Artificially Intelligent MALware Launcher

AIMaL – Artificially Intelligent Malware Launcher

Developers: Endrit Shaqiri (endritshaqiri2016@gmail.com) & Natyra Shaqiri (natyrashaqiri@smccme.edu)

DEF CON 33 Presenter — Red Team Village & Demo Labs
Live demonstrations of AV bypassing, real-time code rewriting, AI-generated evasion functions
Connect with us for collaborations, sponsorship, or recruitment!

Project Summary

AIMaL is a **self-mutating red team evasion engine** that integrates AI (OpenAI API) to dynamically adapt to real-time AV/EDR detection feedback. Designed for adversarial simulation and stealth malware R&D, AIMaL can automatically rewrite its own evasion techniques and payload execution logic based on whether detection is **signature-based or behavioral-based**.

Key Capabilities

- **Multiple Evasion Techniques** (ET): Includes Process Hollowing, Ghosting, Herpaderping, and AI-generated novel methods
- **Multiple Execution Techniques** (XT): Supports APC, Thread Hijacking, and more
- **Payload:** Stealthy Reverse Shell (C++), and more under development
- **AI Feedback Loop:**
    - If **signature-based** detection: Injects junk code, polymorphs shellcode, compresses source ⇒ regenerates binary hash
    - If **behavioral-based** detection: Triggers **LLM Self-Patch Mode**, rewriting or generating a brand-new stealth technique based on real AV behavior logs
- **Bypasses** almost all major AVs including:
    - Kaspersky, Bitdefender, McAfee, ESET, Malwarebytes, Windows Defender
- **Real-Time Code Rewriting:** Uses OpenAI API to rewrite ETs, or build brand-new ET

Technologies Used

- **Stack**: C++, WinAPI, Hell's and Heaven's Gate, OpenAI API, AES-256-CBC, XOR
- **Stealth Techniques**:
    - Fake API noise, syscall mutations (Hell's → Heaven's Gate), polymorphism, execution delay, junk code, PPID spoofing, AMSI & ETW patch, NTDLL unhook
- **Delivery**: GitHub-hosted encrypted payload, runtime download + decryption

Impact & Purpose

- Simulates advanced persistent threat (APT)-like behavior
- Ideal for red team labs, AV/EDR stress testing, or secure AI/malware research
- Built for offensive security research

Available for collaborations and job offers. Contact us! github.com/EndritShaqiri/AIMaL