1. Import,String cua phan mem doc hai nay la gi

Kiểm tra PE Headers, import của Lab03-01.exe là kernel32.dll

2. Chi bao dua tren may chu cua phan mem doc hai nay la gi

Mã độc tạo ra 1 file thực thi C:\Windows\System32\vmx32to64.exe và sao chép phần mềm độc hại vào file này, tên file là một dấu hiệu để nhận biết.

Sau đó, mã độc tạo ra một khóa Run mới trong HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver với giá trị "C:\WINDOWS\system32\vmx32to64.exe" - giúp mã độc khởi chạy khi máy khởi động lại.

3. Co bat ky chi bao nao dua tren mang tren phan mem doc hai nay

Trong Process Explorer, ta thấy mã độc gọi 2 thư viện ws2\_32.dll và wshtcpip.dll, đây là các dll dùng trong việc xử lý các kết nối mạng và thực hiện các thao tác liên quan đến mạng.

Kiểm tra log inetsim và các gói tin được capture trên wireshark, ta thấy mã độc thực hiện query đến DNS www.practicalmalwareanalysis.com. Và sau đó mã độc thực hiện một bắt tay TCP, nhưng không phải là kết nối HTTPS. Kiểm tra Follow TCP Stream, giá trị Entire conversation bằng 256bytes và nội dung Stream chứa 256 bytes ngẫu nhiên, đây là các ký hiệu được mã độc sử dụng để thông báo cho máy chủ C&C rằng máy winserver 2008 bị nhiễm và sẵn sàng điều khiển.