MALWARE ANALYSIS REPORT

General Information

Task ID	20250617-9ODTER_1
Cuckoo Score	10
File Name	-

Machine Learning Classification

Binary Classification	MALWARE
Predicted Malware Type	-

Detected Signatures

Description
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.
A process wrote data to an area of memory in another process.
Suspicious behavior detected: SetThreadContext
Drops file in user directory
Tries to open files used by common browsers to store saved passwords, cookies, user form data etc.
Harvests credentials from local FTP clients
Lokibot is a Password and CryptoCoin Wallet Stealer.
Drops executable file
Drops file in Windows directory