

Endpoint

PC	Server
<ul style="list-style-type: none">• 네트워크 출발지로 동작• 많은 네트워크 접속 행위를 발생• 프로그램 설치/삭제가 빈번 발생• 프로세스 생성/삭제 빈번 발생• 파일 생성/수정/소멸도 많이 발생	<ul style="list-style-type: none">• 도착지의 임무를 수행• 프로그램의 설치/삭제 등이 많이 발생하지 않음

* 윈도우 로그 저장 폴더 `c:\windows\system32\winevt\logs`

EndPoint 로그

- Endpoint 로그는 Endpoint 에서 발생하는 이벤트를 보여줌
 - 호스트의 동작만 보여주는 것이 아님
 - 악성코드에 감염된 호스트 검색 가능
 - 위협사냥의 기본 자료로 사용

*** 위협사냥 : 숨어있는 위협을 탐지해 공격기법과 공격자를 식별하고 제거하는 행위**
- Endpoint 로그의 관리 어려움
 - 엔드포인트 수량이 많아서 대용량 로그 생성
 - PC 호스트별, 사용별 로그를 수집하고 분류

Sysmon

- Microsoft의 Sysinternal suite에 포함된 시스템 모니터링 툴
- 기본 윈도우 이벤트 로그로는 한계가 있는 프로세스 생성, 네트워크 연결, 파일 생성 시간 변경 등의 정보를 추출한 후 윈도우 이벤트 저장소에 저장

* 이벤트 기반 정보가 아닌 ‘행동 기반 정보’를 수집에서 이벤트 저장소에 저장

Sysmon 기능

- 실행 프로세스와 부모 프로세스의 전체 명령 줄을 로그로 저장
- MD5, SHA1, SHA256 알고리즘으로 실행 프로그램의 해시 값을 기록
- 여러 종류의 해시 값을 동시에 기록
- 네트워크 연결에서 IP주소, 포트번호, 호스트명, 포트명 등을 기록
- 레지스트리에서 환경 설정이 변경된 경우 자동으로 다시 읽어 들임

[Win10] Sysmon Installation

❶ 파일 다운로드 후 설치

<https://download.sysinternals.com/files/Sysmon.zip>

```
C:\Users\sysmon\Desktop\Sysmon>dir
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: 1C9F-4DF9

C:\Users\sysmon\Desktop\Sysmon 디렉터리

2022-07-30 오후 03:29 <DIR> .
2022-07-30 오후 03:29 <DIR> ..
2022-05-11 오후 04:49          7,490 Eula.txt
2022-05-11 오후 04:49    7,291,792 Sysmon.exe
2022-05-11 오후 04:49   3,925,928 Sysmon64.exe
                3개 파일             11,225,210 바이트
                2개 디렉터리    10,781,904,896 바이트 남음
```

② sysmon 활성화

C:\>cd /user/sysmon/desktop/sysmon

C:\> sysmon64.exe -accepteula -i

```
C:\Users\sysmon\Desktop\Sysmon>sysmon64.exe -accepteula -i

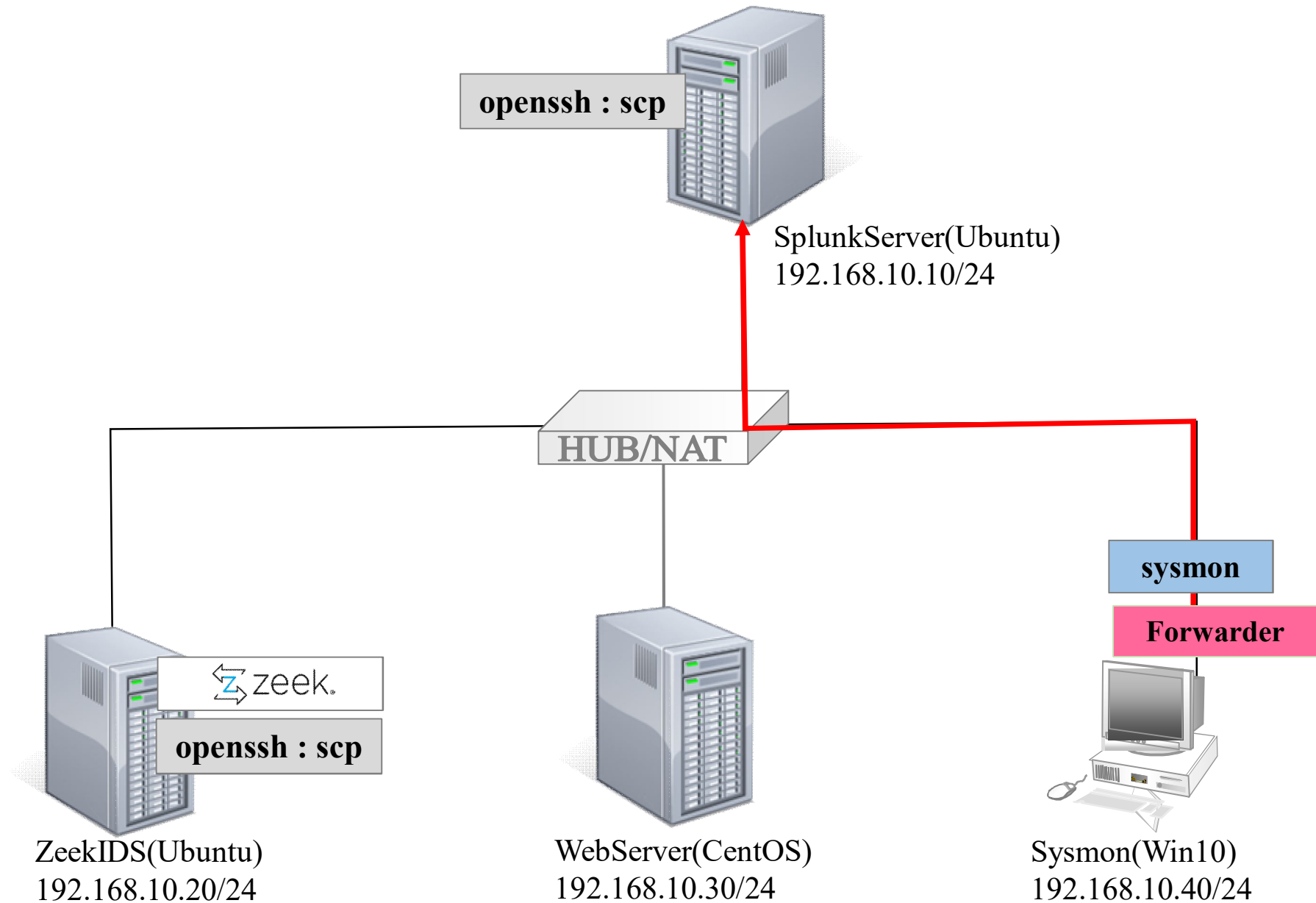
System Monitor v13.34 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\Users\sysmon\Desktop\Sysmon>
```

Sysmon 생성 이벤트 목록

ID	이벤트 이름	활용 방안
1	Process creation	새로운 프로세스가 만들어지면 생성 되는 로그 프로세스가 실행됐을 때 사용된 명령어의 전체 줄을 이벤트로 기록
2	A process changed a file creation time	프로세스가 파일 생성 시간을 수정 시 기록 공격자가 백도어 파일을 설치하면서 운영체제 파일을 위장하는것을 탐지 할 수 있음
3	Network Connection	호스트에서 TCP/UDP 연결기록을 이벤트로 생성 어느 프로세스가 네트워크 접속을 시도했는지 파악할 수 있으며 호스트명, IP주소, 포트번호 등 정보 제공
5	Process terminated	프로세스가 종료되면 이벤트를 생성







❶ \$SPLUNK_HOME/var/lib/splunk

❷ mkdir \$SPLUNK_HOME/var/lib/splunk/sysmon

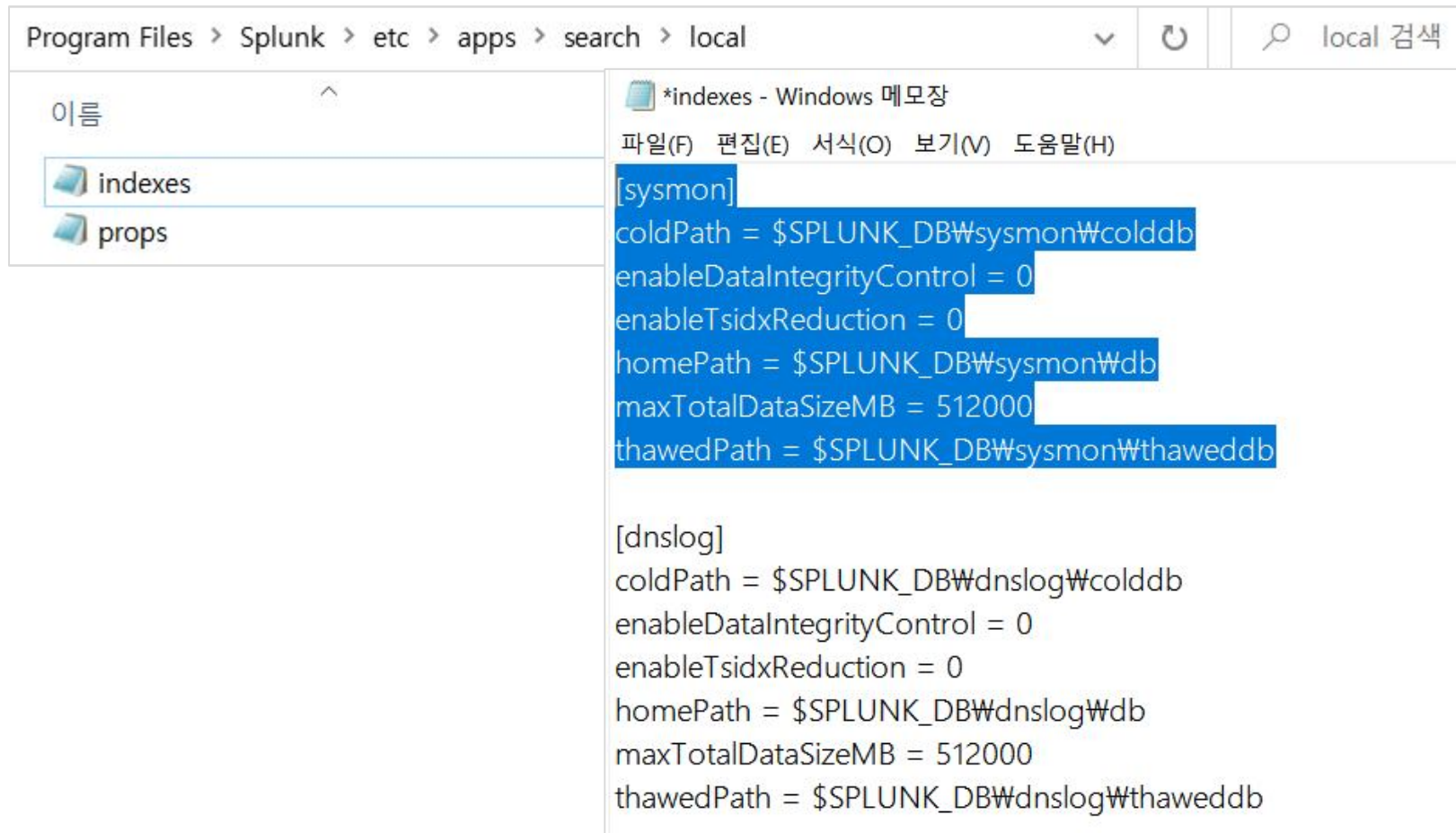
❸ mv sysmon.tgz \$SPLUNK_HOME/var/lib/splunk/sysmon

Program Files > Splunk > var > lib > splunk > sysmon				↻	🔍 sysmon 검색
이름	수정한 날짜	유형	크기		
 sysmon	2020-09-09 오전 9:52	ALZip TGZ File	5,203KB		

❹ tar xvfz sysmon.tgz

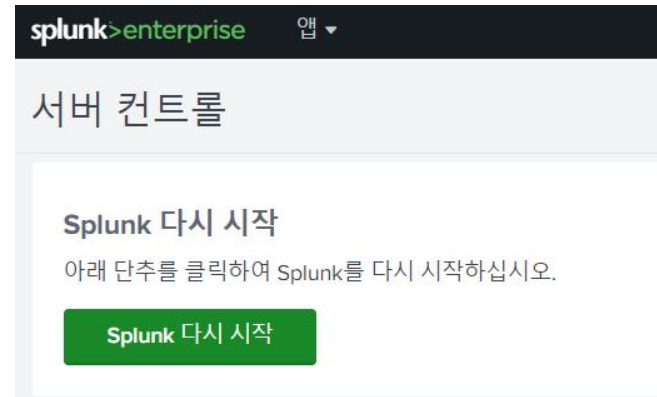
Program Files > Splunk > var > lib > splunk > sysmon			▼
이름	수정한 날짜	유형	
 colddb	2023-01-29 오후 6:04	파일 폴더	
 datamodel_summary	2023-01-29 오후 5:51	파일 폴더	
 db	2023-01-29 오후 6:04	파일 폴더	
 thaweddb	2023-01-29 오후 5:51	파일 폴더	

⑤ indexes.conf 파일을 편집기를 이용해서 sysmon index 관련 환경 설정



⑥ Splunk server 재시작

`$splunk_HOME/bin/splunk restart`



⑦ sysmon 로그 검색

새로운 검색

index=sysmon

✓ 43,784개의 이벤트 (23/01/29 18:05:27.000 이전) 이벤트 샘플링 없음 ▼

이벤트 (43,784) 패턴 통계 시각화

시간 표시줄 형식 지정 ▼ - 축소 + 선택 항목 확대/축소 x 선택 취소

시간 표시줄

리스트 ▼ 형식 페이지당 20개 ▼

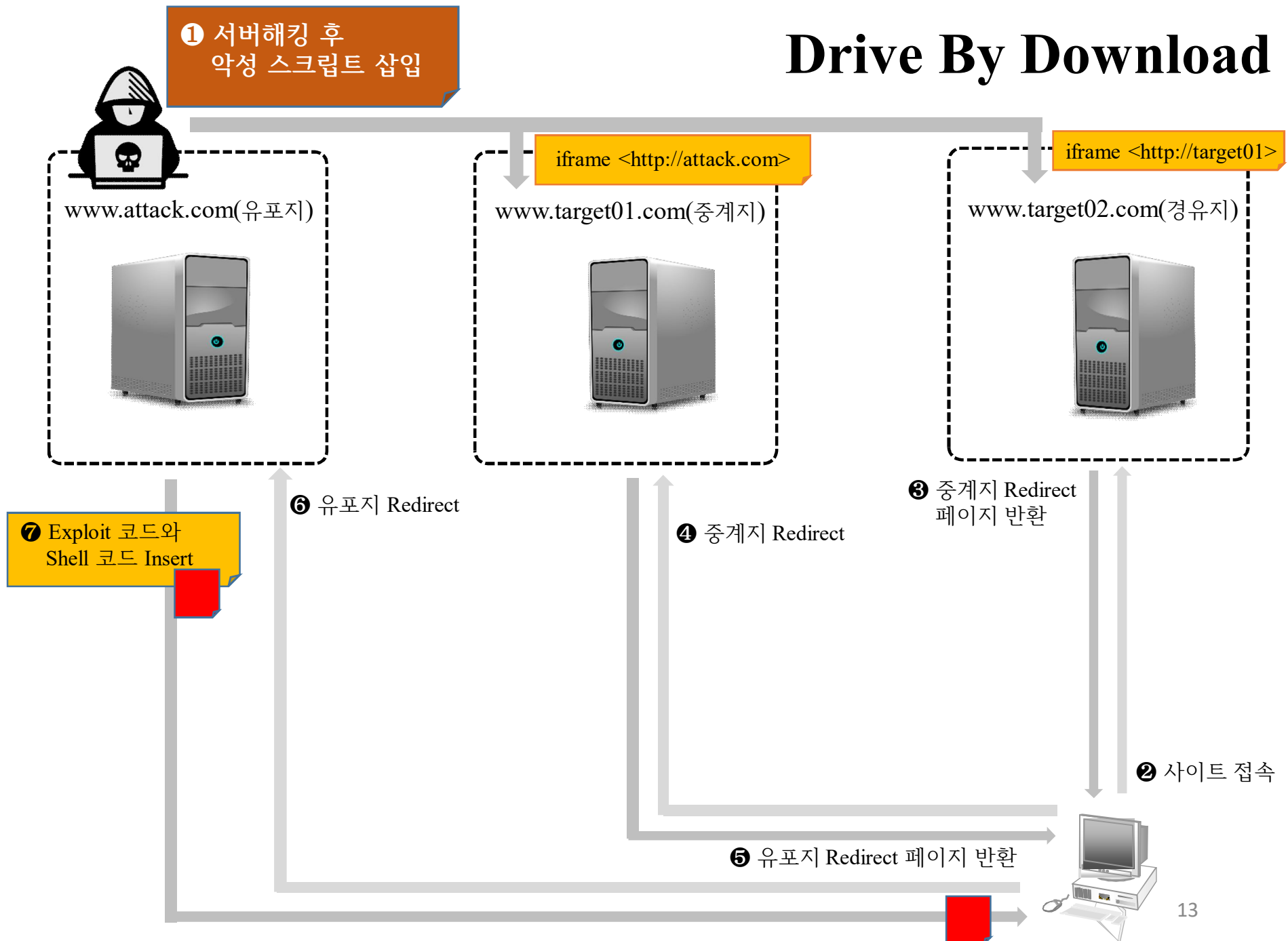
< 필드 숨기기	모든 필드	i	시간	이벤트
선택한 필드		>	20/02/04 22:04:00.000	02/04/2020 10:04:00 PM LogName=Microsoft-Windows-Sysmon/Operational SourceName=Microsoft-Windows-Sysmon EventCode=5 EventType=4 20개 행 모두 표시 host = IEWIN7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational

관심 필드
a collection 4

PC 이상 징후 분석

- ❶ 비정상 폴더에서 exe 파일 실행
- ❷ 파일 실행 후 원본 파일 삭제
- ❸ 실행 후 네트워크 접속 다수 발생
- ❹ 네트워크 Shell 실행

Drive By Download



① 비정상 폴더에서 exe 파일 실행

- 윈도우 실행 파일(시스템폴더) 위치
 - C:\Program Files, C:\Program Files(x86), C:\Windows, C:\Window\system32

- 일반적으로 공격에 사용되는 악성코드는 단독 실행 파일로 동작
 - 시스템 폴더에 설치되지 않음

<<프로그램의 실행 경로를 판단한다면 이상징후를 판별 가능>>

- 인터넷으로 다운로드한 악성코드가 처음부터 시스템 폴더에 복사되지는 않기 때문에
최초 실행 폴더를 기반으로 탐지하는 방법은 유효함
- 악성 코드가 사용자 PC에 다운로드되고 실행이 되었다면 프로세스가 생성되므로 Sysmon
이벤트 코드 1에서 해당 이벤트를 찾을 수 있음

* 백도어 프로그램은 윈도우 정상 파일의 대체로 C:\Windows\System32에 설치되기도 함

```
index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
```

EventCode=1

- EventCode =1 : 프로세스 생성을 의미(exe 파일이 정상적으로 실행되었음을 의미)

```
(CurrentDirectory!="*Program Files*" AND CurrentDirectory!="*system32*")
```

```
(Image!="system32*" AND Image!="*Program Files*" AND Image!="*SysWOW64*")
```

- CurrentDirectory : 실행 파일이 들어있는 디렉터리/ Image 필드 : 폴더와 실행파일명이 저장
- Program Files, System32, SysWOW64 등은 검색에서 제외

```
[ search index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
```

```
EventCode=1
```

```
| rare CurrentDirectory limit=10 showperc=f showcount=f ]
```

- [search] 하위 검색을 나타냄, 2차 검색으로 들어감 (**하위검색을 사용하는 이유? 검색범위줄이기**)
- 시스템 폴더 외에서 실행되고 있는 파일들을 검색
- 악성코드는 소수만이 감염되므로 rare를 이용 (rare 빈도가 낮은 것들을 최상위에 배치(top반대))
- showperc(점유율)과 showcount(점유개수)는 보지 않음(false)

```

index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1
(CurrentDirectory!="*Program Files*" AND CurrentDirectory!="*system32*")
(Image!="system32*" AND Image!="*Program Files*" AND Image!="*SysWOW64*")
[ search index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
  EventCode=1 | rare CurrentDirectory limit=10 showperc=f showcount=f]
| table Image

```

Image ↕
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\notepad.exe
C:\RECYCLE\2.exe
C:\Windows\System32\rundll32.exe
C:\Windows\SoftwareDistribution\Download\Install\AS_Delta.exe
C:\Windows\System32\MpSigStub.exe
C:\Windows\SoftwareDistribution\Download\Install\AS_Base_Patch1.exe
C:\Windows\System32\MpSigStub.exe
C:\Windows\SoftwareDistribution\Download\Install\AS_Engine_Patch_1.1.16600.7.exe
C:\Users\IEUser\Desktop\malsample\CLOP\3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207.exe
C:\Users\IEUser\Desktop\malsample\2017-02-28-Cerber\2017-02-28-Cerber-ryu.exe

휴지통에서 파일을 실행
백신과 같은 보안 제품을 우회하기 위해 공격자들이 자주 사용

② 파일 실행 후 원본 파일 삭제

- 하드 디스크에 저장된 악성코드는 프로세스 상태가 되어야 PC들을 감염시킬 수 있음
- 악성코드 파일 실행 후 원본파일을 디스크에서 삭제해서 분석을 회피하기도 함

*** 프로그램을 실행 후 원본 파일을 디스크에서 삭제하는 행위는 정상 행위 아님**

```
index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1 ParentImage="c:\\windows\\explorer.exe"
```

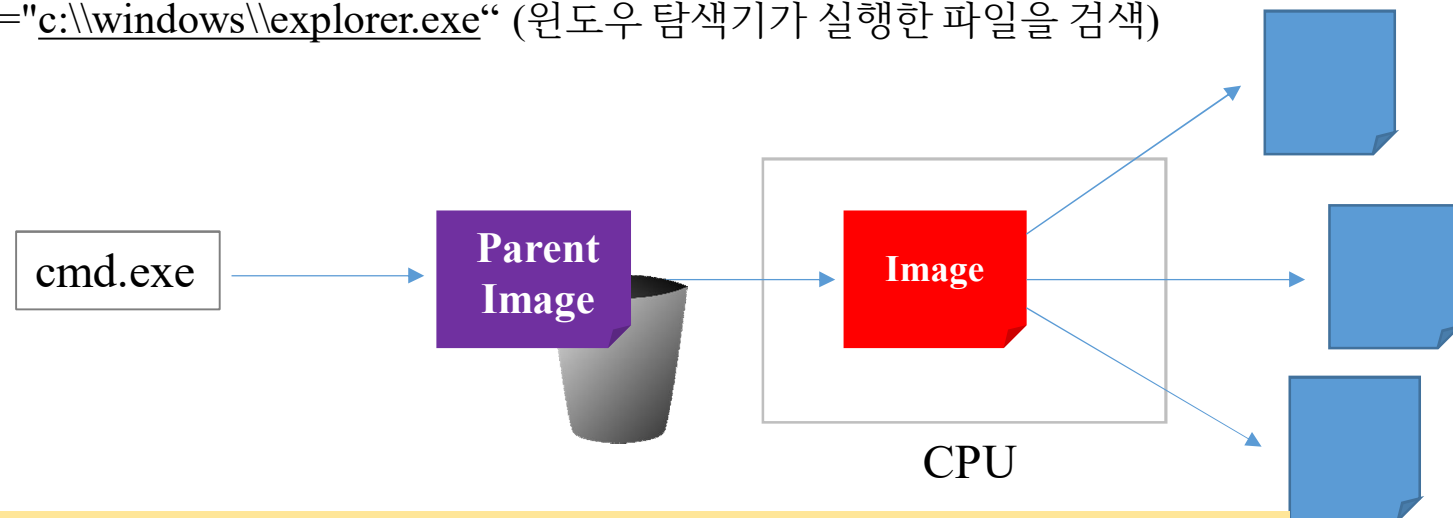
- EventCode = 1 : 프로세스 생성/삭제 관련 로그

실행 파일 스스로 실행 된 것이 아님

```
[ search index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
| where NOT isnull(Image) AND NOT isnull(ParentImage) | search CommandLine="* del *"
```

- Image : 실행 파일 경로

ParentImage="c:\\windows\\explorer.exe" (윈도우 탐색기가 실행한 파일을 검색)



Source program(악성코드)는 실행 중에 자신을 삭제하는 것이 아니라 다른 프로그램을 모두 실행시킨 후(❶) 다른 프로그램을 호출(❷)해서 원본 파일(악성코드)을 삭제한다. 악성코드는 cmd.exe를 호출해서 지우는 방식을 많이 볼수 있다.

```
index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1  
ParentImage="c:\\windows\\explorer.exe"
```

```
[ search index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"  
| where NOT isnull(Image) AND NOT isnull(ParentImage)  
| search CommandLine="* del *"  
| table ParentImage  
| rename ParentImage AS Image ]  
| table Image
```

이벤트 (5)	패턴	통계 (5)	시각화
페이지당 20개 ▼	✎ 형식	미리보기 ▼	
Image ⇅			
C:\Users\IEUser\Desktop\malcode_samples\Intelligent-Mal_100\6c5cd3825936711fe40c774aa38fda22.exe			
C:\Users\IEUser\Desktop\malcode_samples\Intelligent-Mal_100\2ea23e71667b2d9b4a65e829abdd382d.exe			
C:\Users\IEUser\Desktop\malcode_samples\Intelligent-Mal_100\0f45932fc881dede20516e0d6a1a85ad.exe			
C:\Users\IEUser\Desktop\malcode_samples\Intelligent-Mal_100\0f9139868c20b3c0b38ef1b37158b460.exe			
C:\Users\IEUser\Desktop\malcode_samples\Intelligent-Mal_100\0f45932fc881dede20516e0d6a1a85ad.exe			

③ 실행 후 네트워크 접속 다수 발생

- 다른 과다 접속들을 유발하는 트래픽 프로그램 검색

```
index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"  
EventCode=1 (Image!="C:\\windows*" AND Image!="*Program Files*")
```

- 실행 경로가 아닌 곳에서 실행되는 프로세스들을 검색

```
[ search index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"  
EventCode=3 (DestinationIp!="10.0.0.0/8" AND DestinationIp!="172.16.0.0/12" AND  
DestinationIp!="192.168.0.0/16")
```

- EventCode=3에서 (네트워크 정보를 가진로그) 인터넷 접속만을 대상으로 검색한다면
목적지 주소가 사설주소가 아닌 결과만 검색

```
| stats count(DestinationIp) AS total_count dc(DestinationIp) AS uniq_count by Image
```

```

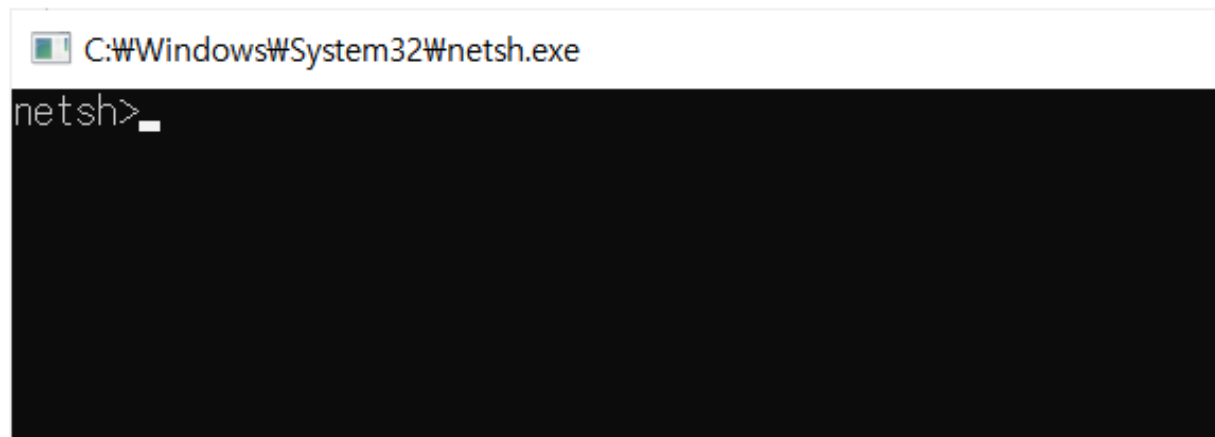
index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1
(Image!="C:\\windows*" AND Image!="*Program Files*")
[ search index=sysmon sourcetype="WinEventLog:Microsoft-Windows-
Sysmon/Operational" EventCode=3
  (DestinationIp!="10.0.0.0/8" AND DestinationIp!="172.16.0.0/12" AND
DestinationIp!="192.168.0.0/16")
  | stats count(DestinationIp) AS total_count dc(DestinationIp) AS uniq_count by Image
  | where total_count > 50 OR uniq_count > 20
  | table Image]
|table Image

```

이벤트 (2) 패턴 <u>통계 (2)</u> 시각화		
페이지당 20개 ▼ ✎ 형식 미리보기 ▼		
ParentImage ↕	Image ↕	CommandLine ↕
C:\Users\IEUser\AppData\Local\Temp\csrss.exe	C:\Windows\System32\netsh.exe	netsh firewall add allowedprogram "C:\Users\IEUser\AppData\Local\Temp\csrss.exe" "csrss.exe" ENABLE
C:\Users\IEUser\AppData\Local\Temp\csrss.exe	C:\Windows\System32\netsh.exe	netsh firewall add allowedprogram "C:\Users\IEUser\AppData\Local\Temp\csrss.exe" "csrss.exe" ENABLE

④ 네트워크 셸 실행

- netsh.exe
 - 현재 실행 중인 컴퓨터의 네트워크 구성을 표시하거나 수정할 수 있는 명령줄 스크립팅 유틸리티
 - 관리자는 netsh을 이용하여 자동 스크립트를 구성하고 배포



```
index=sysmon sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational"
```

```
EventCode=1
```

```
| where match(Image, "netsh.exe$")
```

```
| where NOT isnull(ParentImage)
```

```
| table ParentImage, Image, CommandLine
```

이벤트 (2)	패턴	통계 (2)	시각화
페이지당 20개 ▼	형식	미리보기 ▼	
ParentImage ↕	Image ↕	CommandLine ↕	
C:\Users\IEUser\AppData\Local\Temp\csrss.exe	C:\Windows\System32\netsh.exe	netsh firewall add allowedprogram "C:\Users\IEUser\AppData\Local\Temp\csrss.exe" "csrss.exe" ENABLE	
C:\Users\IEUser\AppData\Local\Temp\csrss.exe	C:\Windows\System32\netsh.exe	netsh firewall add allowedprogram "C:\Users\IEUser\AppData\Local\Temp\csrss.exe" "csrss.exe" ENABLE	