MANDIANT®

Jamie Butler | Director, Research and Development

Jason Shiffer | Architect

Sleuth Kit and Other Open Source Technologies

FASTER RESPONSE

MANDIANT®

Agenda

- Accelerating Incident Response with Open Source
  - Sleuth Kit
  - AFF
  - Lucene
  - Open Protocols and Languages
- Considerations when using Open Source
- Current and Future Initiatives
  - OpenIOC
  - Google Data API
  - Free Tools
- Questions?

Accelerating IR: Sleuth Kit

- Abstraction Layer
  - Mount live volume or image with Sleuth Kit
  - Enumerate files with walking functions and callbacks
  - “Open” individual files for reading and pass opaque “handles”
  - Use reading functions for hashing etc.
  - User can simply call into the engine that is Sleuth Kit
  - New versions of Sleuth Kit can be swapped in and out

Accelerating IR: Sleuth Kit

- Use Cases
  - Supports multiple file system types (FAT, NTFS, EXT2/3, HFS, UFS, etc.)
  - Difference based analysis (API and RAW)
    - File API vs File enumeration with Sleuth Kit
    - Registry API vs Registry enumeration with TSK
    - Independent verification of any file analysis such as hashing
  - Access locked files
    - Paging files
    - Web history files
    - Registry Hive files
  - Unique data items
    - Not available through operating system API
    - Filename date times
    - Deleted files

Accelerating IR: AFF

- Use Case
  - Data+Metadata Container
    - Metadata
    - Compression
    - Integrity Checking
    - Open Format
  - Streaming
    - Memory/Disk usage trade off
    - Hashes become Etags
    - TOC

Accelerating IR: Lucene

- Use Case
  - Full Text Search
    - Handles Tens of Thousands of Documents well
    - Expressive Search Syntax
  - Scoped Search (Signature Matching)
    - Not Exact Match
    - Full Text Search on subsets of Data
    - Starts to fall down when Documents grow more numerous (500k or more)

Open Protocols and Languages

- XML and Xpath
  - Lots of Tools and Resources available
  - Extensible
  - Large files cause many tools to fail
- Python
  - Clean simple syntax
  - Requires careful use for server processes
  - Threads (but not really)
- HTTP/S and OpenSSL
  - Well understood security and performance surfaces
  - Common tools work ubiquitously
  - Difficulty at the edges (HTTP/1.1)

Considerations using Open Source

- Attackers’ omniscience
- Private needs vs. community needs
- Rapid change
  - Interfaces
  - Functionality
- Licensing for commercial use
- Communication

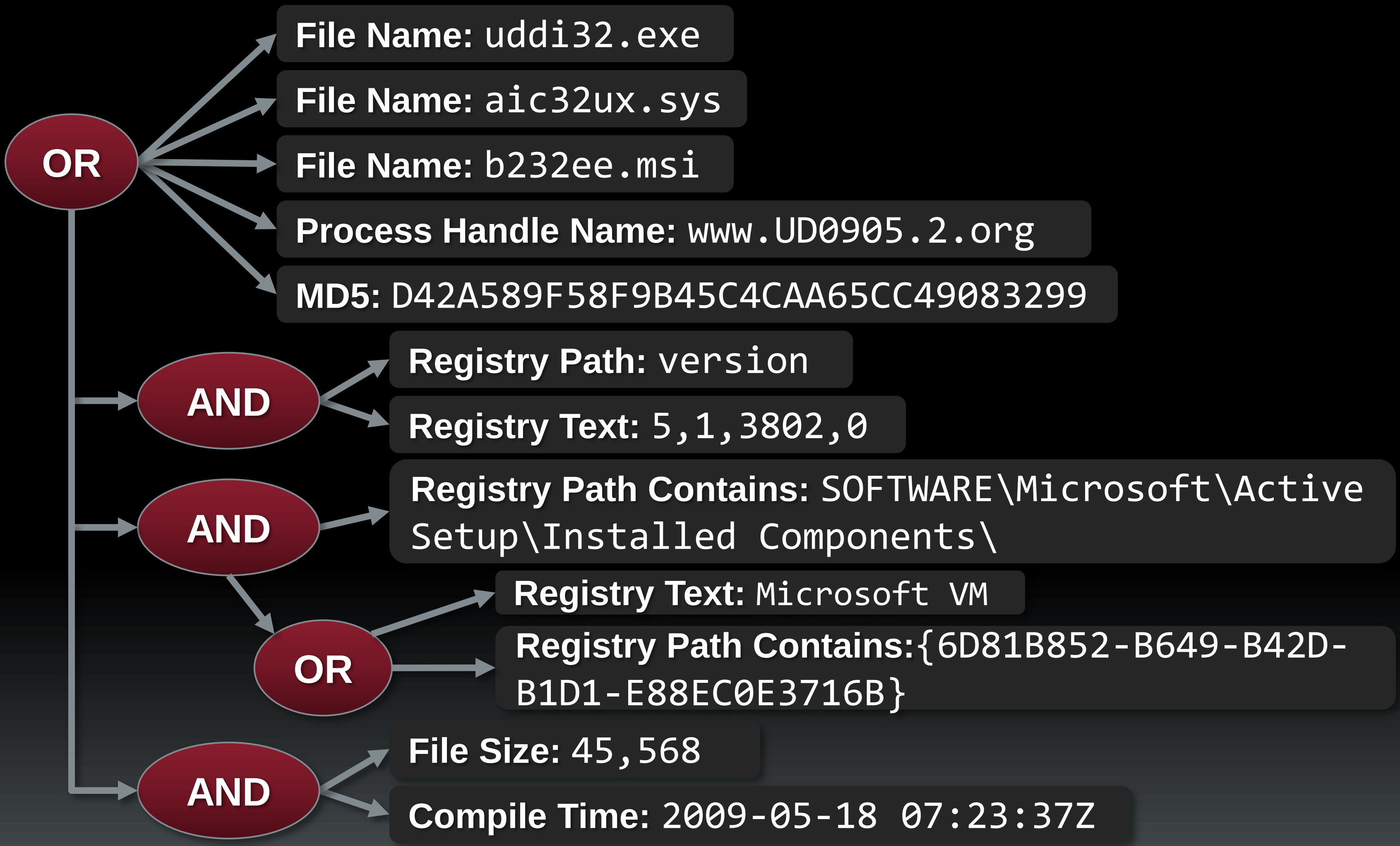
Current and Future Initiatives

- OpenIOC and IOCe (editor)
- Google Data API
- Free Tools

Current Initiatives: OpenIOC

- A format to organize Indicators
- Turns your data into intelligence
- *Designed for data sharing*
- Intentionally extendable
- Technology agnostic
  - Doesn’t require any product
  - Easily converts to needed formats
    - We have some pre-built
    - It is just XML after all

Indicator of Compromise (IOC)



File Name: uddi32.exe

File Name: aic32ux.sys

File Name: b232ee.msi

Process Handle Name: www.UD0905.2.org

MD5: D42A589F58F9B45C4CAA65CC49083299

Registry Path: version

Registry Text: 5,1,3802,0

Registry Path Contains: SOFTWARE\Microsoft\Active Setup\Installed Components\

Registry Text: Microsoft VM

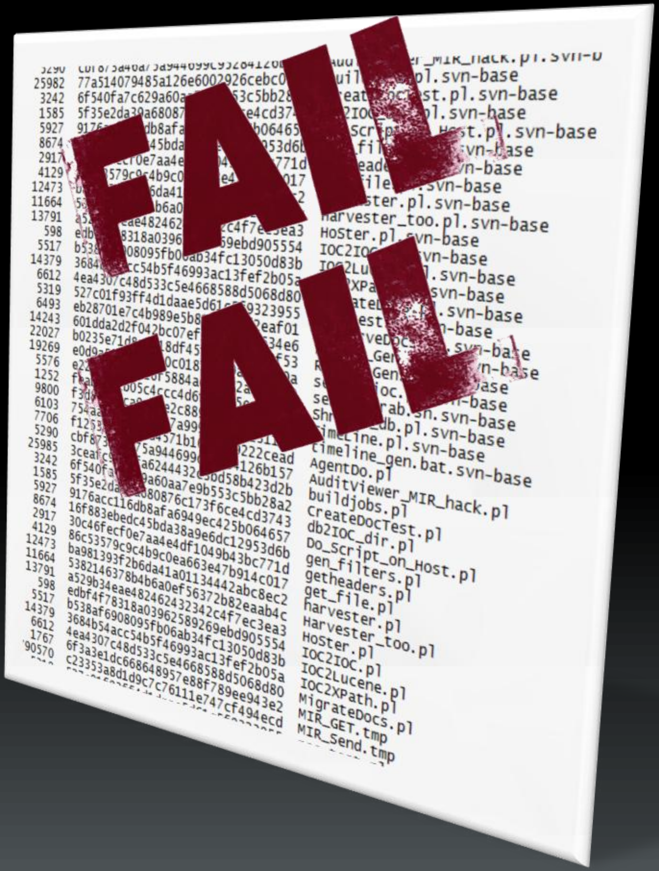
Registry Path Contains:{6D81B852-B649-B42D-B1D1-E88EC0E3716B}

File Size: 45,568

Compile Time: 2009-05-18 07:23:37Z

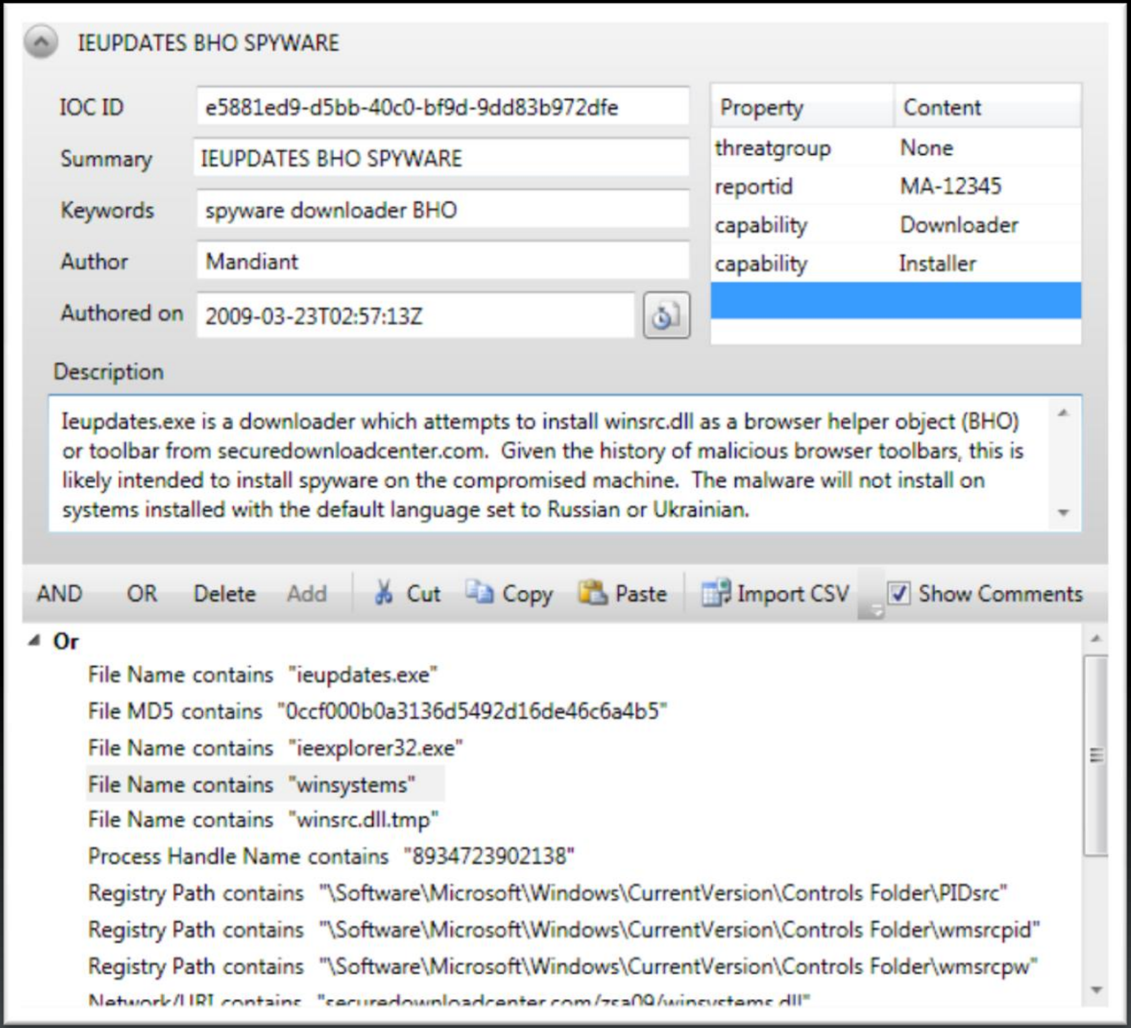
Current Initiatives: Before OpenIOC

- 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??
- Proprietary languages
- Complicated databases
- Black box definitions



Current Initiatives: OpenIOC

- The Why
- The What



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

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

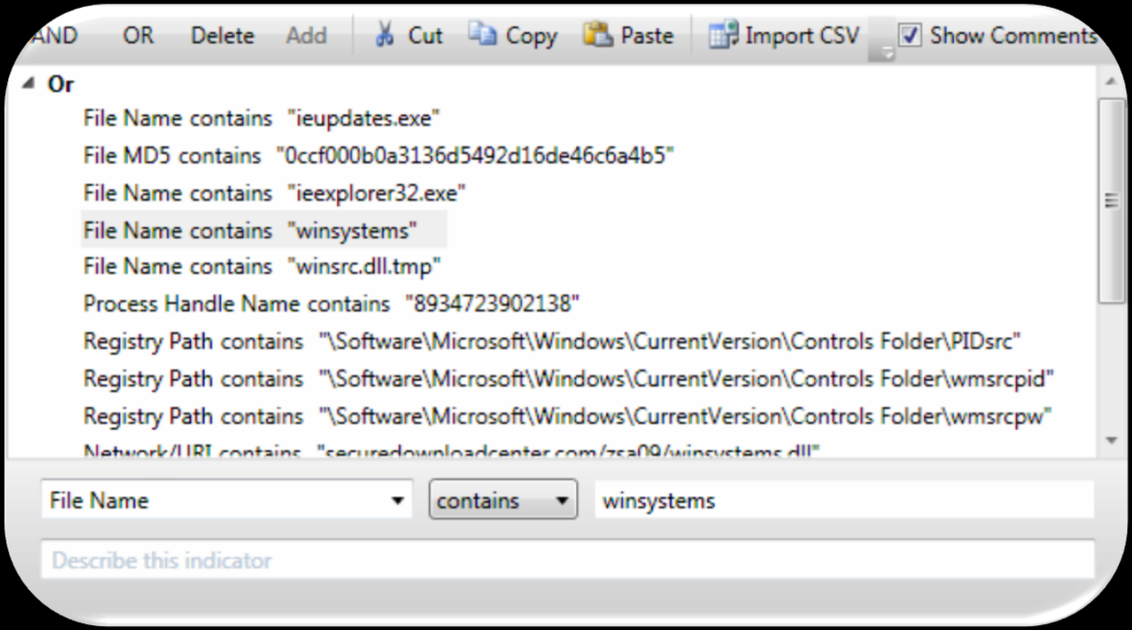
Description

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.

```
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/zsa09/winsystems.dll"
```

Stores what we are looking for

- Content
  - Keyword
- Context
  - Keyword Type
- Construct
  - Logic



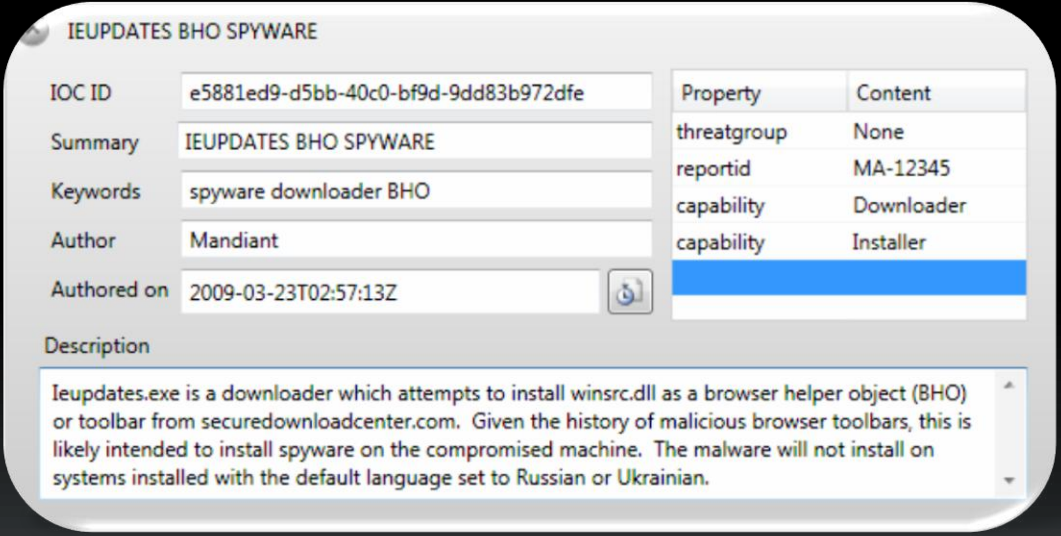
```
Or
    File Name contains  "ieupdates.exe"
    File MD5 contains  "0ccf000b0a3136d5492d16de46c6a4b5"
    File Name contains  "ieexplorer32.exe"
    File Name contains  "winsystems"
    File Name contains  "winsrc.dll.tmp"
    Process Handle Name contains  "8934723902138"
    Registry Path contains  "\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/zsa09/winsystems.dll"
```

File Name ▾ | contains ▾ | winsystems

Describe this indicator

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
Summary	IEUPDATES BHO SPYWARE
Keywords	spyware downloader BHO
Author	Mandiant
Authored on	2009-03-23T02:57:13Z

Property	Content
threatgroup	None
reportid	MA-12345
capability	Downloader
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.

Initiatives: OpenIOC 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

Initiatives: OpenIOC 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

Current and Future Initiatives

- Google Data API
  - Becoming the baseline REST protocol
  - Extensible
  - Open Client Support libraries

Current Initiatives: Free Tools

- Memoryze and Audit Viewer
  - Memory analysis for Windows
  - Supports 2000, XP, 2003, Vista, 2003 64-bit
  - *Windows 7 64-bit support in Q3 2010*
  - UI is open source and written in Python
  - http://blog.mandiant.com/archives/994

Current Initiatives: Free Tools

- Web Historian 2.0
  - Due for release next week at FIRST
  - Supports Internet Explorer, Firefox, and Chrome
  - Uses Sleuth Kit to access locked Web browser files
  - Backend data is stored in SQLite
  - Good sort and filtering capabilities

Q&A

- Email:
  - james.butler@mandiant.com
  - jason.shiffer@mandiant.com
- Blog:
  - http://blog.mandiant.com