AYI NEDJIMI Consultants

LLM et reverse engineering — analyser le malw

16 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture •

Automatisez l'analyse malware avec les LLM : Ghidra + LLM API, classifica
d'IOC, analyse CFG. Guide technique pour analystes malware et reverse e

À RETENIR

A retenir -- LLM et reverse engineering malware

L'integration des **LLM dans le reverse engineering de malware** accelere dram
classification automatique des fonctions (benigne/malveillante/crypto/C2), l
l'annotation automatique du code desassemble reduisent de 60 a 80% le ten
headless + LLM API est la combinaison la plus deployee en 2026. Les halluci
restent la limite principale : valider systematiquement les conclusions LLM av
fonctions critiques. L'analyse du ransomware BlackSuit et de Nitrogen en 20
ces pipelines.

Le **reverse engineering de malware assiste par LLM** represente l'une des avance de code malveillant depuis l'introduction des debuggers interactifs. Face au volum 500 000 nouvelles souches identifies par jour selon Kaspersky Security Bulletin 2 peuvent plus se permettre d'analyser chaque echantillon manuellement. L'integrat Ghidra et IDA Pro permet de transformer des fonctions desassemblees en descrip comprehensibles, d'extraire automatiquement les IOC (Indicators of Compromise) (crypto, network, persistance, C2), et de generer des rapports d'analyse en quelq heures. Cet article presente l'architecture technique complete d'un pipeline de rev code Python pour l'integration Ghidra/LLM, une analyse de cas reels (BlackSuit ra considerations pour le depoiement en production, et les limites importantes a con hallucinations LLM sur du code desassemble complexe.

Architecture du pipeline Ghidra + LLM

Le **pipeline de reverse engineering LLM** se compose de quatre etapes principales

Decompilation Ghidra : utiliser Ghidra en mode headless pour decompiler le bi decompilees en pseudo-C ou en bytecode annote

Preprocessing : normaliser le code decompile (renommer les variables generiq donnees connues, resoudre les appels d'API Windows)

Analyse LLM : soumettre chaque fonction au LLM pour classification, descripti

Agregation et rapport : consolider les analyses par fonction en un rapport d'en malware, les IOC et les recommandations de detection

Réponse sous 24h

Devis gratuit →