Alerta de seguridad informática	2CMV21-00193-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de junio de 2021
Última revisión	16 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 difundida a través de correos electrónicos supuestamente proveniente de la Tesorería General de la Republica.

En el email, el atacante busca persuadir a las personas para descargar el archivo adjunto y lograr que este sea ejecutado. Para ello, el mensaje del correo indica falsamente que existen obligaciones tributarias que se encuentran impagas. El atacante adjunta un vínculo donde el usuario es direccionado a descargar el malware y ejecutarlo en su equipo, donde gatillará su infección.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores SMTP

[135.181.43.175	-	server10.novidadedanets.com]
[95.217.182.245	-	server07.novidadedanets.com]
[95.216.171.205	-	server08.novidadedanets.com]
[135.181.43.87	-	server09.novidadedanets.com]
[135.181.44.248	-	server06.novidadedanets.com]
[195.201.98.138	-	server02.novidadedanets.com]
[195.201.99.101	-	server03.novidadedanets.com]
[195.201.99.112	-	server04.novidadedanets.com]
[195.201.99.227	-	server05.novidadedanets.com]

Correo Electrónico

www-data@server02.novidadedanets[.]com
www-data@server03.novidadedanets[.]com
www-data@server04.novidadedanets[.]com
www-data@server05.novidadedanets[.]com
www-data@server06.novidadedanets[.]com
www-data@server07.novidadedanets[.]com
www-data@server08.novidadedanets[.]com
www-data@server09.novidadedanets[.]com
www-data@server10.novidadedanets[.]com

Asunto

Tesoreria General de la Republica TGR
Regularizacion de un pago no ingresado N
Regularizacion de un pago

IoC URL

https://almadenysusrincones[.]com/wp-forum/imagem/
https://ladiesunlearning[.]com/campers/ixrrbt/900GO10206STS3.zip

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : 900GO10206STS3.zip
SHA256 : ED2BC65531659CBFB937975F088D2560E741BAF4001EEBE44065E9254BADE683

Nombre : 00F30S97823025OSD.msi
SHA256 : 0097E775B3ED33D109E970472D5F8FD5D76CAA2D28E42419BC2C8154033649AF

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: 2021.06.16 17:28:31 -04'00'