Agosto 15 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.mint/zard
Cuenta de correo del remitente:	mateconsadmonsaldana@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ---------
De: Mateconsadmonsaldana <mateconsadmonsaldana@gmail.com>
Date: mié, 14 ago 2024 a las) 8:57 a.m.
Subject: NOTIFICACIÓN AUDIENCIA DE CONCILIACIÓN; RADICADO:83791400T2-2024
To:

Cordial saludo.

Por medio del presente, relaciono la invitación a la audiencia programada mediante Auto de 14/08/2024. Se les recuerda a los apoderados que deben hacer comparecer a la presente audiencia a sus poderdantes, testigos y auxiliares de la justicia, enviándoles el link adjunto.

Para verificar la lectura de los anexos a este correo por favor haga CLICK en el documento para descargarlo, ingresa la clave de acceso: 2970

De la misma manera para el buen desarrollo de la presente audiencia deben tener buena conectividad. La reunión será iniciada 15 minutos antes para hacer las pruebas de los medios tecnológicos que se utilizaran.

Atentamente,

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:	NOTIFICACION AUDIENCIA DE CONCILIACION; RADICADO8379140072-2024..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Agosto 15, 2024 at 08:31:26
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	DDA582996531269B425AC27D419C23FA

SHA1:	A425273D901F582270D634C110D30E9015AC5081
SHA256:	BDDC9C0E9743073C1580664512E8A5E9DC63515E451DB089889E9566CFF21355
SSDEEP:	98304:ss0nyxFc52l1Q3q63Qi6hbk6ChZlppvIVfLdB4Ys6Le9oIx6EBqiRBRIcHtYQzxl:0lQPD

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\NOTIFICACION AUDIENCIA DE CONCILIACION; RADICADO8379140072-2024..exe"	"C:\Users\admin\AppData\Local\Temp\NOTIFICACION AUDIENCIA DE CONCILIACION; RADICADO8379140072-2024..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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