CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Actividad Cibernética

Fecha: 09/07/2023

Problemática: Troyano W32/lockerdb /crypter

Correlativo: AC-0052

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Recientemente fue descubierto el troyano tipo malware identificado como W32/ lockerdb /crypter , este tipo de malware se caracteriza por realizar actividades sin el conocimiento del usuario. Estas actividades suelen incluir el establecimiento de conexiones de acceso remoto, la captura de entradas del teclado, la recopilación de información del sistema, la descarga/carga de archivos, la colocación de otro malware en el sistema infectado, la realización de ataques de denegación de servicio (DoS) y la ejecución/terminación de procesos.

SITUACIÓN

El troyano W32/ locker /crypter se caracteriza por inyectores que insertan código malicioso en los procesos que se ejecutan en una computadora para realizar varias acciones, como descargar malware adicional, interferir con las actividades de navegación web o monitorear las acciones del usuario.

Efectos conocidos por la infección del troyano:

- Corromper los datos del programa
- Otorgar acceso no autorizado a los datos
- Bloquear el programa o provocar una denegación de servicio
- Monitoreo o manipulación de la actividad del navegador web
- Supervisar o manipular las acciones del usuario en el dispositivo afectado
- Descarga de programas o componentes adicionales en el dispositivo afectado
- Permitir que un atacante remoto tome el control completo del dispositivo afecta

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 soluciones de ciberseguridad que permitan mitigar el efecto de estos códigos maliciosos.
- Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos periódicas que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación

DICCIONARIO DE DATOS

- Troyano: malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.
- Código Arbitrario: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
- Malware: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.

REFERENCIAS

1. https://www.f-secure.com/v-descs/trojan_w32_injector.shtml
2. https://www.fortiguard.com/threat-research/map/country/GT
3. https://www.fortiguard.com/encyclopedia/virus/10111052