LAPORAN ANALISIS MALWARE

Informasi Umum

Task ID: 20250614-RSJDPJ_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.
- 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
- Looks up Uninstall key entries in the registry to enumerate software on the system.
- Looks up registry value(s) which can often be used to detect a virtual environment.
- Enumerates physical disk devices, likely attempts to detect a virtual environment.
- Drops file in Windows directory
- Creates or modifies a registry key with a large amount of byte data, possibly to store a binary or configuration.
- Adds run entry to the registry to gain persistence across system reboots.
- Drops file in System32 directory