

LAPORAN ANALISIS MALWARE

Informasi Umum

Task ID: 20250614-2GBI4B_1

Skor Cuckoo: 10

Nama File: -

Hasil Klasifikasi Machine Learning

Klasifikasi Biner: **MALWARE**

Prediksi Jenis Malware: -

Deteksi Signature (Perilaku Mencurigakan)

- 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.
- Looks up registry value(s) which can often be used to detect a virtual environment.
- Drops file in user directory
- Drops executable file
- Uses schtasks.exe to create a new scheduled task.
- Adds run entry to the registry to gain persistence across system reboots.
- Modifies WinLogon for persistence
- Modifies registry value(s) to disable UAC checks.
- Drops file in Windows directory