Alerta de seguridad cibernética	2CMV20-00097-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Octubre de 2020
Última revisión	18 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

21bc812872cddfa29c1dcb0db414cc0a559b200a3d8cbe83efef1a07122c8004
22ea0b5c2d6063b3373459ebaeaa0afba86d58b99478fbb7bc647590ee30d120
2d7e11f92069a1e5ff5ff82a8329a325c0f6e92c46429a27ee17461fd9f426b7
3409ce10d406201a4281ac38585603be076bc59fca5d1758aac06588e8782953
42a54842a06394588bbe22eab0f96256525541b3dbe2ecccd9bc67c6c4284343
590e91cfd2bc7164b8528b3e845e9d45e8328e9148b90c0836936e9d870ca895
5b63a0b32df927fdda9e7a2c8730c690f0d87f2697a36f63b98788762f96572c
6e819ee6c03aab8939875b6ffef183f1d4ee5ef057cab7094bb4abf89ff14e2b
834c99c6f0597f45d28055ce9a2951ce353ee7b9e67520831b799e45a90ec5a1
8fd8974864c46a3f859de4c894933cf9e3eed6c0c38534e0f793992aa8b57f57
9b2897cb72eaf26ad63c4e2093f0afeaa5a5f2915fed7825a4c8c768e73b62cb
a99748fb8129ca164acdee8641b3798db2ec452ae25dec322b4bd05f4e97e28e
b0449f1a1e7963e13d2696b9a3dcba69e9d68128c14da75797d586c67ad89546
b62bd0aadb69c443f30026bc870ccb1bb790da1c7534c04f339a2999dc7edd98
b8cb6d816022529aef9c494f18a512773e78a79da62cd85b03e664fc6b801834
c29e0628b36f838a071e5cf4bdca821647bdd53dab36d762eb02a680f0bf5d03
c5962177a67fc29c23e2648a4a3b58c958c80f1ebe9ad2d08c290d1be03b16f9
f1e0f50f17affa292986ac15ad90bfd8837740f68789b7702249f8ec98dff5c8
fa28af9b6dfccbb9aee76563206a26fc06756830f7638fa308277ef50abbf3ce

IoC Descarga malware Urls

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

hxxps://newmoontec[.]com/wp-content/uploads/8R0lFV/
hxxp://kiasoo[.]com/dl/7y7I1V/
hxxp://malkaragida[.]com/content/Una/
hxxp://xiaolechen[.]com/pollinodial/5lTy0/
hxxp://mallowsvirtualcreatives[.]com/wp-content/2pw1/
hxxps://rfcrfc[.]com/wp-admin/oZ/
hxxp://bbs[.]rfcrfc[.]com/api/V/
hxxp://hoagietesting10[.]com/wp-content/SJ/
hxxp://iscamenabe[.]com/wp-content/1PR/
hxxp://vietmade[.]org/wp-admin/8/
hxxp://www[.]filamchimovies[.]com/wp-admin/8/
hxxps://strattonmobile[.]com/wp-content/yl/
hxxps://blog[.]qgdxzs[.]com/wp-admin/l/
hxxp://vietsex[.]pro/wp-content/PX/
hxxp://vastraindia[.]com/cgi-bin/YZ/
hxxps://sharansundar[.]com/upload/v5n/
hxxps://cmnivaria[.]com/wp-content/dXg/
hxxp://tsrj[.]monster/wp-admin/Hhl/
hxxps://hasem[.]app/storage/OM/
hxxp://musc[.]health/wp-content/h/
hxxp://ladylike[.]house/wp-content/B/

IoC nombre de archivo

Nombres de Archivos con Malware

50229_2020_C_63912.doc
Documento 20.doc
Orden de compra.zip
PO 28151..docx
BL_# BGI-O-10706858 and BGI-O-10709887.PDF.img
14.doc
Informacin 16 10 20.doc
Mensaje-102020.doc
Payment Advice.Img.ace
REP 775.doc
RP72366602E_COVID-19_SARS-CoV-2.doc
CT68756638V_COVID-19_SARS-CoV-2.doc
Documentacin octubre 2020.doc
Documentacin 10.2020.doc
Documento 10-20.doc
XG57626189S_COVID-19_SARS-CoV-2.doc
RY76-79 IF39631198.doc
FB61815806T_COVID-19_SARS-CoV-2.doc

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

181.45.254.35
116.68.206.195
52.58.173.206
72.52.244.66
83.149.84.75
187.9.217.130
116.202.208.87
210.140.45.44
89.201.7.75
203.101.163.77
190.61.250.140
175.107.196.160
83.149.106.4

IoC Correo Electrónico

Correo electrónico de donde fue enviado

gurban@viacorreo.com.ar
rdlstore2@radiancegroup-bd.com
omar.r@electro-sm.com
rakesh@shakunpolymers.com
startextile@cyber.net.pk
robikris22rupoy@gmail.com
fernayes9r@gmail.com
jonespatr72fegwt@gmail.com
fantjame060sp@gmail.com
lacejoly2yu@gmail.com
uzma.euroasia@euroasiachem.com
fadecice330durxt@gmail.com
judivalo036eer@gmail.com
polafutj1ok@gmail.com
quelenluis@playonne.com
kipemilf56crupd@gmail.com
polafutj1leqm@gmail.com
Straight2bank.SG@sc.com
sawijama5zfxaq@gmail.com
fantjame060e@gmail.com
kipemilf56yuah@gmail.com
ralpzand8gody@gmail.com
sugbsimo50acyci@gmail.com
ronasyre474rc@gmail.com
julio.almeida@pansul.com.br
wandaver2skte@gmail.com
solizbula031rfklm@gmail.com
ketcdutj170klyn@gmail.com
info@gsprint.gr
hon-hoan-h@crownpalais.jp
birojs@baltkonsults.lv
jolanta.guza@baltkonsults.lv
anittiff04pzbyz@gmail.com
liaqat.rehman@pil.com.pk
cv@printhouse.com.ar
devlinrobb1s@gmail.com
kashif.sajjad@cyber.net.pk

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: 2020.10.18 16:11:53 -03'00'