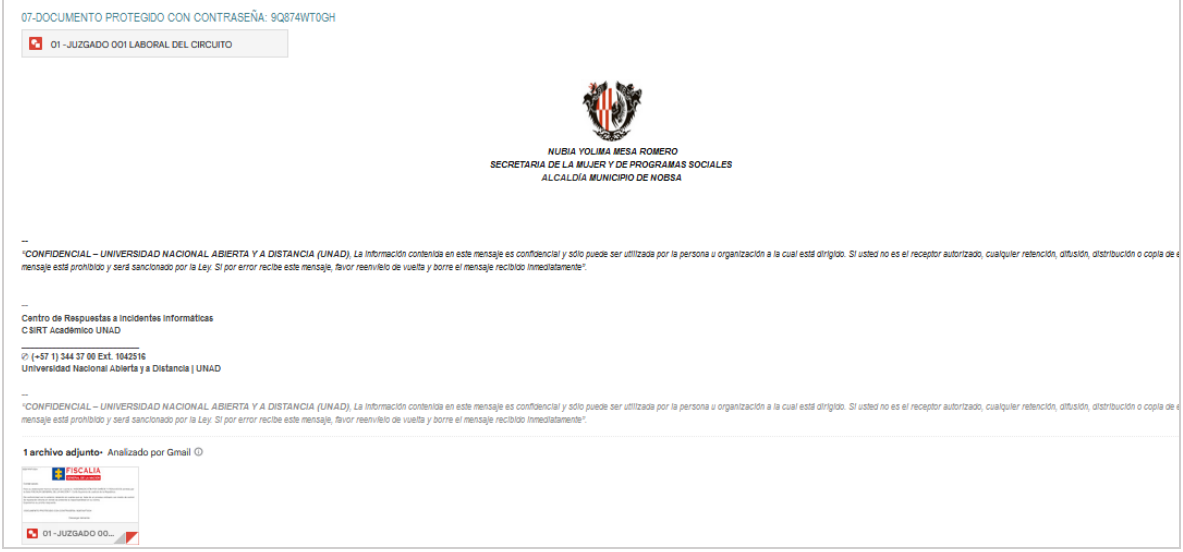
Abril 18 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Program.Unwanted.5065
Cuenta de correo del remitente:	gestionsocial@nobsa-boyaca.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	



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:	01 DEMANDA LABORAL.EXE
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	April 18, 2024 at 17:20:45
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	A2D70FBAB5181A509369D96B682FC641
SHA1:	22AFCDC180400C4D2B9E5A6DB2B8A26BFF54DD38

SHA256:	3EC3A0A4A46D34DA0867CFD2DD6C93C95134367C92E4A3274857415B79453919
SSDEEP:	8AED681AD8D660257C10D2F0E85AE673184055A341901643F27AFC38E5EF8473

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\01 DEMANDA LABORAL.exe"	"C:\Users\admin\AppData\Local\Temp\01 DEMANDA LABORAL.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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