Mayo 14 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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

---------- Forwarded message ---------
De: **Contador Renta Bodegas Sas** <financierorbodegas@gmail.com>
Date: mié, 14 may 2025 a la(s) 10:23 a.m.
Subject: URGENTE EN MORA ESTADO DE CUENTA - CENTRAL DE ALIMENTOS LA PROVEEDORA 14 DE MAYO 2025
To:

Buen dia

De manera respetuosa solicito su colaboración a fin de obtener soporte de pago de la factura adjunta al presente correo, toda vez que la misma aún aparece en cartera sin pago.

Visualizar Factura
Clave: 1405

Agradezco su atención y quedo atento a sus comentarios

--

RENTA BODEGAS

NINI TATIANA GONZALEZ SALAS
CONTADORA
RENTA BODEGAS S.A.S. NIT. 900.748.905 - 6
Calle 136 No 53 - 25
Móvil: 316 752 2097
Email: financierorbodegas@gmail.com

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:	FACT_1405_2025_1111777_MNJHGDTTDB 1245154125126574456252250451 52.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 14, 2025 at 16:08:19
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
MD5:	ADCD695A86AD62ADF15A01E364145FD5
SHA1:	8A07D75BA93DE000F047825C5281E33B6652C17F

SHA256:	FBFAA29E332EE5E89DEA7F8EAADD6E271975C21D2D1AA41C9C9A8E533B6F2798
SSDEEP:	98304:G/9ADTpciOBuYuBnzGcxbgwQLpq8ly5SGkPKnzI8E9P8YyXrQtUX8HYTWG+JN1a2:mmr5tm

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache	C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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