Alerta de seguridad cibernética	2CMV21-00154-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Marzo de 2021
Última revisión	12 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), 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:

1028cae172f9941e75518cf1234f46b6df55940d8c5e6e47d797ef9f7958af2d
1329ff031c1f1ee14d20e7dc1d5f355836b890ced91b24e460da8df629075b39
15bc140115973720159b3ab3bcd84eb03d4225c0888f4011ba1512a83ebca336
16dd5dc583373c32e0b8e3448320ecb5edfdf5bc9d9f6291d318c778b934ab8f
17b3d701b8884cb7fe92ccc55973129cbd7dbea1d4e8fbeb87ebfe456c148c59
18a85a78af1add92325418b1209f07ba003ff04d6270dc2ebd18642e3cb3924f
21ed2210885536a9ab2568e305134364e89e388ea0bff803af4d503a465c3d53
31d1895b84b2553a41d3abdcaf259231e75235a7390a0c32a3f4f39a6a0a09bf
37858f1836da22f3c16f0b62aa18ef52ef91934e4415e0a4e6911dcaf3763afb
37b4554d3a1af6213496e3f45e36a7b7ac6760ba90671bc27d0fa5d9de2c3291
3bc245433cdc0ed5b755643239cce535879f36033baca71372a6bc5f520bdfb9
3f527f6b74eb3aa050429314104c43d2436fab38e7cf70ab72db9304ca4167eb
45b5ea8ca473975c84528216c08fffbf08883f289c6860cdb9b6f94521909dbc
6d507c5f16b5a8bcef7cc715a2693cc83b240563df47e9c37f744eaa6bfbbf61
703ba0d3604d3d88b0305c354eb596f5a946b1cda30a4b6e5cd524cb8012afe5
753cbae11a881b871e3295d65449954817061db5dec53df7b379fee9f21c33d1
7a2811fe02a2edf89723521cd1562aa6bb383918820df3fe01f87020f98f296d
7f22df3a8aca7f8a184f063bbab3de9bfdf3c10c09bf95ee54eab5c8090752e9
85beebafb964a562f652d048c758a3d6ee0c9a2c1f847944b53c965b679e336e
93d935495f7f40deaf07b68afea7d4c953e14914a28b10412498ccd26fa859bb
a1159d62fcb4dcb363be830e689a3872a70e7e71c71c44fabc478ba8dec3b31b
a908ebece5fbe0931bc9be0c7330bafe25f67ade21cba15bb5bab101ccfb5963
adae3a7030b466563ad42ebcdf174b6ac89928a2e50e3697a40a4bf007495c29
b58acc04c92d4df0432f66dcc5721501b7e9c1cc486143e0badf42adec836d84
c23d659803615497f1f9a01af5eb6763505687dd61845749a0dc6e16c9d477fd
caecde573eb1b31ce10a947c2471178e006f99055aa40493eb234d1ce07190ec
cbe045e37356a0d9b86655b93fcda9cab0ce16ab4d39c01fecfbca301b6032b1
d25247dc5c3c487deffe3e7c04833d569136ce6051a6e9dd63d327ded974d704
d578337ed0975cfd23f3edf0544281e226ff04bed93ce4e76cf7ba9683a9c420
d7b0b24695fedabd57e8311ef54ca3a18b38a417508e2d2117707b371373ebb3
e3e38dd48e944f70e5cf324d557ddfd48d7e66d4150a28e88a49dc4e9424565b
eca1e93dc48c110cf049c081ba17fa0bc61560896e0dd19fe655aa45156e2b77
f0a6419a2c90ff826169070629240cbbe573b3aff655e6bf4c06387e2fbe94ba
f4ea1ec8a9feaa61cfb94f41750aa140d0b972ff7a8cd092eafcae9b89600650

f79bb4189ba2ddd3107a8bbc6ac74380c6677a850373255a8bfb32b96fbc0ab8
f8b9d8abdab8eb76a376013e55887bfcda18664d7e73ca42e97ffda183d128f1

IoC nombre de archivo

Nombres de archivos con malware:

ZeFOJ proyecto pdf.arj	New PO.pdf.zip
TT Copy.pdf..rar	New Order.r15
RFQ-0111.gz	MESSAGE/PARTIAL
responder_3.0.3.0-0kali1_all.deb	jquery.js
Quotation 2021000.PDF.html	isr.exe
PubPlatform.exe	invoice copy.zip
produkey-x64.zip	Internet-Start.exe
produkey.zip	favicon.html
PO11032021.doc	Documentos de envÃo originales.zip
pm-1-2.jpg	Copia de pago 11_03_21.iso
PI.html	7348255142.rar
pdfforgeExtension.exe	4215.fnt
Payment Copy.pdf (2).zip	npm-err-failed-using-git.html

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
87.126.174.11	Vivacom
73.98.182.238	Comcast-7922
67.52.174.126	Twc-20001-pacwest
45.85.90.232	Des capital b.v.
31.214.176.32	Soluciones corporativas ip, sl
31.214.176.31	Soluciones corporativas ip, sl
31.214.176.29	Soluciones corporativas ip, sl
31.214.176.27	Soluciones corporativas ip, sl
31.214.176.26	Soluciones corporativas ip, sl
31.214.176.25	Soluciones corporativas ip, sl
31.214.176.23	Soluciones corporativas ip, sl
207.7.86.108	Privatesystems
192.249.122.78	Inmotion
190.146.47.121	Telmex colombia s.a.
166.167.45.101	Cellco
124.29.202.102	Cyber internet services pakistan
108.175.14.66	1&1 ionos se
107.167.82.209	Ioflood
104.223.119.82	Asn-quadranet-global
103.99.1.144	Vietnam posts and telecommunications group
101.1.7.247	Bit exchange systems limited
164.163.147.136	Gaucha online provedor de internet ltda
144.129.119.114	Bhn-33363
103.141.138.124	Vietnam posts and telecommunications group
85.214.160.219	Strato ag
23.235.223.128	Inmotion

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

santander@venex.com.ar
tzijuc@koepfamily.com
sanjay.khan@bhm.co.in
salesaci@arabiancrownintl.com
sales023@bornsun.com.cn
rochelle.ann@petnet.com.ph
qojaluy@koepfamily.com
oy@koepfamily.com
no@koepfamily.com
mohammed.shuji@oceanoil.com
janzsys@koepfamily.com
iucaybu@koepfamily.com
ipysku@koepfamily.com
ierexu@koepfamily.com
hfeluyz@koepfamily.com
ebwotko@koepfamily.com
cs01@jandragon.com
contact@gundersondenton.com
circular@audicubic.com
aqboled@koepfamily.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: 2021.03.12 13:56:53 -03'00'