

## Boletín de Ciberseguridad

Marzo 12 de 2025

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

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Técnica Mitre:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Phishing                                                                                   |
| Malware detectado:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | trojan.marte/venomrat                                                                      |
| Cuenta de correo del remitente:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="mailto:comunicados@ramajuridicascitas.com">comunicados@ramajuridicascitas.com</a> |
| TLP:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | BLANCO                                                                                     |
| Registro grafico relacionado con el Phishing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                            |
| <p>Asunto: Notificación Judicial - Citación por Delitos de Abuso de Confianza y Falsedad de Documentos Públicos</p> <p>Estimado/a<br/>DEMANDADO.</p> <p>Le saludamos cordialmente desde el Poder Judicial de Colombia y le informamos que ha sido citado/a para comparecer ante el Juzgado Cuarto Penal Municipal del circuito departamental, en relación con el proceso judicial por los delitos de <b>Abuso de Confianza y Falsedad de Documentos Públicos</b>.</p> <p><b>Delitos Imputados y Legislación Relacionada:</b></p> <p><b>1. Abuso de Confianza:</b><br/>Conforme al Artículo 250 del Código Penal Colombiano, este delito se tipifica de la siguiente manera:<br/>"El que, aprovechándose de su cargo o de una relación de confianza, se apodere de bienes ajenos con ánimo de lucro, será sancionado con prisión de uno (1) a tres (3) años."</p> <p><b>2. Falsedad de Documentos Públicos:</b><br/>Según el Artículo 289 del Código Penal Colombiano:<br/>"El que falsifique un documento público con el propósito de obtener un beneficio ilícito, será sancionado con prisión de tres (3) a ocho (8) años y multa."</p> <p><b>Detalles de la Citación:</b><br/>Le solicitamos amablemente que asista a la audiencia programada para el día 29 de marzo del 2025 a las 9:30am. Su presencia es fundamental para el avance del proceso judicial.</p> <p><b>¿Cómo Consultar los Detalles?</b><br/>Para que pueda acceder a la información completa y descargar los documentos relacionados con este caso, por favor ingrese al portal web oficial:</p> <p><a href="#">Descargar y Consultar Citación - Portal Judicial</a><br/>Contraseña de acceso: <b>Tribunal2025</b></p> |                                                                                            |

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

## Boletín de Ciberseguridad

|                                 |                                                                            |
|---------------------------------|----------------------------------------------------------------------------|
| <b>Nombre del Archivo:</b>      | ACTA DE CITACION JUDICIAL-PDF.zip                                          |
| <b>Veredicto:</b>               | <b>Actividad sospechosa</b>                                                |
| <b>Fecha del análisis:</b>      | March 12, 2025 at 10:48:05                                                 |
| <b>MIME:</b>                    | application/vnd.microsoft.portable-executable                              |
| <b>Información del archivo:</b> | PE32+ executable (GUI) x86-64, for MS Windows, 6 sections                  |
| <b>MD5:</b>                     | 15313d47cc75b3a33926d771f47da6a4                                           |
| <b>SHA1:</b>                    | 34a021bf8d0f4fe8484afd3ff0832636801be4d9                                   |
| <b>SHA256:</b>                  | 6dff4a4db732b0586f0434733709ef346f2caa0568415d5f71f88ded5bf7d64f           |
| <b>SSDEEP:</b>                  | 98304:voWb27v17i4yln3sHFt2z6f8nYFBLy9CsXYXyQ5rai:vz2VdylcD2q8Y7eCuyyU<br>Z |

Fuente. CSIRT Académico UNAD

### Información de proceso

| CMD                                                   | Ruta Comprometida                                     | Proceso Padre |
|-------------------------------------------------------|-------------------------------------------------------|---------------|
| "C:\Users\<USER>\AppData\Local\Temp\1DO<br>C-PDF.exe" | "C:\Users\<USER>\AppData\Local\Temp\1DO<br>C-PDF.exe" | explorer.exe  |

Fuente. CSIRT Académico UNAD

Cordialmente

### CSIRT Académico UNAD

Correo electrónico: [csirt@unad.edu.co](mailto:csirt@unad.edu.co)

(+57 1) 344 37 00 Ext. 1042516