Alerta de seguridad cibernética	2CMV20-00083-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Septiembre de 2020
Última revisión	15 de Septiembre de 2020

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

8f48bd9f5acb830989f877abf023aab91e06b381849d43fe97ab36ce28e93fe5
9406cead35b06843e0c7b2a749f1612c636327078f6b2c308650612342021 47f
2bbb7a7da660597db9868ab039007e32b8a465463dc8cd6383b14e9c2fcb4452
19a990372249527ec783e1723940cc63ff32442e69a832520cc0a52a59796eb5
98592860d6a035cd56fe7f5c15baf2254c96abee3a08417c35bd0d250cd980e9
388f024cdccbce8d33cca92f84d9176d9132fe060fad30146b54c77f6a2cf6bc
097cb02af6fe32a589db0d2af78e95e68f9ea54ee813f4415d405893af7962d4
5858f78bf66267ae3a316a4421289bec57c6d8262f6af1416a60228978c18efd
c5712b0c4cb9ddf9cc461764d21f9d0e6966411036ae2a1e52d9f65ddb9db9ab
6113e84167123497be9099195d2215e5b2c4671ef04ee40b38a0ce54cda846c1

IoC nombre de archivo

Nombres de Archivos con Malware

DescripciÃ³n de la oferta del producto doc.r11
Quote.pdf.rar
QUOTATION pdf.7Z
N-seo-pricelist.html
INVOICE.iso
paid invoice.pdf.z
FedEx's AWB#5305323204643.zip
Aramco Asia Japan Inquiry - Asia Corporation.gz
GYPSO - AUGUST 2020 STATEMENT.gz
DHL-#AWB130501923096.pdf.z

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

31.14.14.99	104.148.61.172
209.58.153.202	104.148.61.163
209.58.149.67	104.148.61.181
104.148.61.164	104.148.61.183
104.148.61.169	104.148.61.186
199.43.204.183	104.148.61.177
104.148.61.179	

IoC Correo Electrónico

Correo electrónico de donde fue enviado

ventas@bidakis.com	kipemilf56cadyu@gmail.com
oelhoubi@elemtuaz.com.ly	golasage265hyzki@gmail.com
info-jtc@julaiahgroup.com	carlemau296zyer@gmail.com
ventas@bidakis.com	sloneloga1s@gmail.com
sawijama5liadi@gmail.com	ronasyre474n@gmail.com
khan@gbml.co.kr	irapier044qit@gmail.com
Yang@maximixe.com	westelle638nobma@gmail.com
fantjame060ucoib@gmail.com	otiscatr45ubqaz@gmail.com
track@fedex.com	otiscatr45ywuan@gmail.com
ketcdutj170zcjfm@gmail.com	judivalo036fonhp@gmail.com
isendana0haku@gmail.com	burkelynn19efcum@gmail.com
traialet662bvasp@gmail.com	geracore539zeer@gmail.com
turnerthur7soyg@gmail.com	kimgarr459zi@gmail.com
virgpris800b@gmail.com	rika.tamashiro@aramcoasia.com
donahenr845ekwsi@gmail.com	leo@jolofarms.com
michhyma42lh@gmail.com	westelle638vufky@gmail.com
kimgarr459xsu@gmail.com	donnedua0xoape@gmail.com
slavfree818axuca@gmail.com	ronaagus243naj@gmail.com
patrhoyt29la@gmail.com	westelle638iuhui@gmail.com
dysonkizz7qpihe@gmail.com	isabellgreg171atgux@gmail.com
irapier044auozy@gmail.com	lacejoly2bejt@gmail.com
briafloy9irujn@gmail.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: 2020.09.15 17:28:11 -03'00'