Alerta de seguridad cibernética	2CMV21-00136-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Enero de 2021
Última revisión	21 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 **EMOTET**, 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:

5a17dee61b79152ce451f560a17603b291bd0934b4c0bdb69a3328fca8b36771
743b0489a94f04569f1dd9ea1c62d1d5d6ce22b642369e87f974b3635990edb8
11e1780e215a952185315253632033b1e42e269f59252e80ccc002e7ed15c086
c4f94c6960792fe6e062b42c6c149482152a96588a9a5b9c3f7c4a35c974ac50
4142cfc2bb8a067a21c0439bef1d08e1742025b00b3cb1c9619ff7bf0a2b42d6
1fa18e851ad74226caf71eaca19ccba3ba2b1457521c4a4fbe6ba07fb3008333
17420055c7c1b85137e8f5e78a7eab811ae1b4f00b33ce05590e19399286fe2f
fb4541bb676e36bc08711601b21c85ec6a0eec67fa65a2ac53a7e70a8f01c628
75d4b326ca471055fba9d3e4dfbb994e191135130d15f7f1e75fa6a8346bf89d
1b2b0f6f229f819f49cefa1af565aa4e83bf8b1f9df047bebfa9143dbebbb349
51d0ab773047ebaac512a5d397e79534ac5b266afd4ee691d6356a8bd7fe4b11
3602f8e737829acb355fceaf51908fe8a199a2ae44099cedd08d3cb298fc8b53
58bd78843e708ee76feee70fd020e5e0ff29c4ad4df2aebbd48ca6d587b15912
0f0061b80732fc11150a67c1807a75989ce897eb2be6e22d425c4b41f88f98ee
c84de615620cd1a69411f262b2f431ac07909b7705e43c1a97d80f5bfdc3ea33
57c0a7e0c8c758419617cbb0493789572ffd9bad491e5e98ecb0754de052efe3
fafa1cf428d6c5e3cc4e6538a098ed38e2ffbd8c9dc5ea06313648aafe2fa0a4
5f6d69e58850b0965c708c5e8cbf7f3f0a769a42c33abe4a82595f903ad92dbe
922d235666c1b57e9aff2834a273334b7e72c3963d98f1a4d8d02287c540a997
849af1e2dd0cefe909b1e37a24266f716af4687eab7ace3bb9bc28c921c4f999
a6b87278bb77d9a04427862b72b0c109e770f31d1c6c6da47644a2dbd82cad11
fcb1b3759243a11409e9c374d7feef2bd785139f1871e23eb04a745e492b0d84
0ded59b8e793df139715fe181350639f9f92855d28917d5321a8c7ee5ca178dd
13fa691fa4a6d36f4aa041d3159233a3272fe9d6a2837dfafa1a34235833221b
8a4ec0ca950a390ef42dca2eba4cb2baea9d9239ab969b07b0596fa2e601e01c
bd207412e6350e4c7e0f4149a5e2e5f607193dbd98360ec8e696ef42cd6ba4ad
3fe9826f416743be9ec86023808b246c046a0384db9c9c81268ce8fd008c792d
24ff39d73f1df07521eae970f57ccb4c214adec5a1a9e3941890abea7f59810b
4d972e37eedaf19d2f0e71ed55568cce27b0860e54906c5442ca69c2e2f0d360
54accdc2c15133ddabb1dd67159f363044ec299963688259f2947ef9b8160093
f773095273ff78e1678a13fcec9c17b2cce0412f13c0f12e09cdd6173ffc82c3

IoC nombre de archivo

Nombres de archivos con malware:

FCY425003.doc
N05387.doc
M6092461816.doc
A7W5-000277.doc
TD_009625220334.doc
#000941357199.doc
#90003899978.doc
MY CV.doc
Purchasing Inquiry.doc
UO8732500035AC.doc
81261305900029.doc
5TE-00074930.doc
OUG-010121 NNI-012021.doc
426233805179109.doc
MSD-010121 YWL-012121.doc
Scan Jan 20, 2021 at 04.23.doc
LWH-010121 FMD-012021.doc
NQ2258986300BH.doc
OCP_086161072.doc
#N100062693035134.doc
#WF0005985.doc
#0038019536453.doc
S66851.doc
#HEGO0001725983.doc
U_00421.doc
#ZM000223.doc
CN-0006283.doc
#G0WY00688.doc
VJ5765506190GI.doc
FACT - Jan 20, 2021.doc
dokumento O114.doc
FA# 01212021.doc
Scan Jan 20, 2021 at 06.59.doc
CHL-010121 ITQ-012121.doc
Scan Jan 20, 2021 at 06.35.doc

IoC descarga malware URLs

Comunicación de los archivos adjuntos de los correos electrónicos al ser ejecutados:

URI Activas

http://dryaquelingrdo[.]com/wp-content/SI/
http://bardiastore[.]com/wp-admin/A1283/
http://fabulousstylz[.]net/248152296/TpI/
http://abdo-alyemeni[.]com/wp-admin/seG6/
https://www.oshiscafe[.]com/wp-admin/5Dm/
https://nimbledesign[.]miami/wp-admin/C/

URI No activas

http://oxycode[.]net/wp-admin/x/
http://giteslacolombiere[.]com/wp-admin/FV/
http://trendmoversdubai[.]com/cgi-bin/B73/
http://covisiononeness[.]org/new/F9v/
https://lionrockbatteries[.]com/wp-snapshots/C/
https://www.schmuckfeder[.]net/reference/ubpV/
http://cirteklink[.]com/F0xAutoConfig/1Zb4/
http://xunhong[.]net/sys-cache/D0/

IoC dropper de las URLs

Archivos descargados de las Urls (Nombre - Hash):

Hash Sha-256	01e14d7d7d88ef53d4f9443170bff682dc9c72f13451c18c9032a5e440975e98
Nombres Archivos	OmpmNskPc2Z1B.dll B067rLs.dll d30XfEjjvzSGryn.dll rjvUeL.dll PMnkirII19stYbz.dll N5jOe82Si.dll

IoC Comando Control

Tráfico Comando Control (C&C)

12.175.220.98:80

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.

69.89.20.226	114.31.72.17	62.149.158.132
192.185.50.93	207.21.192.5	69.89.25.95
216.10.244.214	103.45.230.198	62.149.157.216
172.104.61.201	103.120.176.28	62.149.157.214
168.95.4.114	62.149.157.213	219.99.187.7
162.210.70.184	62.149.157.212	189.126.112.61
162.210.70.2	62.149.157.215	181.31.135.145
162.251.83.181	198.71.225.36	193.56.28.234
175.107.198.7	69.89.29.114	217.74.103.244
50.116.124.69	201.76.49.59	116.202.193.189
170.249.199.130	62.149.156.87	145.131.7.81
162.252.57.42		

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

silvia.almaraz@loubet.com.mx	finance@pinstarauto.com
christian.sagadraca@nfc.gov.ph	mail@libertylease.nl
visas2@siecindia.com	seiaprod@seia.cl
vikki.tambe@sysnetglobal.com	3d@threenarrewarren.com.au
dnduw@nduwsfamily.com	info@caa-ingenieria.com.ar
ych512@ms75.hinet.net	toanbui@benhvienranghammat.vn
asif@regrowz.in	submission@najmedicine.us
gemma.miaventilation@miachina.net	info@turismoproclusone.it
walaa@metrofiresystems.com	esperanza@protools.mx
pedidos@laveiga.com	progettazione.p@rossini1969.it

zahid@roshnimm.com
sherrera@makler.com.ve
jean-yves.lameyse@paris.notaires.fr
ehernandez@decimas.es
compras@josehuespeehijos.com.ar
Samiuddinr@hotmail.com
SHALEY.NG@ienergy.com.sg
accounts@stopl.in
n.gouveia@qualiconsig.com.br
spg@spgbrindisi.it
ruben@granimarloranca.com
branchmanager.skp@shaheen-traders.com
r_kakita@hamaoka-industry.com
recruitment@shengtai.co.th

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.