Alerta de seguridad informática	2CMV21-00192-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2021
Última revisión	10 de junio 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 del Gobierno de Chile (CSIRT de Gobierno), ha identificado una campaña de malware que suplanta a la empresa Sodimac. Con ella, el atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.

El mensaje del correo indica que, supuestamente, se debe confirmar los datos para realizar el pago correspondiente. El atacante adjunta un archivo con extensión .ZIP, el cual contiene a su vez un archivo .EXE que al ser ejecutado gatilla la infección del equipo.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores Smtp
[mail.kultura.by]

Correo electrónico
estebanrodriguez@123mail.cl

Asunto
procesando pago

IoC Archivo Adjunto

Archivos que se encuentran en el correo (W32/Injector.EPMJ!tr)

Nombre : Factura de proforma.zip
SHA256 : B64B2AFDCF32D3FC94A528A988E814C33FC99BB934ADF70181C7F6322403C43B

Nombre : Factura de proforma.exe
SHA256 : 99D45C44F4DDBA585C9773157BCAF3ED4897C6ADC0BB46F8C141D5D09A6C05E9

IoC URL

www.moodandmystery[.]com
www.s-immotanger[.]com
www.joomlas123[.]info

Imagen del mensaje

Hoy las finanzas prepararán el pago. Por favor reconfirme los datos bancarios adjuntos para el procesamiento del pago, ya que no lleva el nombre de su empresa.

Esperando su confirmación urgente para proceder en consecuencia

Saludos,

José Ignacio Pizarro Concha

Licitador

Subgerencia Administración, Licitaciones y Compras

Gerencia de Administración y Control de Gestión Chile

Pdte.Eduardo Frei Montalva 3092 Renca, Santiago de Chile

Celular: +56 9 39274111 - Oficina: +56 2 2738 1242

SODIMAC
Juntos Construimos Sueños y Proyectos de Hogar

Los Mejores Lugares para Trabajar
Great Place To Work. CHILE 2020

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: 2021.06.10 16:55:29 -04'00'