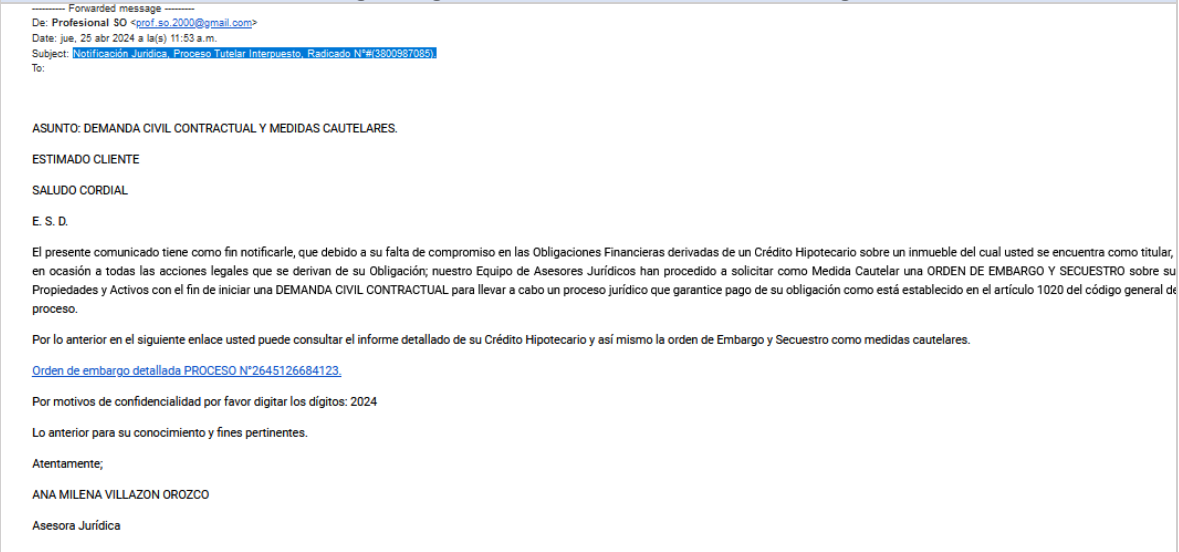
Abril 25 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	Trojan:Win32/Sonbokli.A!cl
Cuenta de correo del remitente:	prof.so.2000@gmail.com
TLP:	**BLANCO**

Registro grafico relacionado con el Phishing



---------- Forwarded message ---------
De: **Profesional SO** <prof.so.2000@gmail.com>
Date: jue, 25 abr 2024 a la(s) 11:53 a.m.
Subject: Notificación Juridica, Proceso Tutelar Interpuesto, Radicado N°#(3800987085).
To:

ASUNTO: DEMANDA CIVIL CONTRACTUAL Y MEDIDAS CAUTELARES.

ESTIMADO CLIENTE

SALUDO CORDIAL

E. S. D.

El presente comunicado tiene como fin notificarle, que debido a su falta de compromiso en las Obligaciones Financieras derivadas de un Crédito Hipotecario sobre un inmueble del cual usted se encuentra como titular, en ocasión a todas las acciones legales que se derivan de su Obligación; nuestro Equipo de Asesores Jurídicos han procedido a solicitar como Medida Cautelar una ORDEN DE EMBARGO Y SECUESTRO sobre su Propiedades y Activos con el fin de iniciar una DEMANDA CIVIL CONTRACTUAL para llevar a cabo un proceso jurídico que garantice pago de su obligación como está establecido en el artículo 1020 del código general de proceso.

Por lo anterior en el siguiente enlace usted puede consultar el informe detallado de su Crédito Hipotecario y así mismo la orden de Embargo y Secuestro como medidas cautelares.

Orden de embargo detallada PROCESO N°2645126684123.

Por motivos de confidencialidad por favor digitar los dígitos: 2024

Lo anterior para su conocimiento y fines pertinentes.

Atentamente;

ANA MILENA VILLAZON OROZCO

Asesora Jurídica

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:	Expediente_Juridico_Detallado_N#89566657856..exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	April 25, 2024 at 17:32:15
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	84025A1BD23886BAA112BE5C05F9B73B
SHA1:	59AAE2AEA80A5D3A6287B5AABE46E701C9A0569C

SHA256:	613D620D7D8C50465B05146B31E1E5139DB23FECF164EE482C130F23AD9A15BA
SSDEEP:	49152:7U7+DRuSHllxa4soE9CWpXubu8KbHshELCEWpKf4NSd5Dfc:7U7qLFK44pcu80Hsh6zq

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Expediente_Juridico_Detallado_N#89566657856..exe"	"C:\Users\admin\AppData\Local\Temp\Expediente_Juridico_Detallado_N#89566657856..exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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