Septiembre 07 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.msil/filerepmalware
TLP:	**BLANCO**

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:	CITACION No 2158952 DEL 6 DE SEPTIEMBRE DEL 2023.exe
Veredicto:	**Actividad Maliciosa**
Fecha del análisis:	September 07, 2023 at 15:00:00
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	2AB95246241013F7D9943927CCBA8BAF
SHA1:	B560E98DF433430CB0752A5AA4B49435DC5DE22D
SHA256:	4BF5E6608AD90C11B9C8E6346FA9081511575A1187FDEC5DBFCC3F6DB1944E0C
SSDEEP:	98304:fHdqsl5lm/uTJPEysRwjFHemlpguSry/ND8x5WS2A9h:f9q8m2TJEysRwjgmlpBD8aqh

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\CITACION No 2158952 DEL 6 DE SEPTIEMBRE DEL 2023.exe"	C:\Users\admin\AppData\Local\Temp\CITACION No 2158952 DEL 6 DE SEPTIEMBRE DEL 2023.exe	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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