Octubre 04 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.
Cuenta de correo del remitente:	rodriguezjorgeb6@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:	Liquidacion00000389387725.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	October 04, 2024 at 14:56:08
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	99D634350E3E891A20846FF50233C687

SHA1:	10C3C935B76578C5B01E6FB6CD38226D52EDC539
SHA256:	D9D075A306A8608E30F95FD450679D99407354DA371D159873FA38A14EACDE5B
SSDEEP:	49152:oIOYx1uI7XDDYt3L5u9r9p9RSS7UlxeWdGkM4feuO8+m3evARXXky37Y2zB9GJyG:DbuI73YtqUid8+mEokA1eiAvkRumaLJ

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Liquidacion00000389387725.exe"	"C:\Users\admin\AppData\Local\Temp\Liquidacion00000389387725.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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