Alerta de seguridad cibernética	2CMV20-00116-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Diciembre de 2020
Última revisión	14 de Diciembre 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

52ccb3c0fdf5a051df5ba003ce61ffe915ecf257bd9d68297648ab5b086a3d0d
4c91df648f693ae2debf244e2c420e33a1bc64fe7e93a52eaa0667e9a9fbd708
6d7b3f594dd9ab03414918168e22ffb656b5c247a1b9f0c87070d12b5f4a81fd
9d55d503a67cb2737b27c0ea77bda519f470fa55053c1cb981b39fce2268dc5e
2886e712b761941f8ee425aef938e646c7f402d96ae5a7bbe65dd67bd26f616f
8f054ae222c2b0e317e614335ddb5e35590f6669191805e0e0c6961b92570ed7
8a5d1545a4f74c34fb41ff8ea74d35aa53d30742bac51ea30c9bf6d49c4eb59b
999e7a8df9428ff11ece63a95ba76bfe4b401cd476e62cc5760972307106ebf2
c28ab91f1ba16035aa3c83299f2e6e3cc642c5fd2c6049a6d764d24342f09b24
88a285f950e2e3cf1252b5765349b663b041f25cdc0543ac37a3c389ffd2b721
7123697173acfb4a007517ac817c37baa4f845bd8f57c972b9a554655f8746a2
55cd40119050214a5b6d4c0cec5a53b45ac687f7e721909f5017c4d546868e00
abdf5b91c52e3318ab4837fab1658c87c6dba52aacd267fdf9db67a68c597f44
3ecc2dc3ca4976a798f1aa3b6b050a4bec65f4cd21ad3818cd748df2cb446733
98b40fa7dffdf75b7d25aa8359a00d5a52c47fd0acc6e20c2ad26a734681c4fe
110138c714087e37609b57da0143acb1c498553837302349ac8b01b06d26d90b
d1a0be9963f086960034166c0f85601a720fbcf3f3d361e6102f7eb6123a4199
349f95f8838f5defa6bf105b34530664b52cb3d041fa7ddfd4f881d75b1b5ff5
742386b285d1ca558bb4d0aca6b30df36b83866e36fd9d26b680cff721de0182
8413f5b1c07582de5020575251ad37dce44d725ce0a04cf1b6ca446063f3f3e4
ae84be04120bc075561e75f8becdbd693773a020f90ae0fc3693ff2b0d72f78b
180bed3d9b16d8da10d85078b967ea926838a4ecded1e5779d7d5306105cd0c7
bb4b4d36e73143f13e28e331cb6392007041874f7fd65c770dc74414f37f647c
6823554e87d94f940123caa646a156231e4c37a4fce1d696c25f65252e6b483a
be79443c0b4eaf793c5513f47bb589a57cd734dd8467272baf612b21894cae8a
eece226f5fc0fb7b309f30c682f2f5616a82170998d1306d89c6d8753664d497
800ae626585bcd63a5bbbb43e3047846bc792110736a273941a89c7ebcc1a4e0
edd079134004b9585cc1f49712b760be6b82922b9c950cff0c3b70c0df7c3802
0ca02b271e05470bab38ce94781f906d7a549e479670db85cbc24b82111c8533
2335dd98b0f7c6310c2a0473eb5a2ee46bf473f960382b9d50a4972fad5597a4
d5c990d38188b6cbf497c2cb4f1498d0ca7045b2379475ce7db3b2bdcb1b947c
22fe1af79a86c8514131fa8f9ae5c913101592a0f7ed9ecd3d3c18d9097691b5
4319771cc6f5370499167b30b80e76e333204fbe70428ca39492c0af19749f78

cb23bcf0d2b097cafd9ba420dfdbbd995e882ffa0f2a22c73966a7e54e55947c
8df34f6c5dca55e6dbc826b143f5471df7c79748e2ac9c9a141fa7c43498179c
729429c708e71d2fd3a5e8f1ae48df56c3967c71ca75c46254bce5fe52ba01fe
995f2f30b23dc76600c4c54fb572dbc35230a036d76d129143c5f61a23df1e1a
9de4d094d14083a2655427dcc8314013cf28b7116b7c7f3eadd5f3d4561daff9
0b82357aecfede97b3cfadee8a9c8be165bcb361d2af5054aa809ddcda70f01b
72243306a41b6f1cd5a13e3097805ffdb0c6d49bcb92497d130ba7c42d521da0
29503850c8b7ba352544c70cee1f7bb2bcf60e67aca4d3677be6c4f44ae812b7
1c7b7a542859113679131de1ac7797a4a65c0650811682010e990ce2eae9538b

IoC nombre de archivo

Nombres de archivos con malware

SAMPLES.zip
Remittance advice PDF.zip
Invoice and Packing list IMAGE.img
RFQ 11054-14122020.gz
PI _GSG-PA-201209.gz
Enquiry.xlsx
DHL Express (Consignment Notification).gz
NL-NL20201027IN.gz
Inquiry.r01
New_order.html
ekey.pdf
powarna .pdf
RSAKJHZZ2U4ZIF.pdf
G75CEUTSE0H.pdf
4718.pdf
ipvre.pdf
briOdF.pdf
3981128653.pdf
chaugepa .pdf
Carta de pago 1 pdf.zip
DHL AWB #887397327783_____PDF__324.r13
CbWX.pdf
emkadefgiosimitem .pdf
GYWOYEKW1U5ELL2.pdf
5TZRR.pdf
Pjddf.pdf
hapy.pdf
VVX6.pdf
5FW3JUG5Y.pdf
H0VH16UUNHV.pdf
contetedva .pdf
6661235714834.pdf
lDcTAY.pdf
inlirucdemuspadi .pdf
538551915926.pdf
93274981557.pdf
7IMN0X49OMGN4EF.pdf
fdKLx.pdf
XHvy.pdf
YP5LQ.pdf
Attachments.zip

IoC servidor SMTP

Direcciones IP del servidor SMTP de donde fue enviado el correo

98.137.69.84
98.137.65.84
95.216.63.47
98.137.65.148
98.137.65.31
206.189.118.13
5.8.93.86
84.38.132.53
45.137.22.125
45.137.22.51
84.38.132.107

IoC Correo Electrónico

Correo electrónico de donde fue enviado

awhazicoo2@yahoo.com
Sudheesh_Poyil@mazruiholdings.ae
sale5@ankainflatable.com
claudio.stella@msg.it
dept3.shabbir@alriaz.com
waves@richermoren.gq
jmtc.import@jaipur.ae
sales@multiimpact.com.my
purchasing@iconjamaica.com
thaodud5pr@hotmail.com
nicola5dswamp@hotmail.com
kataraquejj@hotmail.com
blainebr07l@hotmail.com
meridith3sdom@hotmail.com
calvinmjjs@hotmail.com
hyepfv0sb@hotmail.com
devorabav7@hotmail.com
omar@primeglobaldubai.com
mjjimenez@novasoft.es
parisru0s@hotmail.com
flickcolwadman@hotmail.com
cmaisonmf5@hotmail.com
mickqcrgrappe@hotmail.com
gregs7zynu@hotmail.com
irinauhsegur@hotmail.com
lailayrayl5j@hotmail.com
latdsmisch@hotmail.com
anniekhamocek@hotmail.com
mafillerxs6x@hotmail.com
jennine1kalosb@hotmail.com
mickict5sw@hotmail.com
holleyb4ihbarut@hotmail.com
marietterwzg@hotmail.com
jewelfoots1u@hotmail.com
de89cordon@hotmail.com
trulaballamwg@hotmail.com
joyaquipvvm@hotmail.com
arniedwe@hotmail.com

roberto.c@copttraba.com
stellak8artice@hotmail.com
wecare.ec@dhl.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.