Alerta de seguridad informática	2CMV22-00348-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Septiembre de 2022
Última revisión	22 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 CSIRT de Gobierno. 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 personal, y en él, el atacante responde a una supuesta postulación a un puesto laboral.

Si la víctima interactúa con el archivo adjunto, se ejecuta un malware llamado Agent Tesla, un troyano de acceso remoto (RAT) con varias capas de ofuscación, el cual toma capturas de pantalla, registra el uso de las teclas y sustrae contraseñas de navegadores web.

.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto	Correo de Salida
Curriculum Vitae Rita	vipechi@gmail.com

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre	SHA256
Curr&#65533;culum Vitae Rita.zip	95cec8fc25e5a9779e991f002c78a786c3dd9354acbb0820f90528e9ac39f043
Currículum Vitae Rita.exe	64cc998a2f7e9e180ef01e860eaf4fa6ec9cd397cf10a2798540f84b9af48095

Imagen del mensaje

Buenos días señor,

Mi nombre es Rita y me gustaría postularme para el puesto de asistente según lo anunciado

Adjunto mi currículum.

Gracias de antemano!

Sinceramente:
Rita Magyar

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: 2022.09.22 15:06:27 -03'00'