Alerta de seguridad informática	8FPH22-00564-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de julio de 2022
Última revisión	20 de julio 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 campaña de phishing vía correo electrónico que proviene, supuestamente, del correo Zimbra. En esta campaña, los delincuentes indican falsamente a la víctima que su cuenta de correo electrónico alcanzó su límite en la base de datos y para evitar que se bloquee debe ingresar al enlace disponible en el mensaje. Al ingresar al link, la persona es dirigida a un sitio falso, semejante al correo 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

Urls sitio falso:
https://trzimbrawebadd.weebly[.]com/

Asunto:
Notificación Muy Urgente De Zimbra Admin IT Service Desk

SMTP Host:
[201.238.220.15]

Otros antecedentes

Certificado Digital

Fecha Válido	:	21-11-2021
Fecha Término	:	17-11-2022
Emitido	:	DigiCert Inc

Datos Alojamiento y Dominio

IP	:	[199.34.228.54]
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

miércoles 20-07-2022 10:49

Notificación Muy Urgente De Zimbra Admin IT Service Desk

Para Undisclosed recipients:

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.

Atención: usuario de correo electrónico de Zimbra,

El almacenamiento de su cuenta de correo electrónico de Zimbra ha alcanzado su límite de cuota en nuestra base de datos, para evitar ser bloqueado **HAGA CLIC AQUÍ** para aumentar el límite de almacenamiento de su correo electrónico de Zimbra y proporcione todos los requisitos necesarios. De lo contrario, se cerrará temporalmente su buzón de correo de Zimbra.

Administrador de la mesa de ayuda de Zimbra
Zimbra un producto Synacor
Apoyo técnico
Copyright @ 2022 Todos los derechos reservados.

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: 2022.07.20 16:10:58 -04'00'