Septiembre 12 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.babar/androm
Cuenta de correo del remitente:	liliana.abogada93@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	


---------- Forwarded message ---------
De: **Claudia liliana espinosa ramirez** <liliana.abogada93@gmail.com>
Date: mié, 11 sept 2024 a las 9:05
Subject: ESTADO - PROCESO BANCARIO EMPRESARIAL EXITOSO VALIDAR
To:

BANCO BOGOTA EMPRESARIAL

FECHA: 11 DE SEPTIEMBRE DE 2024

Hemos procesado exitosamente LA TRANSACCIÓN BANCARIA realizada a BANCO BOGOTÁ y el dinero será transferido al banco.

Estado	APROBADA
Referencia	316859127976824348
Transacción #	1123399-1686912798-84381
Método de pago	PSE
Procesador	PSE - ACH Colombia

DESCARGAR EL ARCHIVO ADJUNTO ENVIADO EN ESTE CORREO DE LA TRANSACCIÓN BANCARIA PARA SU VALIDACIÓN

CLAVE PARA DESCARGAR EL ARCHIVO 3518

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:	ARCHIVO TRANSACCIONAL No 87654756347657898997654347658900.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Septiembre 12, 2024 at 16:04:49
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	CF0D816ACEC45F16397B4EBF0C32CAC7

SHA1:	A58750F37C6A88F89D1F5D2789811D24249480E0
SHA256:	AE2D51F8430D85F56521E2445D8B01E6413DDF1A24685AC5AA3CA84DDAABC425
SSDEEP:	98304:to5buM7ObddRqnasNOHNNJJDTbrsZqAALFjT+r2G1ybKsczzcnL8nzAYZHcgUOdd:q+W

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\ARCHIVO TRANSACCIONAL No 876547563476578989976543476589 00.exe"	"C:\Users\admin\AppData\Local\Temp\ARCHIVO TRANSACCIONAL No 876547563476578989976543476589 00.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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