Superintendencia FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES

Departamento CIBERSEGURIDAD

División SEGURIDAD INFORMÁTICA

Centro de Operaciones de Seguridad (SOC)

02/10/2024

Introducción

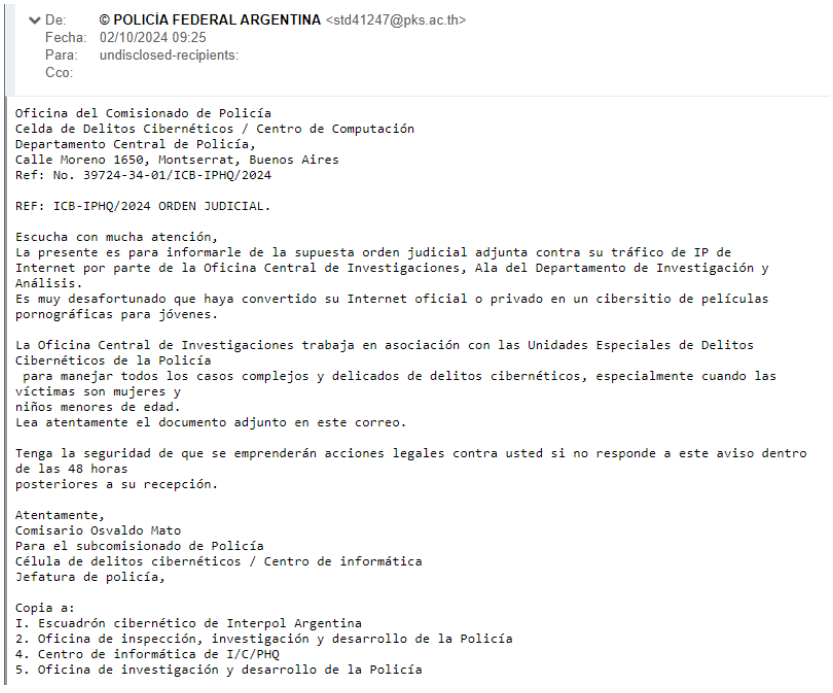
En la fecha del 2 de octubre de 2024, se recibió un correo electrónico que se presenta como una notificación oficial de la "Policía Federal Argentina" sobre una supuesta orden judicial.

Luego de un análisis minucioso de los encabezados y del contenido del mensaje, se han identificado múltiples indicios que sugieren que este correo se trata de un intento de phishing. Se comprueba que el remitente utiliza un dominio educativo tailandés, lo que genera dudas sobre la legitimidad del mensaje, y la dirección de respuesta apunta a una cuenta de Gmail, lo que refuerza la sospecha de fraude. El contenido del correo emplea un lenguaje intimidante y amenazante, típico de intentos de estafa diseñados para manipular a los receptores a través del miedo.

A tal efecto, este informe tiene como objetivo detallar los hallazgos y recomendaciones para mitigar el riesgo asociado a este tipo de correos electrónicos maliciosos.

Desarrollo

A fin de obtener un informe detallado del correo electrónico anteriormente mencionado, que aparentemente proviene de la "Policía Federal Argentina" y que incluye un archivo adjunto, se revisarán aspectos clave como los encabezados del correo (del cual se presenta imagen), el archivo adjunto y el análisis de la autenticidad del remitente, junto con la identificación de posibles intentos de phishing.



De: **© POLICÍA FEDERAL ARGENTINA** <std41247@pks.ac.th>
Fecha: 02/10/2024 09:25
Para: undisclosed-recipients:
Cco:

Oficina del Comisionado de Policía
Celda de Delitos Cibernéticos / Centro de Computación
Departamento Central de Policía,
Calle Moreno 1650, Montserrat, Buenos Aires
Ref: No. 39724-34-01/ICB-IPHQ/2024

REF: ICB-IPHQ/2024 ORDEN JUDICIAL.

Escucha con mucha atención,
La presente es para informarle de la supuesta orden judicial adjunta contra su tráfico de IP de Internet por parte de la Oficina Central de Investigaciones, Ala del Departamento de Investigación y Análisis.
Es muy desafortunado que haya convertido su Internet oficial o privado en un cibersitio de películas pornográficas para jóvenes.

La Oficina Central de Investigaciones trabaja en asociación con las Unidades Especiales de Delitos Cibernéticos de la Policía
para manejar todos los casos complejos y delicados de delitos cibernéticos, especialmente cuando las víctimas son mujeres y
niños menores de edad.
Lea atentamente el documento adjunto en este correo.

Tenga la seguridad de que se emprenderán acciones legales contra usted si no responde a este aviso dentro de las 48 horas
posteriores a su recepción.

Atentamente,
Comisario Osvaldo Mato
Para el subcomisionado de Policía
Célula de delitos cibernéticos / Centro de informática
Jefatura de policía,

Copia a:
I. Escuadrón cibernético de Interpol Argentina
2. Oficina de inspección, investigación y desarrollo de la Policía
4. Centro de informática de I/C/PHQ
5. Oficina de investigación y desarrollo de la Policía

Imagen1. Cuerpo del correo

POLICIA FEDERAL ARGENTINA

DEPARTAMENTO CENTRAL DE POLICÍA,
1650 Moreno Street, Montserrat, Buenos Aires
https://www.argentina.gob.ar/policia-federal-argentina

09672882

Por mandato del Comisario General Juan Carlos Hernández, Comisario de la Fuerza de Policía Argentina; en asociación con ESCUADRÓN CIBERNÉTICO y OFICINA DE INVESTIGACIÓN Y DESARROLLO POLICIAL; que son las Agencias Nodales Nacionales de INTERPOL en Argentina;

Por la presente, le notifico sobre una incautación computarizada de ciberinfiltración capturada en su dirección de protocolo de Internet **(IP)** relacionada con el siguiente análisis:-

- **Pornografia Infantil**
- **Pedofilia**
- **Exhibicionismo**
- **Pornografia Cibernetica**
- **Trafico Sexual**
- **Masturbación**
- **Estafas En Linea Y Participacion En Conspiraciones**

COPIA CERTIFICADA POLICIA CIBERCRIMEN

REPUBLICA ARGENTINA POLICIA FEDERAL

CÓDIGO PENAL DE LA NACIÓN ARGENTINA Código Penal No. 26,**388 ARTÍCULO 2º**. Sección Sustituida por el art. 29 de la Ley Nº 27.401 BO, y el artículo 67B de la Ley de Informática, de 2000 tipifica como delito la publicación o transmisión de actos o conductas sexualmente explícitos en forma electrónica de pornografía juvenil y se castiga en primera condena con pena de prisión.

La Oficina Central de Investigaciones **(CBI)** y las Unidades de Delitos Cibernéticos de **ARGENTINA** desempeñan un rol investigativo contra las víctimas que a través de la tecnología de la información, sugieren, poseen, producen, difunden o acceden a imágenes y materiales pornográficos infantiles dentro de nuestro territorio.

El Gobierno también ha dado una serie de medidas que deben implementar los proveedores de servicios de Internet **(ISP)** para proteger a los niños del abuso sexual en línea. Estas, entre otras, incluyen:

Bloqueo de sitios web que contienen material de abuso sexual infantil extremo, de acuerdo con la "Lista de los peores" de **INTERPOL**, que comparte periódicamente la Oficina Central de Investigaciones La lista se comparte con el Departamento de Telecomunicaciones **(Dot),** que luego ordena a los principales proveedores de servicios de Internet que bloqueen dichos sitios web por discreción.

He decidido ponerme en contacto con usted en forma privada antes de transferir los expedientes de su caso a los fiscales del tribunal para que procesen de inmediato. Con efecto inmediato, responda a este mensaje y exponga sus justificaciones para una nueva revisión antes de que se le impongan las sanciones correspondientes en las próximas **24 horas.**

En caso de no responder en el plazo de **24 horas**, el fiscal establecerá una orden de aprehensión en su contra a través de la Comisaría de Policía más cercana. Después del procesamiento, su información será enviada al Registro Nacional de Delincuentes Sexuales Menores, a las asociaciones que luchan contra la **PEDOFILIA** y a los Medios de Comunicación para su publicación.

Responda Inmediatamente.

Sra. Sandra Moreno,
Jefa De La División De Delitos Informáticos
Contra Niños, Niñas Y Adolescentes D
Policía Federal Argentina

INTERPOL INTERPOL CYBERCRIME UNIT

Comisario General Juan Carlos Hernández, Comisario de la Policía Federal Argentina

CERTIFICADA

Fiscalía de Menores y Delitos Relacionados con la Ciberdelincuencia.

Sede: Departamento Central de Policía,1650 Moreno Street, Montserrat, Buenos Aires

Imagen 2. Archivo adjunto al correo.

Análisis del Encabezado

El análisis del encabezado revela varias irregularidades que sugieren que el correo no es legítimo:

Encabezados Encontrados

Nombre del Encabezado	Valor de Encabezado
Entregado-Para	
X-Reenviado-Encriptado	i=2; AJvYcCUxVPT51bbrT+Jp9h/PNJL+Jz7+17SBuCCsIQnWcpF8IYlYi2lka/CShHP6CpddGSfIgTeRnmBIfSo=@gmail.com
X-Recibido	para 2002:a5d:474a:0:b0:374:b9a1:28f con SMTP id ffacd0b85a97d-37cfba0a5b7mr1748960f8f.43.1727871989651; miércoles, 02 Oct 2024 05:26:29 -0700 (PDT)
ARC-Sello	i=1; a=rsa-sha256; t=1727871989; cv=none; d=google.com; s=arc-20240605; b=hKr3Xj071CAPeLnpMImx9edzMwNLTkVbYwoCslPvYW5+21ZpfLdXz4KS aPLIJx1ivNrWYfCfwYfeOeeX2bCY6rgwdGlk2nRczD0whnxMC9+hm5fOMWmZxBdMn2fU o1+bPsV4vmfG4DCbuyQ7JGXR46yeYP9Si9SsZBQw+kZt2cJ3r82x9zmmZFI 6xc4DBom3GqEldVTY/MuBbMRK7vfTO0rbmGh29m6co
ARC-Mensaje-Firma	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=to:subject:mime-version:dkim-signature; bh=TcpRtubwTh0pX594d/y3bD630R5zhGjigLVjthqQ=; fh=Ibp/VRSLIuLfR9rCpcNCk4Cm3mbST3EWbwPBtQjvbv9/RIDSOtQjvfRU1wv4inewiZjl6h xUK63gY4gFLjaQ1nX2fvbznoo07jWBvJh3r/kow5WJB9UD0IPW39Q2huTm1rBq LPDqX02K17swfJ6S74atejkKBSWBmWmW47GMXI
ARC-Authentication-Resultados	i=1; mx.google.com; dkim=pass header.i=@pks-ac-th.20230601.gappssmtp.com header.s=20230601 header.b=qTVcX+xV; spf=pass (google.com: domain of std41247@pks.ac.th designa 209.85.220.65 como remitente permitido) smtp.mailfrom=std41247@pks.ac.th; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=pks.ac.th; dara=pass header.i=@gmail.com
Retorno-Path	<std41247@pks.ac.th>
Recibido-SPF	pass (google.com: domain of std41247@pks.ac.th designa 209.85.220.65 como remitente permitido) client-ip=209.85.220.65;
Autenticación-Resultados	mx.google.com; dkim=pass header.i=@pks-ac-th.20230601.gappssmtp.com header.s=20230601 header.b=qTVcX+xV; spf=pass (google.com: domain of std41247@pks.ac.th designa 209.85.220.65 como remitente permitido) smtp.mailfrom=std41247@pks.ac.th; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=pks.ac.th; dara=pass header.i=@gmail.com
DKIM-Firma	v=1; a=rsa-sha256; c=relaxed/relaxed; d=pks-ac-th.20230601.gappssmtp.com; s=20230601; t=1727871989; x=1728476789; dara=google.com; h=to:subject:message-id:date:from:to:cc:subject:date:message-id:reply-to; bh=TcpRtubwTh0pX594d/ol/y3bD630R5zhGjigLVjthqQ=; b=qTVcX+xVUCR9wEc/HVQoD2K0RTpN/Rov05yDLP8N+YORg8HyFjiac6TBeqoay+tbt0 XjsXYv+jVqiKqzNPJgF56BXhGgu8LgJw9pTFnhUTtRZ2wSMaJR2D4yykeP+sCu8fh QtcLNIC147uGuiBOYC3JfIG6CHNv2YGMjkUTaTz6RDne5NB5ky/ox91k6cLS+jxuDevP z8YUbjPMgas/12pfv3Th23vazo6fB7RMdR6MO7TZv2IP0/HJqszPDaWSX/QXRu6qDLBf 4xMMM7EI2kOnAE5Z/E6DQOleN
Firma X-Google-DKIM	v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20230601; t=1727871989; x=1728476789; h=to:subject:message-id:date:from:reply-to:mime-version:x-gm-message-state:from:to:cc:subject:date:message-id:reply-to; bh=TcpRtubwTh0pX594d/ol/y3bD630R5zhGjigLVjthqQ=; b=mYCA0Zj+W2a34sSrNLkMlvrdBs1/PpDnV+Z5YZ6YzSDz5Tnht36RyqxvUdy+ZHYveE Wl8aP24ufd9n4yzu9ZJt0Nmeng9UN63mmS/eYT5JyH18Hvd0DJW/OXu0wu3fpQmpQ/aj bA4sGfkEvGoW4N3DyK7q67ayXEjX7TAR78xW4UBsDhLOQvi1auMIRX1afkn9UWN+zeE/ZnXkq5PhJOYrbLxtRjjh8GX6CC6BEwEekTKpeHcx7Tv6pLTLKGjEKAnGGmPWCkyP7cB sg1okVeceB0Im6MBgQcltojHsQ7ZOC8jBhXPD04ZCnGng/xlBMdDJRiEAgu1M
X-Gm-Mensaje-Estado	AOJu0Yy3kJdUl/KX1DtGuj6T2xKkWtDfYbkl0rfekjwzuNRA7g0zXzg5 p9Vkev5Lm4zDtNeIcAsfrY+NzBKL6f1aAoKU5dzs7P3eD2FObER0whwVBpqWJ45X2+AXM0Do6hJ RWejcEJmVo5bu+LIL3Uf2BDRrFnWwDj9rg+
X-Google-Smtp-Fuente	AGHT+IERwwcPacRKAw43mRlF9jPD+u6oZXJYschODUDSKujgGNzEplkHB1aZ6/w4yKRkqWpt0DkxV18ZmmBN4VUy+M4=
MIME-Versión	1.0
Responder-Para	cibercrimenpolicial@gmail.com
De	© POLICÍA FEDERAL ARGENTINA <std41247@pks.ac.th>
Fecha	Mié, 2 Oct 2024 00:25:59 -1200
Mensaje-ID	<CAChLzy64-9pYvoWEOL_c1GGwhx+1rLktGYugWonNy7OvOLe4bQ@mail.gmail.com>
Asunto	Policial Notificación / Orden de Judicial para usted
A	destinatarios no revelados:;
Tipo de Contenido	multiparte/mezclado; boundary="0000000000012edef06237d8cf0"
Bcc	madisisto@gmail.com

Imagen 2: Análisis completo de la cabecera del correo.

Los puntos de interés para este análisis son:

1) **Remitente y Dominio**: El correo se envió desde la dirección std41247@pks.ac.th, que corresponde a un dominio educativo en Tailandia, lo cual no concuerda con la entidad remitente, la "Policía Federal Argentina". Esta discrepancia es un fuerte indicio de suplantación de identidad (phishing), ya que una institución oficial utilizaría el dominio gubernamental argentino (.gob.ar).

De:	© POLICÍA FEDERAL ARGENTINA <std41247@pks.ac.th>
A:	destinatarios no descubiertos:;

2) **Campo "Reply-To"**: El campo Reply-To del correo señala la dirección cibercrimenpolicial@gmail.com.
Ninguna entidad gubernamental utilizaría un servicio como Gmail para comunicaciones oficiales. Esto nos indica que el remitente está enmascarado, y las respuestas al correo irían a un destino controlado por los atacantes.

Reply-To	cibercrimenpolicial@gmail.com

3) **Validación de SPF, DKIM y DMARC**: Los registros SPF, DKIM y DMARC indican que el correo pasó las verificaciones para el dominio de origen (pks.ac.th), lo que significa que el mensaje fue enviado desde un servidor autorizado para ese dominio.
Sin embargo, dado que el dominio no tiene relación con la Policía Federal Argentina, estos resultados no validan la legitimidad del remitente, sino que simplemente confirman que no hubo manipulación en la ruta de envío.

SPF:	**pass** con la IP 209.85.220.65
DKIM:	**pass** con el dominio pks-ac-th.20230601.gappssmtp.com
DMARC:	**pass**

4) **Encabezados encriptados**: La presencia de campos como X-Forwarded-Encrypted y cadenas cifradas sugiere que hay una intención de ocultar la verdadera naturaleza del correo o bien de añadir una capa adicional de confusión. Esto puede indicar un intento de manipulación o falsificación más avanzada.

X-Forwarded-Encrypted	i=2; AJvYcCUxVPT51bbrT+Jp9h/PNJL+Jz7+17SBuCCsIQnWcpF8IYlYi2lka/CShHP6CpddGSfIgTeRnmBlfSo=@gmail.com

Link al sitio de la Herramienta Mx.Toolbox con la que se analizó la cabecera:

MxToolbox - Email Headers

Análisis del Archivo Adjunto

El correo contiene un archivo adjunto en formato de imagen (.jpg) con el nombre NOTIFICACIÓN_DE_ORDEN_JUDICIAL1.jpg (Imagen 2).

El mismo fue analizado y no se encontraron indicadores de compromiso, tales como metadatos maliciosos, contenido incrustado a través de técnicas de esteganografía, explotación de vulnerabilidades en visores de imágenes o hashes.

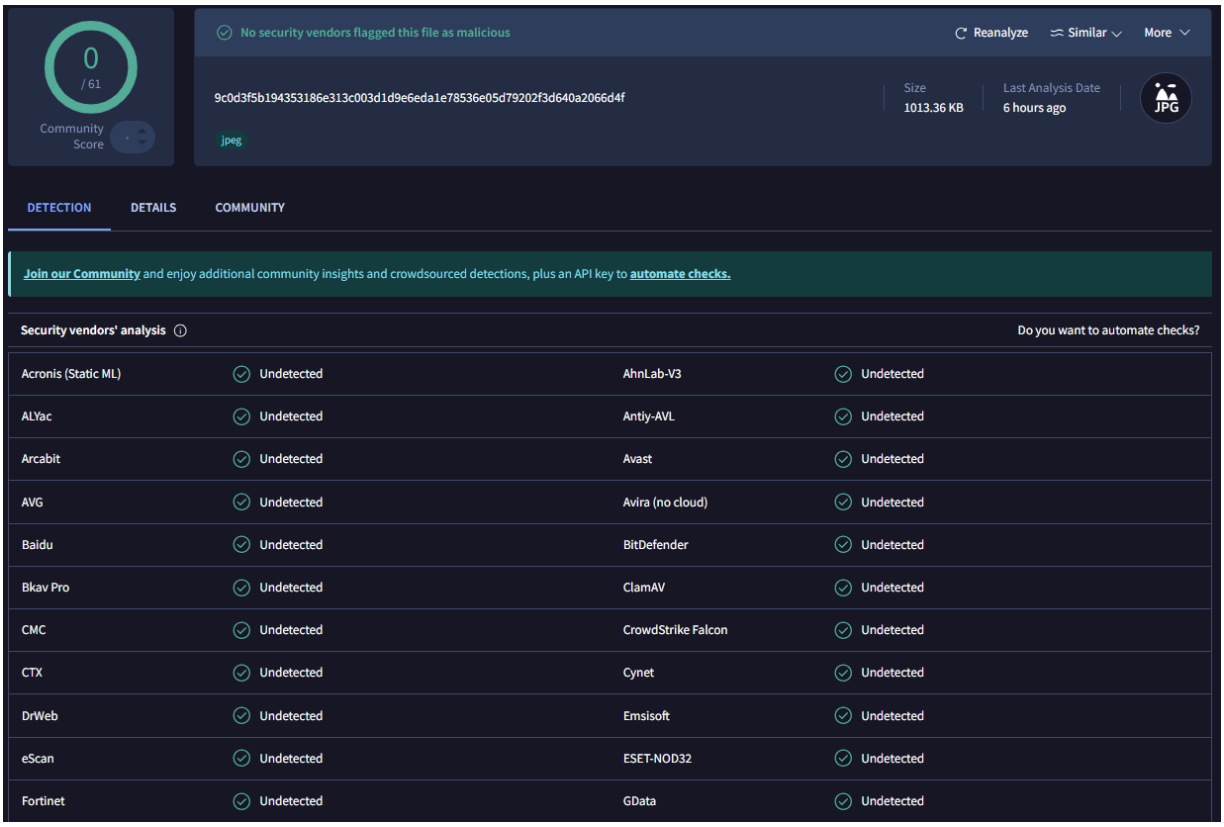


Imagen 3: Análisis del archivo adjunto en Virus Total.

Aunque se presenta como una imagen, es común que los ciberdelincuentes utilicen archivos adjuntos aparentemente inofensivos para distribuir malware o spyware. En muchos casos, las imágenes pueden estar corrompidas o contener exploits que, al ser abiertas, ejecutan código malicioso en el dispositivo del usuario.

Conclusión

El análisis del correo y su contenido ha revelado múltiples indicios que lo clasifican como un intento de phishing:

1) **Remitente enmascarado**: El uso de un dominio educativo de Tailandia, que no guarda relación con la Policía Federal Argentina, demuestra un claro intento de ocultar la verdadera identidad del remitente.

2) **Campo "Reply-To" sospechoso**: La dirección de respuesta a una cuenta de Gmail refuerza la hipótesis de que este correo está diseñado para engañar a la víctima y desviar cualquier respuesta a una cuenta controlada por los atacantes.

3) **Contenido intimidante**: El mensaje utiliza un lenguaje alarmante para inducir pánico en el destinatario y hacerlo actuar rápidamente, lo que es típico en los correos de phishing.

4) **Archivo adjunto peligroso**: El archivo adjunto en formato de imagen no es el adecuado para comunicaciones legales oficiales y podría contener malware o exploits.

En base a estos hallazgos, se recomienda marcar este correo como un intento de phishing y proceder con su eliminación inmediata, sin interactuar con el archivo adjunto ni responder a los remitentes.

Para consultas o avisos de correos similares, ponerse en contacto con esta dependencia mediante el correo oficial: csoc@policiafederal.gov.ar o los internos: 7777, 7701.