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)

25/11/2024

Introducción

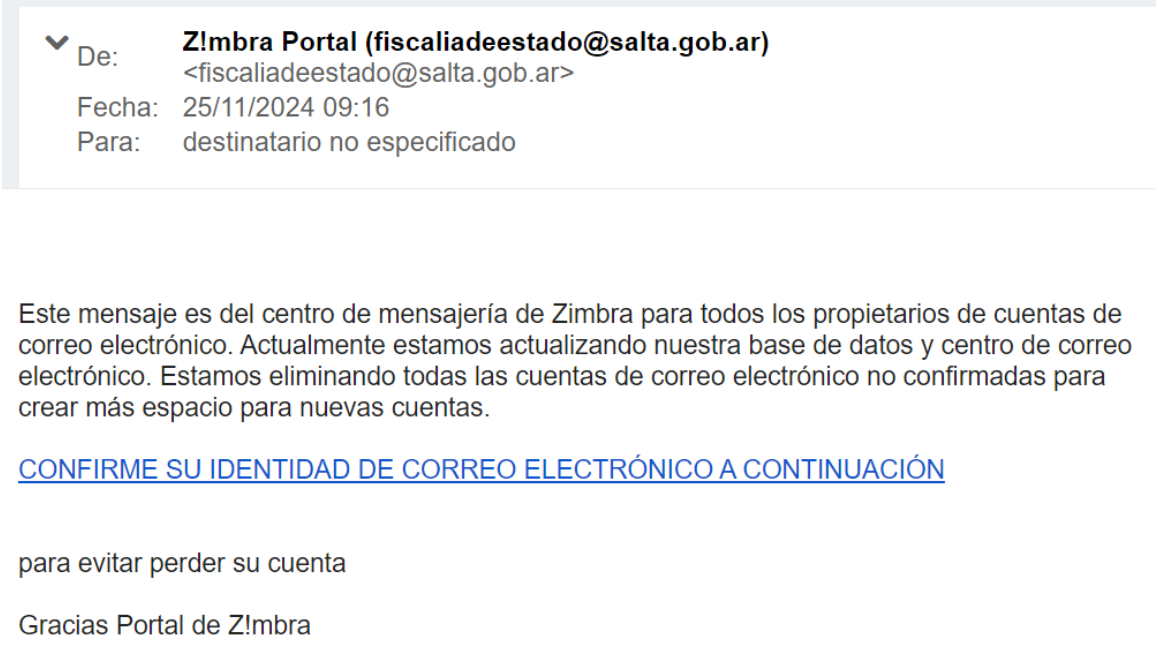
El 25 de noviembre de 2024, se recibió un correo electrónico que se presenta como una notificación oficial del “Portal de Z!mbra" enviado por el correo oficial de la fiscalía de estado de Salta.

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 creador del cuerpo del correo utilizó una cuenta con el dominio oficial del Gobierno de Salta, lo que nos indicó que la cuenta de correo fue vulnerada y con ello los atacantes lograron difundir su intento de Phishing a cuantas cuentas pudieran, ya que recibimos un total de 413 correos a diferentes cuentas institucionales. El contenido del correo fue elaborado de tal forma para que el usuario acceda a un link y este lo direccione a un sitio web idéntico al de inicio de sesión oficial del sistema Zimbra, con la finalidad de obtener credenciales de acceso al sistema Zimbra.

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 "Fiscalía de Estado de Salta" y que incluye un link en el cuerpo de este, se revisarán aspectos clave como los encabezados del correo (del cual se presenta imagen), el link adjunto y el análisis de la autenticidad del remitente, junto con la identificación de posibles intentos de phishing.



De: **Z!mbra Portal (fiscaliadeestado@salta.gob.ar)** <fiscaliadeestado@salta.gob.ar>
Fecha: 25/11/2024 09:16
Para: destinatario no especificado

Este mensaje es del centro de mensajería de Zimbra para todos los propietarios de cuentas de correo electrónico. Actualmente estamos actualizando nuestra base de datos y centro de correo electrónico. Estamos eliminando todas las cuentas de correo electrónico no confirmadas para crear más espacio para nuevas cuentas.

CONFIRME SU IDENTIDAD DE CORREO ELECTRÓNICO A CONTINUACIÓN

para evitar perder su cuenta

Gracias Portal de Z!mbra

Imagen1. Cuerpo del correo

Análisis del Encabezado

El análisis del encabezado no revela irregularidades ya que fue enviado desde un dominio oficial, lo que nos sugiere que la cuenta de correo fue vulnerada:

Servidor de Correo Desde:	correo.salta.gob.ar	**Servidor de Correo a:**	correo.policiafederal.gov.ar

Imagen 2: Análisis de la cabecera del correo.

Los puntos de interés para este análisis son:

1) **Remitente y Dominio**: El correo se envió desde la dirección "fiscaliadeestado@salta.gob.ar", que corresponde a un dominio oficial del Gobierno de Salta, lo cual no concuerda con la entidad que dice ser, el "centro de mensajería de Zimbra".
Esta discrepancia es un fuerte indicio de suplantación de identidad (phishing), ya que una institución oficial no utilizaría el dominio gubernamental argentino (.gob.ar) como centro de mensajería de una herramienta de código abierto.

Mail Server From:	mail.salta.gob.ar
Mail Server From IP:	45.235.88.83
Mail Country From:	Argentina
AS Name From:	SERVICIO ADMINISTRATIVO FINANCIERO DE LA GOBERNACION

2) **Campo "Mail From"**: El campo Mail From del correo señala la dirección fiscaliadeestado@salta.gob.ar. Ninguna entidad gubernamental utilizaría el servicio mail oficial, para realizar comunicaciones de terceros. Esto nos indicó que el remitente no está enmascarado, por lo que quien tenga acceso a esta cuenta de correo, la está utilizando con fines maliciosos.

Mail From:	fiscaliadeestado@salta.gob.ar
Mail From Name:	Z!mbra Portal fiscaliadeestado@salta.gob.ar

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 (salta.gob.ar), lo que significa que el mensaje fue enviado desde un servidor autorizado para ese dominio.
Sin embargo, dado que el contenido del correo y el dominio no tienen relación directa con la Policía Federal Argentina, estos resultados no garantizan la legitimidad del remitente ni del propósito del mensaje. Solo confirman que no hubo manipulación en la ruta de envío.

X-FEAS-SPF	spf-result=pass, ip=45.235.88.83, helo=mail.salta.gob.ar, mailFrom=fiscaliadeestado@salta.gob.ar
X-FEAS-DKIM	Valid
X-FEAS-Client-IP	45.235.88.83

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

MxToolbox - Email Headers

Análisis del Link Adjunto

El correo contiene un link adjunto en formato de hipervínculo con la referencia "CONFIRME SU IDENTIDAD DE CORREO ELECTRÓNICO A CONTINUACIÓN" (Imagen 1).

La misma fue analizada y se encontró que ha sido previamente reportada como una URL maliciosa.

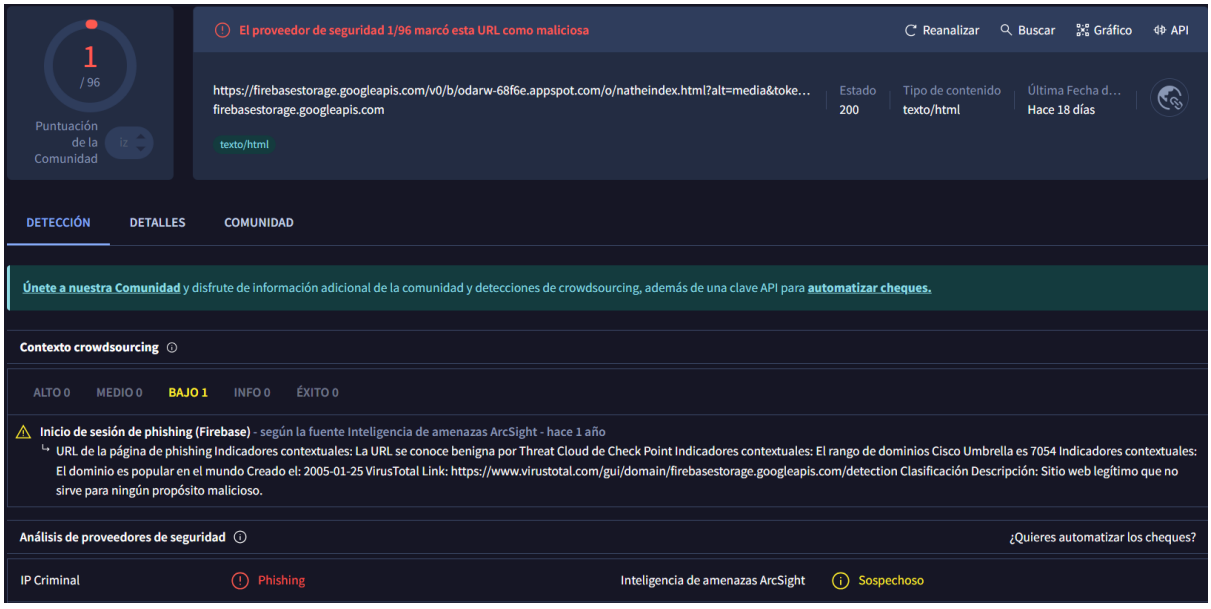


Imagen 3: Análisis del archivo adjunto en Virus Total.

Luego se realizó un análisis a través de un entorno aislado, donde se accedió de forma segura al link y nos encontramos con la siguiente página web:

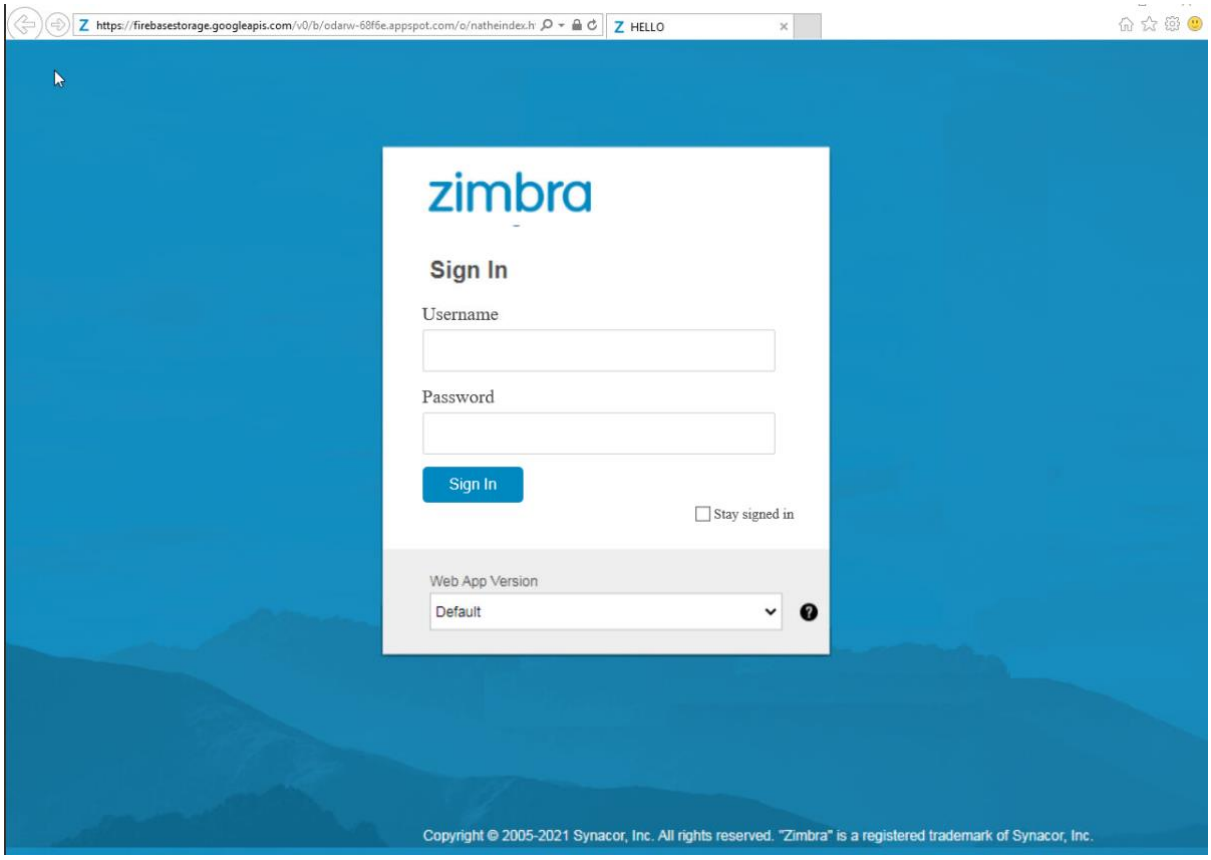


Imagen 4: Sitio Web falsificado.

Se puede observar a simple vista que la URL de la página en la que estamos claramente no es la correcta para el sitio, por lo que concluimos que el sitio fue falsificado. Ya que el sitio oficial de Zimbra se muestra de la siguiente manera con la siguiente URL “mail.zimbra.com”:

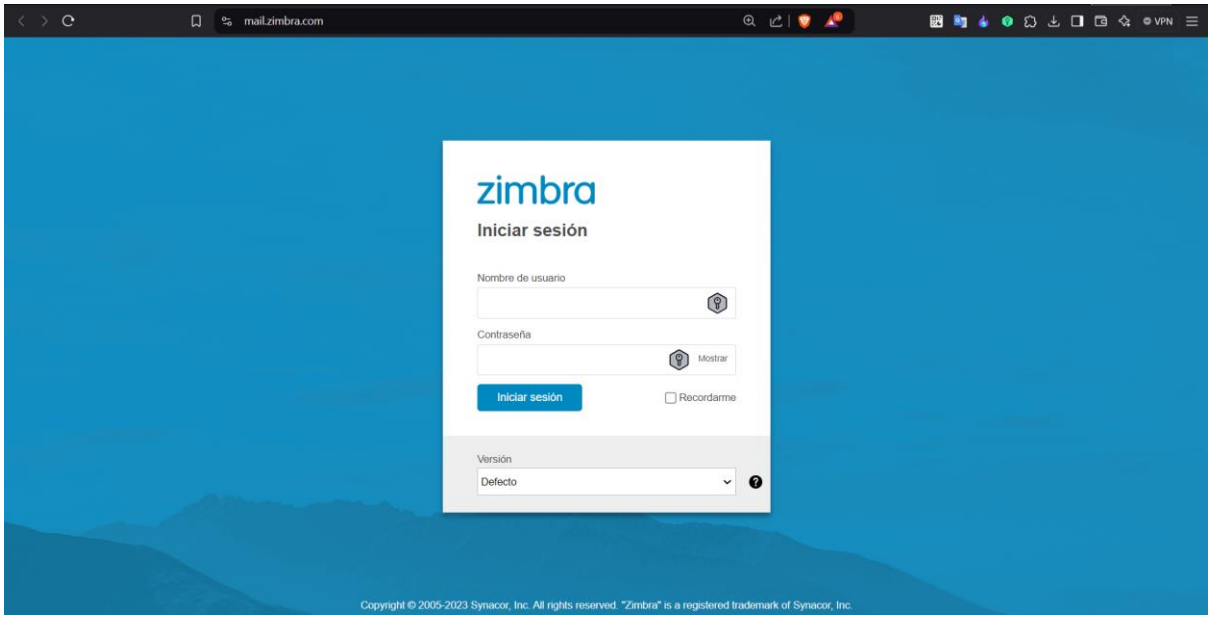


Imagen 5: Sitio Web legítimo de Zimbra.

Posterior a la verificación del sitio, se introdujo un usuario y contraseña aleatorios, para ver como se comportaba el sitio:

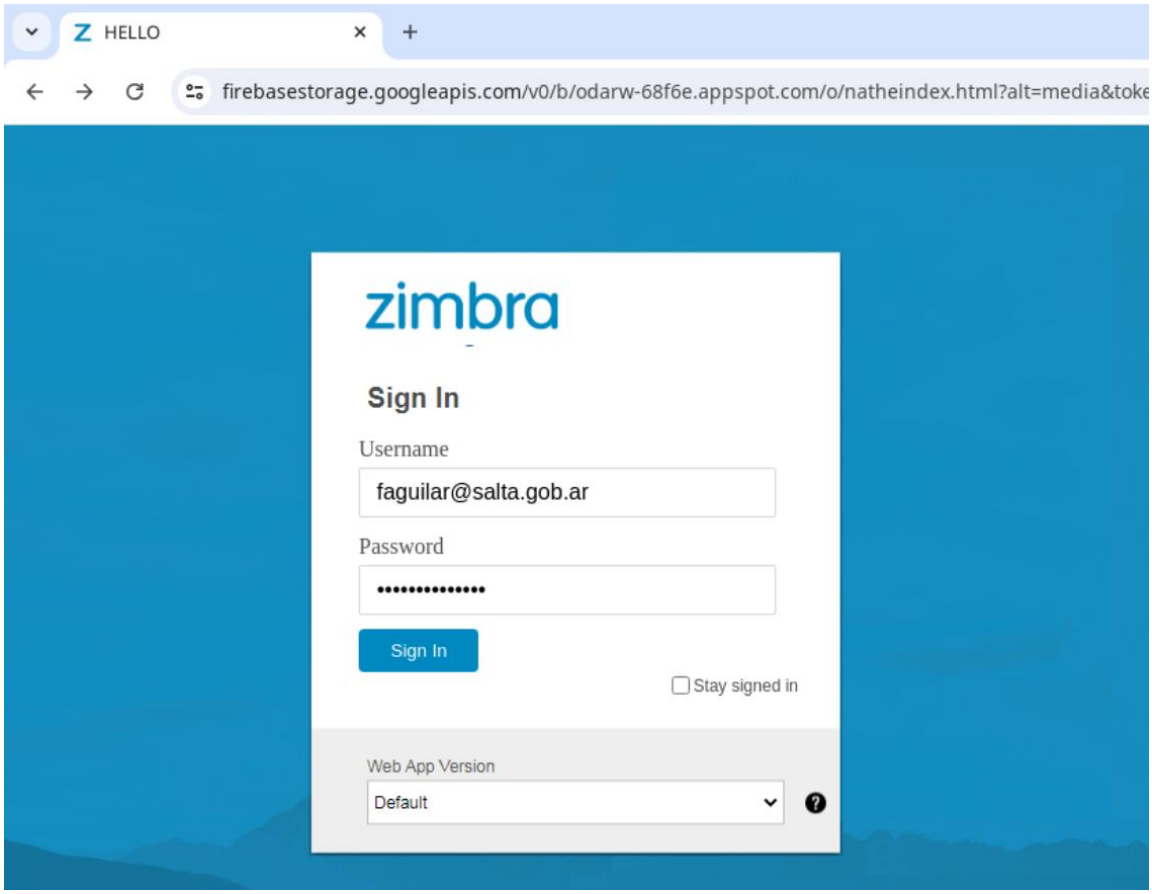


Imagen 5: Prueba de credenciales en el sitio falsificado.

Luego de ingresar las credenciales aleatorias e iniciar sesión, el sitio quedo cargando sin fin.

Imagen 6: Sitio cargando luego de ingresar credenciales.

Luego de observar este comportamiento del sitio, comprobamos que claramente es un indicador de que el sitio no es legitimo y fue creado con el objetivo de robar las credenciales del usuario final.

Conclusión

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

1) **Remitente comprometido:** El correo fue enviado desde una cuenta oficial del Gobierno de Salta, lo que indica que la cuenta fue vulnerada y utilizada para propósitos maliciosos.
2) **Contenido sospechoso:** El mensaje intenta suplantar al sistema Zimbra, utilizando un enlace malicioso que redirige a un sitio web falsificado diseñado para robar credenciales.
3) **Comportamiento del enlace**: El análisis del sitio vinculado muestra que fue creado para simular el inicio de sesión oficial, confirmando la intención de recolectar información sensible.
4) **Redirección a un sitio falsificado:** El enlace adjunto en el correo es malicioso y dirige a un sitio falsificado diseñado para robar credenciales, por lo que no debe ingresarse en ninguna circunstancia.

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 link 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.