Instructions:

Ensure that there are no blockers, such as Adblock extensions, that might prevent the lab from opening in a new tab or affect lab’s functionality.

All the lab-related files and tools are on the desktop in 'Start here' directory.

Scenario:

One of the employees reported receiving an email with a suspicious-looking attachment. Suspecting that a known Threat Actor may be attempting to use phishing to gain a foothold in the organization, you need to analyze the provided file and identify the threat.

Tools:

CyberChef

Wireshark

Strings

VS Code

LECmd

ProcMon