Agosto 26 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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

DESARROLLO DE TRANSACCIÓN REALIZADA

DESCARGAR PDF EN LA PARTE DE ABAJO DE DESARROLLO DE TRANSACCIÓN INTERBANCARIA

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:	out_sig..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Agosto 26, 2024 at 13:26:12
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	E26AF3F92E8F9E8082D660F31353F86D

SHA1:	D185030089248234C9E83AD9216B3B8F7890167A
SHA256:	CB8D0BA3CB1D8F9222E80075CBF88DD0500B557F68D8CDA57CE44258A1D2FD52
SSDEEP:	98304:j6Rb5gwTsPaKvVxNsB3elMvOGvhK5wlkkn768azxco:+kZ

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\out _sig..exe"	"C:\Users\admin\AppData\Local\Temp\out _sig..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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