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)

Requerido por:

Dirección General AGENCIA REGIONAL FEDERAL LITORAL – SANTA FE

Introducción

El día 09 de agosto del corriente año, se recibió en la cuenta csoc@policiafederal.gov.ar un correo electrónico proveniente de la cuenta vchanenko@policiafederal.gov.ar, que sería de procedencia y contenido dudoso. Por tal motivo, se dio intervención al laboratorio de malware a fin de verificar si el contenido presenta algún nivel de peligrosidad.

Desarrollo

Una vez identificado el caso, se procedió al análisis del correo proveniente de "**georgina.crewe@acenet.co.za".** El mismo busca inducir al engaño aludiendo ser personal de soporte de esta Institución y solicita que se actualicen las credenciales de acceso debido a que "expiran". Se visualizan dos enlaces, el primero al cual podemos acceder haciendo clic en el botón **"Use Same Access",** y el segundo que se encuentra al final del cuerpo del mail.


lunes 7/8/2023 17:24

Administrator/policiafederal.gov.ar (georgina.crewe@acenet.co.za) <georgina.crewe@acenet.co.za>

[Service Ticket #1243722860]: Message Delivery Status / 8/7/2023 9:24 PM

Para vchanenko@policiafederal.gov.ar

Mensaje enviado con importancia Alta.
Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Policiafederal SUPPORT

Your Policiafederal password for (vchanenko@policiafederal.gov.ar) is set to expire today, 8/7/2023.

Use the link below to retain credentials.

Use Same Access

Regards,

Policiafederal Team

This email has been scanned by the Symantec Email Security.cloud service.
For more information please visit http://www.symanteccloud.com

Imagen 1. Cuerpo del mail.

Mediante la herramienta de análisis de encabezado se logra identificar que el mismo remitente no se encuentra enmascarado.

Header Name	Header Value
X-MDAV-Result	clean
X-MDAV-Processed	policiafederal.gov.ar, Mon, 07 Aug 2023 18:17:25 -0300
Return-path	<georgina.crewe@acenet.co.za>
Authentication-Results	policiafederal.gov.ar; iprev=pass reason="white listed" policy.iprev=10.1.150.224 (MAIL.georgina.crewe@acenet.co.za)
X-Spam-Processed	policiafederal.gov.ar, Mon, 07 Aug 2023 18:17:25 -0300 (not processed: recipient vchanenko@policiafederal.gov.ar in exclude file)
X-MDArrival-Date	Mon, 07 Aug 2023 18:17:25 -0300
X-Rcpt-To	vchanenko@policiafederal.gov.ar
X-MDRcpt-To	vchanenko@policiafederal.gov.ar
X-Return-Path	georgina.crewe@acenet.co.za
X-Envelope-From	georgina.crewe@acenet.co.za
X-MDaemon-Deliver-To	vchanenko@policiafederal.gov.ar

Imagen 2. Dirección del remitente.

Al acceder al primer enlace pulsando en el botón nos abre la siguiente página de un login del “WebMail”, en donde podemos visualizar que el “Username” ya está escrito y no se puede modificar.

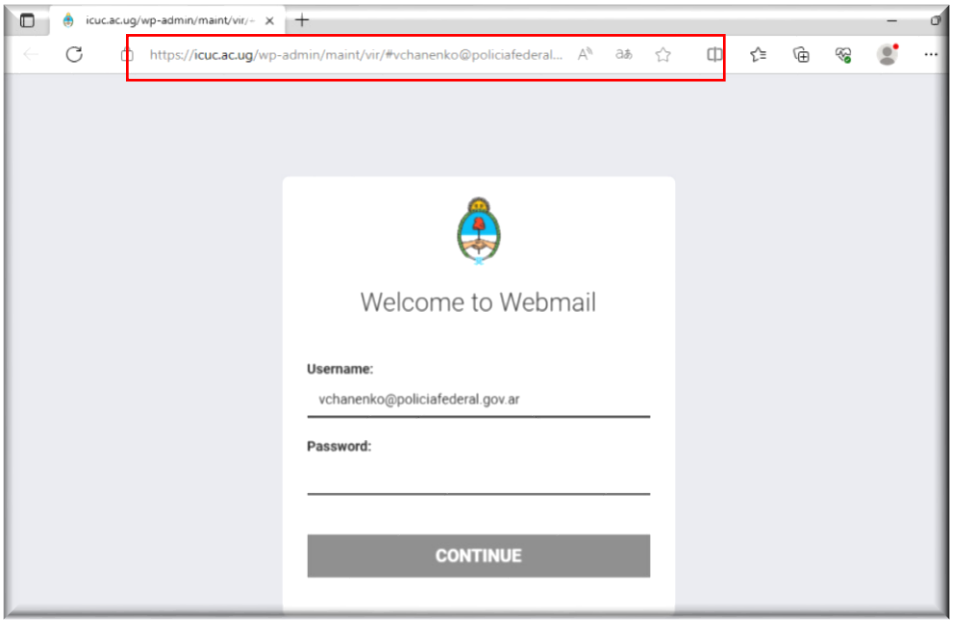

Imagen 3. Login del sitio web falso

Al intentar acceder mediante el uso de una contraseña aleatoria observamos que nos pide que ingresemos la contraseña correcta.

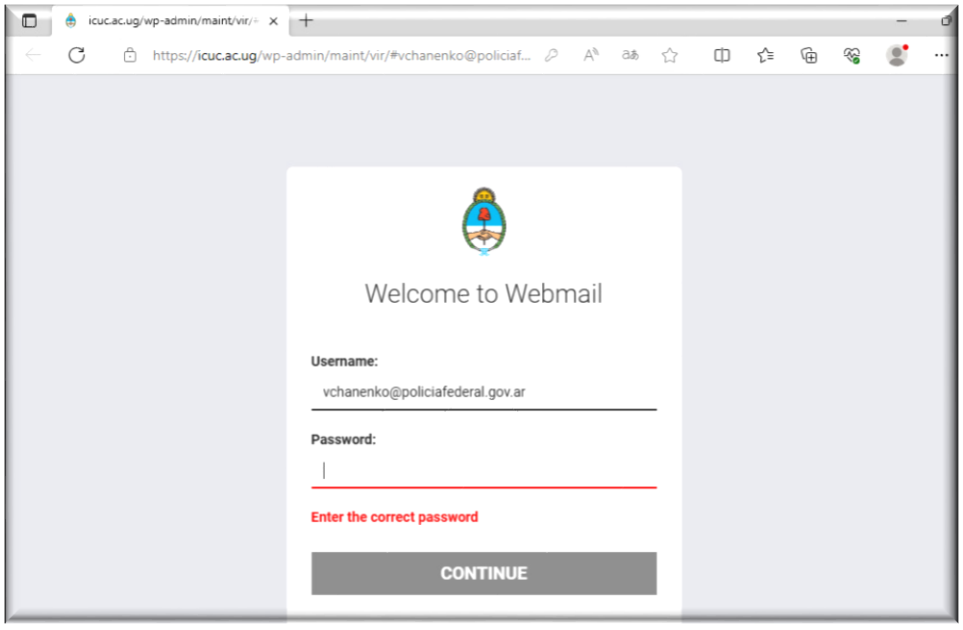

Imagen 4. Login fallido

Al ingresar la contraseña más de 2 veces para tratar de ingresar nos redirige a https://policiafederal.gov.ar.

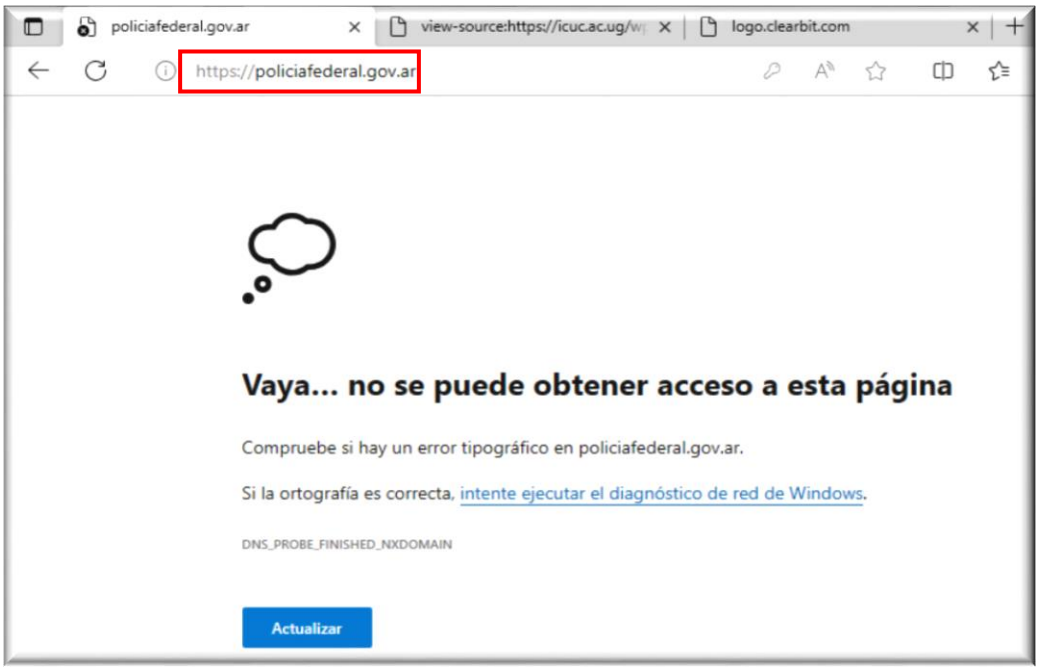

Imagen 5. Sitio al que nos redirige.

Al hacer clic en el segundo enlace nos redirecciona a la siguiente página web, la cual es verídica:

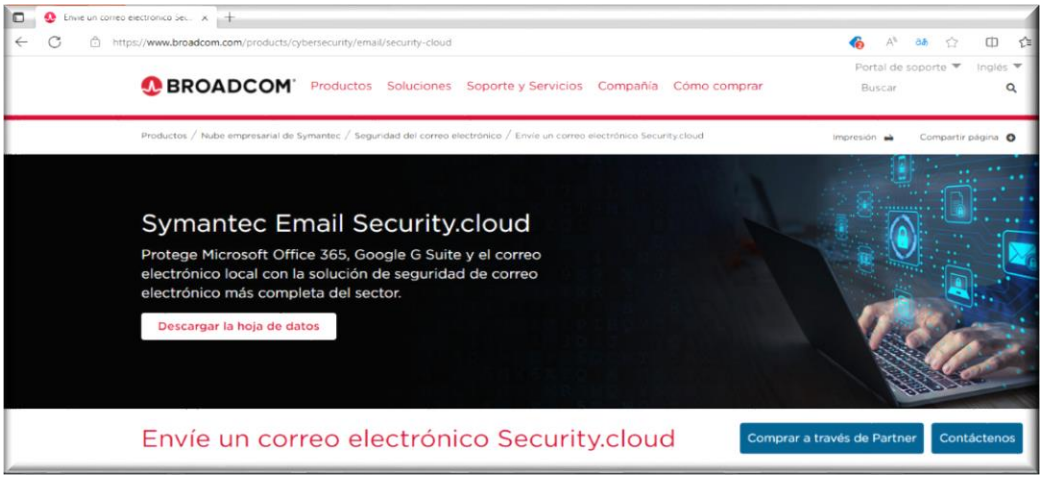

Imagen 6. Sitio al que nos redirige.

Se procede a analizar con diferentes vendors el sitio web del primer enlace arrojando el siguiente resultado.

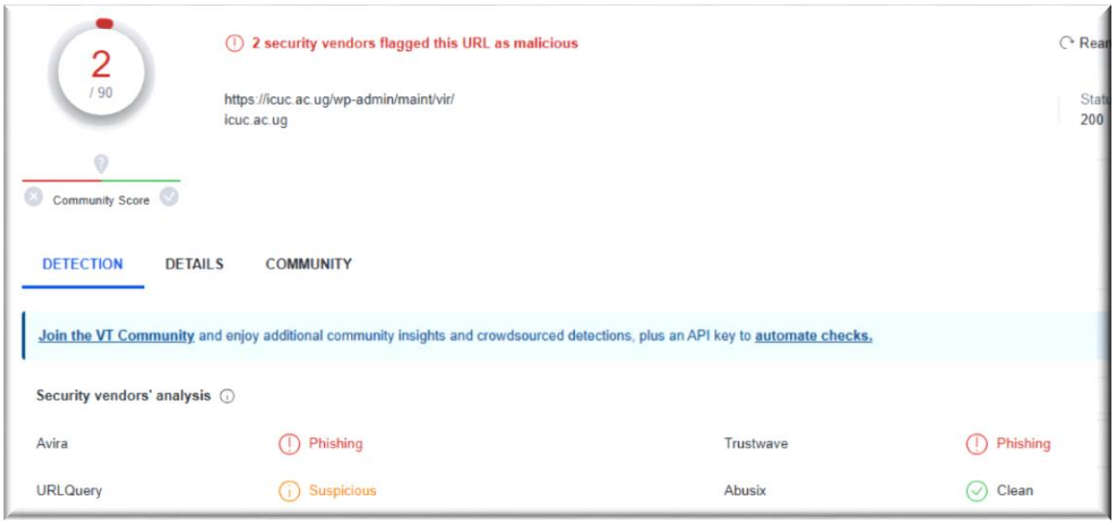

Imagen 7. Reporte del sitio web del login.

Conclusión

En base a lo expuesto en el presente informe, se afirma que el correo electrónico remitido desde **"georgina.crewe@acenet.co.za**" hacia la casilla de Policía Federal **"vchanenko@policiafederal.gov.ar"**, se trata de un Phishing, este es un tipo de ciberataque en el que los estafadores intentan engañar para revelar información personal como contraseñas o datos financieros a través de mensajes falsos que parecen provenir de fuentes legítimas como bancos o empresas reconocidas.

Asimismo, se puede observar que en la página web del primer enlace el campo **"Username"** ya está completo con el mail de la persona a la cual está dirigido, contribuyendo a ser más engañoso.

Se recomienda que, al recibir correos de dudosa procedencia, no ingresar a los enlaces o archivos adjuntos y en ninguna circunstancia complete los datos solicitados, 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 sigan siendo víctimas de este tipo de engaño.