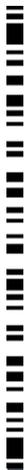




David Ross | Technical Director

The OpenIOC data format

MALWARE IDENTIFICATION

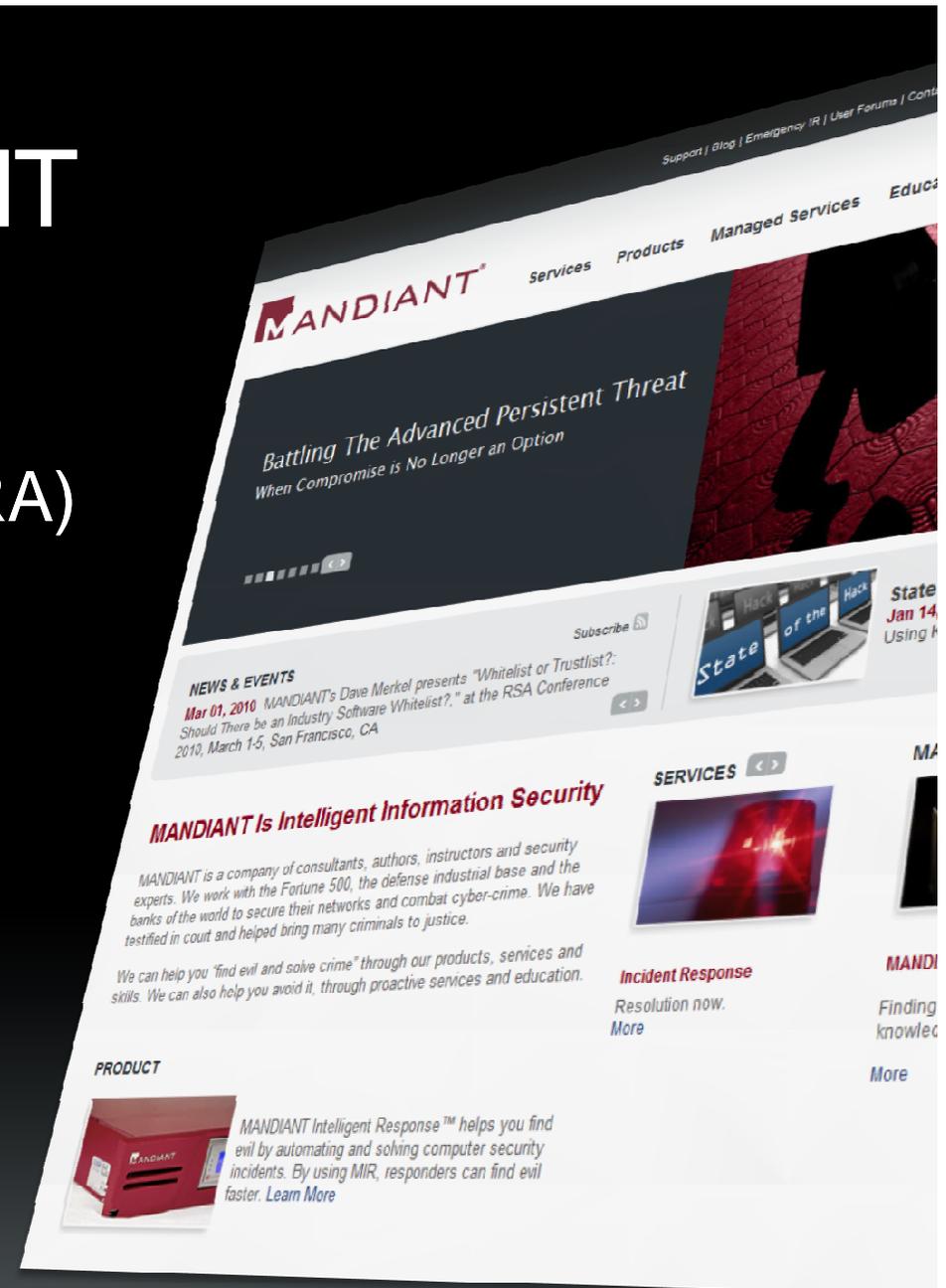


Preview

- What is an Indicator?
- What is OpenIOC?
- Why should I care?
- What is the IOCEditor?
- Where can I get this?

We are MANDIANT

- VISA Qualified Incident Response Assessor (QIRA)
- APT and CDT experts
- Located in
 - Washington
 - New York
 - Los Angeles
 - San Francisco
- Professional and managed services, software and education



Introductions

DAVID ROSS

- Technical Director
- Created OpenIOC format
- Responded to a half million hosts
 - Just last year



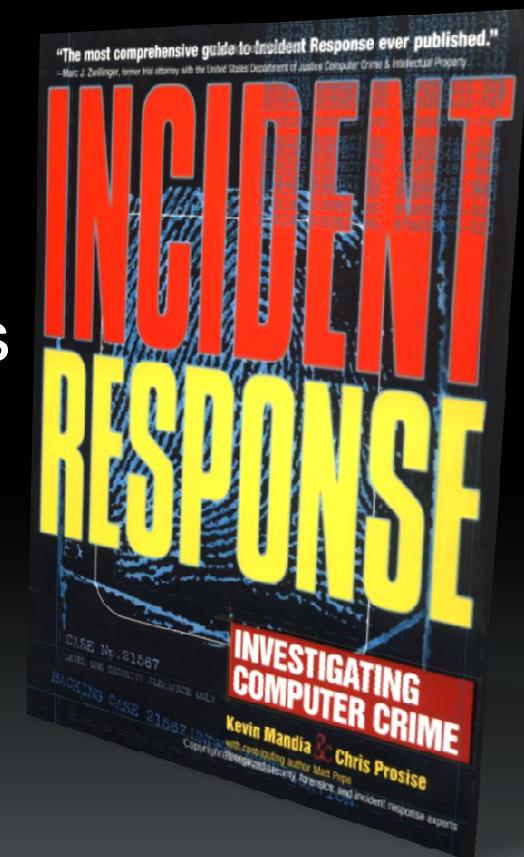
Important note

**All information is derived
from MANDIANT observations
in non-classified environments.**

**Some information has been
sanitized to protect our clients'
interests.**

What is an IOC?

- Indicator of Compromise
- Intelligence used to find evil
 - On a host or on the wire
 - MD5s, file names, packer type
 - Registry keys, mutexes, drivers
 - DNS, IPs, query strings



What is OpenIOC?

- A format to organize your intelligence
- Logical groupings
- Extendable for any indicator type
- XML (of course)

Lists lose relevance

You can not determine:

- why you were looking
- what else is related

Lists are too rigid

Need to look for a new keyword type?

You need to make a new list.

OpenIOC

- A format to organize Indicators
- Turns your data into intelligence
- Designed for data sharing
- Intentionally extendable

OpenIOC is technology agnostic

- Does not require any product
- Easily converts to needed formats
 - We have some pre-built
 - It is just XML after all
- It is used by MIR
 - Really comes alive with MIR

In use for over two years

- Used by MANDIANT
- Based on lessons learned in the field
- Made public by customer request
- 9 out of 10 consultants prefer OpenIOC



THIS is OpenIOC!!!

- The Why
- The What

The screenshot displays the OpenIOC interface for an IOC titled "IEUPDATES BHO SPYWARE". The interface includes a header with a collapse icon and the title. Below the header, there are several input fields for IOC details: IOC ID (e5881ed9-d5bb-40c0-bf9d-9dd83b972dfe), Summary (IEUPDATES BHO SPYWARE), Keywords (spyware downloader BHO), Author (Mandiant), and Authored on (2009-03-23T02:57:13Z). To the right of these fields is a table with two columns: Property and Content. The table contains the following entries:

Property	Content
threatgroup	None
reportid	MA-12345
capability	Downloader
capability	Installer

Below the input fields is a Description section with a text area containing the following text:

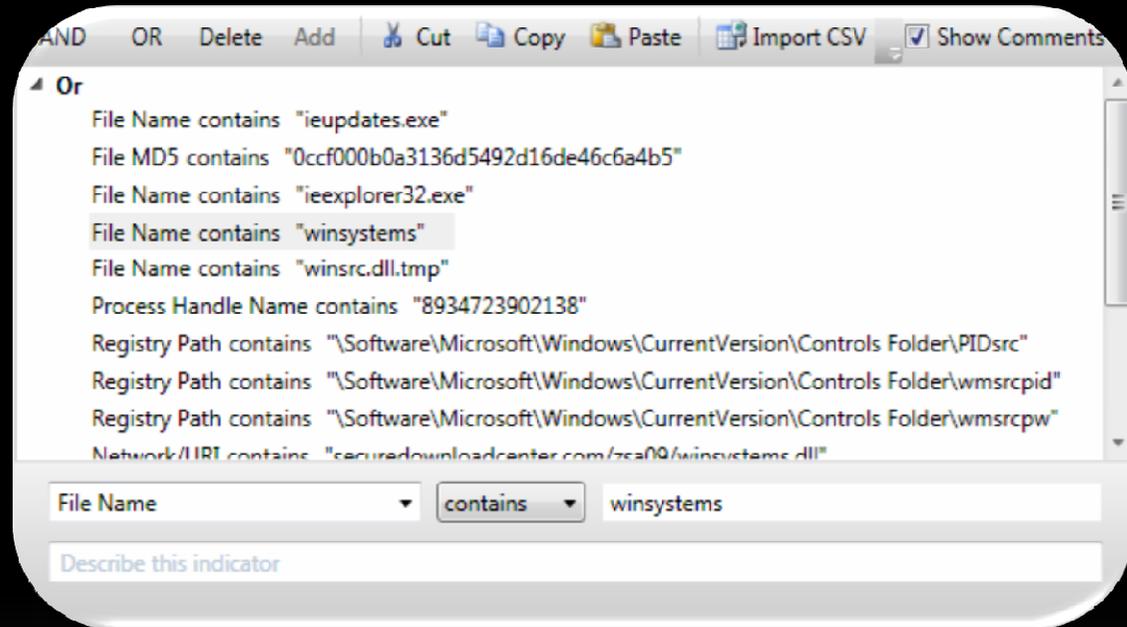
ieupdates.exe is a downloader which attempts to install winsrc.dll as a browser helper object (BHO) or toolbar from securedownloadcenter.com. Given the history of malicious browser toolbars, this is likely intended to install spyware on the compromised machine. The malware will not install on systems installed with the default language set to Russian or Ukrainian.

At the bottom of the interface, there is a toolbar with buttons for AND, OR, Delete, Add, Cut, Copy, Paste, Import CSV, and Show Comments. Below the toolbar is a list of rules under the heading "Or":

- File Name contains "ieupdates.exe"
- File MD5 contains "0ccf000b0a3136d5492d16de46c6a4b5"
- File Name contains "ieexplorer32.exe"
- File Name contains "winsystems"
- File Name contains "winsrc.dll.tmp"
- Process Handle Name contains "8934723902138"
- Registry Path contains "\\Software\\Microsoft\\Windows\\CurrentVersion\\Controls Folder\\PIDsrc"
- Registry Path contains "\\Software\\Microsoft\\Windows\\CurrentVersion\\Controls Folder\\wmsrcpid"
- Registry Path contains "\\Software\\Microsoft\\Windows\\CurrentVersion\\Controls Folder\\wmsrcpw"
- Network/URI contains "securedownloadcenter.com/3ca09/winsystems.dll"

Stores what we are looking for

- Content
 - Keyword
- Context
 - Keyword Type
- Construct
 - Logic
 - We'll get into this later



Along with the 'who' and 'why'

- Name, Description, Author, Category...
- External references
 - Data sources
 - Reports
 - Threat groups

IEUPDATES BHO SPYWARE

IOC ID	e5881ed9-d5bb-40c0-bf9d-9dd83b972dfe	Property	Content
Summary	IEUPDATES BHO SPYWARE	threatgroup	None
Keywords	spyware downloader BHO	reportid	MA-12345
Author	Mandiant	capability	Downloader
Authored on	2009-03-23T02:57:13Z	capability	Installer

Description

Ieupdates.exe is a downloader which attempts to install winsrc.dll as a browser helper object (BHO) or toolbar from securedownloadcenter.com. Given the history of malicious browser toolbars, this is likely intended to install spyware on the compromised machine. The malware will not install on systems installed with the default language set to Russian or Ukrainian.

Advantages

- Keeps indicators with context
 - Quickly determine “why” from “what”
- Sharing with others
 - Easy to combine
 - Generate indicators from multiple sources
 - No more formatting questions

Advantages

- Scalability
 - Thousands of indicators in hundreds of IOCs
- It's only XML
 - Convert to ANY format needed
 - We have lots of examples for this!
- OpenIOC = Force Organizer

The IOC Editor

The screenshot displays the IOC Editor application. On the left, a table lists various indicators:

Description	Author	Id
MGS.EXE	Mandiant	6b4bee70
BCIPM.DLL (SPYWARE)	Mandiant	70eda23c
MED.DLL (DOWNLOADE)	Mandiant	d3d778cc
SVCHOST.EXE (WEB-PAC)	Mandiant	d708bd57
IEUPDATES BHO SPYW	Mandiant	e5881ed9
DEMO: Unsupported bu	Mandiant	ffffff-956

The main window shows the details for the selected indicator, 'IEUPDATES BHO SPYWARE'. The IOC ID is e5881ed9-d5bb-40c0-bf9d-9dd83b972dfe. The summary is 'IEUPDATES BHO SPYWARE'. The keywords are 'spyware downloader BHO'. The author is 'Mandiant' and it was authored on '2009-03-23T02:57:13Z'. The description states: 'Ieupdates.exe is a downloader which attempts to install winsrc.dll as a browser helper object (BHO) or toolbar from securedownloadcenter.com. Given the history of malicious browser toolbars, this is likely intended to install spyware on the compromised machine. The malware will not install on systems installed with the default language set to Russian or Ukrainian.'

Below the description, there is a list of search criteria for this indicator:

- File Name contains "ieupdates.exe"
- File MD5 contains "0ccf000b0a3136d5492d16de46c6a4b5"
- File Name contains "ieexplorer32.exe"
- File Name contains "winsystems"
- File Name contains "winsrc.dll.tmp"
- Process Handle Name contains "8934723902138"
- Registry Path contains "\\Software\\Microsoft\\Windows\\CurrentVersion\\Controls Folder\\PIDsrc"
- Registry Path contains "\\Software\\Microsoft\\Windows\\CurrentVersion\\Controls Folder\\wmsrcpid"
- Registry Path contains "\\Software\\Microsoft\\Windows\\CurrentVersion\\Controls Folder\\wmsrcpw"

At the bottom, there is a search filter: File Name contains winsystems.

Pretty cool, huh?

OpenIOC data feed

The screenshot shows the OpenIOC application interface. The main window displays a list of IOCs with columns for Description, Author, and Id. The entry 'IEUPDATES BHO SPYWARE' is selected. A detailed view of this entry is shown on the right, including its IOC ID, Summary, Keywords, Author, Authored on date, and Description. A red box highlights the selected entry in the list, and red lines connect it to the detailed view. Another red box highlights the detailed view, and red lines connect it to a larger table below.

Description	Author	Id
MGS.EXE	Mandiant	6b4bee70-
BCIPM.DLL (SPYWARE)	Mandiant	70eda23c-
MED.DLL (DOWNLOADE	Mandiant	d3d778cc-
SVCHOST.EXE (WEB-PA	Mandiant	d708bd57-
IEUPDATES BHO SPYW	Mandiant	e5881ed9
DEMO: Unsupported bu	Mandiant	fffffff-956

What we are looking for

The screenshot shows the Mandiant IOC tool interface. The left pane displays a list of IOCs with columns for Description, Author, and Id. The selected IOC is 'IEUPDATES BHO SPYW ARE' with ID 'e5881ed9'. The middle pane shows the details for this IOC, including its ID, summary, keywords, author, and description. The bottom pane shows a search filter for 'File Name contains winsystems'. A red box highlights the search filter, and a larger red box highlights the search results.

Description	Author	Id
MGS.EXE	Mandiant	6b4bee70
BCIPM.DLL (SPYWARE)	Mandiant	70eda23c
MED.DLL (DOWNLOADE)	Mandiant	d3d778cc
SVCHOST.EXE (WEB-PAC)	Mandiant	d708bd57
IEUPDATES BHO SPYW ARE	Mandiant	e5881ed9
DEMO: Unsupported bu	Mandiant	ffffff-956

IOC ID: e5881ed9-d5b

Summary: IEUPDATES BHO

Keywords: spyware down

Author: Mandiant

Authored on: 2009-03-23T0

Description: ieupdates.exe is a downloade or toolbar from securedownl is likely intended to install spy systems installed with the def

Search Filter: File Name contains winsystems

Search Results:

- File Name contains "ieupdates.exe"
- File MD5 contains "0ccf000b0a3136d5492d16de46c6a4b5"
- File Name contains "ieexplorer32.exe"
- File Name contains "winsystems"
- File Name contains "winsrc.dll.tmp"
- Process Handle Name contains "8934723902138"
- Registry Path contains "\Software\Microsoft\Windows\CurrentVersion\Controls Folder\PIDsrc"
- Registry Path contains "\Software\Microsoft\Windows\CurrentVersion\Controls Folder\wmsrcpid"
- Registry Path contains "\Software\Microsoft\Windows\CurrentVersion\Controls Folder\wmsrcpw"

Easy to create indicators

The screenshot shows the Mandiant indicator management interface. On the left, a table lists various IOCs:

Description	Author	Id
MGS.EXE	Mandiant	6b4bee70
BCIPM.DLL (SPYWARE)	Mandiant	70eda23c
MED.DLL (DOWNLOADE)	Mandiant	d3d778cc
SVCHOST.EXE (WEB-PAC)	Mandiant	d708bd57
IEUPDATES BHO SPYW	Mandiant	e5881ed9
DEMO: Unsupported bu	Mandiant	ffffff-956

The main window displays the details for the selected IOC, 'IEUPDATES BHO SPYWARE':

- IOC ID:** e5881ed9-d5bb-40c0-bf9d-9dd83b972dfe
- Summary:** IEUPDATES BHO SPYWARE
- Keywords:** spyware downloader BHO
- Author:** Mandiant
- Authored on:** 2009-03-23T02:57:13Z
- Description:** Ieupdates.exe is a downloader which attempts to install winsrc.dll as a browser helper object (BHO) or toolbar from securedownloadcenter.com. Given the history of malicious browser toolbars, this is likely intended to install spyware on the compromised machine. The malware will not install on systems installed with the default language set to Russian or Ukrainian.

Below the details, a search bar shows the following criteria:

- File Name contains "ieupdates.exe"
- File MD5 contains "0ccf000b0a3136d6492d16de46c6a4b5"
- File Name contains "ie"
- File Name contains "win"
- File Name contains "win"
- Process Handle Name contains
- Registry Path contains
- Registry Path contains
- Registry Path contains

A dropdown menu is open, showing the following options:

- File Name
- File Import Function
- File Import Name
- File MD5
- File Modified Time
- File Name**
- File Owner
- File Path
- File Raw Checksum

The selected option is 'File Name', and the value 'winfont.cpl' is entered in the adjacent field.

Extendable keywords

- Can use ANY keyword type
- You can create new keywords
- It's just XML after all

	EventLogItem/EID		EventLog ID
	EventLogItem/genTime		EventLog GenTime
File Name	EventLogItem/message		EventLog Message
File Path	HookItem/HookedFunction	ProcessItem/name	Process Name
File Full Path	HookItem/HookingModule	ProcessItem/HandleList/Handle/Name	Process Handle Name
File MD5	HookItem/HookedModule	ProcessItem/SectionList/MemorySection/Name	Process Section Name
File Modified Time	UserItem/Username	PortItem/remoteIP	Port Remote IP
File Base Address	ServiceItem/name	PortItem/Path	Port Path
File Detected Anomalies	ServiceItem/serviceDLL		Service DLL
File EntryPoint Sig Name	ServiceItem/path		
File EntryPoint Sig Type	RegistryItem/Path	Email/Subject	Email Subject
File Export Function	RegistryItem/Text	Email/From	Email Sender
File Export Count		Email/To	Email Recipients
File Extra Bytes	FileItem/PEInfo/ExtraBytesAfterLastSection	Email/Date	Email Date (Sent)
File Import Function	FileItem/PEInfo/ImportedModules/Module/ImportedFunc	Email/Body	Email Body Text
File Import Name	FileItem/PEInfo/ImportedModules/Module/Name	Email/AttachmentCount	Email Attachment Count
File Computed Checksum	FileItem/PEInfo/PEChecksum/PEComputedAPI	Email/Attachment/Name	Email Attachment Name
		Email/Attachment/SizeInBytes	Email Attachment Size
		Email/Attachment/MIMEType	Email Attachment MIME Type

The Indicator Terms document

```
<?xml version="1.0"?>
<iocetermlist
  last-modified="2010-03-12T00:41:57.2994379Z"
  description="These terms describe what might be acquired :
  <ioceterm text          = "Email/Subject"
    title                 = "Email Subject"
    data-type             = "xs:string"
    display-type          = "string"
    term-source           = "example/emailaudit" />
  <ioceterm text          = "ProcessItem/HandleList/Handle/Name"
    title                 = "Process Handle Name"
    data-type             = "xs:string"
    display-type          = "string"
    term-source           = "application/vnd.mandiant.mir" />
  <ioceterm text          = "FileItem/Md5sum"
    title                 = "File MD5"
    data-type             = "Md5Sum"
    display-type          = "md5"
    term-source           = "application/vnd.mandiant.mir" />
</ioceterm>
```

Duplicating meaning

- Same problem as proprietary lists
- Use existing terms
- Publish your terms!
- Make mappings



`FileItem/PEInfo/ImportedModules/Module/Name`

Why we are looking for it

The screenshot displays a malware analysis tool interface. On the left, a table lists various IOCs. The entry 'IEUPDATES BHO SPYWARE' is highlighted. A red box highlights this entry and its corresponding detailed view on the right. The detailed view shows the following information:

Property	Content
threatgroup	None
reportid	MA-12345
capability	Downloader
capability	Installer

The detailed view also includes the following fields:

- IOC ID:** e5881ed9-d5bb-40c0-bf9d-9dd83b972dfe
- Summary:** IEUPDATES BHO SPYWARE
- Keywords:** spyware downloader BHO
- Author:** Mandiant
- Authored on:** 2009-03-23T02:57:13Z
- Description:** Ieupdates.exe is a downloader which attempts to install winsrc.dll as a browser helper object (BHO) or toolbar from securedownloadcenter.com. Given the history of malicious browser toolbars, this is likely intended to install spyware on the compromised machine. The malware will not install on systems installed with the default language set to Russian or Ukrainian.

Refer to external data

The screenshot shows a software interface with a table of IOCs on the left and a detailed view of a selected IOC on the right. A red box highlights a table of properties and their values, which is also shown in a larger, detailed view below.

Property	Content
threatgroup	None
reportid	MA-12345
capability	Downloader
capability	Installer

Importing your old lists

- Included feature in IOCEditor
 - Trivial to script (It's only XML)

Configure how imported data columns will be mapped

Column	Column Action	Indicator Term	Condition	Value Form
01F1FC3DA7BBDF74FC9AA80E641059F1	Create items	File MD5	is	{0}
logsysx#exe	Create items	File Name	contains	{0}
1233	Do nothing		is	{0}

All 29 rows will be imported. Ctrl-Click or Shift-Click the data to select rows to import.

01F1FC3DA7BBDF74FC9AA80E641059F1	logsysx#exe	1233	
06483df47e5fe6d6ab09008b5e27eb3c	proforma.doc.scr	3333	
0D58F930A99E9741C309EBCDA2BE7A25	qw03021.exe	75578	
0FDA739B7AC216CE895F0E9822216F78	SEAGENT.exe	23456	
11c26a68b47549a92c338ee29296e157	smyc.dll	34212	
14984CDDE77E62E00425165D82AD4C0C	w32timesvc.exe	12345	
1573FEA7BBE88A7DEC95BFAE4EA76572	werkwl.dll	76554	
1C6DC0A643C65E9549E8DA043C61E376	whhrwoym.sys	334433	
01E9-505E-4E3A43E44E-0-085b-b3	pubkey.exe.dll	3335	

Import

OpenIOC in the Field

- MANDIANT uses OpenIOC every day
 - Centralized all of our intelligence
 - No more private lists
 - Rapid exchange of data across teams

**Every consultant knows
what every other consultant knows.**

Converting OpenIOC

- Your old flat lists of indicators
- HTML
- XPath
- Lucene
- Snort
- Reporting statistics
- Word documents (really)
- Pie charts
- ...it's just xml

Advanced definition constructs

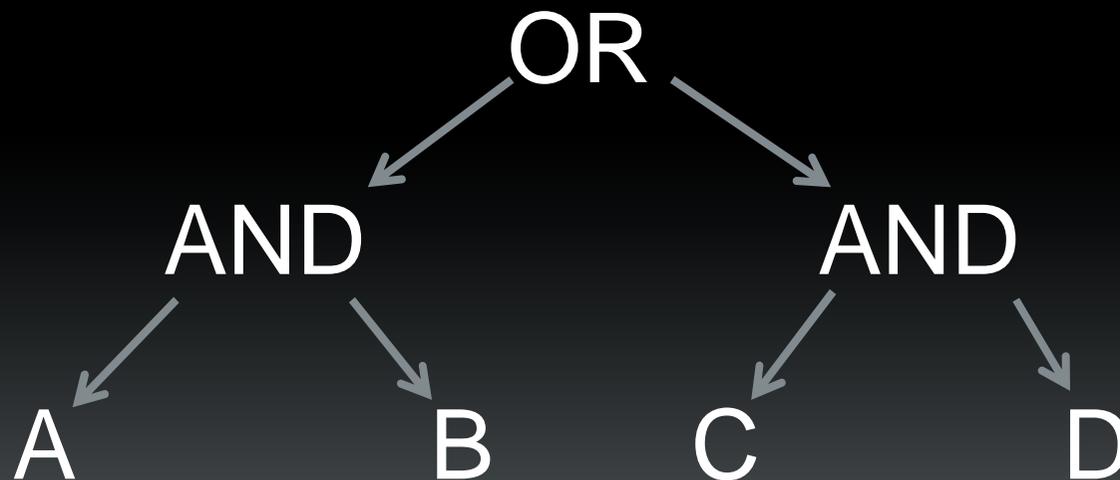
- Why just keywords?
 - Is everything just a string match?
- OpenIOC supports logic
 - AND, OR
 - is, isnot
 - contains, containsnot



Logic Trees

A and B or C and D

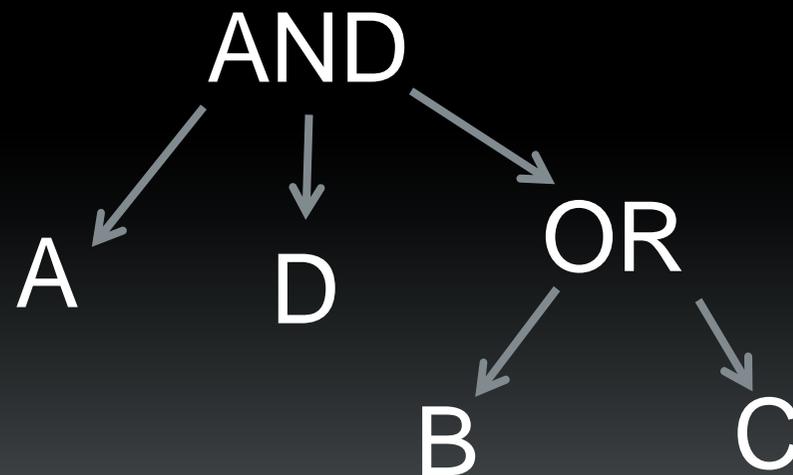
(A and B) or (C and D)



Logic Trees

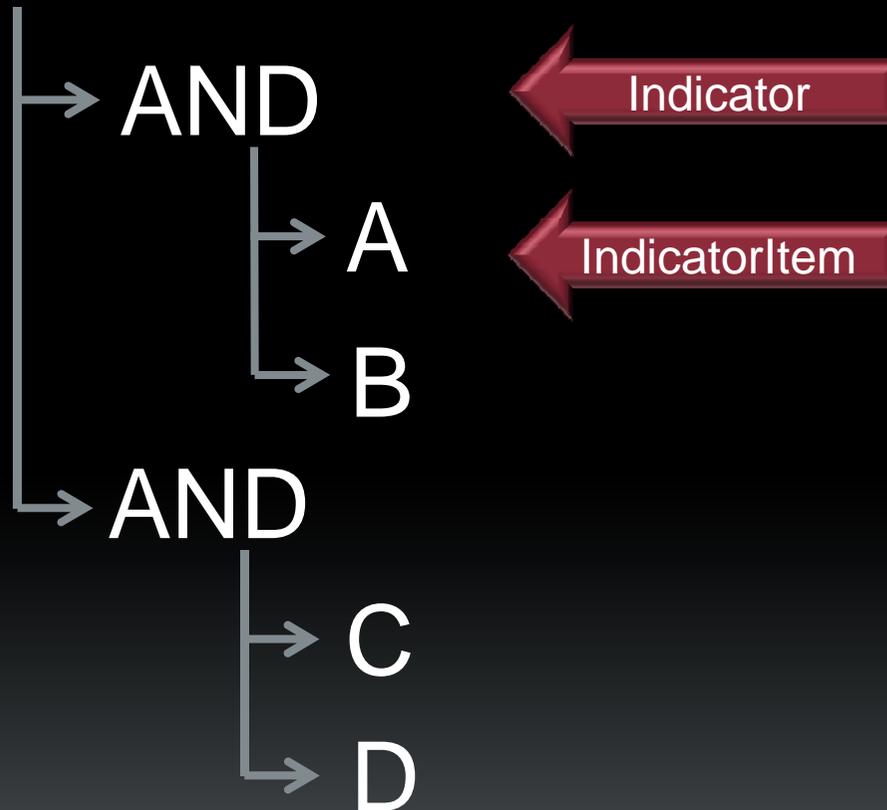
A and B or C and D

A and (B or C) and D



IOC Logic Tree

OR

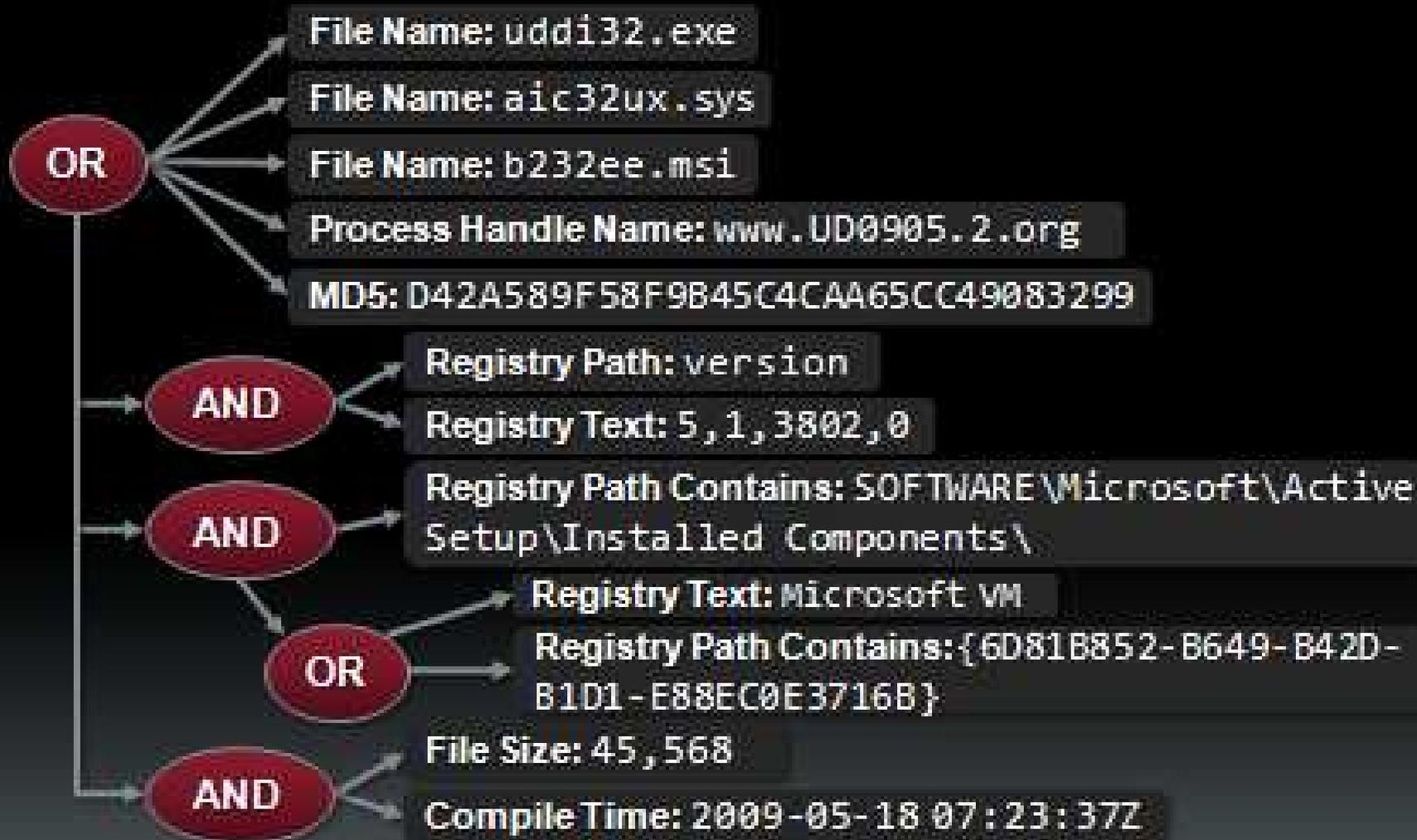


- Indicators are ANDs and ORs
- IndicatorItems are the leaf nodes of data

Allows this...

```
FOR
File Name is sunjre16.exe
File Name is eic16ux.sys
File Name is e216ee.msi
File Name is webserv32.exe
File Name is 60927ux.sys
File Name is b26092.msi
File Name is uddi16.exe
File Name is aic16ux.sys
File Name is b216ee.msi
File MD5 is 5611458A5A03998CB1268190E2818C63
File MD5 is 711F4FE93EAOE8F253FA0643E273FE8B
File MD5 is 4BFDB1ACBB32348E3D4572CD88B9A6FC
File MD5 is CB8990122D2675990C874B4959306793
File MD5 is 8B911B2D548FF26AE6C236D3DA2DDF2C
File MD5 is 402366D37A54CCA71238A0FC771DEE30
File MD5 is 98A9DF9AC85A1755CB3EBE1d4AEA5498
File Name is commdlg64.exe
File Name is ai3lux.sys
File Name is b30ee.msi
File Name is smscfg32.exe
File Name is a0c77ux.sys
File Name is b087ee.msi
File MD5 is 1954EB413FDAADE614031B2231E35C7B
File Name contains \Application Data\Microsoft\Media Player\DefaultStore32.exe
File Name contains \Application Data\Microsoft\Media Index\wmplibrary32.db
File Name contains \Favorites\janny.jpg
Process Handle Name is www.TW0901.2.org
Process Handle Name is www.UG0902.2.org
Process Handle Name is www.UG0905.1.org
Process Handle Name is 1.2.UD0804.1z
Process Handle Name is www.WW0902.1.org
```

...to become this



Takeaway

Easily describe the attacker's TTPs in ways that are difficult or expensive to evade.

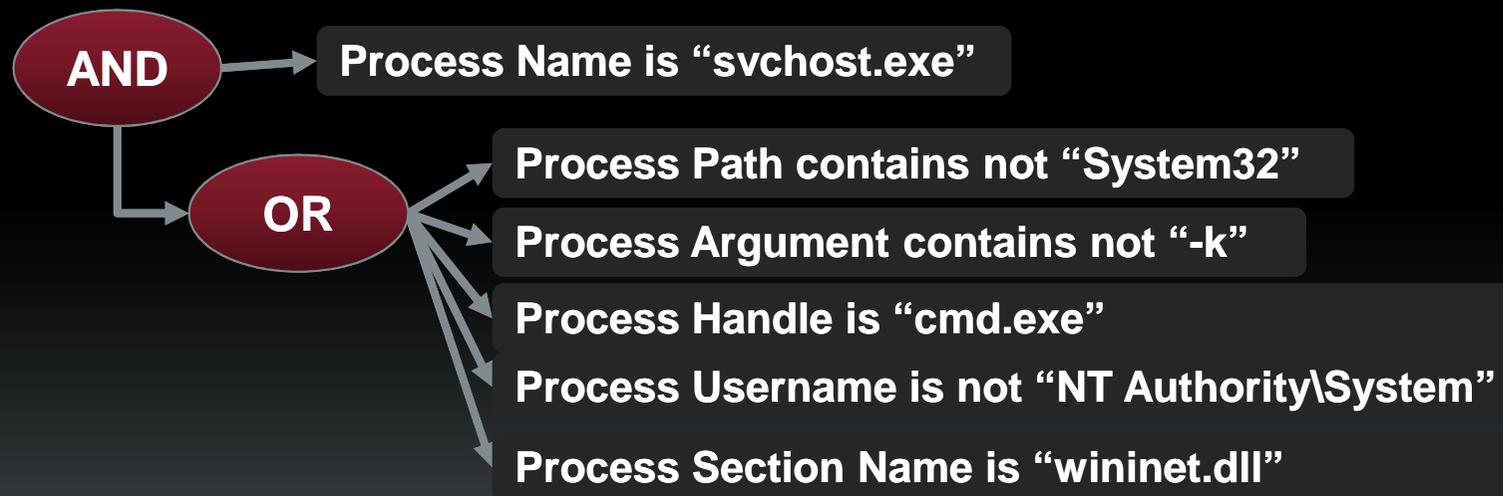
Storing general IR process

- Store general IR knowledge
- Generate 'Generic Indicators'
- Share 'tribal knowledge'



A thousand words in one IOC

“When you see svchost.exe running out of something other than ‘system32’ or it doesn’t have that dash k at the end or it’s not being run as System or...”



Where do I get it?

- www.mandiant.com/products/free_software/ioce/
- IOCe the editor
- Schemas
- XML and XSLT examples
- Much, much more!

Free Software



MANDIANT IOCe is a free editor for Indicators of Compromise (IOCs). [More](#)

Q&A

- david.ross@mandiant.com

- More MANDIANT info
 - <http://www.mandiant.com/>
 - <http://www.twitter.com/mandiant>
 - info@mandiant.com

