| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV20-00098-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Octubre de 2020 |
| Última revisión | 19 de Octubre 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

9cfbbbcff3acfb13c82151c25ea08e17453df5bd5b386f8723c8fe052a75a59d
b10d8ac487e2dfdfbbfa9d4029aea864977661ae8e73bada2b5f179bd6af26ab
5685e71717caf80fca91df51648e35f5d266c49de2b845c375acd6506153545e
207e75c5558fce35381b385a90cdfcf46475be713c42762e3a616396c755aa31

## IoC nombre de archivo

Nombres de Archivos con Malware

Verify your account.html
MKWF 152020.rar
product specification.xlsx
Products.xlsx
Agro Mega Trading RFQ.xlsx

## IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

37.49.225.230
96.9.210.197
103.141.138.129

# IoC Correo Electrónico

Correo electrónico de donde fue enviado

rdlstore2@radiancegroup-bd.com
omar.r@electro-sm.com
administrator@postmaster.net
gurban@viacorreo.com.ar
Suriad.sct@samsung.com
patrhoyt29favy@gmail.com
gateanh@gmail.com
info@oxcardcabman.club
dysonkizz7ox@gmail.com
dysonkizz7y@gmail.com
golasage265ggi@gmail.com
rakesh@shakunpolymers.com
startextile@cyber.net.pk
robikris22rupoy@gmail.com
fernayes9r@gmail.com
jonespatr72fegwt@gmail.com
fantjame060sp@gmail.com
lacejoly2yu@gmail.com
uzma.euroasia@euroasiachem.com
fadecice330durxt@gmail.com
judivalo036eer@gmail.com
polafutj1ok@gmail.com
quelenluis@playonne.com
kipemilf56crupd@gmail.com
polafutj1leqm@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.