

Fuentes utilizadas:

Verificar IP Blacklist y Encabezados: <https://mxtoolbox.com/blacklists.aspx>

Constatar Dominios: <https://exchange.xforce.ibmcloud.com/>

Consultar valides de email: <https://captainverify.com/es/mail-tester.html>

Sandbox: <https://app.any.run/>

Sandbox, Revisión de IP, hashes o URL: <https://www.virustotal.com/gui/home/upload>

Cuentas filtradas: <https://haveibeenowned.com/>

Estimados,

De acorde a la alerta observada en FortiSandbox se comparte el análisis realizado:

Ticket ID: 532

Conclusión:

Veredicto del análisis de alerta.

Recomendaciones:

Se brinda recomendaciones sobre acciones a tomar: Bloqueo del sender malicioso, hash, dominio, url.

Análisis:

1. Revisión consola Operation Center (FortiSandbox).

- **Sender:** mpculiacan@t1.frvemex[.]com
- **Sender IP:** 185[.]201[.]19[.]20
- **Nombre de archivo:** Intimacion_837662.pdf
- **Hash:** b7c4fb3dd21fc27842957bb21a3ba10f9e14997151e16329444f38f4110d6b2e

The screenshot displays two main sections from the FortiSandbox interface. The top section is a table with columns: Severity, Source, Incident Time, Threat Name, and File Name. It shows one entry with a medium risk level, source IP 185.201.19.20, incident time Jul 01 2024 12:55:37, threat name 'Suspicious - Medium', and file name 'Intimacion_837662.pdf'. The bottom section is a verification form asking for an email address to check if it's known. It shows a red message box stating 'mpculiacan@t1.frvemex.com es desconocido' (Unknown). There are also 'Ingresar' and 'Chequear' buttons.

Severity	Source	Incident Time	Threat Name	File Name	
⚠️ C	⚠️ Medium Risk	185.201.19.20	Jul 01 2024 12:55:37	Suspicious - Medium	Intimacion_837662.pdf

Ingrese un correo electrónico para verificar Chequear

mpculiacan@t1.frvemex.com es desconocido Ingresar

Datos del adjunto

- **Nombre de archivo:** intimidaciones.pdf
- **URL:**
hxps://intimidaciones.afip.gob.ar/.k dental/.cl/Documentos_Intimacion/?id=66381&code=IdsLDYxBcmk
hxlapaGtafnMLYavPbGOWPUitlsVFGhnVTgqUojSQVZ
- **HASH:** 017d9891a86d78063b9dda54978214c4

2. Revisión en ADOM FortiMail (FortiAnalyzer)

- Se valida en total “2” correos recibidos con asunto: “**MONOTRIBUTO. Intimación falta de pago. Corte de informacion recibida hasta el 04/07/2024.**”
- **Cuenta afectada:**
dgpericias@policiafederal.gov.ar
ceremonial@policiafederal.gov.ar

#	Date/Time	Session ID	Direction	From	Subject	To	Virus/Botnet
1	12:54:49	461FWIn202748-81UFWWnD32746	In	impulsus@impulsus.com	MONOTRIBUTO. Intimación falta de	policiafederal.gov.ar	FortiSandbox: Unknown
2	12:39:38	461FWInM32581-81UFWhPOG2581	In	impulsus@impulsus.com	MONOTRIBUTO. Intimación falta de	policiafederal.gov.ar	FortiSandbox: Unknown

•

3. Análisis de IP:

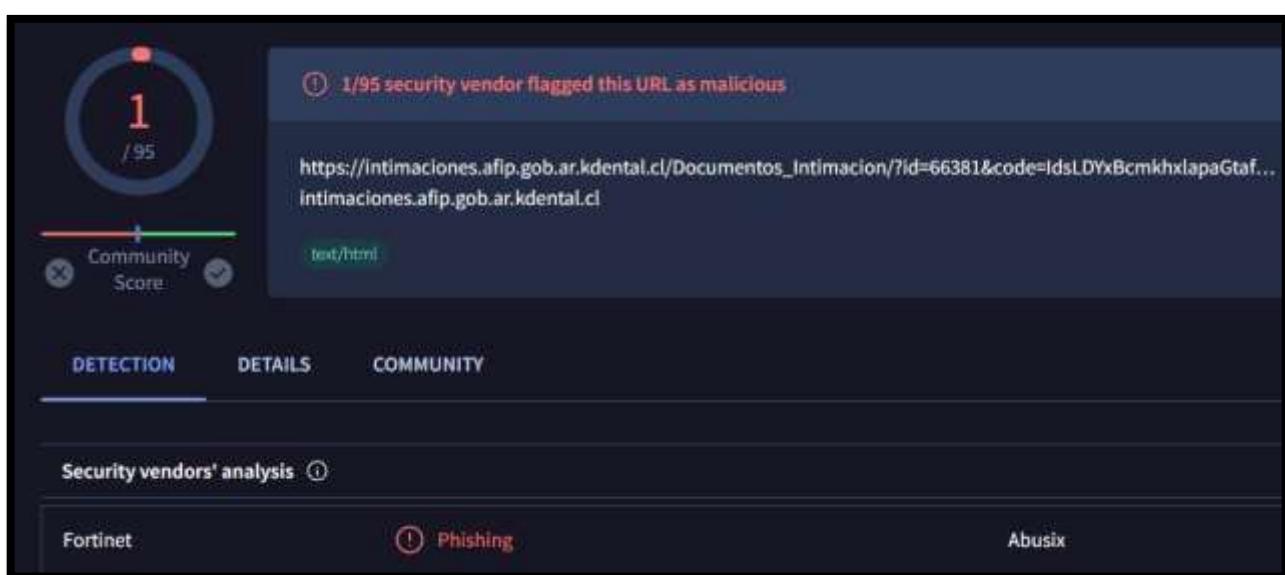
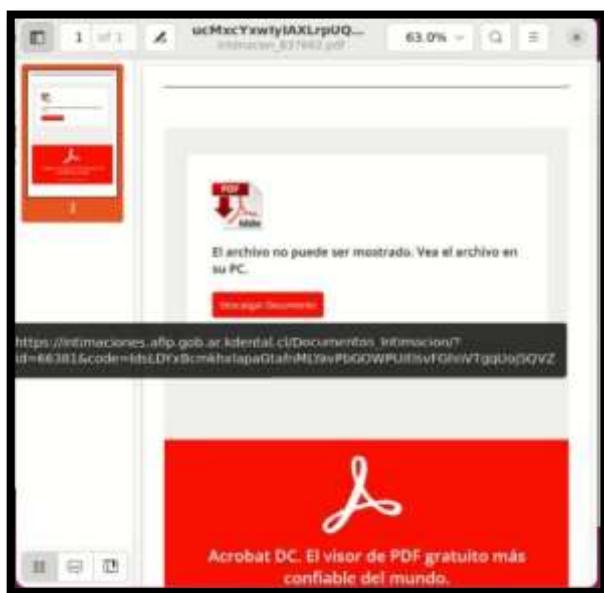
- Se realizó el análisis de la IP del sender la cual no se encuentra como maliciosa.



•

4. Análisis en Sandbox:

- Se analizó el adjunto en cuestión:
 - El archivo posee un link que redirecciona a una descarga de un archivo a url mencionada en el punto 1, la cual está catalogada como PISHING.



Nombre del Oficial Responsable - **Analista del SOC**

División Seguridad Informática