



Identifying & Sharing Threat Information

with OpenIOC

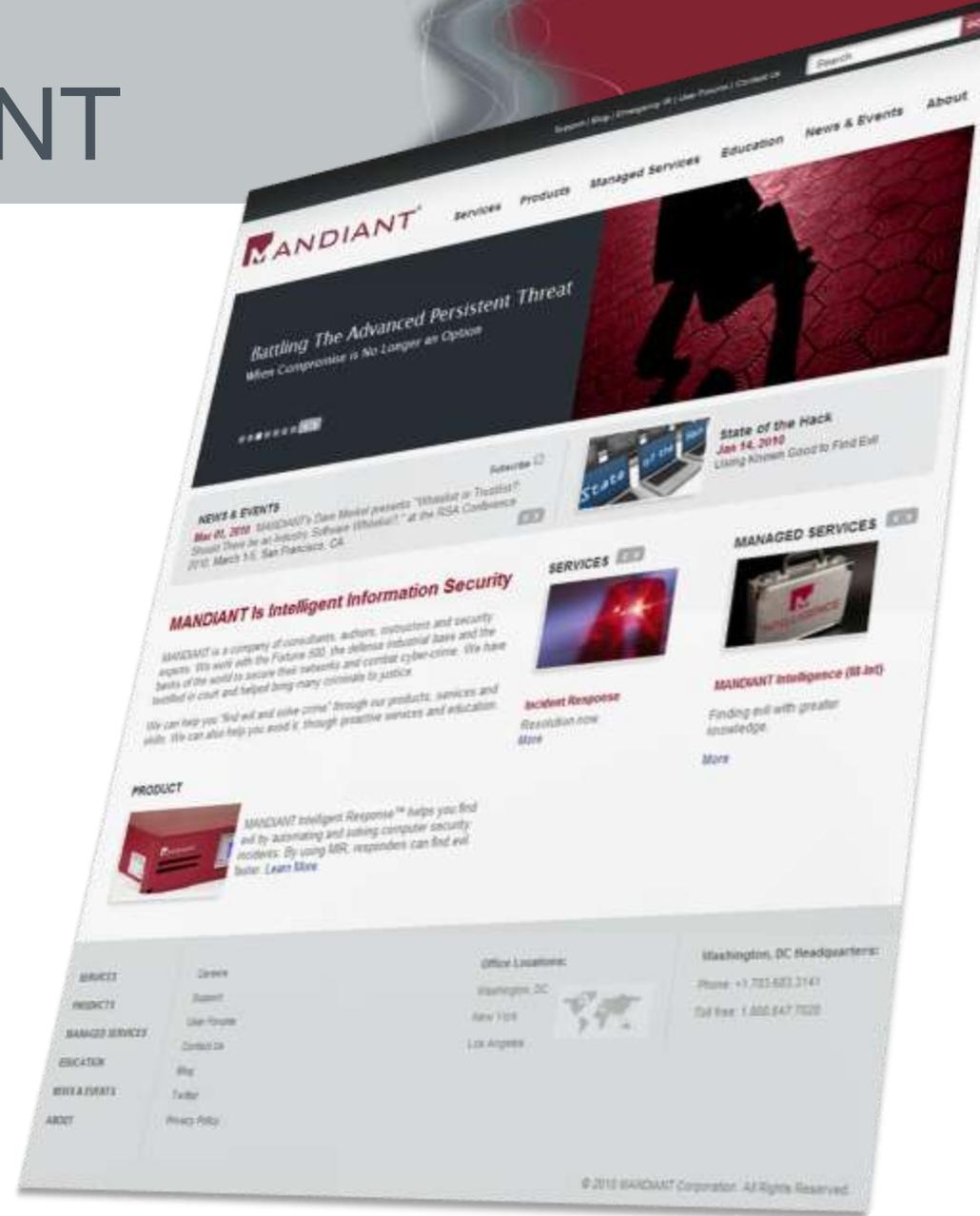
NIST IT SAC -- 11/01/11
Doug Wilson, Principal Consultant
doug.wilson@mandiant.com

**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



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

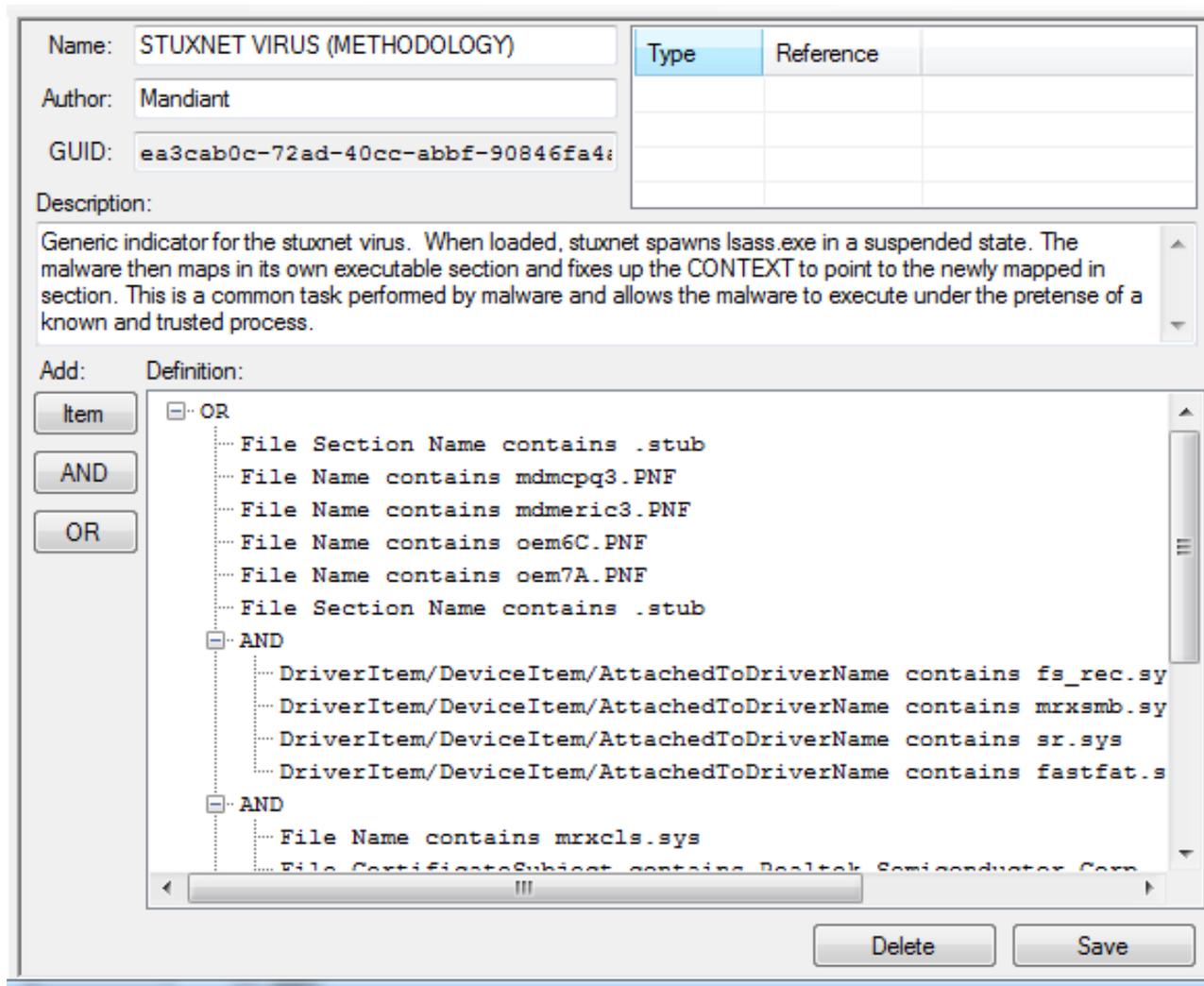
- Lists of stuff to find evil
 - Easy to create
 - Difficult to maintain
 - Terrible to share
- Lists do not provide context
 - An MD5 of what?
 - Who gave me this?
 - Where is the report?
 - Where is the intelligence??
- **Lists encourage reliance on easily mutable forensic artifacts**



OpenIOC allows this...

```
OR
-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 5611468A5A03998CB1268190E2818C63
-File MD5 is 711F4FE93EAOE8F253FA0643E273FE8B
-File MD5 is 4BFDB1ACBB32348E3D4572CD88B9A6FC
-File MD5 is CB8990122D2675990C874B4959306793
-File MD5 is 8B911B2D548FF26AE6C236D3DA2DDF2C
-File MD5 is 402366D37A54CCA71238A0FC771DEE30
-File MD5 is 98A9DF9AC85A1755CB3EBZ1d4AEA5498
-File Name is commdlq64.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.NW0902.1.org
```

...to become this



The screenshot shows a software interface for defining a malware indicator. The fields are filled with the following information:

- Name: STUXNET VIRUS (METHODOLOGY)
- Author: Mandiant
- GUID: ea3cab0c-72ad-40cc-abbf-90846fa4:

The Description field contains the text: "Generic indicator for the stuxnet virus. When loaded, stuxnet spawns lsass.exe in a suspended state. The malware then maps in its own executable section and fixes up the CONTEXT to point to the newly mapped in section. This is a common task performed by malware and allows the malware to execute under the pretense of a known and trusted process."

The Definition field is a tree view showing a logical expression:

- OR
 - File Section Name contains .stub
 - File Name contains mdmcpq3.PNF
 - File Name contains mdmeric3.PNF
 - File Name contains oem6C.PNF
 - File Name contains oem7A.PNF
 - File Section Name contains .stub
- AND
 - DriverItem/DeviceItem/AttachedToDriverName contains fs_rec.sys
 - DriverItem/DeviceItem/AttachedToDriverName contains mrxsmb.sys
 - DriverItem/DeviceItem/AttachedToDriverName contains sr.sys
 - DriverItem/DeviceItem/AttachedToDriverName contains fastfat.s
- AND
 - File Name contains mrxcls.sys
 - File CertificateSubject contains Realtek Semiconductor Corp

Buttons for "Item", "AND", "OR", "Delete", and "Save" are visible at the bottom of the interface.

OpenIOC Terms

- 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

Signatures

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

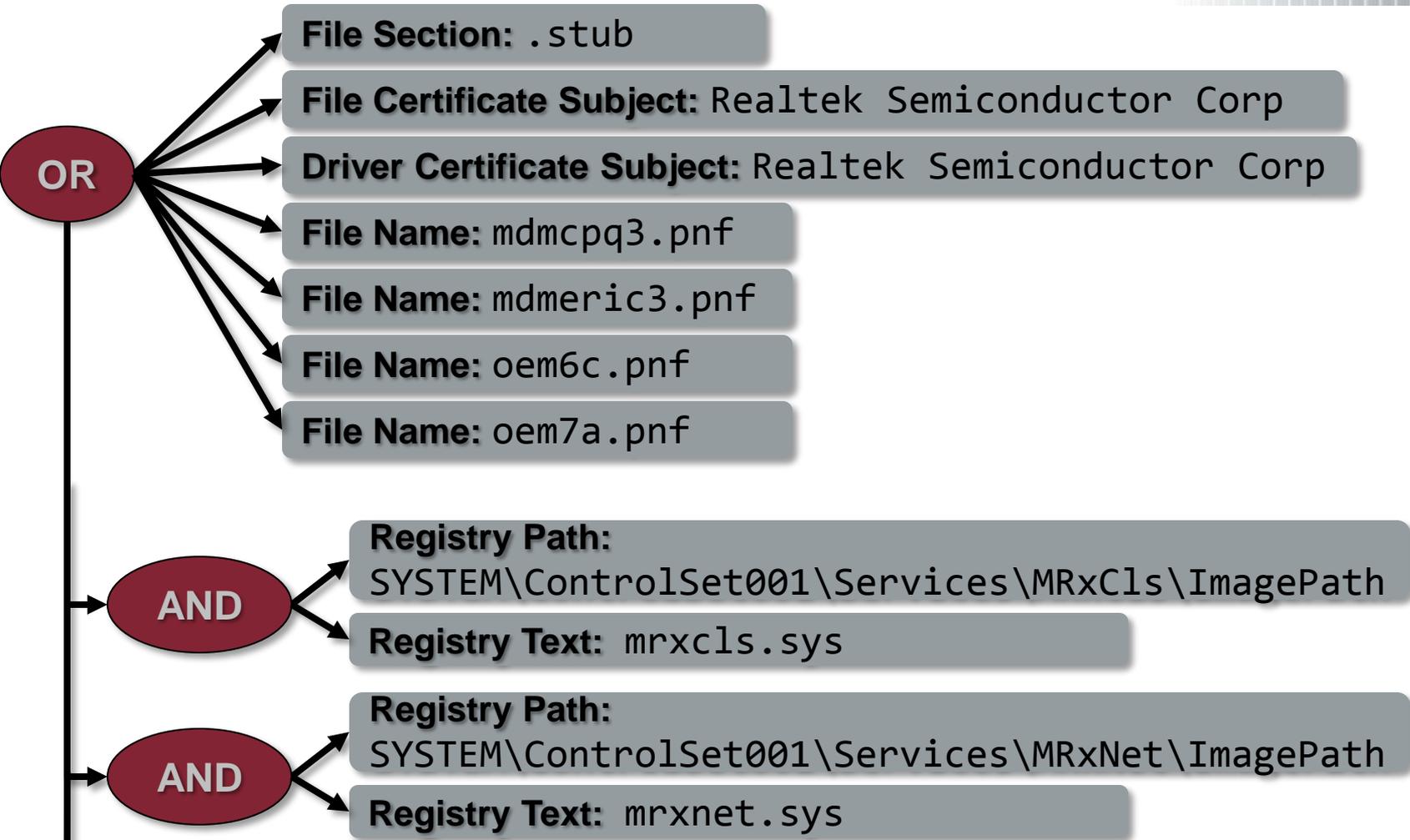
Increasing Complexity

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

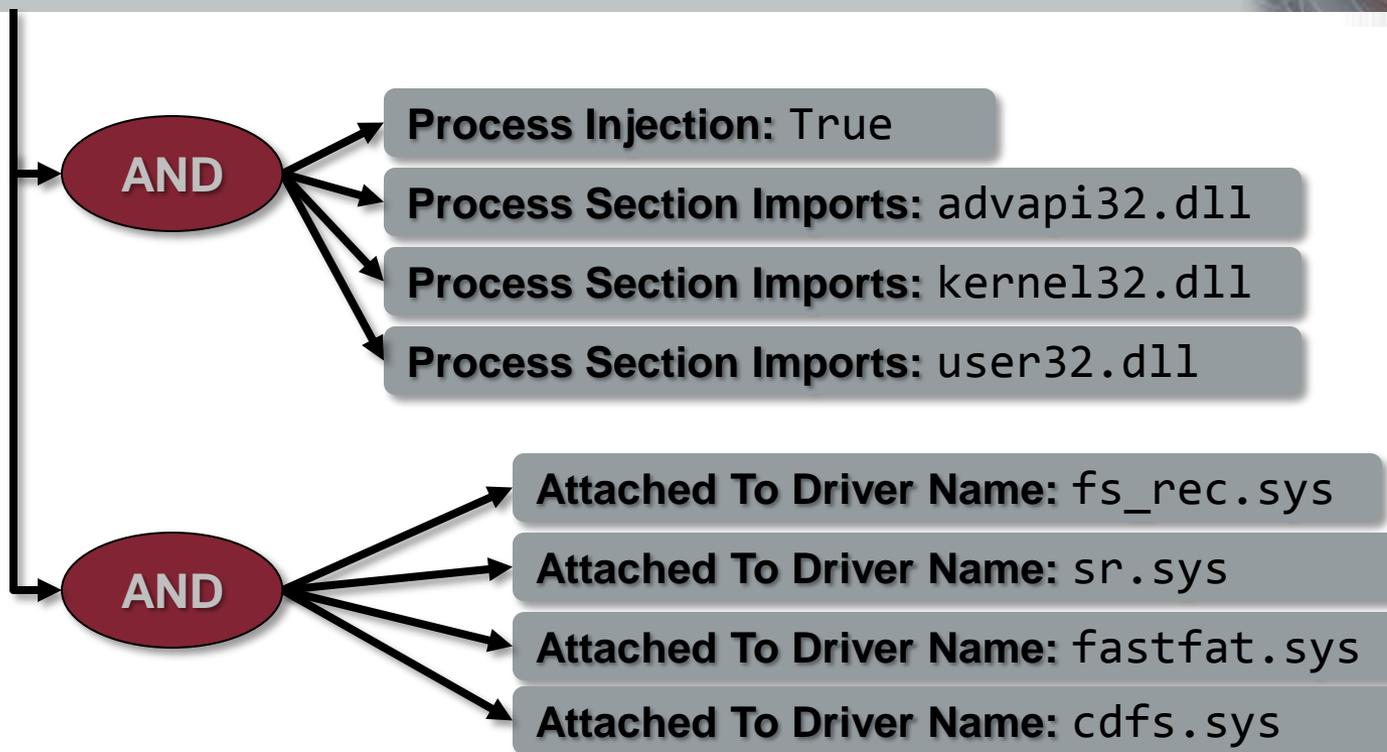
Methodology

- 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

OR

```
File MD5 is d3b07384d113edec49eaa6238ad5ff00  
File Name is hkgina.bat  
File Name is hkgina.dll  
File Name is hkgina.reg  
File MD5 is 0c5356828700473a47fd2afa446c2ef4  
File MD5 is 7e0fc8f0add8c862f1663b24e8d52649  
File Name contains outhk.dat
```

Specific

AND

```
File Size is [24000] TO [26000]  
File Compile Time is 2007-07-26T16:43:27Z
```

AND

```
File Detected Anomalies contains checksum_is_zero  
File Detected Anomalies contains overlapping_headers  
File EntryPoint Sig Name is kkrunchy  
File EntryPoint Sig Type is Packer  
File Export Function contains WlxLoggedOutSAS
```

Generic

AND

```
Registry Path contains Windows NT\CurrentVersion\WinLogon\GinaDLL  
Registry Text contains hkgina.dll
```

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\svrsvc.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
  [...] Service Name is ...
```

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
    ... 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



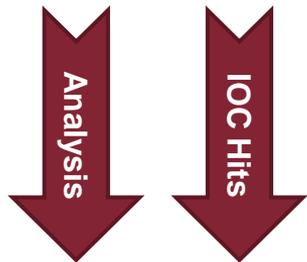
Buzzwords Aside. . .

- **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

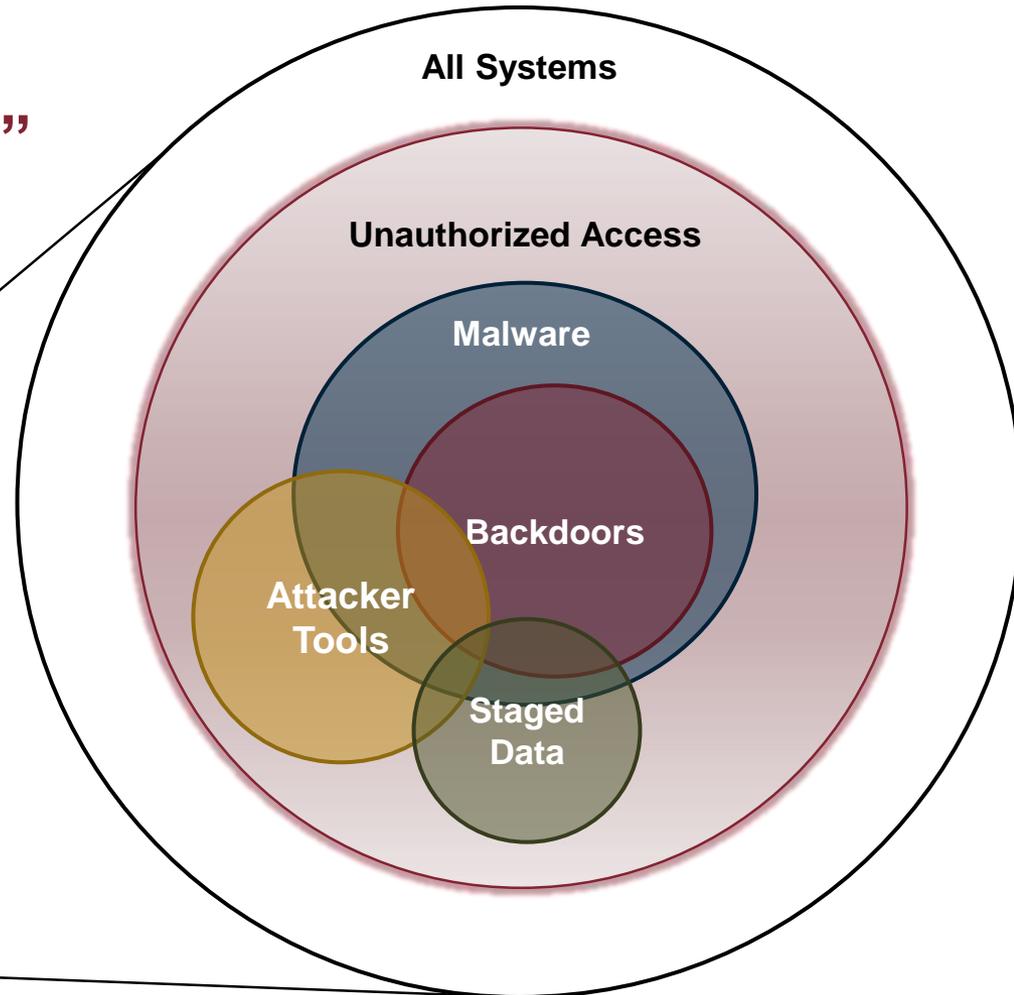
- ***Limited knowledge*** from initial breach detection (or notification)
- ***Fully scoping*** the compromise before remediation
- Conducting ***enterprise scale*** host and network-based forensic analysis
- ***Rapid detection, response, and containment*** is the new prevention

Scoping the incident

What is a “compromised” system?



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



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?

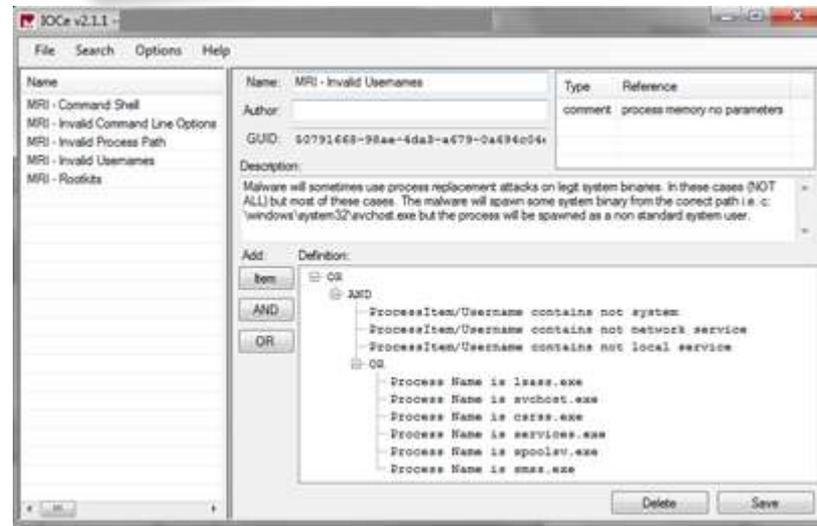


Free Tools and Resources for Use with OpenIOC

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.

A screenshot of a Windows command prompt window titled "Administrator: C:\Windo...". The window displays the usage information for the "mandiant_ioc_finder.exe" tool. The text is as follows:

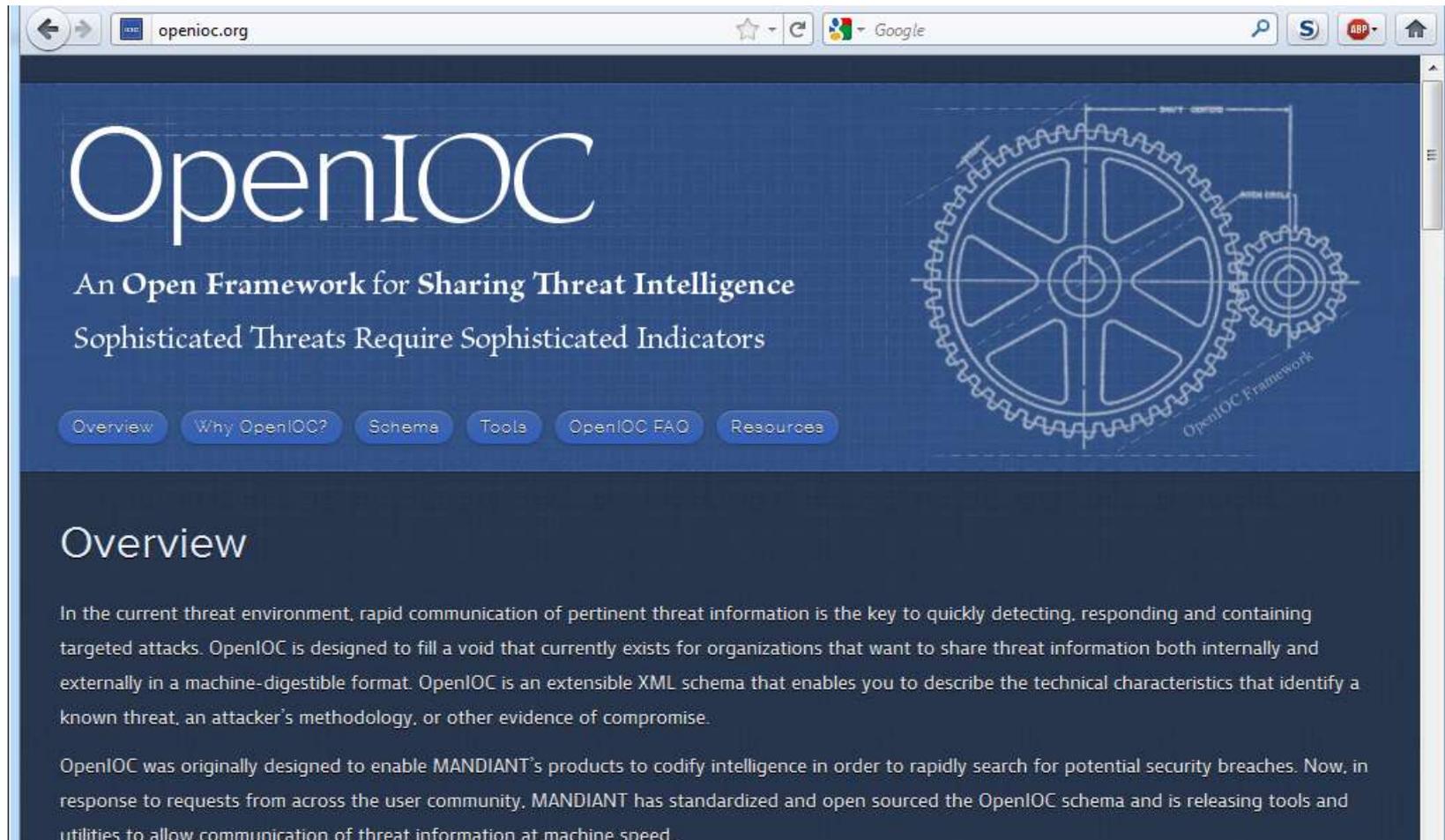
```
mandiant_ioc_finder.exe

Usage:

mandiant_ioc_finder
collect
[-o output_dir]
[-d drive_list]
[-s script_file]
[-q] [-v] [-h]

mandiant_ioc_finder
report
[ [-i input_iocs]...]
[-s source_data]
[-t html|doc]
[-o output_folder (html)
or file (doc)]
[-q] [-v] [-h]
[-w verbose|summary|off]
```

Just one more thing . . .



The screenshot shows a web browser window with the address bar displaying "openioc.org". The page features a dark blue background with the "OpenIOC" logo in large white letters. Below the logo, the text reads "An Open Framework for Sharing Threat Intelligence" and "Sophisticated Threats Require Sophisticated Indicators". A navigation menu contains buttons for "Overview", "Why OpenIOC?", "Schema", "Tools", "OpenIOC FAQ", and "Resources". On the right side, there is a technical diagram of interlocking gears with labels "SHIFT CENTER" and "OPEN ENDS". The "Overview" section is visible at the bottom, containing two paragraphs of text.

OpenIOC

An Open Framework for Sharing Threat Intelligence
Sophisticated Threats Require Sophisticated Indicators

[Overview](#) [Why OpenIOC?](#) [Schema](#) [Tools](#) [OpenIOC FAQ](#) [Resources](#)

Overview

In the current threat environment, rapid communication of pertinent threat information is the key to quickly detecting, responding and containing targeted attacks. OpenIOC is designed to fill a void that currently exists for organizations that want to share threat information both internally and externally in a machine-digestible format. OpenIOC is an extensible XML schema that enables you to describe the technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise.

OpenIOC was originally designed to enable MANDIANT's products to codify intelligence in order to rapidly search for potential security breaches. Now, in response to requests from across the user community, MANDIANT has standardized and open sourced the OpenIOC schema and is releasing tools and utilities to allow communication of threat information at machine speed.

- 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-union
 - 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