Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	2CMV20-00110-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Noviembre de 2020
Última revisión	28 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

3f84f4066f10a19dbd3a8166e191ce77f9b30cb063bc2958e7adfeb0ff4ba73e
765479a105fd76a3f3793014597a9f96fc9c6b62e9a0752eb0b9ba9b8e8d7221
559414341d8cfd33236037c31aacc503edf05f5babde9ef10e641638d9c2c36e
e2a62f1e976390ab92ba2448f9949bee0fb8b71a41e38c4e9cba597a2f9b12cf
b828f049dfe16d430ab605d22751b7b9d6f09d80072b728b499ba3dbe428f7a2
de16ac1476751c9c3299908201515af30e740c2b6133783b34dccfd9a6416df9

IoC nombre de archivo

Nombres de archivos con Malware

BL / SURRENDER PDF.htm
po-9098-update.rar
PO983767467.rar
PEDIDO DE COMPRA-34002174,pdf.iso

IoC servidor SMTP

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

202.230.222.70
202.230.222.69
188.93.233.117
202.230.222.68
202.230.222.67
202.230.222.66
202.230.222.65
202.230.222.64
202.230.222.63
202.230.222.62
202.230.222.71
104.168.245.162
92.60.142.98

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

export@tesartesisat.com
jetchehu@zeni.com.ar
pt@hinewdubai.pw
support@hengfengsteel.org

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.