Alerta de seguridad cibernética	2CMV20-00114-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Diciembre de 2020
Última revisión	09 de Diciembre 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

3db1645da329db133422580f08fc00efc17e78b36391f9621768b1839144cb12
4bce4a37c46c2d4363233c765be3cbb1f09175b50cdf0bc478277fdc339de223
5b6b7091336852b3387dd61a8f5582b8cd37c588a97097b065fd880a87d26fc5
6563bd898c439db46cb97c53dd8d9eaed24c1f8eb7078ba6a3c94d102580ac58
7536f9bad9507f873f8ee30ee5183bbe9b8ab4f264f47c8f64a9a6e46900ef1c
775ec2cefa2f4a37b05c04f1fe940795a0e2a3bdb3378e9165a9583ff6077eca
85838d336fd5ee8fd104a18889abd32421058048f2e20214e6e59129c3911d8e
990b8fa9568fb787fc4fdada1881b706484fd4944b77f1704913927c9f7590a4
ca4ca641512bf28bf726e62e22e166ec57f923c6fb20ea38d9bc06f5355608d5
d310f011b50e507121cb5949d18dbb864759ff9d0eac0b28f60db8f33f37f2b0
eb0be54dca8a4bb378534e01eaf53e4634b52009e519f6fb4f285a81bcc86a65
f0466c8703e9dc96c1fcc6c22166d582f9a193dd191770c461099e0998a97f8e

IoC nombre de archivo

Nombres de Archivos con Malware:

12-7-2020_06-59-10-PM.zip
Verify your account.html
FOB QUOTES #W092072DB6720.zip
DEBIT NOTE_INA10197.zip
NEW ORDER POR79345.doc
scha.doc
Invoice Act N2.ace
PO_103.r09
invoice + packing list DEC 3 by DHL.zip
Times Shipping - USD.zip
filename=awele.lzh
Shipment Document BL,INV and packing list.jpg.ace

IoC servidor SMTP

Direcciones IP del servidor SMTP de donde fue enviado el correo:

74.208.175.156
37.49.225.143
190.210.15.194
179.41.18.118
103.99.1.174
68.183.86.92
45.35.196.138

IoC Correo Electrónico

Correo electrónico de donde fue enviado

dmconstrucciones@adinet.com.uy
administrator@postmaster.net
spunkycats23@yahoo.com
ostrum@surry.net
hhafeez@takweenai.com
Hanan@dhl.com
Alex@lhdottie.com
mayzin.kywe@hoysan.com
info@ouchem.cn
shipping@dhl.com
boskotech2@gmail.com
chanauspicious@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: 2020.12.09 14:05:21 -03'00'