Alerta de seguridad cibernética	2CMV21-00175-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2021
Última revisión	10 de mayo 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:

f8a1e977ba90a5621e67a1b04ca4740893ff4279ec4712eb22d8267a0c3a01de
f773364cd11c5155ccad0e4d3ed770a0ece02e81a6372f23fc285bdd9f301b0f
f00763eaa902104adfc7cb5ff64dfe6fde7ad2069f78f9125de5993f3f1226c6
e9d949a4df2e374fee8983e43e0e78cdc49faf0afbed9160b3aea898f0155f2c
e9cec5347ad80420939f1fedcdb7d321ee7cbf79ef22f41c860cbc4f668772bb
e52cfd603333173f5a5fe560e256dbd05389a09b86ddde41808a748506f3aa44
df64df82b18e852a3b662b4b26e46a1077fd298c0b9133ba7a8f084b988a4b0f
cfa82fecc8818cf2dd19a0a21c51794fdb62719bffa121ee28bfa79e7b859490
cb678fece33a4de8aabc9d527a8188a407dc6432072b9a1cc4f293028dd335ac
c031dd1d1ef57bdc41821dc77387ef4f3db03defe3e0979e5993456130d03fb9
bbe05176a0d58aefdf00b3d58227f923e20d66c140157d2e804c460db6bf73af
bbd1bb83290480d23e3246704ae43deea19e8fd310630a3e4b23639a1530fd5a
ba77c9c1a124c51af298551e5d4fb90e5b9ac1b37d835d8cf1e6521bd9ee4f53
a2b084545d31feaff2d64383b0d3aad3d380c5b44c65f24ed05aede02e9ad410
a2907290b9082b133e5f4d82407976db26620a692834195cbf6a334061c76367
a2442bb8a9aeb8af98ccfb07ad9afd62bdbedeb942971a8644d63687dbb65490
9abfb60a643a4db9a7013e6560270f355f2f71d09eb294603d22649195d49f95
971bd748d074f5233dbea165c1b6db2afad91f05ff898042895d2d2051d28325
96cef47a692b9c60d05616e1dae9db6c27e58e20b18a188e5ed0b6293e4adf60
95821be68f627aa047e696021d92a10a4c5d32e7fc9970a765c20f4e3c33081a
8eff78d6fcb3902acc848308a2bec0e803c6c4cca746e99d8c72a11f145251a3
8cf7e34befe07f3cee7e0ead01e73688f6be60f811f906829c4f7710723bc842
8250b28f46bb373012a66272a51ff34fa06e8497acb16ce554f60bacdbb73c48
821cc34f2f220c59fd0b551b6d42524ca71de94fa6ae1df911f210d0cfbc407d
7c1023dfa81cf45740a1e582dbfaf95bbc53d72db2c36ed0dbcf48ca23690fa6
78e048deb6bcc6fce5fc427ca0d24a3f7cc03f132b67b90581d1807cea90ab30
73f6a73c8b2a485e925274c78f67a66547d852d80b6dfa85ab8cb21e88a7975b
6bbe2215d505698ade9984521c8ed04dfa3fe0df4f39fdb117f9ec850259518b
5fc19377f8bf125c1cbb188c56ef38d7e849a99908b598ea24326b632708ce3c
5e5783ed2dac9e02718ca9e83f96c8ab3a51866e3456d5f0d94ea16ef470a547
5c30c2e02b3395c9d7ed86a9e8ff3fa7429d9bc3aa616509eac09a39f2a8ea15
5959b4ba12113d69501c49165c3e338164d77e4c0091a5c373c6ce60a1dd762c
515dc9e81f8516340fe3c2f245a3ba060bce8352271cac12df1e69e05e00ffaa
50354ae251c2db7888f43ba824f6c97467bb44d7a256db784940d64f11c481c3
4f4f6819151dac871b3419d1813627d42e6c167b5d124dd35bd1c18b3d20c7aa
4c52f2b312e5be2d215c9e2b7d16b15af31dc1984e299e9e58c3cc46cc6b5e78

499054675c3a255635b3272d4840935648a03fc913f830976b57ec86a741cff2
47695f6748c9c5ffc76ac08c4a83099d74592894e539562a13a169d3818ae989
4429816be97d6247601c2696c571e32a0ffcd4bd523b24ddc2b5e66c7b2b3c3e
361864c83f51be22d7f72888a7fe160bce989157e2befb0e7ac52216638663fa
08d1027f9318093b5e28bf6a9082f7ede5b101e29e92cc54ae88bde19d1fda05

IoC nombre de archivo

Nombres de archivos con malware:

209352.zip
BANK ACCOUNT DETAILS.rar
cccEDS03932,pdf.7z
dhl_1010.rar
dhl_pago.exe
dhl_pago.img
Documentos_Santander.PDF_____.img
EDS03932,pdf.7z
informe bancario.xlsx_____.img
LPO-6809.rar
MV GENCO RESOLUTE VOY 1 DESCRIPTION.zip
New Order Requirement 2204.ace
New order.zip
Order 122001-220 guanzo.rar
pago_635.img
Payment Advice Note from 10.05.2021 to 608760.zip
PO010052021.doc
QUOTATION_210905 Img.jar
RE WRONG IBANPAYMENT RETURNED.zip
REQUEST FOR PRICE QUOTE - URGENT.pdf.zip
Shipment Document BL,INV and packing List.ace
SHIPPING DOCUMENT.HTM
SOA PDF.rar
SwiftCopy-10-2021-pdf.z
Tender Overview 10052021.doc
VM-(ðŸ“ž)---41_52682.htm

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
146.82.91.211	Adexus S.A.
185.222.57.229	RootLayer Web Services Ltd.)
143.198.61.188	DIGITALOCEAN-ASN
217.146.81.63	Hyonix LLC
190.98.225.43	Gtd Internet S.A.
103.139.44.91	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
143.110.225.122	DIGITALOCEAN-ASN
31.210.20.71	Des Capital B.V.
103.151.122.176	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
103.139.44.129	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
31.210.21.118	Des Capital B.V.
23.106.122.190	Leaseweb Asia Pacific pte. ltd.
103.28.70.140	Hyonix LLC
45.144.225.21	Des Capital B.
45.12.213.248	Zomro B.V.
46.183.221.116	DataClub S.A.

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: 2021.05.10 19:20:59 -04'00'