| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00135-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Enero de 2021 |
| Última revisión | 20 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, 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

354e51b2ad7dd7ae40aa58987a27041b0a2ae4490a1177e983b47fcba19423c9
689c85c9bf479544446c251bdc7c4d743ee2c6005f52a0bfa69b5debe26ad0be
cdffc1adc6130ea4ac7b0a16d581c8db0b88ea84fda2c1edb12ee302418dd530
76ffbc488b52655000facf0b042eba699d17270c09e24b5703ac3c5a6859ebfb
f5e146e75878be0e926a587ae7c2ea9663e7873c2aaf63783f6675813fcf4200
90676a5067149360647a5ff7374dba0e94711d70c444f000663bf5d4a6b21f98
b439ae33bd80f4011660b3ceeb8659f3f1298ea36e79bf80e2accc12abfc2b94
9085abde0721f2f03e9e9d2afb9054c3bbdc937c32b099ec798850641f760fda
0568208fcaa7f6fa90c4abad9ea4c0676a155d09c3c51e4d8a6bdb5e55bafc3b
bc33d6bc28fc97ffb5eaae725a7c505357873a471fc928911fdc4c1bdce9a799
a2bf56911e84445f16ca2c0477de6a5592a55610ad56fffe5e65b08728bdbd08
eae24d230cc1c80d0a12778d3436c87ac52581ed5fb8840a618b8fafc5f34da8
93ecbff92cfadfdaf26093aa377048328d19821c09fdb6c8a926d3751f28ceab
0dba6290a0f9faafc903c56c6e9016f7654d7514188b6b41bfab5ecf6b41a1df
8b1bffbc02fafbfbf0dedf65e6b42dd3a12b6e8e6729b8460fadc8e528cbdea7
f63e6c0d5d4fa2e878b16720402523ad433d57bf4f32d7b7588cdcef7bf998bd
6ff6c454e8fe34e2d87a20fc6f6a1a28e463e4f29e5ca5e8b28134cf416d9356
4bcd9f19f8f8429746d3db3ce167f53b33d72116f7ab178e80f1115a0cb9b995
cd6726bcbd4e3241444d8bfb0da56997fefa4a614c3f2e6509f615d43b95f004
2aa5c3ef55242ccb530f5ae466e0ccf5eff7ee0e99a14dfbab77b84b1f231a24
997ef8fc2e605fe96c860961640c040cd4e4e850ae6ef4f7ff0f42582364694d
c8532382f27748bba7557246d4a6e66a084dd6748c4af5f75ab8f59b0d522558
7e6c8d2b812feb9ce8686b301f9df78d69bf9a7bde4572ec7da309a59ec62dab
ecccba19ec91e0fd9fd4e599bd95f5f465d5c68bf774f17e7f8e4b3162ccb97b
bfccc1d871347a0f216cd12e591faafc8cc1150b0e013de934288e20739b065b

# IoC nombre de archivo

Nombres de archivos con malware:

Statement of Account as of_01_20_2021.xlsm
printouts of outstanding as of_01_20_2021.xlsm
Emailing - DI661XXTVA 899.doc
mmena@mma.gob.cl-profile-update.html
Documents for RFQ - 920et- mini products for River side Project..img
RGQ-010121 WMP-012021.doc
TT Copy 02650019918751423 Pdf.gz
DHL Tracking.doc.html
INV_098789.rar
Consignment Details PL&BL Draft.gz
Groupo Dani Order_pdf.zip
Shipping Document PL&BL Draft.img
PO00001-2021.zip
PO #049766.zip
MV CAPE SUN-CTM CAL. pdf.gz
INV0009876.r09
Purchase Order RFQ-HL51L07.ace
owerri.html
Tender Material for PUMPS, VALVES AND PIPES for 3 Month- by 25012021.html
PO.zip
PO #047428.zip
swift copy.arj
ORDER3898.cab
Parulian Nainggolan CV.xlsx
New Order_PO#060317_007_Pdf_____.iso
eInvoicing,pdf.iso
Pi_74725794.zip

## IoC servidor SMTP

Direcciones IP del servidor SMTP de donde fue enviado el correo:

| | | | | |
|---|---|---|---|---|
| 39.40.26.238 | 98.187.237.162 | 159.89.224.7 | 103.199.17.185 | 37.46.150.218 |
| 185.222.57.238 | 45.145.185.72 | 180.214.237.140 | 45.133.203.50 | 185.244.216.174 |
| 77.139.57.60 | 37.49.225.241 | 64.225.53.63 | 117.102.98.79 | 155.94.136.43 |
| 192.185.201.2 | 193.239.147.142 | 172.93.201.206 | 192.158.231.119 | 164.90.152.242 |
| 192.185.149.46 | 160.20.147.58 | 103.141.138.130 | 128.199.15.190 | 144.208.127.207 |

## IoC Correo Electrónico

Correo electrónico de donde fue enviado:

| | |
|---|---|
| 5057040@qq.com | Nancy@riversideprojects.com.au |
| accounting@ocs.co.id | paule.a@mageneet.com |
| amy.gan@jcb.com | redirect@amgeneralinsurance.com |
| anna@findaproperty.gi | sabrina@comitras.com |
| delivery@bedslide.com | sandeepgill@combytellc.com |
| info@absolare.com | scott@webbimpressions.com |
| info@dhlexpressgrp.pw | shelly@royal-bike.com |
| info@dhlexpressint.pw | sscrm@cmhk.com |
| info@howw.com | terence.so@otlsystems.com |
| jhewitt@wayfair.com | tien.mai@r-pac.com |
| jquijano@plantacmm.com | vnsales6@juwonmetal.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.