Introduction

What is DocGuard-Watch

DocGuard Watcher is an endpoint application that structurally analyzes and detects malware activities in documents such as Office, PDF and HTA with the help of DocGuard Api.

DocGuard-Watcher runs as a "windows service" within the operating system. Among its duties, it is to follow the File I/O (File writing, creation, update and renaming etc.) processes that occur in the operating system by using the Windows Callback structure, and then to send the relevant file in DocGuard to be scanned and write the result into the Windows Event Log. Thanks to this service, which does not have any interface, the activities of the document files on the endpoint will be automatically recorded under the "Event Log" and will be available to applications such as Siem and EDR.

Event Log Record types

DocGuard-Watcher has 3 different Event Log record types in itself. Among these types, Warning messages are turned off by default.

1. **Information Log** : This record type is used by DocGuard-Watcher to start and stop the service and to analyze the output of the file sent to the analysis. Event ID number is 10000.
2. **Warning Log** : This record type is used for cases where exceptions occur on the application side while DocGuard-Watcher is running. Event ID number is 10001.
3. **Error Log** : It is the format used when there is no Registry-Path, the entered credentials are not valid and there is an internet access problem. The Event ID number is 10002.

Supported extensions

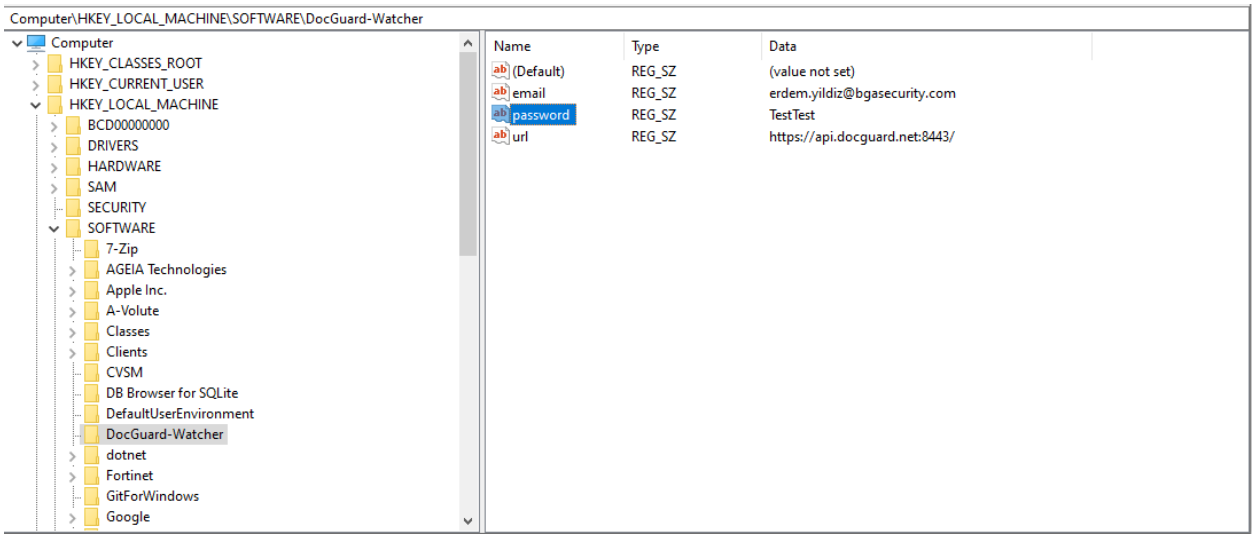
- .hta
- .pdf
- .slk
- .csv
- .doc
- .dot
- .docx
- .docm

- .dotx
- .dotm
- .wll
- .xls
- .xll
- .xlw
- .xlt
- .xlsx
- .xlsm
- .xlsb
- .xlam
- .xltx
- .xltm
- .ppt
- .pps
- .pptx
- .pptm
- .ppsx
- .ppam
- .ppa
- .rtf
- .bin
- .pub

Setup

Registry

It is necessary to create a key named DocGuard-Watcher under “Computer\HKEY_LOCAL_MACHINE\SOFTWARE\” and add “email”,”password” and “url” fields into it.



- email = “”
- password =””
- url = “https://api.docguard.net:8443/”

Create a service

To create the DocGuard-Watcher service in Windows, you can use one of the commands below, which is suitable for you.

The following command can be used to create a service normally.

- sc create DocGuard-Watcher binpath="C:\Path\DocGuard-Watcher.exe"

If warning messages are desired to be seen in EventLogs, the command should be as follows.

- sc create DocGuard-Watcher binpath="C:\Path\DocGuard-Watcher.exe --warning"

Notes

- DocGuard-Watcher sends your files to the DocGuard Api service by marking them as public in the Default installation. This means that the analysis results are also visible to other users. If you only want a private analysis specific to your profile, you should sign up to the application via https://app.docguard.io and write your membership information to the values under the Registry key.

- **Privacy**: DocGuard app does not take care of your files. After your files are analyzed, they are automatically deleted for a certain period of time and only the metadata and

analysis results suitable for analysis are stored in the database. For companies that are sensitive about privacy, DocGuard can also be easily deployed to corporate systems with Docker. For this, you can contact via https://docguard.io.