Alerta de seguridad informática	2CMV21-00213-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de agosto de 2021
Última revisión	18 de agosto de 2021

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 de Gobierno) ha identificado una nueva campaña de malware. A través de ella, el atacante busca persuadir a las personas para descargar un archivo adjunto y ejecutarlo en su equipo, donde gatillará la infección con malware. El mensaje del correo suplanta a la identidad de la Universidad de Chile, con el pretexto de una falsa cotización.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores Smtp
cp31.cpanelhosting.rs

Correo Electrónico
[office@scor.rs]

Asunto
SOLICITUD DE OFERTA (Universidad de Chile) EUI894/CL463

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : SOLICITUD DE OFERTA 18-08-2021·pdf.rar
SHA256 : CF319EF6390C70A7EA468A4FB14F6AEEC8CB708C8621E9CCACF482E564C24715

Nombre : REQUEST FOR OFFER 18-08-2021·pdf.exe
SHA256 : 00BD94F5DC7EB6E30CFE1DB9E7E7E6538C34768A6364D5B5D0F07209FB94F650

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: 2021.08.19 11:36:15 -04'00'