## Boletín de Ciberseguridad

Agosto 26 de 2024

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

Técnica Mitre:	Phishing		
Malware detectado:	trojan.remcos/gmgg		
Cuenta de correo del remitente:	rrhh@esehospitallocal.gov.co		
TLP:	BLANCO		
Registro graf	fico relacionado con el Phishing		
Personal Humany Ett Hought Look 4-1-111  De Reporte Humany Ett Hought Look 4-1-111  De las 15, 15, 15, 15, 15, 15, 15, 15, 15, 15,			
PECHL 34 DE ADDITIO DE BIDA			
Cordial saluto			
Se comunica que dentro del proceso ORDINARIO LABORAL DE PRIMERA INSTANCIA con redicado ADOSTO DE 2024, HECIÁNDO A LAS NUEVE DE LA MAÑAM (\$10 A.M) misma que se replicará de	3931-40393 quide umades son paties o apoderados, se 1jú como fecha para fevar a cabo las diligencias del aní culo TT del CPTG3 el dia LUMES, (35) DE manero virtual a travia del enlace de la plateforma TEARS.		
Se suinita corredidamente a los apoderados policiales responsabilizares de la asistencia unha a autobarea administración con protección la imporbibilizar de compantam	al de sus producteres y testigni o tersena si tay lugar y efica, quienes debedin contar con un equipo que tenga blimana, micolitono y partentes		
DESCARGAR EL ARCHIVO ENVADO EN ESTE CORREO DEL PROCESO ORDINARIO LABORAL	DE PRIMERA INSTRUCIA		
CLINE PARK DESCARGAR EL ARCHIVO ADJUNIO 1008			
* Para acceder a la audiencia por favor copiar y pirpar al anlate de la audiencia es al naserpa	dor de forma situate y en metaria da molypolis caso de Sadas hame uno de los instructivos.		
Andream Hermin Angly (170 Int. 1821 An American Angle			

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:	out_sig.exe
Veredicto:	Actividad sospechosa
Fecha del análisis:	Agosto 26, 2024 at 11:01:50
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	A2F672A48F20F69A981C24C4AC9F7A34

# Boletín de Ciberseguridad

**SHA1**: 2AFC0F87C56665A55CA318C795E7035C1A525C9E

**SHA256**: 4DF31CAB3C799C3713A6B86B1F5E114DA9D67DEE6BB5A35E2B125367417C8246

SSDEEP: 49152:1m73Dky/w3fFDvpNySSRE21/oN0Q9znDpSgEylDgu+oY:o73WvVxNsB1QNLDEyVEoY

Fuente. CSIRT Académico UNAD

## Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\out	"C:\Users\admin\AppData\Local\Temp\out	explorer.exe
_sig.exe"	_sig.exe"	

Fuente. CSIRT Académico UNAD

Cordialmente

### **CSIRT Académico UNAD**

Correo electrónico: <a href="mailto:csirt@unad.edu.co">csirt@unad.edu.co</a> (+57 1) 344 37 00 Ext. 1042516