MALWARE ANALYSIS REPORT

General Information

Task ID	20250614-INYRQB_1
Cuckoo Score	10
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.
Created a process with a different parent than the creating process.
A privilege for an access token was adjusted. Windows uses the token to control the ability of the user to perform various system-related operations.
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
Drops file in Windows directory