| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00161-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 31 de Marzo de 2021 |
| Última revisión | 31 de Marzo 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 de Gobierno), 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 de los archivos adjuntos en los correos electrónicos:

15730e1d21f85849f2ebc73123128f8090caf2875031aece1e873f753f384ca9
2c7d043ef1315e5fe82e0dfb32c2a1c2d6d73251b6269283908df0f46340c128
46772ef430645cb795ec68328b68ae2e3e380bb692596d4fe00dc0cc09f0c717
4c72f894b1f77f39a841ea11ab8572d81c3fd525e78ceacf4b4cad4234aed667
533a44c34e8c2e3363cdd8cd4da7400d55d0642ed7a00c31fc448f769532c6e0
5fbedda881ce3eb91a839ccd4215d1caf22cf4f1295681ac303277688beb1f1d
69f8384dea7a61d574fc76efce0f9db1f942f58902a2aaa4211ab3a64c6a8878
6e51f766d318169ef070c77c7a1ee09284c8d6b3223cca08aa514acde6856e05
79d315e7bbf748dae57c0f5da69997de76df1c99b82b3ac8c22eb8ef98e188dc
7dc7244e1b2fb0730881cc0dc7c3dfcadfd683e57d4f08e8ea26ce5ca4e9ed90
85bc6624c9e44abc68ac6cba4760fec0b3384721954e2419eb6d3f8e86ae300a
87f4a7aae17466cfe271d8d1389e2ece68d497218590179e32c189292e910efa
9197636d1d6a324534aae7c13305fb10a421e5bfe579eb9929cd1b3e1f174b6c
a68f9d2f10ffa3d46d3c5f2f8a673eb8910dc00a30c3b1f06d92bc7f80e91600
a802f1405d05351dcaec66458fde76740a3d37c23ece666439d1a25d8bb9fb11
afa742615635ebe941e8b3609e3eda046bf4e9b9494cc18609c40d4e416111d7
b342c20f7a99734ce6f49ec432d155e760c09d4bb264e54736bffa55e992ddbb
c16a4eb88fc1ff28dc111479d0458f1268a909fc1354ae279ffde8f4dc32219c
c3b550e62986878230e04940a7503a684ecc95c9c0ae764a806892170f94a8e8
c5e1e50d3fdf47624ab94d1aaa1373ab05c841e64242dfba4b03a2980b234304
c7accb573b13bd9b786063b2d586f779c57d00a01ba6e7e4c2262c52a397a48d
d009bf653901f3f56cfe36ed4e724422fa1a0f16eb5175ed8a66d8ca82594239
dcf080025c78b8a4aa12e3a96834e5cbac015b8be178a400a0836d8cbb292df0
de8b95c67562881fe0e5bcb2e22b673d0acbdb8a848d0c3f835b28237e52d546
e4c37c77632e0ac493520a7c4dc3f56cd22a5b40e51f890643544f1044803c10
e67d88b394e780c4c96d4f49583d73fd383b051e967736696509d766329a1d0a
e8c21beda9b685209b0017fd413cc807d30fea80b18f112c19baf0fdb42dee9d
ec1cc9e522caef5f608aa965d33671e142d5cf801deef50d31cfe4755a4e71cc
f3343704cbf630ed889003d45e94b81794cf64021fba0c6b907846c4c98c83f9
fc026ebe0a13bd1b0a0ee4b66e0ebc869db554427e6dd17217f1b3e527e82ae2

# IoC nombre de archivo

Nombres de archivos con malware:

Swift Copy.ace
Statement of Account as of 03292021.xls
RFQ - NÃºmero de orden 846729.zip
Purchase Inquiry list  items 0092021 .pdf.Z
printouts of outstanding as of 03292021.xls
payment advice, EUR 61,676.rar
Original BL, Invoice & Packing List.html
ORDEN DE PAGO _001708158.rar
Santander_Documentos.PDF.img
Sales_Receipt_9449.xls
Sales_Receipt_1220.xls
Purchase_Order_7025.xls
Payment-Advise-smktb-Xerox.html
Payment_Receipt_3715.xls
Jvaldes-29231-3510-45-277726.HTM
INQUIRY.xlsx
Gtagle-18940-6267-51-036135.HTM
FACTURA.r00
#QUOTATION.gz
Factura proforma, pedido nuevo.zip
ENQUIRY - SPHERETECH INTERNATIONAL DOHA QATAR.doc
CUADRO FINAL DE MAINTENANCE.zip
CUADRO FINAL DE MAINTENANCE.arj
Comprobante de pago bancario.zip
BID DOCUMENTS _ARAMCO TUM009021.PDF.Z

# 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.

| IP | Etiqueta de sistema autónomo |
|---|---|
| 37.26.26.71 | Uninet |
| 211.219.248.163 | Korea telecom |
| 192.185.55.25 | Unifiedlayer-as-1 |
| 104.47.38.50 | Microsoft-corp-msn-as-block |
| 93.39.109.35 | Fastweb |
| 79.10.124.244 | Telecom italia |
| 112.25.159.234 | China mobile communications corporation |
| 185.78.85.242 | Survivor bilisim teknolojileri a.s. |
| 192.185.145.3 | Unifiedlayer-as-1 |
| 199.127.218.11 | Apyli-as |
| 45.62.234.199 | Datacity |
| 103.137.212.5 | Rainbow network limited |
| 221.115.191.113 | Arteria networks corporation |
| 45.133.1.141 | Des capital b.v. |
| 45.137.22.138 | Rootlayer web services ltd. |
| 159.89.171.146 | Digitalocean-asn |
| 37.252.96.159 | Comvive servidores s.l |
| 168.235.110.64 | ramnode |
| 189.50.50.10 | Total telecom ltda-me |
| 101.36.119.223 | Ucloud information technology (hk) limited |
| 151.73.90.69 | Wind tre s.p.a. |
| 37.49.225.182 | Peenq.nl |
| 91.64.208.212 | Vodafone gmbh |
| 84.38.133.114 | Dataclub s.a. |
| 134.209.64.219 | Digitalocean-asn |
| 212.86.101.131 | Zomro b.v. |
| 2.32.92.118 | Vodafone italia s.p.a. |
| 196.203.86.28 | Tunisia backbone as |

# IoC Correo Electrónico

Correo electrónico de donde fue enviado:

abwlemy@fargoforecast.com
ci@fargoforecast.com
ckaefcu@fargoforecast.com
davidb.jackson@hammondtractor.com
defdcridiv3@defense.tn
dsnco.cl@gmail.com
eromero@mmr.com.pe
fredasekini09@gmail.com
gaurav@fortunex1.com
Lincoln.Atkinson@msc.com
ljlep@fargoforecast.com
mariaclaradable@gmail.com
mitchell@demuntzoeker.be
mohammed.ali@algharshobgroup.com
Monica.Cavita@assistcard.com
Nakis.Kassos@gmcg.global
Niko.Barnett@msc.com
ojsor@fargoforecast.com
peter@vertexpc.com
quickbooks@notification.intuit.com
Ricky.Parry@msc.com
rilzu@fargoforecast.com
RoseGutierrez@gmail.com
saleh@wonderinter.com
sales@guang-qi.com
shihad@alhakbanigroup.com
tcymdyo@fargoforecast.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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.31 09:38:28 -03'00'