Alerta de seguridad informática	8FPH22-00539-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de junio de 2022
Última revisión	09 de junio de 2022

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.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una campaña de phishing vía correo electrónico que proviene, supuestamente, del administrador de Zimbra. En esta campaña, los delincuentes indican falsamente a la víctima que: “La contraseña de su cuenta de correo web de Zimbra ha vencido hoy” Para ello, el atacante solicita mantener la contraseña actual y actualizar la cuenta de correo web de Zimbra en un enlace que adjunta en el mensaje. Al ingresar, la persona es dirigida a un sitio falso, semejante al login de Zimbra, donde se expone al robo de su usuario y contraseña (credenciales).

Observación

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

Indicadores de compromiso

URL sitio falso:
https://zimbradesk11001.weebly[.]com/

Asunto:
Su contraseña de correo electrónico de Zimbra ha expirado hoy

Correo de salida:
mdpm07990@gmail[.]com

SMTP Host:
[209.85.218.43]

Otros antecedentes

Certificado Digital

Fecha Válido	:	21-11-2021
Fecha Término	:	17-11-2022
Emitido	:	DigiCert TLS RSA SHA256 2020 CA1

Datos Alojamiento y Dominio

IP	:	[199.34.228.53]
Número de sistema autónomo (AS) IP	:	27647
Etiqueta del sistema autónomo IP	:	WEEBLY
Registrador IP	:	ARIN
País IP	:	US
Dominio	:	weebly[.]com
Registrador Dominio	:	Safenames Ltd SafeNames Ltd.

Imagen del mensaje

jueves 09-06-2022 9:44

Postmaster© <mdpm07990@gmail.com>

Su contraseña de correo electrónico de Zimbra ha expirado hoy

Para undisclosed-recipients:

FALSO CSIRT

ADVERTENCIA: REMITENTE EXTERNO

El remitente de este correo, es externo al Ministerio del Interior y Seguridad Publica. Si no tiene certeza de su origen, por seguridad, NO abra archivos adjuntos y NO haga click en enlaces (puede verificar el destino de un enlace, pasando el cursor sobre éste). Ante sospechas o dudas, reporte a la mesa de ayuda.

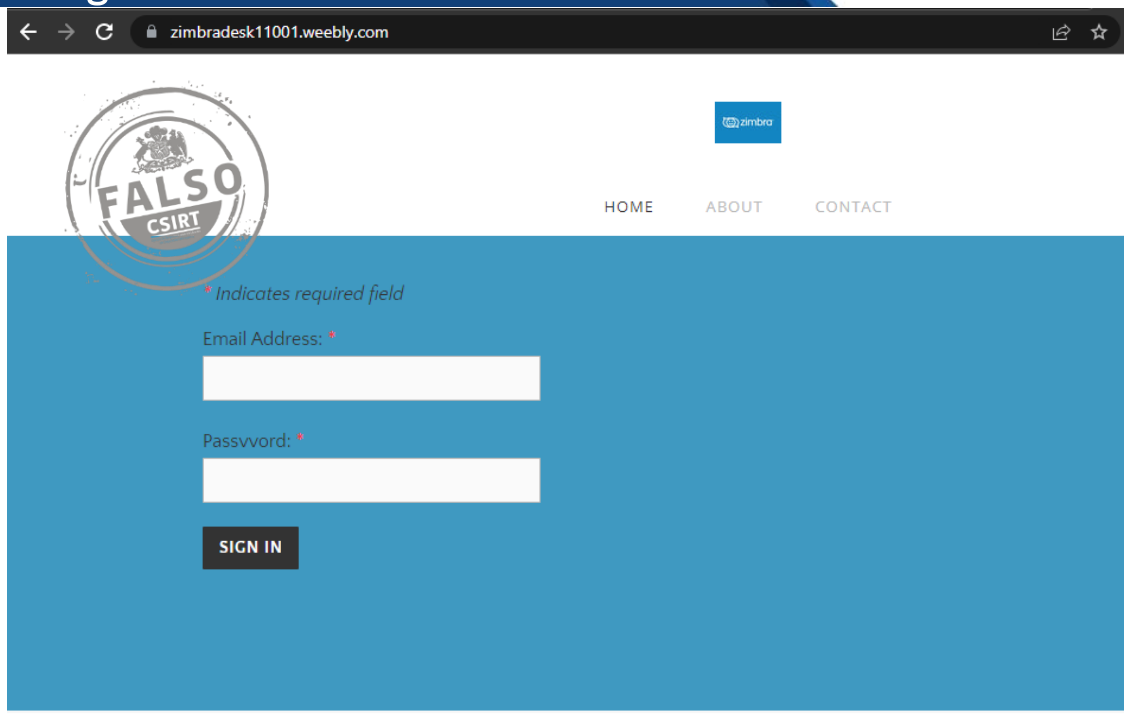
Estimado usuario de la cuenta de Zimbra

La contraseña de su cuenta de correo web de Zimbra ha vencido hoy, por favor Siga los pasos a continuación para mantener la Contraseña Actual y actualice su cuenta de correo web de Zimbra. Haga clic en Conservar Contraseña Actual

Es posible que no se envíen más mensajes si no se realiza ninguna de las acciones anteriores.

Administrador Zimbra©
Soporte de mesa de servicio
Derechos de autor 2022

Imagen del sitio



Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- 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 sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.09 23:21:46 -04'00'