

# LAPORAN ANALISIS MALWARE

## Informasi Umum

**Task ID:** 20250614-M9AD9L\_1

**Skor Cuckoo:** 9

**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.
- 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