Septiembre 23 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.jalapeno/msil
Cuenta de correo del remitente:	osselynequennlove2003abc@gmail.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	


---------- Forwarded message ---------
De: **Jossly Herrera** <osselynequennlove2003abc@gmail.com>
Date: vie, 20 sept 2024 a la(s) 10:11 a.m.
Subject: Fwd: Aviso de Prejuicio - PDF PROTEGIDO CLAVE 20240920
To:

Fecha: 20/09/2024
A: Jossly Herrera

Estimado/a Jossly,

Le recordamos que la factura No. 0515163512005611 se encuentra pendiente de pago. Le solicitamos que realice el pago a la brevedad posible para evitar cargos adicionales.

PDF PROTEGIDO CLAVE 20240920

1 archivo adjunto · Analizado por Gmail

Le recordamos q...

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:	Le recordamos que la factura No. 0515163512005611 se encuentra pendiente de pago. Le solicitamos que realice el pago a la brevedad posible para evitar cargos adicionales..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Septiembre 23, 2024 at 13:44:48

MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:	0F364EF71328910F527720C59678BAF4
SHA1:	6A6B85F2D4B76E75C74E6E20AF0B378C7651A5B9
SHA256:	524DEAF97B5343E87F291FB7BEB74021230F049AA59927D4A2EEE19CE7521C74
SSDEEP:	3072:KoVfiCTmeo24aJ3MDgGVRLDqAm4ethIX5:KifBTloCNMDgLAbethI

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\d6c5bf04-58af-4aca-804c-cc121fd7b0d9.exe"	"C:\Users\admin\AppData\Local\Temp\d6c5bf04-58af-4aca-804c-cc121fd7b0d9.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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