Agosto 29 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	filerepmalware
Cuenta de correo del remitente:	ybecerra@acuavalle.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

——— Forwarded message ———
De: Yolanda Becerra Valdivia <[redacted]@acuavalle.gov.co>
Date: jue, 29 ago 2024 a las 11:19
Subject: FORMA DE PAGO REALIZADO - TRANSACCIÓN INTERBANCARIA ACH VALIDAR
To:

BANCO BOGOTÁ

FECHA: JUEVES 29 DE AGOSTO DE 2024

Apreciado(a) Cliente,

BANCO BOGOTÁ ha generado el siguiente documento.

Tipo de Documento: Factura de venta
Número: FE183454
Fecha Emision: 29/08/2024
Forma de Pago: Transaccion interbancaria
Valor: 25,*******.00

A continuación encuentra adjunto el documento electrónico generado el cual debe abrir y descargar para validar toda la información correspondiente.

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

CLAVE PARA DESCARGAR EL ARCHIVO 6057

Si tiene inquietud respecto a la información contenida en el documento electrónico, debe comunicarse con el emisor o proveedor del producto o servicio adquirido.

YOLANDA BECERRA VALDIVIA
Técnico Administrativo II
Dpto. Facturación, Recaudo y Cartera
Acuavalle S.A. E.S.P.
teléfono 6203400 ext 1222

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:	res_out.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Agosto 29, 2024 at 18:48:50
MIME:	application/x-dosexec

Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	D68F798B98CAE6CE17A1268202BC8E0F
SHA1:	7EE915CACFEA2A70A10208BDB041CE91E27C8EB9
SHA256:	DE89365DF6D33B6383513168A53D41F6BF34CB9FBA26595B5F459F4BE9D9414C
SSDEEP:	98304:boCAwM5hOIEktBE+yetNcRcCHJtm6CNozgGoy0HjErGZqUG2u5pXWsolOs8NoGuO:b+w

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\res_out.exe"	"C:\Users\admin\AppData\Local\Temp\res_out.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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