# Alerta de Seguridad Cibernética

| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00130-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 07 de Enero de 2021 |
| Última revisión | 07 de Enero de 2021 |

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

9c3a55f232d16099aefb638734d0bf5e3cfc1d353511cc940b8bc78eb8eade43
edccbee11901bbab7e53ce56b3f91ded2ebfe855f0529e9af035bf02926f23d7
af82c606594a45a22ee92b565a0f660c5747e865b42b2bff0c8f54973c6430a5
75da0babaec2dc03b34b3ac5a3a1d29befb6e45edcf9e079af9150416df63df4
f41191d034c431b657fe3879db9d982768d93e77fff9ba0cae2f7aa6de52a6e6

## IoC descarga malware URLs

URLs que son disparadas por la infección inicial del malware. Podrían existir otras no detectadas:

https://mirvalgroup[.]com/wp-includes/FOeYo/
https://wp.gensoukyou[.]org/souzinv_old/1a/
https://walkerswebshop[.]com/images/O7/
http://mail.ninosindigochile[.]cl/1989-gmc-oq21w/ZVTCY/
http://www.dirgantaratuba[.]com/cgi-bin/PX4K/
https://unimedunihealth[.]com/wp-includes/E/

## IoC nombre de archivo

Nombres de archivos con malware:

INVOICE.rar
Purchase Order KV_RQ-7436819.ace
New PO.zip

## IoC servidor SMTP

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

82.57.200.98
82.57.200.99
81.91.176.150
69.12.73.228
82.57.200.100
203.128.6.25

## IoC Correo Electrónico

Correo electrónico de donde fue enviado:

vcalzolari64@tim.it
eva@hkshengpin.com
chad@greaterdimensions.com
marketing@aruj.com.pk

## 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.