Alerta de seguridad informática	2CMV21-00195-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2021
Última revisión	22 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 se hace pasar como proveniente de la Tesorería General de la Republica. El atacante busca persuadir a las personas de descargar el archivo adjunto y ejecutarlo.

El mensaje del correo indica falsamente que existen obligaciones tributarias que se encuentran impagas. El atacante adjunta un vínculo que, si el usuario hace clic en él, descarga un malware, el que de ser ejecutado en el equipo gatillara su infección.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores SMTP

[103.30.17.62 - envio01.novidadedanets.com]
[103.30.17.54 - envio02.novidadedanets.com]
[103.30.17.55 - envio03.novidadedanets.com]
[103.30.17.52 - envio04.novidadedanets.com]
[103.30.17.56 - envio05.novidadedanets.com]
[103.30.17.26 - envio06.novidadedanets.com]
[103.30.17.32 - envio07.novidadedanets.com]
[103.30.17.9 - envio08.novidadedanets.com]

Correo Electrónico

www-data@envio01.novidadedanets.com
www-data@envio02.novidadedanets.com
www-data@envio03.novidadedanets.com
www-data@envio04.novidadedanets.com
www-data@envio05.novidadedanets.com
www-data@envio06.novidadedanets.com
www-data@envio07.novidadedanets.com
www-data@envio08.novidadedanets.com

Asunto

Notificacion TGR.

IoC URL

http://treasuredmemoriesportraits[.]com/webgit/imagens/?28706&_mbox=Junk&_caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0

https://www.mediafire[.]com/file/343krzblh084yph/VER__0588744558fCA.zip

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : VER__0588744558fCA.zip
SHA256 : D951401CC332CCBC7BE8B50512D13061162FD99E80E11947942273DBDBB4A437

Nombre : VER__0588744558fCA.msi
SHA256 : 77E19EEB9AC37EFB541EF647F401A372F5ED2098690156AE6A42AE65B906DEA6

Nombre : -.dll
SHA256 : B3B6EE98ACA14CF5BC9F3BC7897BC23934BF85FC4BC25B7506FE4CD9A767047A

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: 2021.06.22 19:21:47 -04'00'