Boletín de Ciberseguridad

Agosto 26 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing			
Malware detectado:	trojan.filerepmalware/remcos			
Cuenta de correo del remitente:	juridicoaguirred@gmail.com			
TLP:	BLANCO			
Registro grafico relacionado con el Phishing				
- Promoting manage De dies Appetre (III. III.				
DESARROLLO DE TRANSACCIÓN REALIZADA				
Has recibile una norficación correspondente a una transacción realizada a través de tuaseto por	al bancarie			
Nos. de listura (22				
fine, de referencia 3: Ut30:				
Fecha de la transacción: Lunes 25 de agosto de 2004				
Nos. de sampreduarde CCCIT				
DESCARGAR FOF EN L	A PARTE DE ABAJO DE DESARROLLO DE TRANSACCIÓN INTERBANCARIA			
	CLAPE DE ACCESO AL POP; 2912			
**CONFIDENCIAL - UNIVERSIDAD NACIONAL ADERTA Y A DISTANCIA (ANAD), La Adomición contemida en exis mentaja es confidencial y són pueda par unitada por la partiena o operacion o la sual este desego. El cated no es el recupirol accompany, cualquer relativiste, debativo, altantico de cual accompany and profitate y cual accompany por la Ear. El por tentr recibe asse mentaja. Nacion tentral y cuals y tentre al mentaja recibilista mentaja installa men				
	cón comercia en este merciaje sis confidencial y sós puede ser uclibada por la pustona a organización e la cual está dirigido. Si votad no en al dr y perá sanctinado por la Ley Si por artor nuclea este mentaja, favor neenvéals de usata y borre al mentaja recibido intendamentos.			
Yarchivo edjunto- Anetocki por Great ()				

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_sigexe
Veredicto:	Actividad sospechosa
Fecha del análisis:	Agosto 26, 2024 at 13:26:12
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	E26AF3F92E8F9E8082D660F31353F86D



Boletín de Ciberseguridad

SHA1:	D185030089248234C9E83AD9216B3B8F7890167A
SHA256:	CB8D0BA3CB1D8F9222E80075CBF88DD0500B557F68D8CDA57CE44258A1D2FD52
SSDEEP:	98304:j6Rb5gwTsPaKvVxNsB3elMvOGvhK5wlkkn768azxco:+kZ

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
_sigexe"	_sigexe"	

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

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