Diciembre 23 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	downloader
Cuenta de correo del remitente:	andasupra@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ---------
De: **Andres David Suarez Prada** <andasupra@gmail.com>
Date: mar, 17 dic 2024 a las 15:52
Subject: Transacción APROBADA verificar diciembre 17 de 2024 - ref. IOlYYp_1676648075109_qh3d41ly86
To:

BANCOLOMBIA NOTIFICACIONES TRANSACCIONALES

Tu transacción fue APROBADA

Hemos procesado exitosamente la transacción bancaria a continuación la información detallada:

Estado	APROBADA
Referencia	IOlYYp_1676648075109_qh3d41ly86
Transacción #	184245-1676648180-91852
Monto	COP $******.00
Método de pago	Canales virtuales BANCOLOMBIA
Procesador	Bancolombia S.A.

VER AQUÍ O DESCARGUE EL ARCHIVO PDF ADJUNTO CON LA TRANSACCIÓN PARA LA VERIFICACIÓN BANCARIA

CLAVE PARA LA DESCARGA 9273

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:	TRANSACCION APROBADA PDF DICIEMBRE 17 DE 2024.ba
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	December 23, 2024 at 17:29:12

MIME:	text/x-msdos-batch
Información del archivo:	DOS batch file, ASCII text, with CRLF line terminators
MD5:	48BADE693DC1990D287BF481BF2C9B78
SHA1:	8A7C4AC1148F7E68A3AC56934CA641A6D3EA2A2A
SHA256:	3D4EA424C3999B9CD0670BB6AC21E897E57C9061AEB5B68781FB26DEC327D909
SSDEEP:	12:w73Pv7OzbDmViuVM1t2likVHEAr72OPwzHJSxfRHLjWeoJm4DzoCJUiJDHX//Uie:w73PzEDmIuVM6VF72OPqSV9mx5D3bFCl

Fuente. CSIRT Académico UNAD

Información de proceso

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