CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenazas cibernéticas

Fecha: 06/11/2023

Problemática: Actor de amenazas «Lazarus Group» incrementó su actividad maliciosa

Correlativo: AC-0094

Institución / Sector: Público y Privado

CONTEXTO

kaspersy dio a conocer que un grupo de ciberdelincuentes aliado a Corea del Norte, está detrás de una nueva campaña de ciberataques mediante la explotación de fallas de seguridad conocidas.

Nivel de priorización

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

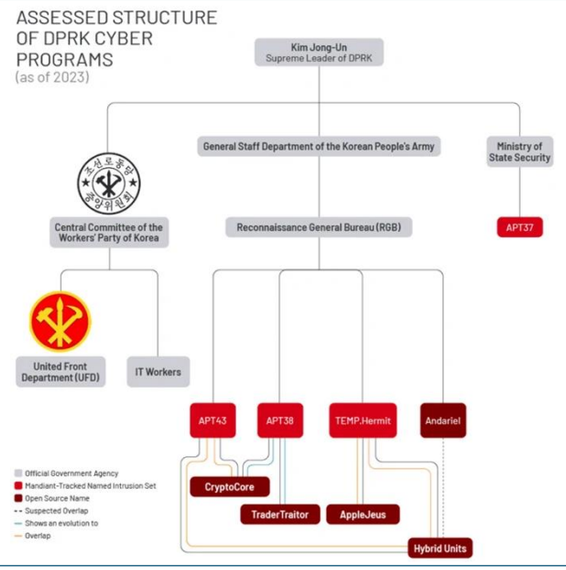
Matriz de Evaluación

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

RECOMENDACIÓN

- Deshabilite los protocolos de red heredados que pueden usarse para interceptar el tráfico de red
- Asegúrese de que todo el tráfico cableado y/o inalámbrico esté encriptado adecuadamente.
- Utilice las mejores prácticas para los protocolos de autenticación, como Kerberos, y asegúrese de que el tráfico web que pueda contener credenciales esté protegido por SSL/TLS.
- Utilice dispositivos de red y software de seguridad basado en host para bloquear el tráfico de red que no es necesario dentro del entorno
- Limite el acceso a la infraestructura de red y los recursos

ANEXO



REFERENCIAS

The hacker News
https://thehackernews.com/2023/10/lazarus-group-targeting-defense-experts.html

KASPERSKY
https://securelist.com/apt-trends-report-q3-2023/110752/