Alerta de seguridad informática	2CMV22-00353-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de septiembre de 2022
Última revisión	30 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 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 phishing con malware. En ella, un mensaje es enviado por los delincuentes desde una dirección de correo de la empresa Enertik, y en él se habla de una posible compra de unos artículos

Se adjunta en el email un archivo .img, que en realidad contiene un archivo .exe, el que de ser ejecutado despliega un malware de la familia Agent Tesla, que actúa como info stealer, pudiendo sustraer contraseñas de correos y de navegadores, realizar capturas de pantalla, y registrar las pulsaciones de las teclas (como un keylogger).

Observamos el empleo de siete tácticas, entre las que podemos encontrar: acceso inicial (phishing), ejecución (el usuario ejecuta un fichero malicioso), persistencia (agrega una llave de ejecución), evasión de defensa (desofuscacion/ofuscación de archivos o información, modificación de registros), acceso a credenciales (captura de credenciales), descubrimiento (enumeración de archivos de sistema y descubrimiento de llaves de registros) y colección (colección automatizada para recolectar información del sistema y colección de correo electrónico).

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto	Correo de Salida
Ordenar	info@enertik.ar

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre	SHA256
Payment copy_00000988.PDF.zip	8f3295bfd93ef5affb09b0f2c5ccde4aa33b0c94c117cbfb4b09045fe6201d3e
Payment copy_00000988.PDF.exe	2f33e37286a03dee0a89bbac812d166203e5ddb1f6c2571110a08690a0df1bd0
nBFb.exe	5ebaba50a78cc3750b1f00750110d368b9522f96939a5d89a5dcc63a346add16

Imagen del mensaje

Hello [redacted]

Payment completed on behalf of my boss. Please confirm receipt .

as i will have to return to my boss with feedback

Thanks

Regards
[redacted]

----------Forwarded message---------- ----------

From: bruce.zhu
Sent: 28 September 2022 09:25
To: ACCOUNTS < [redacted] >

Cc: [redacted]

Subject:Re: PAYMENT FOR INV

Hi Denise,
Please find the bank details (attached) and Please forward the remittance details to their email ID [redacted] for confirmation.

Regards.
[redacted]

Sent from my iPhone

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 17:37:47 -03'00'