Septiembre 13 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Trojan.TR/Dropper.Gen
Cuenta de correo del remitente:	andreskatzenstein@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ---------
De: D katzenstein <andreskatzenstein@gmail.com>
Date: vie, 13 de sept de 2024, 10:53 a. m.
Subject: NOTIFICACION SENTENCIA TUTELA SEGUNDA INSTANCIA RAD; 2024-00211
To:

Cordial saludo,

En documento adjunto, el Juzgado Veinte Penal del Circuito con Funciones de Conocimiento, notifica decisión proferida dentro de la acción de tutela bajo radicado 2024-00211, emitida en segunda instancia.

En la parte inferior encontrara documento XML con la informacion detallada y escrito de tutela.

El Documento a visualizar cuenta con clave de acceso: (1159)

Por favor acusar recibido,

Cordialmente,

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

AVISO DE CONFIDENCIALIDAD: Este correo electrónico contiene información de la Rama Judicial de Colombia. Si no es el destinatario de este correo y lo recibió por error comuníquelo de inmediato, respondiendo al remitente y eliminando cualquier copia que pueda tener del mismo. Si no es el destinatario, no podrá usar su contenido, de hacerlo podría tener consecuencias legales como las contenidas en la Ley 1273 del 5 de enero de 2009 y todas las que le apliquen. Si es el destinatario, le corresponde mantener reserva en general sobre la información de este mensaje, sus documentos y/o archivos adjuntos, a no ser que exista una autorización explícita. Antes de imprimir este correo, considere si es realmente necesario hacerlo, recuerde que puede guardarlo como un archivo digital.

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:	OfxSENTENC1ATUTELARADICAD0202400211.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Septiembre 13, 2024 at 11:28:54
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	0BE22EC6371B90546836CAA3B3990DBD

SHA1:	024A3E12C248CB1912BFCD6CBF0D8E5EED1E77E8
SHA256:	586E3716114E7AD01D36785D3560C2C0FF95E79D123298A027DE9A92B45A0AF0
SSDEEP:	49152:Ui4mAEDXSW4wa6DDRhZn/QBlf/jmPNIS3OyWfsjBZ1uXQ+PF0fvnGkqmMeLnZNLb:1AaCwa6DXROynFZ1uMvnGGjLApvicpC

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\OfxSENTENC1ATUTELARADICAD0202400211.exe"	"C:\Users\admin\AppData\Local\Temp\OfxSENTENC1ATUTELARADICAD0202400211.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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