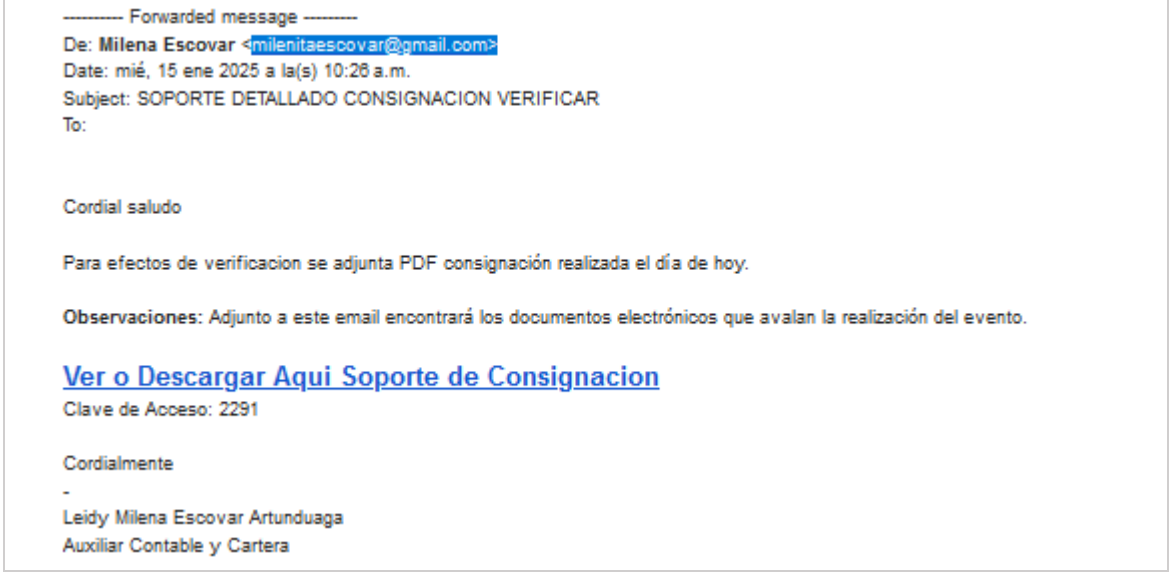
Enero 16 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Script:SNH-gen [Trj]
Cuenta de correo del remitente:	milenitaescovar@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Milena Escovar** <milenitaescovar@gmail.com>
Date: mié, 15 ene 2025 a la(s) 10:26 a.m.
Subject: SOPORTE DETALLADO CONSIGNACION VERIFICAR
To:

Cordial saludo

Para efectos de verificacion se adjunta PDF consignación realizada el día de hoy.

Observaciones: Adjunto a este email encontrará los documentos electrónicos que avalan la realización del evento.

Ver o Descargar Aqui Soporte de Consignacion
Clave de Acceso: 2291

Cordialmente
-
Leidy Milena Escovar Artunduaga
Auxiliar Contable y Cartera

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:	ConsignacionRef00005125198435811982615280051 28.js
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	January 16, 2025 at 14:15:25
MIME:	application/javascript
Información del archivo:	JavaScript source, Unicode text, UTF-8 text, with very long lines (440), with CRLF line terminators

MD5:	00A4BA139E436FACB9861B2AC35024FB
SHA1:	16396955FCB4BDF72D8F67FE37ED6C17A39BB9C2
SHA256:	9AE6DE36BE82DD3F67DAB2F0406030F65E72461702AE41E097D75925F4D468EC
SSDEEP:	1536:xyyVPkspf9s3r8MHps2DxE7EhpdH54HeI7YUnt44KnayzQ6VSYMLR5vUVtOvivcM:kyJksp9YVHVRutCzQ6V6L7uHGi

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Windows\System32\WScript.exe" C:\Users\admin\AppData\Local\Temp\ConsignacionRef0000512519843581198261528005128.js	"C:\Windows\System32\WScript.exe" C:\Users\admin\AppData\Local\Temp\ConsignacionRef0000512519843581198261528005128.js	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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