

Boletín de Ciberseguridad

Julio 27 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

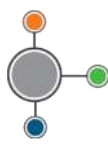
Técnica Mitre:	Phishing
Malware detectado:	trojan.msil/remcos
Cuenta de correo del remitente:	nfo@expresodelsol.com
TLP:	BLANCO
Registro grafico relacionado con el Phishing	
	

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:	FALLO DE TUTELA; RAD 6638921600-2024..ex
Veredicto:	Actividad sospechosa
Fecha del análisis:	Julio 27, 2024 at 10:34:27
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	B54DC1F211608BDD38E535A4E045EF1C



Boletín de Ciberseguridad

SHA1:	C4E8DCE7BB152B7C7CC2A978C1393A02A1CFAD82
SHA256:	932F92403AB63909D4A9EA1A182C3B35C53625908855CB0E333BA86AC831BBC4
SSDEEP:	3072:0bZOylIXfOOQpf0SAWkGUF5hl/itoPHt3:0bYAObf0VWmF5hl/itoPt

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\FA LLO DE TUTELA; RAD 6638921600- 2024..exe"	"C:\Users\admin\AppData\Local\Temp\FA LLO DE TUTELA; RAD 6638921600- 2024..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

Correo electrónico: csirt@unad.edu.co

(+57 1) 344 37 00 Ext. 1042516