Boletín de Ciberseguridad

Julio 24 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing			
Malware detectado:	ado: Trojan:Win32/Sonbokli.A!cl			
Cuenta de correo del remitente:	addy.salazar@unad.edu.co			
TLP:	BLANCO			
Registro grafico relacionado con el Phishing				
— Forwarded message —	-			
De: Addy Patricia Salazar Jaime Gody salazar@unad.edu.co				
Date: mié, 24 jul 2004 a lejs) 3:19 p.m. Subject: ADMISIÓN TUTELA: RAD-9899082381-2004.				
Subject Administration to Jeda, AAU (1008)(1220) - 1224.				
Fordial saludo				
Cordial saludo,				
	dal, mediante providencia profetida el día de hoy. ADMITIÓ la Acción de Tutela de la referencia instaurada en contra de esa entidad; con el anta -petición-			
Por medio del presente me permito NOTIFICARLE que este Despacho Judio				
For medio del presente me permito NOTIFICARLE que este Despacho Judio propósito de que se ampare el derecho presuntamiente conculcado al accion VER DOCUMENTOS ADJUNTOS AQUI CLAVE DE ACCESO 1719	ante -petición-			
Por medio del presente me permito NOTIFICARLE que este Despacho Judio propósito de que se ampere el derecho presuntamente conculcado al accion VER DOCUMENTOS ADJUNTOS AQUI CLAVE DE ACCESO: 1719 POR DISPOSICIÓN DEL CONSEJO SUPERIOR DE LA JUDICATURA EN MATI	ibria. De retención documental se informa a los usuarios que los memoriales. Escritos, contestaciones de tutela yi			
For medio del presente me permito NOTIFICARLE que este Desparbo Judio propósito de que se ampare el derecho presuntamente conculcado al accion VER DOCUMENTOS ADJUNTOS AQUI CLAVE DE ACCESO. 1719 POR DISPOSICIÓN DEL CONSEJO SUPERIOR DE LA JUDICATURA EN MATO O SOLICITUDES ÚNICAMENTE SE RECIBIRÁN EN FORMATO PDE.	eria. De retención documental, se informa a los usuarios que los memoriales, escritos, contestaciones de tutela y:			
For medio del presente me permito NOTIFICARLE que este Desparbo Judio propósito de que se ampare el derecho presuntamente conculcado al accion VER DOCUMENTOS ADJUNTOS AGUI CLAVE DE ACCESO: 1718 POR DISPOSICIÓN DEL CONSEJO SUPERIOR DE LA JUDICATURA EN MATI O SOLICITUDES UNICAMENTE SE RECIBIRAN EN FORMATO POE. De no ser competente para concoer de la presente acción constitucional, info	eria. De retención documental, se informa a los usuarios que los memoriales, escritos, contestaciones de tutela y:			

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:	ADMISIÓN TUTELA. RAD5639002361-2024exe	
Veredicto:	Actividad sospechosa	
Fecha del análisis:	Julio 24, 2024 at 15:42:10	
MIME:	application/x-dosexec	
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows	

Boletín de Ciberseguridad

MD5:	08DE0922416FF5585C39B6203A743DC7	
SHA1:	312D60177DCFE3CDA5333429D44E782C2351DF16	
SHA256:	AEFA426BE947899E87899823B42DAB1649D52913FC377E8A12399F09ABD3F3E6	
SSDEEP:	98304:a+AwSFMB5CInmD8a0aeDv7X42TXdblKy7NRyVX19RsBVG2/5wttu16ebbg8t	
	Q.IW8-ZAnRherFaVTb.lrIF	

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\AD	"C:\Users\admin\AppData\Local\Temp\A	explorer.exe
MISIÓN TUTELA. RAD5639002361-	DMISIÓN TUTELA. RAD5639002361-	
2024exe"	2024exe"	

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

Correo electrónico: csirt@unad.edu.co

(+57 1) 344 37 00 Ext. 1042516