Alerta de seguridad cibernética	2CMV21-00173-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de abril de 2021
Última revisión	28 de abril 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:

0432d7d30283a74a01e466fd289f35040c30e48b29e73e149b3374d6e07f752c
048518f8b11aa405bde1b4c8d71e9537b1a7200a5c816fa4fb451476c93e18b0
07b1bddd60ba94eb9b1d304d068d39ca3e8ce1d190accea08102f32551839cfb
0b5172660a81c31765d166bcae95cf648bfbfca599a8adadcf504c1a1ff973b6
0ba92d397ba717cead88c29be8935dc04917e248504d8c16b6b44a02920aff56
0e13f3fd36b3add7f3e7221975469ad8e7a625d9c4be5b7ba81d75dc5576b8d1
0edb8c8d9ff0709677aca64cc723b82302d244cfb9dc69129674aa417d495321
11ec8c695558777665276c406b5c435fa87ef81912dd18d4f82629589f36c74b
1730da6bbda8300eca3cc4ebd072fbeba77dc964e86af7c672dd02f4034dcc74
17fe063619c08c97dd6ebaa9e4e47df51852a2873e2a13f0260620add41b34d4
1cb3b34388e2d48113df87ebbda683117d978fc4ce1f17cb5c1d09ddf353edee
270094a04bd98204e670de290b23650f21749695cc370cb0eb18f26f05e98eef
2c21d8f271d81bd393a2a509e154b254bf5064ba9e4d95be860a9bdf1c0fd5b6
2cf709ace0280783623acbc9fb826c931a647c3305fc1e1a1c3f9411638d386e
2e682bc8983776309a853f887f16dc5ea3fb9c61519c67f3262757d2ca747b47
3a0f55d13641d30db8dcde1abc0120c0ded4c35d6fb907bdfbcedeeb29b4aeb3
42c36caf58671da2a6e90667cd25855f4f85c8ab9ced1f12a493a6d0da8271e8
4549d011b949eb75c36b49772f47368ccfe9931a021fd434850dc45a56458c2c
45812edf47ba8b8d20db1674bd19f38ca5459d125602b8c5ec3aea2dfc9ff328
45baf56d201786cc94c817345e7afafe75e9815700bce36799971cd76983fdae
4d632467af35b152b404bad6ccb8298ff8860500bdaee9e6a87b192e3d7b1383
4e49a6eaacc7abbb0a5fe51657d2fb986a0f392118d593dc4a59fb3fe8db6bee
514de68ddc8a32c2a8a62fdd0bf2a494c6120a2da46b15a20724fca4499847e8
5d7deb44ec0daaac2216e4ab7a1034033e0c0818c12f5d7332278c094ac3a029
676edb4d46cdcd7c680e3fd3975d787ac4a3e5c704fe1cecc0ab13735bf32b26
7813058478aa477d0e397f275ee6f31877c8059bec82f0dbb48160af799c77e8
78855573c8fd546b70baf202cfdc65a9f0f9da0d8170dfa5689ee618f7613130
7b6e793102058d786cd54fcdaa3633a91083e5b3d358c95e7d17e199723894a2
80da74ac91a4cb0bcd7af65334fe67d09d495e9c1eba52ee8383dcfe2107fcf2
8d3d3d54ee6d432a075e9d21d959404accdc25d44baa25e6cf17fce34b8bee82
8f47f3a107ba22caf91ca8019baabd6d2d46bf9b6ce79f0d34ae98c31624083a
96ee0d500aa147d71bc99c27b5e4fb534c3e120bf2d165907ca4612f8023cc9f
9ac24a51135efe8b707fad83090bba020b67df7da026a3805025480bcb0d8040
9ddea1c5a5c08a83a3b2a7282b1b651a984e0e7ca7dea1c1085bf2a1fc77c994
a9bc6403435e0f077bd24f94ef0a100ed114b588513f474450605e38523b1920

b4b18b1a1c8b6d7d979d93897d1b710fc81d4309b3e3a07ea757d1ce95428357
c0ded1fae7b9bc0422ae464c86d6cc2e64d7536a3f660d91c521ca52db6d0d21
c60bb0ef48e4a7ed7f414bf7a4678a4adaa83e8fcbccb7607f5b3b98f29c2d18
d0527be82e7950e363f7030e931be288c4222019e5f3876a98d6b021feb185ee
d745b4373a1db12c38d23c946abce152bf064cd74ed7efd67fcc17e179816240
e06b9da757791b7ed2b58617bdad9ec542f91cbeb74b817f25b1a4d569a3d08e
e9c102eeb57bd3cb741238b0328a8eeb0f441493ae96a8c791cb5e087bebe558
eadfd82f1ccb229f3bb5bf229e04de7a36156e8799a04a9c5d31c60de7c6f217
f8da473ee2c2398e5574c79d35b4d195598fa22418b3aba36e245bcb11bc5c51
fa084536ab457ebff57cf069faa57fe1a3d69076a628427793d5706c67af26cd
fe62cb2dd8dc13f7c15e84d090a6d112d6f84845129182fd3ca0154b560d98f2

IoC nombre de archivo

Nombres de archivos con malware:

ARIX SRLVl (MN) - Italy.zip
Attached bank swift copy for your reference..zip
AWB#25042021178834.PDF.rar
BL PL & CI Copy DHL Shipping Docs,pdf.zip
BL PL & CI Copy DHL Shipping Docs.PDF.rar
Detalles del envÃo.PDF_____.r10
DHL SHIPMENT NOTIFICATION,6207428452.ppt
DOWNLOAD AND RUN TO UPGRADE YOUR EMAIL.exe
El nuevo pedido estÃ¡ en la lista adjunta.zip
factura.PDF.z
IMG_60_741_612.R01
IMG_6037_020120.R01
Invoice 01859.rar
KAS-560734.r01
LPO.rar
NEW ENQUIRY 200283.gz
NO.20-3027 order LHG-050320-01.xls
Order Items.gz
Order specs No12.gz
ORDER_0011_20201230_AMNIS.GZ
P.I.cab
PANTA,xlx.rar
Payment Advice Note from 28.04.2021 to 608760.zip
Payment Copy.doc
PI PDF.zip
Proforma Invoice 21000020.zip
PUR-21601146 SOP-21001146_PDF.GZ
PURCHASE ORDER_PDF_____.iso
QUOTATION SAM-S210118A_XLS.GZ
Receipt Confirmation.pdf.rar
Request 126-21-11HAR.cab
Sales Order.eml.7z
Solicitud de cotizaciÃ³n.zip
specifications.zip
VESSEL PARTICULARS.zip

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
157.90.50.57	Hetzner Online GmbH
45.143.147.194	Hyonix LLC
50.210.204.193	COMCAST-7922
81.144.138.194	British Telecommunications PLC
87.125.174.245	Vodafone Spain
103.138.109.241	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
103.151.122.244	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
103.245.209.226	HK Kwaifong Group Limited
128.199.152.121	DIGITALOCEAN-ASN
190.210.196.123	NSS S.A.
195.140.213.222	Hydra Communications Ltd
198.244.135.246	OVH SAS
103.145.252.28	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
138.117.148.93	SOC. COMERCIAL WIRENET CHILE LTDA.
138.68.65.174	DIGITALOCEAN-ASN
143.198.55.51	DIGITALOCEAN-ASN
181.30.31.36	Telecom Argentina S.A
185.222.57.142	RootLayer Web Services Ltd.
185.222.57.90	RootLayer Web Services Ltd
185.6.88.18	Siportal Srl
187.39.254.56	CLARO S.A
199.250.200.47	IMH-IAD
31.210.20.195	Des Capital B.V.
31.210.20.199	Des Capital B.V.
45.137.22.120	RootLayer Web Services Ltd
45.137.22.133	RootLayer Web Services Ltd.
51.79.14.27	OVH SAS
64.188.20.247	ASN-QUADRANET-GLOBAL
68.183.10.90	DIGITALOCEAN-ASN
77.247.110.43	ABC Consultancy
82.142.14.233	Free SAS
84.38.133.6	DataClub S.A.
88.198.112.68	Hetzner Online GmbH

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

ramon.huidobro@gmail.com
a.varghese@fugro.com
accounts@ccmarine.in
angelyim@chargeurs-pcc.com
AP@nestle.com
ctelesca@amnistreasury.ch
docusign@capitolcitystorage.com
docusign@johngallison.com
gvu@un.org
info@basarimuhendislik.com
info@erapres.com.tr
info@gac.com
info@hvcontratistas.com.pe
koukharsky@koukharsky.com.ar
marina.a@scorpiosmykonos.com
marlene@heliosemalharia.com
nsakiya@sinopec.com
ops@csdvlp.com.sg
p_jamei@godakhtar.co.ir
purchase.pmgroup@mail.ru
purchasing@springmarine.com
ross.kohlbeck@amerhart.com
sahajdeep.khanuja111.sk9@gmail.com
sales@amalgamuae.com
sales1@agiindustries.com
sanjeev.shukla@bioayurveda.in
sghanavati@mpc.ir
sherif.elgendy@adesgroup.com
sherly@zbqishuai.cn
siddharth.kharat@kwe.com
ssparks@hemsaw.com
Teresa.Fuentes@gmail.com
test@sferalegal.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: 2021.04.28
15:45:52 -04'00'