FILE-MD

USER MANUAL

Version 1.0

IMF SECURITY

This

Page

Left

Intentionally

Blank

TABLE OF CONTENTS

This

Page

Left

Intentionally

Blank

1 ABOUT FILE-MD

1.1 WHAT IS FILE-MD?

FILE-MD is a directory and file scanner capable of using multiple plugins to perform additional analysis. The B9-Plugin uses the B9 library for initial analysis results. The B9 Library is an advanced static file analyzer that uses specialized tests, Yara rules and machine learning models to determine the degree of malice. Results are provided in JSON, the B9 plugin produces tailored reports in CSV. FILE-MD is a Windows utility for auditors, blue teamers, incident responders, malware analysts, threat hunters, and forensics professionals. The goal of FILE-MD is to fill a gap in Windows static file Malicious Discovery (MD) for small, medium, large businesses and even enterprise users to provide a tool that is faster than traditional techniques to improve and refine their information security programs.

FILE-MD with all its features is a multi-tool for blue team defenders and incident responders replacing many individual tools into one easy to use standalone utility.

With FILE-MD your team will be able to:

- Scan individual files, a directory and/or sub-directories of files, or even a file share of files for signs of files malicious crafting,
- Scans binaries and Office documents as well as PDF's
- Create a summary and detailed report of static file analysis for one to thousands of files
- Create a printable report of strings and output details for each file
- Use a plug-in architecture to add additional features

2 GETTING STARTED

2.1 REQUIREMENTS

FILE-MD is designed for Microsoft Windows© based systems. FILE-MD runs on the following operating systems:

- Windows 7 workstation or later 64bit
- Windows 2008 Server or later 64bit

2.2 HOW TO GET HELP OR ASK QUESTIONS ABOUT LOG-MD PROFESSIONAL

FILE-MD hosts a Slack Channel community named "***log-md.slack.com***". FILE-MD users will be asked if they would like to join when the FILE-MD order is fulfilled by an email from us. If you want to be added to the Slack channel, please email us with the email(s) you want to add to:

- info@IMFSecurity.com

You can also send an email to us at the same email above and we will be glad to answer any questions.

2.2.1 Help Videos

We have also recorded some videos on how to use, malware analysis, and hunting with LOG-MD to help you, give you some ideas, help to understand the tool use, or see the tool in action. There are links to the videos on the LOG-MD website, and you can view the videos on our YouTube channel.

- Our website – https://www.imfsecurity.com/TBD/
- YouTube Channel - TBD

2.3 WHAT VERSION DO I HAVE?

Just type the following to get the version of FILE-MD that you are using;

- FILE-MD -v   Full version information including expiration date

```
FILE-MD -v

File-MD.exe v.5.12 Copyright 2024 B9Software.

 ____   ___
| __ )/ _ \
|  _ \ (_) |
| |_) \__, |
|____/  /_/ v.3.5.13.13
Copyright 2024 B9Software. All rights reserved
See EULA for terms of use and privacy policy
Distributed by IMF Security LLC
Demo License expires: 2024-07-04
```

2.4 How to use FILE-MD

- Open an Administrative Command Prompt
- Navigate to the directory you have FILE-MD stored

Type “***FILE-MD -h***” then enter to review the Help menu seen in ***Figure 1***.

FIGURE 1 – FILE-MD Help Screen

FILE-MD -h

```
Usage of file-md:
  -L int
       Number of levels (0 - 9)
  -h   Usage
  -i string
       Input folder or file name
  -o string
       Output folder (default "Current Folder")
  -r   B9 Reports
  -s   B9 Strings
  -t   B9 Tags
  -v   Version
  -x   No Plugins
```

3 Saving output from FILE-MD

FILE-MD provides you multiple options to save the output. FILE-MD allows you to either save the output to the current working directory (\Reports) or a directory or file share you specify. The output location can either be a mapped drive to a server, saved to the local drive, or USB device. This provides the user with the most flexibility to control their output. To specify the output location, use the "**–o**" option and specify either a relative path or a full path such as;

- ***FILE-MD -L 1 -i <filename> –o Reports***
- ***FILE-MD -L 5 -i C:\Users –o File-MD\Reports***
- ***FILE-MD -L 1 -i <filename> –o D:\%computername%_FMD_Reports***

Note: The directory you specify must exist, FILE-MD will not create the directory for you unless you do not specify a folder then the reposts are saved in the current working directory ***\Reports*** folder.

3.1 Output Files

FILE-MD produces several reports with the details of the scan. The reports are prepended with the computer--name so that multiple systems can be stored in the same folder such as a file share. These files are also designed to easily be consumed into a log management or SIEM solution. The basic results of the scan produce three files, they are;

- <computer-name>_Report_File-MD_All.csv – All details of the scan (no reports or strings)
- <computer-name>_Report_File-MD_Error.csv – Any errors on files that were scanned
- <computer-name>_Report_File-MD_Summary.csv – Summary of the results of the scan

4 Scanning files

FILE-MD is designed to statically scan collect specific security relevant log events that are most important to auditors, blue teamers, incident responders, malware analysts, threat hunters, and forensics professionals.

> *If you have a need for something we do not collect, by all means send us an email, describe you would like, the justification, and an example for it, and we will seriously consider it!*

FILE-MD can scan directory levels 0 to 9 levels deep. Why only 9 levels deep? Limiting how deep you recurse into a directory structure keeps the speed up, the file size down and the results easier review. In the typical Windows C:\Users folder, just going 5 folders deep (L 5) will results in 3000-4000 files or more. FILE-MD is designed to limit the impact to the disk and system you are scanning. This means if you want to scan more than 9 folders deep, you will have to restart FILE-MD and specify the 10th level as the starting point and scan 9 folders deep from there. This prevents analysts from launching burdensome scans against file shares that contain tens of thousands of files impacting performance to the system.

4.1 Scanning Options

There are several options that one can select when scanning files or folders, they are;

L – the level of folders you want to scan (0-9) default is 2

i – the item that you want to scan

s – capture the strings for each file scanned

r – create detailed text report for each file scanned in a sub-folder of the folder specified in ***-o***

t – capture the tags that resulted from analyzing the file during the scan

x – Turn off all plugins, used for timing how long a directory might take or how many files exist

4.1.1 Levels

This is where you specify the levels down a folder tree you want to scan. As stated earlier, FILE-MD is designed to limit how many folders at once you can scan to limit impact to the system since it is scanning all the files, performing math and analysis of the files scanned. The following are examples of the levels you can specify.

0 – The root of the folder specified, example; C:\ProgramData

1 - The root of the folder specified, example; C:\ProgramData\<1st level of directories>

2 - The root of the folder specified, example; C:\ProgramData\<Dir1>\<2nd level of directories>

3 thru 9 same as above up to nine folders deep

4.1.1.1 Level Examples

The following of some examples of using the level ***capital L*** option;

- File-MD -L 0 -i D:\ - Scan just the root of the D: drive
- File-MD -L 0 -i H:\ - Scan just the root of a typical H: home drive
- File-MD -L 1 -i H:\ - Scan the root and one folder deep of a typical H: home drive
- File-MD -L 5 -i C:\Users - Scan the Uses directory and 5 levels deep
    - C:\Users\Bob\AppData\Local\Temp\Dir_x and all other folders below C:\Users

If you wanted to scan further than the 9th folder deep, you would just specify that 10th level and go from there, for example;

- File-MD -L 9 -i C:\Users\Bob\AppData\Local\Temp\Dir_x
- File-MD -L 9 -i C:\Users\Bob\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

4.2 Scanning a single file

FILE-MD is designed to scan a single file and statically analyze the file to produce a series of results. Often an analyst wants to scan only one file at a time that is found during an investigation. To scan a single file simply specify the location of the file, the ***-L*** option is not needed when scanning a single file;

- File-MD -i <path_and_suspicious_filename>
- File-MD -i C:\ProgramData\System.dll -o D:\File-MD\Reports

You can also use the ***-r*** (text report) and/or the ***-s*** (strings) option as well to get the detailed text report of the file and also the list of readable strings in the file. You may also specify the ***-t*** (tags) option to see the list of tags that were triggered during the scan. More on the ***-r***, ***-s*** and ***-t*** options below. An example of using these flags are;

- File-MD -i C:\ProgramData\System.dll -o D:\File-MD\Reports -r -s -t

4.3 Scanning multiple files

FILE-MD is designed to scan multiple files and statically analyze these files to produce a series of results. Often an analyst wants to scan multiple files at a time that were found and harvested during an investigation. To scan multiple files simply specify the location of the files, the ***-L*** option is needed when scanning multiple files since a directory is specified;

- File-MD -i <path_of_files> (will store reports in the folder \Reports)
- File-MD -i C:\ProgramData\System.dll -o D:\File-MD\Reports

You can also use the ***-r*** (text report) and/or the ***-s*** (strings) option as well to get the detailed text report of the file and also the list of readable strings in the file. You may also specify the ***-t*** (tags) option to see the list of tags that were triggered during the scan. More on the ***-r***, ***-s*** and ***-t*** options below.

4.4 Scanning a directory of files

FILE-MD is designed to scan a directory and/or all sub-directories up to 9 levels deep and statically analyze these files to produce a series of results. Often an analyst wants to scan all files or a directory structure during an investigation. To scan a directory and sub-directories simply specify the location of the files, the ***-L*** option is needed when scanning directories requires how many levels deep is going to be scanned;

- File-MD -L 5 -i C:\Users (will store reports in the folder \Reports)
- File-MD -L 5 -i C:\Users -o D:\File-MD\Reports
- File-MD -L 5 -i C:\Users -o D:\File-MD\Reports -r -s

You can also use the ***-r*** (text report) and/or the ***-s*** (strings) option as well to get the detailed text report of the file and also the list of readable strings in the file. You may also specify the ***-t*** (tags) option to see the list of tags that were triggered during the scan. More on the ***-r***, ***-s*** and ***-t*** options below.

4.5 Scanning a File Share

FILE-MD is designed to scan file shares up to 9 levels deep and statically analyze these files to produce a series of results. Often an analyst wants to scan all files of a file share structure during an investigation. Keep in mind you can only go 0 folders deep so will need to run a series of scans to go deeper. To scan a file share simply specify the location of the files, the ***-L*** option is needed when scanning directories requires how many levels deep is going to be scanned;

- File-MD -L 5 -i H: (will store reports in the folder \Reports)
- File-MD -L 5 -i H: -o D:\File-MD\Reports_Home_Drives
- File-MD -L 5 -i P: -o D:\File-MD\Reports_Public_Drive -r -s

You can also use the ***-r*** (text report) and/or the ***-s*** (strings) option as well to get the detailed text report of the file and also the list of readable strings in the file. You may also specify the ***-t*** (tags) option to see the list of tags that were triggered during the scan. More on the ***-r***, ***-s*** and ***-t*** options below.

4.6 Strings

FILE-MD can provide a report of the readable strings from a file that is scanned. These strings are recorded in the same type of text report that ***-r*** provides discussed more below. If you specify ***-r*** and ***-s***, both results are in the same file. Strings are another detail investigators use to find readable strings that can show API calls, IP address, domains and other details that are not obfuscated by compiled code. An example of create the result reports and to capture the strings of a file;

- File-MD -i C:\ProgramData\System.dll -o D:\File-MD\Reports -s

The following is an example of what can be found in the strings output;

```
"B9 Strings":""
  "This program cannot be run in DOS mode."
  "8Rich"
  ".textq3"
  ".rdata"
  ".data"
  ".rsrc"
  "h WE3"
  "\\zGj"
  "YYu=9"
  "YYuZ9"
  "YYuI9E"
  "u2j|V"
  "YhTVE"
  "YYuC9E"
  "YYuh9E"
```

4.7 Reports Option

FILE-MD can also produce more details in a report per file using the ***-r*** option. These detailed results of the scans are stored in the following folder and random filename;

- <computername>_Report_File-MD_Folder\<1385210605.txt>

Each report in this folder are text files (.txt) with additional information about the scanned file including the hashes, entropy, tags and other details analysts typically use when investigating files. The ***summary*** and ***all*** results also have some of this data in a ***.CSV*** format for easier viewing. Not all the details are in ***summary*** and ***all*** results, thus this option. The file names used for the reports and unique and listed in the last column of the ***ALL*** results file;

- <computer-name>_Report_File-MD_All.csv

Explanation of what each item in the report means will be discussed in "***Analyzing the Results***" later in this document. Below is an example of one of the reports.

Typical output when specifying the ***-r*** option

```
"B9 Report":""
   "B9 Version":" B9 v.3.5.13.13 Copyright 2024 B9Software",
   "B9 Report Date":" 2024-06-24 10:18:47.7570767 -0500 CDT m=+27.282121901",
   "Name":" Malware_putty.exe",
   "Size":" 483328",
   "Date":" 2012-05-10 15:30:14 -0500 CDT",
   "eCode":" 1",
   "Majic":" MZ ",
   "File_Sig":" 4d5a9000",
   "MD5":" 67eab16df0eb1e37c28921a756921b8e",
   "SHA1":" 4823d7533605f915d6e0236b0e875ac053ab966c",
   "SHA256":" dd8dcf118eedcab3336f524040e0a523033cdb30b64facaed970e486e000f798",
   "SHA512":"
f20f88be4791e1a73b594c087f2e12b04a8e29e0bfde8f51d768820ccd494ffb4d4664ff6e36d60593c2b1b22060f0d66b281ab
0738018ed24319719b80fb031",
   "CRC32C":" 962038d",
   "SSDEEP":" 12288|Q743NHanev1s4kd83ubHX2+v1g8YyCCTlaG9PnV6I|sgN6nY13ebHX2+tlNl7V6",
   "PDB Path":" ",
   "B64 Count":" 0",
   "VSInfo":" 0",
   "Assembly Version":" Not Found",
   "Comments":" Not Found",
   "LegalTrademarks":" Not Found",
   "TranslationString":" Not Found",
   "StringFileInfo":" 8080904B0",
   "CompanyName":" Simon Tatham",
   "ProductName":" PuTTY suite",
   "FileDescription":" SSH, Telnet and Rlogin client",
   "FileVersion":" Release 0.62",
   "ProductVersion":" Release 0.62l",
   "LegalCopyright":" Copyright  1997-2011 Simon Tatham.",
   "Entropy":" 6.636312",
   "FilePacker":" No matches found.",
   "Certificates":" None found.",
   "YaraCount":" 0",
   "Macro":" 0",
   "Moxie":" 1000",
   "Imported DLL Count":" 10",
   "B9Ref":" -7b5e7caf80fbafea",
   "B9Tag":" 17435",
   "B9 Result":" 'Malware_putty.exe', is likely suspicious.",
   "Total Time": "160.9509ms"
```

4.8 TAGS

FILE-MD provides you with a way to see the tags that triggered during the scan. These tags are short for the rules that flagged the file as suspicious or malicious. Below is an example of the tags shown in ***bold and italic*** from a scan that led to the result of suspicious.

```
File-MD.exe -i "c:\users\Stoopid User\AppData\Local\Malware_putty.exe" -t
File-MD.exe v.5.12 Copyright 2024 B9Software.
Searching...
Processing 1 of 1  100%: MZ  suspicious c:\users\Stoopid
User\AppData\Local\Malware_putty.exe
Windows, Suspicious, Entropy, Moxie, vsInfo

Completed time 0s
Total 1, Good 0, Malicious 0, Suspicious 1, Low 0, Unspecified 0
```

4.9 NO PLUGINS

FILE-MD uses a plugin architecture to run the various options. This option is provided for the analyst to scan a target to see how long the scan will roughly take. Below is an example of the -x option in use to understand how long a scan may take on a folder;

```
File-MD.exe -L 3 -i C:\users -x
File-MD.exe v.5.12 Copyright 2024 B9Software.
Searching...
Processing 19 of 364 - 5%: C:\users\Public\AccountPictures\S-1-5-21-868446741-1414273077-
1995815538-1003\{B26C1284-3298-4681-97C8-EE229DDB4DE6}-Image1080.jpgProcessing 307
of 364 - 85%: C:\users\root\ntuser.ini                                        ans-msrans-
msng__v0.7.pptxg
Completed time 44s
```

Notice that it took 44s, but keep in mind that once plugins are enable the time will likely increase. The take away for this feature is that 364 files took roughly 44s to scan.

5 Analyzing the Results

Once the results have been created it is now time to analyze them to see what they tell you about the files. It is important to note that good files can be crafted poorly or use similar functions that maliciously crafted files do, so keep in mind there will always be false positives. The goal is to reduce the sheer volume of files that an analyst needs to look at and help the analyst discover malicious files to review more closely.

5.1 Using the Summary Results

This report is where to start as it is short and contains the basic details to help an analyst find suspicious and malicious files quickly.

5.2 Using the All Results

This report has more data than the summary results and contains the location and name of the detailed report of each file if ***-r*** and/or ***-s*** is used. This report is used to go the next level deep during the investigation.

5.3 The Error Results

This report contains any files that could not be scanned to help troubleshoot any issues and know if a file might be too large to scan would be an example of an error found in this report.

5.4 The Detailed Report

When using the ***-r*** and/or ***-s*** options the details will be found in these reports. One report per file is created containing the details and strings if ***-s*** is selected.

The detailed report contains the following entries:

Name – The name of the file scanned
Size – The size of the file
Date – The date of the file
eCode - ??
Majic – This tells you the type of file it is, MZ, PDF, Doc, etc.
File_Sig – This is the beginning of the file that indicates the type of file MZ = 4d5a9000
MD5 – The MD5 hash of the file
SHA1 – The SHA1 hash of the file
SHA256 – The SHA256 hash of the file
SHA512 – The SHA512 hash of the file
CRC32C – The Cyclic Redundancy Check of the file
SSDEEP – The SSDeep or Fuzzy hash of the file
PDB Path – The developer path of the compiled file
B64 Count – If any base64 code exists in the file and the count
VSInfo – The Visual Studio version of a file if used
Assembly Version – The assembly version of a file if used
Comments – Meta data of a file that contains comments by the developer
LegalTrademarks – Meta data about the signer of the file

TranslationString - ??
StringFileInfo - ???
CompanyName - Meta data about the signer of the file
ProductName - Meta data about the product name of the file
FileDescription - Meta data about the description of the file
FileVersion - Meta data about the version of the file
ProductVersion - Meta data about the product version of the file
LegalCopyright - - Meta data about the signer of the file
Entropy – The entropy of the file
FilePacker – If any packers are used
Certificates – How many certificates were found in the file
YaraCount – How many Yara rules were matched
Macro – If signs of a macro were found
Moxie – If any signs of moxie were found in the file
Imported DLL Count – How many imported Dlls were found
B9Ref – B9 ??
B9Tag – Tag numbers found
B9 Result – The result of the analysis
Total Time – The total time the scan of the file took in milliseconds

5.4.1 Strings

String output with the ***-s*** option is also stored in the detailed reports for each file. The following is a good article on the use and importance of strings:

- https://library.mosse-institute.com/articles/2022/05/the-strings-tool-extracting-text-for-digital-forensics/the-strings-tool-extracting-text-for-digital-forensics.html

Analysts use data in strings to find words or details that help to identify details of the file or malware that can help find other artifacts involved in an incident.

6 LICENSE

This document is licensed under a Creative Commons Attribution 3.0 Unported License.

Copyright © 2016-2020 IMF SECURITY LLC. All rights reserved

7 REVISION HISTORY

Date	Revision	Description
07/15/2024	Ver 1.0	Initial release