Alerta de seguridad cibernética	2CMV20-00105-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2020
Última revisión	16 de Noviembre 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

e67fdd41896f179eb8a8e33171011687a75d64149a2b9d70e418a56702d8037f
fe51cfe8bfebd7912fab5269ba2f2f8bed2b455045d0e6de78cee6e05d090606
e6c9a39863fe8541b4a57b54fd2fd342de4c8246c19798e7a1d25f5ab6d7b7f0
70d2867c766b54c413360ee05632ef75f5dd67d414dfdb23a1eb5d7831ef2681
e35022da0ce64e1fa71838f4db5344ccb9d432065ae01a6ef6f50f8437645ab1
4983bd5fd9e1316ddc152720390bfa6ca83de9493eb0f12d76fa585f3795ffa7
bbe85d35d87417aaddee6aefc5701dfe76fe7b22b9fe2d675c50e33a67ee4fef
6116d689621dbb133b8aa118c9f777044ff3416ff57d83e4ed3fa5310cfaef25

IoC nombre de archivo

Nombres de Archivos con Malware

mgj5zf1.jpg
PI.gz
SOA oct 2020.rar
Scan Copy of COO.r00
Fact-029283-121120.img
HBL CreditCard 4902.gz
TT COPY.zip
01181450011155.gz

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

82.114.162.38
23.238.48.117
203.124.39.163
103.99.1.172
203.124.39.163
190.145.77.219
185.222.57.252

IoC Correo Electrónico

Correo electrónico de donde fue enviado

a-m-wahlstrom@abbeytitle.com
tech@lyship.com
personnel@technosteel-uae.com
prvs=05820a4f30=Watania@yemen.net.ye
teresa.seguei@floramatic.com
atiqa@rdlpk.com
jimmy.leatherbank@gmail.com
atiqa@rdlpk.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: 2020.11.16 22:37:31 -03'00'