



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)

Dirección General Agencia Regional
Federal NEA Corrientes

Introducción

El día 11 de abril del corriente año, se recibió un correo electrónico proveniente de la cuenta vchanenko@policiafederal.gov.ar perteneciente a la Dirección General Agencia Regional Federal NEA Corrientes, informando posible phishing.

Desarrollo

Una vez identificado el caso, se procedió al análisis del correo proveniente de “**01051292@polri.go.id**”. Se observó en primera instancia que el mail se encuentra en idioma italiano. El mismo simula ser una “Notificación de caducidad de contraseña”, en el cuerpo del mensaje refiere que el día 8 de abril vence la contraseña y hay un link para ingresar y mantener la misma.



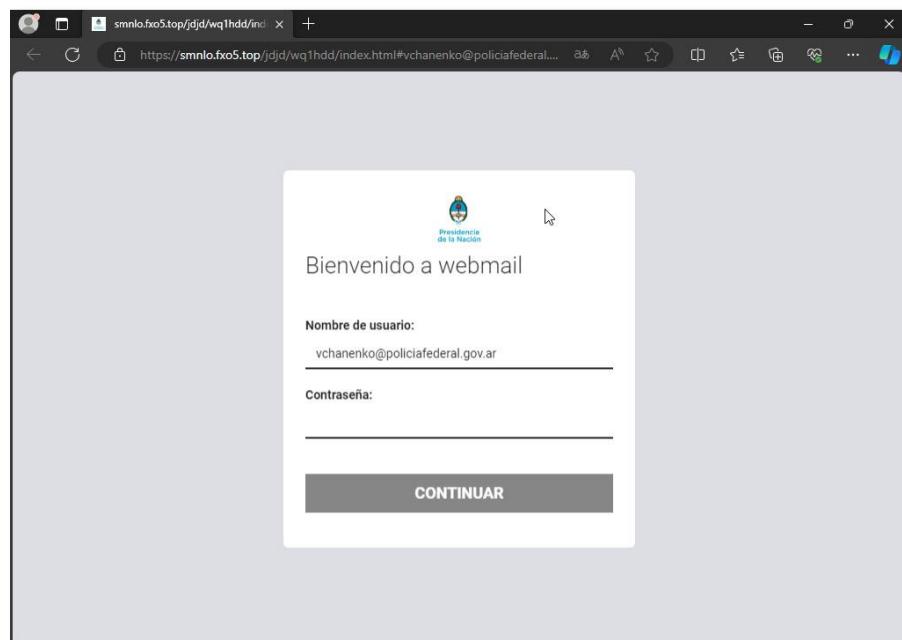
Imagen 1. Cuerpo del mail.

Se procede a analizar el encabezado del mismo, el cual se puede observar que no se encuentra enmascarado siendo el remitente original: “**01051292@polri.go.id**”.

X-MDAV-Result:	clean
X-FEAS-SPF:	spf-result=pass, ip=120.29.231.221, helo=mailprotection1.polri.go.id, mailFrom=01051292@polri.go.id
X-FEAS-DKIM:	Valid
X-FEAS-Client-IP:	120.29.231.221
X-FE-Last-Public-Client-IP:	120.29.231.221
X-FE-Envelope-From:	01051292@polri.go.id
X-FE-Policy-ID:	4:1:1:policiafederal.gov.ar
X-MDAV-Processed:	policiafederal.gov.ar, Mon, 08 Apr 2024 15:44:57 -0300
X-Spam-Processed:	policiafederal.gov.ar, Mon, 08 Apr 2024 15:44:56 -0300
X-MDArrival-Date:	Mon, 08 Apr 2024 15:44:56 -0300
X-Rcpt-To:	vchanenko@policiafederal.gov.ar
X-MDRcpt-To:	vchanenko@policiafederal.gov.ar
X-Return-Path:	01051292@polri.go.id
X-Envelope-From:	01051292@polri.go.id
X-MDaemon-Deliver-To:	vchanenko@policiafederal.gov.ar

Imagen 2. Encabezado.

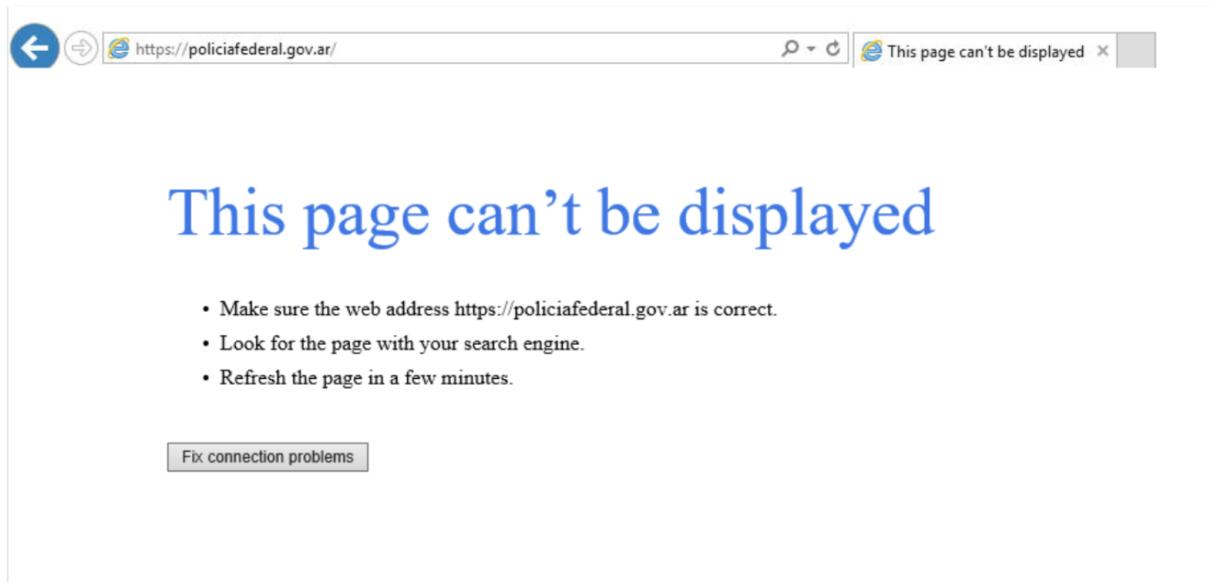
Continuando con el análisis, una vez que se ingresa al link del mail, nos dirige al sitio: [“https://internal-hexagonal-frog.glitch.me?rt=vchanenko@policiafederal.gov.ar”](https://internal-hexagonal-frog.glitch.me?rt=vchanenko@policiafederal.gov.ar) para luego automáticamente redirigirnos a la siguiente dirección: [“https://smnlo.fxo5.top/jdjd/wq1hdd/index.html#vchanenko@policiafederal.gov.ar”](https://smnlo.fxo5.top/jdjd/wq1hdd/index.html#vchanenko@policiafederal.gov.ar) el cual simula ser un login de mail y contiene una imagen de presidencia de la nación. El usuario no se encuentra en un campo editable, pero si así el de la



contraseña.

Imagen 3. Sitio de login.

Al completar el campo de contraseña con caracteres aleatorios, nos indicara que la contraseña es incorrecta y se reintente escribir de nuevo. A los 3 intentos nos



dirige a la dirección: "www.policiafederal.gov.ar" la cual no se encuentra activa.

Imagen 4. Redirección web.

Se analizaron ambos sitios con la herramienta Virustotal. Dando los dos como resultado: **PHISHING**.

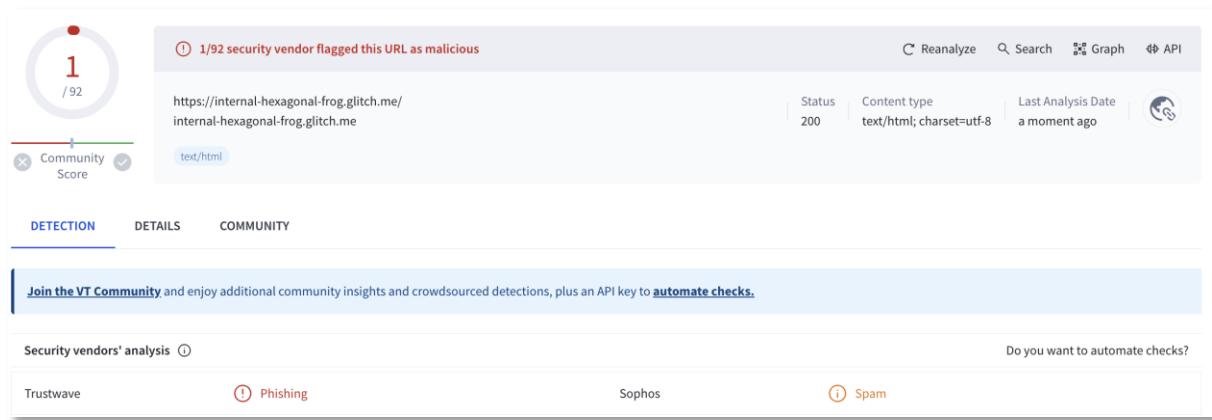


Imagen 5. Sitio: "<https://internal-hexagonal-frog.glitch.me?rt=vchanenko@policiafederal.gov.ar>"

1 / 92

1/92 security vendor flagged this URL as malicious

<https://smnlo.fxo5.top/jdjd/wq1hdd/index.html>

smnlo.fxo5.top

text/html

Status 200 Content type text/html Last Analysis Date 3 hours ago

Community Score

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Trustwave Phishing Sophos Spam

Do you want to automate checks?

Imagen 6. Sitio: “<https://smnlo.fxo5.top/jdjd/wq1hdd/index.html>#vchanenko@policiafederal.gov.ar””

Se realizó un informe del dominio con la herramienta MXtoolbox de la dirección de mail: “**01051292@polri.go.id**”, el mismo se encuentra en varias listas negras, con varias advertencias de seguridad.

9 Problems		
Category	Host	Result
blacklist	mailprotection1.polri.go.id	127.0.0.2
blacklist	mailprotection1.polri.go.id	Blacklisted by SORBS SPAM
spf	polri.go.id	Too many included lookups (14)
smtp	mailprotection1.polri.go.id	Warning - Does not support TLS.
smtp	mailprotection1.polri.go.id	7.419 seconds - Warning on Connection time
smtp	mailprotection1.polri.go.id	9.312 seconds - Not good! on Transaction Time
dns	polri.go.id	At least one name server failed to respond in a timely manner
dns	polri.go.id	Local NS list does not match Parent NS list
dns	polri.go.id	SOA Serial Number Format is Invalid

Imagen 7. Análisis con herramienta MXtoolbox.

Se utilizó la herramienta SysInspector para averiguar si el ingreso al sitio, realizó algún cambio peligroso en el sistema operativo, dando como resultado negativo.



Imagen 8. Análisis con herramienta Sysinspector.

Conclusión

En base a lo expuesto en el presente informe, y en referencia al mail remitido por la Dirección General AGENCIA REGIONAL FEDERAL NEA CORRIENTES, se determinó que la maniobra empleada consiste en una técnica de Ingeniería Social del tipo **Phishing**, la misma intenta suplantar la identidad de un login de mail de la Presidencia de la Nación, para robar credenciales.

Se recomienda, al recibir correos de dudosa procedencia, no ingresar a los enlaces o archivos adjuntos y en ninguna circunstancia completar los datos solicitados en los mismos, a su vez, reportarlo cuanto antes a nuestra División a través de la casilla de correo electrónico csoc@policiafederal.gov.ar.

Al respecto, se requirió a la División CENTRO FEDERAL DE DATOS el bloqueo preventivo de la cuenta maliciosa como también a la División SEGURIDAD EN REDES DE DATOS para el bloqueo de las conexiones maliciosas, con el fin de evitar que los usuarios de nuestra Institución sean víctimas de este tipo de engaño.

Ayudante Moreno – Sargento Gauna