Agosto 30 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.dcrat/filerepmalware
Cuenta de correo del remitente:	claus3d.diseno@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ----------
De: CLAUS DISEÑO <claus3d.diseno@gmail.com>
Date: vie, 30 ago 2024 a la(s) 10:56 a.m.
Subject: Casillero Jurídico, Notificación Fiscal Conciliación Obligatoria (Proceso Legal N° 55534709355938945
To:

JUZGADO PENAL Y DE GARANTÍAS

Estimado(a)

REMISORIO DE CITACIÓN

De manera atenta me permito adjuntar el Oficio No 00989873-24 del 30 de agosto de 2024, para el conocimiento de la medida cautelar decretada al interior del proceso de la referencia.

Se le advierte que el oficio deberá ser radicado por usted ante las entidades correspondientes e igualmente deberá indicarle a la entidad que cualquier manifestación puede ser enviada.

Así mismo, le adjunto el documento para la consulta al expediente digital.

894623586432487238947328432l-232-32

CONTRASEÑA DEL DOCUMENTO: 2024

Casillero Judicial No: 423986421-17

Att: Claus Matos Piñeros.

Abogado y Asesor Fiscal.

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:	Caso_Fiscal_Desarrollado_N#56789098765..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Agosto 30, 2024 at 16:15:16
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	AC2ED62743FBA8C2D5F6C96B5B1D4966

SHA1:	78F55DD52550B264ACE72673498FB870DC7AB7EF
SHA256:	2B64E4DC2F51830BD3269086538FE05E54A5C08C0E89B35F1C201019A4CDBBF3
SSDEEP:	49152:uMDkQ51ms7iQQAPpAuAPpAQoTbwYFBBMn:VkAiQ

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Caso_Fiscal_Desarrollado_N#56789098765..exe"	"C:\Users\admin\AppData\Local\Temp\Caso_Fiscal_Desarrollado_N#56789098765..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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