Diciembre 17 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan
Cuenta de correo del remitente:	ap@freshstartproduce.net
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:	NOTA TRANSACCIONAL DICIEMBRE 17 DE 2024.bat
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	December 17, 2024 at 16:08:26
MIME:	text/x-msdos-batch
Información del archivo:	DOS batch file, ASCII text, with CRLF line terminators
MD5:	B9DCB558520B7B747E58EA71581BDF09
SHA1:	76AB7E0B2C1DE4B0DCAD77B421C06AAAFDE4D1F1
SHA256:	2A1409E75FBD695BF6C0FD51F7E8E975443C5333A6BF36E36DD01081319E4D30

SSDEEP:	12:w7l7DnZbDmViuVM1t2shYHEAr7N2R2zHhophrKeR+m4DzoCJJKCDHe0/JKCcqpWX:w7BDnJDmIuVMPi7NcQhyrWxPKCD+6KCs

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\NOTA TRANSACCIONAL DICIEMBRE 17 DE 2024.bat" "	C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\NOTA TRANSACCIONAL DICIEMBRE 17 DE 2024.bat" "	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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