Alerta de seguridad cibernética	2CMV20-00095-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Octubre de 2020
Última revisión	13 de Octubre 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

25b871c94fcc1825b19de313875a06512f650480b6623ec678dee76732c52e0b
9448ce645e7ef7b92ff30c17421ed56b4f3bbe4fce2b4628a48b3cfa8ed02ac7
d5a68a111c359a22965206e7ac7d602d92789dd1aa3f0e0c8d89412fc84e24a5
c76a517fd1250e77c7bd26fe7223022d0e71bb2e75e3ca5c482face6185f1dc4
951056d1e8f319981af056a90c40242d9395e15514b1b1fd21b9195ecca86cf7
b8bd6daac2cd0522341b9ff441e1e2de2743cf81a5be741b85ada3ed846a44ab
986d13ef556fa85418e10e1d257128863978b00fdd6f472d7ea562fdb934fde5
2e2fdc459173a51caa1daf9e0ebb7fbfde276af0c0475e0976fc765f0c41a496
98b8260952aab2ef1951e2d44220099cbb7d9f41e6ae02d24263b37eb4f1940e
e12c89c9008e11dc9aa6a149891d1fb3fbd3ee36b3f8bac80678501ef84b55ea
a64a09207ffc6026ce5328160b8f03896fcf99591d9412882073b871e074e422
754043513b719af4582157adb569baa9b9576db59c2044360c1cfd64c55be667
707801ccfb066a8838ababb07c44745055f848a670c4bf5daa2cfbb5b26f0a76
fa6e36ba51f502c55fe5f336911f3b6ceb01c71b8dff340add249982a20d74ec

IoC nombre de archivo

Nombres de Archivos con Malware

L1452III-HASB-6582018-R02.zip
P01012.doc
Fechas de pago programadas.xls
ENQ-1303-MR-016.rar
QUOTATION_TEM PDF.GZ
QUOTATION.gz
P.O List (2).arj
IMG_20200921_213128_resized_20200921_095209264.img
HSBC Payment Advice 11102020_PDF.img
Order1008202009.rar
New Order - 87654456 Ref-FOB-Pdf.xz
PO.PDF.cab
PO#0014969.arj
Order List.arj
Company Brochure.gz

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

156.96.44.206
23.251.226.1
37.49.225.235
23.251.226.2
23.251.226.4
23.251.226.6
185.222.57.234
193.23.127.34
185.19.185.40
185.222.57.174
185.222.57.81
159.89.173.209

IoC Correo Electronico

Correo electrónico de donde fue enviado

Shinas@gmail.com
admin@grabenhorst.de
carlemau296pui@gmail.com
glenshan72nwudy@gmail.com
gunnclar77euhje@gmail.com
heroldsmith6@gmail.com
judivalo036weee@gmail.com
koepketemi17bukej@gmail.com
mayur.lad@timetechnoplast.com
pedugjuf5jvqy@gmail.com
pratmeshshetty@rustomjee.com
raymondjeffery316@gmail.com
rooneyleo1@gmail.com
sales@acetech.co.jp
sales@idealtech.com.my
sophia.le@sotrans.com.vn
virgpris800tvi@gmail.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.