

침해 지표 활용



JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개요

1. 침해 지표 소개
2. 침해 지표 관련 표준
3. 침해지표 활용

침해 지표 소개

침해 지표 소개

■ 침해지표?

• 침해 지표 – IOC(Indicators Of Compromise)

✓ 침해 혹은 감염을 확인할 수 있는 포렌식 아티팩트

• 일반적인 침해 지표

✓ IP 주소

✓ 악성코드의 MD5 해시

✓ C2 URL

• 포렌식 침해 지표

✓ 악성코드의 정적, 동적 분석 정보를 활용

✓ 악성코드가 삭제된 이후에도 침해 혹은 감염 탐지 가능

✓ 초기 분석 시 알려진 악성코드의 실행 흔적을 탐지하는 용도로 활용

✓ 조직 내부망의 추가적인 감염 시스템을 찾는 용도로 활용

침해 지표 관련 표준

▪ 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">
```

■ Cyber Observable eXpression (CybOX)

- 운영 도메인에서 확인할 수 있는 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/>
- 아티팩트 별 XML 스키마 예제 – <http://cybox.mitre.org/language/version2.0/#samples>
- **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

▪ 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 dot COM



The image shows a screenshot of the OpenIOC website. The top section features the 'OpenIOC' logo in a large, white, serif font. Below the logo, the text 'An Open Framework for Sharing Threat Intelligence' and 'Sophisticated Threats Require Sophisticated Indicators' is displayed in a smaller, white, serif font. To the right of the text is a technical diagram of two interlocking gears. The larger gear is labeled 'SHAFT - CENTERS' and 'OPEN END', and the smaller gear is labeled 'OPEN END'. The text 'OpenIOC Framework' is written along the bottom curve of the larger gear. Below the main text and diagram is a horizontal navigation bar with five buttons: 'Overview', 'Why OpenIOC?', 'Schema', 'Tools', and 'Resources'. The 'Overview' button is highlighted. Below the navigation bar is a dark blue section with the heading 'Overview' in a large, white, serif font. The text in this section describes the purpose of OpenIOC as a machine-digestible XML schema for sharing threat intelligence.

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.

침해 지표 관련 표준

■ OpenIOC 용어 – <http://openioc.org/terms/Current.iocterms>

- 500여 개 특성
- 필요 시 추가

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 기능

• 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

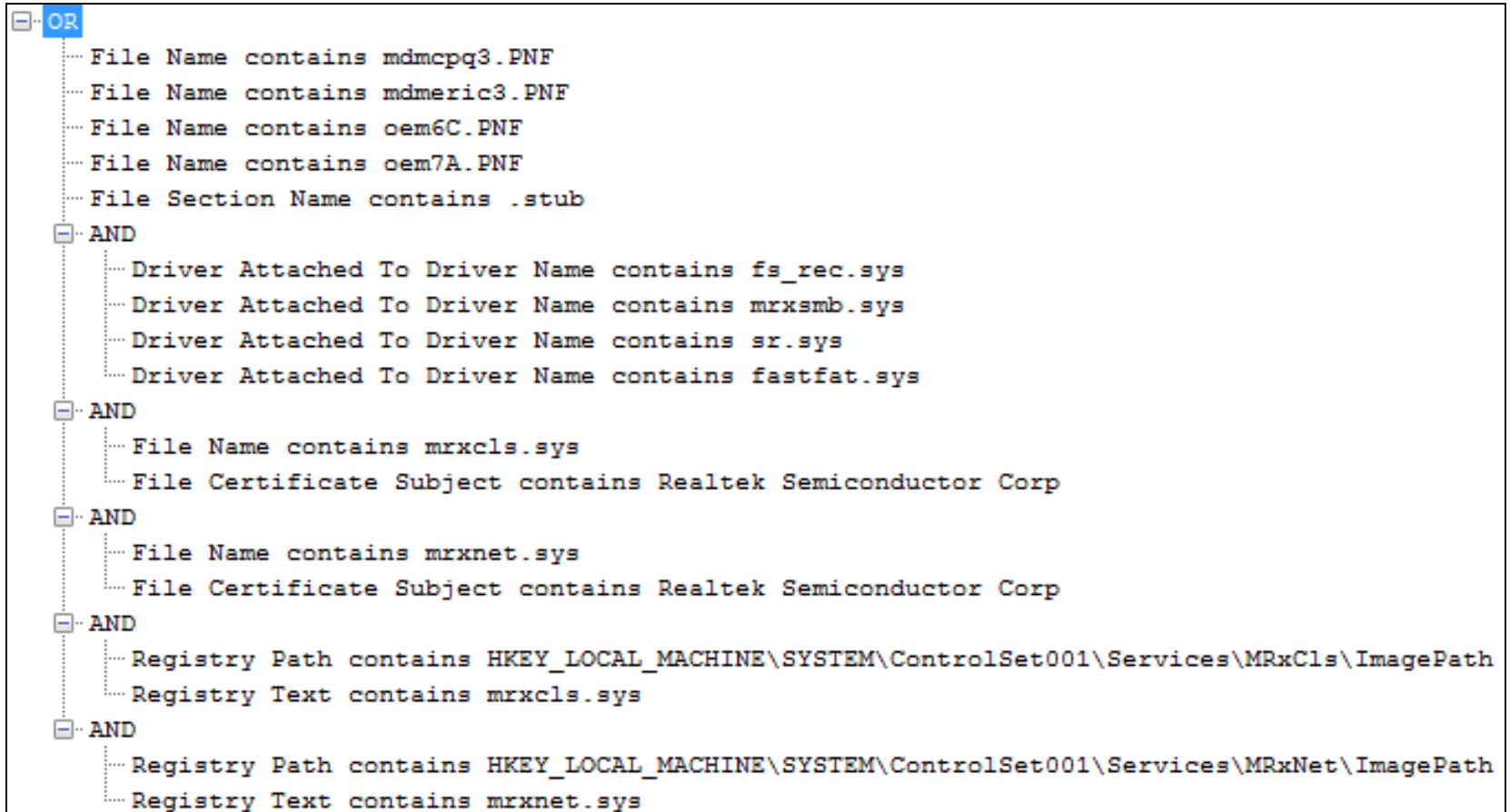
• 늘어나는 복잡성

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

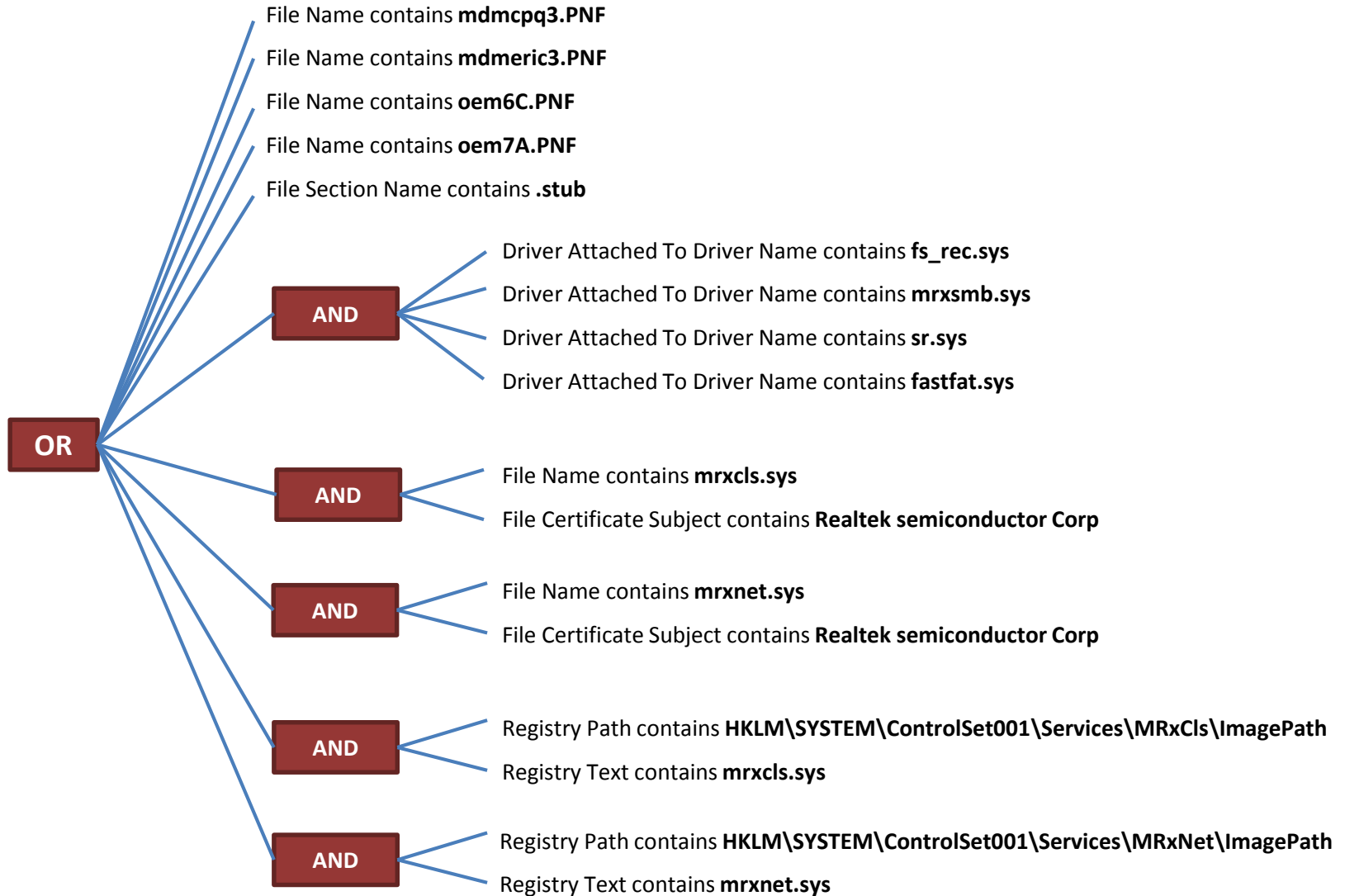
• 방법

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

■ OpenIOC Stuxnet 예제



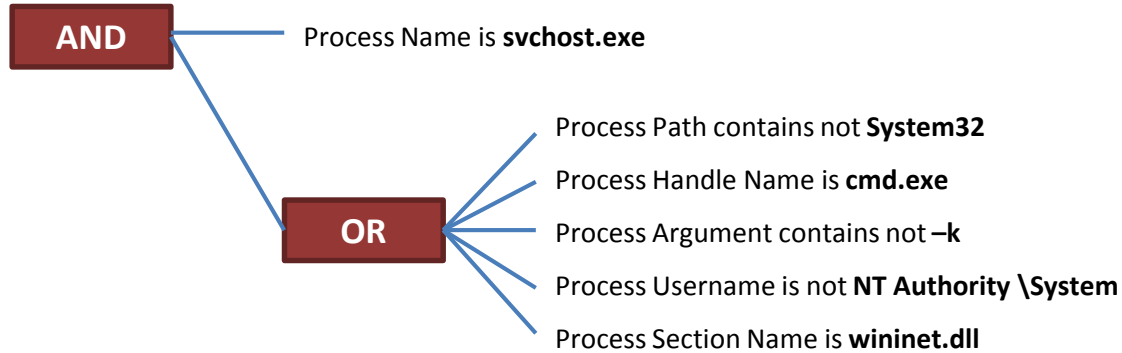
■ OpenIOC Stuxnet 예제



■ OpenIOC MSBGT 예제

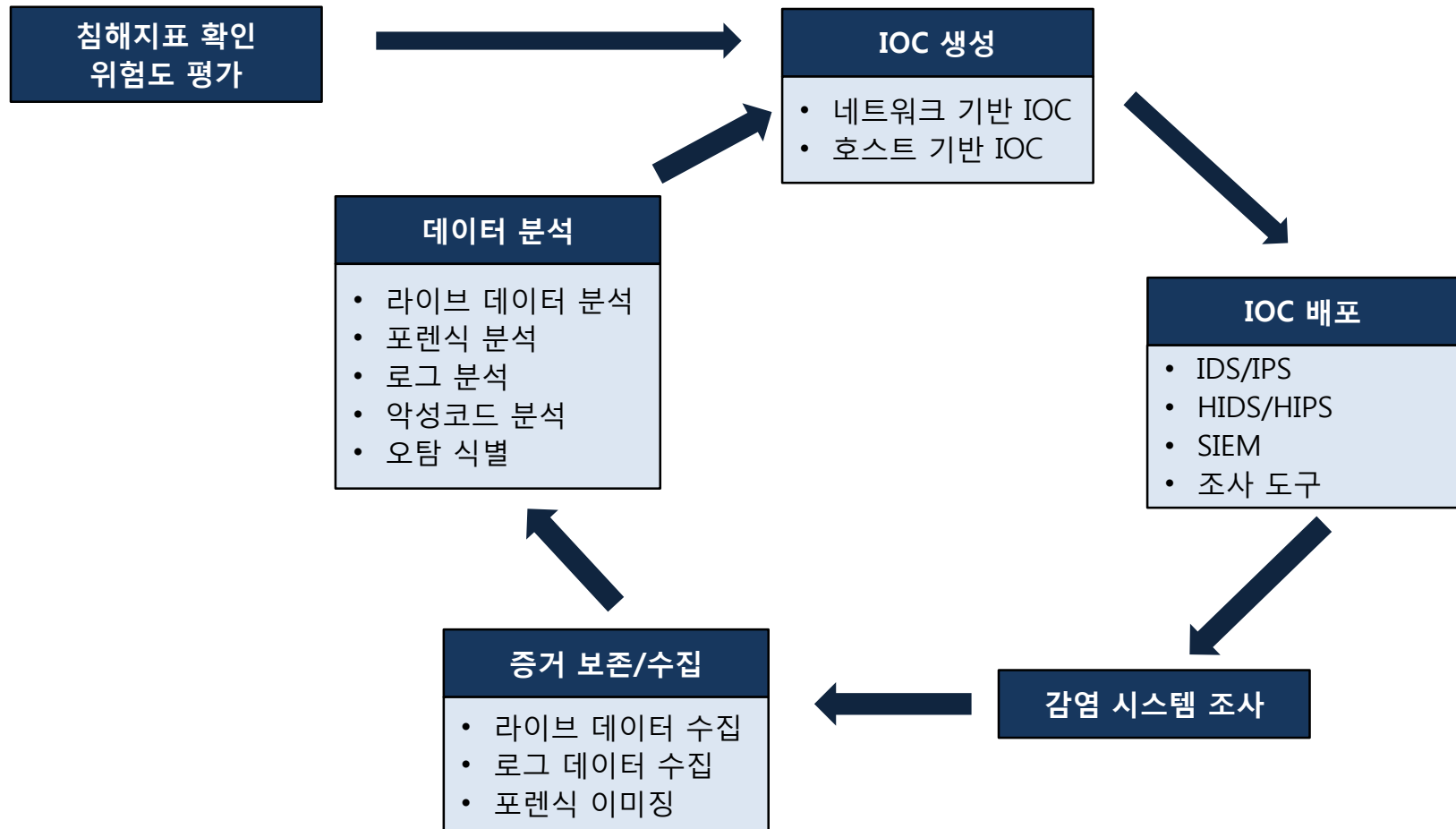


▪ OpenIOC svchost 예제



침해지표 활용

■ OpenIOC 활용



▪ OpenIOC 활용

• 활용 방안

- ✓ 특정 조직 내의 추가적인 침해 시스템 탐지
- ✓ 유사한 유형의 침해 흔적을 다른 조직에 적용할 때
- ✓ 침해사고 이외에 안티포렌식(IOAF) 탐지 등으로 확장 적용

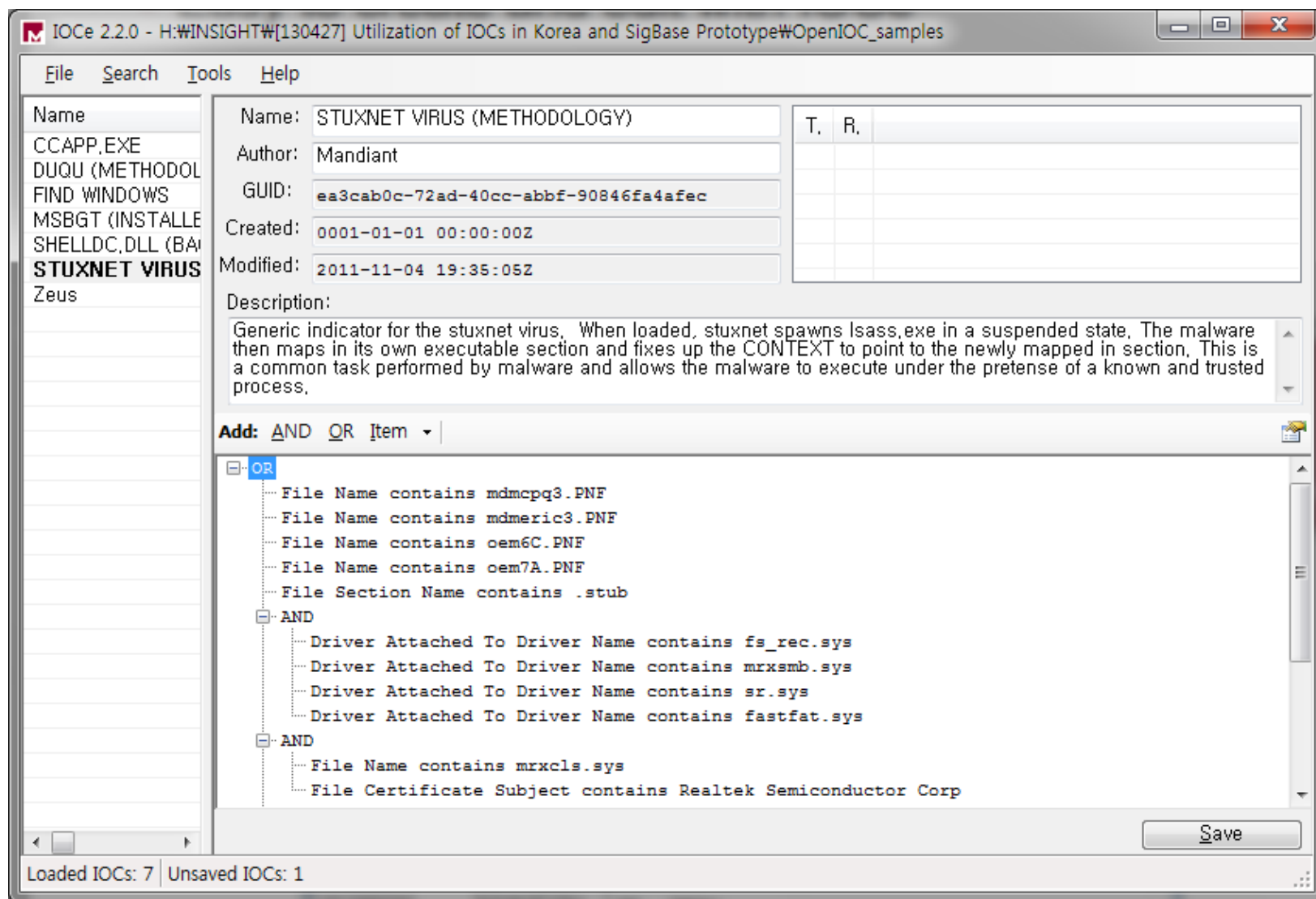
• 국내 상황

- ✓ 침해사고 대응 시 IOC 데이터를 제대로 활용하지 못함

• 발전 방향

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

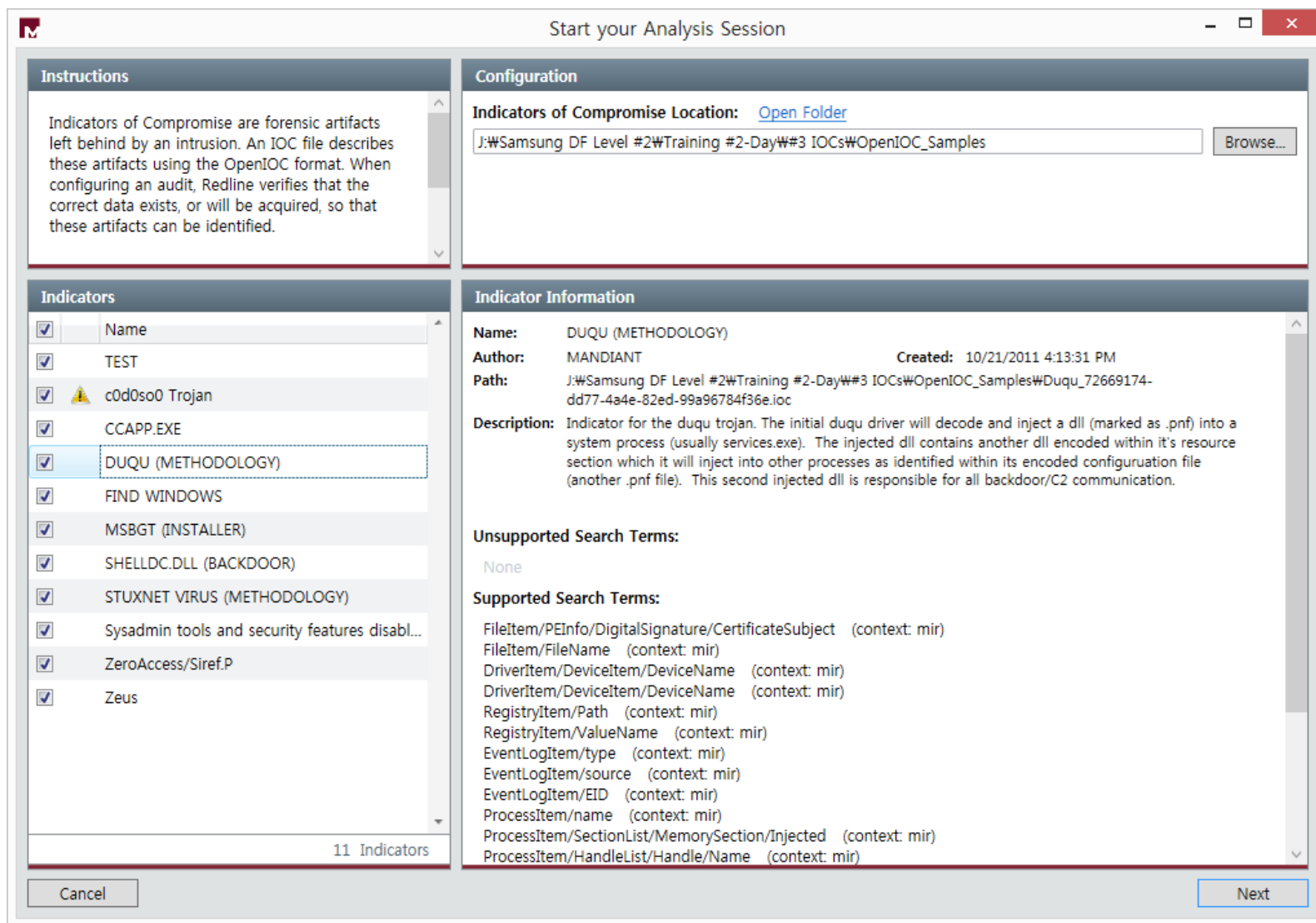
- **OpenIOC Editor** – <http://www.mandiant.com/resources/download/ioc-editor/>



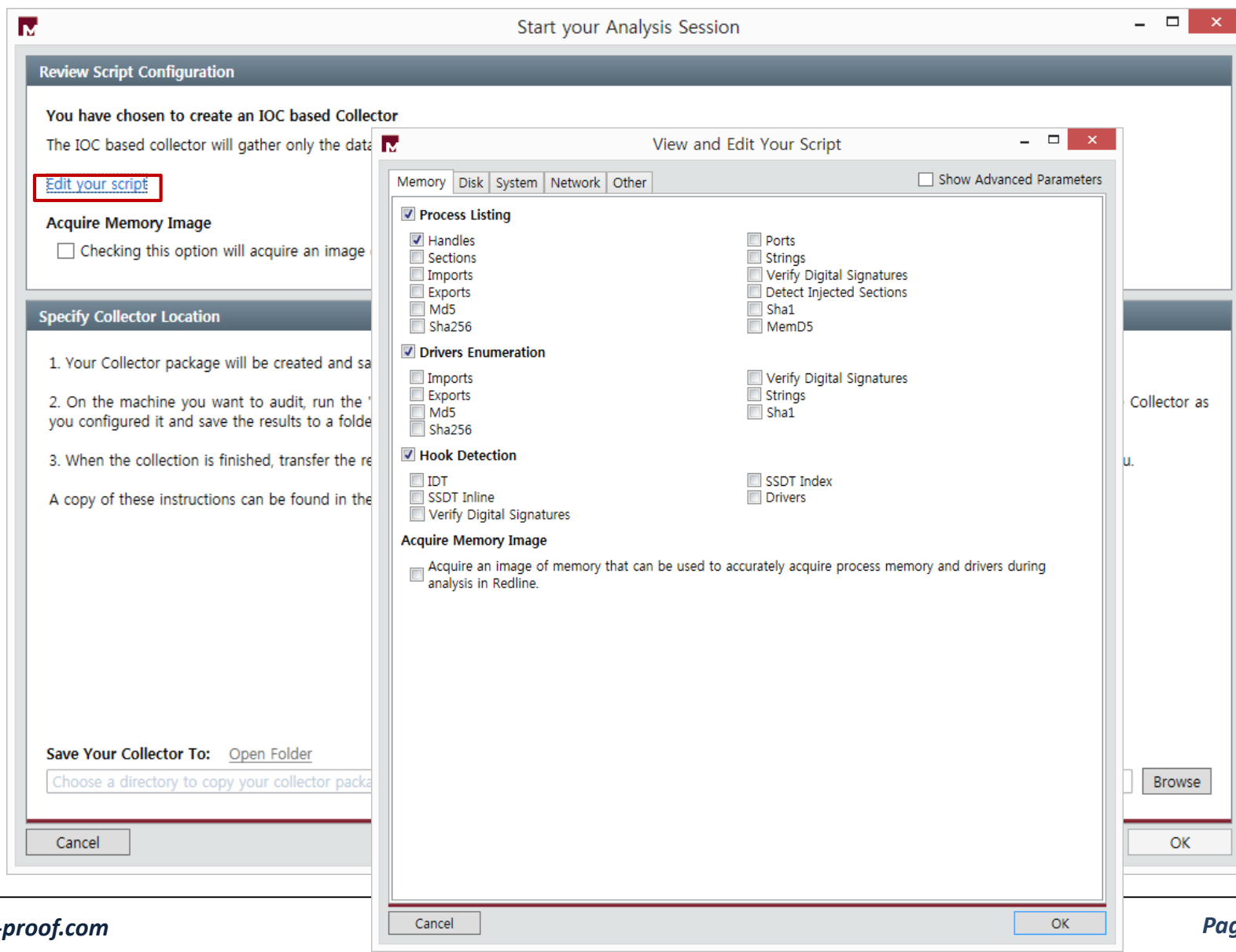
- **Redline** – <http://www.mandiant.com/resources/download/redline>



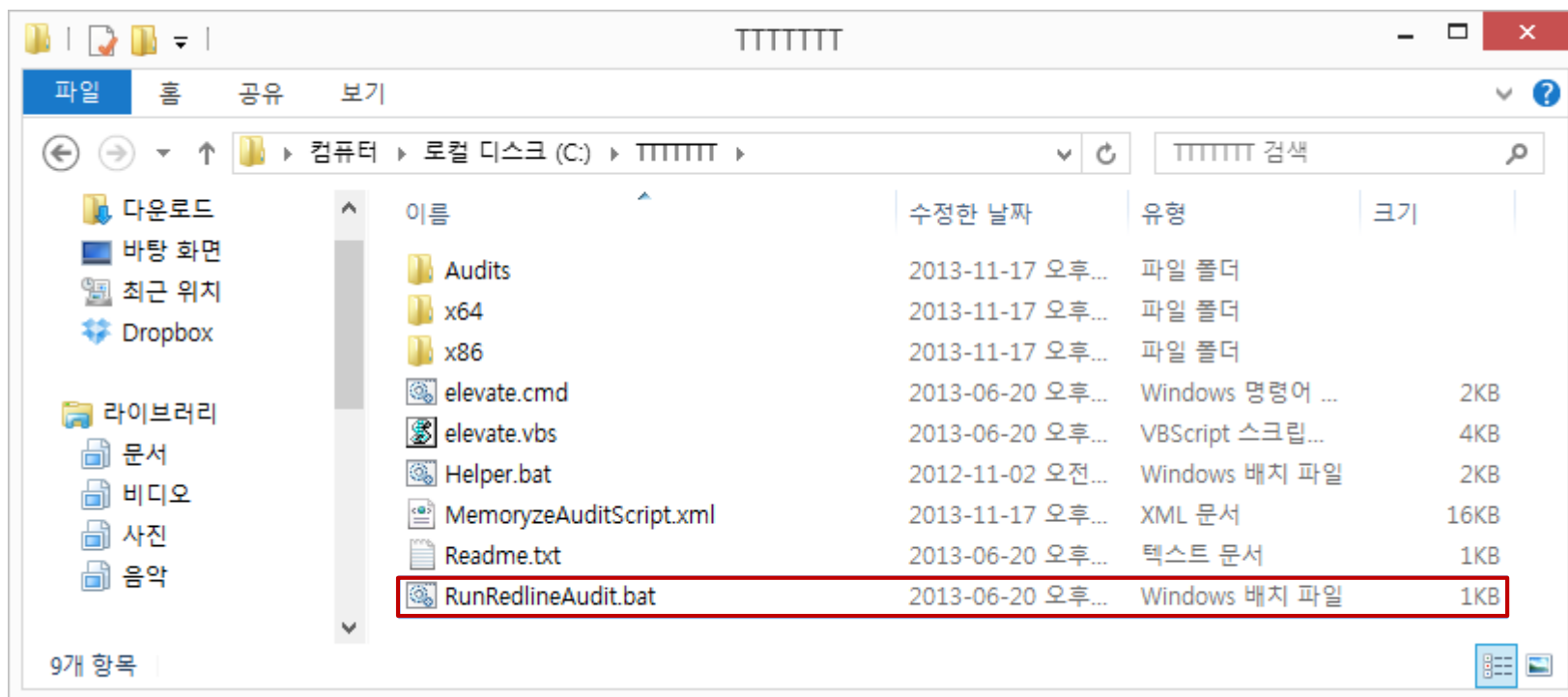
- Redline – <http://www.mandiant.com/resources/download/redline>



- Redline – <http://www.mandiant.com/resources/download/redline>



- Redline – <http://www.mandiant.com/resources/download/redline>



- **Redline** – <http://www.mandiant.com/resources/download/redline>



- Redline – <http://www.mandiant.com/resources/download/redline>

Start your Analysis Session

Instructions

Select the location of your audit data folder produced by your data collector. Redline will analyze this data to aid in navigation and to assist in the identification of potential issues. Redline can also search for Indicators of Compromise (described below) at this time. If you wish to search for Indicators of Compromise (IOCs) at a later time, this option can be found under the

Configuration

Audit Location: [Open Folder](#)
C:\TTTTTTT\Audits\PRONEERW20131117145649 [Browse...](#)

☒ **Indicators of Compromise Location:** [Open Folder](#)
J:\Samsung DF Level #2\Training #2-Day\#3 IOCs\OpenIOC_Samples [Browse...](#)

Indicators

<input type="checkbox"/>	Name
<input type="checkbox"/>	TEST
<input type="checkbox"/>	c0d0so0 Trojan
<input type="checkbox"/>	CCAPP.EXE
<input type="checkbox"/>	DUQU (METHODOLOGY)
<input checked="" type="checkbox"/>	FIND WINDOWS
<input type="checkbox"/>	MSBGT (INSTALLER)
<input type="checkbox"/>	SHELLDC.DLL (BACKDOOR)
<input type="checkbox"/>	STUXNET VIRUS (METHODOLOGY)
<input type="checkbox"/>	Sysadmin tools and security features disabl...
<input type="checkbox"/>	ZeroAccess/Siref.P
<input type="checkbox"/>	Zeus

11 Indicators

Indicator Information

Name: FIND WINDOWS
Author: Mandiant **Created:** 1/1/0001 12:00:00 AM
Path: J:\Samsung DF Level #2\Training #2-Day\#3 IOCs\OpenIOC_Samples
WFind_Windows_c32ab7b5-49c8-40cc-8a12-ef5c3ba91311.ioc
Description: This is a sample IOC that will hit on a number different artifacts present on a Windows computer. This IOC is used to test or illustrate the use of an IOC.

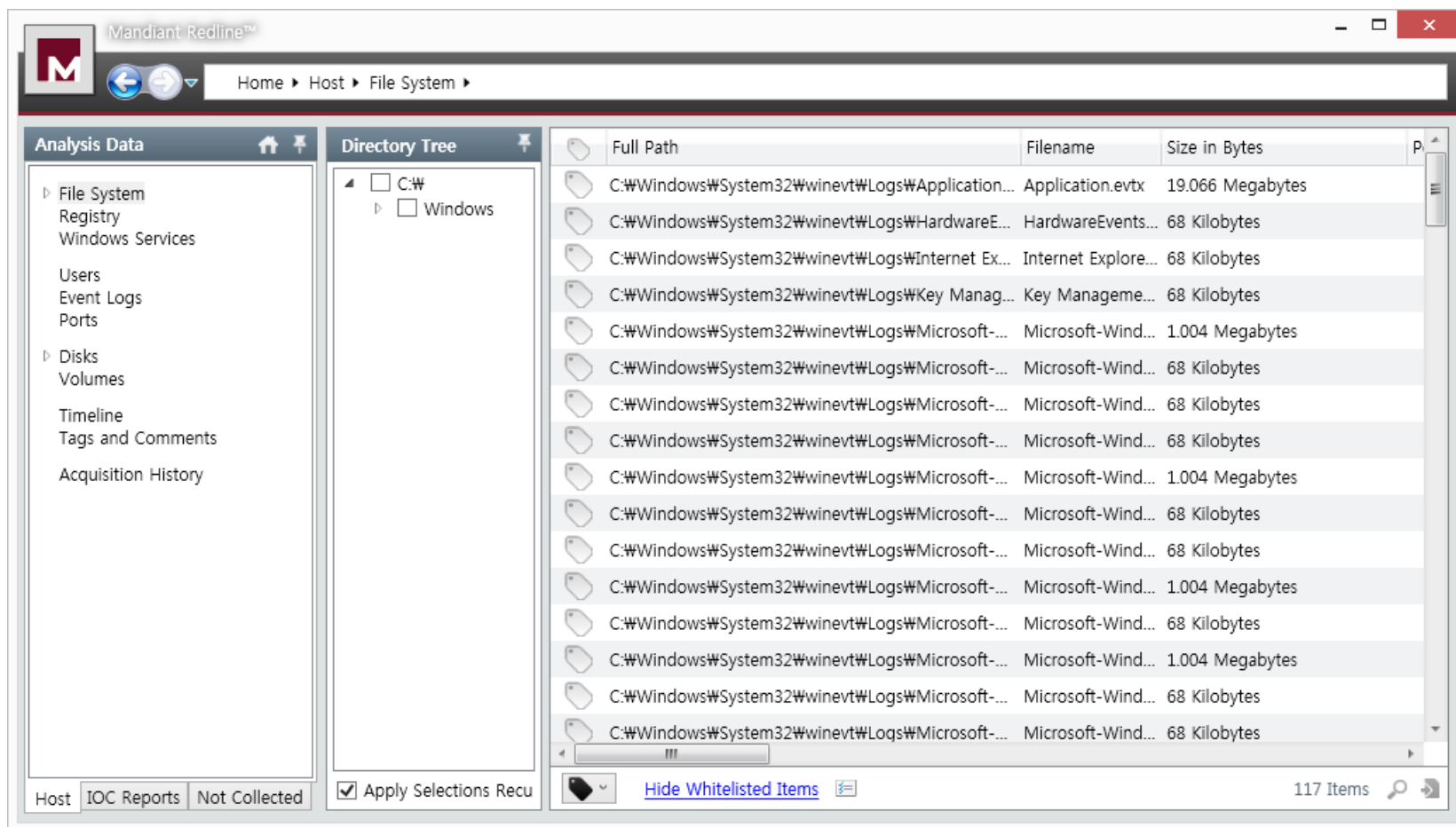
Not Collected Search Terms:
None

Unsupported Search Terms:
None

Supported Search Terms:
FileItem/FullPath (context: mir)
FileItem/FileName (context: mir)
FileItem/FileExtension (context: mir)
ProcessItem/name (context: mir)
EventLogItem/EID (context: mir)
UserItem/Username (context: mir)
ServiceItem/name (context: mir)
RegistryItem/Path (context: mir)
PortItem/localPort (context: mir)
VolumeItem/DriveLetter (context: mir)
DiskItem/DiskName (context: mir)

[Cancel](#) [Next](#)

- Redline – <http://www.mandiant.com/resources/download/redline>



- Redline – <http://www.mandiant.com/resources/download/redline>

The screenshot displays the Mandiant Redline web application. The browser window title is "Mandiant Redline™". The address bar shows the URL "http://www.mandiant.com/resources/download/redline". The breadcrumb navigation is "Home > IOC Reports > IOC Report (2013-11-18 오전 12:23:39)".

The interface is divided into two main sections. On the left is the "Analysis Data" sidebar, which contains a list of reports. The selected report is "IOC Report (2013-11-18 오전 12:23:39)". At the bottom of this sidebar are buttons for "Create a New IOC Report", "Host", "IOC Reports", and "Not Collected".

The main content area is titled "IOC Report (2013-11-18 오전 12:23:39)". It displays a list of file paths under the heading "FIND WINDOWS- (UID: c32ab7b5)". Each entry includes a file path and a "View Hits +" link. The file paths are:

- C:\Users\JK\AppData\Local\Temp\IOCFinderAudits\20131118002339\66103244-617d-47d1-9b09-f1ee1f77bdba\20131118002339\mir.w32apifiles.65115b5f.xml
- C:\Users\JK\AppData\Local\Temp\IOCFinderAudits\20131118002339\66103244-617d-47d1-9b09-f1ee1f77bdba\20131118002339\mir.w32disks.3e5f247a.xml
- C:\Users\JK\AppData\Local\Temp\IOCFinderAudits\20131118002339\66103244-617d-47d1-9b09-f1ee1f77bdba\20131118002339\mir.w32eventlogs.46313923.xml
- C:\Users\JK\AppData\Local\Temp\IOCFinderAudits\20131118002339\66103244-617d-47d1-9b09-f1ee1f77bdba\20131118002339\mir.w32ports.2d2c3e6f.xml
- C:\Users\JK\AppData\Local\Temp\IOCFinderAudits\20131118002339\66103244-617d-47d1-9b09-f1ee1f77bdba\20131118002339\mir.w32registryapi.3976127a.xml

Below the list of file paths is a section titled "Report Details". It contains the following information:

- 1 out of your 1 Indicators of Compromise have hit against this Session.
- Report Location: C:\Users\JK\AppData\Local\Temp\1206f0dd-8f77-40da-af07-5b17879e85a0\index.html

A vertical "Details" button is located on the right side of the main content area.

