Alerta de seguridad informática	8FPH22-00608-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2022
Última revisión	03 de octubre de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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 nueva campaña de phishing vía correo electrónico.

En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente: *"Hemos actualizado nuestras funciones de correo web de Zimbra a la versión estándar de 2022 para brindarle un mejor servicio. Estamos eliminando todas las cuentas de correo electrónico no utilizadas del año 2021 y aumentando el tamaño del buzón a la versión estándar actualizada de 2022."*

De abrir el enlace, 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 redirección:

https://roaccessload[.]click/Web-Client-Upgrade/

URL sitio falso:

https://roaccessload[.]click/Web-Client-Upgrade/

Asunto	Correo de Salida	SMTP Host
Actualización de cuenta	wcamargo@grupoasd.com.co	[190.60.225.13]

Otros antecedentes

Certificado Digital

Fecha Valido	19 Sept 2022
Fecha Término	18 Dec 2022
Emitido	cPanel, Inc.

Datos Alojamiento y Dominio

IP	[34.105.31.161]
Número de sistema autónomo (AS) IP	396982
Emitido Etiqueta del sistema autónomo IP	GOOGLE-CLOUD-PLATFORM
Registrador IP	ARIN
País IP	US
Dominio	roaccessload.click
Registrador Dominio	https://namecheap.com

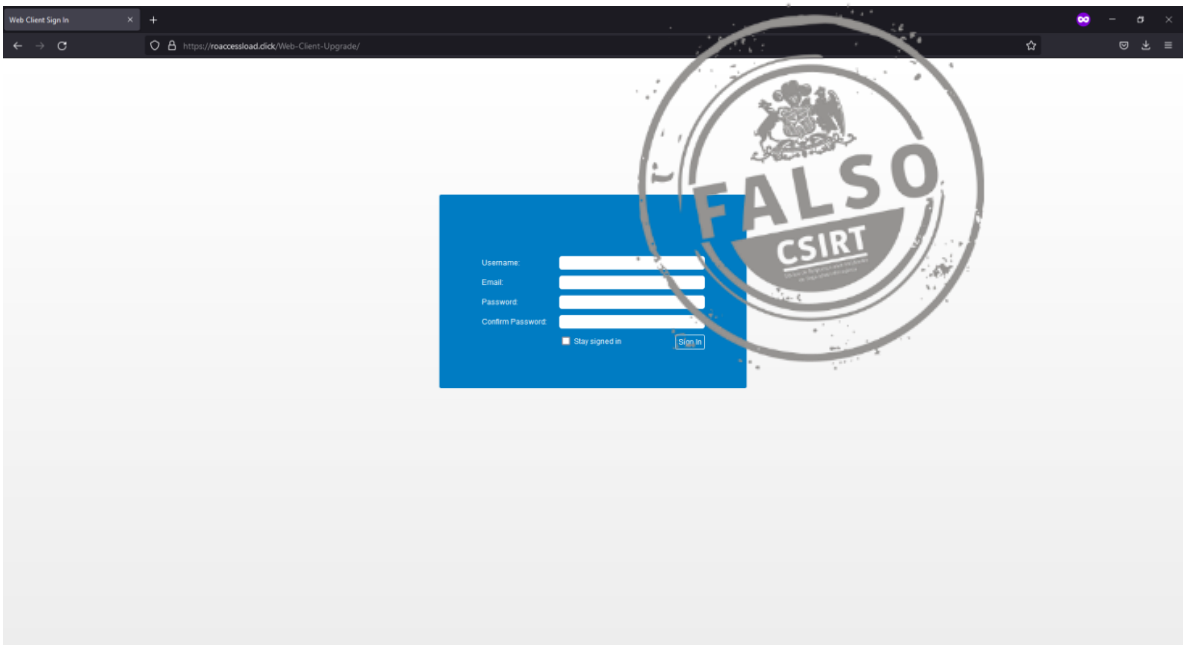
Imagen del mensaje

Actualización de cuenta,

Hemos actualizado nuestras funciones de correo web de Zimbra a la versión estándar de 2022 para brindarle un mejor servicio. Estamos eliminando todas las cuentas de correo electrónico no utilizadas del año 2021 y aumentando el tamaño del buzón a la versión estándar actualizada de 2022. Para disfrutar de este servicio y continuar usando su cuenta Zimbra, se le solicita que verifique su cuenta.

Haga clic aquí e INICIAR SESIÓN para verificar su cuenta

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: 2022.10.03 16:08:06 -03'00'