Alerta de seguridad cibernética	2CMV21-00152-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Marzo de 2021
Última revisión	08 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:

1f29f028fa98c6bc13f16a560cce47516b18a23cf7bc2ae3c96e3dc05d4fd907
a79c8527653260a362ccb804a3f2916461f54f844b93d30e00294b976c49e12a
bb112d4e23f3835f3a1d8badc92b3081e4d92e8c73a7837e90f2f29b7ef6da65
a5304c2f60b15a67a86f7611b2ff47e5b2a39000a93929ba93f995b2c7d4b7d1
bc408f72c8be09e949ccc77140d5a7994429fb1a2c61a709e13905e331e070ae
c35e35461f5e7f082ece0a7c56a0a0c52d8e33e6066326ef0193729b4b4bdba8
5f81706144c6ab4979d34f5f5e874b6a74c14d061fb9b2994b21456076696c1a
768e3902e97b4f455c601938013a3bb54ff9cf069e2249d3a47c191f8097f69e
11c2e6a14362b67851b39d700438412b812c60a42c6ea2bbceaf8500efdea4b1
f31eb91f999f372c0bf29efebd9b7aff42fc737895f5e8f79f73f419ac7da279
849f6ca81256c6c83749cae8ea06fdc298d0a5bdbffdf8fdf699969e859d2dc8
4a5d3f604434e49d1c7930783a99ff4de0c68264300ec0534e9e779fbf8c269d
4a32747eaf957a032a507675509b32c1b8f890c0316e58f7a01bcbdca3ccbfd3
1950780ba11f97f2e67d0c16d66be88afc0a0269c568ab53d468fbe20e06250f
c8c0f14667c269845970022ca4c61267b3e8f554e7cbc0c91963c55f1ad97832
6b610061618fd7775855d695fc4af8518f312ba53d6709c657d560165e4d7c79

IoC nombre de archivo

Nombres de archivos con malware:

ZeFOJ proyecto pdf.arj
Swift mensaje.zip
New order is in the attached list.zip
CotizaciÃ³n.r00
Attachment 1 Instructions to Bidders.doc
BID-RFx 5500296898.doc
Trial PO 08.3.21.xlsx
PRODUCT CTG. ORDER (1).zip
BANK FORM.doc
INVOICE.PDF.gz
QUOTE B1020281.PDF.ar
PO080320210.doc
invoice.cab
orden de compra pdf.zip
RFQ#100027386.exe
$24,363.98.PAYMENT.COPY.PDF.Gz
Purchase order no. PECPUR20-21517_PDF.Z
INVOICE.doc

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
190.210.186.137	NSS S.A.
49.12.124.200	Hetzner Online GmbH
192.232.198.199	UNIFIEDLAYER-AS-1
84.38.133.32	DataClub S.A.
103.151.122.27	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
37.49.225.171	PEENQ.NL
142.147.97.145	UNREAL-SERVERS
45.85.90.232	Des Capital B.V.
37.49.225.139	PEENQ.NL
174.136.28.112	AS-TIERP-36024
199.127.59.214	FIBERHUB
66.154.98.110	PERFORMIVE
31.210.20.191	Des Capital B.V.

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

rania@lecercle.me
Lourdes.Martinez@heidelberg.com
osaimiao@sabic.com
info@starlinktradings.com
codink@sealcode.com
acts@sreetrans.in
account@db.com
sales@shshenke.com.cn
info@acc.com
ops@tanbinhshipping.com
ivan@aikom-kvalitet.com
marjie@aimstelecom.com
sales@carlinkmotors.com
noreply@ir.netease.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: 2021.03.08 12:00:30 -03'00'