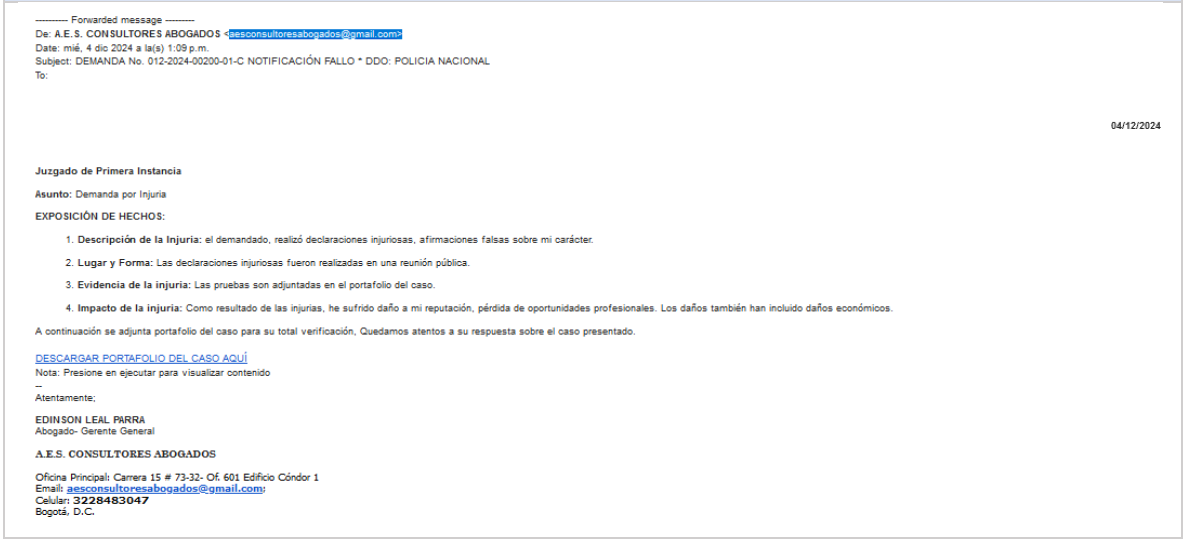
Diciembre 06 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

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



---------- Forwarded message ---------
De: A.E.S. CONSULTORES ABOGADOS <aesconsultoresabogados@gmail.com>
Date: mié, 4 dic 2024 a la(s) 1:09 p.m.
Subject: DEMANDA No. 012-2024-00200-01-C NOTIFICACIÓN FALLO * DDO: POLICIA NACIONAL
To:

04/12/2024

Juzgado de Primera Instancia

Asunto: Demanda por Injuria

EXPOSICIÓN DE HECHOS:

1. **Descripción de la Injuria:** el demandado, realizó declaraciones injuriosas, afirmaciones falsas sobre mi carácter.
2. **Lugar y Forma:** Las declaraciones injuriosas fueron realizadas en una reunión pública.
3. **Evidencia de la injuria:** Las pruebas son adjuntadas en el portafolio del caso.
4. **Impacto de la injuria:** Como resultado de las injurias, he sufrido daño a mi reputación, pérdida de oportunidades profesionales. Los daños también han incluido daños económicos.

A continuación se adjunta portafolio del caso para su total verificación, Quedamos atentos a su respuesta sobre el caso presentado.

DESCARGAR PORTAFOLIO DEL CASO AQUÍ
Nota: Presione en ejecutar para visualizar contenido
--
Atentamente;

EDINSON LEAL PARRA
Abogado- Gerente General

A.E.S. CONSULTORES ABOGADOS

Oficina Principal: Carrera 15 # 73-32- Of. 601 Edificio Cóndor 1
Email: aesconsultoresabogados@gmail.com;
Celular: 3228483047
Bogotá, D.C.

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.

Se realiza la verificación del archivo en mención, donde:

1. **El archivo no cuenta con ninguna protección mediante contraseña**: Para el usuario final, la ausencia de una contraseña en este tipo de archivos representa un alto riesgo. Al no estar protegido, el archivo puede ser abierto de manera inmediata, aumentando la probabilidad de que el usuario, sin sospechar de su naturaleza maliciosa, lo ejecute. Esto reduce significativamente el tiempo de reacción necesario para identificar la amenaza antes de que cause daño. Además, la facilidad de acceso elimina cualquier barrera

que pudiera obligar al usuario a detenerse y cuestionar la legitimidad del archivo, lo que incrementa el riesgo de infección y exposición de información sensible.

2. **El archivo descargado está comprimido y contiene dos accesos directos maliciosos**: Al extraer el archivo comprimido, se identificó dos accesos directos que aparentan ser archivos legítimos, pero que, al analizar sus propiedades, se observan que estan configurados para ejecutar acciones maliciosas. En las pestañas "Documento Web" de los accesos directos, se encontraron dos URL con la siguiente dirección: file://\\77.105.161.126@80\file\nlfb.exe y file://\\77.105.161.126@80\file\qtlh.exe

   Esta dirección apunta a un servidor remoto, desde el cual se intenta descargar y posiblemente ejecutar un archivo denominado build.exe. Este comportamiento indica un claro intento de los atacantes de explotar el acceso del usuario para conectarse a un recurso externo y ejecutar un archivo potencialmente malicioso.

   Para el usuario final, este tipo de ataque representa un riesgo crítico porque:

- **Ejecución inadvertida de malware**: El acceso directo puede ser engañosamente presentado como un archivo legítimo, aumentando la probabilidad de que el usuario lo abra sin sospechar de su naturaleza maliciosa.
- **Exposición a servidores maliciosos**: Al intentar acceder a la dirección especificada, el sistema del usuario podría exponer información como la dirección IP o credenciales de red, facilitando un ataque más amplio.
- **Automatización del proceso malicioso**: La configuración del acceso directo permite que la descarga y ejecución del archivo se realice de manera rápida y silenciosa, sin intervención adicional del usuario, reduciendo las posibilidades de detección temprana.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	4b4e5745d6e7c73c1713ba35982593ae81b514c1f7c707cf56ac244bea057df9.unknown
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	diciembre 06, 2024 at 08:52:38
MIME:	application/vnd.microsoft.portable-executable
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows, 7 sections
MD5:	e25387353c3ce8180f33af30bdb57d83
SHA1:	f27e04b2723e501cef851185774bf9dc7b1df414
SHA256:	4b4e5745d6e7c73c1713ba35982593ae81b514c1f7c707cf56ac244bea057df9
SSDEEP:	6:JyXSvVG/FTVmJtOFJblvstXbPAbhYNraUr5aK+d9osv:cXaVWfmJtOFJB0tLov

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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