CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenaza Cibernética

Fecha: 03/10/2023

Problemática: Grupo de Amenaza persistente avanzada (APT)

Correlativo: AC-0077

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Investigadores de ESET ligaron al grupo Lazarus APT, vinculado a Corea del Norte a un ciberataque dirigido a una empresa aeroespacial española.

SITUACIÓN

Actores de amenazas se hicieron pasar por reclutadores de Meta a través de la red social LinkedIn Messaging y enviaron dos desafíos de codificación a los empleados de la organización con el objetivo de engañarlos para que abrieran el archivo ejecutable con código malicioso. La víctima descargó y ejecutó en un dispositivo de la empresa el archivo lo que desencadeno el ataque. El primer desafío es un proyecto muy básico que muestra el texto "¡Hola, mundo!", el segundo imprime una secuencia de Fibonacci: una serie de números en la que cada número es la suma de los dos anteriores.

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**

RECOMENDACIONES

- Verifique la fuente de información de los documentos que recibe
- Nunca entre en la web de su banco pulsando en links incluidos en correos electrónicos
- El phishing sabe idiomas, por lo que puede atacarte por medio de distintos idiomas

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.
- Phishing: Estafa o fraude informático mediante correo electrónico, mensaje de texto u otro medio tecnológico donde se suplanta la identidad de una persona o empresa de confianza
- APT (Advanced Persistent Threat): Amenaza avanzada persistente es una amenaza que se caracteriza por estar dirigida a un objetivo específico

REFERENCIAS

BLEEPING COMPUTER
https://securityaffairs.com/151771/apt/lazarus-targets-spanish-aerospace-firm.html