Lab1-1

Q1: Does either file match any existing antivirus signatures?

Q2: When were these files compiled?

Q3: Are there any indications that either of these files is packed or obfuscated?

Q4: Do any imports hint at what this malware does?

Q5: Are there any other files or host-based indicators that you could look for on the infected system?

Q6: What network-based indicators could be used to find this malware?

Q7: What would you guess is the purpose of these files?

Lab1-2

Q1: Does either file match any existing antivirus signatures?

Q2: Are there any indications that either of these files is packed or obfuscated?

Q3: Do any imports hint at what this malware does?

Q4: Are there any other files or host-based indicators that you could look for on the infected system?

Lab1-3

Q1: Does either file match any existing antivirus signatures?

Q2: Are there any indications that either of these files is packed or obfuscated?

Q3: Do any imports hint at what this malware does?

Q4: Are there any other files or host-based indicators that you could look for on the infected system?

Lab1-4

Q1: Does either file match any existing antivirus signatures?

Q2: Are there any indications that either of these files is packed or obfuscated?

Q3: Do any imports hint at what this malware does?

Q4: Are there any other files or host-based indicators that you could look for on the infected system?