Alerta de seguridad informática	2CMV20-00050-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Febrero de 2020
Última revisión	12 de Febrero 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware global de fabricantes de moldes.

El mensaje del correo en inglés, incita que se abra el archivo adjunto para poder revisar una lista de productos ofrecidos al usuario que recibe este correo.

En el mensaje se adjunta un archivo comprimido, al momento de abrir el ejecutable que se encuentra dentro del archivo ZIP se activa el malware.

Indicadores de compromisos

Servidor Smtp
[213.159.30.223]

Sender
Info[@]doriane-copar[.]com

Asunto
Re: Re: Re: New Order

Archivos adjuntos.

Archivo : New Purchase Order.zip
SHA-256 : 25B69382D17809765F860032C352BA56079A0D49DE6C1F3A26BBD3FF066243F0

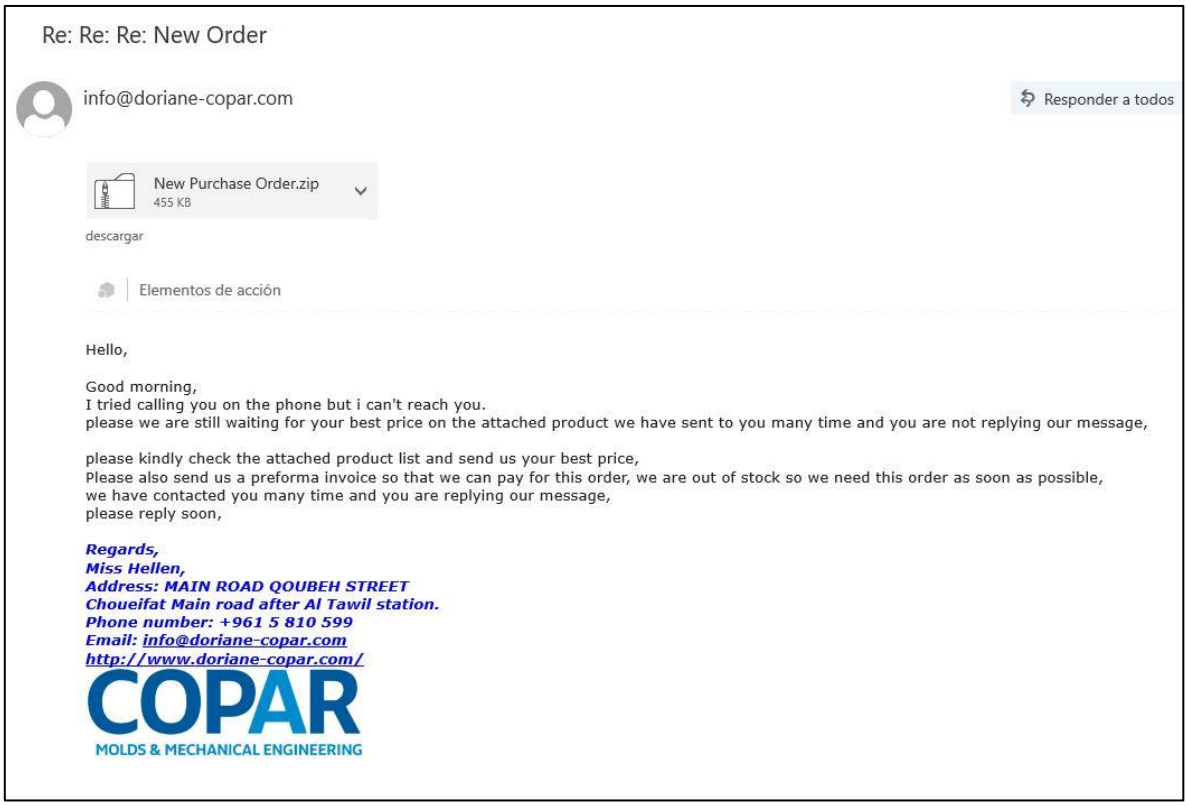
Archivo : orderpdf.exe
SHA-256 : CC6D0E75AD2304C433455CB5C33070A68B05F28AEF8F3B37607384E589CE12F5

Archivo : skype.exe
SHA-256 : cc6d0e75ad2304c433455cb5c33070a68b05f28aef8f3b37607384e589ce12f5

Archivo : XZSKS.exe
SHA-256 : CC6D0E75AD2304C433455CB5C33070A68B05F28AEF8F3B37607384E589CE12F5

Archivo : skype.vbs
SHA-256 : E38BA5103826050DE43C264999C85E39932C289D89F938611BAC4BDA3CFAC7BE

Imagen Mensaje



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.12 18:06:57 -03'00'