Alerta de seguridad informática	8FPH20-0087-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2020
Última revisión	06 de Enero de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico que intenta engañar a los usuarios del correo electrónico corporativo Zimbra.

El correo informa sobre una supuesta expiración de contraseña en 2 días. Para evitar que esto suceda, el usuario debe seleccionar el enlace adjunto. Al seleccionar “Conserve mi cuenta”, la víctima es dirigida a un sitio falso del correo corporativo donde se le solicita el nombre de usuario y contraseña.

Observación
Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

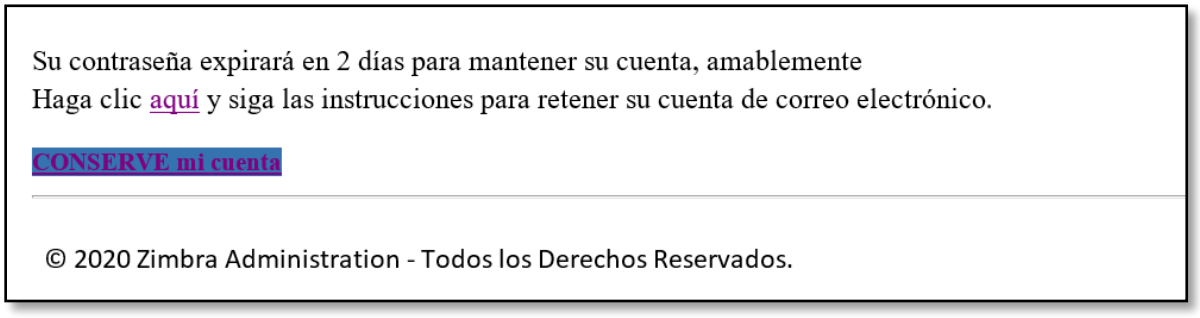
Url's:
https[:]//moremusclemethod[.]com/login[.]php

Smtp Host
[198.38.91.78]

Sender
interna@correo[.]com

Subject:
Actualización de caducidad de contraseña

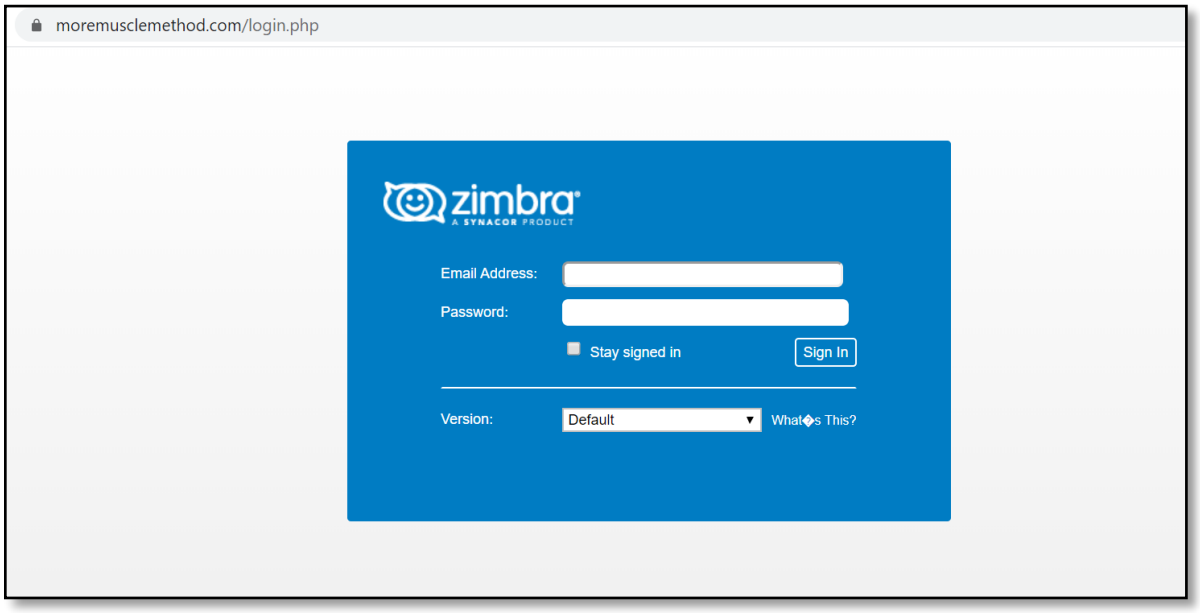
Imagen Phishing Correo


Su contraseña expirará en 2 días para mantener su cuenta, amablemente
Haga clic aquí y siga las instrucciones para retener su cuenta de correo electrónico.

CONSERVE mi cuenta

© 2020 Zimbra Administration - Todos los Derechos Reservados.

Imagen Sitio Web



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas
- Visualizar los sitios web que se ingresen que sean los oficiales

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.06 19:25:33 -03'00'