Alerta de seguridad cibernética	2CMV21-00146-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Febrero de 2021
Última revisión	12 de Febrero 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 catalogado como **MSIL/Kryptik – Ransomware**. Estos 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:

ab7c46fafb73625c9bc58a6b15a7ad52cedbdd5886b85d717b778c9a40193dc9
507fb91596e6dd95613d904b1f6dc86fd72c4d6deaee18839f8f3726ce5be670
b6c5511697a047d1d608f32dd0d9f6f235a91543896ec052c24b23c0a4478d59
9299a3dd0540b4f75af5d12c704c8c3ecd47b25c51c306924b437c2eb775becc
399a9435ee5cc7337d31af4ae62f8571bba3c29ee5b2db75259ef941e0d68de1
706510df18e068c711cfb975f00d1aeb1046787906d3cda0a3fc1f65b3be2282
e1f8e1e3b6cfee7a4e599abbd8324bb5108833119ba962984b86636c68ab05a1
1f6e98fa8b73a3e5304424d15a2d87d95ceb7e1b201732bd5cf7d2beb51d9c01
504c437eb6137e7bfaaf311d8b0bf3209ee5737a4cc0d787eb39bd8f61de0a80
ee7607a15c6026a59f52a0ed0ca8817835a713c12fd14b3f3348e5bdf8692700
7c4543586d38c0599ce0c712d2689cfec66bc862a1796f48784be6250ca5d97a
a052adecf1d257ebb7e99ace172086279e8232a69eff5f1e67eeb7d7cbc253f6
77ee808fba1f3c3ff78f2bcfe345876b68194831c91ae3186dca552b2e0bda01
ca947a5c7c0303ff1a61935527a1d6d35f0379a9728d18a364259db7729cefde
5564713f24f79a2fa73d6ff90de5ca49d139f88588ac9c9635df5e54ea468ff1
d7d76fb7adc91c1f533131372caf8b532cdf322e461230b44c43bb5993f8e4b0
a0c15fcd0d4a98382f73154b9003ef407962c5d986e577c0e2e2411c58c3bb42
b98df3a3770bdb3853e8a455a26b80783de34f60879dd282fc2d2e953832b9ee

IoC nombre de archivo

Nombres de archivos con malware:

Ref-Number_MT10300238402293.zip
invoice doc.z
datos bancarios442.img
Orden de compra.r00
103....1325374.arj
103....13253745.7z
New Purchase Order#00171.zip
COPIA DE PAGO BCP 07.arj
Transfer Application.gz
IMG 02-11-2021.gz
IMG_5436435423.zip
PAYMENT_DETAILS.rar
DHL Update Form.pdf.zip
purchase order1111.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
180.214.239.43	
173.0.142.242	Apyl Inc
46.16.59.84	10dencehispahard, S.L.
66.96.184.10	10dencehispahard, S.L
185.4.132.177	The Endurance International Group, Inc.
103.99.1.147	Fragkoulis Maounis & Sia OE
45.11.19.224	Vietnam Posts And Telecommunications Group
45.137.22.121	RootLayer Web Services Ltd.
185.235.165.234	M247 Ltd
103.145.255.216	
77.247.110.116	Vitox Telecom
84.38.133.27	DataClub S.A.
103.141.138.131	Vietnam Posts And Telecommunications Group
193.142.58.49	HostSlim B.V.

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

account@trenchless.in
support@chinesestandard.net
gerencia@inemflex.com.co
sventa02@lustingsons.cl
claudete.lima@excelbr.com.br
phil@cyber.net.pk
customercare@oswalcastings.co.in
power@poweronline.com.mx
imports@tutanota.com.de
nour.fawaz@intertech-group.com
bizinfo@sg.marshallcavendish.com
account@staroverseas.co.th
purchase@arabico.ae
account@trenchless.in
Catharina.dew@accellgroup.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: 2021.02.12 13:15:37 -03'00'