

User Guide

MANDIANT IOCe™

Version 2.2.0.0



MANDIANT IOCe™

MANDIANT IOCe is a free editor for Indicators of Compromise (IOCs). IOCs are XML documents that help incident responders capture diverse information about threats including attributes of malicious files, characteristics of registry changes, artifacts in memory, and so on. IOCe provides an interface into managing data within these IOCs.

MANDIANT IOCe Features

MANDIANT IOCe can:

- Manipulate the logical structures that define the IOC
- Apply meta-information to IOCs including detailed descriptions or arbitrary labels
- Convert IOCs into XPath filters
- Manage lists of "Terms" that are used within IOCs

Supported Operating Systems

IOCe officially supports the following operating systems:

- Windows XP
- Windows 2003
- Windows Vista
- Windows 7

Requirements

- IOCe requires the Microsoft .NET Framework, Version 3.5 or greater.

Overview of IOCe Use

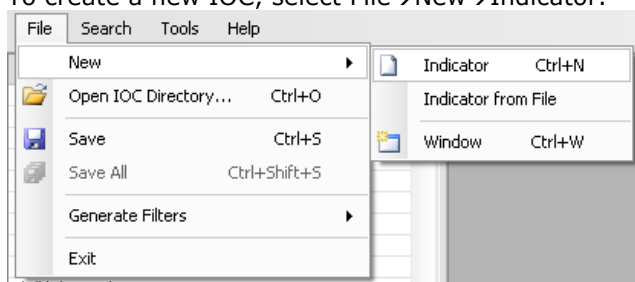
General

At a basic level, IOCe can be considered an editor for IOC files (.ioc extension). However, IOCe has additional features that provide capability beyond just editing an IOC. IOCe can also be used for generating XPath filters, and comparing two IOCs.

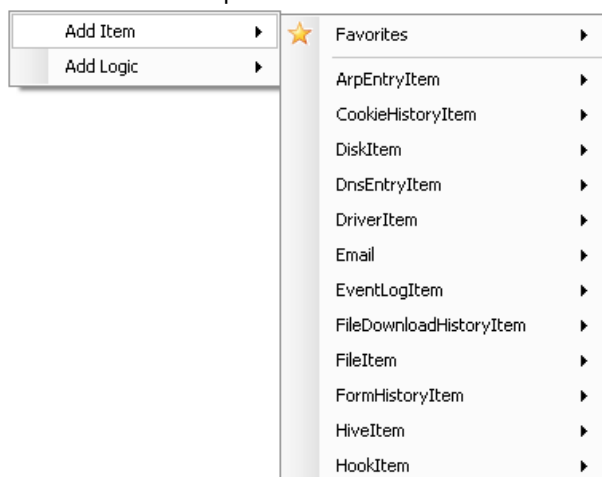
Quick Start

If you are eager to begin using IOCe, here is a brief description of how to get started.

1. Launch the IOCe application and either open an empty directory or open a directory of existing IOCs. To open a directory, select File→Open IOC Directory from the main menu bar
2. To create a new IOC, select File→New→Indicator.



3. From here you can begin adding the meta information and expressions to the IOC.
 - a. Name, Author, and Description are pretty self-explanatory. The box on the right is for any references (see below).
 - b. The Definition area is where the expressions in an IOC are added. To add an expression under the top level OR, right-click in the Definition area and select Add Item. You will be presented with a menu of available Indicator terms.



IOCe Graphical User Interface

GUI Basics

The IOCe GUI consists of three main areas: a listing of all loaded IOCs, the meta information, and the definition.

- The left-hand listing of IOCs allows for sorting based on the available columns (name, created date, updated date, source, or GUID). Selecting an IOC in this list will render the contents on the right side.
- The meta information section is used to add the name, author information, description, and any references that may provide further information or context to an IOC. The references are displayed in the top-right box. You can right-click to add a reference. Several reference types are available, and if something different is needed, just use the "Add Other" option.
- The definition area is where the expressions that make up the IOC are contained.

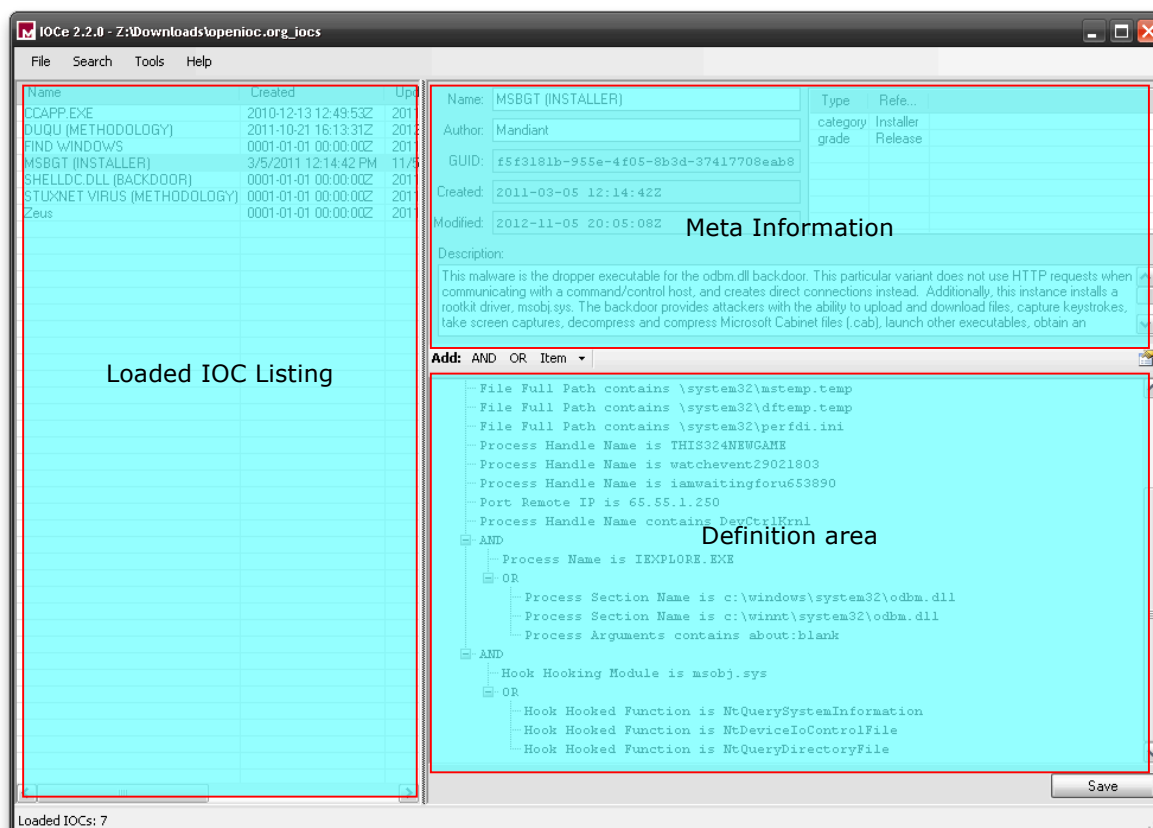


Figure 1: IOCe Interface

Creating an IOC

To create an IOC, either select the File→New→Indicator menu option, right-click in the IOC Listing on the left and select the New Indicator menu item, or use the keyboard shortcut Ctrl+N. A new item will be created with a name of "*New Unsaved Indicator*", from here you can change the name, add the author, add some references, and build the definition.

The references can be whatever information you want to add that may help further explain the piece of malware you are describing. The built-in options are Group, Report, Comment, Category, Grade, and Threat Group. The final option is Other, this allows you to add whatever item you would like.

For further details on what goes in the Definition portion of an IOC, please refer to the section titled "Building an Indicator of Compromise."

Saving an IOC

To save an IOC, simply click on the Save button located in the bottom right of IOCe. This will write the IOC to the directory that IOCe is currently set to.

If changes are made to an already existing IOC, they will be marked as "dirty" and highlighted yellow in the IOC Listings on the left as shown in the following example.

File Search Options Help			
Name	Created	Upd.	
ACELPVC (UNKNOWN)	12/23/2009 4:41:36 PM	1/25.	
AK.EXE (DROPPE...	6/23/2010 3:39:2...	1/25.	
First Logic Example	1/25/2011 5:22:40 PM	1/25.	
HTRAN (TUNNEL...	9/24/2009 11:44:...	9/24.	
JAVA (DOWNLOADER)	8/10/2010 7:29:04 PM	8/10.	
MSBIZ (BACKDOOR)	9/24/2009 11:41:21 PM	9/24.	
Second Logic Example	1/25/2011 5:26:51 PM	1/25.	

Figure 2: "Dirty" IOC example

To save the "dirty" IOCs, you can either click on each individual highlighted IOC and then click the Save button, or use the File→Save All menu option to do it automatically.

If you attempt to exit IOCe while "dirty" documents still exist, it will warn you that there are unsaved changes. Clicking Yes will save all changes and exit, Clicking No will not save anything and then exit, and Clicking Cancel will allow you to go back and make any further changes.

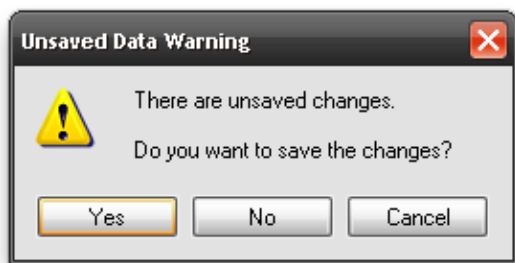


Figure 3: Unsaved changes warning

Searching

Searching is extremely easy in IOCe. To search for anything found in the loaded IOCs, select the Search→Search for Keyword menu option. This will open a small window where you can type in the keyword you want to look for.

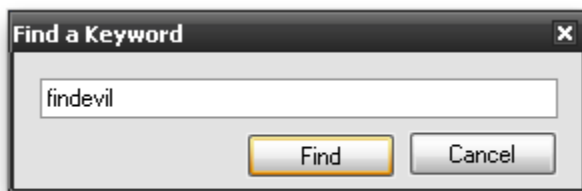


Figure 4: Search Window

Once you have typed in what you want to search for, click the Find button to begin searching. Once a hit is found, it will be selected and the details will be displayed on the right side of IOCe. To continue searching for the same keyword, select Search→Continue Last Search.

Building an Indicator of Compromise

Terminology

For the purposes of this guide, the following terminology will be used:

Expression: The definition of a condition, which when true, suggests that intrusion activity is present.

Simple Expression: An expression that can be defined without using "AND" or "OR" logic operators.

Complex Expression: An expression that combines multiple simple expressions using "AND" or "OR" logic operators.

Indicator of Compromise (IOC): A combination of expressions (simple, complex, or both), usually grouped together for the purposes of describing a single piece of malware. Each IOC is given a unique ID number within the IOCE (represented as the GUID in meta information and also is the filename of the IOC).

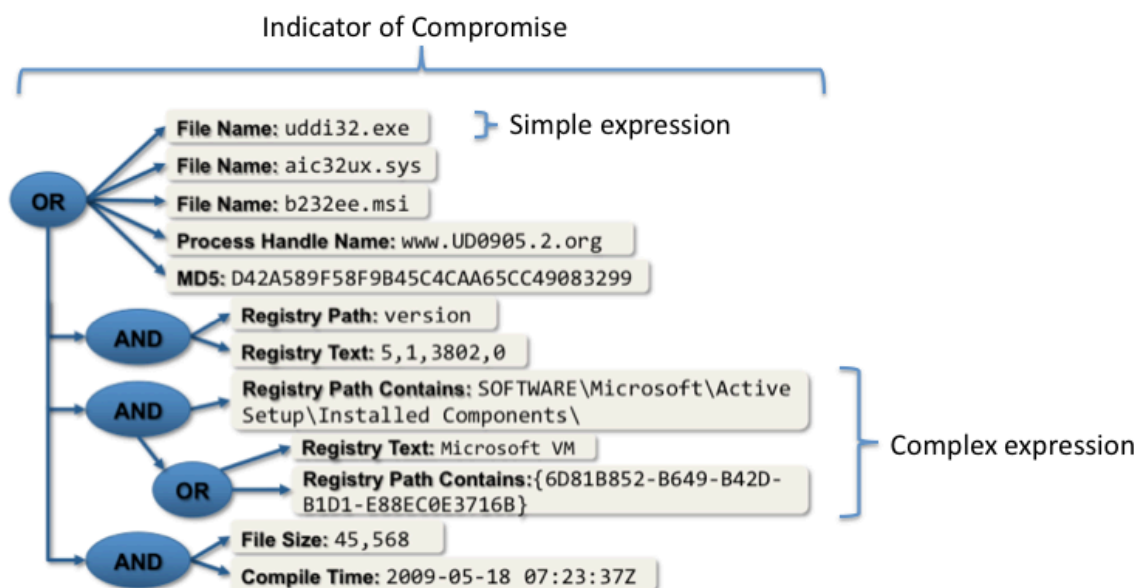


Figure 5: IOC structure

IOCe Logic

Each IOC is defined by a logic tree comprised of expressions. The logic tree starts out with a top-level "OR" structure. When expressions are added to this structure (by right-clicking and choosing "Add Item"), an IOC will hit as long as one of the expressions describes a true circumstance. Sometimes an IOC will be comprised of a collection of simple expressions (MD5 hash, file name, etc.) listed in the top-level "OR" structure, with no need for a more complex logic tree, for example:

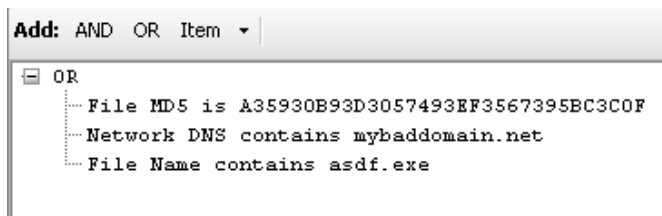


Figure 6: Simple logic example

In pseudo code, the above indicator is described as follows:

```
(File Name is asdf.exe) ||
(File MD5 is A35930B93D3057493EF3567395BC3C0F) ||
(Network DNS contains mybaddomain.net)
```

When required, logic branches can be built with "AND" and "OR" substructures to form complex expressions. Each "AND" and "OR" applies to the branches in its substructure only. For example:

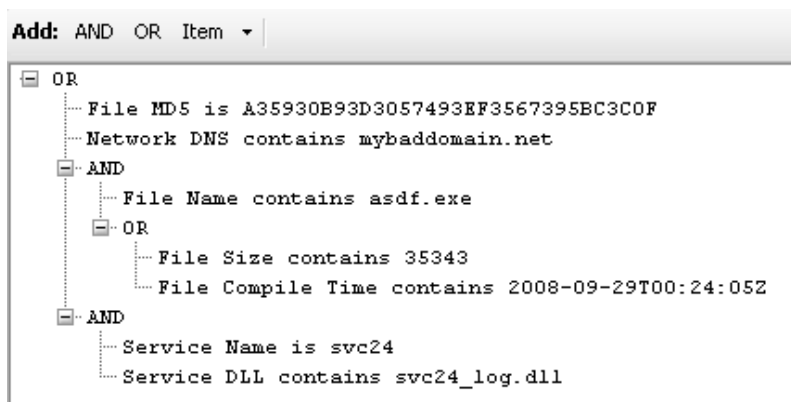


Figure 7: Logic branch example

In pseudocode, the above indicator is described as follows:

```
(File MD5 is A35930B93D3057493EF3567395BC3C0F) ||
(Network DNS contains mybaddomain.net) ||
((File Name is asdf.exe) &&
((File Size is 35343) || (File Compile Time is 2008-09-29T00:24:05Z))) ||
((Service Name is svc24) && (Service DLL contains svc24_log.dll))
```

Note: Logically, "AND" and "OR" structures should be alternated; there is no reason to have an "OR" structure fall directly beneath another "OR" structure, or for an "AND" structure to fall directly beneath another "AND" structure.

Building the Definition

To add a new item, right-click in the definition area and select "Add Item". There are a number of different expression categories available within IOCe that are determined by the contents of the

Indicator Terms files (see section titled "Indicator Terms" for further details). Some of the items available for use ("FileItem", "RegistryItem", etc.) are pictured below:

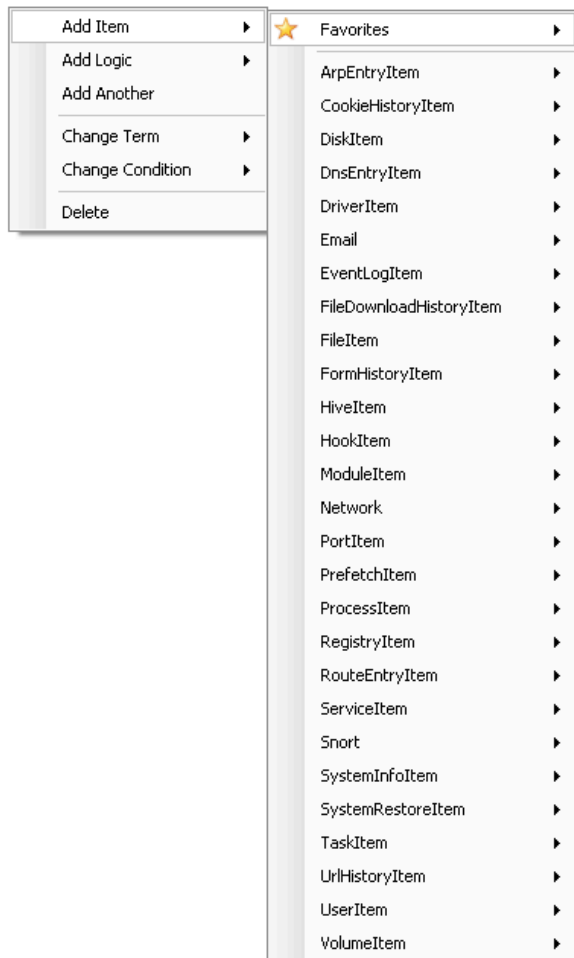


Figure 8: Add Item menu options

To add a File's MD5 sum, click on Add Item→FileItem→ File MD5. This will add a text box where you can type in the MD5 sum that you would like to look for.

To add more items, continue with the right-click Add Item→{Whatever item is needed}

Tip: If you have several of the same type to add, once you select the correct item from the "Add Item" menu and add your information, you can just click on the "Item" button to add the same item type again.

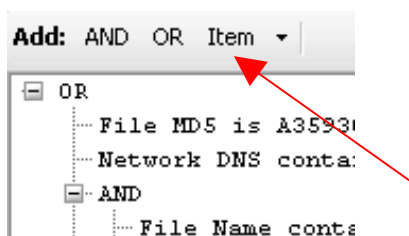


Figure 9: Item button

Expressions come with conditions. By default, a newly created expression will use “contains”. However, other conditions (“is”, “is not”, “does not contain”) can be applied as needed using the “Change Condition” menu item:

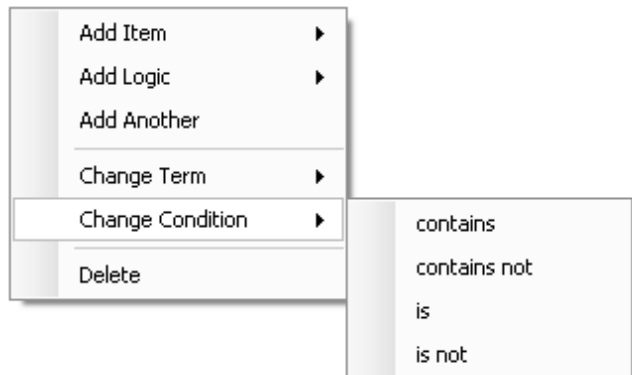


Figure 10: Change Condition menu option

To add a level of logic, either click on the “AND” or the “OR” button to the left of the Definition area, or right click in the Definition and select “Add Logic” then click on the logic item you need.

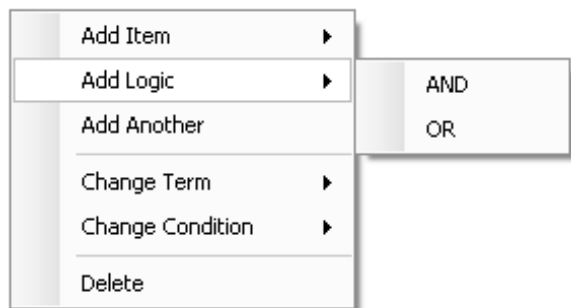


Figure 11: Add Logic menu option

Indicator Terms

Adding/Editing

To provide the terms that are available for adding, IOCe uses indicator terms files. These files are in the same directory as the IOCe executable and have an extension of .iocterms. The ones that ship with IOCe are E-mail, MIR-1.3.3, MIR-1.4, and Favorites.

In order to edit existing terms or add your own, there is a terms editor built-in. To get to it, select Tools→Edit Indicator Terms. This will bring up a window showing all terms available.

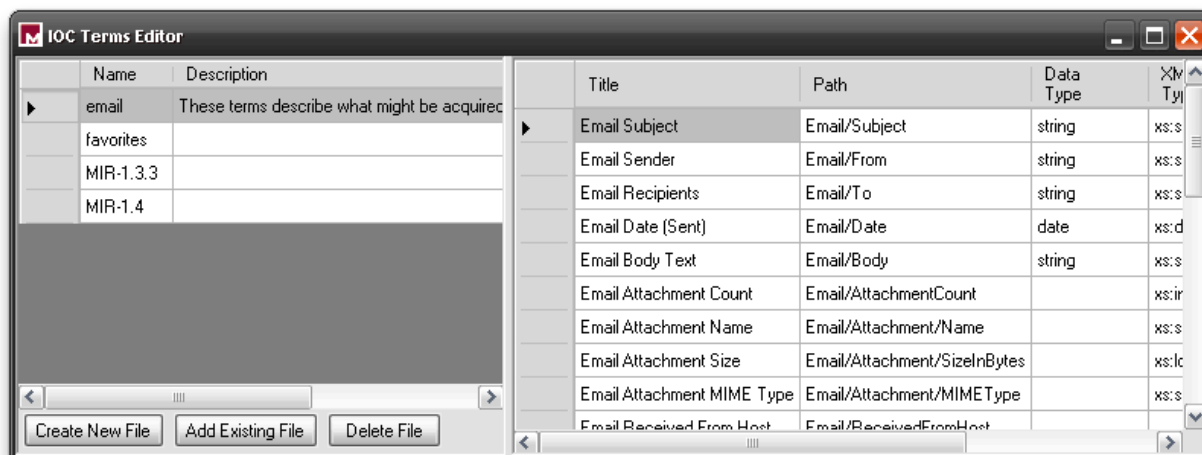


Figure 12: IOC Terms Editor

To add a new terms file, click on the “Create New File” button. This will bring up the standard dialog to save a file. Once that is done, you can begin to add terms.

To add a term, scroll to the bottom of the list (if adding to an existing terms file), find the empty field and begin adding your new term.

Favorites

To add a term to the Favorites menu, you can either add your terms to the existing favorites term file, or add a new one. In order to get items to populate the Favorites menu, you just need to name the terms file something that starts with “favorites”.

Note: It is preferable to create a new favorites term file so that your terms don’t get overwritten with any future updates to IOCe.

IOC Diff

Comparing two IOCs

To see what has changed between IOCs, an IOC Diff tool is available. This works best if you have two different directories opened. To open another directory, use the File→New→Window menu option. This will open a new IOCe window that can be pointed to a different directory without losing what you already have open.

To start comparing two IOCs, click on Tools→Compare Two IOCs, this will open the IOC Diff window.

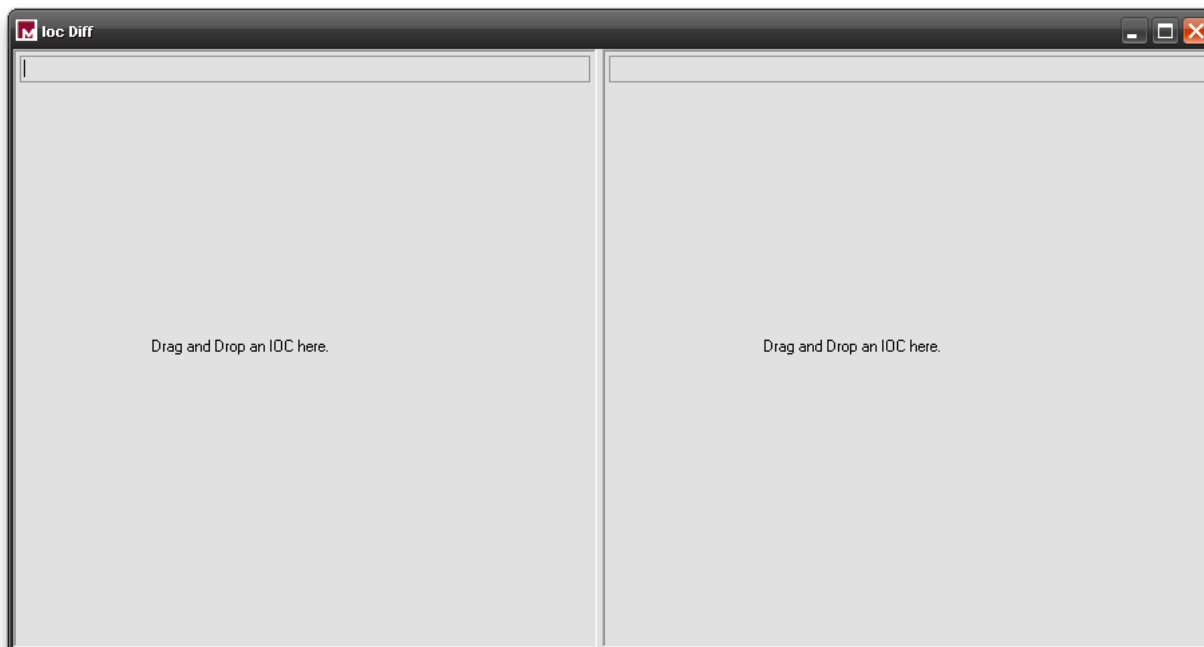


Figure 13: IOC Diff window

From each of the IOCe windows that contain the IOCs you would like to compare, simply drag and drop each IOC onto the left or right panes. Once the second IOC has been dropped, IOCe will compare the differences between the two. The changes have been color-coded, red means that the item was changed or deleted; orange means that the item has been moved to a different layer of logic.

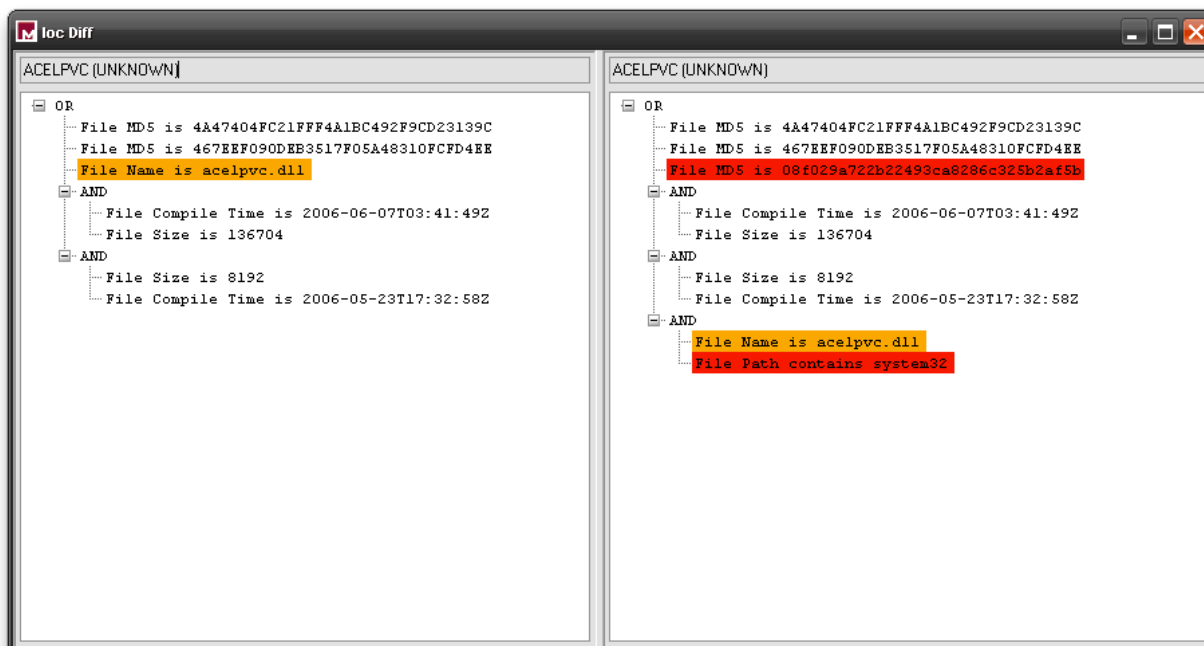


Figure 14: Comparing two IOCs

IOCe Use Cases

Mandiant Intelligent Response (MIR)

There are important items to note about creating IOCs that will be used with MIR.

1. There is currently no way to logically relate two separate objects. For example, the malware may create two separate registry keys, with the paths REG_A and REG_B. On their own, the two registry key paths are not unique. However, the existence of both keys in registry is significant. Unfortunately, an "AND" substructure such as the following is invalid:

(RegistryItem->Registry Path is REG_A) AND (RegistryItem->Registry Path is REG_B)

MIR will interpret this logical relation as an attempt to describe the same object: a registry key with the path REG_A and REG_B at the same time, which cannot happen.

2. Once an "AND" or "OR" substructure is created, all expressions in the logic substructure must fall within the same category:

(**FileItem**->File Name) AND (**FileItem**->File Size) **VALID**

(**FileItem**->File Name) AND (**RegistryItem**->Registry Path) **INVALID**

If you need to generate the XPath filters for use in an Audit, select the File->Generate Filters menu option. You can either generate filters for all IOCs, or just selected ones.

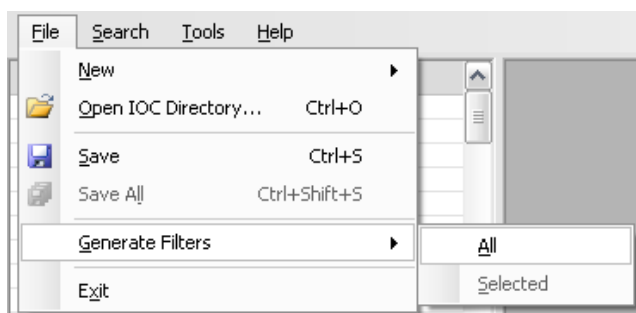


Figure 15: Generate Filters menu option

Other Use Cases

Please refer to the Mandiant IOCe forums for other use cases. <http://forums.mandiant.com>

LICENSING NOTICES

Your use of MANDIANT IOCe is governed solely by the EULA, which shown below:

End-User License Agreement

IMPORTANT! PLEASE READ CAREFULLY.

THIS END-USER LICENSE AGREEMENT (THE "AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU AND MANDIANT CORPORATION ("MANDIANT"). BY CLICKING "I AGREE" BELOW, YOU ACCEPT ALL TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT WISH TO ACCEPT THIS AGREEMENT, YOU SHOULD CLICK "CANCEL" IN WHICH CASE YOU WILL NOT BE ABLE TO USE THE 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 Mandiant IOCe™ software (the "Software") 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 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 CLICKING "I AGREE" BELOW, YOU CONSENT TO BE BOUND BY THESE TERMS AND CONDITIONS.