Alerta de seguridad informática	8FPH-00075-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2019
Última revisión	11 de Diciembre de 2019

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 supuestos mensajes bloqueados producto de que el buzón habría sobrepasado el límite de espacio de la cuenta. Los estafadores persuaden al usuario para que seleccione el enlace de “actualizar ahora”. Al seleccionar dicho enlace, la víctima es dirigida a un sitio falso de correo 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:

http[:]//bdmzip[.]co[.]uk/wp-admin/Zimbra/login[.]php

Smtp Host

[76[.]74[.]187[.]78]
[119[.]59[.]107[.]83]

Sender

admin@apccas2019regis[.]com

Subject:

Webmail Requiere actualización

Imagen Phishing Correo

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: 2019.12.11 17:42:01 -03'00'