Alerta de seguridad informática	2CMV21-00346-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Septiembre de 2022
Última revisión	21 de Septiembre de 2022

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 de Gobierno) ha identificado una nueva campaña de phishing con malware. En ella, el mensaje es enviado desde una dirección de correo que suplanta a una entidad municipal.

En el correo, el atacante no describe nada, solo adjunta un archivo comprimido para que sea abierta por el receptor del mensaje. Si la victima ejecuta el archivo con un supuesto pdf, este acciona un tipo de malware llamado Redline.

Redline es un ejemplo de MaaS (Malware-a-as-Service) utilizado para sustraer información. Es capaz de recopilar información como inicios de sesión, contraseñas, datos de autocompletar, cookies y detalles de tarjetas de crédito de todos los navegadores web de los equipos que infecta.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto	Correo de Salida
(sin asunto)	egis.lolol@gmail.com

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre	SHA256
Document_iXRMjTBCuC_2.zip	8d02bd62d1e1f6c1e71ab8c5133933ce58b908a6bf01130877320c2c2f9a7ac1
Document_iXRMjTBCuC.zip	11c48b78a99bace6753b56701d4f17a39c300ad1fd3b511679907b290614a263
Document.pdf.rar	2315c1385b4bedcc4f7fe0b08a383450c873ba81033e7ef347697c4032cd78a8
Document.pdf.scr	dc7ef7b92c427b3e04afe4cb73ce3b766c1e53b24d1cf68e96a3785840cfe0fb
annotation.UnsupportedAppUsage.module10.exe	140813a0a56d26c95c94addd1d44462cd93d51d5f66b9bd2ea00b94f9b8d8d52

Command and Control

62.204.41[.]139:25190
http://193.106.192[.]223/annotation.UnsupportedUsage.module10_Nmntgivf.bmp

Imagen del Mensaje

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

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.21 15:40:32 -03'00'