MALWARE ANALYSIS REPORT

General Information

Task ID	20250614-M9AD9L_1
Cuckoo Score	9
File Name	-

Machine Learning Classification

Binary Classification	MALWARE
Predicted Malware Type	-

Detected Signatures

Description
A process wrote data to an area of memory in another process.
A process was created using a dropped executable.
Drops file in user directory
Drops executable file
Uses schtasks.exe to create a new scheduled task.
Modifies registry value(s) to disable UAC checks.
Adds run entry to the registry to gain persistence across system reboots.
Modifies WinLogon for persistence