waht is Yara ? : Yara is one of the most used tools for malware research,
it is used to create signature detection and very useful for malware hunting.
The python library allows using Yara in your scripts with your own set of rules.

Output : [Note ! : The detection for metasploit staged malware only !]

[stager_reverse_tcp_nx_api_call_x64, stager_reverse_tcp_nx_next_mod_x64, stager_reverse_tcp_nx_loop_modname_x64, stager_reverse_tcp_nx_get_next_func_x64, stager_reverse_tcp_nx_loop_funcname_x64, stager_reverse_tcp_nx_finish_x64]