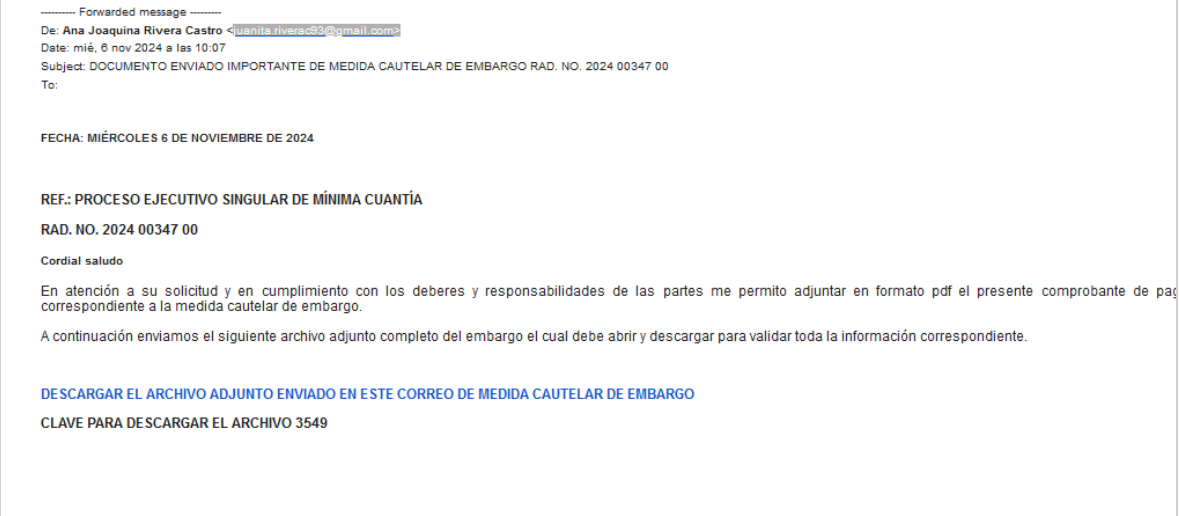
Noviembre 07 de 2024

## COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

| | |
|---|---|
| **Técnica Mitre**: | Phishing |
| **Malware detectado**: | Trojan.BAT.Obfus.aq |
| **Cuenta de correo del remitente:** | juanita.riverac93@gmail.com |
| **TLP:** | **BLANCO** |
| **Registro grafico relacionado con el Phishing** | |



---------- Forwarded message ---------
De: **Ana Joaquina Rivera Castro** <juanita.riverac93@gmail.com>
Date: mié, 6 nov 2024 a las 10:07
Subject: DOCUMENTO ENVIADO IMPORTANTE DE MEDIDA CAUTELAR DE EMBARGO RAD. NO. 2024 00347 00
To:

**FECHA: MIÉRCOLES 6 DE NOVIEMBRE DE 2024**

**REF.: PROCESO EJECUTIVO SINGULAR DE MÍNIMA CUANTÍA**

**RAD. NO. 2024 00347 00**

**Cordial saludo**

En atención a su solicitud y en cumplimiento con los deberes y responsabilidades de las partes me permito adjuntar en formato pdf el presente comprobante de pag
correspondiente a la medida cautelar de embargo.

A continuación enviamos el siguiente archivo adjunto completo del embargo el cual debe abrir y descargar para validar toda la información correspondiente.

DESCARGAR EL ARCHIVO ADJUNTO ENVIADO EN ESTE CORREO DE MEDIDA CAUTELAR DE EMBARGO

CLAVE PARA DESCARGAR EL ARCHIVO 3549

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 DE MEDIDA CAUTELAR DE EMBARGO RAD. NO. 2024 00347 00.bat |
| **Veredicto:** | **Actividad sospechosa** |
| **Fecha del análisis:** | November 07, 2024 at 15:33:52 |
| **MIME:** | text/plain |
| **Información del archivo:** | Unicode text, UTF-8 text, with very long lines (2718), with CRLF line terminators |
| **MD5:** | 24E3C5A8C5CE37EFB76A08A124A2F525 |
| **SHA1:** | 1378FA68873D9CE2368AAC281632FF5DAB2F59D0 |

| | |
|---|---|
| **SHA256:** | 233BCA3F0A5F3DBC98D3765ECC8631FD552366A78F052CC13C970B94A107E459 |
| **SSDEEP:** | 6144:vZuSzJTZolPPaVOZwrXQJ5RV5RFVVjRbVbJlv8:B |

Fuente. CSIRT Académico UNAD

**Información de proceso**

| CMD | Ruta Comprometida | Proceso Padre |
|---|---|---|
| C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\DOCUMENTO DE MEDIDA CAUTELAR DE EMBARGO RAD. NO. 2024 00347 00.bat" " | C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\DOCUMENTO DE MEDIDA CAUTELAR DE EMBARGO RAD. NO. 2024 00347 00.bat" " | explorer.exe |

Fuente. CSIRT Académico UNAD

Cordialmente

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