Boletín de Ciberseguridad

Agosto 29 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing		
Malware detectado:	trojan.gen3/remcos		
Cuenta de correo del remitente:	ruizwendy25.28@gmail.com		
TLP:	BLANCO		
Registro grafico relacionado con el Phishing			
Trinsted Heaville On White Mark Committee Trinsted Com Not to the Open Committee Trinsted Com Not to the Open Com Aske St. 17 ale Sample ACLARCION ACRICAL ON PROJECTS To			
DESCRIPTION AND ADDRESS OF A STATE AND ADDRESS OF A STATE ADDRESS OF A			
Machine little delicated: The electrical little is a tombook to top the electrical delication are represented and an appropriate and appropria			
DESCRIBURA MARGOS PER COM REPUBBLICADA DE DESCRIBO. COCINDO DE ACCESSO, DESA			
**CONFICENCIAL - UNIVERSIDAD NACIONAL ASSESSA VA DISTANCIA (NAVA): La información continuos de unite incomina in continuos de unite incomina de continuo de unite incomina de continuo de			
Coultry in The provide a million information. Coloff Assistance (MAC)			
(i) (=PP () total (F int Eye, 1640))) (introducing National (Author)) (All (Author))			
CONCRETED TO THE STREET OF STREET OF STREET AND STREET OF STREET O	n orderen y all park no allies for a person organisation is usual right. If other is a length without particle contact which attraction can always and the interest contact of the contact		
Territins adjunts: Analizatis per Smid S)	gl.		

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:	ACUSACIÓN JUDICIAL EN PROCESO.exe
Veredicto:	Actividad sospechosa
Fecha del análisis:	Agosto 29, 2024 at 19:56:16
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	DE7501B72C10BD5D7DB619F83F3543EB

Boletín de Ciberseguridad

 SHA1:
 81FA72784EEA2CDF026D78CBF93B4A0C910E776E

 SHA256:
 B6F488A9F6BA3A28BA0A0A3D23DB66A372B61AC8CD2CCD3AC7430FFA9611FAC6

 SSDEEP:
 98304:cAAgraWCHFhA4UMw7HOVpEFyGE4Gy0ABo1Qvc4klbib1J0CfhHxT9h7jbnhgMjNL:HIq

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\AC	"C:\Users\admin\AppData\Local\Temp\AC	explorer.exe
USACIÓN JUDICIAL EN PROCESO.exe"	USACIÓN JUDICIAL EN PROCESO.exe"	

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

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