1. List the malware’s significant imports and strings, and its host-based andnetwork-based indicators.

Significant strings:

* System
* Molloc
* Action 001 does decryption

Significant imports:

* libc.so.6
* putchar@@GLIBC\_2.2.5
* system@@GLIBC\_2.2.5
* malloc@@GLIBC\_2.2.5
* \_\_isoc99\_sscanf@@GLIBC\_2.7

Host-based indicators:

* \_\_libc\_start\_main

Network-based indicators:

* none
* Connection made using TLSv1.2(tls.handshake.version:0x0303)



Significant strings, imports, host-based indicators, network-based indicators



Checks values, encrypts and decrypts

What it does:  
calls native functions, contains native function calls, from a malicious API. Has imported apis.

Data manipulation

Defense Evasion:  
Obfuscated files or information

Encode data using XOR

Encrypt data using AES

Reference AES constants