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 grafico relacionado con el Phishing	

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

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 _sig.exe"	"C:\Users\admin\AppData\Local\Temp\out _sig.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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