Agosto 11 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing, Credentials In File, Software Discovery, Non-Standard Port, Query Registry, System Information Discovery
Malware detectado:	AsyncRAT
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:	---FISCALIA GENERAL DE LA NACION --(1).REV
Veredicto:	**Actividad maliciosa**
Fecha del análisis:	Agosto 11 de 2023 - Hora 17:20:00
MIME:	application/x-7z-compressed
Información del archivo:	7-zip archive data, version 0.4
MD5:	C263D2009CFE4ABD34ADDCACA24DD4F3
SHA1:	3B6E95AA51C0B1432F5EC42774828CB2C0014FE8
SHA256:	2588F53684B8794F050EB6128BA2D25E801F7C9EF3887D3F47692612F39E0DEF
SSDEEP:	3072:fWRAjVmOzXM3ikEtSp+A+0/9hX91nNOuEuhRDpheUFTVx9LuIX:fWqjVu3ikEtSpzlhX91NIFheAVzZ

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Procesos relacionados
"C:\Users\admin\Desktop\---FISCALIA GENERAL DE LA NACION --.exe"	"C:\Users\admin\Desktop\---FISCALIA GENERAL DE LA NACION --.exe"	• explorer.exe • vbc.exe • cmd.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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