Mayo 16 de 2025

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.penguish/asyncrat
Cuenta de correo del remitente:	rochakaren937@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

---------- Forwarded message ---------
De: **Karen Rocha** <rochakaren937@gmail.com>
Date: jue, 15 may 2025 a las 14:57
Subject: RADICADO ; 12204368910329-2024; EMITO FALLO DE TUTELA
To:

Cordial saludo;

De conformidad con lo normado en el artículo 15 del Decreto 2760 de 1992, en concordancia con el artículo 291 numeral 2 y el artículo 612 del C.G. del Proceso, en cumplimiento de lo ordenado por el Juzgado Primero Penal Municipal Para Adolescentes con Función de Control de Garantías, por medio de la presente me permito ***NOTIFICARLE EN FORMA PERSONAL FALLO DE TUTELA DEL 15 de MAYO del 2025 ,*** con el cual se ***DECLARA IMPROCEDENTE EL AMPARO SOLICITADO EN LA ACCIÓN Y SE DICTAN OTRAS DISPOSICIONES*** dentro del trámite del proceso.

Con tal propósito, adjunto copia del precitado proveído el cual podrá observar al final de este correo el cual tiene como clave de acceso : **1505**

Atentamente,

ELSA RUTH HERNÁNDEZ PINEDA
SECRETARIA

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

ART.20 LEY 527 DE 1999; ART. 191 Y 612 C.G.P.; ART. 56 Y 57 CPACA.
CRA. 9 Nº 14B-61 TUNJA
TELÉFONO (098) 7438984; FAX. (098) 7438997.
Email. j01prmpaladtun@cendoj.ramajudicial.gov.co

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:	15-05-2025_FACT_125448725212556993332655552.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	May 16, 2025 at 17:57:44
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
MD5:	DCC9A4B03E126F3205E8596D4F93B4F3
SHA1:	A4FC99BD5DAFAFB8CDA5DA51D1694E2409C209DD

SHA256:	486E05B780FAD9B2281A1923F8653E0C725D2FC304894CD6E9DD5BF3ECCD705F
SSDEEP:	98304:G/9ADTpciOSTmWh5s78aXq7ltAIGYdnIEGrpfcaqJRQ5GU/KqXCJjQKL7sPG4mXT:5d5QnoCbk

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\{49D63430-1EFA-4E66-A54F-751AB9022FE1}\.cr\15-05-2025_FACT_12544872521255699333265552.exe" -burn.clean.room="C:\Users\admin\AppData\Local\Temp\15-05-2025_FACT_12544872521255699333265552.exe" -burn.filehandle.attached=676 -burn.filehandle.self=732	"C:\Users\admin\AppData\Local\Temp\{49D63430-1EFA-4E66-A54F-751AB9022FE1}\.cr\15-05-2025_FACT_12544872521255699333265552.exe" -burn.clean.room="C:\Users\admin\AppData\Local\Temp\15-05-2025_FACT_12544872521255699333265552.exe" -burn.filehandle.attached=676 -burn.filehandle.self=732	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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