Alerta de seguridad cibernética	2CMV21-00265-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de diciembre de 2021
Última revisión	30 de diciembre 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.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) comparte una serie de Indicadores de Compromiso (IoC) obtenidos del análisis realizado a múltiples campañas de phishing con archivos adjuntos que contienen malware, los que están circulando en el ciberespacio nacional y representan un riesgo para los sistemas informáticos, así como para los usuarios en general.

CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Observación

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

IoC hash

Hash SHA-256 de los archivos adjuntos en los correos electrónicos:

N°	HASH	Tipo Malware
1	883d702af603ae021218da994040382660c48ecd76bac4be1a8e670881b17082	MSIL/Kryptik
2	71a0e72a83e3a8df998aedc83fbbbcdf261000b34f37cf10fa9f432a7cc4b70f	W32/Generic
3	a02968737104558993a408e3629fa7d7907065998d2c9749c9ce829e549a0670	MSIL/Zilla
4	1f15e558398fde6bac4830d5c4558ceecfc16a93702d30ce99e2ec9f6441c90d	FSA/RISK_HIGH

IoC nombre de archivo

Nombres de archivos con código malicioso:

N°	Archivo Malware
1	SHIPPING ADVICE 4081791001.zip
2	NEW ORDER CF211-24400.r00
3	Product Inquiry Catalogue.gz

IoC servidor SMTP

Direcciones IP de servidor SMTP. Se debe tener consideración que podrían aparecer direcciones de Servicios Cloud reconocidos, ya que este apartado informa desde donde salieron los correos electrónicos maliciosos.

N°	IP	Etiqueta de sistema autónomo	ASN
1	2.56.59.69	AS-SERVERION	AS 399471
2	2.58.149.105	AS-SERVERION	AS 399471
3	2.56.56.64	AS-SERVERION	AS 399471

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: 2021.12.30 09:25:40 -03'00'