Identifying & Sharing Threat Information

with OpenIOC

NIST IT SAC -- 11/01/11

Doug Wilson, Principal Consultant
doug.wilson@mandiant.com

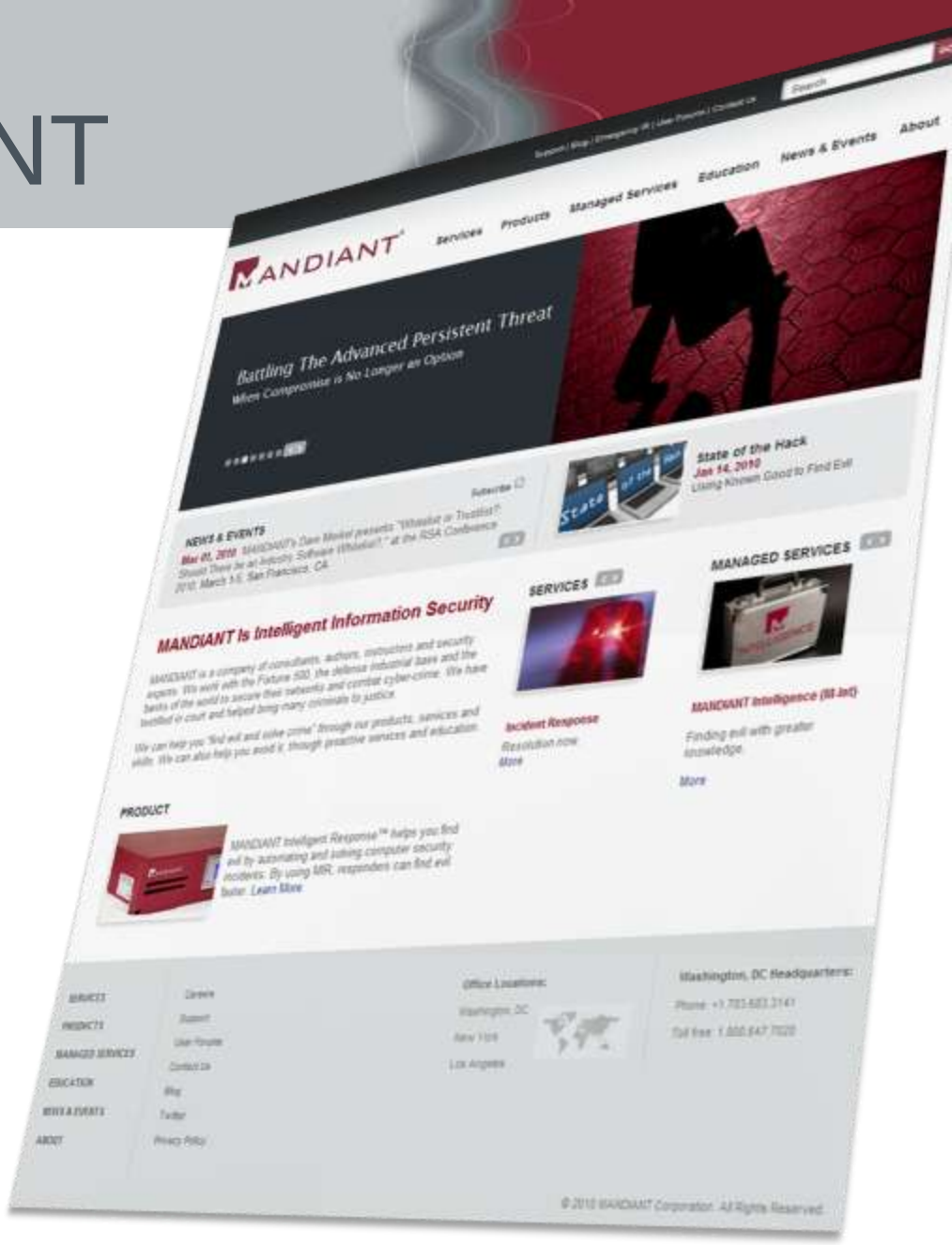
Important Note

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

Some information has been sanitized to protect our clients' interests

We are MANDIANT

- VISA Qualified Incident Response Assessor (QIRA)
- APT & CDT experts
- MCIRT – newly launched
- Application and Network Security Evaluations
- Located in
  - Washington (2 locations)
  - New York
  - Los Angeles
  - San Francisco
- Professional and managed services, software and education



About Me

MANDIANT

DOUG WILSON

- Principal Consultant
  - OpenIOC Advocate
- Background
  - Incident Response
  - Multi-Tiered Application Architecture
- Supports IAD Center for Assured Software (CAS)
- DC Local: OWASP DC, AppSec DC, DHS SwA Forum

Our Agenda

- Introduction to OpenIOC
- IOC Examples
- IOCs and the Investigative Process
- Free Tools for use with OpenIOC
- And one more thing. . .

Intro to OpenIOC

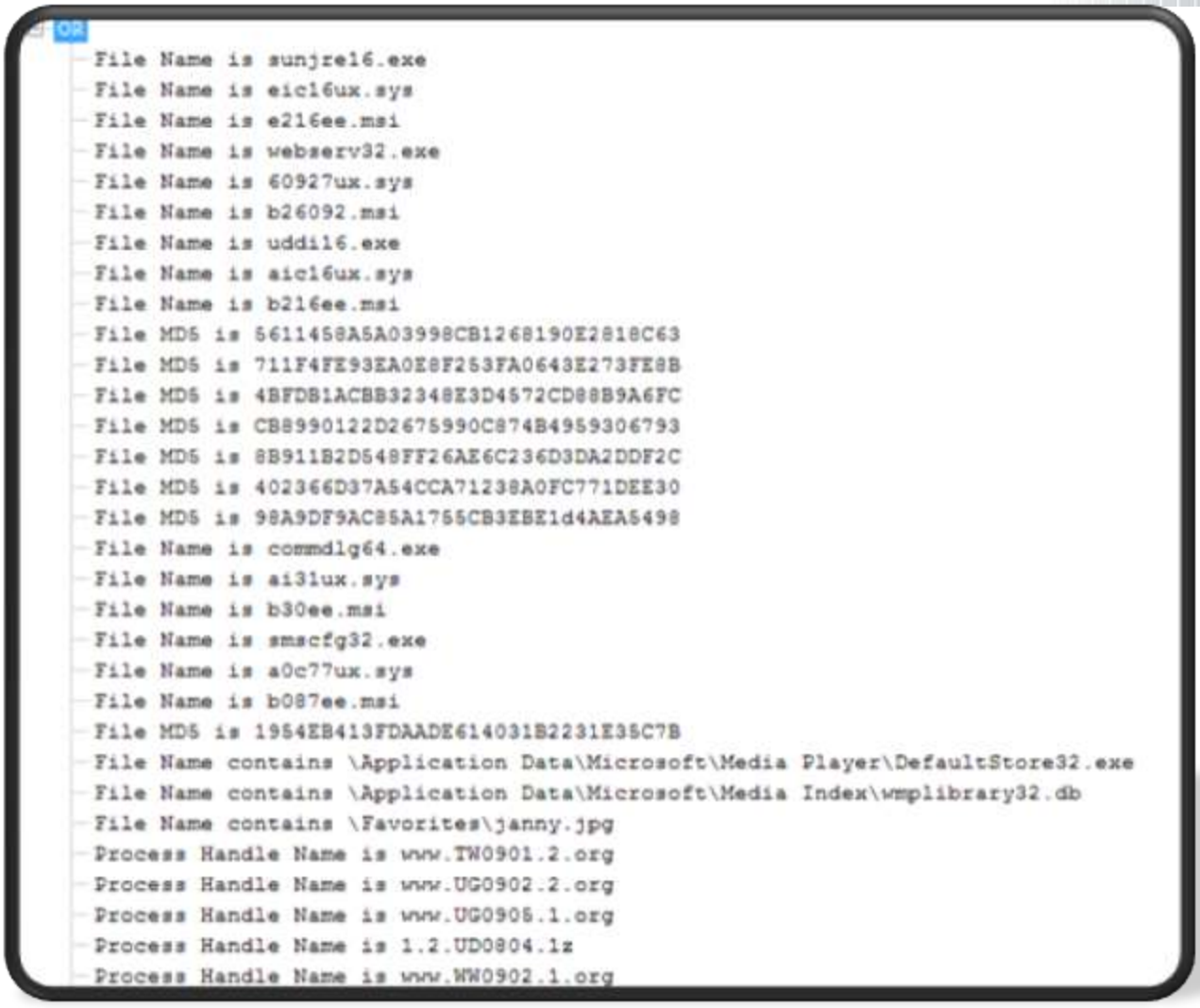
The OpenIOC Format

- IOC = “Indicator of Compromise”
- OpenIOC =
  - Way to organize your Threat Intelligence
  - XML based
  - Logical groupings of forensic artifacts
  - Based on real world experience
  - Extendable & expandable

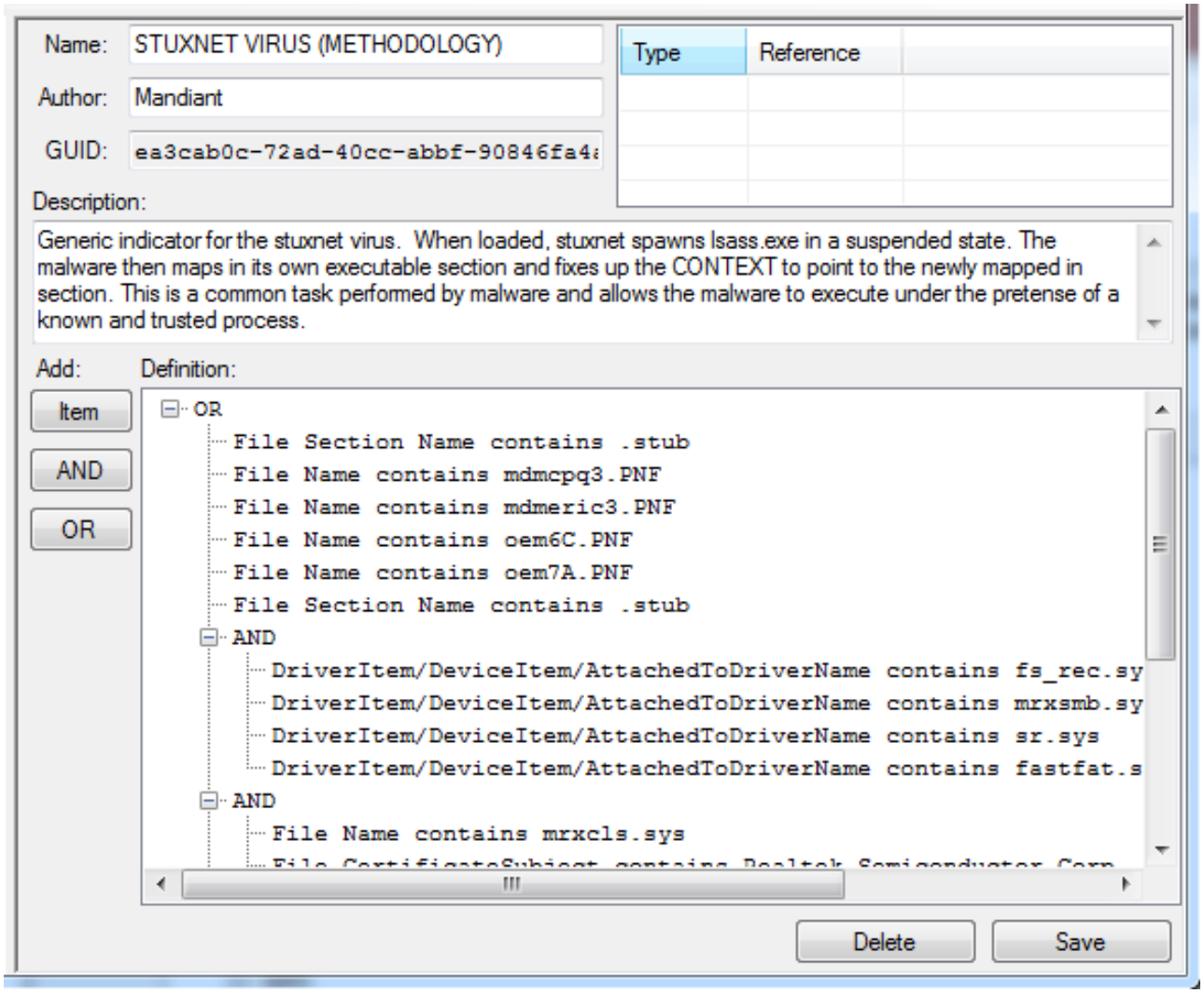
Before OpenIOC

- Lists of stuff to find evil
  - Easy to create
  - Difficult to maintain
  - Terrible to share
- Lists do not provide context
  - An MD5 of what?
  - Who gave me this?
  - Where is the report?
  - Where is the intelligence??
- **Lists encourage reliance on easily mutable forensic artifacts**

OpenIOC allows this…



…to become this



OpenIOC Terms

MANDIANT

- 37 terms shown (out of over 500)
- MANDIANT terms drawn from real world
- Terms easily added if needed.

Characteristics	Definition of Characteristic
File Accessed Time	Last access time of a file
File Attribute	Attributes of a file (Read-only, Hidden, System Directory, etc.)
File Changed Time	File name modified of a file
File Compile Time	Checks the compile time of a file
File Created Time	Creation time of a file
File Digital Signature Description	Description of whether the signature is verified or not
File Digital Signature Exists	Verifies that a digital signature exists
File Digital Signature Verified	Verifies a digital signature is valid
File Export Function	Export function declared by a file
File Extension	Extension of a file
File Full Path	Full path for a file
File Import Function	Import function declared by a file
File Import Name	Import name declared by a file
File MD5	MD5 of the file
File Modified Time	Modified time of a file
File Name	Name of a file
File Owner	Owner of the file
File Path	Path of a file
File PE Type	Checks the PE type of a file

Characteristics	Definition of Characteristic
File PeakEntropy	Peak entropy of a file
File Raw Checksum	Calculated checksum of a file
File Size	Size of the file
File Strings	Readable strings of a file's binary data
Network DNS	DNS queries on a network
Network String URI	URI associated with network traffic
Network String User Agent	User agent associated with network traffic
Process Handle Name	Name of a process handle
Process Name	Name of a process
Registry Key ModDate	Modification time of a registry key
Registry NumSubKeys	Checks the total number of subkeys associated to a registry key
Registry Path	Path of a registry item
Registry Text	Contents of the registry text field
Service Descriptive Name	Description text of a service
Service DLL	DLL implemented by a service
Service Name	Name of a Service
Service Path	Path to the service file
Service Status	Checks the current status of a service

IOC Examples

IOC Functionality

MANDIANT

Signatures

- File specifics: MD5, compile time, file size, file name + path, etc.
- Memory entities: Services, Processes, Handles, Mutexes
- Registry entries: Unique entries, persistence mechanisms

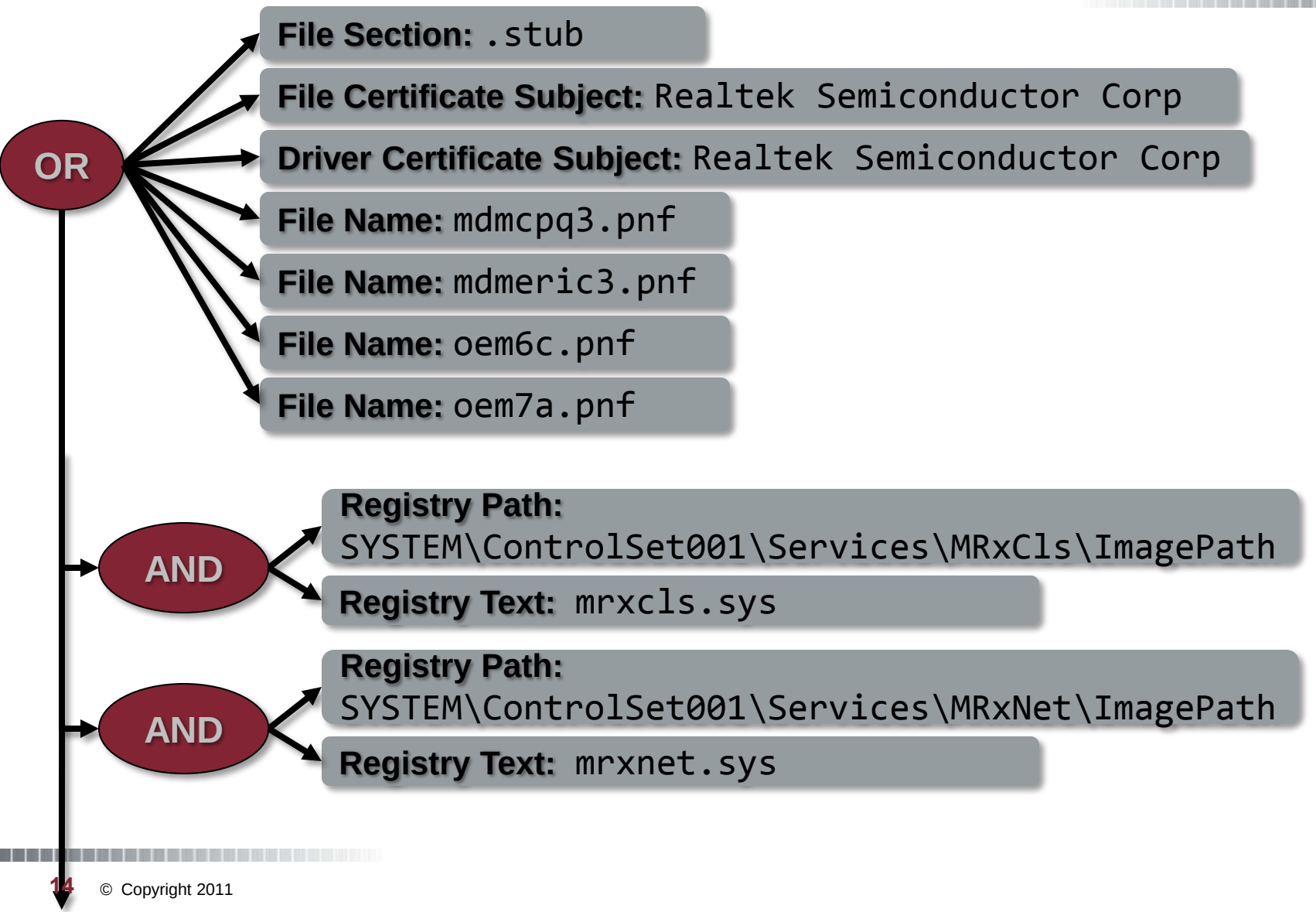
Increasing Complexity

- Combine these together logically to create powerful searches.
- Look for commonalities across groups of malware
- Use on collections of data to look for anomalies

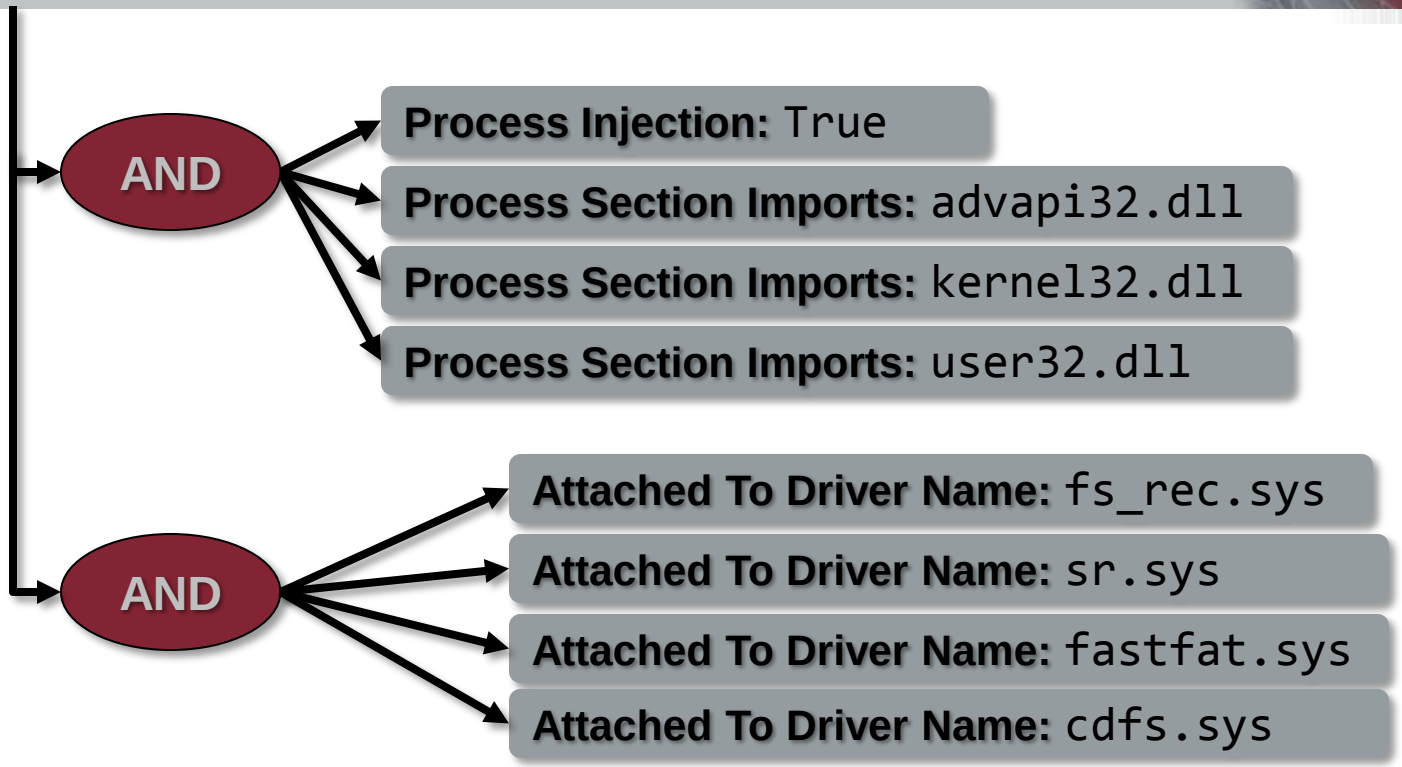
Methodology

- Focus on what attacker *does* rather than what malware *is*
- Look for attacker behavior beyond compromise and exploits
- Staging locations, naming conventions, recurring behaviors

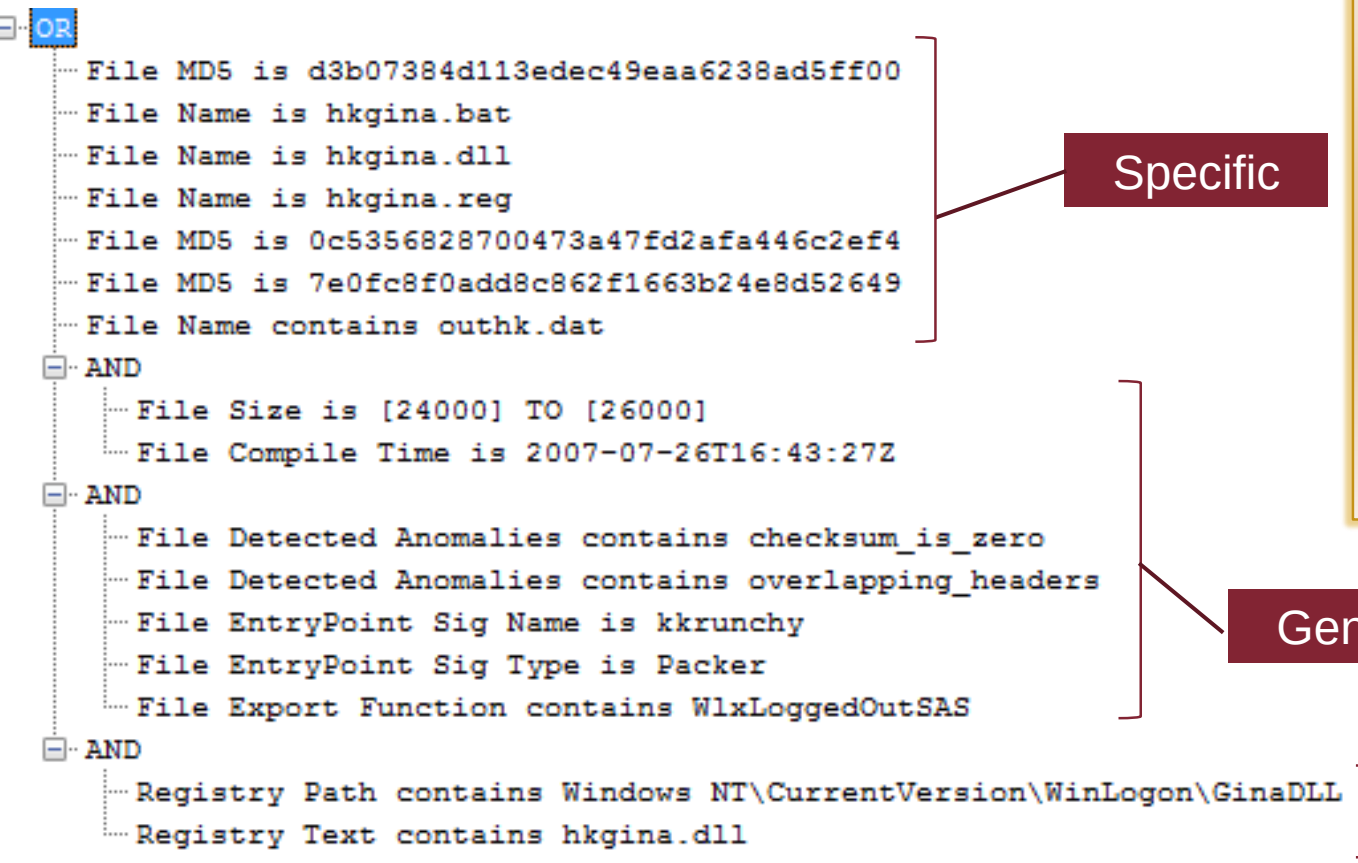
Stuxnet IOC



Stuxnet IOC



Combining Functionality



Specific

Generic

Specific

Malware Analysis Report

...This malware is a "GINA" (Graphical Identification and Authentication) replacement. It records all users who log on to the system and their passwords to file "outhk.dat"...

Working on a collection

Known Services (excerpts)

```
AND
    Service Name is themes
    Service DLL contains not \system32\shsvcs.dll
    Service DLL contains not \system32\themeservice.dll
AND
    Service Name is shellhwdetection
    Service DLL contains not \system32\shsvcs.dll
AND
    Service Name is lanmanserver
    Service DLL contains not \system32\srvsvc.dll
```

Whitelist by ServiceDLL name

Whitelist by service Digital Signatures

```
AND
    Service Name is lanmanserver
    ServiceItem/serviceDLLSignatureVerified is false
AND
    Service Name is termservice
    ServiceItem/serviceDLLSignatureVerified is false
    Service Path Signature Verified is false
AND
    Service Name is trkwks
    ServiceItem/serviceDLLSignatureVerified is false
AND
```

Methodology

```
OR
  AND
    File Name is index.dat
    File Strings contains System Volume Information
  AND
    File Name contains hh.dat
    File Strings contains 2011 Salary.chm
  URL History URL contains www.innocuous-site.org
  EventLog user contains ADOMAIN\User12
  File Owner is ADOMAIN\User12
```

Activity-based:
- Files opened
- CHM file opened
- Website visited

Compromised User:
- Events generated
- Files owned

Evidence of suspicious scheduled tasks

```
OR
  AND
    OR
      File Full Path contains \Windows\SchedLgU.txt
      File Full Path contains \Winnt\SchedLgU.txt
    OR
      File Strings contains at1.job
      File Strings contains at2.job
      File Strings contains cmd.exe
      File Strings contains at3.job
      File Strings contains at4.job
      File Strings contains at5.job
```

IOCs and the Investigative Process

The Current Threat

MANDIANT

Buzzwords Aside. . .

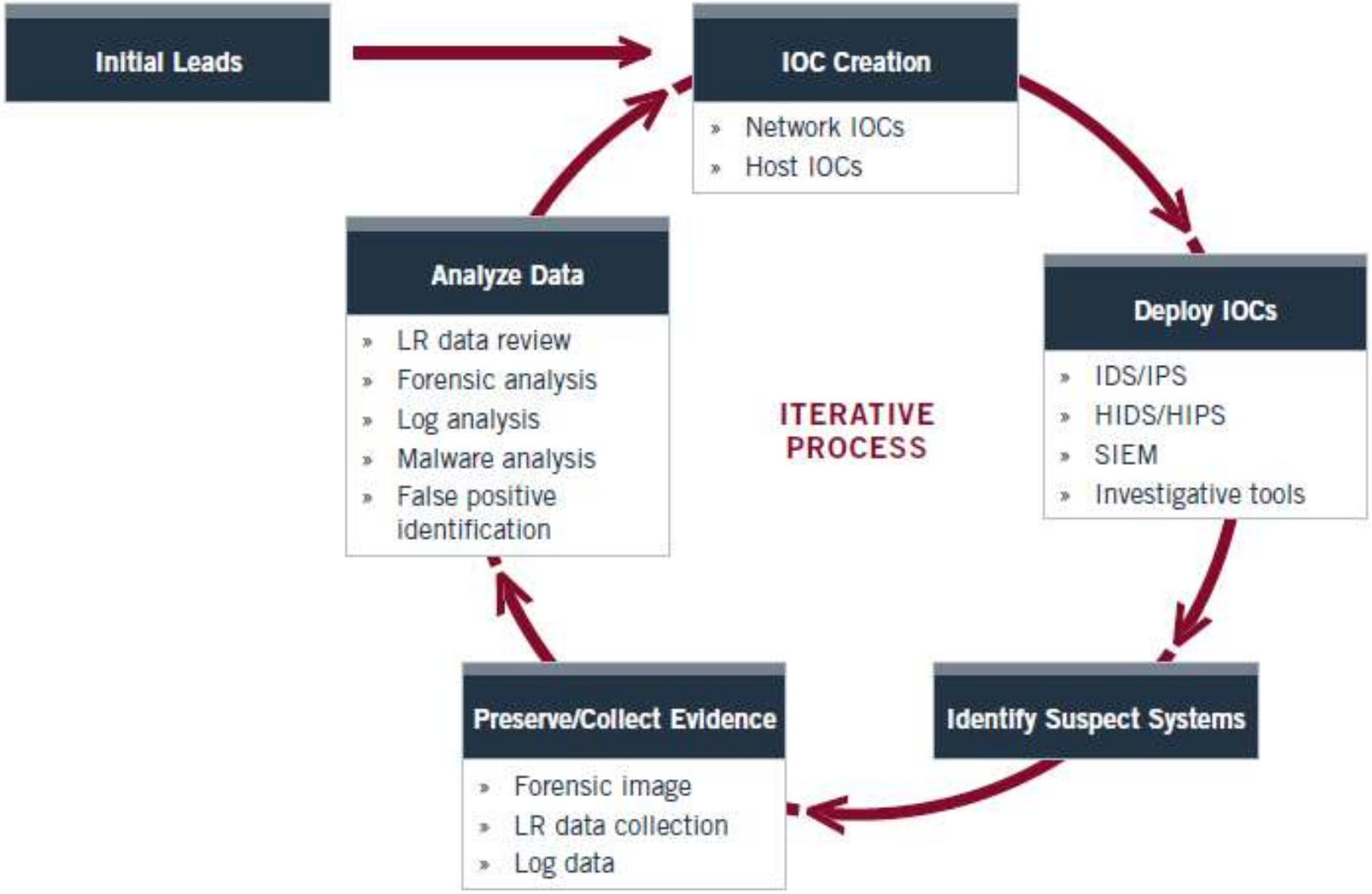
- ***Who*: Well-equipped adversaries with specific collection objectives**
- ***How*: Exploitation, persistence, data theft remain trivial**
  - "Perimeter" (Layer 8 - users) insecurity
  - Internal network insecurity
  - Unreliable preventative controls

Investigative Challenges

MANDIANT

- ***Limited knowledge*** from initial breach detection (or notification)
- ***Fully scoping*** the compromise before remediation
- Conducting ***enterprise scale*** host and network-based forensic analysis
- ***Rapid detection, response, and containment*** is the new prevention

Using IOCs in the investigative lifecycle



Scoping the incident

MANDIANT

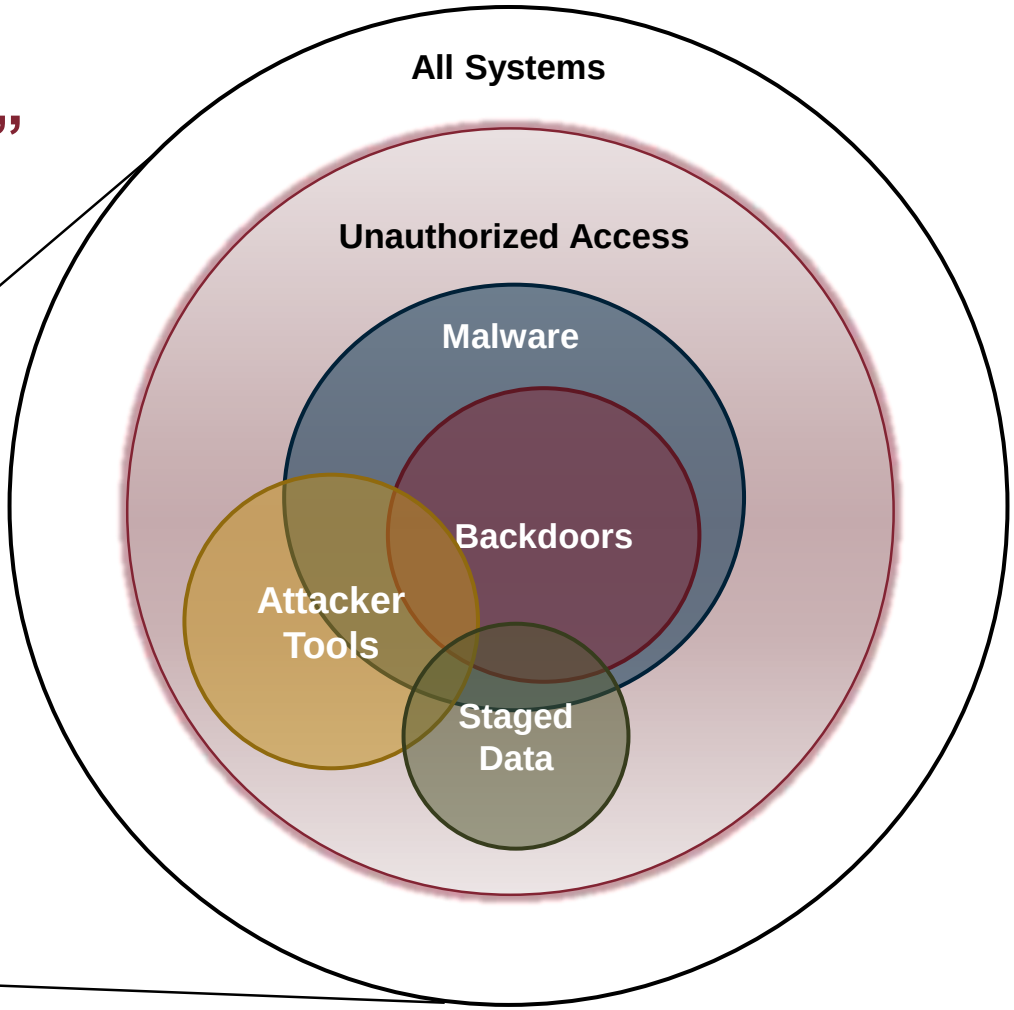
Investigative Process

Analysis

IOC Hits

- Backdoored systems
- Systems with malware
- Accessed systems
- Systems with staged data
- Compromised credentials

What is a "compromised" system?



Superior logical indicators

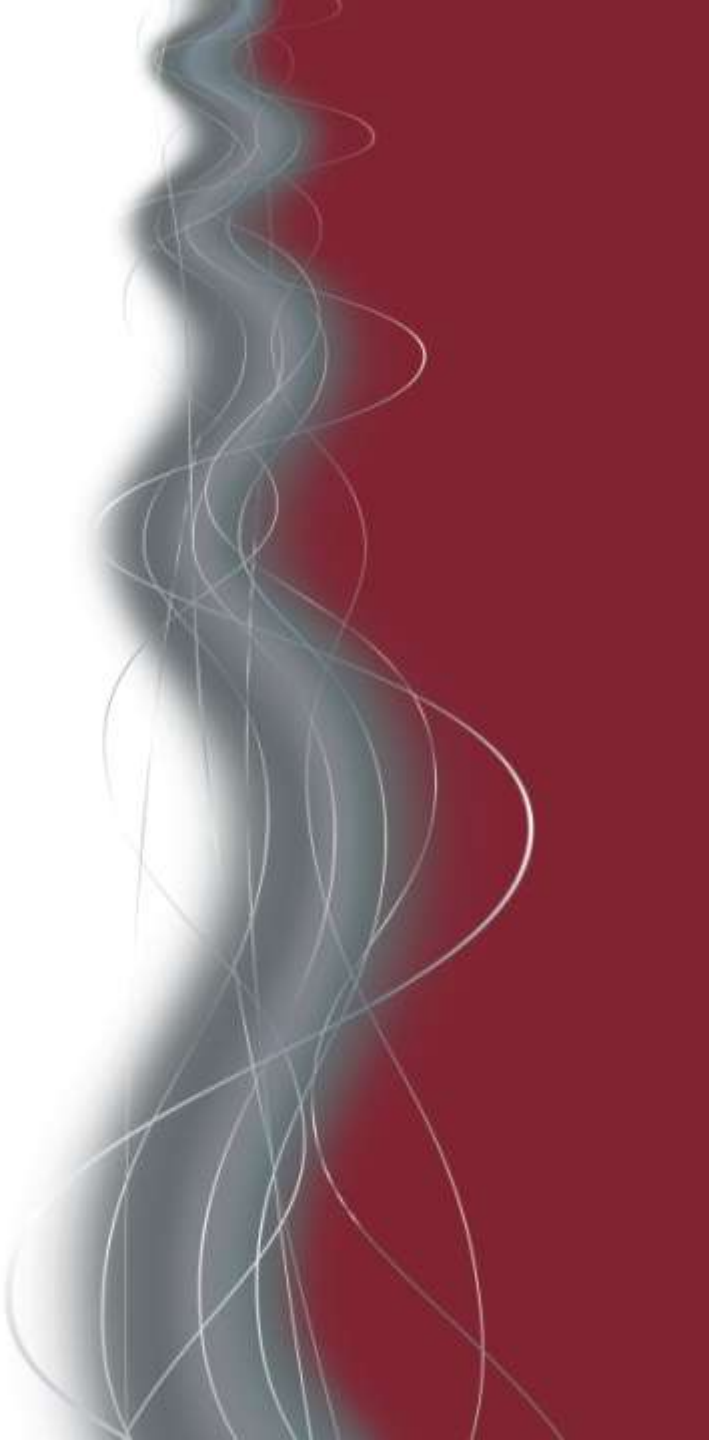
Based on real world experience

Customizable and expandable

Covers entire scope of the incident

That’s pretty cool.

But don’t you charge a lot of money for this?

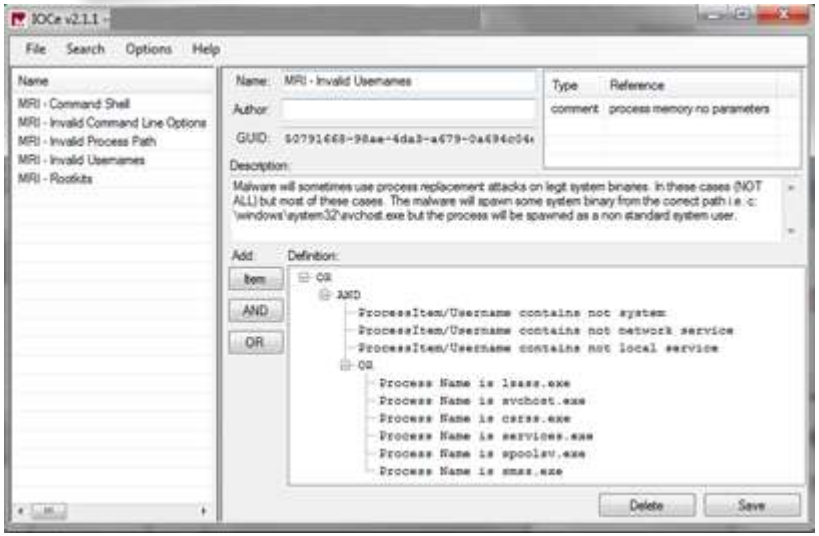


Free Tools and Resources for Use with OpenIOC

MANDIANT IOC Editor

- www.mandiant.com/products/free_software/ioce/

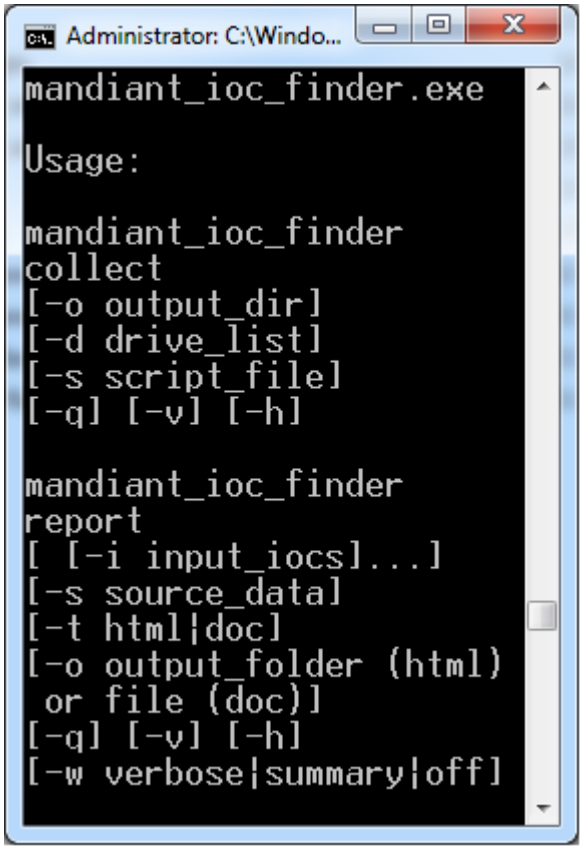
- Create an IOC from scratch
- Edit an IOC in a GUI
- Compare/Diff IOCs
- Export to XPATH queries



MANDIANT IOC Finder

- www.mandiant.com/products/free_software/iocfinder/

- Command line tool
- Collect live response
- Run IOCs against collection of data
- Output in HTML or Word
- Completes the ability to do workflow with free tools.



Just one more thing . . .

OpenIOC.org

Free resources

- Free tools
  - IOC Finder
  - IOC Editor
  - Redline
  - Memoryze
  - Audit Viewer
  - Highlighter
  - Red Curtain
  - Web Historian
  - First Response

- Resources
  - OpenIOC.org
  - M-trends Reports
  - forums.mandiant.com
  - M-unition
    - blog.mandiant.com
- Education
  - Black Hat classes
  - Custom classes
- Webinar series
  - Sign up

M-Trends 2011

Download the full report

http://www.mandiant.com

Identifying & Sharing Threat Information

with OpenIOC

Doug Wilson, Principal Consultant
doug.wilson@mandiant.com