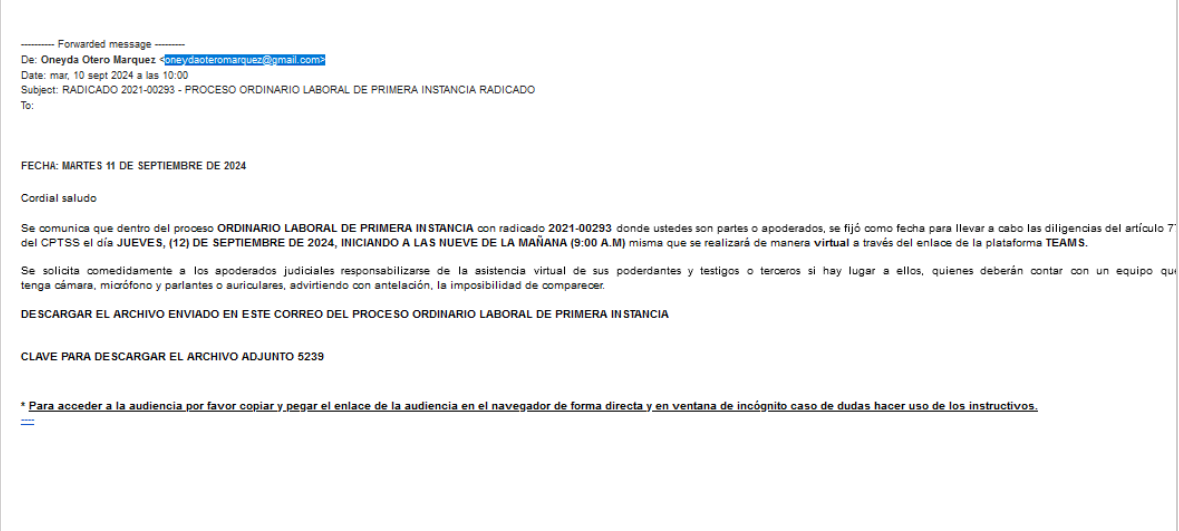
Septiembre 10 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Trojan.Injector!1.FCCE (CLASSIC)
Cuenta de correo del remitente:	oneydaoteromarquez@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



---------- Forwarded message ---------
De: **Oneyda Otero Marquez** <oneydaoteromarquez@gmail.com>
Date: mar, 10 sept 2024 a las 10:00
Subject: RADICADO 2021-00293 - PROCESO ORDINARIO LABORAL DE PRIMERA INSTANCIA RADICADO
To:

FECHA: MARTES 11 DE SEPTIEMBRE DE 2024

Cordial saludo

Se comunica que dentro del proceso **ORDINARIO LABORAL DE PRIMERA INSTANCIA** con radicado **2021-00293** donde ustedes son partes o apoderados, se fijó como fecha para llevar a cabo las diligencias del artículo 7
del CPTSS el día **JUEVES, (12) DE SEPTIEMBRE DE 2024, INICIANDO A LAS NUEVE DE LA MAÑANA (9:00 A.M)** misma que se realizará de manera **virtual** a través del enlace de la plataforma **TEAMS.**

Se solicita comedidamente a los apoderados judiciales responsabilizarse de la asistencia virtual de sus poderdantes y testigos o terceros si hay lugar a ellos, quienes deberán contar con un equipo qu
tenga cámara, micrófono y parlantes o auriculares, advirtiendo con antelación, la imposibilidad de comparecer.

DESCARGAR EL ARCHIVO ENVIADO EN ESTE CORREO DEL PROCESO ORDINARIO LABORAL DE PRIMERA INSTANCIA

CLAVE PARA DESCARGAR EL ARCHIVO ADJUNTO 5239

* **Para acceder a la audiencia por favor copiar y pegar el enlace de la audiencia en el navegador de forma directa y en ventana de incógnito caso de dudas hacer uso de los instructivos.**

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:	RADICADO 2021-00293 - PROCESO ORDINARIO LABORAL DE PRIMERA INSTANCIA RADICADO.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Septiembre 10, 2024 at 15:11:52
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows

MD5:	A6285E774EDDB0B80F584B73C331D77D
SHA1:	3BC57F5177FE257743310C8298C3D4159FDA85E8
SHA256:	0E995312276107AB21BE64E93A25616EF54832B3FC45E3478099023E3B10017C
SSDEEP:	98304:YvpBdWdmdADDdc7ds1gqz51aZGCrW/CeUpMkwVcqXIGOq6L3t/C5o24MDX7xNTH1:ve

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\RADICADO 2021-00293 - PROCESO ORDINARIO LABORAL DE PRIMERA INSTANCIA RADICADO.exe"	"C:\Users\admin\AppData\Local\Temp\RADICADO 2021-00293 - PROCESO ORDINARIO LABORAL DE PRIMERA INSTANCIA RADICADO.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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