CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenaza Cibernética

Fecha: 13/05/2022

Problemática: Ransomware criptográfico

Correlativo: AC-0037

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

La Oficina Federal de Investigaciones (FBI), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y el Departamento de Salud y Servicios Humanos (HHS) de Estados Unidos, emitieron un comunicado para informar sobre la actividad realizada por el actor de amenazas "Hive Ransomware", que ha afectado a más de 1,300 compañías en todo el mundo y, han recibido aproximadamente 100 millones de dólares en pagos de rescate (extorsión) para recuperar la información.

SITUACIÓN

Hive ransomware sigue el modelo de ransomware-as-a-service (RaaS). El método de intrusión inicial dependerá de qué afiliado apunte a la red. Los actores de Hive obtuvieron acceso inicial a las redes de las víctimas mediante el uso de inicios de sesión de un solo factor a través del Protocolo de escritorio remoto (RDP), redes privadas virtuales (VPN) y otros protocolos de conexión de red remota. En algunos casos, los actores de Hive omitieron la autenticación multifactor (MFA) y obtuvieron acceso a los servidores de FortiOS mediante la explotación de vulnerabilidades y exposiciones comunes (CVE) CVE-2020-12812. Esta vulnerabilidad permite que un actor cibernético malintencionado inicie sesión sin solicitar el segundo factor de autenticación del usuario (FortiToken) cuando el actor cambia las mayúsculas y minúsculas del nombre de usuario. Los actores de Hive también obtuvieron acceso inicial a las redes de las víctimas al distribuir correos electrónicos de phishing con archivos adjuntos maliciosos y al explotar las siguientes vulnerabilidades identificadas como CVE-2021-31207 CVE-2021-34473 CVE-2021-34523 contra los servidores de Microsoft Exchange. Después de obtener acceso, el ransomware Hive intenta evadir la detención mediante la ejecución de procesos para:

- Identificar los procesos relacionados con las copias de seguridad, el antivirus/antispyware y la copia de archivos y luego finalice esos procesos para facilitar el cifrado de archivos.
- Detener los servicios de instantáneas de volumen y elimine todas las instantáneas existentes a través devssadminen la línea de comandos o a través de PowerShell.
- Eliminar los registros de eventos de Windows, específicamente los registros del sistema, seguridad y aplicaciones [T1070].

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

A continuación se muestra el siguiente link https://www.cisa.gov/uscert/ncas/alerts/aa22-321a donde podrá encontrar las recomendaciones necesarias para mitigar y minimizar el riesgo ante un ataque cibernético.

- 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

- Atacante: Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.
- Código Arbitrario: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit).
- Ransomware: Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella.

REFERENCIAS

1. https://www.cisa.gov/uscert/ncas/alerts/aa22-321a
2. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31207
3. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34473
4. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34523