Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	2CMV20-00122-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Diciembre de 2020
Última revisión	18 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

ad49792b1c23ff2ac87b924a4c6575d0e06f5c2a5520172d85addf0a9b7b5236
454b93f25bcca014d758bf7d8caac0c615c328bd35fa9be0fc03732dfc7209d9
aecd152282def027bfd51b70b018af2c80dabf50c52ba4100c71c1047fe027dd
78cb5ccd1e9ae32d83d8eb6c4144e17150709c210fee9b28a692169809a0f81f
131c0800e1400e25fba579755d90f9a3afcf7fcefe86e5b7178b8c4389cfa89c
2fa4d0c9f754437c49482bceba78a4f36d60b11995ade031ce731028698cb615
81bb2dfe82ab75a170c4d73d51633e7879468a5bb22024eefed8fdc2abf5cab3
697234a66ea01428164440034fcd15f9dc45ff3434f090f641bab6ebf0e95a26
17360343aeba1cad7a0e07554d295d3f84c4a82b5a949272ff89f5ef5dab9a30
c2aa078c0aa7586366efa7b9190004dbdbed735abf183483da41030eba155d0a

IoC nombre de archivo

Nombres de archivos con Malware

PI-OEED22GMS.ppt
PI-OEED20GMS.pps
REQUEST FOR QUOTATION.r00
JTC20-PO074.075.zip
Purchase-Inquiry.lha
Cfresard-71538-8693-22-022476.HTM
mail21575.zip
DHL Detail.lzh
Spec.zip
KMT_00983839300.pdf.z
PROFORMA INVOICE.zip

IoC servidor SMTP

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

45.11.19.69
154.127.53.116
104.47.32.55
45.88.76.19

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

crm@aminequipments.com
jack.miller@chamundeshwari.com
rohit@axonoutsourcing.com
modial@globalnet.es
supply1@tsl-me.com
divakar@integraqatar.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.