INFO-Y-119 Malware Reverse Engineering

name:
student number:
date:

The malware sample is available on the cloud share:

https://cloud.cylab.be/s/WoJCSxR9kLacFtw

with name:

sample.zip
(password: KmsErm2025!)

1. Flag to indicate prior infection (5pt)

a. Does the malware create a mutex or a semaphore that is used to indicate an already compromised host? If so, what is its full name and can it be used as an IoC (explain why)?

b. Does the malware create a registry key that is used to indicate an already compromised host? If so, what is its full name and can it be used as an IoC (explain why)?

c. Does the malware create a file that is used to indicate an already compromised host? If so, what is its full path and can it be used as an IoC (explain why)?

2. Persistence (5pt)

a. Does the malware save an executable file to the local filesystem with the purpose of being persistent? If so, what is its full path name and content, does the malware try to hide it? Can the file path be used as an IoC (explain why)?

b. How is the malware launched at startup? Can this mechanism be used as an IoC (explain why)?

3. CnC channel (5pt)

a. What is the hostname of the CnC server? Can it be used as an IoC (explain why)?

b. Is there a welcome message sent by the malware to the CnC server? If so what is it, and can it be used as a network IoC (explain why)?

4. Action on target (5pt)

a. What are the capabilities of the malware on the victim machine?

b. How is this implemented?

Brussels, 24jan25

Signature