

**Custom indicator of compromise documentation**

# Preamble

CERTitude is a network-based host scanner that enables searching for Indicator of Compromise (IOC) on a large scale from a single workstation.

The tool can be broken down into two main components:

* The Python-driven web interface that allow scan planning and result visualization;
* The IOC scanner, running in parallel, also written in Python.

CERTitude is using indicator of compromise from the OpenIOC framework, along with custom indicators described in this documentation.

# Custom indicators of compromise

## GetRecentFiles

This feature will look through all the recently opened files (up to several months).

### Definition

**Name:** RecentFileItem

**Attributes:**

* Type;
* last\_write\_time;
* hive;
* key\_path;
* attr\_name: Filename;
* reg\_type;
* attr\_type;
* attr\_data.

## GetStartupFiles

This feature will look for every files being opened at startup.

### Definition

**Name:** StartupFileItem

**Attributes:**

* Type;
* last\_write\_time;
* hive;
* key\_path;
* attr\_name: Filename;
* reg\_type;
* attr\_type;
* attr\_data.

## MRUHistory

This feature will look for the last run commands executed.

### Definition

**Name:** MRUHistoryItem

**Attributes:**

* Type;
* last\_write\_time;
* hive;
* key\_path;
* attr\_name: command content;
* reg\_type;
* attr\_type;
* attr\_data.