Alerta de seguridad informática	2CMV21-00129-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2020
Última revisión	06 de Enero 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 suplantando al Banco BBVA.
El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.
El mensaje del correo indica que se adjunta una factura de pago.
El atacante adjunta un archivo comprimido que al ser ejecutado gatilla la infección del equipo.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

Datos del encabezado del correo

Servidor Smtp
[82.223.166.252 - mlmc822.servidoresdns.net]

Sender
huelvacamion@tacografosdigitales[.]es

Asunto
Orden de pago BBVA.PNG

IoC Archivo adjunto

Archivos que se encontraban adjunto en el correo

Nombre: Orden de pago BBVA.tgz
SHA256: BEFC59F442467A63D160C1A04B424C73087D398E8BD1870D8950E8E7C97C0B30

Nombre: Orden de pago BBVA.tar
SHA256: CFEA06D5F9BC813FCB6446F194BA79D8A5D1ED001AFA55CE312CB85F36D7A28C

Nombre: Orden de pago BBVA.exe
SHA256: EC810BF129F8ACC2DDD94E9761C34BDF7A071DD8041A4F74E410524EB9BE8A6F

IoC Comunicación de Red

"Username: ": "AQkRUHcnkX56Zj",
"URL: ": "http://oDS1ux8jHuPIBx1B[.]com",
"To: ": "catalinafuster@palmaprocura[.]com",
"ByHost: ": "smtp.1and1[.]es:587",
"Password: ": "=0AviqwAV",
"From: ": "catalinafuster@palmaprocura[.]com"

Imagen del mensaje

Querido señor, señora

Nos complace informarle que su cliente ha confiado a BBVA la gestión del pago de las facturas detalladas en el documento adjunto.

Saludos cordiales,
Facturación y pago

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.

CSIRT Gobierno de Chile