Alerta de seguridad informática	2CMV20-00055-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Marzo de 2020
Última revisión	24 de Marzo de 2020

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), ha identificado una campaña de malware a través de un correo electrónico que cuyo supuesto remitente sería la compañía de Courier Chileexpress.

El mensaje del correo indica que tienen en sus depósitos un pedido a nombre del receptor del correo. El atacante dispone de un código y un enlace para que la persona pueda obtener más información sobre el envío. Al seleccionar el enlace la persona es dirigida a un sitio donde se descarga un archivo ZIP, el cual contiene un archivo Html que al ser ejecutado direcciona a otro sitio donde se descarga de forma automática otro archivo ZIP. Este, una vez que es descomprimido, permite obtener otro archivo con extensión MSI. Al ser ejecutado, se gatilla un script y se procede a la descarga el malware.

INDICADORES DE COMPORMISO

Servidor Smtp
www01[.]subtraverse[.]intra [138.229.82.138]

Sender
apache@www01[.]subtraverse[.]intra

Asunto
Chilexpress - Tenemos un pedido en nuestro deposito en su nombre

Url's
http://voxpopuli[.]com[.]ar/site/wp-includes/customize/--/https[:]/www[.]chilexpress[.]cl/?cliente=
http://104[.]41[.]36[.]91/0091024871289/0009201940192[.]ogg

Hash MD5
6cc06e2f71aaf392fb12da494c8294d4
c00f05300eab399ac2ac6a448714aae5
f54c6fa901539fc160b1a7d2e35e3243

IMAGEN DEL MENSAJE

RECOMENDACIONES

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- 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.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.24 18:40:25 -03'00'