

# Utilization of IOC, IOAF and SigBase

---

*JK Kim*

*forensic-proof.com*

*proneer(at)gmail.com*

*Security is a people problem...*



# Utilization of IOC, IOAF



## IOC – Indicator Of Compromise

### ▪ 침해지표 – IOC

- 운영체제 혹은 네트워크의 침해를 확인할 수 있는 포렌식 아티팩트
- **일반적인 침해 지표**
  - ✓ IP 주소
  - ✓ 악성코드의 MD5 해시
  - ✓ C2 URL
- 컴퓨터 포렌식, 사고 대응에서 주로 사용됨
- IDS와 같은 보안 장비/솔루션에서 침해를 확인하는 용도로 사용



## 침해지표 관련 표준 (1)

### ▪ IODEF (The Incident Object Description Exchange Format), *RFC 5070*

- 컴퓨터 보안사고 대응팀(CSIRTs) 간의 사건 정보 교환용 XML 포맷
- 사건의 세부 내용에 대한 XML 스키마 정의
- [Code Red Worm](#) 예제

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This example demonstrates a report for a very old worm (Code Red) -->
<IODEF-Document version="1.00" lang="en" xmlns="urn:ietf:params:xml:ns:iodef-1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:ietf:params:xml:ns:iodef-1.0">
<Incident purpose="reporting">
  <IncidentID name="csirt.example.com">189493</IncidentID>
  <ReportTime>2001-09-13T23:19:24+00:00</ReportTime>
  <Description>Host sending out Code Red probes</Description>
  <!-- An administrative privilege was attempted, but failed -->
  <Assessment>
    <Impact completion="failed" type="admin"/>
  </Assessment>
  <Contact role="creator" type="organization">
```



## 침해지표 관련 표준 (2)

### ▪ Cyber Observable eXpression (CybOX)

- 운영 도메인에서 확인할 수 있는 상태 속성, 이벤트 통신, 명세, 특성에 관한 표준 스키마
- 이벤트 관리/로깅, 악성코드 특성, 침입 탐지, 사고 대응/관리, 공격 패턴 등
- 오브젝트 별 정의 스키마 – <http://cybox.mitre.org/language/version2.0/#samples>
- [아티팩트 별 XML 스키마 예제](#)
- **변환 도구 지원** – <https://github.com/CybOXProject/Tools/tree/master/scripts>
  - ✓ cybox\_to\_html
  - ✓ cybox\_to\_oval (Open Vulnerability and Assessment Language)
  - ✓ email\_to\_cybox
  - ✓ openioc\_to\_cybox



## 침해지표 관련 표준 (3)

### ▪ Open IOC by Mandiant

- XML 기반의 위협 정보(Threat Intelligence) 표현 프레임워크
- 논리적인 그룹 형식으로 포렌식 아티팩트를 정리
- 실제 경험을 바탕으로 구성, 유연한 확장성
- [Stuxnet](#) 예제

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="ea3cab0c-72ad-40cc-abbf-90846fa4afec" last-modified="2011-11-04T19:35:05" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>STUXNET VIRUS (METHODOLOGY)</short_description>
  <description>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.</description>
  <keywords>methodology</keywords>
  <authored_by>Mandiant</authored_by>
  <authored_date>0001-01-01T00:00:00</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="73bc8d65-826b-48d2-b4a8-48918e29e323">
      <IndicatorItem id="b9ef2559-cc59-4463-81d9-52800545e16e" condition="contains">
```



## OpenIOC (0)

- Open IOC dot COM

The image shows a screenshot of the OpenIOC website. The top section features the 'OpenIOC' logo in a large, white, serif font on a dark blue background. Below the logo is the tagline 'An Open Framework for Sharing Threat Intelligence' and the subtitle 'Sophisticated Threats Require Sophisticated Indicators'. A navigation bar contains five buttons: 'Overview', 'Why OpenIOC?', 'Schema', 'Tools', and 'Resources'. To the right is a technical diagram of interlocking gears with labels 'SHUT CONTROL' and 'OPEN FRAMEWORK'. Below this is an 'Overview' section with 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.



## OpenIOC (1)

### ▪ Open IOC Terms – [Full List Indicator Terms](#)

- 500여 개 특성
- 필요 시 추가 가능

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





## OpenIOC (2)

### ▪ Open IOC Functionality

#### • 시그니처

- ✓ 파일 → MD5, 컴파일 시간, 파일 크기, 파일 이름, 경로 등
- ✓ 레지스트리 → 유일한 항목 (Key, Value, Data), 지속성 여부
- ✓ 메모리 → 프로세스명, 서비스명, 핸들, 뮤텍스 등

#### • 늘어나는 복잡성

- ✓ 정확도를 높이기 위해 논리적(OR, AND) 조합
- ✓ 악성코드 그룹의 공통적 특성 탐지, 비정상적 데이터 수집 시 사용

#### • 방법

- ✓ 악성코드가 아닌 악성코드 행위에 초점
- ✓ 침해나 익스플로잇을 넘어 공격자의 행동을 탐지
- ✓ 반복된 행동, 이름 변환, 위치 변경 등을 탐지



## OpenIOC (3)

- IOC 생성과 편집 → IOCe

The screenshot shows the IOCe 2.2.0 application window. The title bar reads "IOCe 2.2.0 - H:\WINSIGHTW[130427] Utilization of IOCs in Korea and SigBase Prototype#OpenIOC\_samples". The menu bar includes "File", "Search", "Tools", and "Help".

The left sidebar lists several IOCs, with "STUXNET VIRUS" selected. The main area displays the configuration for this IOC:

- Name:** STUXNET VIRUS (METHODOLOGY)
- Author:** Mandiant
- GUID:** ea3cab0c-72ad-40cc-abbf-90846fa4afec
- Created:** 0001-01-01 00:00:00Z
- Modified:** 2011-11-04 19:35:05Z
- Description:** 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.

Below the description, there is a section for "Add: AND OR Item" with a tree view of rules:

- OR**
  - 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**
  - Driver Attached To Driver Name contains fs\_rec.sys
  - Driver Attached To Driver Name contains mrxsmb.sys
  - Driver Attached To Driver Name contains sr.sys
  - Driver Attached To Driver Name contains fastfat.sys
- AND**
  - File Name contains mrxcls.sys
  - File Certificate Subject contains Realtek Semiconductor Corp

At the bottom of the window, it shows "Loaded IOCs: 7 | Unsaved IOCs: 1" and a "Save" button.



## OpenIOC (4)

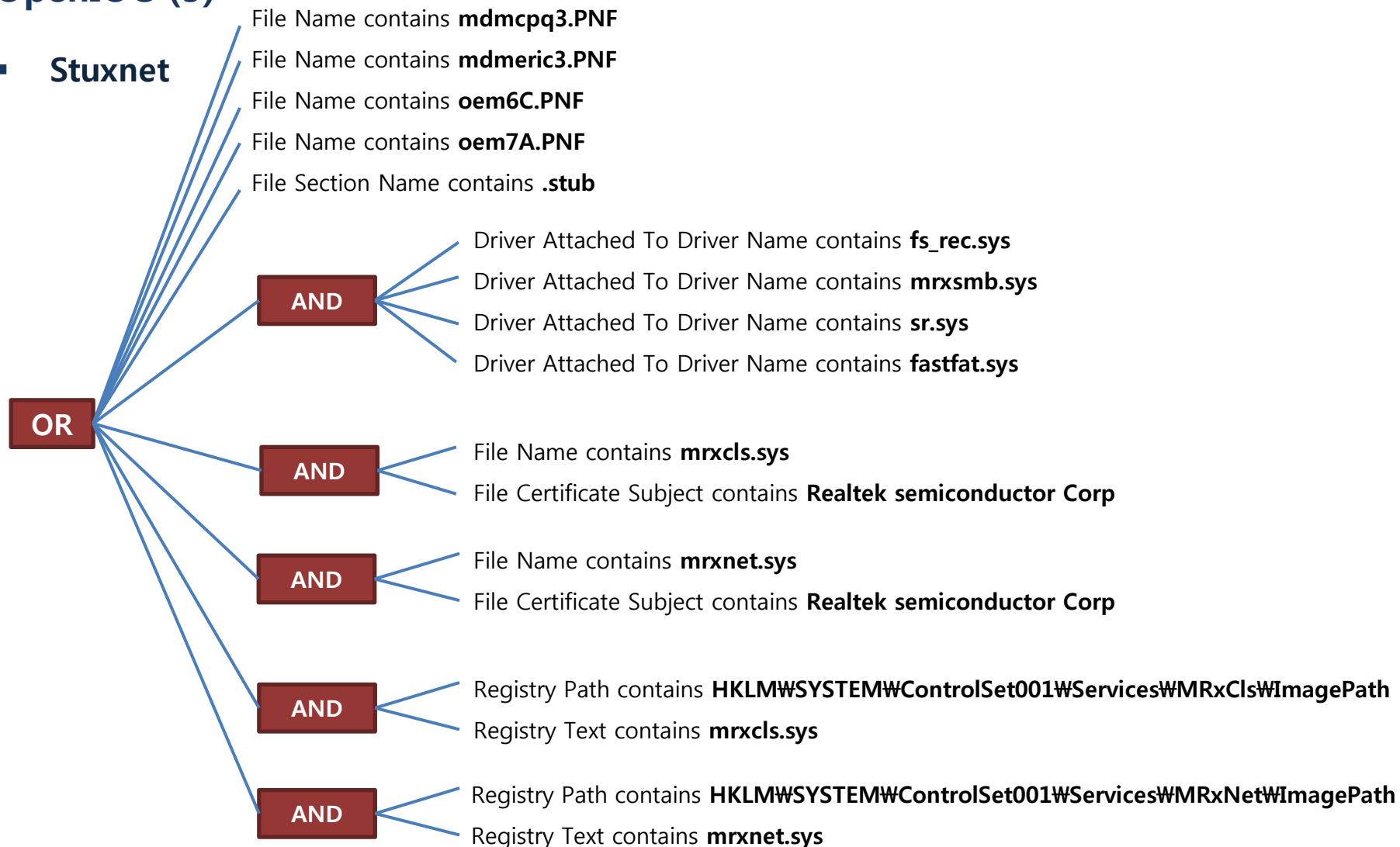
- [Stuxnet 예제](#)

```
OR
  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
    Driver Attached To Driver Name contains fs_rec.sys
    Driver Attached To Driver Name contains mrxsmb.sys
    Driver Attached To Driver Name contains sr.sys
    Driver Attached To Driver Name contains fastfat.sys
  AND
    File Name contains mrxcls.sys
    File Certificate Subject contains Realtek Semiconductor Corp
  AND
    File Name contains mrxnet.sys
    File Certificate Subject contains Realtek Semiconductor Corp
  AND
    Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\ImagePath
    Registry Text contains mrxcls.sys
  AND
    Registry Path contains HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\ImagePath
    Registry Text contains mrxnet.sys
```



## OpenIOC (5)

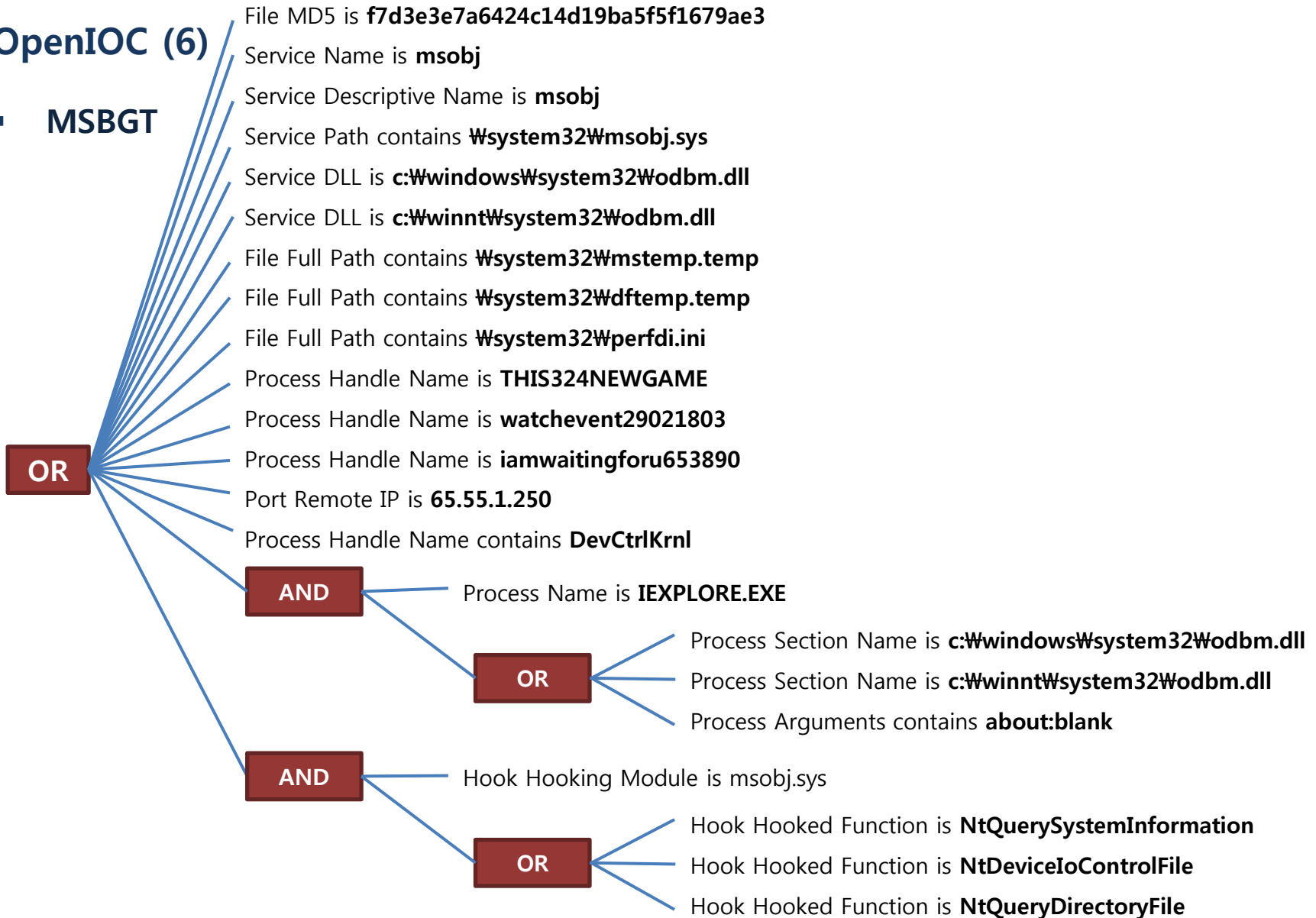
### Stuxnet





## OpenIOC (6)

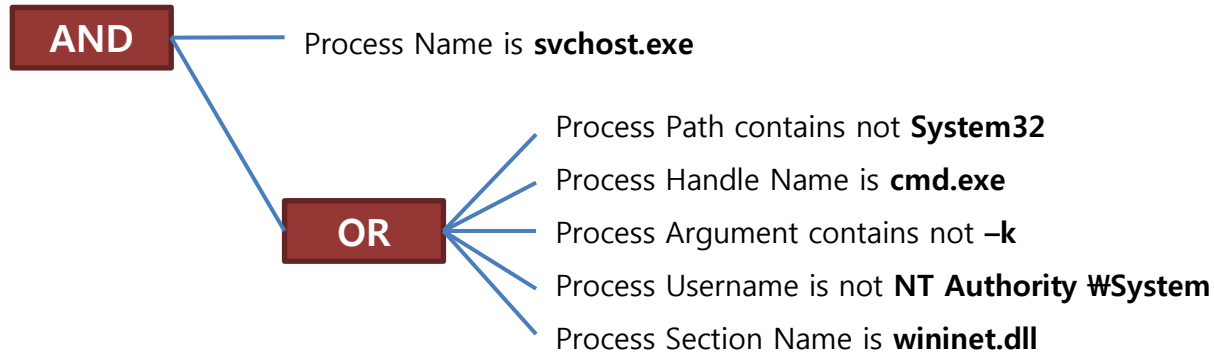
### ▪ MSBGT





## OpenIOC (7)

- Malicious **svchost.exe**







## OpenIOC (9)

### ▪ 조사에서 IOC 활용하기

- 특정 조직 내의 추가적인 침해 시스템 탐지
- 유사한 유형의 침해 흔적을 다른 조직에 적용할 때 → 변형을 통해 IOC 강화





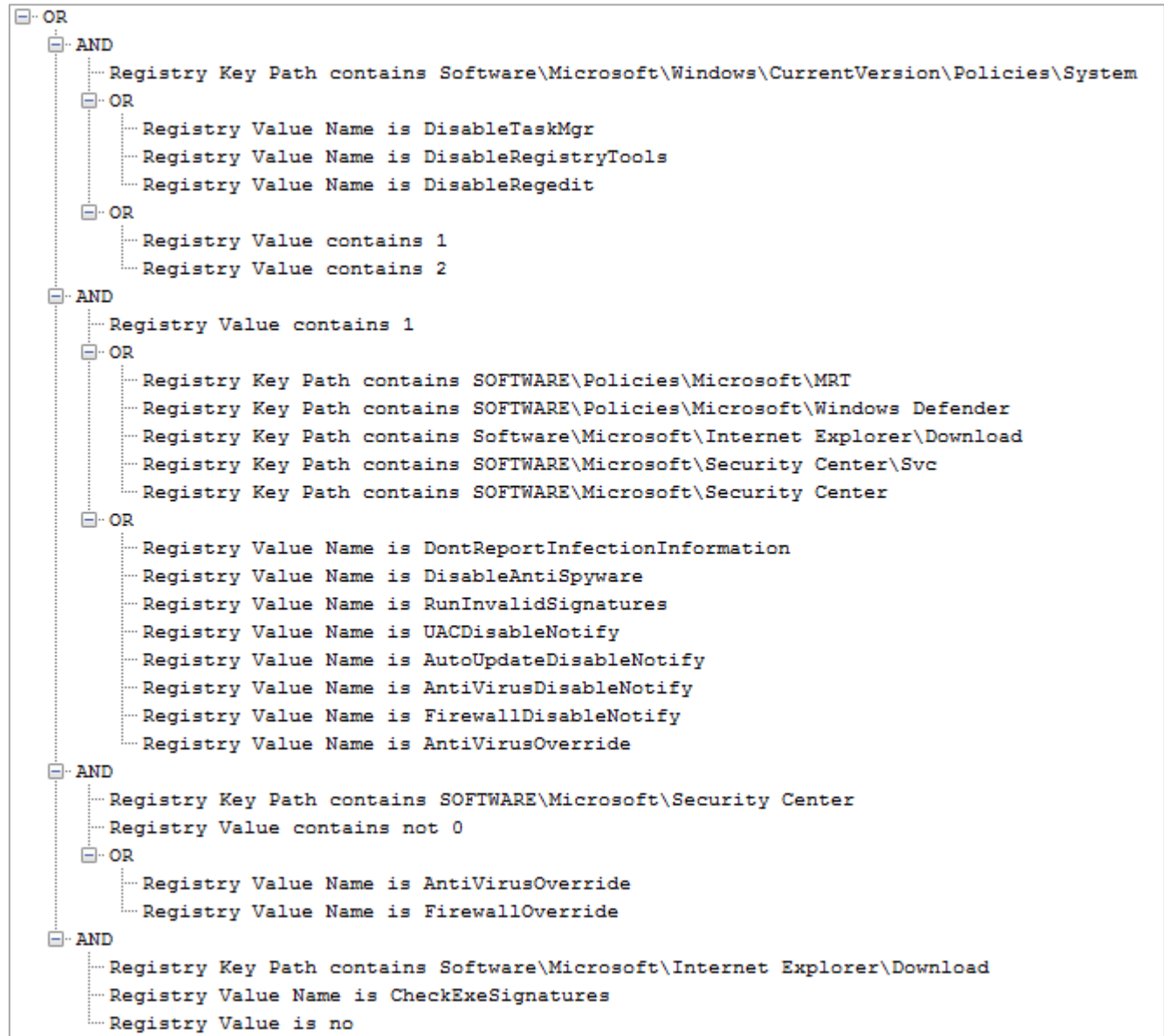
## OpenIOC Testing

- **Sysadmin(TaskManager, Regiedit) disabled**
  - **MD5:** [51ad6e2129bed025a73d6b22965df5ca](#)
  - **SHA256:** 2e700139283bbff3f45ac37453198498da0064eea5bdf6f5a934477738629d4a
  - **AhnLab-V3:** Spyware/Win32.Zbot
  - **Avast:** Win32:Downloader-OIB [Trj]
  - **BitDefender:** Trojan.Generic.KDV.620000
  - **Kaspersky:** Trojan-Ransom.Win32.Gimemo.rul
  - **McAfee:** PWS-Zbot.gen.zg
  - **Microsoft:** DDoS:Win32/Abot.A



## OpenIOC Testing

- IOC Rules





## OpenIOC Testing

- 테스트 방법

1. Windows XP VM에서 악성코드 실행 → 재부팅 후 explorer.exe 실행이 되지 않음
2. VMDK 파일을 Z:₩ 볼륨에 마운트
3. IOC Finder를 이용해 Z:₩ 볼륨의 정보 수집
4. IOC Finder를 이용해 수집된 정보에서 해당 악성코드 IOC 흔적 검색



## OpenIOC Testing

- `mandiant_ioc_finder.exe`

The screenshot shows a Windows command prompt window titled "관리자: C:\Windows\system32\cmd.exe". The prompt is at "C:\Temp\Mandiant IOC Finder\x64>". The command "mandiant\_ioc\_finder.exe" has been entered. The output shows the usage instructions for the tool, which are highlighted with a red box in the original image:

```
Usage :  
mandiant_ioc_finder collect [-o output_dir] [[-d drive]...] [-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]
```



## OpenIOC Testing

- `mandiant_ioc_finder.exe collect -o c:\Wtemp -d z:\W`

```
관리자: 명령 프롬프트 - mandiant_ioc_finder.exe collect -o c:\Wtemp -d z:\W
c:\WTemp\Wmandiant IOC Finder\Wx64>mandiant_ioc_finder.exe collect -o c:\Wtemp -d z:\W
04-26-2013 23:49:25 Setting up dependencies...
04-26-2013 23:49:25 Starting collection...
04-26-2013 23:49:25 Running built-in collection script at ./lib/script.xml...
04-26-2013 23:49:25 Auditing (w32system) started at 04-26-2013 23:49:25
04-26-2013 23:49:25 Auditing (w32system) finished. (Took 0 seconds)
04-26-2013 23:49:25 Auditing (w32disks) started at 04-26-2013 23:49:25
04-26-2013 23:49:25 Auditing (w32disks) finished. (Took 0.047 seconds)
04-26-2013 23:49:25 Auditing (w32volumes) started at 04-26-2013 23:49:25
04-26-2013 23:49:25 Auditing (w32volumes) finished. (Took 0.031 seconds)
04-26-2013 23:49:25 Auditing (w32hivelist) started at 04-26-2013 23:49:25
04-26-2013 23:49:25 Auditing (w32hivelist) finished. (Took 0.016 seconds)
04-26-2013 23:49:25 Auditing (w32network-arp) started at 04-26-2013 23:49:25
04-26-2013 23:49:26 Auditing (w32network-arp) finished. (Took 0.156 seconds)
04-26-2013 23:49:26 Auditing (w32network-route) started at 04-26-2013 23:49:26
04-26-2013 23:49:26 Auditing (w32network-route) finished. (Took 0.125 seconds)
04-26-2013 23:49:26 Auditing (w32network-dns) started at 04-26-2013 23:49:26
04-26-2013 23:49:26 Auditing (w32network-dns) finished. (Took 0.016 seconds)
04-26-2013 23:49:26 Auditing (w32ports) started at 04-26-2013 23:49:26
04-26-2013 23:49:26 Auditing (w32ports) finished. (Took 0.031 seconds)
04-26-2013 23:49:26 Auditing (w32prefetch) started at 04-26-2013 23:49:26
<Issue number="0" level="Error" summary="Operating System is unsupported. Prefetch is only
The audit was unable to start or encountered an error during its execution.
04-26-2013 23:49:26 Auditing (w32prefetch) finished. (Took 0.016 seconds)
04-26-2013 23:49:26 Auditing (w32tasks) started at 04-26-2013 23:49:26
04-26-2013 23:49:27 Auditing (w32tasks) finished. (Took 0.733 seconds)
```





## 국내에서의 활용

### ▪ 현재 상황

- 국내 침해사고 대응 시 IOC 데이터를 거의 활용 안함
- IOC 데이터를 관리하는 곳도 존재하지 않음

### ▪ 활용 방안

- KISA? AhnLab? Hauri? NCSC?
- 사이버테러와 같은 사고 분석 시 IOC 데이터만 교환하여 효율적인 조사 가능
- 평시 침해사고 분석을 위해 IOC 데이터를 관리하는 곳이 필요 → 공개? 비공개?



## 그럼 IOAF는?

- **IOAF** – Indicators of Anti-Forensics
  - 안티포렌식 도구의 흔적 지표로 안티포렌식 행위 여부 탐지
  
- **통합적인 지표 데이터베이스 필요**
  - IOC (Indicators of Compromise)
  - IOAF (Indicators of Anti-Forensics)



# SigBase: Signature Database



## Signature Database

### ▪ 시그니처 데이터베이스의 필요

#### • 다양한 파일시그니처 모음 존재

- ✓ 리눅스 파일(file) 명령
- ✓ 공개 확장자 모음 - [http://en.wikipedia.org/wiki/List\\_of\\_file\\_formats](http://en.wikipedia.org/wiki/List_of_file_formats)
- ✓ 공개 시그니처 모음 - [http://www.garykessler.net/library/file\\_sigs.html](http://www.garykessler.net/library/file_sigs.html)
- ✓ 웹 기반의 질의형 시그니처 - <http://www.filesignatures.net>
- ✓ 바이너리 구조 기반 파일 식별 도구 TrID - <http://mark0.net/soft-trid-e.html>

#### • 문제점

- ✓ 단순한 파일 확장자, 파일 헤더/푸터 시그니처에 대해서만 정보 제공
- ✓ 입력 폼이 유연하지 않음



## Signature Database

### ▪ SigBase의 주요 고려사항

#### • 단순한 웹 기반 인터페이스

✓ 입력폼만 존재

- hexa 형식의 시그니처 (리틀, 빅 엔디안 모두 고려)
- 문자열 시그니처

#### • 단순한 헤더/푸터 기반의 시그니처에서 포렌식 시그니처로 확장

✓ 컴파운드 파일의 스트림 시그니처

✓ JPEG 내부 구조별 시그니처

✓ 다양한 포렌식 아티팩트 시그니처

✓ ... ..



## Signature Database

### ▪ SigBase 주요 컬럼

- 확장자
- 형식
- 시그니처 (Hex)
- 시그니처 (문자열)
- 오프셋
- 크기
- 설명

<b>Extension</b>	.doc	.db
<b>Format</b>	Compound Document Format	Windows <a href="#">IconCache</a> Format
<b>Signature (Hex)</b>	57 00 6F 00 72 00 64 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00	57 69 6E 34
<b>Signature (String)</b>	WordDocument (Unicode)	Win4
<b>Offset</b>	0	4 (4h)
<b>Size</b>	24 (18h)	4 (4h)
<b>Description</b>	WordDocument Stream	<p>Windows IconCache.db file</p> <p><b>Windows 9x/NT4/2K :</b></p> <ul style="list-style-type: none"> <li>- %SystemDrive%\Windows\ShellIconCache</li> <li>- %SystemDrive%\Winnt\ShellIconCache</li> </ul> <p><b>Windows XP :</b></p> <ul style="list-style-type: none"> <li>- %SystemDrive%\Documents and Settings\%UserName%\Local Settings\Application Data\IconCache.db</li> </ul> <p><b>Windows Vista/7 :</b></p> <ul style="list-style-type: none"> <li>- %UserProfile%\AppData\Local\IconCache.db</li> </ul>



## Signature Database

- **구축과 활용**
  - 초기 데이터베이스 구성은 수동
  - 지속적인 업데이트 방안
    - ✓ 회원 가입을 통한 시그니처 접수
  - 다양한 포렌식 아티팩트 시그니처 확인 가능
  - 웹 API 지원을 통한 활용



- **Using Indicators of Compromise to Find Evil and Fight Crime (Slide),**  
[http://www.us-cert.gov/sites/default/files/gfirst/presentations/2011/Using\\_Indicators\\_of\\_Compromise.pdf](http://www.us-cert.gov/sites/default/files/gfirst/presentations/2011/Using_Indicators_of_Compromise.pdf)
  
- **Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC,**  
[http://openioc.org/resources/An\\_Introduction\\_to\\_OpenIOC.pdf](http://openioc.org/resources/An_Introduction_to_OpenIOC.pdf)
  
- **Using IOC (Indicators of Compromise) in Malware Forensics,**  
[http://www.sans.org/reading\\_room/whitepapers/incident/ioc-indicators-compromise-malware-forensics\\_34200](http://www.sans.org/reading_room/whitepapers/incident/ioc-indicators-compromise-malware-forensics_34200)
  
- **Identifying & Sharing Threat Information with OpenIOC,**  
<http://scap.nist.gov/events/2011/itsac/presentations/day2/Wilson%20-%20OpenIOC.pdf>

