IOC Finder

User Guide

Release 1.0

Latest Edition: https://forums.mandiant.com/topic/official-mir-documentation

IOC Finder

User Guide

End User License Agreement (EULA)

THIS END-USER LICENSE AGREEMENT (THE "AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU AND MANDIANT CORPORATION ("MANDIANT"). BY USING THIS SOFTWARE, YOU ACCEPT ALL TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT WISH TO ACCEPT THIS AGREEMENT, DO NOT INSTALL OR OTHERWISE USE THIS SOFTWARE.

Use

Subject to the terms and conditions of this Agreement, MANDIANT hereby grants you a non-exclusive, non-transferable license to install and use the accompanying software (the "Software") in a non-commercial capacity on an unlimited number of computers.

Reproduction and Distribution

You may copy and distribute the Software, provided that you do not modify the Software or the distribution package (the .MSI, .ZIP or .EXE file as distributed by MANDIANT) in any way or otherwise create any derivative works based on or including the Software. You may not sell the Software or bundle it for redistribution with other software products. You may not make or distribute copies of the Software for commercial use, whether in conjunction with any third party software or otherwise. Any copy that you make of the Software, in whole or in part, is the property of MANDIANT. You agree to reproduce and include in their entirety all copyright, trademark and other proprietary rights notices on any copy or any portion thereof of the materials you receive under this Agreement. You agree to provide MANDIANT with notice each time you distribute the Software, or, in the event of a widespread distribution, to provide a single notice when you offer the Software for download or otherwise distribute the Software to more than one recipient.

Reservation of Rights

MANDIANT reserves all rights not expressly granted pursuant to this Agreement. This Agreement is not a sale of the Software, any copies or part thereof, or any other software, and you shall have no title to or ownership in the Software, or any copies or part thereof, regardless of the form on which the original and any copies may exist. MANDIANT reserves the right to offer upgrades to the Software, either for a fee or without cost, at MANDIANT's sole discretion. Any such upgrades may be subject to their own End-User License Agreements, and may not be copied and distributed except by the terms of those Agreements, if applicable.

Proprietary Rights

The Software contains valuable trade secrets of MANDIANT. You agree not to decompile, disassemble, analyze, or otherwise reverse engineer the Software. The Software is protected by United States and international copyright laws. The names, marks, brands, logos, designs, trade dress and other designations MANDIANT uses in connection with the Software are proprietary to MANDIANT. Except as stated above, this Agreement does not grant you any intellectual property rights in the Software.

Prohibited Actions

You agree not to modify, sell, lease, or create derivative works of the Software. You agree not to use the Software for rental or as a part of a commercial time-sharing or service bureau operation. You may not use the Software for any illegal purpose, and you may not use the Software to access or examine any computer, or data from any computer, that you do not have the unequivocal legal right to access or examine.

Disclaimer of Warranties

YOU AGREE THAT THE SOFTWARE IS PROVIDED TO YOU "AS IS" AND WITHOUT ANY WARRANTIES OR REPRESENTATIONS OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT.

Indemnification

YOU AGREE TO INDEMNIFY MANDIANT AND ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES AND AGENTS, AND SHALL HOLD IT HARMLESS AGAINST ANY CLAIMS, LOSSES OR DAMAGES ASSERTED BY ANY ENTITY, WHETHER BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT, PRODUCT LIABILITY OR OTHERWISE, INCLUDING COURT COSTS AND REASONABLE ATTORNEYS' FEES, ARISING OUT OF OR IN CONNECTION WITH YOUR USE OF, OR ATTEMPTED USE OF, THE SOFTWARE.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MANDIANT SHALL NOT BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY TYPE ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR THE SOFTWARE. MANDIANT shall not be liable for any use of the Software, including the access, examination, or modification of data on any computer by the user without unequivocal legal right. You acknowledge that MANDIANT has agreed to make the Software available in reliance on the exclusions and limitations of liability and disclaimers of warranty set forth above and that the same form an essential basis of the bargain between the parties.

Export of Products

You agree that you will not, directly or indirectly, ship, transfer, transmit, export or re-export, or knowingly permit any of the foregoing with respect to the Software, or any technical information about the Software, to any country for which the United States Export Administration Act, any regulation thereunder, or any similar United States law or regulation, requires an export license or other United States Government approval, unless the appropriate export license or approval has been obtained.

Termination

You may terminate this Agreement at any time by deleting the Software. MANDIANT may terminate this Agreement at any time by providing you with individual notice, or by posting a notice on its website at www.mandiant.com. When this Agreement terminates or expires, all rights granted to you will cease, and you must immediately destroy or purge from your computer system the Software and all copies in your possession.

Governing Law and General Provisions

The Agreement shall be governed by the laws of the Commonwealth of Virginia, excluding the application of its conflict of law rules and the United Nations Convention on Contracts for the International Sale of Goods. Both parties hereby submit to the exclusive jurisdiction of the Alexandria Circuit Court in Alexandria, Virginia, and the United States District Court for the Eastern District of Virginia. If any part of any provision of this Agreement shall be invalid or unenforceable, such part shall be deemed to be restated to reflect, as nearly as possible, the original intentions of both of the parties in accordance with applicable law, and the remainder of the Agreement shall remain in full force and effect. This Agreement may only be modified in a writing signed by an officer of MANDIANT. MANDIANT's failure to enforce or exercise any right or provision of this Agreement shall not constitute a waiver of such right or provision. This Agreement is the complete and exclusive statement of the agreement between you and MANDIANT and supersedes any proposal or prior agreement, oral or written, and any other communications between you and MANDIANT relating to the subject matter of this Agreement.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND UNDERSTAND IT. BY INSTALLING OR USING THE SOFTWARE YOU CONSENT TO BE BOUND BY THESE TERMS AND CONDITIONS.

Table of Contents

Chapter 1
IOC Finder Quick Start

Mandiant IOC Finder is a command-line utility used in host-level analysis. The tool supports a two-phase workflow:

- collection of host data to structured files and directories; and the
- generation of IOC hit reports for this data.

1. Collecting Data

1. Copy `mandiant_ioc_finder.exe` to a portable storage device (PSD), typically a large USB drive.
2. At the Host computer, install the PSD. Using Windows File Explorer, identify the drive letter for the PSD.
3. Open the command-line terminal and run the following commands:

```
cd X:
mandiant_ioc_finder collect
```

4. IOC Finder will perform a full collection of data suitable for general IOC matching. This may take several minutes, depending on the data capacity (memory and drive space) of the Host.

   By default data is collected from Windows `%SYSTEMDRIVE%`, and the captured data are stored on the current working drive.

   Status reports during this operation are sent to `STDOUT`; user-correctable and system errors are sent to `STDERR`.

5. When data collection is complete, the captured data is located in a subdirectory named after the Host. You may then collect data from other Hosts, or generate an IOC report.

2. Generating Reports

1. Collect data from Host computers to a portable storage device (PSD).

   If you used `mandiant_ioc_finder` to collect the data, the directory structure is managed automatically.

2. At a workstation, install the PSD. Using File Explorer, identify the drive letter for the PSD.
3. Open the command-line terminal and run the following commands:

```
cd X:
mandiant_ioc_finder report -i [iocs]
```

where *[iocs]* is a path to an IOC zipfile, directory of IOCs, or an individual IOC file.

4. IOC Finder will analyse the collected data, looking for and reporting on IOC hits. This may take several minutes, depending on the amount of collected data.

   By default, the current working directory is the root directory for source data collections.

   Status reports during this operation are sent to `STDOUT`; user-correctable and system errors are sent to `STDERR`. The status reports take the form `<collection timestamp>, <hostname or IP>, <IOC hit name>`.

5. When the report is complete, your terminal history (or redirected output file) will contain a list of all Hosts that show indications of compromise, what those compromises are, and when the compromising data was captured.

Chapter 2
IOC Finder Command-line Options

The `mandiant_ioc_finder` command can take several parameters that support you in collecting data and creating IOC reports:

- During collection, there are options for specifying an output directory and specifying storage devices from which to capture data.
- During analysis, there are options for specifying the source directory (allowing you to analyse a single collection instead of all collections), for specifying IOC source files (allowing you to customize the search), and to generate full HTML and DOC files suitable for presentation and documentation.

Please see the command-line help (`mandiant_ioc_finder -?`) for usage details. For your convenience, this help is duplicated below:

Name

mandiant_ioc_finder — collect host system data and report on the presence of Indicators of Compromise

Synopsis

`mandiant_ioc_finder` collect [-o *[output_dir]*] [-d *[drive_list,]*...] [-s *[script_file]*] [-q] [-v] [-h]

`mandiant_ioc_finder` report [-i *[iocs]* [-i *[input_iocs]*...]] [-s *[source_data]*] [-t html | doc [-o *[output_file]*]] [-w] [-q] [-v] [-h]

Description

MANDIANT IOC Finder is a free tool for collecting host system data and reporting the presence of Indicators of Compromise (IOCs) in that data. IOCs are open-standard XML documents that help incident responders capture diverse information about threats.

IOC Finder has two operating modes: *collect* and *report*. The utility is used to collect data from a single Host system, and to generate reports from one or more collections of such data. IOCs are accepted as zip files or directories; generated reports can be created in HTML or MS Office Open XML. Indicator identification messages are printed to STDOUT if the `-q` (quiet mode) option is not used.

Options

mandiant_ioc_finder collect

`-o [output_dir]`
: Path to an alternate directory for Host data collections instead of the current working directory.

`-d [drive_list,...]`
Collect data from the specified drives instead of `%SystemDrive%`. Separate drive letters with commas, do not use whitespace.

`-s [script_file]`
Experimental: Path to a custom data collection script, which will be executed instead of the built-in presets optimized for use with IOC Finder.

`-q`
Quiet mode. Suppresses output to STDOUT and STDERR.

`-v`
Print version info.

`-h`
This help page.

mandiant_ioc_finder report

`-i [iocs]`
Path to an IOC file, directory of IOC files, or a zipfile containing IOC files. IOC files must conform to the OpenIOC 1.0 or later standard.

Multiple -i flags may be specified to combine multiple sources. If alternatives are not used, default presets are used.

`-s [source_data]`
Path to a directory containing one or more Host data collections. IOC Finder expects the directory structure to conform to the MIR Agent Local Data Collection layout standard. See *the section called "Collection Files" (p. 5)* for details.

`-t html|doc`
Generate an HTML or MS Office Open XML report.

`-o [output_file]`
Specify the directory path for HTML reports, or path and filename for MS OOXML reports.

If `-o [output_file]` is not specified:

`.\report\[timestamp]` is used for HTML reports

`.\report_[timestamp].doc.xml` is used for MS OOXML reports.

`-q`
Quiet mode. Suppresses runtime message output to STDOUT and STDERR.

Note that indicator match messages are always printed to STDOUT.

`-v`
Print version info.

`-h`
: This help page.

Collection Files

When the *collect* command is invoked, MANDIANT IOC Finder performs a full data collection from the Host. This is an unfiltered collection, suitable for general IOC hit matching requirements. Different IOC sets can be used against the same IOC Finder data collection without having to perform an additional collection.

Data collections are stored in standard MIR Agent Local Data Collection layout standard, as follows:

```
<hostname>
    <collection dir named by yyyymmddhhmmss>
    <collection dir named by yyyymmddhhmmss>
    <collection dir named by yyyymmddhhmmss>
    ...
<hostname>
    <collection dir named by yyyymmddhhmmss>
    <collection dir named by yyyymmddhhmmss>
    <collection dir named by yyyymmddhhmmss>
    ...
...
```

Output

IOC Finder provides three forms of output:

STDOUT/STDERR
: IOC Finder reports status for the *collect* and *report* commands to STDOUT. User-correctable and system errors are reported through STDERR. Status and error messages can be silenced using the `-q` option.

  Hit notifications can not be silenced. Hits are always reported on STDOUT and take the following form:

  [date-time stamp], [hostname or IP], [IOC]

HTML
: With `-t html` an interactive web-page document is generated. On the left, a navigation panel selects **View by Hosts** and **View by Indicator**. In the center, a list of IOCs is presented, with controls to drill-down to hit details about the hit source. On the right, a **Details** panel shows a full description of the IOC hit.

MS OOXML
: With `-t doc` a Microsoft Word document is generated. The first page presents a summary of findings (hosts with hits, and which hits were detected). Remaining pages examine the details for each host, with full information on the Host environment, and detailed information for all hits.

Status

IOC Finder returns:

`0`
: No errors.

`1`
: Errors were encountered.

Version

MANDIANT IOC Finder version 1.0.0, Build 9

Compatibility

OpenIOC Version 1.0 with terms supported by MIR Agent 2.1

MANDIANT

WWW.MANDIANT.COM

REV: