ALERTA

Ciberatacantes aprovechan IA para desarrollo de amenazas

COLCERT AL-1807-037

TLP:CLEAR

NullBulge

"Esta organización ha demostrado una capacidad notable para infiltrarse en las cadenas de suministro de software"

NullBulge es un nuevo y sofisticado grupo de ciberdelincuentes que ha emergido en el panorama de las amenazas cibernéticas, centrando sus ataques en comunidades de desarrolladores de inteligencia artificial (IA) y videojuegos. A pesar de proclamarse defensores de los artistas y oponerse a la IA, sus acciones revelan un claro interés financiero

Modo de operación:

El grupo distribuye malware a través de estos canales, infectando archivos y paquetes con código malicioso que permite el acceso remoto a los sistemas de las víctimas.

Impacto en la seguridad digital Nacional:

También se distribuye otro tipo de malware como:

Async RAT: Un troyano de acceso remoto visto en Colombia en multiples eventos.
Xworm: Un gusano que se propaga automáticamente a través de redes.
Ransomware LockBit personalizado: Un tipo de ransomware.

Para protegerse y evitar técnicas de estos ciberataques:

- **Verificar la procedencia del software:** Desconfiar de software descargado de fuentes no confiables.
- **Mantener los sistemas actualizados**: Aplicar parches de seguridad de forma regular.
- **Utilizar herramientas de seguridad:** Implementar soluciones de seguridad robustas, como antivirus y sistemas de detección de intrusos.
- **Segmentar las redes**: Aislar las redes internas para limitar el impacto de una posible infección.

NullBulge es un grupo de ciberatacantes altamente sofisticado que representa una amenaza creciente para la comunidad e Infraestructuras Críticas.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://www.infosecurity-magazine.com/news/nullbulge-anti-ai-hacktivist-group/

https://hackread.com/disneys-internal-slack-breached-nullbulge-leak-data/

COLCERT