MALWARE ANALYSIS REPORT

General Information

Task ID	20250614-RTR65F_1
Cuckoo Score	8
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.
The process deleted its own executable
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.
Enumerates physical disk devices, likely attempts to detect a virtual environment.
Drops file in user directory
Drops executable file