CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenaza Cibernética

Fecha: **10/10/2023**

Problemática: **Campaña cibernética Grayling APT**

Correlativo: **AC-0085**

Institución / Sector: **Sector Público y Privado**

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	**Alto**	**Alta**	**Alta**

CONTEXTO

Investigadores de ciberseguridad de Symantec Threat Hunter descubrieron la campaña de ataque cibernético bajo el nombre «Grayling APT» en todas las industrias.

SITUACIÓN

Actor de amenazas de procedencia desconocida ha sido vinculado a una serie de ataques dirigidos a organizaciones de los sectores de fabricación, TI y biomédico en Taiwán.

Symantec Threat Hunter atribuyó los ataques a una amenaza persistente avanzada (APT) que rastrea con el nombre de «Grayling». La evidencia muestra que la campaña comenzó en febrero de 2023 y continuó al menos hasta mayo de 2023.

El grupo de APT está explotando cadenas de ataque que aprovechan la carga lateral de DLL a través de SbieDll_Hook para cargar una variedad de cargas útiles, incluidas Cobalt Strike, NetSpy y el marco Havoc, junto con otras herramientas como Mimikatz

Según el informe emitido por el ente investigador es probable que el objetivo de la actividad sea una agencia gubernamental ubicada en las islas del pacífico, así como entidades en Vietnam y Estados Unidos, con el objetivo de recopilar información de inteligencia.

RECOMENDACIONES

- **Auditar aplicaciones en busca de vulnerabilidades de seguridad explotables.**
- **Monitorear y analizar patrones de tráfico e inspección de paquetes asociados a protocolos que no siguen los estándares de protocolo y flujos de tráfico esperados.**

DICCIONARIO DE DATOS

- **Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.**
- **Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.**
- **Puerta Trasera: Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.**
- **APT: Ataques a una amenaza persistente avanzada**

REFERENCIAS

https://thehackernews.com/2023/10/researchers-uncover-grayling-apts.html

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks