Noviembre 13 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	downloader.msil/ratx
Cuenta de correo del remitente:	carlosagudelo2@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

-------- Forwarded message --------
De: **Carlos Andres Agudelo serna** <carlosagudelo2@gmail.com>
Date: mar, 12 de nov de 2024, 12:09 p. m.
Subject: AUTO CONCEDE IMPUGNACIÓN TUTELA RAD.2024-00178.
To:

Cordial Saludo,

A continuación este Despacho Judicial, les notifica que con auto de fecha 12 de noviembre de 2024, se concedió el recurso de impugnación al fallo de tutela emitido en la radicación del asunto. Anexo auto en formato PDI

El siguiente documento cuenta Clave de acceso: 1719

República de Colombia
Rama Judicial del Poder Público

JUZGADO TERCERO PENAL MUNICIPAL
CON FUNCIÓN DE CONTROL DE GARANTÍAS

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:	AUTO CONCEDE IMPUGNACIÓN TUTELA RAD.2024-00178..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	November 13, 2024 at 08:58:35
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
MD5:	CE6B3FC4341079072CFC988323A24FF4
SHA1:	C29B78BE1F60D424AA86F6E82F79CAFC701DAFF2
SHA256:	EC37EE5F6B5D6FFA748775C70F3C3519DDCD4BBF7971F20FA97565A9593C8D0D

SSDEEP:	98304:g0Bzycsd8a/3odfCTW9kDNftSLKujcMIDZ62qCxLD6bovMgALooap0zcKtvqpjec:scnH

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\AUTO CONCEDE IMPUGNACIÓN TUTELA RAD.2024-00178..exe"	"C:\Users\admin\AppData\Local\Temp\AUTO CONCEDE IMPUGNACIÓN TUTELA RAD.2024-00178..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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