Alerta de seguridad cibernética	2CMV20-00117-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Diciembre de 2020
Última revisión	15 de Diciembre 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.

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), 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

9de7df8b38954c9d93fa69070d28d5b587d1ede9193fbc0c0a6a565955a88fbd
f469d7a84ba48d8c9a9ae5bfbfa38b708a74d330a2507a7a527d8eb32c0c40af
5de89393ff5a01bf9f790962c2cc5298c289ecaf99ca78611a86fa90c9d9b58b
99975fa5c19cbe2b174de1f227beadd6c04256e1428bea86491f965cdbe90cd8
ea9976cebb98e32374c7bc02123b185169c27232abe3578a39001451b4b27bfa
81d7d4b3560d7ad69ac41afd0bf67d99a3986d9704754b11221e6a67a2630829
33dcdaad80453451ab94299814bdd08766436af6f79bc1b19f7c05335e85ddc5
5491593e9f76a18a85972662a47de82ac3786b473faa05a88518ebaef57bc1e3
6dcdd0af7032e97516308bf8f6b0d8a75f69697ac34ff9ac567716fc35192cff
0a9e3fa71406b6678645937c466c02d671138b2eb449419001cf16e08dc960f1

IoC nombre de archivo

Nombres de archivos con malware

Items Order_pdf.gz
msg9054.pif
PO 952109.Img.zip
PO..xlsx
Purchase order10025153.zip
Quotation No. 233.xlsx
scan_098.rar
signed sales contract.rar
SWIFT_OUT_Confirmation.gz

IoC servidor SMTP

Direcciones IP del servidor SMTP de donde fue enviado el correo

79.110.52.195
37.120.206.112
45.137.22.56
62.36.20.208
23.83.133.171
51.79.157.206
193.56.28.122
98.137.64.146
98.137.65.32
98.137.66.147
98.137.65.206

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

Aboutmile@bremileintl.ga
jessica@vortexfield.eu
service@lhexagoneso.com
ivilopeZ@Orange.es
sales@jetfleetmgmt.com
sales6@nomila.com
sales@esteelsuppliers.com
invex@retemail.es
maigranada25@yahoo.fr
marni@pt-dju.com
harikrishna@vijayadiagnostic.in

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: 2020.12.16 09:17:17 -03'00'