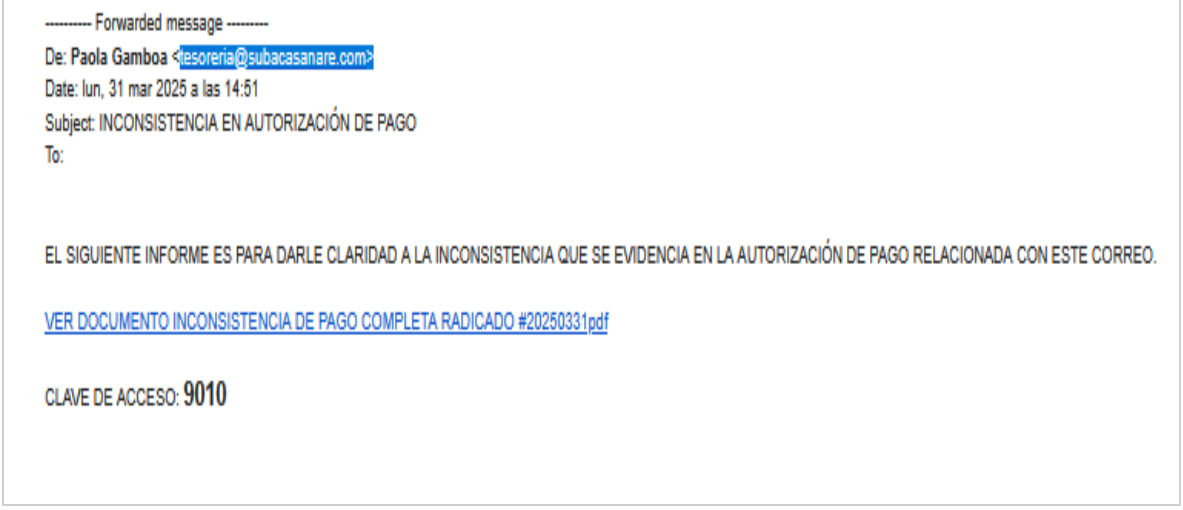
Marzo 31 de 2025

**COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING**

| | |
|---|---|
| **Técnica Mitre**: | Phishing |
| **Malware detectado**: | dropper.zbot |
| **Cuenta de correo del remitente:** | tesoreria@subacasanare.com |
| **TLP:** | **BLANCO** |
| **Registro grafico relacionado con el Phishing** | |



---------- Forwarded message ---------
De: **Paola Gamboa** <tesoreria@subacasanare.com>
Date: lun, 31 mar 2025 a las 14:51
Subject: INCONSISTENCIA EN AUTORIZACIÓN DE PAGO
To:

EL SIGUIENTE INFORME ES PARA DARLE CLARIDAD A LA INCONSISTENCIA QUE SE EVIDENCIA EN LA AUTORIZACIÓN DE PAGO RELACIONADA CON ESTE CORREO.

VER DOCUMENTO INCONSISTENCIA DE PAGO COMPLETA RADICADO #20250331pdf

CLAVE DE ACCESO: 9010

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:** | DOCUMENTO_COPIA_INCONSISTENCIA_EN_AUTORIZACION_DE_PAGO_RADICADO_20250331_ad89498418f4f481941c8a41f84fa18941489448f48a41894f41a654r454f545f1f45f45f654pdf.vbs |
| **Veredicto:** | **Actividad sospechosa** |
| **Fecha del análisis:** | April 01, 2025 at 12:06:33 |
| **MIME:** | text/plain |
| **Información del archivo:** | ASCII text, with very long lines (557), with CRLF line terminators |
| **MD5:** | 994824949C72C38B5BD55C0697A657C1 |

| | |
|---|---|
| **SHA1:** | 8970D4697DCD6C62E11A3FE47524574EA130AE6C |
| **SHA256:** | FB66632CD45196CC46DD75FFB02537E72772D6998F39743969BBAA1852362592 |
| **SSDEEP:** | 3072:rCpR5lE5i6wxEWHfh0z46CuxDhM3g1JgKv:ylE5i6mjHfngxOdKv |

Fuente. CSIRT Académico UNAD

**Información de proceso**

| CMD | Ruta Comprometida | Proceso Padre |
|---|---|---|
| "C:\WINDOWS\System32\OpenWith.exe" C:\Users\admin\AppData\Local\Temp\679ed67f-b6ae-4ebd-a7b6-01276766e964.vba | "C:\WINDOWS\System32\OpenWith.exe" C:\Users\admin\AppData\Local\Temp\679ed67f-b6ae-4ebd-a7b6-01276766e964.vba | explorer.exe |

Fuente. CSIRT Académico UNAD

Cordialmente

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