




## Boletín de Ciberseguridad

Diciembre 27 de 2024

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

<b>Técnica Mitre:</b>	<a href="#">Phishing</a>
<b>Malware detectado:</b>	<a href="#">trojan.msil/ratx</a>
<b>Cuenta de correo del remitente:</b>	<a href="mailto:referenciahes@gmail.com">referenciahes@gmail.com</a>
<b>TLP:</b>	<b>BLANCO</b>
<b>Registro grafico relacionado con el Phishing</b>	
	

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>	VISUALIZAR PROCESO POR NEGLIGENCIA MEDICA CON RADICADO 20015-50-75341-2024-02712-00; 891200952-82; ESE HOSPITAL EDUARDO SANTOS - LA UNION NARIÑO.exe
<b>Veredicto:</b>	<b>Actividad sospechosa</b>
<b>Fecha del análisis:</b>	December 27, 2024 at 17:28:49
<b>MIME:</b>	application/vnd.microsoft.portable-executable
<b>Información del archivo:</b>	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
<b>MD5:</b>	D6E2D07244A6748C5F45E64F7C8C95B5



## Boletín de Ciberseguridad

<b>SHA1:</b>	F961CC6C1E58E82CC18E7A3347C5DFC247345F0D
<b>SHA256:</b>	A3E7B5ECC6FF323AC3E57197CD82AA0CC8FFA07ABF3488A804E29C2725E696E0
<b>SSDEEP:</b>	98304:O8cvWUuBJqqLb4F6wrC4vY4PHep1s9gmcFDwnVxXqfoUNZTN7:O

Fuente. CSIRT Académico UNAD

### Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\459413 96-6ada-4d0d-8ed6-14133cebe146.exe"	"C:\Users\admin\AppData\Local\Temp\459413 96-6ada-4d0d-8ed6-14133cebe146.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