Threat Name: Config_File_Detection

Threat Category:

Configuration File Identification

Threat Description:

The YARA rule Config_File_Detection detects common configuration file extensions such as .ini, .conf, and .cfg, which are often used in system configurations and malware persistence mechanisms.

Indicators of Compromise (IoCs):

.ini

.conf

.cfg

Detection Mechanism:

Matches file names containing common config file extensions.

Possible Attribution & Use Cases:

Used in identifying configuration files for malware persistence.

Recommended Actions:

Monitor changes to configuration files in sensitive directories