Agosto 29 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.gen3/remcos
Cuenta de correo del remitente:	ruizwendy25.28@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

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:	ACUSACIÓN JUDICIAL EN PROCESO.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Agosto 29, 2024 at 19:56:16
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	DE7501B72C10BD5D7DB619F83F3543EB

SHA1:	81FA72784EEA2CDF026D78CBF93B4A0C910E776E
SHA256:	B6F488A9F6BA3A28BA0A0A3D23DB66A372B61AC8CD2CCD3AC7430FFA9611FAC6
SSDEEP:	98304:cAAgraWCHFhA4UMw7HOVpEFyGE4Gy0ABo1Qvc4klbib1J0CfhHxT9h7jbnhgMjNL:Hlq

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\AC USACIÓN JUDICIAL EN PROCESO.exe"	"C:\Users\admin\AppData\Local\Temp\AC USACIÓN JUDICIAL EN PROCESO.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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