Alerta de seguridad cibernética	2CMV20-00118-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Diciembre de 2020
Última revisión	16 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

784a771a6c4bebd30e298277853632f485a14867a262295fe5dfd2c4087f6e97
7205dba904395dfb5f958d3a2781ed25ed9bcde885956ce34c2a0ec1b9ae55c6
476ec5a648c3159681feb1040aeffc59f4913d6f1fc29f8f5a03bd04be62694d
b48d12b7623bfed724e8d19c7d93fae540295f2490eaf3702be3d2a5a5751bc3
75dbeb9d3c43cf8ad17eca74dc39bd0d230731df3e37a5aa4cad4717bfd7e163
4524f84146912b008015a0baf214e6f950281d45278426ff183aa4ce6690da44
f2143634b15c89c84f9086c891c2bd51bd03411b625bfa43ba40a16836ed8cf3
d4f4e52c7ebf5c75e74ff3dcd32f2944e0595da63e9ee70541b83e1ccb80275c
5e201ff705d6225abee529b228670b2f9bce7a3cf5b99a7475c40df0a511caf2
af1c84e4a3c0f70d7871314c884366e7de3c23afad9594ffb6e04099deacb129
f554c01536217162995e590ef9c085a25a3af0f2857d3a20f27979fb67b7b2e7
892b3f9200b6dd5cb181cda7e006da91591ff3979efb27188754c6209b28b77b
632fe1c443696ff0f67adb10012caa948046f04ceae3d3e509921e368ae89cbe

IoC nombre de archivo

Nombres de archivos con malware

DHL Details.img
IMG-033-020.xlsx
mail1233.pif
NALCO SOA122020.r00
Order_BC012356.pdf.zip
Pedido 0045201512.7z
quotation 301086.gz
Shipping documents.html
ssdr_SOA2143083-pdf.html
TNT Express_xlxs.zip
USD44,880.65 Payment advice note from 15.12.2020.iso
Vessel particulars.zip

IoC servidor SMTP

Direcciones IP del servidor SMTP de donde fue enviado el correo:

79.110.52.195
23.108.57.65
40.107.80.57
213.236.3.9
210.236.45.1
52.162.219.104
107.150.18.142
198.23.221.43
204.44.127.166
142.11.194.202

IoC Correo Electrónico

Correo electrónico de donde fue enviado

Aboutmile@bremileintl.ga
info@semshred.com
GBVACCARO@voegol.com.br
rodolfo.torrillo@superdyop.com.ar
Noreply_Nalco_SOA@ecolab.com
e_dehghani@mehrarad.ir
trf.1850458928.2512675.9@informationservcies.hbsc.co.tk
webmaster@ft.dk
grutze2@yahoo.es
edwin@andalanfluids.com
0000718103@pccity.pccity.es
purchasing05@willing.com
19933o@dejazzd.net
sales1@mikronix-gauges.com
info@minlmax.com

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.