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

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:schema: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">
```

침해 지표 관련 표준

- **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

침해 지표 관련 표준

- **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">
```

침해 지표 관련 표준

- **OpenIOC dot COM**

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

침해 지표 관련 표준

OpenIOC 기능

- **시그니쳐**
  - ✓ 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

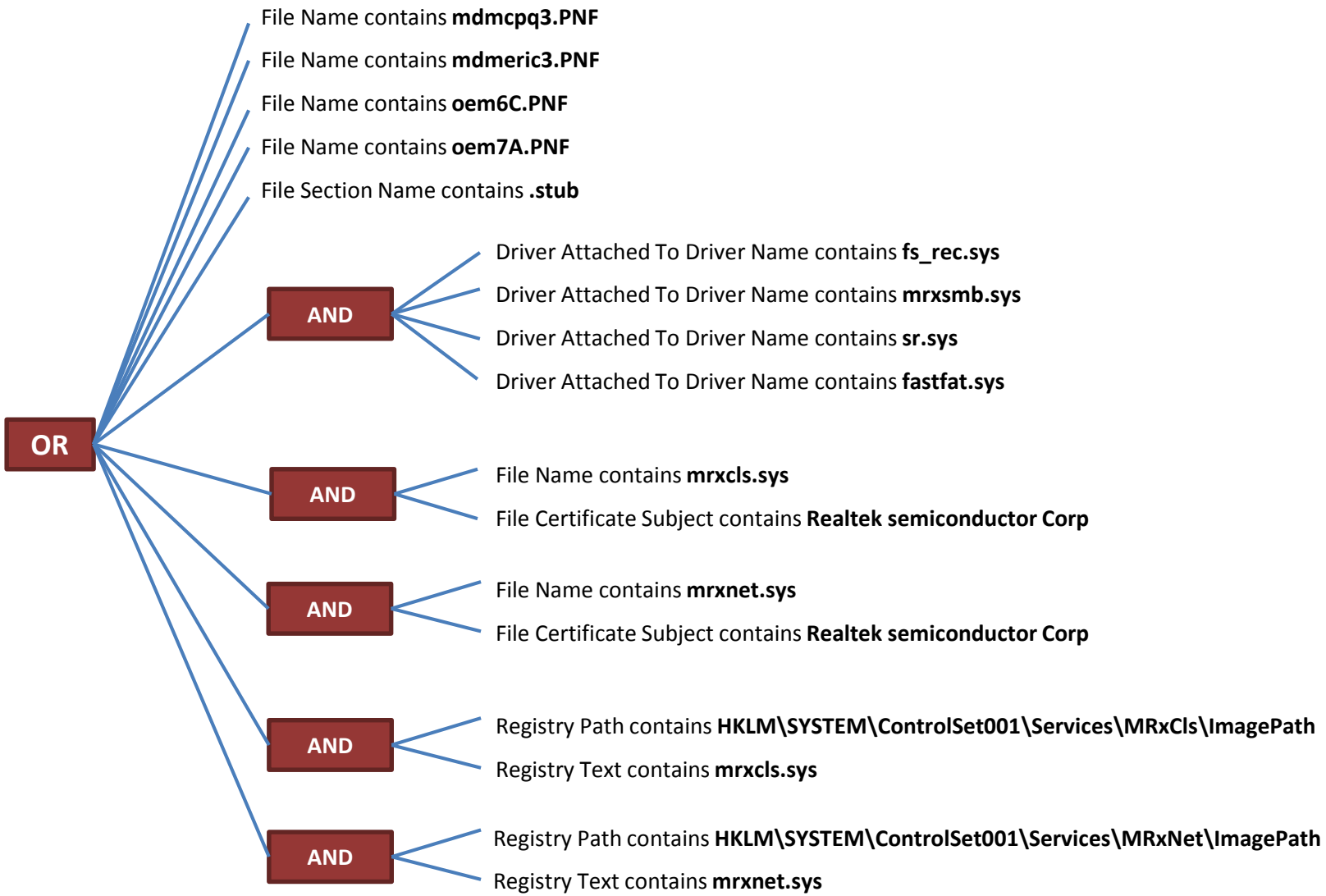
침해 지표 관련 표준

- OpenIOC 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
```

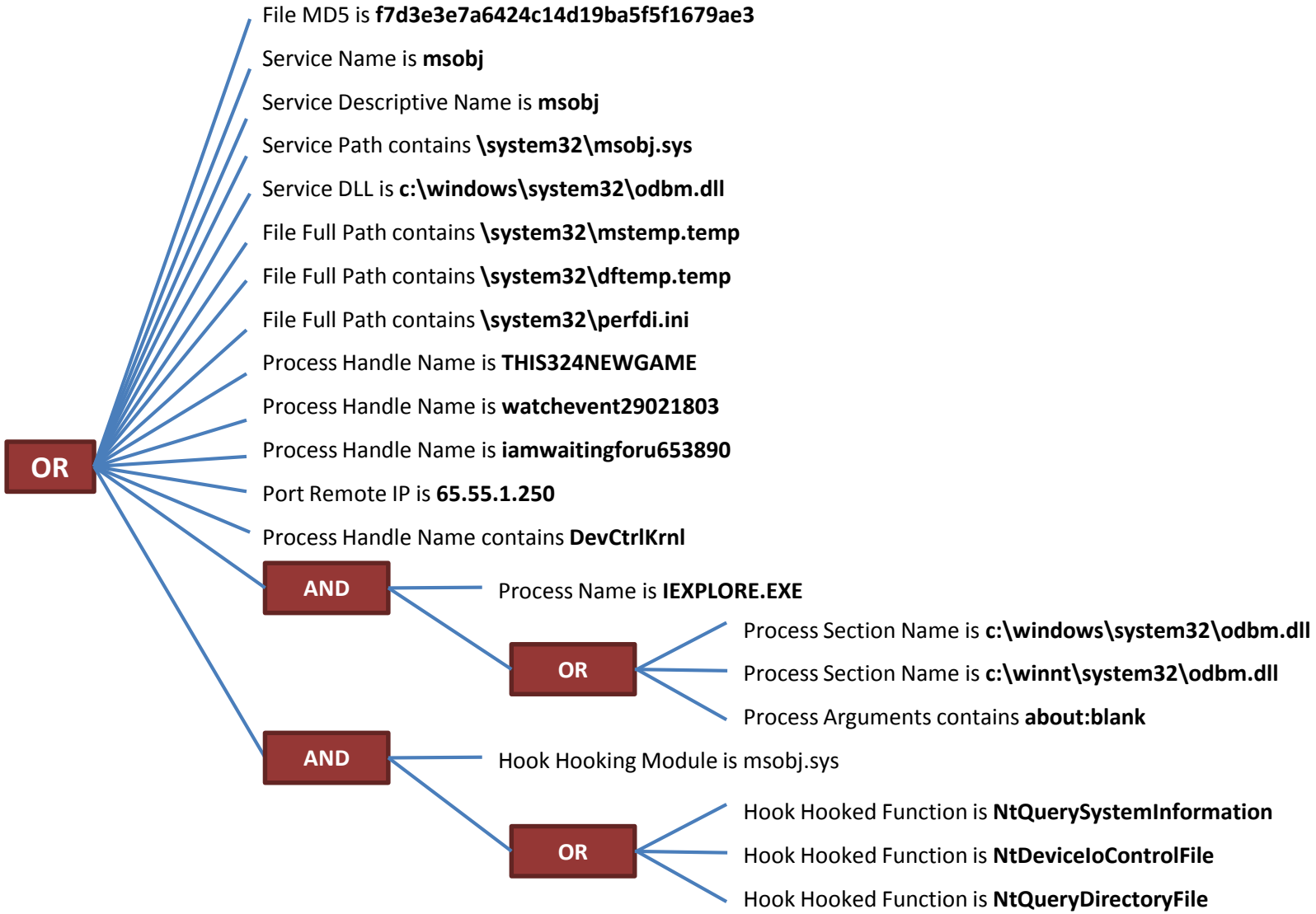
침해 지표 관련 표준

- **OpenIOC Stuxnet 예제**



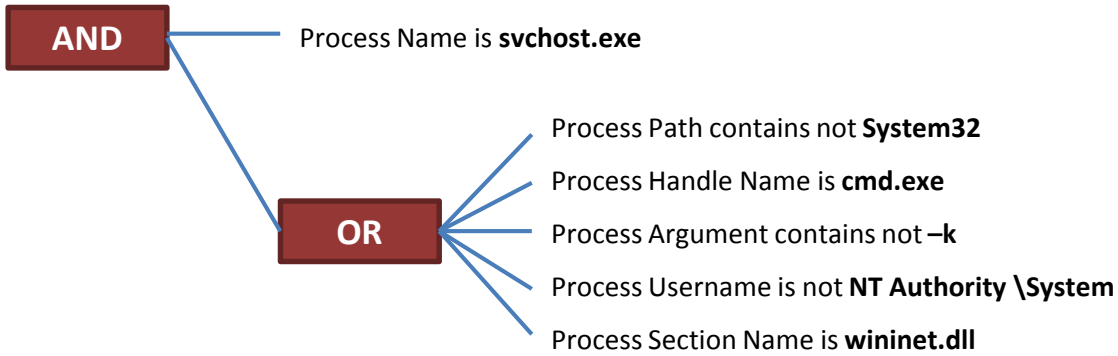
침해 지표 관련 표준

- **OpenIOC MSBGT 예제**



침해 지표 관련 표준

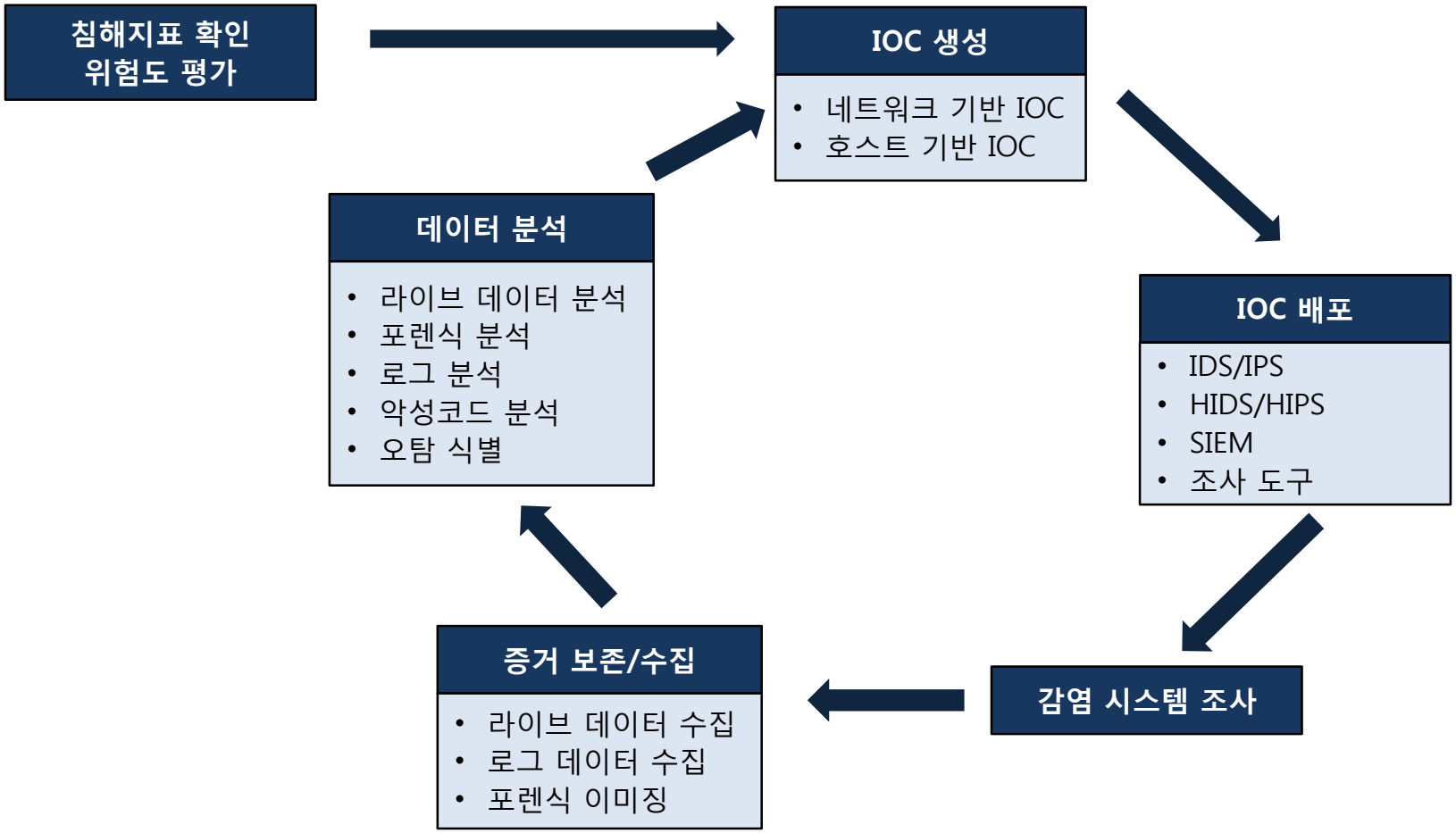
- **OpenIOC svchost 예제**



침해지표 활용

침해지표 활용

- **OpenIOC 활용**



침해지표 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

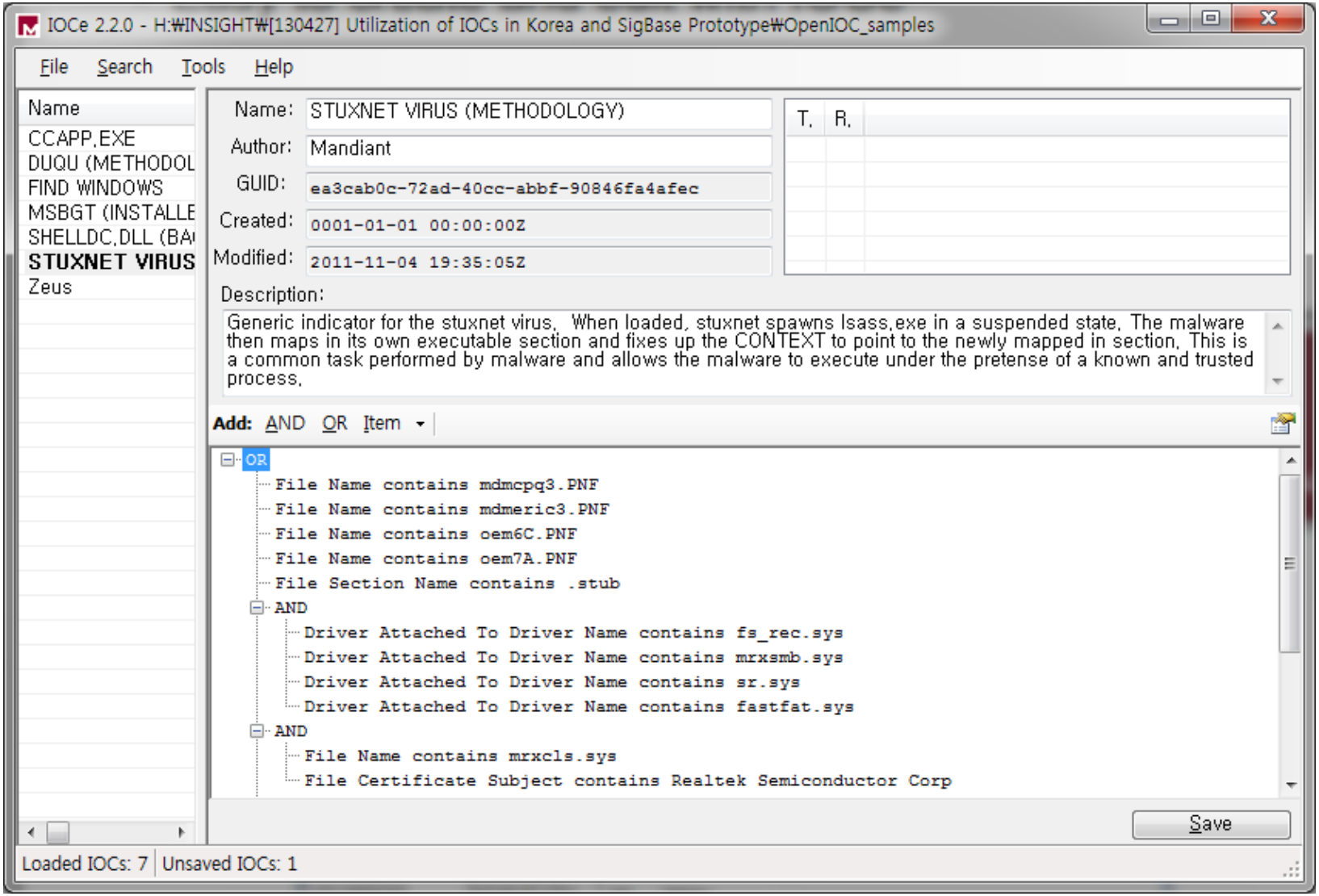
- ✓ 침해사고 대응 시 IOC 데이터를 제대로 활용하지 못함

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?

침해지표 활용

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

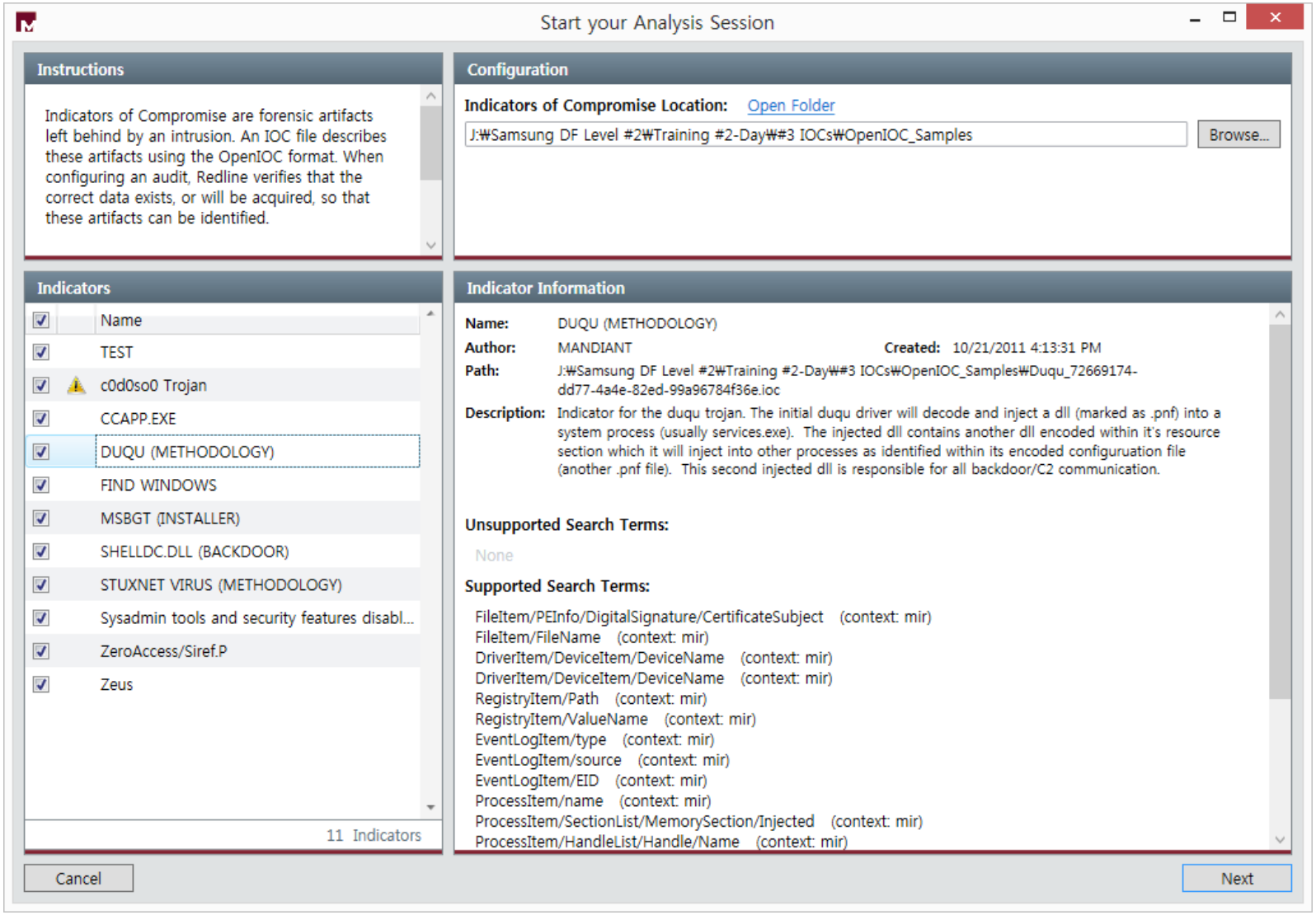


침해지표 활용

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

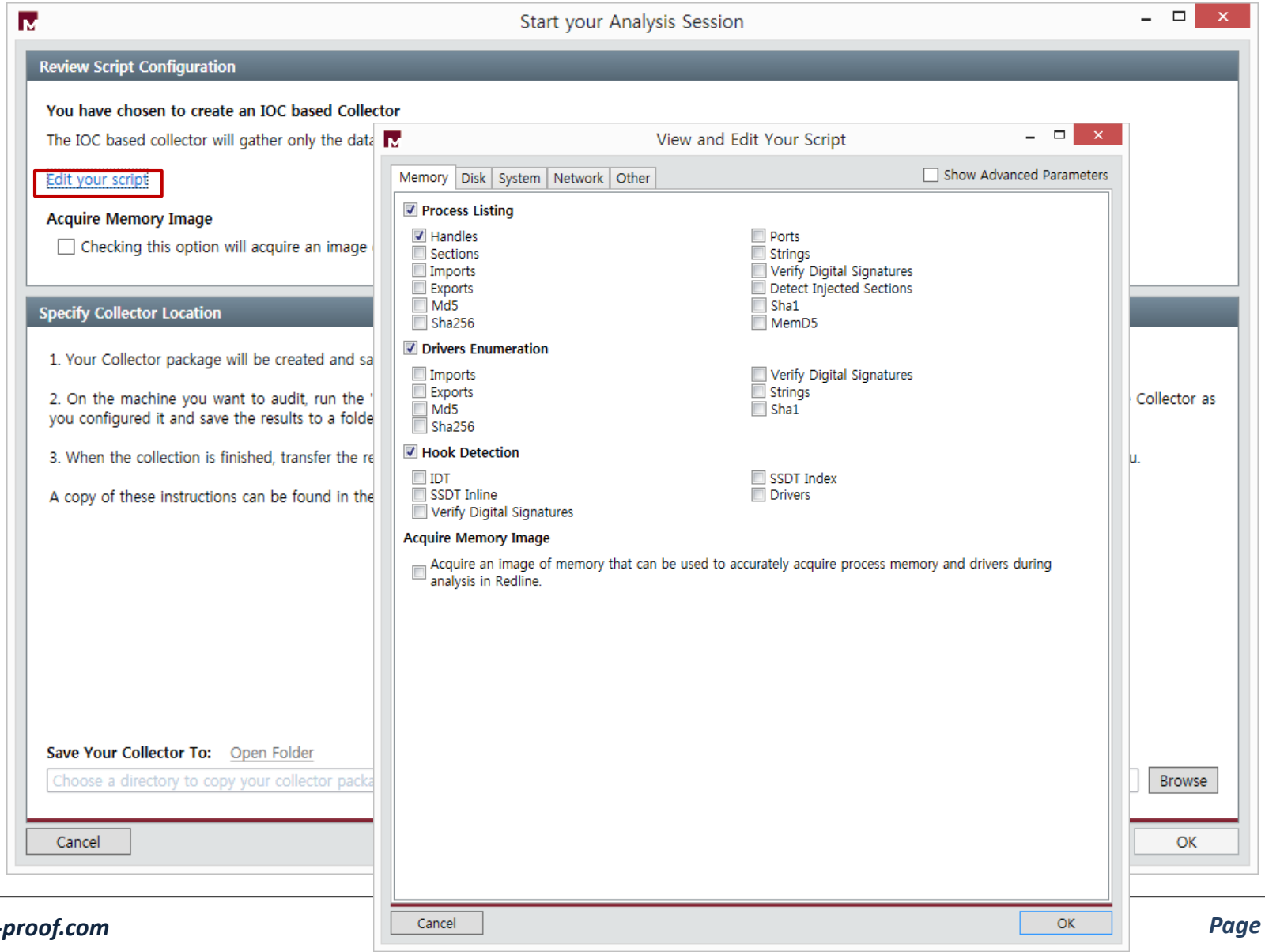
침해지표 활용

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



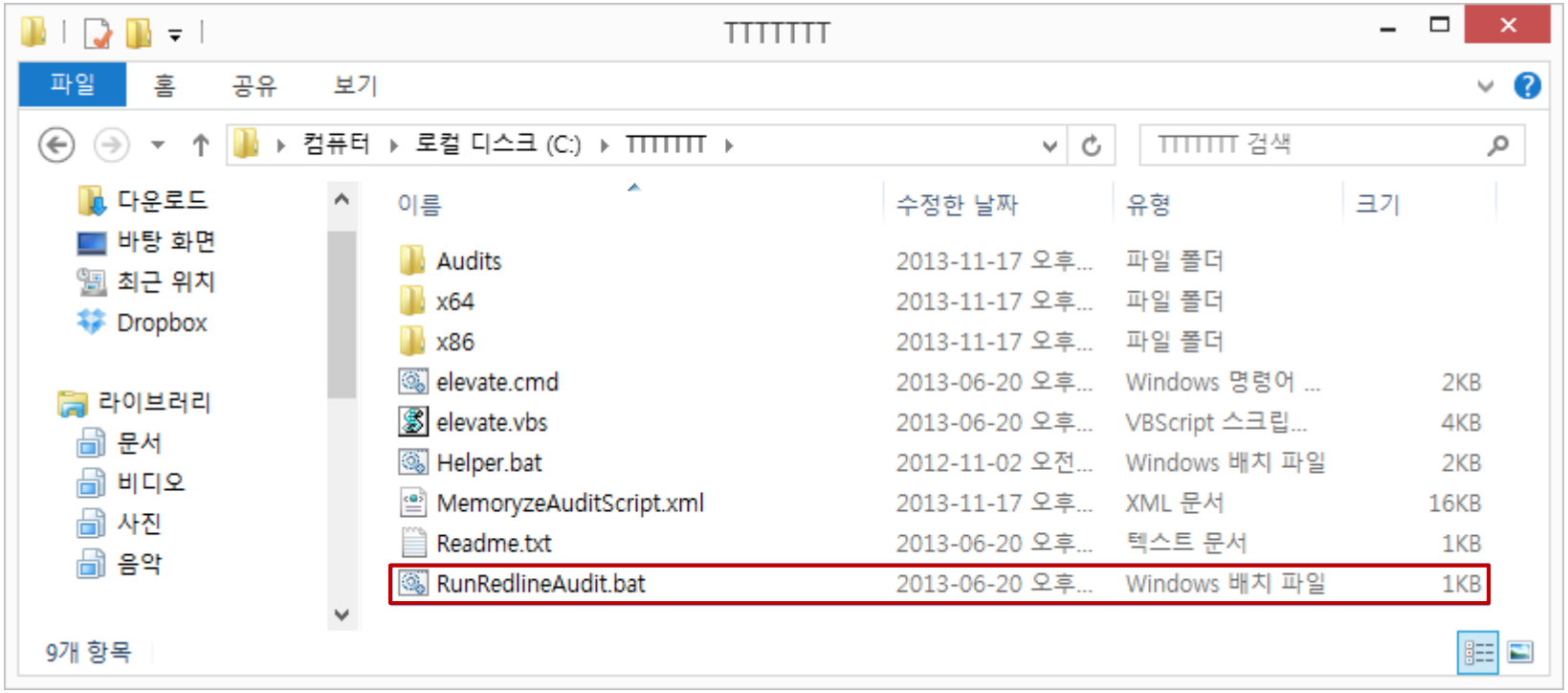
침해지표 활용

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



침해지표 활용

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

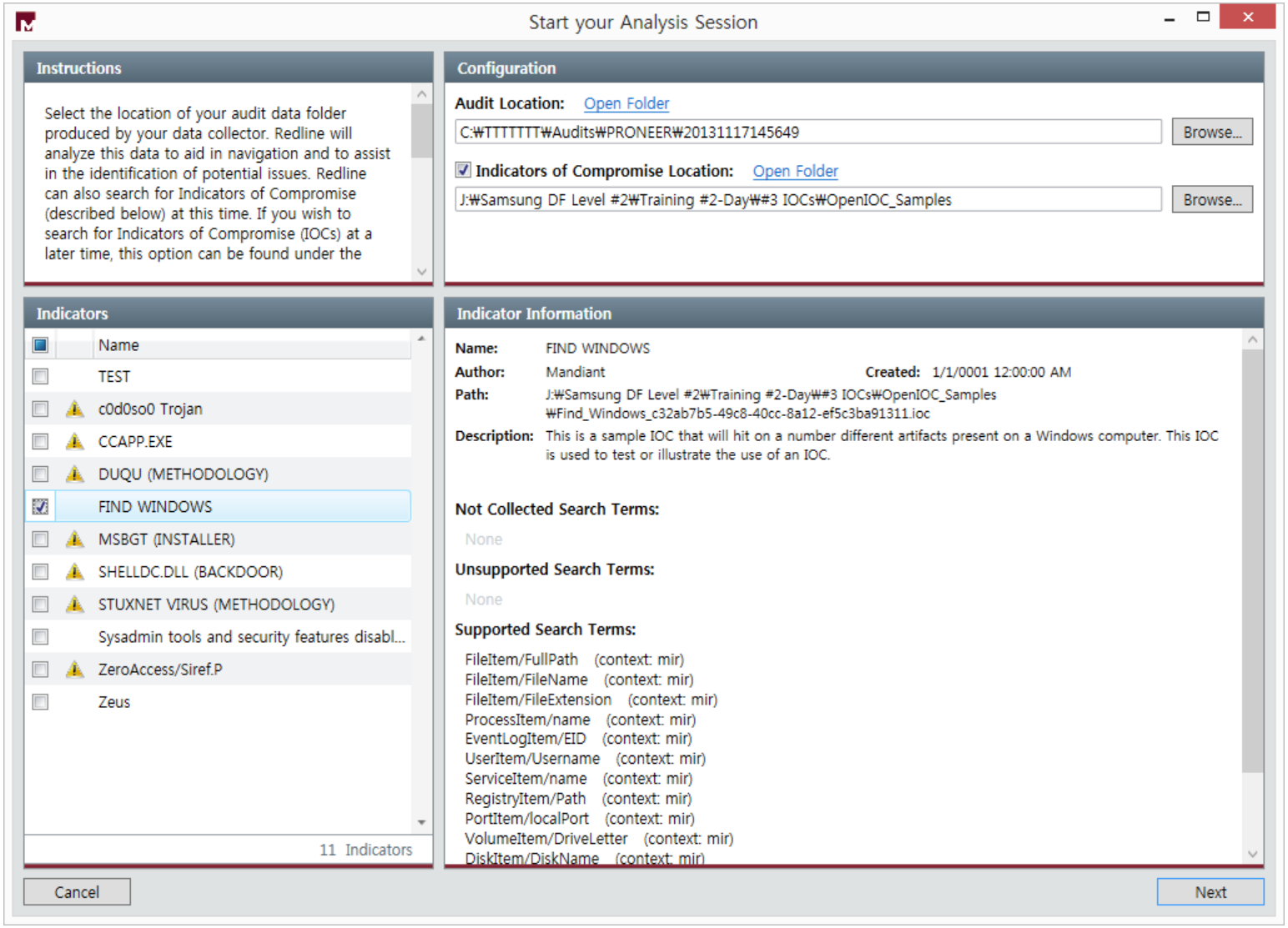


침해지표 활용

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

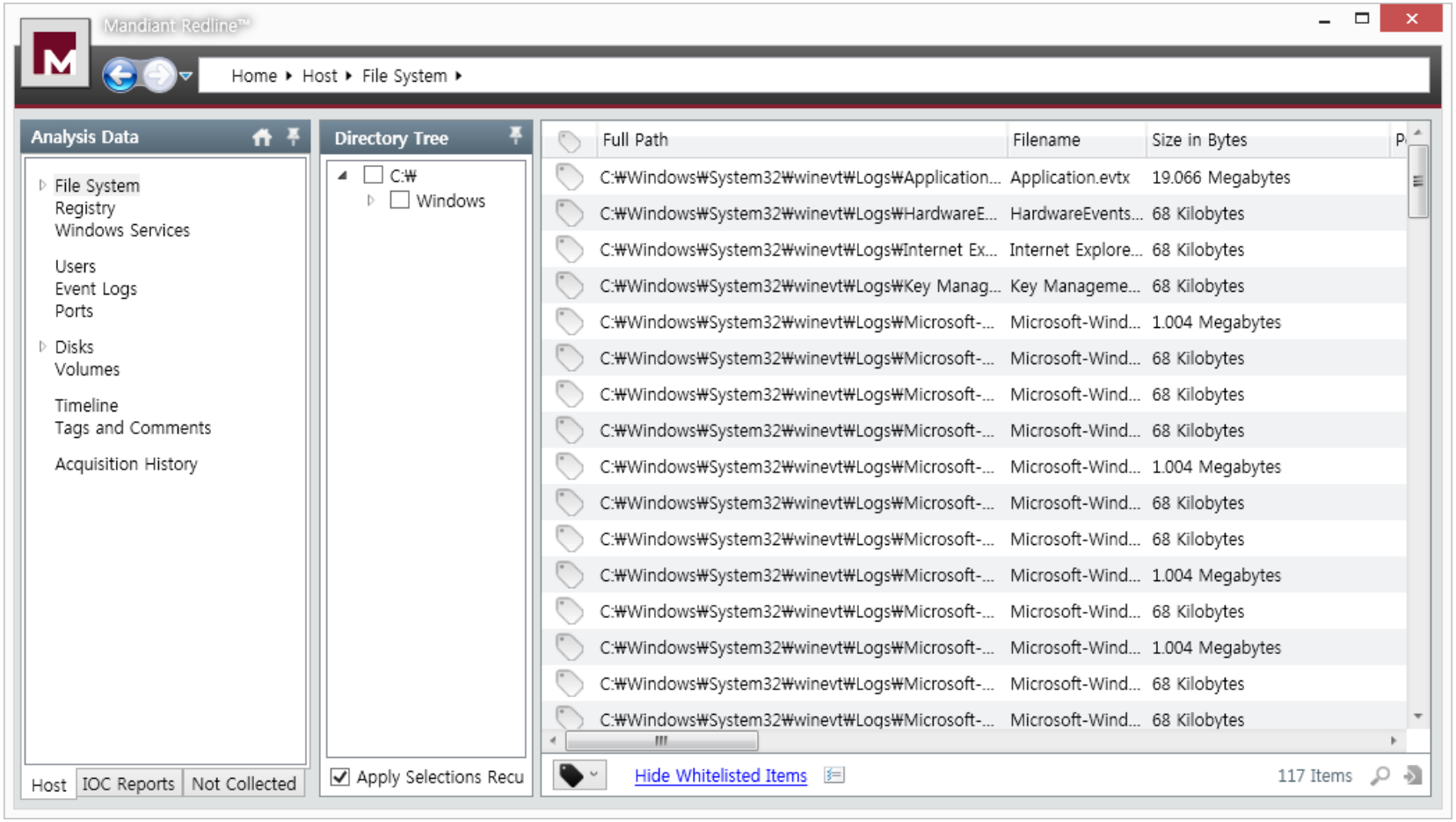
침해지표 활용

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



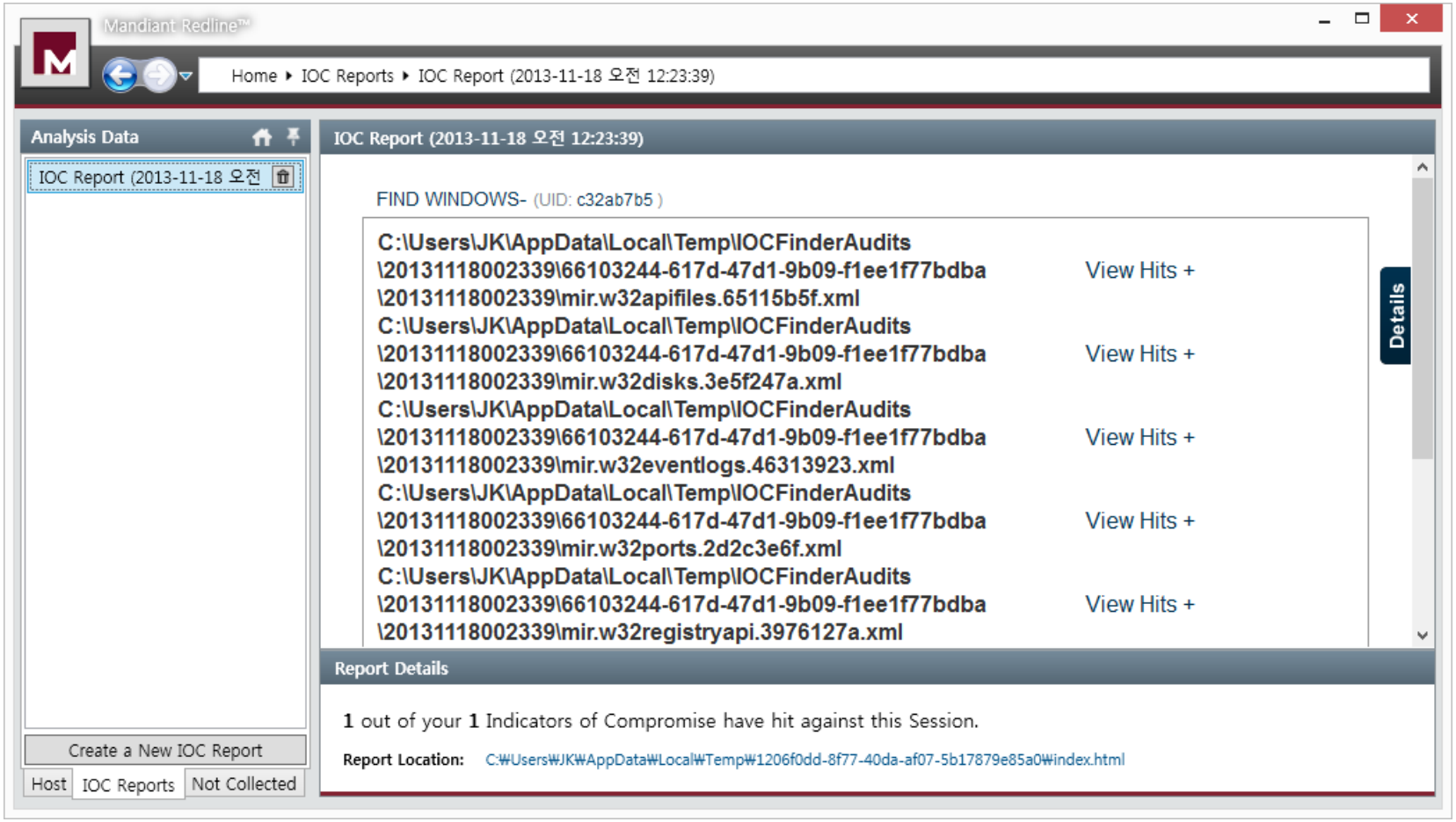
침해지표 활용

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



침해지표 활용

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



질문 및 답변