Alerta de seguridad cibernética	2CMV20-00106-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2020
Última revisión	18 de Noviembre 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

ecb448d3b0c7d86ffc87e6c8a073bce412e7767826bf505ec4d26b9f799100dc
30de7b26e71dfa42859f03eedd475c8b38b2c453e0a8c7ed1e8417412317c7c6
337c613260fcc3e6a106da88bc60f99d9079116f2094085ac5cb8b497b819e2c
65fd502b8dbe07244adc4b956bd77eb077652f011ec6d55c65cde8edd623e8d4
c89a4ae21bc0aca7e57261ec4c0b4c3f4607167bc400e62ba4b09416c8bbf148
3d0495416c10ec60cdd0aa9189d519d516b6caee2d77e7458175113b74d78b34
c0de23b56e1fe15356f009ff76a214fe35f0c265838220bac2034e18816bffae
0f1fc79048538455989cb13006fc8f04838baaf649f942b5822639e02855fe59
b51e68a52d085aeec83086f3763c7fc12747b8123ee8227eb780a38cf2e2062e
a503b07c67997fa3f2ddc0d2d98bc9660268b99d13f6ab09ac39a000d4889754
68230ef6e3efc29eea5bbd5dab1c8ca4de9df2598b8f9156fb8ebc0a5bbf23dc
6172434eb1ad5c668f2470ad07d3e3e015455fef4451f712eb5e29c7a5d2b205
fca4f23dee3ae9b5ef4e4d2ff8711ada04591ca316217d34011d815dfa43ba9a
e34317bb799040db5ac6d4821d19f6d0b9dba1ed1151217f3af0cd4ff1cde887
21ce7c7809b66a85c380b9131843a246098c51a1da43df3adc2bf4b6698620c2
d81bd9b51d9746aa98406f9c05c5b70d8c14a5235b78ff847d6a3fbc18feb129
5aa66e468b69c5c39744ac23da7affc929f579fa31c10e32b2e8c7142b660aa9
cb316023b967173374bcf1ff23a0a9d0abafc6ae392400eae0c517a779ae9e3a
9c90e683f72057ea25f5281223c16b56cb3a20d358772d6b5ffe1802a10ba11d
c674034c60787e367d74a1dc8458920cfc2ba0f06dc4ab97178f8ead652af9cb

IoC nombre de archivo

Nombres de Archivos con Malware

PO 229562.zip
Orden de compra.zip
appointmentletter.xlsm
MV MILTON VOY 32 SPECS.xlsm
Pago de facturas.zip
TNT Original Invoice.xlsx
Orden No. 1820.zip
vessel's particulars.xlsm
invoice & packingpdf.z
COA & Invoice 47885.PDF.7z
Shipping Docs.rar
Confirmacion del pedido.zip
DHL Shipment Notification 7680615294 for 16 Nov\x0921.doc
message18171.zip
message.pif
order2020.PDF.gz
Order#19201905DOC.rtf
INQUIRIES (Stien.de) Groups Purchase.gz
QRN-CLJC-06112020149.PDF.rar
Product Specification & Quantity.doc
P.O. #HBG00356.doc.rar

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

72.52.244.66
88.218.16.246
88.218.16.246
74.208.120.53
68.66.241.149
74.208.120.53
88.218.16.194
185.222.58.118
172.98.201.44
64.227.65.86
81.42.224.67
81.42.224.67
45.137.22.50
45.137.22.134
45.137.22.75
199.96.83.10
64.227.65.86
185.222.58.102

IoC Correo Electrónico

Correo electrónico de donde fue enviado

purchases@vnkc.com
iqra@gifaconsulting.com
ops.pakistan@gac.com
ops.pakistan@gac.com
vipechi@gmail.com
In.tntimportclearance@tnt.com
h.valdes@maiconmetal.cl
operation@platinship.net
matt.williams@newfacultymajority.info
aabros@aabrosgroup.com
chanpitou.acc@widegatetrans.com
elopez@apiassa.com
logistic@bellstone.in
rgsfv@hotmail.com
carvi@sumi.es
sales@supplyafrica.co.tz
oliviahaendra@oil-gas.com
adriannaameida206@gmail.com
fzat@chevorn.com
jarrie.lu@huiliansh.com
arasheedu@yhdo.org

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.