Alerta de seguridad cibernética	2CMV21-00138-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2021
Última revisión	25 de Enero 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), comparte una serie de Indicadores de Compromiso (IoC) obtenidos del análisis realizado a múltiples campañas de phishing con archivos adjuntos que contienen malware catalogado como **MSIL/Kryptik y Wacatac**, 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:

e785b9df7a3848de00d34c09968f29b9a60d2bc99d0a67b743beda66ecc1e534
30d2ab012c781742249e962105127383ca1a9511ee31e37ae9679156c8678414
4dc0440cf9d2fcf0be2a006dc6576fd946a71e0e18d826dfd2e458e8d3b03b3f
6704fb0e9569d0bf2fb207c045fae37fa2213f02a526678f2b09dbb608856cfa
86eb6cb673d76cf76312c584873effd76c4a12f73c98188e43a5e50aded5b381
b5c32583f3b2d083f603c516afef770c77e5b353a5972a3fa728dfb9bb8b352a

IoC nombre de archivo

Nombres de archivos con malware:

HTMY-209871640.zip
Payment_Advice_pdf.cab
RFQ for the supply of materialsservices for P.O. No. - 4700001838.zip
PURCHASE ORDER.zip
RFQ RPM202011-776JD.img
Quotation for T10495.zip
CONTRACT AGREEMENT.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.

160.20.147.181
23.227.199.25
94.198.40.46
104.168.144.234
154.16.67.6
103.141.138.130
185.222.57.238

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

marketing@oldtile.com.my
whybrta.control@wernerco.com
office@metreoxporters.net
tr@purfactory.pw
commerciale@tecnomill.net
accounts@primaryfreight.com
regulatory@hds.com.jo

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.