Alerta de seguridad informática	2CMV22-00350-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2022
Última revisión	26 de septiembre 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware.

En ella, el mensaje es enviado desde una dirección de correo personal, y en el correo el atacante habla de una supuesta propuesta de oferta.

Si el usuario interactúa con el archivo adjunto, se encontrará con un archivo que se asemeja a un PDF, pero a través del cual el atacante puede obtener un listado de los servicios que se ejecutan en los dispositivos remotos y en los dispositivos de la infraestructura de la red local, incluso aquellos que pueden ser vulnerables a la explotación de software remoto.

.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto	Correo de Salida
PO 2209-0651	kim@merperle.shop

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre	SHA256
PO 2209-0651.zip	1808ff7039d835ecfd81803d6c1f8e6115e63c6df76fc94095d7bb7de1060cda
PO 2209-0651.exe	c56318c1a198033aa2b413978062cd8ecc805cac7951551b9cd8be94b3350a3c
Hsmpqaej.exe	fa163f94d25970b412b0bbb5a233af3e7d79f63fe843ea3df9052a9cf1902d40

IoC URL

URL
https://cdn.discordapp.com/attachments/1022102382827548685/1022696052064796713/Hsmpqaej_Zznxxbyy.png

Imagen del mensaje

Dear : Mr/Ms

We are pleased to enclose herewith our P.O for your attention and further action.

Kindly reply this email to indicate that you have received the P.O

Thank you and best regards.

[redacted]

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: 2022.09.26 13:06:55 -03'00'