Alerta de seguridad informática	2CMV22-00354-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2022
Última revisión	03 de octubre 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 (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware. En el correo malicioso, el atacante habla de una cotización para que la victima caiga en su engaño. También el victimario pide confirmar el precio y la disponibilidad de los productos y el periodo de entrega, adjuntan una lista con los supuestos productos que necesita.

Una vez habiendo interactuado con el archivo adjunto en el correo nos encontramos con un programa malicioso llamado Agent Tesla, un RAT (troyano de acceso remoto) que puede asimismo desplegar otros tipos de malware. Además, realiza numerosas operaciones de espionaje, como el registro de lo que se digita (actúa como un keylogger), la toma de capturas de pantalla, la sustracción de contraseñas y cookies de múltiples navegadores web, además de robar información de correos electrónicos

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto	Correo de Salida
Solicitud de cotización	juanmorales@gmail.com

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre	SHA256
Solicitud de cotizacion.zip	def80745672b71f12f1abb6e98c4e4ca8ed86937bd34f6990702162e65814d58
Solicitud de cotizacion.exe	7a86925eea6d198fb22db8c38502b2cdf4def0f39505d855f66579e2fefa4ce4
GISV.exe	e9d9dbaf6675d4f9ce01ad9dbe355979a4d5f64d1f2237214578e0ebe3e937e7

Imagen del mensaje

Buenos días [redacted]

¿Puede confirmar el precio y la disponibilidad de los productos adjuntos?

Háganos saber el período de entrega y cite su mejor precio FOB en la lista de productos adjunta según lo requieran nuestros clientes.

Su respuesta será apreciada pronto.

Sinceramente,

[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: 2022.10.03 17:21:55 -03'00'