Junio 21 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Trojan.Loader
Cuenta de correo del remitente:	asambleadelcesarjuridica@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:	ACH REF NO 14924814284625465416342314314654234 JUNIO 21 DE 2024.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Junio 21, 2024 at 13:15:12
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	635FCA54115C9C3BF6F51CA84005E53E

SHA1:	2A1668BC978587C2F654BA971A45502D1EE63FB8
SHA256:	F19B23392F32DE8C242691B3F3E8B626037BC507D79612D6004628E98EEC7C74
SSDEEP:	98304:PkgX2/EB7ktV5Uh6kW+JrnyZaUlnK8VP0kTM+qnKK+tPlitaJJTvS:tkW

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\ACH REF NO 14924814284625465416342314314654234 JUNIO 21 DE 2024.exe"	"C:\Users\admin\AppData\Local\Temp\ACH REF NO 14924814284625465416342314314654234 JUNIO 21 DE 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