# FASTREANDO

## NullBulge: ciberatacantes aprovechan la IA para crear nuevas amenazas

### Resumen

Ha emergido un nuevo grupo de ciberdelincuentes llamado NullBulge, que ataca comunidades de desarrolladores de inteligencia artificial y videojuegos. Aunque dicen defender a los artistas y oponerse al uso indebido de IA, sus actividades demuestran un claro interés financiero. Sus operaciones incluyen distribución de malware, infiltración de la cadena de suministro de software, acceso remoto ilícito, y uso de ransomware, entre otras tácticas. El riesgo es considerado de nivel medio.

### Detalles de la amenaza: quiénes, objetivos y motivación

El grupo autodenominado NullBulge se perfila como un actor emergente que combina rasgos de hacktivismo con claros intereses económicos. Sus objetivos principales se centran en comunidades y proyectos vinculados con la inteligencia artificial, como modelos, plugins y repositorios de datos, así como en desarrolladores y modders de videojuegos y plataformas de código como GitHub o Hugging Face. Aunque se presenta como un movimiento de protesta contra el uso de la IA que, según ellos, perjudica a los artistas, sus actividades evidencian motivaciones de lucro mediante la filtración y venta de datos, extorsión y otras prácticas ilícitas.

### Modo de operación (tácticas, técnicas y procedimientos)

El grupo NullBulge se infiltra en comunidades digitales creando cuentas o proyectos que aparentan ser legítimos y útiles, como paquetes de software o modificaciones para inteligencia artificial y videojuegos. De esta forma, logran generar confianza entre desarrolladores y usuarios.

Una vez ganada esta confianza, distribuyen código o binarios contaminados en repositorios públicos o paquetes de terceros. Al ser descargados e instalados, estos componentes activan el malware oculto, comprometiendo los equipos y entornos de desarrollo.

Dentro de los sistemas, los atacantes despliegan herramientas que les permiten establecer persistencia y movimiento lateral, como troyanos de acceso remoto (RATs). Con ellas roban credenciales, exploran secretos en repositorios y pipelines de CI/CD, y amplían su control sobre la red.

Posteriormente, se produce la exfiltración de información sensible, incluyendo mensajes, código y credenciales, que puede ser utilizada para extorsión o publicada de forma masiva como demostración de poder.

**Malware asociado**

- AsyncRAT (Troyano de Acceso Remoto – RAT): otorga control remoto completo al atacante, con funciones como keylogging (capturar y registrar pulsaciones de teclado), captura de pantallas, transferencia de archivos y ejecución de comandos. Se distribuye usualmente mediante adjuntos maliciosos o binarios trojanizados.

- XWorm (gusano / troyano de acceso remoto modular): combina funciones de acceso remoto con capacidad de propagación automática a través de redes, además de descargar y ejecutar cargas adicionales.

- LockBit (ransomware personalizado): cifra archivos, elimina o deshabilita copias de seguridad, roba información y exige rescates. Funciona bajo el modelo de Ransomware como servicio, lo que facilita la creación de variantes adaptadas para evadir defensas y propagarse en redes comprometidas.

## Recomendaciones (Buenas prácticas de protección).

Para mitigar el riesgo y proteger los sistemas, aplicaciones y redes se debe realizar lo siguiente:

1. **Verificar la procedencia del software**
    - Descargar solo de fuentes confiables y autorizadas
    - Evitar software pirateado o no verificado
2. **Mantener los sistemas actualizados**
    - Instalar parches de seguridad tan pronto estén disponibles
    - Actualizar sistemas operativos, marcos de trabajo, librerías, software de terceros
3. **Utilizar herramientas de seguridad robustas**
    - Antivirus con firma y comportamiento
    - Sistemas de detección de intrusos (IDS/IPS)
    - Monitoreo continuo de logs de seguridad
4. **Segmentar las redes**
    - Separar componentes críticos del resto de la red
    - Limitar accesos según necesidad (principio de mínimo privilegio)
5. **Capacitación y concienciación de usuarios**
    - Formar al personal sobre phishing, ingeniería social, riesgos de instalar software desconocido
    - Promover buenas prácticas de seguridad al manejar software y recursos externos

Tomado de: articles-383602_Documento_1.pdf