CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Incidente informático en la región del Caribe

Fecha: 1/09/2022

Problemática: Incidente cibernético en Servicios Públicos en la República de Chile

Correlativo: AA-0017

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT del Gobierno de la República de Chile, informa sobre un incidente en progreso que afecta a un servicio del gobierno, durante la jornada del jueves 25 de agosto de 2022, el cual ha interrumpido el funcionamiento de sus sistemas y servicios en línea.

SITUACIÓN

De acuerdo a la investigación realizada por el Centro Estratégico de Monitoreo-CEM,, la naturaleza del incidente corresponde a un Ransomware que afectó servidores Microsoft y VMware ESXi en redes corporativas de la institución. El ransomware en cuestión tiene la capacidad de detener los servicios de máquinas virtuales en ejecución y cifrar archivos relacionados con las máquinas virtuales. Para llevar a cabo la infección utilizaría el algoritmo de cifrado de clave pública NTRUEncrypt, dirigido a archivos de registro (.log), archivos ejecutables (.exe), archivos de bibliotecas dinámicas (.dll), archivos de intercambio (.vswp), discos virtuales (.vmdk), archivos de instantáneas (.vmsn) y archivos de memoria (.vmem) de máquinas virtuales, entre otros.

La infección del ransomware con características de infostealer realiza las siguientes acciones conjuntas:

Roba credenciales desde los navegadores
Enumera dispositivos de extracción como HDD y pendrives, y
Posee capacidades de evasión de antivirus con timeout.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

RECOMENDACIONES

Considere implementar:

1. Servicios de Antivirus/Antimalware.
2. Herramientas de Prevención de Intrusiones en la red (IDS)
3. Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)
4. Herramientas de Detección y Respuesta Extendidas (XDR)

Es importante:

5. Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
6. Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos y programas ofimáticos.
7. Implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de datos que se pueden usar para restaurar datos de la organización.

DICCIONARIO DE DATOS

1. Infostealer: Nombre genérico de programas informáticos maliciosos del tipo troyano, que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial.
2. Endpoint Detection and Response-EDR (Detección y Respuesta de Amenazas de Puntos Finales): Tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas
3. Extended Detection and Response - XDR (Detección y Respuesta Extendidas): Tecnología de ciberseguridad que monitorea y mitiga las amenazas de ciberseguridad
4. Cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.
5. Malware: Es un programa malicioso que tiene como característica principal su alto grado de dispersabilidad, es decir, lo rápidamente que se propaga.
6. Ransomware: Es un tipo de malware que impide y/o secuestra el acceso a archivos del sistema infectado, en ocasiones cifrándolos, y coacciona al usuario para pagar un rescate a cambio de su liberación.

REFERENCIAS

1. Documentación alerta CSIRT https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-incidente-en-servicio-publico/
2. https://www.welivesecurity.com/la-es/2022/09/02/ataque-ransomware-compromete-sistemas-sernac-chile/

ÁREA PARA DEFINICIONES

La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.

La presente herramienta tiene aplicación práctica derivado a un proceso previo de análisis con base al contexto y la situación del evento, sin embargo, se aclara que el presente sirve como guía y marco de referencia.