHA256:	b41a948c0018a4669f6e2461cd826adb5f2d0caffc05618c9b44a2491946600c
SSDEEP:	196608:j3GPDyJF9SC3MdeGgNSoEeDcSozefxyPEtd:QuJF9nfNncZUyMP

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\<USER>\Downloads\01 PROCESO JUDICIAL EN SU CONTRA.exe"	"C:\Users\<USER>\Downloads\01 PROCESO JUDICIAL EN SU CONTRA.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

Correo electrónico: csirt@unad.edu.co

(+57 1) 344 37 00 Ext. 1042516