Alerta de seguridad informática	2CMV2-00310-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de Agosto de 2022
Última revisión	9 de Agosto 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) ha identificado una campaña de phishing con malware. El mensaje es enviado de una dirección de Solutionmakers, en el cual hace referencia a una venta de servicio. En el correo se adjuntan tres archivos, uno en .PDF y dos en formato .xlsx. Estos últimos contienen un programa malicioso (malware) que al descargarlos y ejecutarlos (abrirlos) se produce la infección del equipo.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto
ودبی ـ الـ ریـ اض دورا ت(Cursos de Riad y Dubái)

Correo de Salida
ahmed@solutionmakers.online

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: ar-plan-2022.xlsx
SHA256: 20044bc3515379b70e4d42b57ff3ac32d5b590a0d185c8b5da2cea830f3368ed

Nombre: en-plan-2022.xlsx
SHA256: 2e72514a05ff383452a3dc1f1a8be040c3a1ebc23a224dc480064322efb85eb7

Nombre: mime-part--43583-43993.pdf
SHA256: 401eb0cdb84e642291539b684b9da7128c07ec540649753a7ae4e72b8f1910b3

Imagen del mensaje

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: 2022.08.09 15:18:18 -04'00'