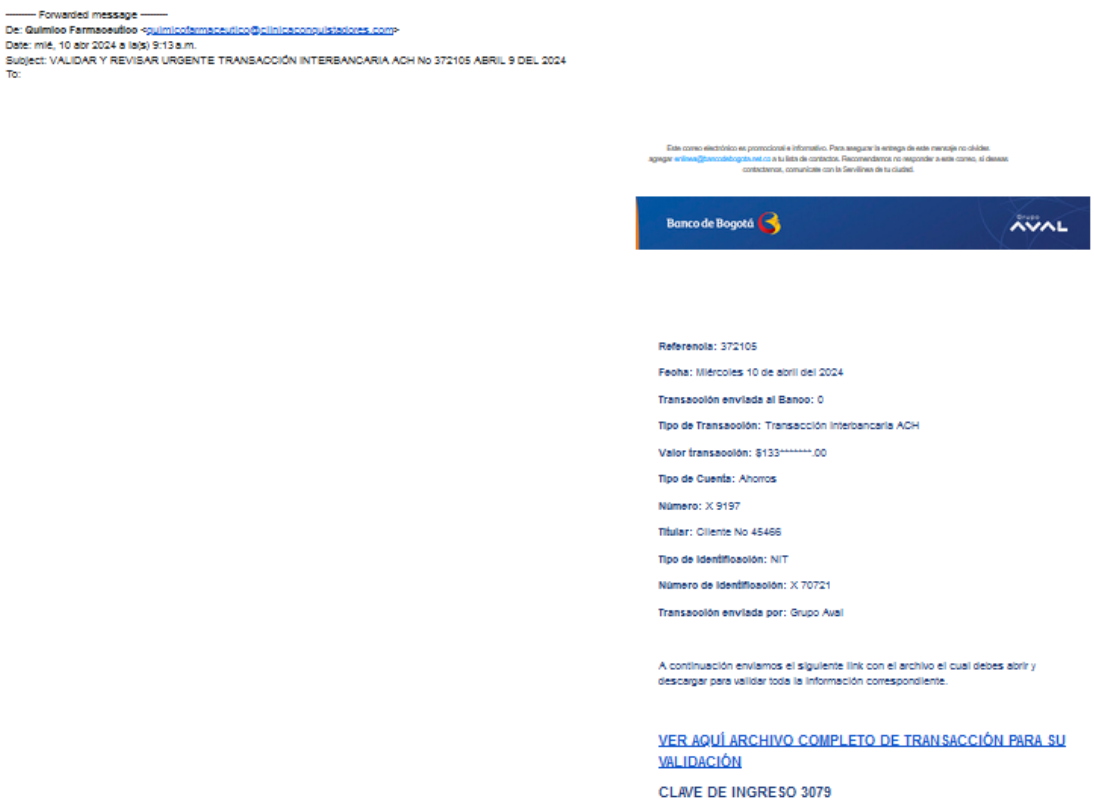
Abril 15 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.gvff
Cuenta de correo del remitente:	quimicofarmaceutico@clinicaconquistadores.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



—— Forwarded message ——
De: Quimico Farmaceutico <quimicofarmaceutico@clinicaconquistadores.com>
Date: mié, 10 abr 2024 a la(s) 9:13 a.m.
Subject: VALIDAR Y REVISAR URGENTE TRANSACCIÓN INTERBANCARIA ACH No 372105 ABRIL 9 DEL 2024
To:

Este correo electrónico es promocional e informativo. Para asegurar la entrega de este mensaje no olvides agregar enlinea@bancodebogota.net.co a tu lista de contactos. Recomendamos no responder a este correo, si deseas contactarnos, comunícate con la Sevillana de tu ciudad.

Banco de Bogotá — Grupo AVAL

Referencia: 372105
Fecha: Miércoles 10 de abril del 2024
Transacción enviada al Banco: 0
Tipo de Transacción: Transacción Interbancaria ACH
Valor transacción: $133*******.00
Tipo de Cuenta: Ahorros
Número: X 9197
Titular: Cliente No 45466
Tipo de Identificación: NIT
Número de Identificación: X 70721
Transacción enviada por: Grupo Aval

A continuación enviamos el siguiente link con el archivo el cual debes abrir y descargar para validar toda la información correspondiente.

VER AQUÍ ARCHIVO COMPLETO DE TRANSACCIÓN PARA SU VALIDACIÓN

CLAVE DE INGRESO 3079

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:	REF No 372105 REVI VALI ABRIL 9 DEL 2024.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	April 15, 2024 at 14:50:32
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	A971EE83FD5AB858FDF78C12A58CE10A
SHA1:	F93CA19E48410B0AB7FFD23B3797EAE54F3B8CC5
SHA256:	3EC3A0A4A46D34DA0867CFD2DD6C93C95134367C92E4A3274857415B79453919
SSDEEP:	98304:Hd8uCiMeVvg0eyFOTC+r0qYbFwmCdqOn602NGokrOiLD:CxN

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\REF No 372105 REVI VALI ABRIL 9 DEL 2024.exe"	"C:\Users\admin\AppData\Local\Temp\REF No 372105 REVI VALI ABRIL 9 DEL 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