Alerta de seguridad cibernética	2CMV20-00080-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Agosto de 2020
Última revisión	31 de Agosto 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

09fe3fdbea7c4614855237eb2a19b1efa3d204591a11eb2d0b2a34c4f30d9da9
0e46c07eeabe6829beb260251ed62eb4724d318954cb3ead3eb8bb8133f4f2bc
3209a985960e1272ea8f886f8096b103577aa5aa041150ee14c5445ad82cedac
ca35b7fab0b94484f4865d1804251255d5a5778567715d70496a11e76d26aeba
db0f02e7fe6714d6e101c8441b4b31e20929fd6cda45a6df3ab425341218b14d
e4023c3ed629d16ec28bf13929b329b798cbc0cc05aafa2abf04045d9209eae4
e71e6d04f1065ef25ec0c07652439fbd663c1113afd6314690a1b0d2c6dcae87
4d27b24408ccaed59ba5977e7e7309fc42fc9964bc4e3d4cd3ac363f1b539454
b15af175de8cf5d1a9527f047643f5039a1506dee07822e6d73746fc60d67dad
67d62b54619a4b53ddaebbacf6b88f623933cfe54340797a92c3012b65b8a11b
c8613cbe02f1e23ab87fcce103efa89cc8da78705c42ca373fa45f3d213b9f5a

IoC Descarga malware Urls

Urls que son disparadas por la infección inicial del malware, podrían existir otras ulrs no detectadas en este proceso.

hxxp://qstride[.]com/img/0/
hxxp://tskgear[.]com/wp-content/uploads/2015/06/pz/
hxxp://vermasiyaahi[.]com/cgi-bin/8/
hxxp://www[.]weblabor[.]com[.]br/avisos/QIU9/
hxxp://viniciusrangel[.]com/experimental/VIhMh1/
hxxp://westvac[.]com/wp-content/GOYx/
hxxps://viewall[.]eu/cgi-bin/SbhZP9X/

IoC nombre de archivo

Nombres de Archivos con Malware

Spare Part (KITO)_____.gz	INV.GZ
Payment copy.rar	file-2808.doc
PO.P.D.F.cab	Inv_9302.doc
SWIFT Invoice.P.D.F.exe	Orders.zip
TT Payment Invoice.P.D.F.exe	MENSAJE-2608-SF-9932629.doc
DHL Documents.PDF.cab	ZG6224479756XA.doc

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

104.148.61.170	104.148.61.178	104.148.61.165
92.223.93.162	103.146.234.10	104.148.61.168
139.59.89.144	104.148.61.171	37.48.85.221
104.148.61.175	104.148.61.173	173.212.242.213

IoC Correo Electronico

Correo electrónico de donde fue enviado

garyxu@icoolglobal.com	medinaluca1kntiu@gmail.com
sokgim.lua@ikano.asia	fadecice330motoy@gmail.com
glenshan72wcpo@gmail.com	itsupport.gopinath@newtoncsc.com
sales@tcfs.net.in	fantjame060pee@gmail.com
Daniel-Wei@co.ac.uk	lacejoly2muua@gmail.com
accounts01@shipping.sinosteel.com	sales@mickmgmt.com
patrhoyt29hejy@gmail.com	michcons458nacyo@gmail.com
wandaver2nygnx@gmail.com	klostocc091akiz@gmail.com
sawijama5qe@gmail.com	trojlita384qiqyi@gmail.com
fui.manak@mojaz.org	chris@admatehellas.gr

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.