

## Boletín de Ciberseguridad

Junio 25 de 2024

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

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                            |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|-----------------|------------------------------------------------------------|------------------------|----------|---------------------------|-----------------|-------------------------------|------------|---------------------------------|------------|--------------------|---------------|
| <b>Técnica Mitre:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Phishing                                                   |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>Malware detectado:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Trojan.Loader                                              |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>Cuenta de correo del remitente:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | cosegarsas@gmail.com                                       |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>TLP:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | BLANCO                                                     |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>Registro grafico relacionado con el Phishing</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                            |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <p>----- Forwarded message -----<br/> De: cosegar sas &lt;cosegarsas@gmail.com&gt;<br/> Date: lun, 24 jun 2024 a la(s) 9:38 a.m.<br/> Subject: NOTIFICACIÓN DE TRANSACCIONES APROBADAS VALIDAR INFORMACIÓN ENVIADA URGENTE JUNIO 24 DE 2024<br/> To:</p> <div>  <p>Notificación de transacciones</p> <p>Hola,</p> <p>Usted ha recibido una notificación correspondiente a una transacción realizada a través de la Sucursal Virtual Personas de Bancolombia.</p> <p>La información relacionada con esta transacción es:</p> <table> <tr> <td><b>Detalle:</b></td><td>Transferencia por Sucursal Virtual Personas desde ****3-57</td></tr> <tr> <td><b>Cuenta destino:</b></td><td>****0-15</td></tr> <tr> <td><b>Valor transferido:</b></td><td>\$ 200,*****.00</td></tr> <tr> <td><b>Número de comprobante:</b></td><td>0000001228</td></tr> <tr> <td><b>Fecha de la transacción:</b></td><td>2024/06/24</td></tr> <tr> <td><b>Comentario:</b></td><td>transferencia</td></tr> </table> <p><a href="#">PARA VER EL ARCHIVO COMPLETO Y APROBAR TRANSACCIÓN DESCARGAR AQUI</a></p> <p>CLAVE DE INGRESO 4433</p> </div> |                                                            | <b>Detalle:</b> | Transferencia por Sucursal Virtual Personas desde ****3-57 | <b>Cuenta destino:</b> | ****0-15 | <b>Valor transferido:</b> | \$ 200,*****.00 | <b>Número de comprobante:</b> | 0000001228 | <b>Fecha de la transacción:</b> | 2024/06/24 | <b>Comentario:</b> | transferencia |
| <b>Detalle:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Transferencia por Sucursal Virtual Personas desde ****3-57 |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>Cuenta destino:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ****0-15                                                   |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>Valor transferido:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | \$ 200,*****.00                                            |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>Número de comprobante:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 0000001228                                                 |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>Fecha de la transacción:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2024/06/24                                                 |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |
| <b>Comentario:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | transferencia                                              |                 |                                                            |                        |          |                           |                 |                               |            |                                 |            |                    |               |

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

|                            |                                                            |
|----------------------------|------------------------------------------------------------|
| <b>Nombre del Archivo:</b> | PDF NO 198648468468468462462464621464 JUNIO 24 DE 2024.exe |
| <b>Veredicto:</b>          | Actividad sospechosa                                       |
| <b>Fecha del análisis:</b> | Junio 25, 2024 at 10:57:10                                 |

## Boletín de Ciberseguridad

|                                 |                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------|
| <b>MIME:</b>                    | application/x-dosexec                                                                              |
| <b>Información del archivo:</b> | PE32 executable (GUI) Intel 80386, for MS Windows                                                  |
| <b>MD5:</b>                     | E22C450B39F481D8E4F0C76F7171FA8C                                                                   |
| <b>SHA1:</b>                    | 15A66834DA4F65F8AB1BFDFE67F8D4EC629B9F47                                                           |
| <b>SHA256:</b>                  | A767D54CF6D67C873068C3BB7922A315BB7D172154E19195F59D87DADF37C109                                   |
| <b>SSDEEP:</b>                  | 98304:tD05tX1z7HI+eJw0b+gN7JsJJo/JYs8LWxmIlZBXA/ANA4DCOJPonx3flAracvw<br>T:M/xmoBXA4N5IPonx3flOX+B |

Fuente. CSIRT Académico UNAD

### Información de proceso

| CMD                                                                                                  | Ruta Comprometida                                                                                    | Proceso Padre |
|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|---------------|
| "C:\Users\admin\AppData\Local\Temp\PDF NO<br>198648468468468462462464621464<br>JUNIO 24 DE 2024.exe" | "C:\Users\admin\AppData\Local\Temp\PDF NO<br>198648468468468462462464621464<br>JUNIO 24 DE 2024.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