

Forum: [Hack Forums](#)

Thread: [BeatRev - POC For Frustrating/Defeating Malware Analysts](#)

DI?E - October 6, 2022, 7:34 pm

The first time the malware runs on a victim it AES encrypts the actual payload(an RDLL) using environmental data from that victim. Each subsequent time the malware is ran it gathers that same environmental info, AES decrypts the payload stored as a byte array within the malware, and runs it. If it fails to decrypt/the payload fails to run, the malware deletes itself. Protection against reverse engineers and malware analysts.

Check it out: <https://github.com/Octoberfest7/BeatRev>

NotKover - October 6, 2022, 7:43 pm

(Oct 6, 2022 07:34 PM)DI?E Wrote: [\[CITE\]](#) The first time the malware runs on a victim it AES encrypts the actual payload(an RDLL) using environmental data from that victim. Each subsequent time the malware is ran it gathers that same environmental info, AES decrypts the payload stored as a byte array within the malware, and runs it. If it fails to decrypt/the payload fails to run, the malware deletes itself. Protection against reverse engineers and malware analysts.

Check it out: <https://github.com/Octoberfest7/BeatRev>

Cool find, i thought about making something similar for my loader but i felt it unnecessary