KDFS 2017 분석보고서

팀원 조현호, 김용현

목 차

그림 목차

표 목차

I. 개요

윈도우 이벤트 로그는 시스템, 보안, 어플리케이션 등 시스템 상태 및 사용자의 행위에 따라 발생하는 다양한 이벤트가 일정한 형식으로 기록되는 로그를 말한다. 또한 윈도우 운영체제의 구성요소 뿐만 아니라, 안티바이러스 소프트웨어와 같은 Third-Party 어플리케이션에서도 Windows API를 사용하여 이벤트 로그를 기록할 수 있다. 이렇게 다양한 종류의 로그들이 저장되는 특성 상, 윈도우 이벤트 로그는 침해사고, 기업보안 감사 등 다양한 포렌식 관점에서 활용할 수 있으며, 디지털 포렌식 수행 시 간과해서는 안 될 중요한 아티팩트(Artifact)[1] 중 하나로 꼽힌다.

윈도우 이벤트 로그는 미리 정의된 이벤트 항목이 자동으로 기록되지만, 모든 이벤트가 분석에 활용되는 것은 아니다. 특히 가장 많이 활용되는 System, Security 로그는 실제 분석에 활용되는 이벤트보다 활용되지 않는 이벤트가 대부분이다. 그렇기 때문에 각 상황별로 분석에 필요한 이벤트를 선별하여 분석하는 것이 필요하다. 또한 USB 사용 기록이나 원격 접속 기록 등 특정 행위에 대한 증거 자료로 활용할 수 있는 어플리케이션 이벤트가 많기 때문에, 이러한 이벤트들을 사전에 파악해야만 실제 분석에서 효과적인 분석을 할 수 있을 것이다.

본 분석보고서는 총 5장 및 부록으로 구성되어 있다. 1장은 본 분석 보고서의 개요에 대한 내용이 담겨 있으며, 2장은 윈도우 이벤트 로그 포맷인 EVTX 포맷과 구성요소에 대해 설명한다. 3장과 4장에서는 제시된 각 시나리오에 대한 이벤트 분석 절차 및 방법과 각 이벤트 구성요소에 대한 상세 분석 내용을 담고 있다. 마지막으로 5장과 부록에서는 보고서 결론과 이벤트 감사 설정 이벤트 사용 설정 등 분석에 필요한 부가적인 설정 방법에 대해 설명한다.

[1] 운영체제나 어플리케이션을 사용하면서 생성된 흔적

II. EVTX 파일 구조

1. EVTX 포맷 개요

Windows XP 이전까지는 바이너리 기반의 EVT 포맷이 사용되었으며, Windows Vista 이후로 현 시점 까지 EVTX 포맷이 사용되고 있다. EVT 포맷에서는 System, Security, Application 로그 단 3개 항목에 모든 정보를 저장하며, 저장되는 정보 또한 비교적 제한적이다. EVTX 포맷의 경우 System.evtx, Security.evtx, Application.evtx 뿐만 아니라 각 용도별 개별 파일에 로그를 저장하며, 비교적 유연한 자료구조와 XML 기반 데이터 저장 방식을 채택하여 보다 다양하고 넓은 범위의 데이터를 저장하고 있다.

본 EVTX 파일 구조의 주요 내용들은 오픈소스 타임라인 분석도구인 Plaso(Log2Timeline)의 윈도우 이벤트 로그(EVTX) 처리 라이브러리로도 사용되고 있는 Joachim Metz의 libevtx(https://github.com/libyal/libevtx)의 문서[2] 를 인용하여 작성하였다.

2. EVTX 파일

Windows Vista 이후로 사용되는 이벤트 로그 EVTX 파일들은 별도의 설정의 변경이 없는 한 %SystemRoot%₩system32₩winevt₩Logs 폴더에 저장된다. Windows XP 이전의 EVT와는 달리, 각 이벤트 로그들은 System.evtx, Security.evtx, Application.evtx 및 다수의 파일에 로그가 저장된다.

이러한 EVTX 파일은 4,096 바이트의 파일 헤더와, 65,535 바이트로 구성된 청크(chunk) 하나 이상으로 구성되어 있다.

File Header (4,096 Bytes)
Chunk 0 (65,535 Bytes)
Chunk 1 (65,535 Bytes)
...
Chunk n (65,535 Bytes)

1 EVTX File

[2] Joachim Metz - Windows XML Event Log (EVTX) format : https://github.com/libyal/libevtx/blob/master/documentation/Windows%20XML%20Event%20Log%20(EVTX).asciidoc

3. 파일 헤더

EVTX 파일 헤더는 4,096바이트의 바이너리로 구성되어 있으며, 아래와 같은 구조를 가지고 있다.

File Header (4,096 Bytes)
Chunk 0 (65,535 Bytes)
…
Chunk n (65,535 Bytes)

->

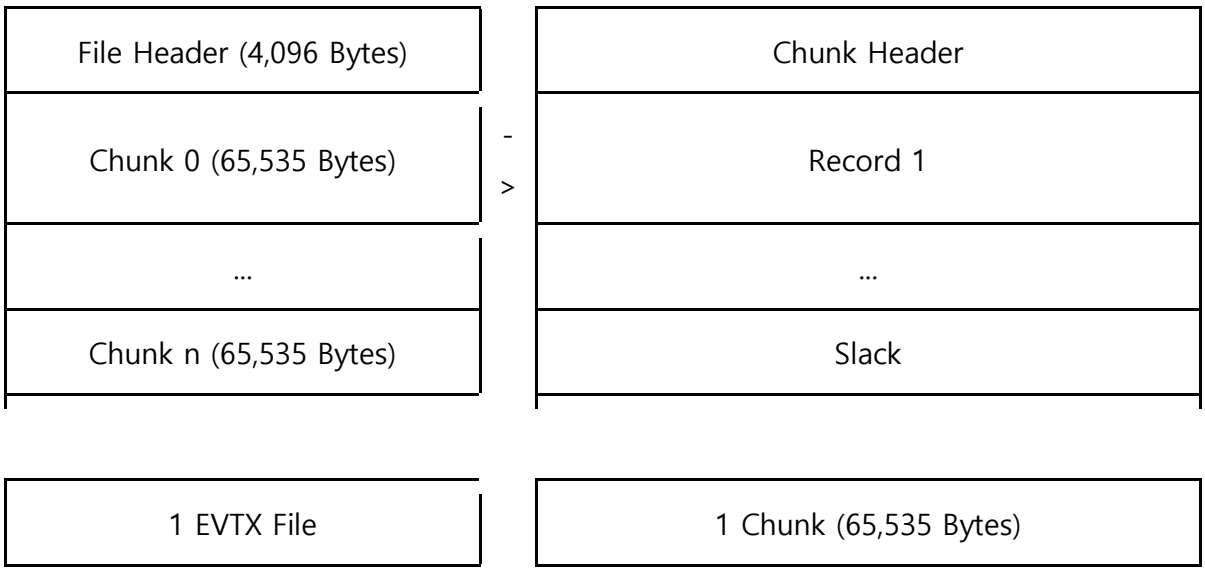
오프셋	사이즈	값	설명
0	8	ElfFile₩x00	EVTX File Signature
8	8		First Chunk Number
16	8		Last Chunk Number
24	8		Next Record Identifier
32	4	128	Header Size
36	2	1	Minor Version
38	2	3	Major Version
40	2	4,096	Header Block Size (or chunk data offset)
42	2		Number of chunks
44	76		Unknown(Empty Values)
120	4		File flags *
124	4		Checksum CRC32 of the first 120 bytes of the file header
128	3,968		Unknown(Empty Values)

1 EVTX File	1 File Header (4,096 Bytes)

* 파일 플래그는 0x0001인 경우 Dirty, 0x0002인 경우 Full 상태를 나타낸다

4. 청크

각 청크는 65,535 Bytes의 바이너리로 구성되어있으며, 각 청크는 청크 헤더 및 하나 이상의 이벤트 레코드를 가진다.



5. 청크 헤더

청크 헤더는 각 청크에 대한 위치정보 및 식별자, 체크섬 등의 데이터를 담고 있다.

Chunk Header
Record 1
Record 2
Record 3
...
Record n
Slack

->

오프셋	사이즈	값	설명
0	8	ElfChnk₩x00	Chunk Header Signature
8	8		First Event Record Number
16	8		Last Event Record Number
24	8		First Event Record Identifier
32	4		Last Event Record Identifier
40	4	128	Header Size
44	4		Last Event Record Data Offset
48	4		Free Space Offset
52	4		Event Record Checksum
56	64		Empty Value
120	4		Flags
124	4		Checksum

1 Chunk (65,535 Bytes)

1 Chunk Header

6. 이벤트 레코드

이벤트 레코드는 하나의 이벤트 항목을 말한다. 하나의 이벤트 레코드는 이벤트 시그니처 및 사이즈 정보, 레코드 식별자, 기록일시, 이벤트 데이터(바이너리 XML), 백업 사이즈 수를 포함한다.

Chunk Header		오프셋	사이즈	값	설명
Record 1	->	0	4	₩x2a₩x2a₩x00₩x00	Event Record Signature
Record 2		4	4		Size
Record 3		8	8		Event Record Identifier
...		16	8		Datetime
Record n		24	가변		Event Data (Binary XML)
Slack		가변	4		Backup of Size

1 Chunk (65,535 Bytes)	1 Event Record

7. 이벤트 데이터

이벤트의 주요 내용을 담고 있는 이벤트 데이터는 Binary XML 형태로 구성되어 있다. 이벤트 Provider 및 이벤트 ID 별 용도가 정해져 있는 만큼 그 이벤트를 구성하는 태그 및 속성들의 표현 방법도 상이하다. 그러나 모든 이벤트 데이터의 루트 태그(Event 태그) 아래에는 System 태그가 존재하며, 이벤트 로그 분석 시 System 태그를 통해 알 수 있는 다음과 같은 항목들을 선별 기준으로 삼아 필요한 이벤트만을 선별한 후 분석하게 된다.

System 태그 이후로는 일반적으로 EventData 태그 또는 UserData 태그가 존재하며, 해당 태그를 통해 해당 이벤트에서 다루고자 하는 주요 정보를 알 수 있다.

태그	용도	예시
EventID	이벤트 ID	텍스트 값 : 307
Computer	컴퓨터 이름	텍스트 값 : Computer
Provider	Provider 정보	Name 속성 : Microsoft-Windows-PrintService Guid 속성 : {747EF6FD-E535-4D16-B510-42C90F6873A1}
Channel	채널	텍스트 값 : Microsoft-Windows-PrintService/Operational
TimeCreated	이벤트 기록일시 (UTC)	SystemTime 속성 : 2017-10-18T13:08:51.086271300Z

<표 1> System 태그 아래의 주요 태그

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
 <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4689</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>13313</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2017-10-22T03:37:22.523064800Z" />
  <EventRecordID>180559</EventRecordID>
  <Correlation />
  <Execution ProcessID="4" ThreadID="5552" />
  <Channel>Security</Channel>
  <Computer>UNKNOWN</Computer>
  <Security />
 </System>
 <EventData>
  <Data Name="SubjectUserSid">S-1-5-21-117826221-3775045649-4029944430-1001</Data>
  <Data Name="SubjectUserName">Unknown</Data>
  <Data Name="SubjectDomainName">UNKNOWN</Data>
  <Data Name="SubjectLogonId">0x36f71</Data>
  <Data Name="Status">0x0</Data>
  <Data Name="ProcessId">0x1170</Data>
  <Data Name="ProcessName">C:₩Windows₩System32₩notepad.exe</Data>
 </EventData>
</Event>
```

이벤트 로그 예시

III. 시나리오별 분석절차 및 방법

악성코드 분석, 기업 보안감사 2가지 시나리오에 대한 분석을 위해 챌린지에서 제시한 필수 이벤트 6개와 추가 이벤트 10개를 포함하였다. 각 수집 이벤트는 단일 시나리오에 한정되지만, 일부 이벤트는 2가지 시나리오를 분석하는데 모두 이용될 수 있다.

분석 이벤트	악성코드	기업보안	시나리오 항목	
			악성코드	기업보안
로그인/로그오프	**O**	**O**	초기침투	근태 관리
PC 시작 종료		**O**		근태 관리
응용프로그램 사용 정보	**O**	**O**	초기침투, 악성행위	비인가 프로그램 사용
윈도우 서비스 정보	**O**	**O**	연결유지	비인가 프로그램 사용
외부장치 연결정보		**O**		기밀정보 유출
시스템 시간 변경 정보	**O**	**O**	악성행위	근태 관리
윈도우 이벤트 초기화	O		악성행위	
자동실행	O		연결유지	
윈도우 업데이트	O		초기침투	
윈도우 방화벽	O		거점확보	
원격접속 이력	O		초기침투	
어플리케이션 에러	O		초기침투	
소프트웨어 설치		O		비인가 프로그램 사용
문서 인쇄		O		기밀정보 유출
윈도우 계정관리	O		연결유지	
무선네트워크 연결		O		기밀정보 유출

<표 2> 분석 이벤트 별 적용 시나리오 항목

Case #1 악성코드 행위 분석

1. 시나리오

디지털 포렌식에 관심이 많은 심기호군은 인터넷 쇼핑을 하던 중에 갑자기 컴퓨터가 느려지는 증상을 느꼈다. 그래서 안티바이러스 소프트웨어를 이용해서 검사를 한 결과, 악성으로 탐지된 파일이 발견되었다.

2. 이벤트 로그 분석방법

본 분석보고서에서는 악성코드 유입에서부터 완료까지의 악성코드 라이프 사이클을 **①초기 침투, ②거점확보, ③권한상승, ④악성행위, ⑤연결유지**, 총 5개 단계로 분류하고, 각 단계별로 악성코드 감염 시 발생하는 다양한 행위를 확인하기 위한 윈도우 이벤트 분석방법을 제시한다.

구분	이벤트 항목	목적
① 초기침투	응용프로그램 사용정보	악성코드의 실행여부 및 감염원인 확인
	어플리케이션 에러	악성코드의 감염원인(취약 프로세스) 확인
	윈도우 서비스 정보	PSExec와 같은 툴에 의한 원격 명령 실행 여부 식별
	로그온/로그오프	무단 원격접속에 의한 악성코드 감염여부 탐지
	원격접속(RDP) 기록	
	윈도우 업데이트	누락된 윈도우 업데이트 항목 식별
② 거점확보	윈도우 방화벽	악성코드에 의한 방화벽 정책 변경 여부 확인
③ 권한상승	로그온/로그오프	관리자권한 로그인 성공, 실패 이력 확인
	어플리케이션 에러	권한상승 익스플로잇에 의한 흔적 확인
④ 악성행위	응용프로그램 사용정보	악성코드 실행원인 또는 공격자 침입 이후 악성행위 확인
	시스템 시간 변경	안티포렌식 목적의 시스템 환경 변경
	윈도우 이벤트 초기화	안티포렌식 목적의 흔적 제거

⑤ 연결유지	자동실행 등록	악성코드의 지속 실행을 위한 자동실행 등록 확인
	윈도우 서비스	악성코드의 지속 실행을 위한 서비스 등록 확인
	윈도우 계정관리	공격자의 백도어 계정 등록 여부 확인

2.1. 초기침투 단계

인터넷 쇼핑을 하던 중 느려진 정황 상, Drive-By-Download[3] 에 의한 감염일 가능성이 높을 것으로 추정된다. 그러나 원격접속에 의한 감염이나 인터넷 쇼핑 이전에 발생한 스피어 피싱, 내부전파에 의한 감염 등의 요인들도 배제할 수 없다. 악성코드 감염 침해사고에서는 최초 감염 경로를 확인하는 것이 가장 중요하다. 그 이유는 감염 경로를 빠르게 파악하여 감염 원인을 차단함으로써 재감염을 억제하고, 악성코드에 감염되는 PC가 추가적으로 발생하지 않도록 해야 하기 때문이다. 악성코드에 감염되는 경로는 매우 다양하며, 본 분석보고서에서는 크게 4가지로 분류하여 감염 원인에 대해 가정하였다.

항목명	용도
윈도우 업데이트 기록	누락된 윈도우 업데이트 항목 식별
응용 프로그램 사용정보	악성코드의 실행여부 및 감염원인 추정
어플리케이션 에러	악성코드의 감염원인(취약 프로세스) 추정
윈도우 서비스 정보	PSExec와 같은 툴에 의한 원격 명령 실행 여부 식별
원격접속(RDP) 기록	무단 원격접속에 의한 악성코드 감염여부 탐지
로그온/로그오프	

<표 3> 초기침투 단계에서 활용할 수 있는 윈도우 이벤트

2.1.1 취약점에 의한 악성코드 감염

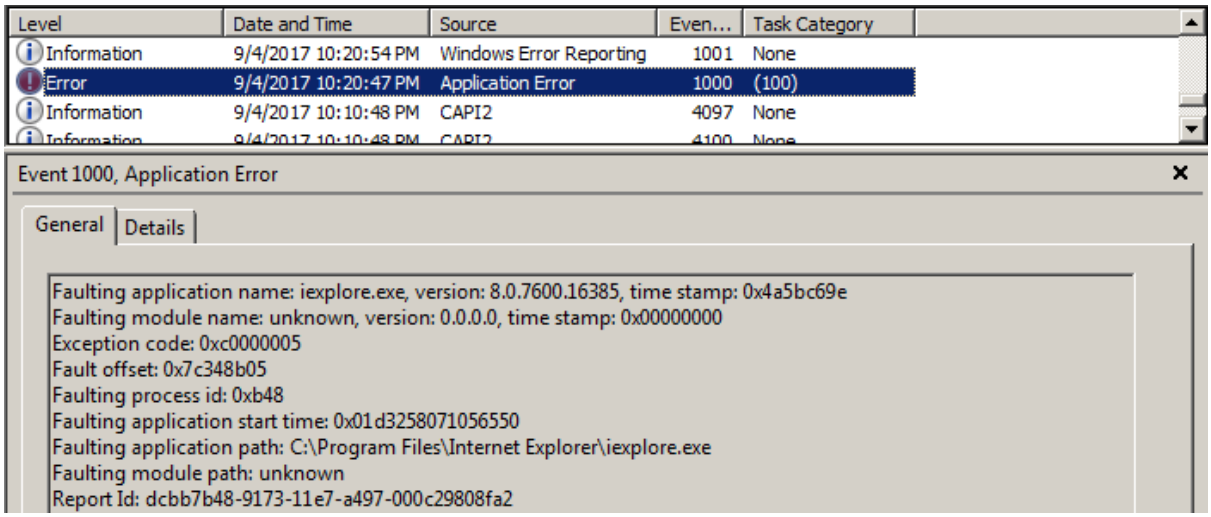
2.1.1.1 Drive By Download

Drive-By-Download의 경우, 사용된 취약점의 유형에 따라 관련 증적도 다르게 나타난다. Internet Explorer 자체의 취약점인 경우, Windows 업데이트 항목을 체크하여 누락된 업데이트 항목을 체크하면, 해당 시스템에 적용 가능한 취약점을 식별할 수 있으며 앞으로의 조사/분석의 방향을 잡는 데 도움을 줄 수 있다.

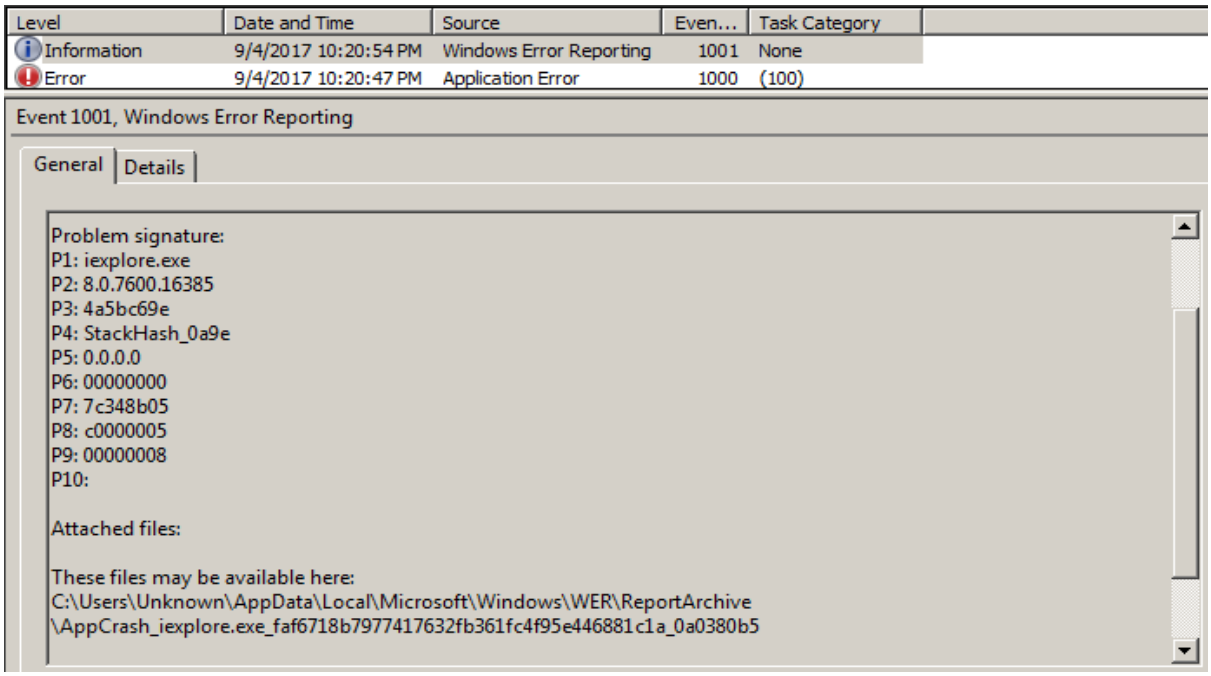
[3] 웹 페이지에 악의적인 스크립트를 삽입하고, 해당 페이지에 접근한 사용자의 동의/인지 없이 악의적인 소프트웨어를 다운로드, 실행하도록 하는 기법

Drive-By-Download에 이용되는 취약점은 메모리 핸들링 취약점을 이용하는 사례가 많으며, 공격 대상 시스템에 맞게끔 정교하게 작성되지 않은 경우 어플리케이션 에러 관련 이벤트 로그가 기록될 수 있다.

아래는 CVE-2012-1889(MS12-043) 취약점 공격 시도에 실패, 어플리케이션 에러가 발생한 후 이벤트 로그에 기록된 항목 예시이다. 이벤트 ID 1000(Application Error) 및 1001(Windows Error Reporting)이 확인된다.

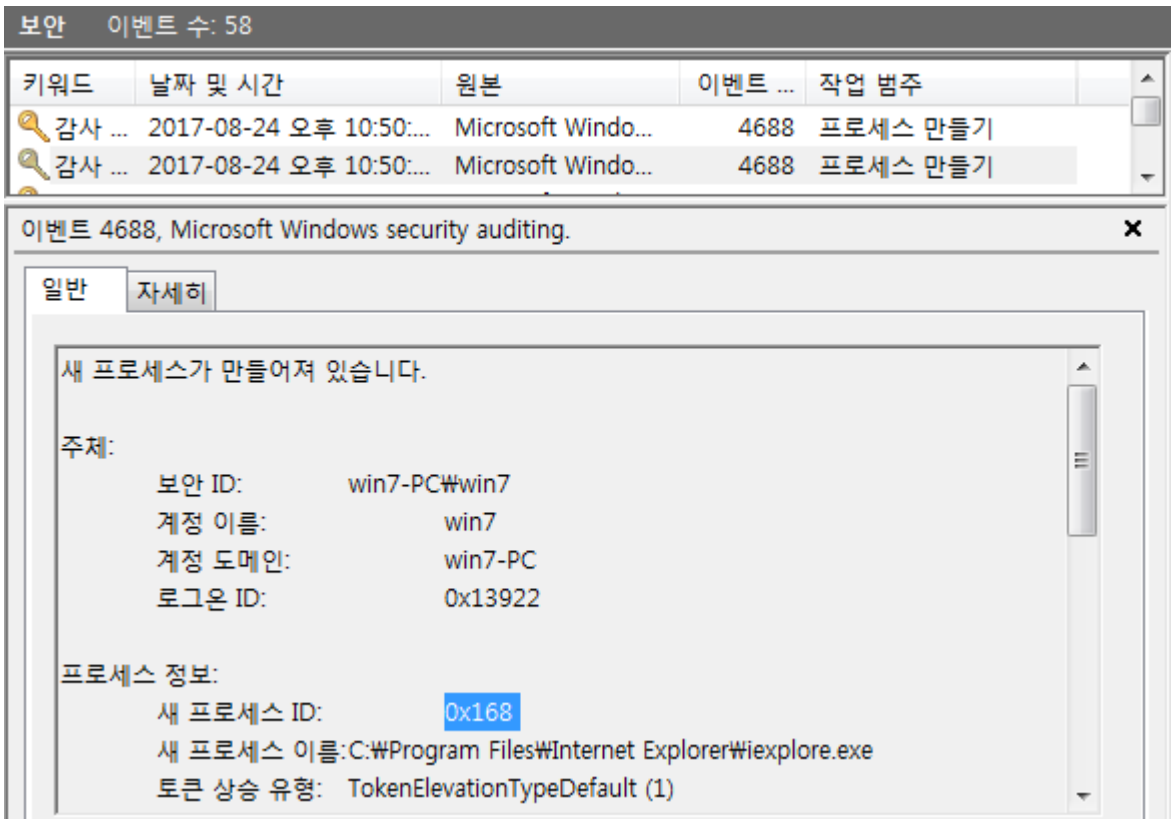


<그림 1> 익스플로잇 실패에 의한 어플리케이션 에러(1000) 이벤트



<그림 2> 익스플로잇 실패에 의한 윈도우 에러 리포팅(1001) 이벤트

CVE-2014-6332(MS14-064) 취약점 테스트 결과, 특별한 이벤트 로그는 남지 않았으며 미리 설정해둔 프로세스 추적감사 기능을 통해 iexplore.exe(Internet Explorer)를 부모 프로세스로 하여 calc.exe(계산기) 프로세스가 실행되는 것을 확인할 수 있었다. 이처럼 브라우저 등을 부모 프로세스로 하여 생성되는 프로세스 중 일반적인 상황이 아닌 경우를 의심해볼 수 있다.



<그림 3> 익스플로러 프로세스 생성 이벤트

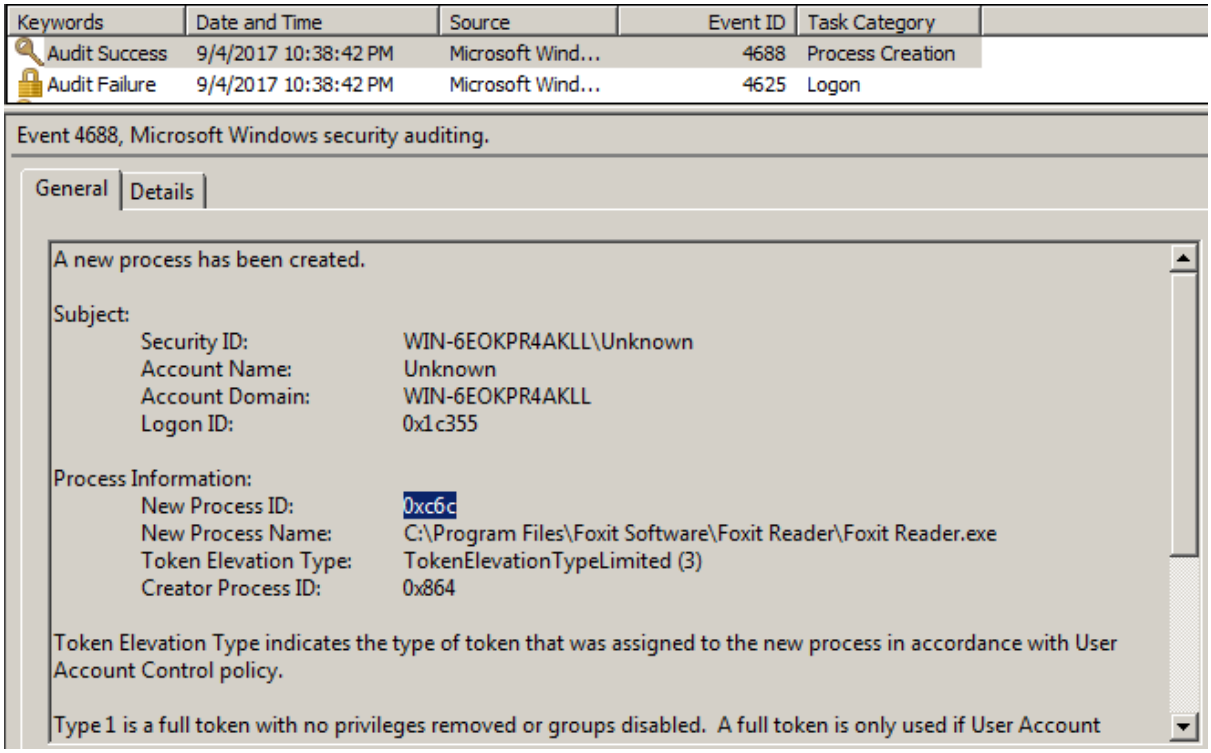
<그림 4> 익스플로잇에 의한 계산기 프로세스 생성 이벤트(Drive By Download)

자바 취약점을 사용하는 익스플로잇에 의한 공격의 경우, java.exe 실행 이벤트를 발견할 수 있으나, 자바 익스플로잇에 의해 침해가 이루어졌는지의 여부는 java.exe 이벤트 이후 발생한 악성 프로세스의 실행 이벤트, 전후로 발생한 인터넷 접속기록, 임시파일 등을 추가로 활용하여 식별하여야 한다.

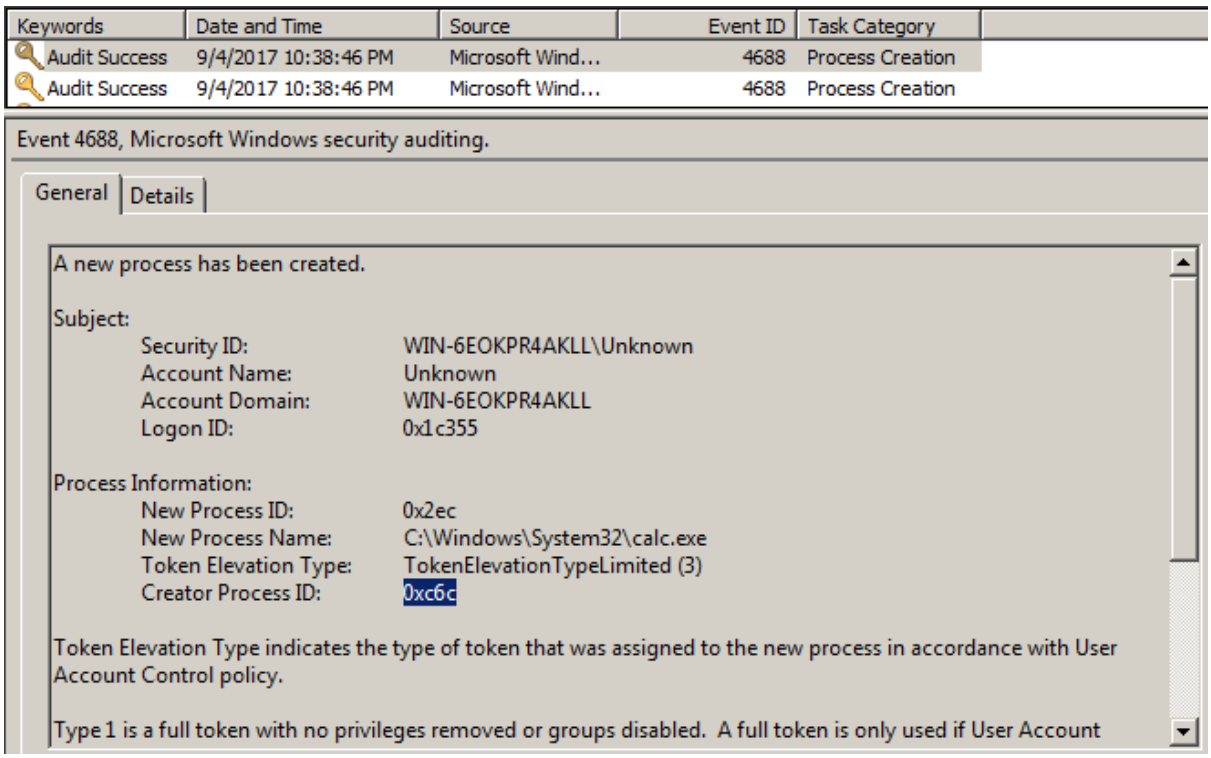
2.1.1.2 문서편집기/뷰어 취약점

문서편집기, 뷰어 취약점도 대상 소프트웨어의 메모리 핸들링 취약점을 이용하는 케이스가 많으며, 공격 대상 시스템에 맞게끔 정교하게 작성되지 않은 경우 어플리케이션 에러 관련 이벤트 로그가 기록될 수 있다.

앞서 소개한 브라우저 취약점 악용 사례와 동일하게, 문서 편집기나 뷰어 등을 부모 프로세스로 하여 생성되는 프로세스 중 일반적인 상황이 아닌 경우를 의심해볼 수 있다.



<그림 5> 문서편집기 프로세스 생성 이벤트



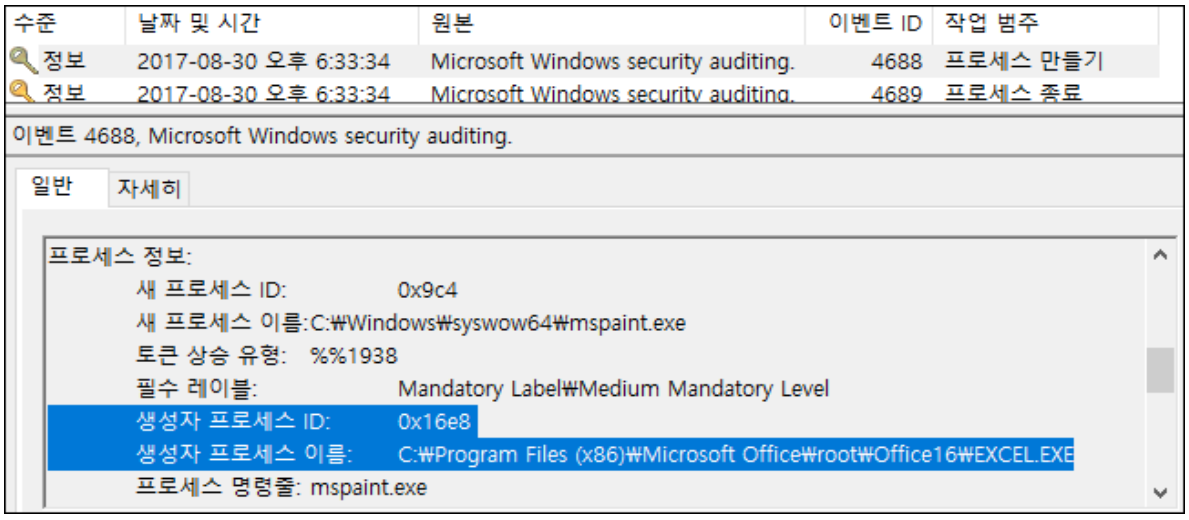
<그림 6> 문서편집기 프로세스 생성 후 익스플로잇에 의한 계산기 프로세스 생성 이벤트

2.1.2. 오피스 매크로에 의한 감염

최근에는 마이크로소프트 오피스 제품군의 매크로 기능을 활용한 악성코드 유포도 증가하는 추세이다. 이러한 매크로의 실행과 관련한 직접적인 이벤트 로그는 발생하지 않는다. 또한 매크로를 이용한 악성코드가 메모리 조작 관련 취약점을 악용하는 경우는 거의 없기 때문에, 어플리케이션 에러 이벤트가 발생할 여지도 거의 없다.

그러나 상당수의 경우 매크로 코드 내에서 악성 바이너리를 다운로드하거나 드랍(Drop)한 후 실행시키는 동작을 수행하기 때문에, 문서 편집기나 뷰어 등을 부모 프로세스로 하여 생성되는 프로세스 중 일반적인 상황이 아닌 경우를 의심해볼 수 있다. 이러한 이벤트 전후로 발생한 최근 문서, 점프리스트, 파일시스템 타임라인 등을 활용하여 악성문서를 식별할 수 있다.

그러나 프로세스 생성/종료 이벤트는 프로세스 추적 감사 기능을 활성화해야만 기록되므로 사고 발생 이전에 해당 기능을 활성화할 필요가 있다.



<그림 7> 오피스 매크로에 의한 mspaint.exe(그림판) 실행

2.1.3. 내부전파 기법이 이용된 악성코드 감염

동일 네트워크 내 타 PC가 침해되어 악성코드 유포에 이용되는 경우도 종종 발견된다. 최근에는 PsExec와 같은 정상적인 원격 관리용 도구를 활용하여 내부 네트워크로 전파되는 악성코드도 발견되고 있기 때문에, 내부전파 기법의 이용 여부도 점검할 필요가 있다.

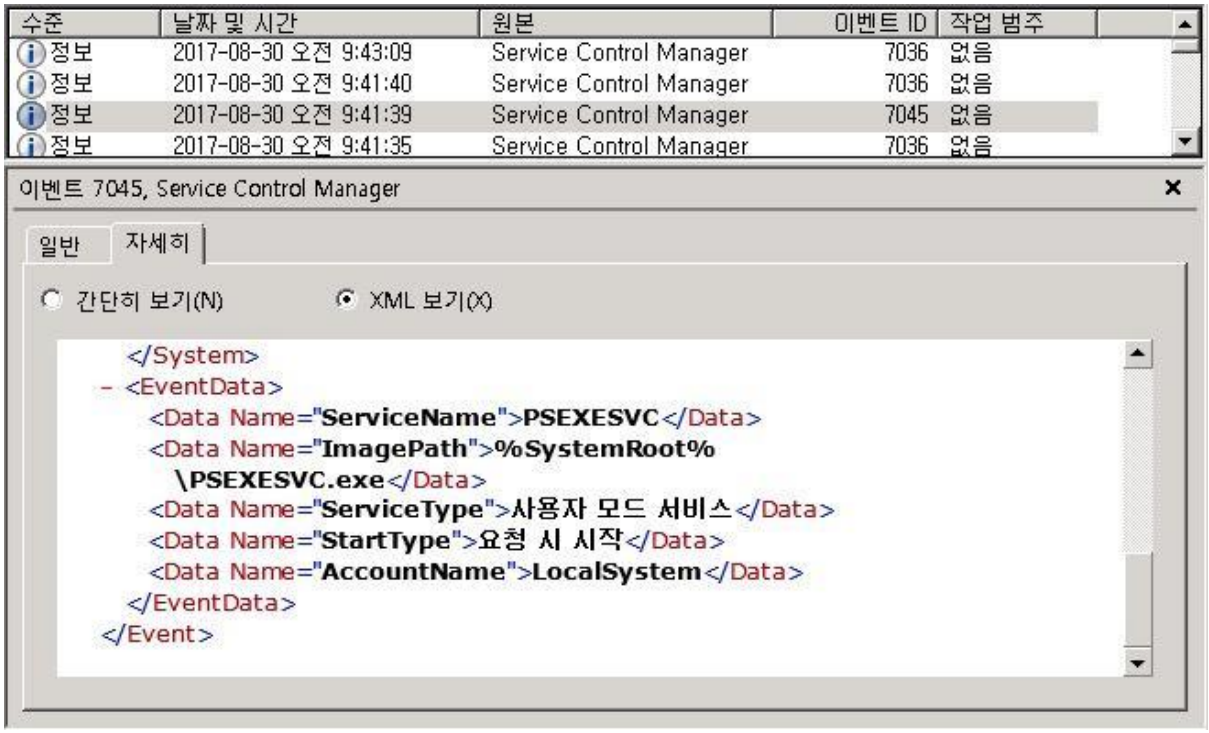
이러한 공격 툴 시도의 상당수는 로그온 이벤트 및 프로세스 생성 이벤트 등을 통해 확인할 수 있으며, 경우에 따라 서비스 등록 이벤트를 통해 확인할 수 있는 경우도 있다.

또한 Windows OS의 취약점을 이용한 기법이 존재하므로, Windows 업데이트 항목을 체크하여 누락된 업데이트 항목을 식별할 필요가 있다.

2.1.3.1. PSExec

PSExec는 일반적인 관리용 도구이나, 악성코드 및 공격자에 의한 내부전파에도 빈번하게 악용되고 있다. PSExec를 이용하여 원격 명령을 수행할 시, 대상 호스트에 NTLM 인증을 수행하게 되며, 이에 따라 로그온 이벤트인 이벤트 ID 4624(Microsoft-Windows-Security-Auditing)가 발생한다. (로그온 타입 3, 로그온 프로세스 NtLmSsp, 패키지명 NTLM V2)

또한 PSExec의 기본 옵션을 변경하지 않고 원격 명령을 수행하였다면, 피제어 시스템에 'PSEXESVC' 서비스가 추가되며, 이에따라 이벤트 ID 7045(Service Control Manager)를 가지는 이벤트 로그가 기록된다.



<그림 8> 원격 명령 수행에 의한 PSEXESVC 서비스 등록 이벤트

이외에도 기본적으로 활성화되어있지 않은 이벤트 로그 항목(5140 : $ADMIN, 4688 : PSEXESVC.EXE 프로세스 생성)을 통해서도 PSExec의 시도를 확인할 수 있다.

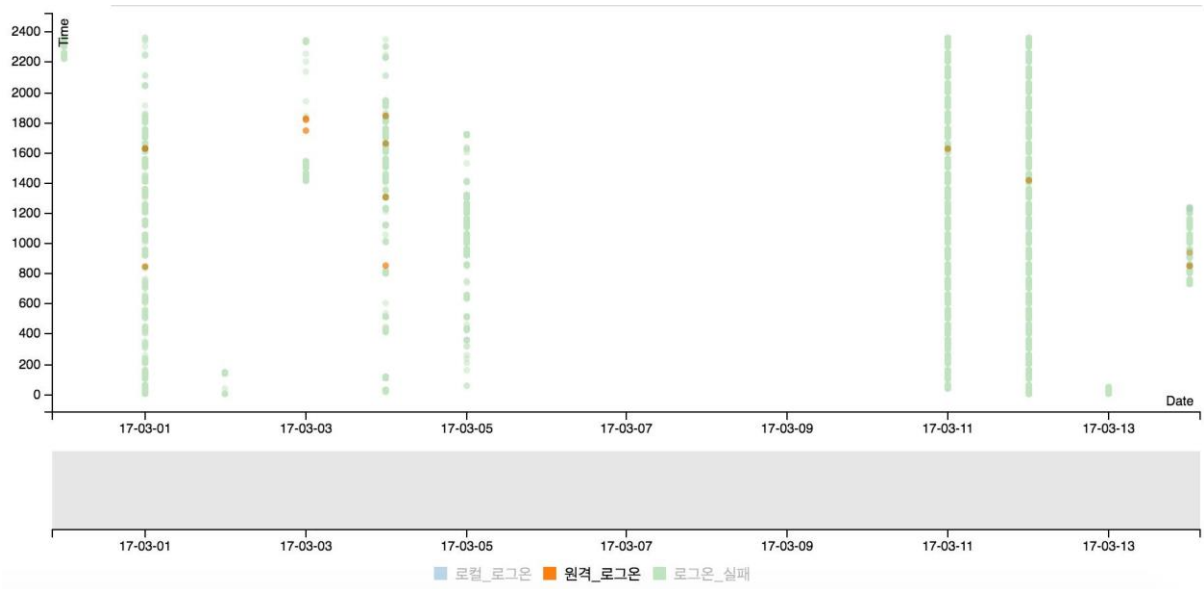
항목	특징
로그온	로그온 타입 3 로그온 프로세스 NtLmSsp 패키지명 NTLM V2
서비스	'PSEXESVC' 서비스 (기본 설정을 변경하지 않고 사용할 시)

<표 4> PSExec 증적

2.1.4. 원격접속(RDP)을 이용한 악성코드 감염

Apocalypse와 같은 랜섬웨어는 공격자가 접속 가능한 서버를 대상으로 RDP Bruteforce 공격을 수행하고, 침입에 성공하였을 시 대상 시스템에 접속하여 랜섬웨어를 수동으로 감염시키기도 한다. 이러한 원격접속 관련 이벤트 로그를 검토하여 침입여부를 확인할 수 있다. 그러나 로그인 실패 시도는 로그인 실패 감사를 설정하여야만 기록되며, 실패 감사를 설정하지 않은 상태에서 RDP Bruteforce 여부를 추정하기 위해서는 RDP 로그인 성공 이벤트와 Microsoft-Windows-TerminalServices-RemoteConnectionManager / 261 의 갯수를 통해 추정하는것이 최선으로 보여진다. 이벤트 ID 261의 경우 단순 TCP 연결 수립 시에도 발생하므로, 포트스캐닝과 RDP 클라이언트의 접근시도와는 구분할 수 없다.

2.1.4.1. RDP Bruteforce



<그림 9> Bruteforce 에 의한 로그온 실패 이벤트 다수 발생

Microsoft-Windows-Security-Auditing의 로그온 이벤트 중, 로그온 타입 3 / 10을 가지는 성공/실패 이벤트의 발생일자를 x축, 발생시각을 y축으로 한 Scatter Plot을 작성했을 때, 로그인 실패 이벤트(4625)가 세로 직선을 그리는 현상이 관찰되는 경우 RDP Bruteforce 계열의 공격이 시도되었음을 확인할 수 있다. 그러나 로그온 실패 이벤트는 로그온 감사 설정을 통해 실패한 로그온 이벤트를 로깅하도록 설정하여야 한다.

이외에도 악성코드에 감염될 수 있는 다양한 시나리오가 존재한다. 본 문서에서는 보편적인 사례 일부만 소개하였고, 각 상황에 따라 분석가의 적절한 판단을 통해 적합한 증적을 찾아내는 것이 중요하다.

2.2. 거점확보 단계

공격자에 의해 악성코드가 실행되면 악성코드에 감염된 PC를 제어하기 위해 C&C 서버와 통신하거나 정보유출, 백도어 접근을 위해 외부와 통신을 연결하는 단계이다.

이벤트 분석항목	목적
윈도우 방화벽 정책	악성코드에 의한 방화벽 정책 변경 여부 확인

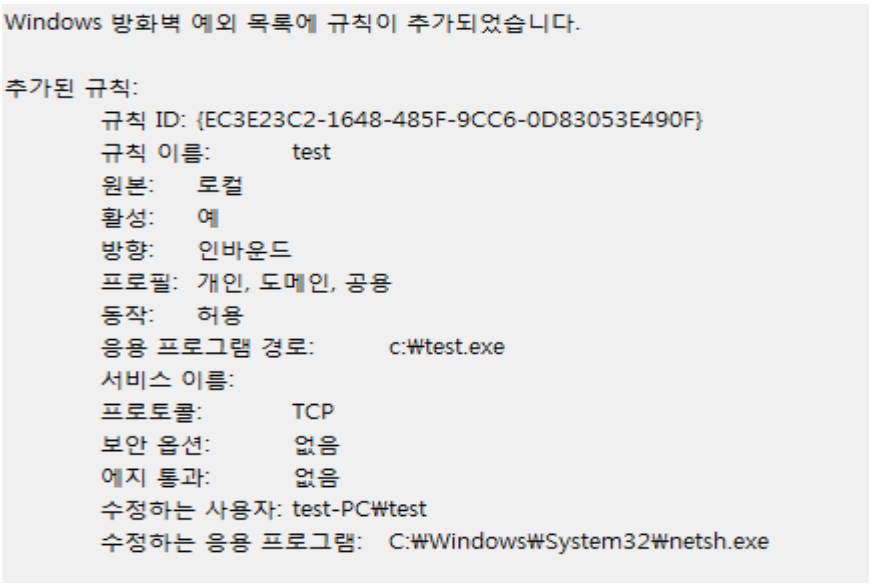
<표 5> 거점확보 시도 단계에서 활용할 수 있는 이벤트 분석항목

2.2.1. 운영체제 방화벽 우회

운영체제 방화벽이 활성화되어 있는 경우 외부와 통신이 어렵기 때문에 방화벽 정책을 제거하거나 예외 처리 함으로써 공격 거점을 확보해야 한다. 따라서 악성코드가 외부와 통신하기 위해 방화벽 정책을 수정하였는지, 알 수 없는 프로그램 또는 포트가 방화벽 정책에 등록되어 있는지 윈도우 방화벽 이벤트를 통해 확인할 수 있다. 방화벽 정책 수정 시 일반적으로 커맨드 명령어를 이용하기 때문에 netsh.exe 명령어를 통해 방화벽 정책이 수정되었는지 확인이 필요하다.

※ c:₩test.exe 의 인바운드 TCP 7777포트 허용 명령어 예시

```
netsh advfirewall firewall add rule name="test" dir=in action=allow
program=c:₩test.exe protocol=tcp localport=7777
```



<그림 10> 방화벽 예외 추가 이벤트 발생 화면

2.3. 권한상승 단계

권한상승 단계는 공격자, 공격 유형에 따라 생략될 수 있다. 그러나 제한된 권한을 얻은 공격자는 추가적인 악성 행위를 위해 권한 상승을 시도한다. 권한상승 방법은 다양하지만 윈도우 이벤트 정보에서 이러한 시도는 익스플로잇 실행에 의한 어플리케이션 에러나, 정보 수집을 통해 획득한 관리자 계정을 이용하여 로그인하는 경우 발생하는 이벤트를 통해 확인할 수 있다.

이벤트 분석항목	목적
어플리케이션 에러	권한 상승 익스플로잇에 의한 어플리케이션 에러 가능성 확인
로그온/로그오프	관리자 권한 로그인 성공, 실패 이력 확인

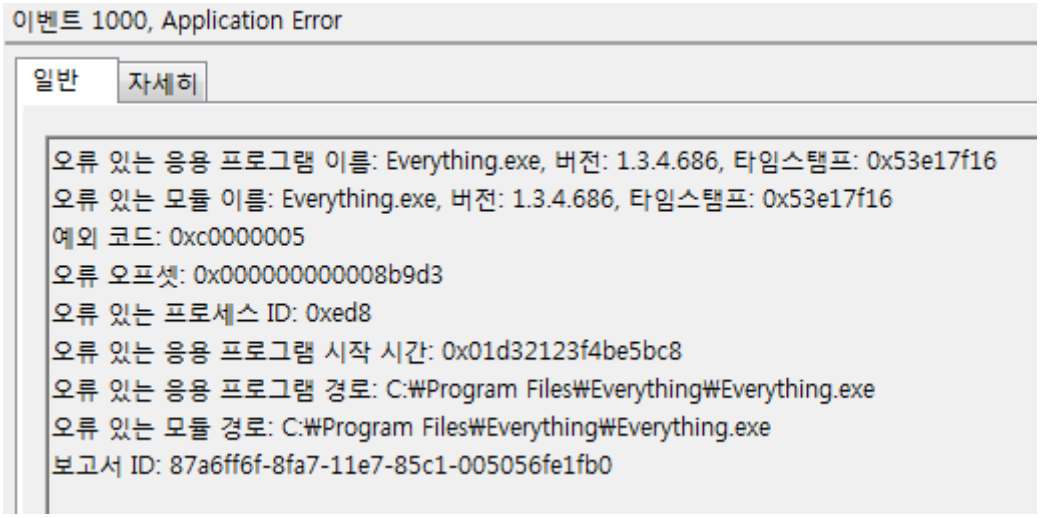
<표 6> 권한상승 단계에서 활용할 수 있는 윈도우 이벤트

2.3.1. 익스플로잇 실행에 의한 어플리케이션 에러

제한된 권한을 가진 공격자가 관리자 권한으로 실행되는 소프트웨어의 취약점을 이용하여 권한상승을 시도하는 것은 가장 일반적인 방법이다.

메모리 조작을 이용한 취약점이 사용되었을 경우 프로그램이 오동작하여 에러가 발생할 가능성이 존재하며, 이에따라 어플리케이션 에러 관련 이벤트 로그가 기록될 수 있다.

관리자 권한을 가지고 실행되는 프로그램에서 이러한 이벤트 로그가 발생하였을 경우 익스플로잇을 이용한 권한상승 등의 행위를 의심해 볼 수 있다.

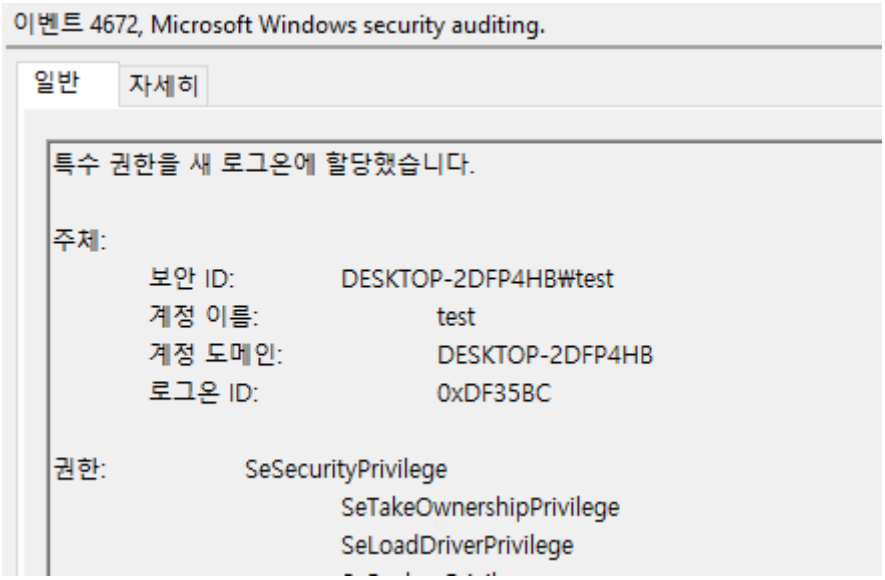


<그림 11> 어플리케이션 에러 이벤트 예시

2.3.2. 관리자 로그인 이력 확인

초기 침투한 시스템에서 mimikatz와 같은 인증정보 추출 도구 등을 이용하여 공통 관리자의 인증정보를 획득했거나, 미상의 방법으로 획득한 계정 정보를 획득하여 타 시스템에 관리자 권한으로 로그인하는 경우 피접속 시스템의 로그인 이벤트를 통해 확인할 수 있다.

패스워드 대입 공격을 사용하였을 경우 다량의 로그인 실패 이력이 발생하며(별도 설정 필요), 이외 사용하지 않는 관리자 계정으로 로그인이 성공한 경우 등을 통해 권한 상승 시도를 확인할 수 있다.



<그림 12> 관리자 로그인 발생 이벤트

2.4. 악성행위 단계

악성행위 단계는 실행된 악성코드의 목적을 달성하기 위한 주요 기능이 실행되는 단계로 악성행위는 내부전파, 정보유출, 키로깅, 암호화 등 매우 다양하고 대부분의 경우 이벤트 로그에 직접 기록되지 않기 때문에 윈도우 이벤트를 가지고 모든 악성행위를 확인하기에는 무리가 있다. 따라서 분석 보고서에서는 내부 전파 및 파일 암호화와 관련된 악성행위에 대한 이벤트 로그를 분석하였다.

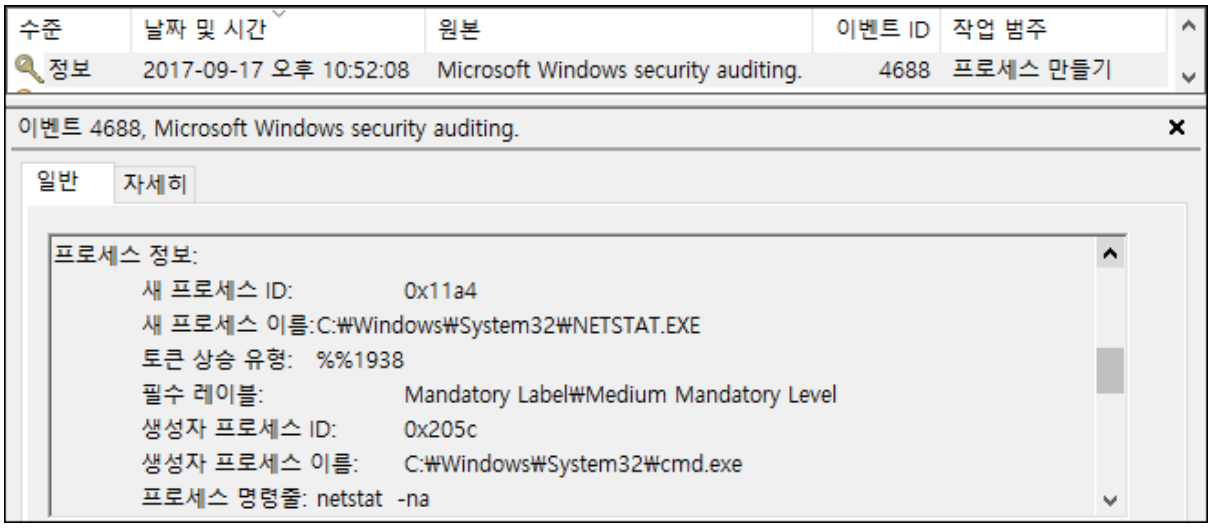
이벤트 분석항목	목적
응용프로그램 사용정보	내부확산을 위한 시스템/네트워크 정보 수집
시스템 시간 변경 정보	안티포렌식 목적의 시스템 환경 변경
윈도우 이벤트 초기화	안티포렌식 목적의 흔적 제거

<표 7> 악성행위 단계에서 활용할 수 있는 윈도우 이벤트

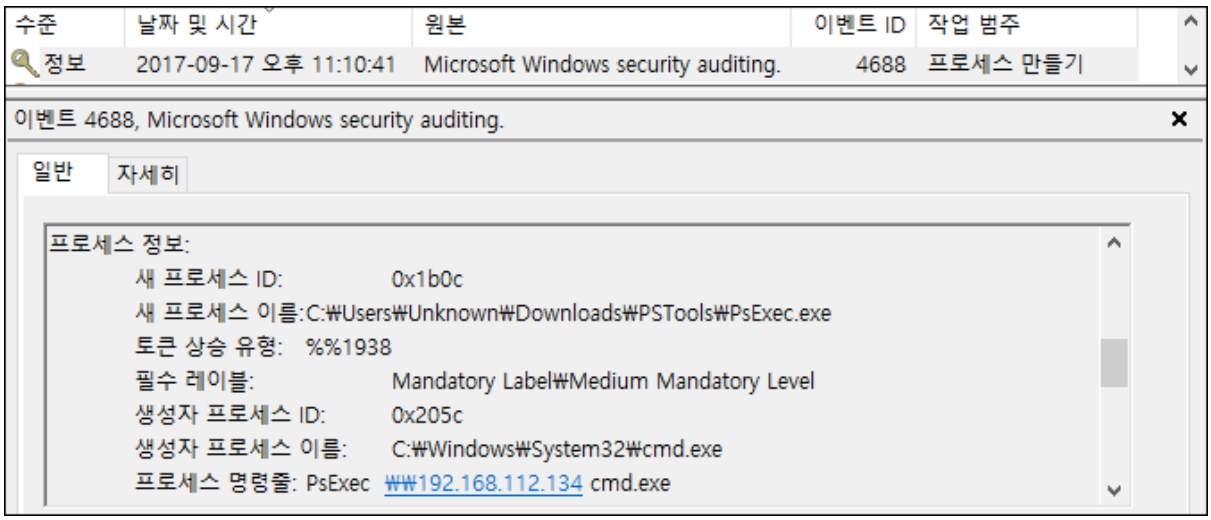
2.4.1. 내부 확산

감염된 시스템을 거점으로 활용하여 네트워크에 연결된 다른 PC를 감염시키는 내부 확산을 시도할 수 있다. 랜섬웨어 또는 APT, Worm과 같은 공격 유형의 악성코드가 이에 해당되며, 주로 네트워크 공유폴더를 통해 접근하거나 원격 실행 명령어를 이용하여 취약한 PC를 감염시키는 방법으로 내부 확산을 시도한다. 공격자가 내부 확산을 위해 정보를 수집하는 과정에서 특정 명령어를 실행하거나 로그인을 시도한 이벤트가 발생할 수 있다.

내부 확산을 위한 기법은 다양한 유형이 존재하므로, 분석가는 내부 확산 기법이 활용될 시 생성되는 다양한 증적들을 검토하여야 한다.



<그림 13> 내부 네트워크 정보 수집을 위한 명령어 실행



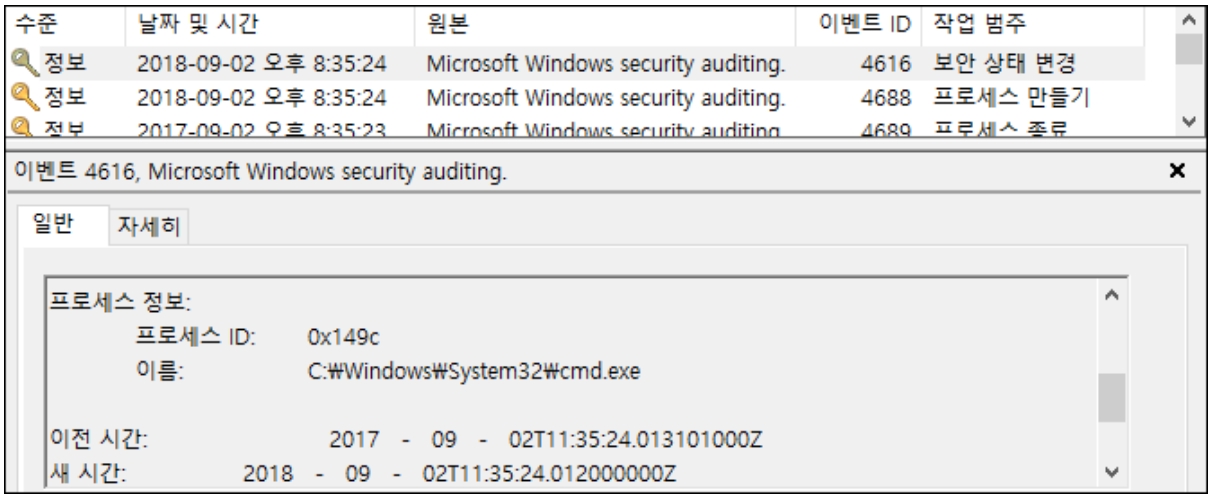
<그림 14> 프로세스 추적 감사 및 명령줄 감사 활성화 시 확인 가능한 명령줄

2.4.2. 안티 포렌식

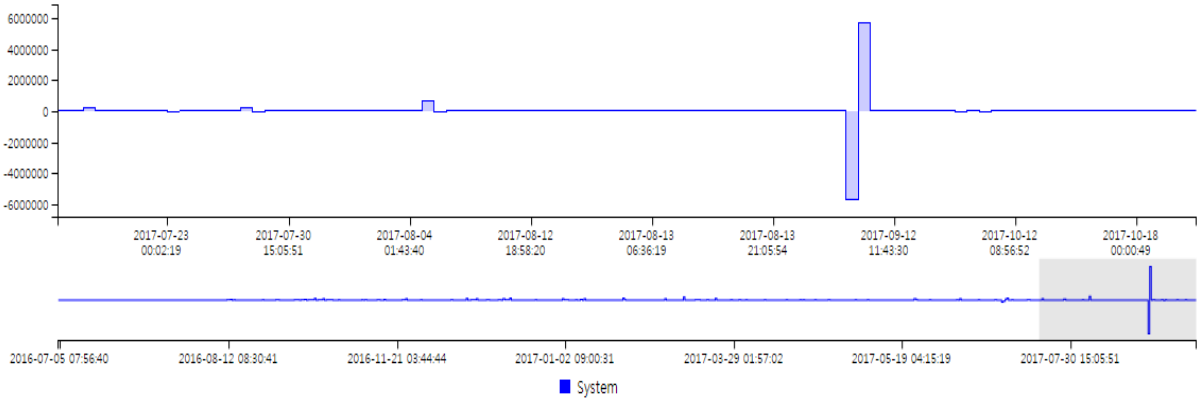
안티 포렌식이란 포렌식 분석을 방해하기 위한 기술로 공격자가 시스템에 남긴 흔적을 훼손하거나 숨기는 행위를 의미한다. 윈도우 이벤트에서 찾을 수 있는 안티 포렌식 행위는 시스템 시간을 변경하여 공격자의 행위를 분석하기 어렵도록 하거나, 이벤트 로그를 삭제하여 악성코드 설치 시간, 접근 IP 등 공격 흔적을 감출 수 있다.

2.4.2.1. 시스템 시간 변경

시스템 시간을 변경하면 파일 생성, 관련 로그 기록 등 이후 발생하는 행위의 시간정보가 변경된 시간에 맞춰지기 때문에 타임라인 기반 분석이 어렵게 된다. 특히 악성코드의 경우 감염 추정 시간을 기반으로 파일의 생성 시간을 확인하는데, 시스템 시간이 변경된 경우 타임라인의 범위에서 벗어나기 때문에 분석에 방해가 된다. 따라서 시스템 시간 변경 여부를 먼저 확인하고 변경된 시간을 보정한 후 분석을 진행해야 한다.



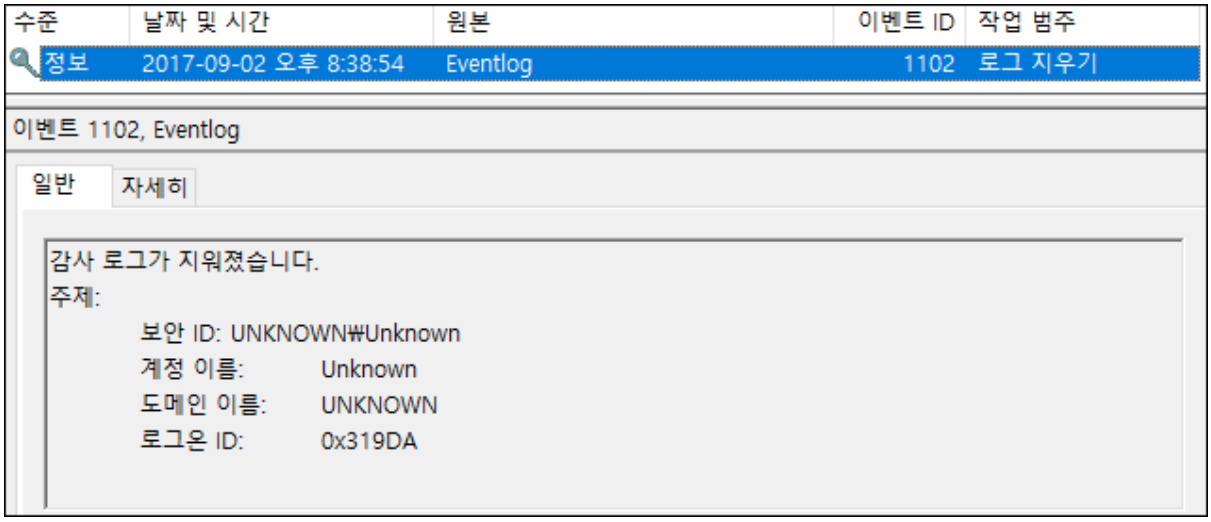
<그림 15> 시간 정보 변경 이벤트 발생 화면



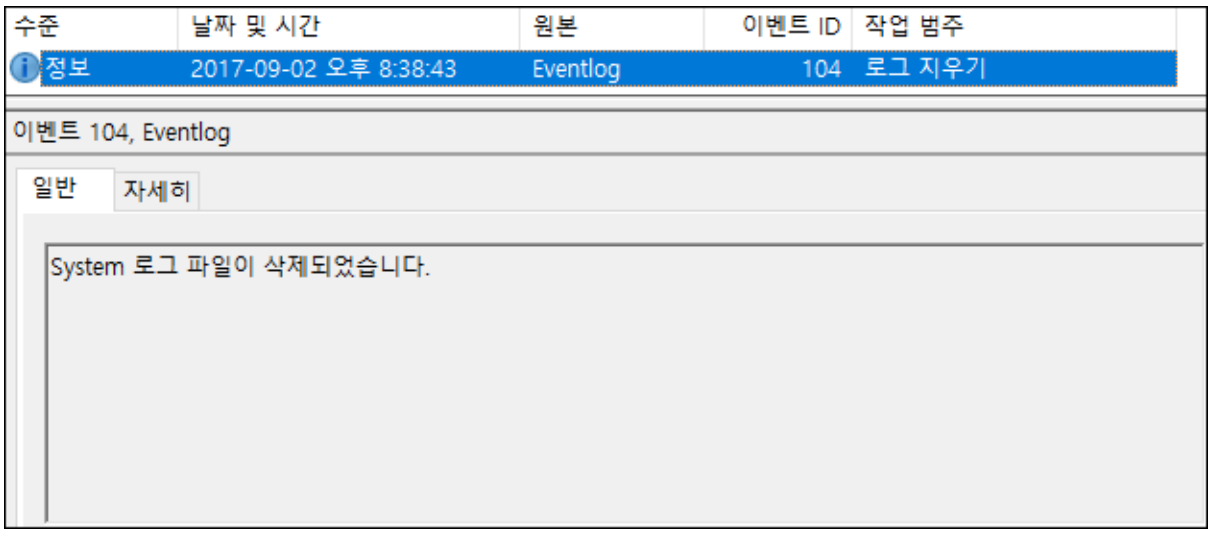
<그림 16> 악성코드에 의한 비정상 시간 변경 그래프 예시

2.4.2.2. 이벤트 로그 삭제

이벤트 로그 삭제는 사용자가 의도적으로 삭제하기 전에는 발생하지 않기 때문에 이벤트 로그 삭제가 발생했다는 것은 공격 행위가 있었고, 공격 행위를 숨기기 위해 공격자가 의도적으로 삭제했다는 것을 의미한다.



<그림 17> Security 로그 삭제 시



<그림 18> 그 외 로그 삭제 시

2.5. 연결유지 단계

한번 실행된 악성코드는 운영체제가 재시작 되더라도 지속적으로 감염된 상태를 유지할 수 있도록 특정 운영체제 영역에 자신을 등록한다. 특정 영역은 레지스트리, 폴더, 윈도우 서비스 등이며 해당 영역에 알려지지 않은 임의의 프로그램이 등록되어 있는지 확인해야 한다.

프로그램 등록 시, 분석자가 쉽게 알아차리지 못하도록 프로그램 이름을 윈도우 기본 프로그램 이름과 유사하게 변경하여 등록할 수 있기 때문에 실행 경로, 실행파일명을 유심히 확인해야 한다. 또한 원격 접속 등을 위해 백도어 계정을 생성할 수 있기 때문에 연결유지 단계에서는 공격자가 남겨놓은 흔적을 확인해야 한다.

이벤트 분석 항목	용도
자동실행 등록	악성코드의 지속 실행을 위한 자동실행 등록 확인
윈도우 서비스	악성코드의 지속 실행을 위한 서비스 등록 확인
윈도우 계정관리	공격자의 백도어 계정 등록 여부 확인

<표 8> 연결유지 단계에서 활용할 수 있는 윈도우 이벤트

2.5.1. 악성코드 자동실행 등록

악성코드가 자동으로 실행될 수 있도록 등록하는 방법은 여러 가지가 있다. 대부분은 윈도우 로그온 레지스트리의 자동실행 영역에 악성코드를 등록하지만 시작프로그램 폴더, 스케줄러, 윈도우 서비스, BHO 등도 이용되고 있다.

2.5.1.1. 윈도우 로그온

윈도우 로그온은 운영체제가 실행될때 자동으로 실행되도록 등록하는 레지스트리로 일반적으로 자동실행 등록을 위한 항목으로 가장 많이 이용된다.

HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run

HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce

HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Userinit

HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Shell

HKLM₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩Wds₩rdpwd

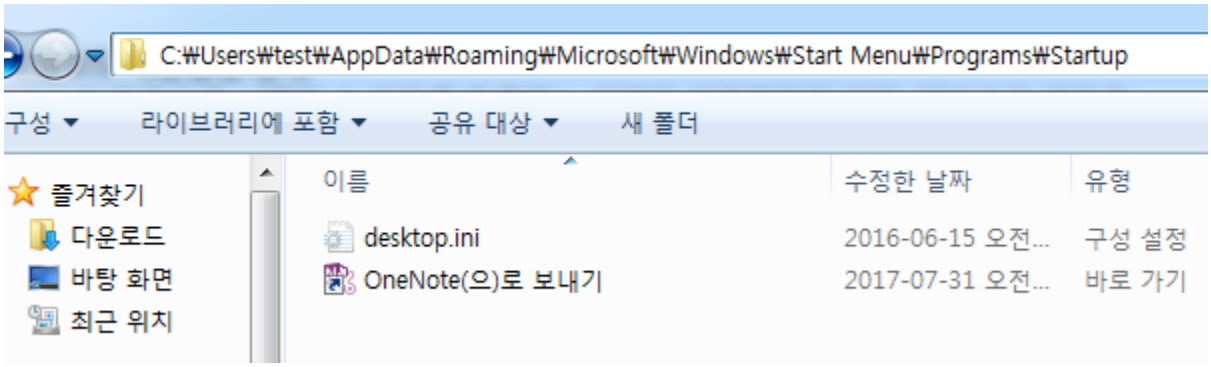
<자동실행 레지스트리 주요 경로>

2.5.1.2 시작 프로그램 폴더

시작 프로그램 폴더는 운영체제가 시작할 때 자동으로 실행할 프로그램을 등록해 놓은 폴더로 특정 사용자에 대한 폴더와 공통 폴더 2개의 영역이 존재한다. 시작 프로그램 폴더에 악성코드의 실행 파일 또는 링크파일을 복사하면 운영체제가 시작될때마다 자동으로 실행된다.

₩Users₩{사용자명}₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu₩Programs₩Startup
₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Startup

<자동실행 폴더 주요 경로>



<그림 19> 시작 프로그램 폴더

2.5.1.3 작업 스케줄러

작업 스케줄러는 사용자가 원하는 날짜, 시간에 작업이 실행될 수 있도록 예약하는 기능으로, 악성코드를 지속적으로 실행할 수 있도록 등록할 수 있다. 작업 스케줄러는 at.exe, schtasks.exe 윈도우 기본 명령어를 이용하여 등록할 수 있으며, at.exe 를 이용하여 스케줄러를 등록하면 등록된 프로그램 실행시 사용자 화면에 나타나지 않고 백그라운드에서 동작하기 때문에 at.exe를 주로 이용한다.

프로그램 구분	내용
at.exe	백그라운드(background) 작업에 주로 사용
schtasks.exe	포어그라운드(foreground) 작업에 주로 사용

2.5.1.4. 윈도우 서비스

윈도우 서비스는 운영체제 시작 시 자동으로 실행되는 기능을 말하며, 구동되는 기능은 백그라운드에서 실행된다. 특히 사용자가 윈도우 로그인하기 전 실행되기 때문에 윈도우 로그온 레지스트리나, 시작프로그램 폴더보다 실행 우선순위 높고 윈도우 서비스로 실행되는 기능은 UAC(User Access Control)의 영향을 받지 않기 때문에 실행 권한에 대한 제약이 없어 더 강력하다고 볼 수 있다.

2.5.1.5. BHO(Browser Helper Object)

BHO란 인터넷 익스플로러에 별도의 외부 기능을 지원하기 위해 사용되는 DLL 모듈을 의미하며, 익스플로러 실행시 자동으로 DLL 모듈이 실행된다. 인터넷 이용시 자동으로 실행되는 특성 때문에 애드웨어, 웹사이트 계정탈취 등의 악성코드에서 이용되고 있다.

HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Browser Helper Objects
HKCU₩Software₩Microsoft₩Internet Explorer₩UrlSearchHooks
HKLM₩Software₩Microsoft₩Internet Explorer₩Toolbar
HKLM₩Software₩Microsoft₩Internet Explorer₩Extensions

<BHO 레지스트리 주요 경로>

2.5.2. 백도어 계정 추가

악성코드가 실행된 이후 원격 접속(RDP)을 목적으로 임의의 백도어 계정을 추가할 수 있다. 운영체제 계정 목록에 시스템 기본계정, 사용자 계정 이외에 임의의 계정이 등록되어 있는지, 또는 사용하지 않는 계정의 패스워드가 변경된 기록이 있는지 확인해야 한다. 주로 커맨드 명령어를 이용하여 계정 생성, 패스워드 변경 등의 작업을 수행하고 윈도우 이벤트에 기록이 남게 된다.

계정 생성 : net user {계정명} /add 패스워드 변경 : net user {계정명} {패스워드}

계정 생성, 패스워드 변경 명령어

Case #2 기업 보안감사

1. 시나리오

얼마 전 CISO가 새로 부임한 보안업체 큐리어스에서는 내부 기밀문서 보안 실태를 점검하기 위해 보안감사를 실시하기로 했다. 회사 보안정책 상으로 금지하고 있는 외부저장장치 연결 여부와 불필요한 프로그램 설치 여부를 확인하고, 추가적으로 업무시간 준수 및 근무태만 정도를 파악하려고 한다.

2. 이벤트 분석 방법

기업 보안감사 시나리오는 근태 관리, 기밀정보 유출, 불필요 프로그램 설치로 분류하고 분석을 진행하였다.

구분	항목	목적
근태관리	로그온/로그오프	로그온/로그오프 시간의 타임라인 분석을 통한 태업여부 확인
	PC 시작/종료	PC 가동시간의 타임라인 분석을 통한 태업여부 확인
	시스템 시간 변경 정보	시스템 시간 변경을 통한 출퇴근 기록 조작 여부 확인
기밀정보 유출	외장 저장매체 분석	자료유출 목적의 비인가 저장매체 연결여부 확인
	문서 인쇄	기밀문서 인쇄시도 확인
	무선네트워크 접속	자료유출 목적의 비인가 AP 연결 여부 확인
불필요 프로그램 사용	윈도우 서비스 정보	비인가/악성 소프트웨어에 의한 윈도우 서비스 추가여부 확인
	응용 프로그램 사용정보	비인가 소프트웨어(메신저, 게임 등)의 설치여부 확인

<표 9> 기업 보안감사 관련 분석 이벤트

2.1 근태/태업 확인

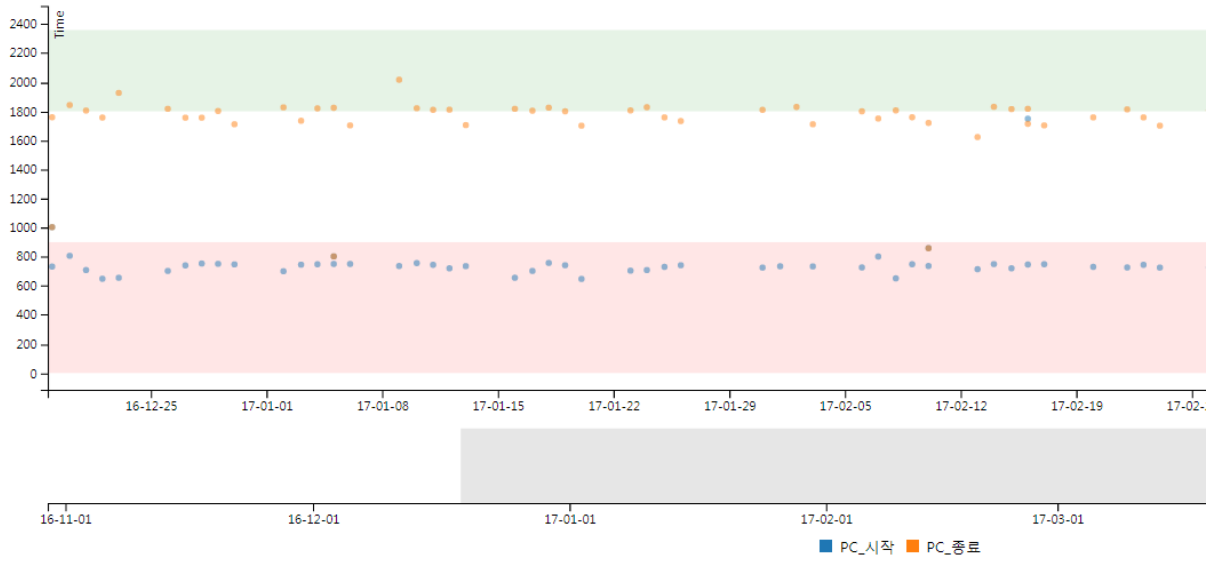
근태/태업 확인은 직원의 출/퇴근 시간, 업무 시간 중 자리비운 시간을 통해 확인할 수 있다. 이를 위해 PC ON/OFF 기록, 로그인/로그오프 기록을 확인할 수 있으며, 시스템 시간 변경정보를 통해 의도적인 출퇴근 시간 변경 여부도 확인 해야 한다.

이벤트 분석 항목	용도
로그온/로그오프	로그온/로그오프 시간의 타임라인 분석을 통한 태업여부 확인
PC 시작/종료	PC 가동시간의 타임라인 분석을 통한 태업여부 확인
시스템 시간 변경 정보	시스템 시간 변경을 통한 출퇴근 기록 조작 여부 확인

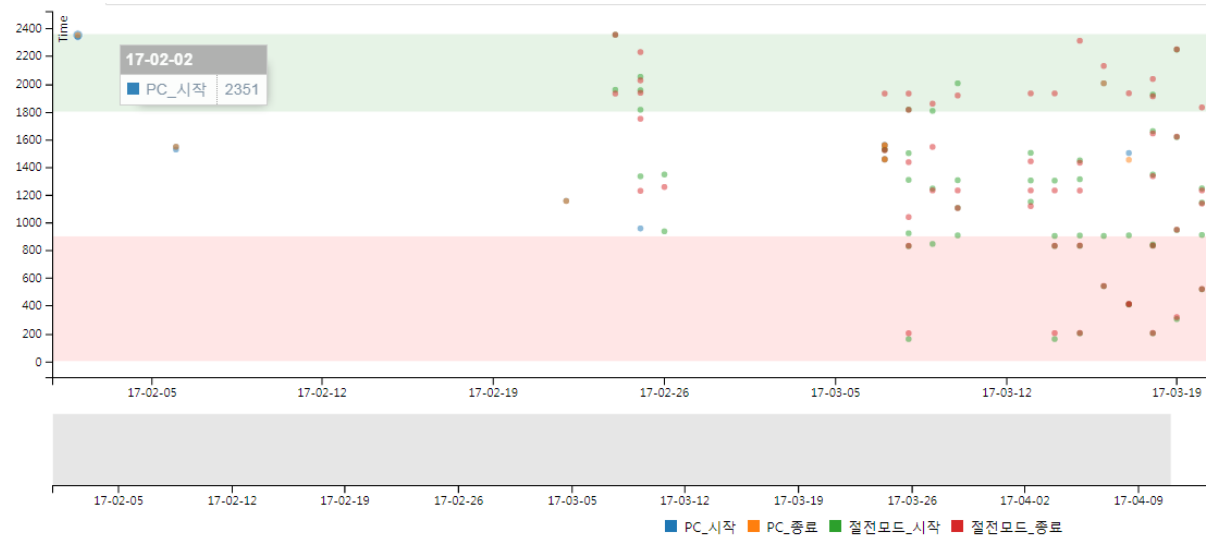
<표 10> 근태/태업 확인 단계에서 활용할 수 있는 윈도우 이벤트

2.1.1. PC ON/OFF 기록

직원의 출/퇴근 시간을 확인하기 위해서는 PC ON/OFF 기록을 확인해야 한다. 대부분의 업무가 PC를 통해서 이루어지기 때문에 출/퇴근 시간과 PC ON/OFF 시간은 거의 일치한다고 볼 수 있다. 출/퇴근 시간을 확인하여 지각 또는 조퇴 여부를 확인할수 있으며, 새벽 시간과 같이 이상 시간대 PC 사용 기록이나 보안솔루션 우회를 위한 안전모드 부팅 여부를 통해 정보 유출 행위도 의심할 수 있다.



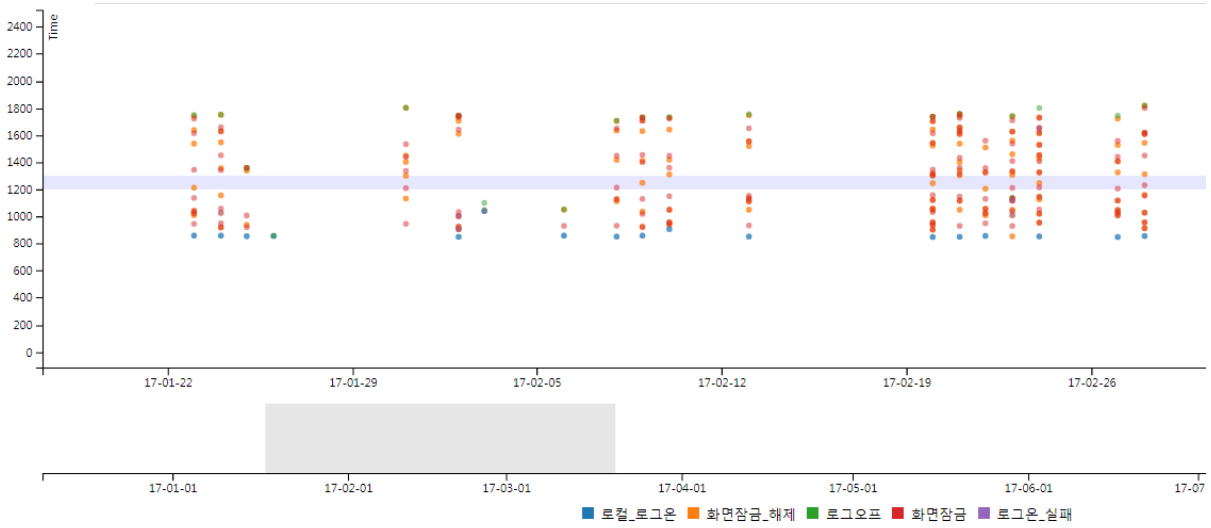
<그림 20> 일반적인 근태 그래프 예시



<그림 21> 지각, 새벽 시간 대 PC 사용 그래프 예시

2.1.2. 로그온/로그오프 기록

로그온/로그오프 기록을 통해 근무시간 중 자리를 비운 시간과 자리로 돌아온 시간을 알 수 있다. 자리를 비우기 전 화면을 잠그거나, 일정 시간이 지나면 자동으로 화면이 잠기도록 화면보호기가 설정된 경우 해당 시간을 확인할 수 있으며, 자리에서 돌아온 경우 잠금 해제를 위해 다시 로그온을 해야하기 때문에 해당 시간을 확인할 수 있다.



<그림 22> 빈번한 자리비움 로그온/로그오프 그래프 예시

2.1.3. 시스템 시간 변경 정보

출/퇴근 시간을 조작하기 위해 시스템 시간을 의도적으로 변경한 후 사용할 수 있기 때문에 의도적으로 시스템 시간을 변경하였는지 확인해야 한다.

<그림 23> 시스템 시간 변경 이벤트

2.2. 기밀 정보 유출

내부 기밀 정보의 경우 USB 메모리, 외장 하드디스크 등을 이용하여 파일 형태로 자료를 반출하거나 기밀 문서를 프린터로 인쇄하여 출력물 형태로 반출하는 방법으로 유출할 수 있다. 그렇기 때문에 외장 저장장치 사용 기록 및 문서 인쇄 기록을 확인해야 한다. 또한 내부 네트워크에서 웹하드, 상용 메일 등 사용이 불가능한 경우 모바일 테더링 등을 이용하여 자료를 전송할 수 있기 때문에 무선네트워크 사용 기록도 확인해야 한다.

이벤트 분석 항목	용도
외장 저장매체 분석	자료유출 목적의 비인가 저장매체 연결여부 확인
문서 인쇄	기밀문서 인쇄시도 확인
무선네트워크 접속	자료유출 목적의 비인가 AP 연결 여부 확인

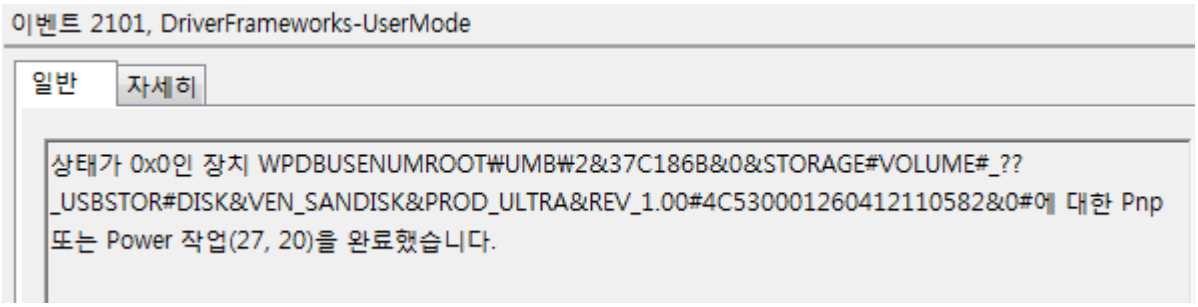
<표 11> 기밀 정보 유출 확인 단계에서 활용할 수 있는 윈도우 이벤트

2.2.1. 외부 저장장치 사용 기록

정보를 유출하기 위해 사용하는 외부 저장장치는 USB 형태의 메모리, 디스크가 가장 많이 사용되고 있으며, CD/DVD 매체도 일부 사용되고 있다. 두가지 모두 대용량의 데이터를 저장할 수 있기 때문에 정보유출이 의심되는 경우 해당 장치의 사용기록을 확인해야한다. 또한 한대의 PC를 여러명이 같이 사용하는 공용PC의 경우 외부 저장장치 사용 기록과 사용자 로그온 기록을 결합하여 해당 장치를 사용한 사용자를 추가로 확인할 수 있다.

2.2.1.1. USB 저장매체 사용 기록

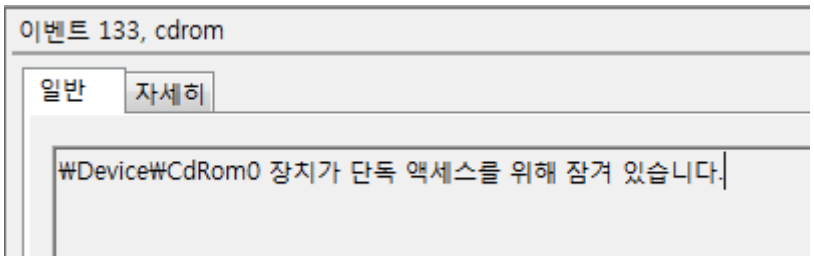
USB를 이용하는 저장매체는 외장 메모리, 외장 디스크, 모바일(스마트폰, 태블릿 등)기기가 있다. USB 저장매체를 사용하게 되면 최초 연결 시 드라이브가 설치되기 되면서 이벤트가 기록되고, 매 연결/해제 시 마다 이벤트가 발생한다. 이벤트 발생시 제조사명, 제품명, 시리얼번호가 기록되기 때문에 해당 시점에 어떤 USB 저장매체가 기록되었는지 알 수 있다. 다만 모바일 장치, 외장 디스크의 경우 운영체제 특성상 이벤트가 기록되지 않거나 일부 제한적인 정보만 기록되기 때문에 유의하여 분석이 필요한다.



<그림 24> USB 저장매체 연결 이벤트

2.2.1.2. CD/DVD 레코딩 기록

CD, DVD 는 저장 가능 용량에 차이만 있을뿐, 그 외 외형, 크기 등은 동일하다. CD/DVD 레코딩 기록은 일반적으로 **발생하지** 않기 때문에 레코딩 기록이 존재하는 경우, 레코딩 시간, 사용자를 확인하고 실제 정보 **유출** 여부를 확인 해야 한다. 다만, 광학 매체 사용기록은 파일명, 용량 등의 세부적인 정보가 이벤트로그에 기록되지 않기 때문에 사용 여부만 확인할 수 있다.



<그림 25> CD/DVD 레코딩 이벤트

2.2.2. 문서 인쇄 기록

망분리 및 DRM 솔루션 등을 활용하여 내부 문서파일 보안에 신경을 쓰더라도, 인쇄된 문서의 외부 반출은 관리의 효율성 및 인권 등의 문제로 인해 통제하기 어려우며, 이러한 점을 악용하여 고객정보와 같은 중요 문서들을 인쇄/유출하는 사례도 종종 발생한다.

문서 인쇄 기록도 윈도우 이벤트 로그로 남길 수 있지만, 이를 위해선 이러한 보안사고 발생 전 인쇄 기록을 활성화 해두어야 한다.

위치	인쇄한 사용자	문서번호	문서이름	프린터 이름	프린터 포트	페이지 수	부수	스풀 파일 경로	Time Created(Local)
\\김용현-인트라넷	X1210018	2	보물지도.hwp	SINDOH A401_407 Series PCL5e	IP_192_168_192_100	1	1	C:\Windows\system32\spool\PRINTERS\00002.SHD	2017-09-07 11:09:01.483346+09:00

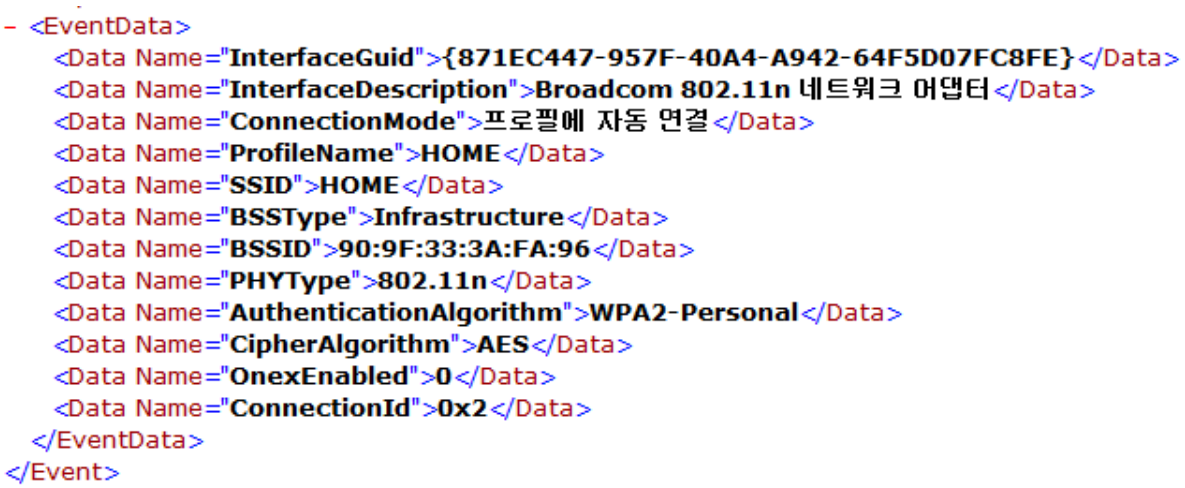
Showing 1 to 1 of 1 rows

<그림 26> 문서 인쇄 기록

2.2.3. 무선네트워크 사용 기록

노트북은 무선랜카드가 기본으로 장착되어 있기 때문에, 기업 내에서 노트북을 사용하는 경우 보안 정책 우회를 위한 비인가 네트워크 접근 기록 유무를 확인해야 한다. 기업 내에서 상용 메일이나 웹하드 등 정보유출 가능성이 있는 웹사이트를 차단하고 있는곳이 많기 때문에, 악의적인 내부자가 이러한 보안 정책을 우회하기 위해 노트북 또는 USB타입의 무선랜카드를 통해 테더링 기능을 이용, 보안 정책을 우회할 여지가 있다.

무선 네트워크 연결이 성공한 경우 8001번 이벤트가 기록되며 해당 이벤트 속성 정보를 통해 연결된 무선 AP 정보를 확인할 수 있다.



<그림 27> 무선네트워크 연결 성공 8001번 이벤트

2.3. 비인가 프로그램 사용

비인가 프로그램을 지정, 사용여부를 모니터링하는 것은 기업 내 보안, 저작권 관련 분쟁 예방, 태업 억제 등을 위해 반드시 필요하다. 윈도우 이벤트 로그를 통해 프로그램의 설치여부를 확인할 수 있다.

이벤트 분석 항목	용도
소프트웨어 설치	비인가 소프트웨어(메신저, 게임 등)의 설치여부 확인
응용 프로그램 사용정보	

<표 12> 기밀 정보 유출 확인 단계에서 활용할 수 있는 윈도우 이벤트

2.3.1. 소프트웨어 설치

소프트웨어 설치 시 기록되는 이벤트 로그를 통해 비인가 소프트웨어의 사용여부를 식별할 수 있다. 소프트웨어 설치 이벤트를 확인하여 정보유출 목적의 특정 프로그램이 설치되었는 확인할 수 있다. 특히 원격제어 프로그램(TeamViewer, VNC 등) 또는 가상 머신(Vmware, VirtualBox 등)을 설치후 데이터 유출에 이용할 수 있기 때문에 인가된 프로그램 외 설치된 프로그램이 있는지 확인해야 한다.

2.3.2. 응용프로그램 사용 정보

설치파일 형태로 배포되는 비인가 프로그램도 있지만, 설치가 필요 없는 무설치 소프트웨어를 적발해야할 필요도 있다. 운영체제 설치 후 별도로 설정을 해둔 상태가 아니라면, 이러한 소프트웨어의 사용이력은 윈도우 이벤트 로그로 기록되지 않는다. 따라서 사전에 프로세스 추적 감사 설정을 통해 실행되는 응용프로그램 이벤트를 기록하도록 설정해두어야 한다.

IV. 목적별 윈도우 이벤트 분석항목

본 문서에서는 파일명 - 이벤트 아이디 매치 대신, Provider Name - 이벤트 아이디 매치를 통해 정리하였다. 이는 동일한 이벤트 ID임에도 상이한 이벤트가 발견될 소지가 있으며(e.g, Microsoft-Windows-Kernel-General 1, EMET 1), 이벤트 파일 이름이 변경되더라도 실제 이벤트 로그 내 XML내 기재되어있는 Provider Name은 변경되지 않기 때문에 보다 용이한 분석이 가능하기 때문이다.

본 문서에서 다루는 분석항목 일부는 기본적으로 비활성화되어 있기 때문에, 사전에 관련 로깅 정책을 활성화하여야만 기록되는 이벤트도 있다. 그러한 경우 활성화 방법은 각 항목에서 기술하였다.

각 상황에 대한 이벤트 로그 조사 시 많은 이벤트 유형을 찾을 수 있었으나, 본 문서에서는 유의미한 결과를 얻는 데 도움이 되는 속성을 포함한 이벤트 ID 중심으로 정리하였고, 해당 이벤트를 제공하는 Provider, 이벤트 ID, 또 주요 속성에 대한 XPath 경로 및 해당 정보에 대한 설명을 함께 기재하였다.

1. 로그온 / 로그오프

1.1. 분석 개요

로그온/로그오프 시 발생하는 이벤트를 통해 직원의 출퇴근, 근무 시간 중 자리비움 또는 외부 해커의 원격 로그인 등 다양한 정보를 확인할 수 있다. 또한, 추가 감사로그 설정을 하게되면 화면잠금이나 로그인 실패와 같이 보다 상세한 기록 확인이 가능하다.

구분	시나리오	이벤트 ID	비고
사용자의 출퇴근 시간에 관한 정보	기업보안	4624 4647	
사용자가 근무 도중 자리비운 시간에 관한 정보	기업보안	4647 4800	
다른 직원의 불법적인 로그온 시도에 관한 정보	기업보안	4625	
외부에서 해당 컴퓨터로 원격 로그인 시도에 관한 정보	악성코드	4624 4625	

<표 13> 로그온/로그오프 이벤트를 통해 알 수 있는 정보

1.2. 이벤트 상세 분석

1.2.1. 로그온 성공

로그온 성공시 4624 이벤트가 발생하며, Logon Type 값을 통해 로컬 로그인, 원격 로그인, 화면보호기 잠금 해제 등의 로그인 당시의 상황을 구분할 수 있기 때문에 근태 정보, 외부 해킹 등 다양한 상황에 대해 확인할 수 있다.

유형	구분	설명
2	대화형	콘솔에서 키보드로 로그인
3	네트워크	네트워크를 통한 원격 로그인 (파일 공유, IIS 접속 등)
4	자동실행(스케줄)	스케쥴에 등록된 배치 작업 실행 시 미리 설정된 계정 정보로 로그인
5	서비스	서비스가 실행될 때 미리 설정된 계정 정보로 로그인
7	잠금해제	화면보호기 잠금해제시

8	네트워크(평문암호)	유형 3과 비슷하나 계정 정보를 평문으로 전송할 때 발생
9	새 자격	실행(RunAS)에서 프로그램 실행 시 /netonly 옵션을 줄 때
10	원격 대화형	터미널 서비스, 원격 접속, 원격지원으로 로그인
11	캐쉬된 대화형	PC에 캐쉬로 저장된 암호로 자동 입력 로그인시

<표 14> 로그인 유형별 구분

1.2.2. 로그오프

사용자가 로그오프 버튼을 눌렀을 때 4647 이벤트가 발생한다. 로그오프 이후 4624 이벤트 Logon Type 2번 발생한 경우 자리에서 돌아온 것을 알 수 있다.

1.2.3. 화면잠금

사용자가 작업도 중 일시적인 화면잠금(윈도우+L) 또는 화면보호기에 의한 화면잠금 시 4800 이벤트가 발생하며, 이벤트로 계정 로그온 이벤트 감사를 설정해야만 기록된다. 화면잠금 이벤트를 통해 근무시간 도중 사용자의 일시적인 자리비움 여부를 확인할 수 있으며, 이벤트 발생 이후 4624 이벤트 Logon Type 7 번 발생한 경우 자리에서 돌아온 것을 알 수 있다.

1.2.4. 로그온 실패

로그인 실패시 4625 이벤트가 발생하며, 로그인 실패 이벤트는 추가적인 감사로그를 설정해야만 기록된다. 로그인 실패시 기록되는 상태코드인 SubStatus 값을 이용하여 로그인 실패 이유를 알 수 있다.

상태코드	설명
0xC0000064	사용자 이름이 존재하지 않습니다.
0xC000006A	사용자 이름이 올바르지만 암호가 잘못되었습니다.
0xC000006C	암호 정책을 충족하지 않습니다.
0xC000006D	시도한 로그온은 사용자 이름이 잘못되어 유효하지 않습니다.
0xC000006E	사용자 계정 제한 때문에 로그인하지 못했습니다.
0xC000006F	사용자 계정에 시간 제한이 있으며 지금은 로그온할 수 없습니다.

0xC0000070	사용자가 제한되었으며 원본 워크스테이션에서 로그온할 수 없습니다.
0xC0000071	사용자 계정의 암호가 만료되었습니다.
0xC0000072	사용자 계정이 현재 비활성화되어 있습니다.
0xC000009A	시스템 리소스가 부족합니다.
0xC0000193	사용자의 계정이 만료되었습니다.
0xC0000224	처음 로그인하기 전에 사용자가 암호를 변경해야 합니다.
0xC0000234	사용자 계정이 자동으로 잠겼습니다.

<표 15> 로그인 실패 SubStatus 상태 코드

로그인실패, 화면잠금 이벤트의 경우 계정 로그온 이벤트 감사, 로그온 이벤트 감사를 활성해야만 발생한다. (부록. 감사항목 설정 참조)

1.3. 주요 이벤트 ID 목록

Provider	Microsoft-Windows-Security-Auditing	**추가설정**	불필요
이벤트 ID	4624	**운영체제**	Win7 / Win10
발생조건	사용자 로그인 시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="LogonType"] – 로그인 종류 /Event/EventData/Data[@Name="IpAddress"] – 아이피 주소		

Provider	Microsoft-Windows-Security-Auditing	**추가설정**	필요
이벤트 ID	4625	**운영체제**	Win7 / Win10
발생조건	사용자 로그인 실패 시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="SubStatus"] – 로그인 실패 이유 /Event/EventData/Data[@Name="IpAddress"] – 아이피 주소		

Provider	추가설정	이벤트 ID	발생조건
Microsoft-Windows-Security-Auditing	불필요	4647	로그오프
Microsoft-Windows-Security-Auditing	필요	4800	화면 잠금

2. PC 시작 / 종료

2.1. 분석 개요

시스템 로그에서 발생하는 다양한 이벤트를 통해 시스템의 ON/OFF 시간을 확인할 수 있다. 일반적인 시스템 시작/종료 외에 안전모드 부팅 및 임의 강제종료 여부를 확인할 수 있으며, 절전모드를 사용하는 경우 해당 시작/종료 시간을 확인할 수 있다.

구분	시나리오	이벤트 ID	비고
사용자의 출퇴근 시간에 관한 정보	기업보안	12, 13 42, 1	
안전모드 부팅 여부(보안솔루션 우회 등)	기업보안	12	
PC 강제 종료 여부	기업보안	41	

2.2. 이벤트 상세 분석

2.2.1. 전원 온/오프

이벤트 아이디 12, 13 이벤트를 이용하여 PC의 시작/종료 시간을 확인할 수 있다. 다만 물리적인 방법으로 운영체제를 강제로 종료되는 경우 이벤트 아이디 13번이 기록되지 않기 때문에, 종료 이벤트가 존재하지 않는 경우 운영체제가 강제 종료되었다고 추정할 수 있다.

※ 강제종료 확인 방법

운영체제가 강제종료되었을 경우 41번, 6008번 발생하는 이벤트가 발생한다. 하지만 종료되는 방법(전원 플러그 OFF 등)에 따라 강제 종료 시간이 기록되지 않거나(41번), 이벤트가 누락(6001번)될 가능성이 있어, 분석 프로그램 구현시 1차적으로 41번 이벤트를 참고하고 종료 시간이 기록되지 않는 경우 운영체제 시작 이벤트(12번)가 발생되기 전 마지막 생성 이벤트의 시간을 참조하는 방식으로 확인이 가능하다.

2.2.2. 안전모드 부팅

부팅시, 이벤트 아이디 12번의 Bootmode 값을 이용하여 안전모드 부팅 여부를 확인할 수 있다.

Bootmode	내용
0	일반 부팅
1	안전모드 부팅

<표 16> 방화벽 활성화/비활성화 속성

```
- <EventData>
    <Data Name="MajorVersion">10</Data>
    <Data Name="MinorVersion">0</Data>
    <Data Name="BuildVersion">10240</Data>
    <Data Name="QfeVersion">16506</Data>
    <Data Name="ServiceVersion">0</Data>
    <Data Name="BootMode">0</Data>
    <Data Name="StartTime">2017-08-03T03:27:20.494948200Z</Data>
  </EventData>
</Event>
```

<그림 28> 부팅 이벤트 속성

2.2.3. 절전모드 온/오프

일반적인 전원 온/오프 뿐만 아니라 미리 설정된 절전모드에 의해 피씨가 종료되거나 다시 시작될 수 있다. 절전모드에 진입할 경우 42번 이벤트가 발생하고, 절전모드에서 깨어날 경우 이벤트 아이디 1번이 발생한다.

2.3. 주요 이벤트 ID 목록

Provider	추가설정	이벤트 ID	발생조건
Microsoft-Windows-Kernel-General	불필요	12	시스템 시작
Microsoft-Windows-Kernel-General	불필요	13	시스템 종료
Microsoft-Windows-Kernel-Power	불필요	41	시스템 강제 종료
Microsoft-Windows-Kernel-Power	불필요	42	절전모드 시작
Microsoft-Windows-Power-Troubleshooter	불필요	1	절전모드 해제

3. 응용 프로그램 사용정보

3.1. 분석 개요

응용 프로그램 사용 정보를 모니터링 하도록 설정되어 있다면 침해사고 분석, 기업 내 저작권 위반 및 비인가 프로그램 사용여부 적발 등 다양한 곳에 활용할 수 있다. 그러나 응용 프로그램 사용 정보의 로깅은 기본적으로 비활성화 되어있으며, 로컬 보안 정책의 편집을 통해 **'프로세스 추적 감사' 정책을 활성화**하여야 한다.

또한, Windows 8.1 이상인 경우 그룹 정책 편집을 통해 **'프로세스 명령줄 감사'** 설정을 수행함으로써 프로세스 생성 시 이용된 명령행도 추가로 기록할 수 있다.

구분	시나리오	이벤트 ID	비고
악성코드 실행여부 식별	악성코드	4688,4689,500,505	
비인가 소프트웨어 실행여부 식별	기업보안	4688,4689,500,505	
비인가 문서 열람여부 식별	기업보안	4688,4689,500,505	

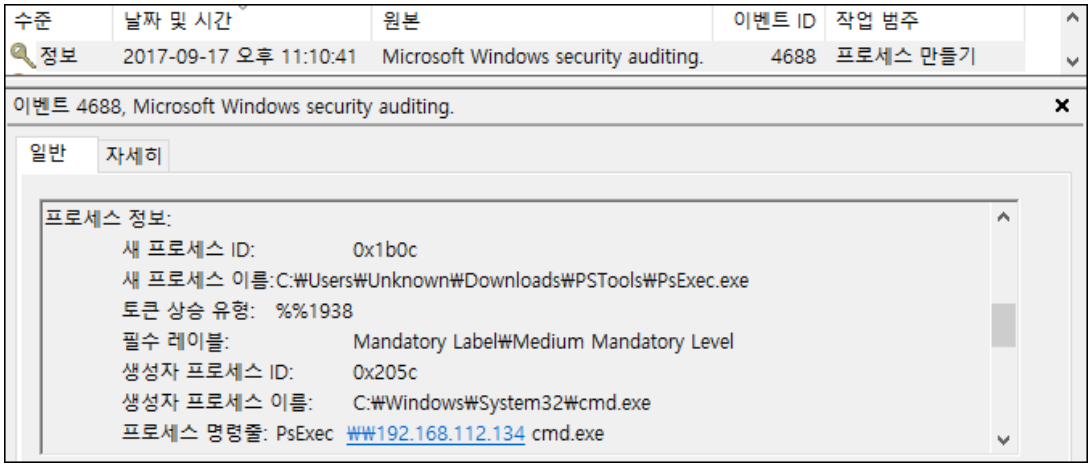
3.2. 이벤트 상세 분석

3.2.1. Microsoft-Windows-Security-Auditing

프로세스 추적 감사 설정이 활성되어 있는 경우, 프로세스 실행 시 이벤트 ID 4688을 가지는 이벤트가 기록되며 만들어진 프로세스 ID, 이름, 부모 프로세스 ID를 확인할 수 있다. 또한 프로세스 명령줄 감사 설정(Windows 8.1 이상)이 되어있는 경우 해당 프로세스 실행 시 사용된 명령줄을 확인할 수 있다.

윈도우 10에서는 부모 프로세스의 ID 및 프로세스 이름이 남아 분석이 용이하나, 윈도우 7의 경우 부모 프로세스 ID만 기록되고 프로세스 이름은 기록되지 않는다.

프로세스 종료 시 이벤트 ID 4689를 가지는 이벤트가 기록되며, 종료된 프로세스의 ID 및 이름, 종료 상태를 확인할 수 있다.

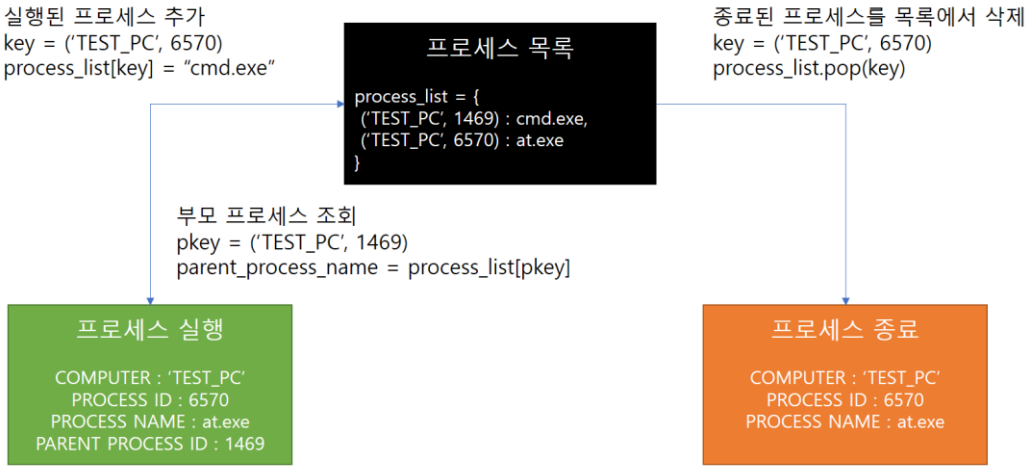


<그림 29> 프로세스 생성 시 기록되는 이벤트 로그

※ 부모 프로세스 이름 확인 방법

윈도우 7 환경에서 생성된 프로세스 실행 이벤트 로그 분석 시, 부모 프로세스의 이름까지 파악하기 위해서는 부모 프로세스 ID를 프로세스 ID로 가지는 이벤트를 탐색해야 한다.

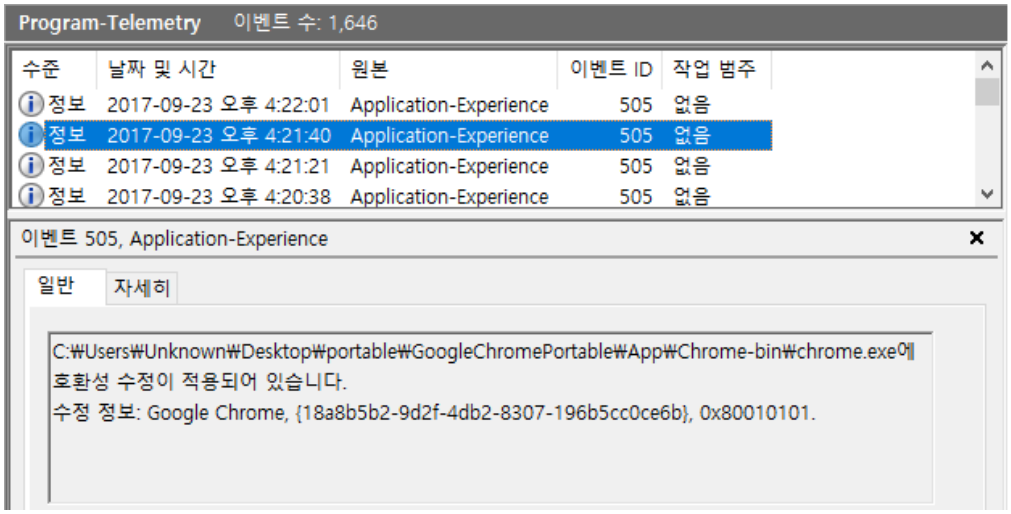
분석 프로그램 구현 시 프로세스 관련 이벤트를 시간 순으로 정렬하고, 프로세스 실행/종료 시 발생하는 이력을 기록하여 해당 이력을 참조하는 방법으로 구현하였다.



3.2.2. Microsoft-Windows-Application-Experience

Windows의 호환성 수정 기능이 적용된 프로세스가 생성되는 경우, 이벤트 ID 500 또는 505를 가진 이벤트가 기록된다. 해당 이벤트는 별도의 설정 없이도 기록되므로, 프로세스 추적 감사가 설정되지 않은 상황에서 제한적이나마 실행되었던 프로세스를 확인할 수 있다.

단, 실행되는 모든 프로세스가 호환성 수정을 필요로 하는 것은 아니기에 모든 프로세스의 실행이 기록되지 않으며, 프로세스가 종료된 경우 관련 이벤트가 발생하지 않는 점을 유의하여야 한다.



<그림 30> 어플리케이션 호환성 수정 적용 이벤트 로그

3.2.3. 이외 활용 가능한 단서

실행된 프로그램이 네트워크 통신을 하는 경우(RAT 악성코드 등), 윈도우 방화벽 정책 이벤트를 통해 이러한 프로그램의 경로 및 최초 실행시기를 알아낼 가능성도 있다.

3.3. 설정 상황별 조사가능 범위

프로세스 추적 감사	프로세스 만들기 이벤트에 명령줄 포함 (Windows 8.1 이상)	식별가능 정보
X	X	프로세스(제한적)
O	X	프로세스
O	O	프로세스, 명령줄

3.4. 주요 이벤트 ID 목록

3.4.1. Microsoft-Windows-Security-Auditing

Provider	Microsoft-Windows-Security-Auditing	**추가설정**	필요
이벤트 ID	4688	**운영체제**	Win7 / Win10
발생조건	프로세스 생성 시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="ProcessID"] – 부모 프로세스 ID /Event/EventData/Data[@Name="NewProcessId"] – 생성된 프로세스의 PID /Event/EventData/Data[@Name="NewProcessName"] – 생성된 프로세스 경로 /Event/EventData/Data[@Name="ParentProcessName"] – 부모 프로세스 경로 (윈도우10 한정) /Event/EventData/Data[@Name="CommandLine"] – 명령행(윈도우 10 한정, 명령줄 포함 정책 설정 시)		

Provider	Microsoft-Windows-Security-Auditing	추가설정	필요
이벤트 ID	4689	운영체제	Win7 / Win10
발생조건	프로세스 종료 시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="ProcessId"] – 종료된 프로세스의 PID /Event/EventData/Data[@Name="ProcessName"] – 종료된 프로세스 경로 /Event/EventData/Data[@Name="Status"] – 상태		

3.4.2. Microsoft-Windows-Application-Experience

Provider	Microsoft-Windows-Application-Experience	추가설정	-
이벤트 ID	500, 505	운영체제	Win7 / Win10
발생조건	호환성 수정이 적용된 프로세스 생성 시		
주요 속성 (XPath)	/Event/UserData/CompatibilityFixEvent/ProcessId – 프로세스 ID /Event/UserData/CompatibilityFixEvent/StartTime – 프로세스 시작 시간 /Event/UserData/CompatibilityFixEvent/ExePath – 실행파일 경로 /Event/UserData/CompatibilityFixEvent/FixName – 어플리케이션 이름* * 관리자 권한으로 실행 시 'RunAsAdmin' 으로 표시		

4. 윈도우 서비스 정보

4.1. 분석 개요

공격자 또는 악성코드 제작자들은 지속적인 침투/실행을 위해 악성 프로세스를 윈도우 서비스 항목으로 추가하는 방법을 사용하기도 한다. 또한 내부전파(Lateral Movement)를 위해 주로 사용되는 도구인 PsExec와 같은 도구는 피제어 시스템에 윈도우 서비스를 추가하기도 한다. 윈도우 서비스 관련 이벤트를 점검하는 것은 이러한 기법의 사용여부를 탐지하는 데 도움이 될 수 있다.

뿐만 아니라, 웹 서버 및 DBMS와 같이 데몬 형태로 동작하는 프로그램을 설치했을 경우 윈도우 서비스 항목이 추가될 가능성이 높으며, 이러한 경우 서비스 추가 이벤트 로그에서 서비스가 추가된 시간을 통해 설치시점을 추정할 수 있기도 하다.

구분	시나리오	이벤트 ID	비고
윈도우 서비스를 이용한 악성코드 지속실행 시도 식별	악성코드	7045 7036 7040	
서비스명을 통한 비인가 소프트웨어 설치 시도 추정	기업보안		

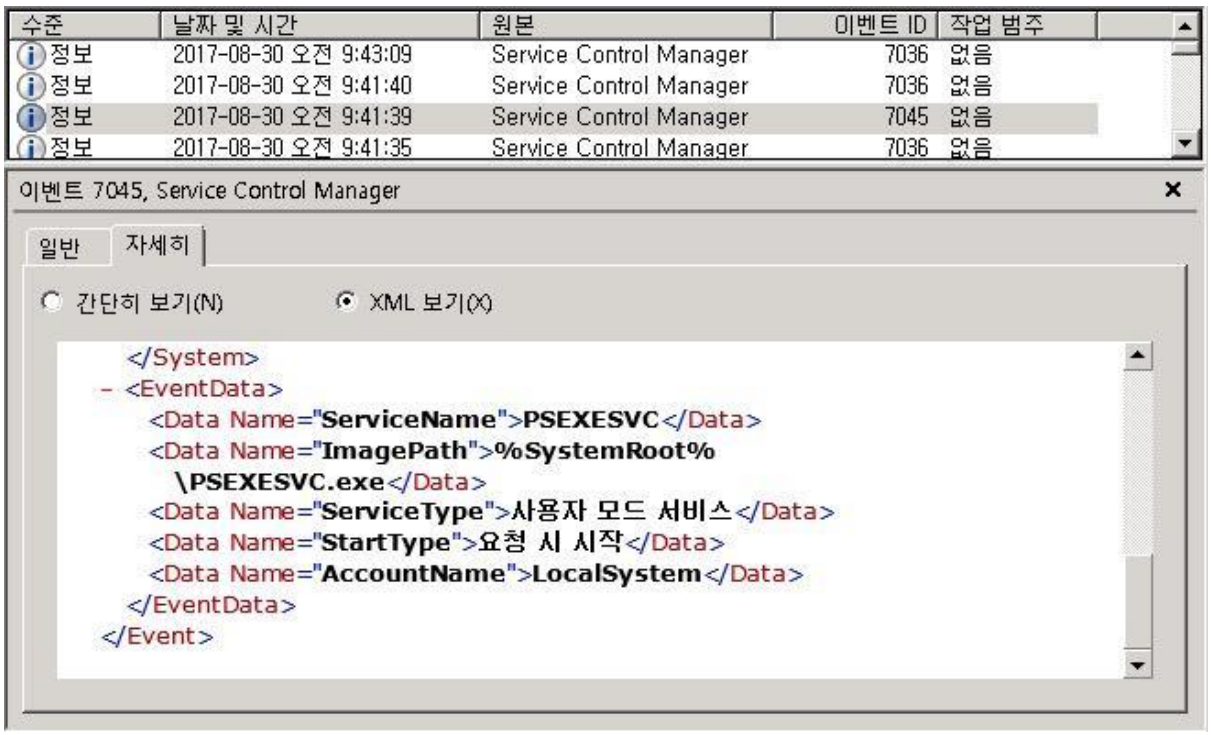
4.2. 이벤트 상세 분석

4.2.1. 서비스 설치

아래는 윈도우 서비스 추가 시 발생하는 이벤트 ID 7045(Service Control Manager)의 예시이다.

새로운 서비스가 추가될 시, 이벤트 ID 7045(Service Control Manager)를 가지는 이벤트 로그가 생성된다. 이 이벤트를 통해 추가된 서비스의 이름, 실행 파일의 경로, 서비스 유형, 시작 유형 등의 정보를 확인할 수 있다.

아래 이벤트는 PSExec를 사용하여 원격 시스템에 명령을 전송했을 때, 피제어 시스템에 기록되는 이벤트로 이러한 이벤트를 통해 내부전파 기법에 의한 피해가 있는지 추정할 수 있다. (물론 해당 툴은 정상적인 툴로, 관리자에 의한 정상적인 사용일 가능성도 있다. 따라서 관리자 인터뷰 등을 추가적으로 수행해야 한다.)



<그림 31> PsExec 피제어 시스템에 기록되는 서비스 생성 이벤트

윈도우 서비스는 다양한 목적으로 사용되며, 악성코드의 지속 실행을 위해서 사용되기도 한다. 또한 웹 서버, DBMS 등의 제품을 설치할 시, 해당 서버 데몬을 자동 구동시키기 위해 윈도우 서비스를 등록하는 특성을 이용하여 소프트웨어 설치 시점을 추정할 수 있기도 하다.

4.2.2. 서비스 상태 변경

서비스 상태가 변경될 시, 이벤트 ID 7036(Service Control Manager)을 가지는 이벤트 로그가 생성되며, 이 이벤트를 통해 변경된 서비스의 이름과 변경된 상태 등의 정보를 확인할 수 있다.

4.2.3. 서비스 시작유형 변경

서비스 시작 유형이 변경될 시, 이벤트 ID 7040(Service Control Manager)을 가지는 이벤트 로그가 생성되며, 이 이벤트를 통해 변경된 서비스의 이름과 변경된 상태 등의 정보를 확인할 수 있다.

4.3. 주요 이벤트 ID 목록

Provider	Service Control Manager	추가설정	-
이벤트 ID	7045	운영체제	Win7 / Win10
발생조건	서비스 설치		
주요 속성 (XPath)	/Event/EventData/Data[@Name="ServiceName"] – 서비스 이름 /Event/EventData/Data[@Name="ImagePath"] – 실행 경로 /Event/EventData/Data[@Name="ServiceType"] – 서비스 유형 /Event/EventData/Data[@Name="StartType"] – 시작 유형 /Event/EventData/Data[@Name="AccountName"] – 계정 이름		

Provider	Service Control Manager	추가설정	-
이벤트 ID	7036	운영체제	Win7 / Win10
발생조건	서비스 상태 변경		
주요 속성 (XPath)	/Event/EventData/Data[@Name="param1"] – 서비스 이름 /Event/EventData/Data[@Name="param3"] – 변경된 상태 이름 /Event/EventData/Binary – 바이너리 데이터		

Provider	Service Control Manager	추가설정	-
이벤트 ID	7040	운영체제	Win7 / Win10
발생조건	서비스 시작유형 변경		
주요 속성 (XPath)	/Event/EventData/Data[@Name="param1"] – 서비스 표시이름 /Event/EventData/Data[@Name="param2"] – 이전 상태 /Event/EventData/Data[@Name="param3"] – 변경된 상태 /Event/EventData/Data[@Name="param4"] – 서비스 이름		

5. 외장 저장매체 사용 기록

5.1. 분석 개요

외장 저장매체는 일반적으로 가장 많이 사용되고 있는 USB 형태의 저장매체와 CD/DVD 같은 광학 저장매체로 분류할 수 있다.

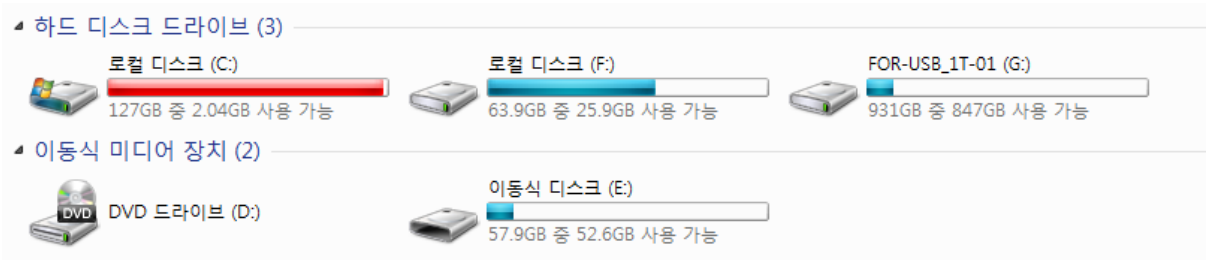
구분	시나리오	이벤트 ID	비고
사용자가 USB 저장매체를 최초로 연결한 시간 정보	기업보안	10000 20001	
사용자가 USB 저장매체를 연결/해제한 히스토리 정보	기업보안	2101 2012 1006	
사용자가 광학저장매체를 레코딩한 시간 정보	기업보안	133	

<표 17> 외장 저장매체 사용 기록 이벤트를 통해 알 수 있는 정보

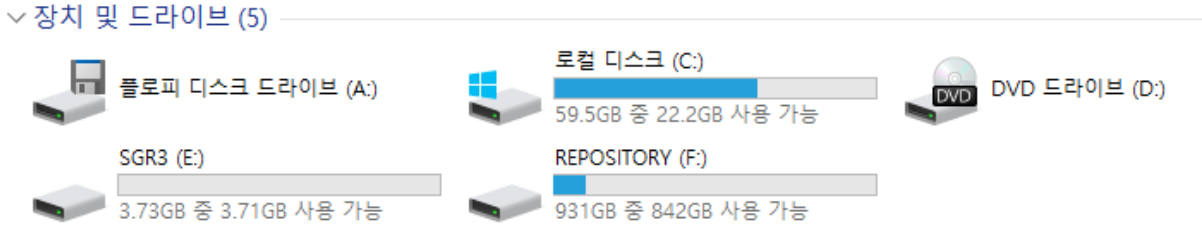
5.1.1. USB 저장매체

USB 형태로 이용할 수 있는 저장매체는 플래시 메모리, HDD/SSD 디스크, 모바일 장치가 있다. 이러한 USB 저장매체를 PC에 연결 또는 해제 시 다양한 이벤트가 동시에 발생하지만 모든이벤트가 분석에 필요한 정보는 아니다. 예를들면, 전원 관리, 드라이브 모듈 로드 등 동일한 이벤트가 두번 이상 발생하거나, 동일한 이벤트가 연결/해제 시 모두 발생하는 등 분석에 불필요한 이벤트 아이디도 발생하기 때문에 연결 해제 여부, 시점을 정확하게 파악하기 위해서는 분석에 필요한 이벤트만 선별하는것이 필요하다. 윈도우 8 이상부터는 기본적으로 외장 저장매체 관련 이벤트가 비활성화 되어있기 때문에 별도로 로그수집 기능을 활성화 해야 수집이 가능하다.

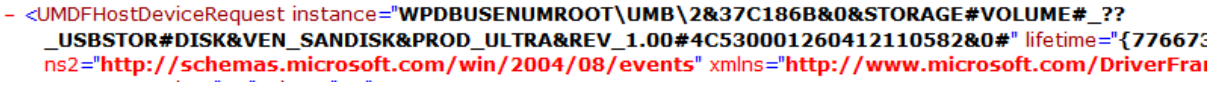
윈도우7 운영체제에서 외장 디스크는 이동식 미디어 장치가 아닌 하드 디스크 드라이브로 분류되기 때문에 연결/해제 기록이 기록되지 않고 최초 드라이버 설치를 위한 연결 기록만 알 수 있다. 그러나 윈도우10 운영체제에서는 하드 디스크와 이동식 장치의 구분을 두지않으며 하드 디스크의 연결/해제 기록도 기록된다. 다만 기록되는 정보에 한계가 있어 레지스트리 정보와 결합 해야 특정 장치 정보를 확인할 수 있다. 또한 모바일 기기의 경우 제품명 등 기기 정보는 레지스트리에 기록되고 윈도우 이벤트에는 분류코드가 기록되기 때문에 레지스트리에 기록되는 스마트폰 제품명이나 소유자 이름명과 같이 장치 정보가 기록되지 않는다.



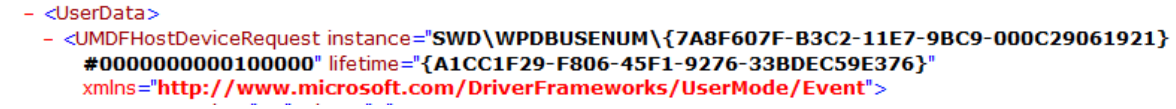
<그림 32> Windows 7 하드디스크, 이동식 미디어 표시 화면



<그림 33> Windows 10 하드디스크, 이동식 미디어 표시 화면



<그림 34> Windows 7 외장메모리, 하드디스크 연결시 이벤트 기록 정보



<그림 35> Windows 10 하드디스크 연결시 이벤트 기록 정보

구분	최초 연결	연결/해제	특징
외장 메모리	O	O	제조사, 제품명 정보 기록 (리더기 사용 시 리더기의 정보가 기록)
외장 디스크(Win7)	O	X	제조사, 제품명 정보 기록
외장 디스크(Win10)	△	△	제조사, 제품명, 시리얼 정보 기록되지 않음
모바일 기기	△	△	제조사, 제품명 정보 기록되지 않음

5.1.2. 광학 저장매체

USB 저장매체 사용으로 지금은 많이 사용되지 않지만 CD/DVD 사용기록을 통한 정보유출 가능성도 존재한다. 광학매체를 레코딩하는 방법은 윈도우에서 제공하는 기본 기능을 이용하거나 전용 레코딩 프로그램(Nero 등)을 이용하는 방법이 있다.

5.2. 이벤트 상세 분석

5.2.1. 연결된 저장매체 목록

USB 저장매체의 경우 저장매체가 최초로 시스템에 연결될 때 드라이버를 설치하기 위해 시스템 로그에 10000번 이벤트와 20001번 이벤트가 발생하게 된다. 다만 SDD/HDD 디스크는 시스템에서 이동식 저장매체가 아닌 디스크 장치로 인식되며 10000번 이벤트가 발생하지 않기 때문에, 20001번 이벤트만 단독으로 발생하는 경우 디스크 장치로 판단할 수 있다. 벌크제품과 같이 시리얼 번호가 없는 USB저장매체 또는 모바일 장치의 경우 최초 연결 시 운영체제에서 임의의 생성번호를 부여한다. 연결되는 시스템이 다르면 생성번호도 변경되기 때문에 장치 확인 시 주의가 필요하다.

또한, SD카드 등을 리더기를 통해 연결할 시 SD카드의 정보가 아닌 리더기의 정보가 기록된다. 따라서 디지털 포렌식 수행 시 이러한 점을 유의하여 조사를 진행하여야 한다.

구분	시리얼 번호 예시
플래시 메모리(시리얼 O)	DISK&VEN_제조사명&PROD_제품명&REV_버전#시리얼번호&#
플래시 메모리(시리얼 X)	DISK&VEN_제조사명&PROD_제품명&REV_버전#&Pnp관리자생성번호&#
SSD/HDD 디스크(Win7)	DISK&VEN_제조사명&PROD_제품명&REV_버전₩시리얼번호&
SSD/HDD 디스크(Win10)	SWD₩WPDBUSENUM₩{RegistryId}₩#
모바일 장치	VID_제조사코드&PID_제품코드₩Pnp관리자생성번호

<표 18> 장치 별 시리얼 번호 구분방식

5.2.2. 외장 저장매체 연결/해제 기록

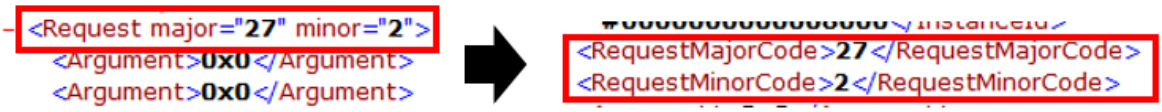
장치의 연결/해제 기록은 SSD/HDD 디스크의 경우 별도로 기록되지 않고, 플래시 메모리 또는 모바일 장치만 기록된다. 장치가 연결/해제 될 때 마다 여러 이벤트가 발생하게 되는데, 연결시 2101번, 해제시 2102번 이벤트를 이용하여 식별할 수 있다. 해당 이벤트가 기록되는 영역의 기본 저장 용량은 1MB로, 용량이 크지 않기 때문에 PC 사용환경에 따라 다르지만 약 2~4주간의 저장매체 연결/해제 정보를 확인할 수 있다.

5.2.3. 모바일 장치 구분

외장저장매체는 USB 메모리, 외장 하드디스크가 주로 사용되고 있지만, 최근 스마트폰 연결(MTP)을 통한 저장매체를 많이 사용하고 있다. 스마트폰 역시 윈도우 이벤트만으로는 한계가 존재하는데, 연결되는 스마트폰의 제품명, 사용자명(Label) 등은 윈도우 레지스트리에 기록되기 때문에 이벤트 로그에 기록되는 정보 만으로는 기록되는 코드번호를 이용하여 제조사, 연결된 장치가 모바일 장치인지 여부 정도만 확인이 가능하다. 모바일 장치 최초 연결시 발생하는 20001번 이벤트에서 설치되는 드라이버 이름(DriverName)이 wpdmtp.inf 이거나, 연결시 발생하는 2005번 이벤트에서 로드되는 드라이버 모듈(ModulePath)이 WpdMtpDr.dll인 경우 해당 장치가 모바일 장치로 식별할 수 있다.

5.2.4. 디스크 파티션 정보(Win 10)

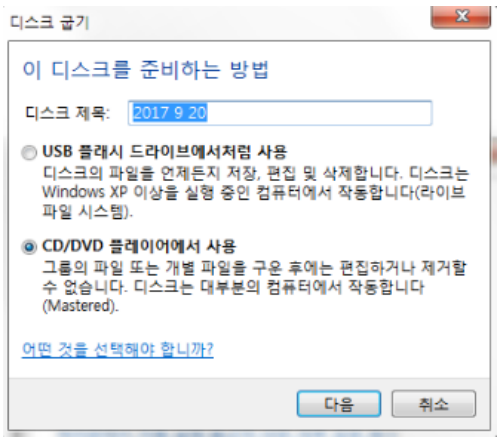
윈도우 10 운영체제에서 외장형 디스크의 윈도우 7 운영체제와 달리 경우 제조사명, 제품명, 시리얼번호가 기록되지 않고 RegistryId 값으로 기록된다. 그러나 연결된 디스크 정보가 별도의 파티션 이벤트에 기록되기 때문에 해당 이벤트의 저장장치의 RegistryId와 파티션 이벤트의 RegistryId를 매치하여 연결된 제조사명, 제품명, 시리얼번호 및 추가적으로 디스크용량, 파티션 테이블 정보 등을 확인할 수 있다. 파티션 이벤트는 윈도우 최신 업데이트(1703) 이후에 이벤트가 기록된다. 또한 업데이트 이후 기존에 기록되던 xml 형태가 달라지는 부분이 발생하기 때문에 분석에 유의하여야 한다.



<그림 36> 이벤트 형태 변경 예시

5.2.5. 광학저장매체 사용기록

광학매체가 레코딩 되는 경우 133번 이벤트가 발생하게 되며, 해당 이벤트가 발생한 경우 CD 또는 DVD 매체가 레코딩되었다고 볼 수 있다. 다만 윈도우 디스크 굽기 기능을 이용하여 레코딩 한 경우 만 이벤트가 기록되기 때문에 참고 정보 정도로만 활용 가능하다.



<그림 37> 윈도우 디스크 굽기 기능

레코딩 방법		133번 이벤트 기록 여부
디스크 굽기 기능 사용	USB 플래시 드라이버에서처럼 사용	X
	CD/DVD 플레이어에서 사용	O
전용 레코딩 도구(Nero 등) 사용		X

5.3. 주요 이벤트 ID 목록

Provider	추가설정	이벤트 ID	발생조건
Microsoft-Windows-DriverFrameworks-UserMode	필요(Win10)	2101	장치 연결
Microsoft-Windows-DriverFrameworks-UserMode	필요(Win10)	2102	장치 해제
Microsoft-Windows-DriverFrameworks-UserMode	불필요	10000	최초 연결 (메모리, 모바일)
Microsoft-Windows-UserPnp	불필요	20001	최초 연결(메모리, 디스크, 모바일)
cdrom	불필요	133	광학매체 레코딩

Provider	Microsoft-Windows-Partition	**추가설정**	불필요 (윈도우 업데이트 필요)
이벤트 ID	1006	**운영체제**	Win10
주요 속성 (XPath)	/Event/EventData/Data[@Name="Manufacturer"] – 제조사명 /Event/EventData/Data[@Name="Model"] – 모델명 /Event/EventData/Data[@Name="SerialNumber"] – 시리얼번호 /Event/EventData/Data[@Name="Capacity"] – 용량 /Event/EventData/Data[@Name="RegistryId"] – 레지스트리 아이디		

6. 시스템 시간 변경 정보

6.1. 분석 개요

시스템 시간 관련 정보는 주로 안티포렌식 / 알리바이 조작을 식별하기 위해 확인해야 하는 정보로, 분석 전 시스템 시간과 실제 시간의 오차 및 시스템 시간 변경여부는 반드시 점검하여야 한다.

시스템의 시간은 사용자가 임의로 변경하지 않더라도 시간 동기화 등이 수행되며 변경될 수 있다. 따라서 변경 전 시간과 변경 후 시간의 차이가 비교적 길고, Windows 커맨드라인에서의 날짜 변경(cmd.exe의 date 명령)과 같이 일반적이지 않은 시스템 시간 변경 등을 중점으로 검사해야 하므로, 기존시간 및 변경시간, 변경한 프로세스를 확인할 수 있는 이벤트 ID 4616(Microsoft-Windows-Security-Auditing)이 안티포렌식 여부 탐지에 적합하다.

구분	시나리오	이벤트 ID	비고
안티포렌식을 위한 시간 조작여부 및 방법 식별	악성코드/기업보안	4616, 1	

6.2. 이벤트 상세 분석

시스템 시간 변경 시, 이벤트 ID 4616(Microsoft-Windows-Security-Auditing), 이벤트 ID 1(Microsoft-Windows-Kernel-General) 를 가지는 이벤트가 발생한다. 두 이벤트 모두 변경 전 시간과 변경 후 시간을 확인할 수 있지만, 이벤트 ID 4616에서는 시간을 변경한 프로세스를 확인할 수 있는 관계로 이벤트 ID 4616이 안티포렌식 탐지에 조금 더 적합하다고할 수 있다.

<그림 38> cmd의 date 명령을 이용한 시간 변경 시

6.3. 주요 이벤트 ID 목록

6.3.1. Microsoft-Windows-Security-Auditing

Provider	Microsoft-Windows-Security-Auditing	**추가설정**	-
이벤트 ID	4616	**운영체제**	Win7 / Win10
주요 속성 (XPath)	/Event/EventData/Data[@Name="PreviousTime"] – 변경 전 시간 /Event/EventData/Data[@Name="NewTime"] – 변경 전 시간 /Event/EventData/Data[@Name="ProcessName"] – 시간을 변경한 프로세스 /Event/EventData/Data[@Name="ProcessId"] – 시간을 변경한 프로세스 ID		

6.3.2. Microsoft-Windows-Kernel-General

Provider	Microsoft-Windows-Kernel-General	**추가설정**	-
이벤트 ID	1	**운영체제**	Win7 / Win10
주요 속성 (XPath)	/Event/EventData/Data[@Name="PreviousTime"] – 변경 전 시간 /Event/EventData/Data[@Name="NewTime"] – 변경 전 시간		

7. 윈도우 이벤트 초기화

7.1. 분석 개요

시스템에 침투한 공격자 또는 악성 사용자는 목적 달성 후 자신의 흔적을 지우기 위해 이벤트 로그를 초기화하기도 한다. 이러한 윈도우 초기화는 Microsoft-Windows-Eventlog Provider의 이벤트 ID 1102, 104 를 통해 확인이 가능하며, 보안 로그를 삭제했을 시 이벤트 ID 1102, 그 외 로그를 삭제했을 시 이벤트 ID 104를 가진 이벤트가 기록된다.

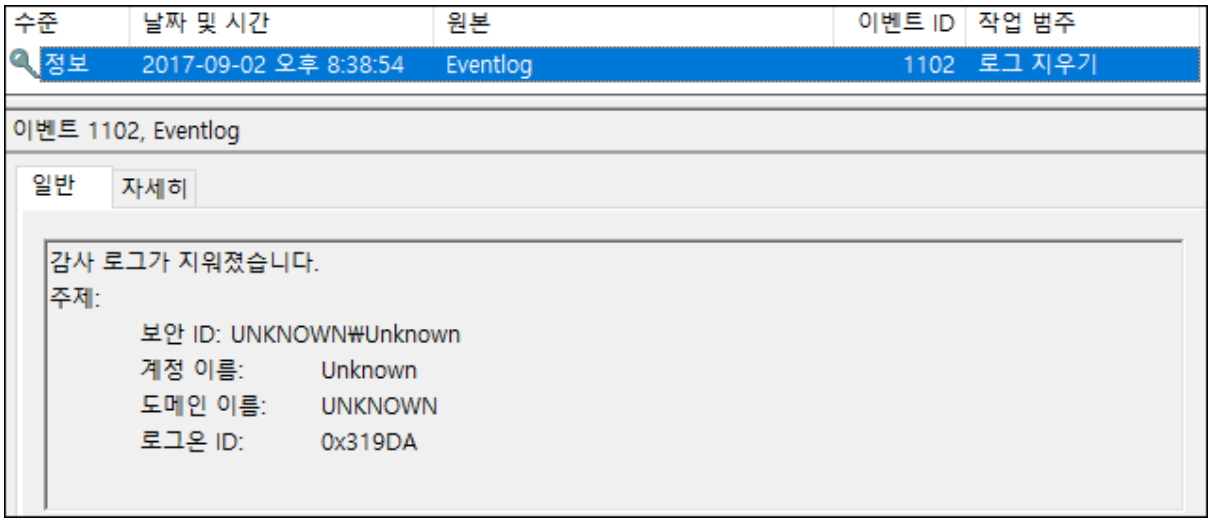
악의적인 사용자/공격자의 이벤트 로그의 삭제를 대비하여 제 3의 호스트에 윈도우 이벤트를 전달, 보관하는 체계를 구축해둔다면 이러한 이벤트 초기화 행위에 대해 대응할 수 있으나, 이러한 체계가 준비되지 않았을 경우 삭제된 레코드를 복구하여 분석하여야 한다.

구분	시나리오	이벤트 ID	비고
안티포렌식 목적 윈도우 이벤트 초기화 여부 / 시간 식별	악성코드 / 기업보안	1102,104	

7.2. 이벤트 상세 분석

7.2.1. 보안 로그의 삭제

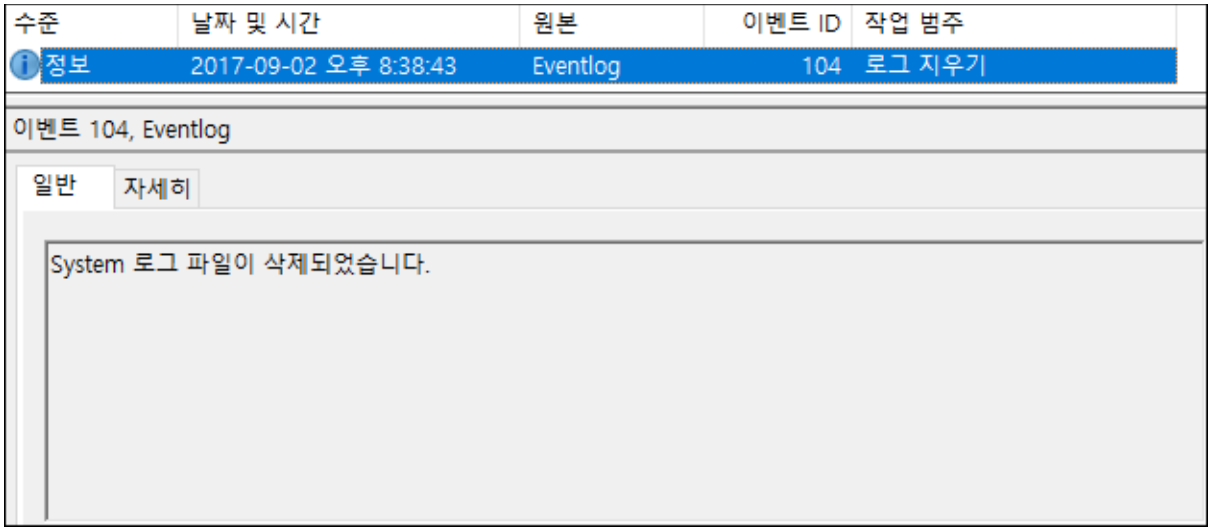
보안(Security) 로그 삭제 시 이벤트 ID 1102 가 기록된다.



<그림 39> Security 로그 삭제 시

7.2.2. 그 외 로그의 삭제

보안(Security) 로그 외 다른 로그가 삭제되었을 경우 이벤트 ID 102가 기록된다.



<그림 40> 그 외 로그 삭제 시

7.3. 주요 이벤트 ID 목록

Provider	Microsoft-Windows-Eventlog	**추가설정**	-
이벤트 ID	1102	**운영체제**	Win7 / Win10
발생조건	Security 이벤트 로그 삭제 시		
주요 속성 (XPath)	/Event/UserData/LogFileCleared/SubjectUserSid – 삭제한 사용자 SID /Event/UserData/LogFileCleared/SubjectUserName – 삭제한 사용자명 /Event/UserData/LogFileCleared/SubjectDomainName – 삭제한 사용자 도메인명 /Event/UserData/LogFileCleared/SubjectLogonId – 삭제한 사용자 로그온 ID		

Provider	Microsoft-Windows-Eventlog	**추가설정**	-
이벤트 ID	104	**운영체제**	Win7 / Win10
발생조건	Security 이외의 이벤트 로그 삭제 시		
주요 속성 (XPath)	/Event/UserData/LogFileCleared/Channel – 삭제된 로그의 Provider 이름 /Event/UserData/LogFileCleared/BackupPath – 삭제된 로그의 Backup Path /Event/UserData/LogFileCleared/SubjectUserName – 삭제한 사용자명 /Event/UserData/LogFileCleared/SubjectDomainName – 삭제한 사용자 도메인명		

8. 자동실행 등록

8.1. 분석 개요

웹 브라우저 또는 원격 접속 등 외부 침입을 통한 최초 공격 성공 이후 지속적인 공격을 위해 재부팅되더라도 악성 프로그램이 다시 실행될 수 있도록 작업 스케줄러, 시작 프로그램, 자동 실행 레지스트리에 등록하게 된다.

구분	시나리오	이벤트 ID	비고
시작 프로그램, 자동실행 레지스트리(로그온, BHO)에 등록된 악성 프로그램 정보	외부침입	4663 4657	
작업 스케줄러에 등록된 악성 프로그램 정보	외부침입	106 140 200 201	

<표 19> 자동실행 등록 이벤트를 통해 알 수 있는 정보

8.2. 이벤트 상세 분석

8.2.1. 작업 스케줄러 등록/실행

자동실행을 위한 작업 스케줄러는 at.exe, schtasks.exe 명령어를 이용하여 등록 할 수 있다. 작업 스케줄러에 등록되면 이벤트 ID 106, 140이 발생하며 각 명령어마다 발생 유무가 다르기 때문에 모두 확인이 필요하다.

구분	스케줄러 등록		스케줄러 변경	
	106	140	106	140
at.exe	O	O	-	-
schtasks.exe	O	X	X	O

작업 스케줄러에 등록된 특정 조건(날짜, 시간)이 만족하는 경우 실행되는 프로그램을 통해 어떤 프로그램이 실행되었는지 알 수 있다. 이벤트 ID 200, 201을 통해 실행된 명령어, 프로그램 시작/종료 여부를 확인할 수 있다.

8.2.2. 시작 프로그램 폴더/자동실행 레지스트리 등록

시작 프로그램 또는 자동실행 레지스트리에 악성 프로그램을 등록하는 경우 직접적인 관련 이벤트는 발생하지 않는다. 따라서 자동실행 등록 여부를 확인하기 위해서는 개체 액세스 감사 설정 후 각 자동 실행 대상 경로에 감사 설정을 해야만 확인할 수 있다. 로그온, BHO(Browser Helper Objects) 등록된 프로그램에 대하여 확인할 수 있다.

※ 부록. 폴더, 레지스트리 감사 설정 참고

구분	경로	비고
로그온	₩Users₩{사용자명}₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu₩Programs₩Startup ₩ProgramData₩Microsoft₩Windows₩Start Menu₩Programs₩Startup	폴더
	HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Userinit HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Shell HKLM₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩Wds₩rdpwd	
BHO	HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Browser Helper Objects HKCU₩Software₩Microsoft₩Internet Explorer₩UrlSearchHooksHKLM₩Software₩Microsoft₩Internet Explorer₩Toolbar HKLM₩Software₩Microsoft₩Internet Explorer₩Extensions	

<표 20> 시작 프로그램 폴더 / 자동실행 레지스트리 경로

8.3. 주요 이벤트 ID 목록

Provider	추가설정	이벤트 ID	발생조건
Microsoft-Windows-TaskScheduler	필요	106	스케줄러 등록
Microsoft-Windows-TaskScheduler	필요	140	스케줄러 변경
Microsoft-Windows-TaskScheduler	필요	200	스케줄러 동작 시작
Microsoft-Windows-TaskScheduler	필요	201	스케줄러 동작 완료
Microsoft-Windows-Security-Auditing	필요	4663	폴더 액세스
Microsoft-Windows-Security-Auditing	필요	4657	레지스트리 액세스

9. 윈도우 업데이트 기록

9.1. 분석 개요

침해사고 조사 시, 다양한 침해사고의 원인을 파악하기 위해 운영체제의 업데이트 기록을 통해 해당 시스템에서 발생 가능한 취약점 공격을 식별하여 조사 범위를 좁힐 수 있다.

Microsoft에서 제공하는 운영체제 업데이트 목록을 기반으로 윈도우 업데이트 이벤트 로그를 통해 해당 운영체제에서 업데이트 여부를 확인 후 취약점 공격 가능 여부 추정할 수 있다. 실제 보안점검/모의침투를 위한 오픈소스 도구인 'Windows-Exploit-Suggester'[4] 가 Microsoft에서 제공하는 업데이트 목록을 기반으로 적용 가능한 취약점을 식별하고 있으며, 이처럼 업데이트 기록은 초기 침해사고분석 시 중요한 아티팩트로 활용 될 수 있다.

구분	시나리오	이벤트 ID	비고
최근 운영체제 업데이트 기록	외부침입	19	

<표 21> 윈도우 업데이트 이벤트를 통해 알 수 있는 정보

9.2. 이벤트 상세 분석

9.2.1. 윈도우 업데이트 기록

윈도우 업데이트가 성공한 경우 19번 이벤트가 발생하며 발생된 이벤트를 통해 업데이트된 제품 종류, 시간 등을 확인할 수 있다.

그러나, 윈도우 업데이트 관련 이벤트는 System.evtx 파일에 기록되기 때문에, 일정시간이 지나면 다른 시스템 관련 이벤트 로그가 축적되어 최대 보존 크기에 도달, 업데이트 관련 이벤트가 삭제 될 가능성이 높다. 따라서 이벤트 로그만으로 전체 업데이트 기록을 확인하는데는 한계가 있으며, 최근 업데이트 목록 중 누락된 업데이트 또는 지속적인 업데이트 여부 등을 통해 해당 시스템에 악용 될 수 있는 취약점을 확인해야 한다.

9.3. 주요 이벤트 ID 목록

Provider	추가설정	이벤트 ID	발생조건
Microsoft-Windows-WindowsUpdateClient	불필요	19	업데이트 성공
Microsoft-Windows-WindowsUpdateClient	불필요	20	업데이트 실패

[4] https://github.com/GDSSecurity/Windows-Exploit-Suggester

10. 원격접속(RDP) 기록

10.1. 분석 개요

윈도우 기반 웹서버의 침해사고를 조사하다 보면, 웹 어플리케이션 취약점에 의해 침투된 후 공격자에 의해 생성된 사용자 계정에 의한 원격접속 행위가 흔히 발견된다. 원격접속 이벤트를 검토하여 공격자의 접속시간을 식별, 해당기간의 이벤트 로그 뿐만 아니라 파일시스템, 프리패치 등의 아티팩트를 추가 확인하여 공격자의 행위를 추정할 수 있다.

원격접속 관련 이벤트는 Microsoft-Windows-Security-Auditing, Microsoft-Windows-TerminalServices-RemoteConnectionManager, Microsoft-Windows-TerminalServices-LocalSessionManager Provider 에서 확인할 수 있다.

RDP 관련 이벤트 로그는 다양한 곳에 남지만, 각 영역마다 장단점이 있으므로 사고 발생 시점이나 목적 등을 고려하여 관련 증적을 적절하게 선택하여야 한다.

구분	시나리오	이벤트 ID	비고
원격접속 기록 확인을 통한 악성 공격자의 침입여부 식별	악성코드	4624,4625 21~25 1149,261	
원격접속 기록 확인을 통한 인가되지 않은 사용자의 접근 식별	기업보안		

10.2. 이벤트 상세 분석

10.2.1. Microsoft-Windows-Security-Auditing

Microsoft-Windows-Security-Auditing 에서는 보안과 관련된 다양한 로그가 기록된다. 원격접속 관련 이력은 명시적 자격 증명을 사용한 로그온(4648) 이후 로그온 이벤트(4624)가 발생하며, 로그오프 시 로그오프 이벤트(4647) 가 발생한다. 원격접속을 통해 로그인 되는 경우 로그온 타입 '10'과 원격지 IP, 세션 번호 등이 함께 기록된다.

'로그온 감사' 기능을 통해 실패한 로그온 이벤트를 감사하도록 설정할 시, 로그인에 실패했을 경우 로그온 실패 이벤트(4625)가 남게 되므로 RDP Bruteforce 공격의 시도 여부를 확인할 수 있다는 장점이 있다.

다만, Security.evtx에는 원격접속 외에도 다양한 보안 관련 로그가 축적되므로 최대 이벤트 크기에 도달해 오래된 원격 접속 이력이 지워질 가능성이 높다. 이러한 경우 개별 파일에 기록되는 LocalSessionManager, RemoteSessionManager 항목을 통해 추가확인할 필요가 있다.

10.2.2. Microsoft-Windows-TerminalServices-LocalSessionManager

Microsoft-Windows-TerminalServices-LocalSessionManager 에서는 로그온 성공(21), 셸 시작 알림(22), 세션 로그오프 성공(23), 세션 연결 끊김(24), 세션 다시 연결 성공(25) 이벤트를 통해 연결/해제 시점 및 재연결 여부 등을 보다 상세히 확인할 수 있다. 그러나 본 Provider에서는 로그온 실패 흔적과 접근 시도는 기록되지 않음을 유의하여야 한다.

10.2.3. Microsoft-Windows-TerminalServices-RemoteConnectionManager

Microsoft-Windows-TerminalServices-RemoteConnectionManager 에서는 사용자 인증 성공(RDP 접속) 시 이벤트 ID 1149가 생성되며, 사용자명, 도메인명, 원격지 IP를 확인 가능하다. 그러나 연결 해제시에는 별도의 이벤트가 생성되지 않으므로 해당 Provider를 통해 연결 종료시점은 확인하기 어렵다.

또한 RDP 포트로의 TCP 연결 수립 시 이벤트 ID 261을 가진 이벤트가 기록되나, 이는 정상적인 RDP 클라이언트 뿐만 아니라 단순 TCP 연결 수립 시에도 기록된다. 또 해당 이벤트에는 원격지 정보 등 유의미한 정보가 없기 때문에 단순히 특정 시간에 RDP 포트 접근이 발생했는지의 여부 확인만 가능하다.

10.3. 주요 이벤트 ID 목록

10.3.1. Microsoft-Windows-Security-Auditing (로그온)

Provider	Microsoft-Windows-Security-Auditing	**추가설정**	불필요
이벤트 ID	4624	**운영체제**	Win7 / Win10
발생조건	로그온 성공 시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="LogonType"] - 로그온 타입 * /Event/EventData/Data[@Name="IpAddress"] - 원격지 IP /Event/EventData/Data[@Name="IpPort"] - 원격지 Port /Event/EventData/Data[@Name="TargetUserSid"] - 대상 사용자 SID /Event/EventData/Data[@Name="TargetUserName"] - 대상 사용자 이름 /Event/EventData/Data[@Name="TargetDomainName] - 대상 도메인 이름 /Event/EventData/Data[@Name="TargetLogonId"] - 로그온 ID * RDP 접속의 경우, 로그온 타입이 '10'으로 찍힌다.		

Provider	Microsoft-Windows-Security-Auditing	추가설정	필요(실패감사)
이벤트 ID	4625	운영체제	Win7 / Win10
발생조건	로그온 실패 시 (‘로그온 감사 – 실패’ 설정 필요)		
주요 속성 (XPath)	/Event/EventData/Data[@Name="LogonType"] – 로그온 타입 * /Event/EventData/Data[@Name="IpAddress"] – 원격지 IP /Event/EventData/Data[@Name="IpPort"] – 원격지 Port /Event/EventData/Data[@Name="TargetUserSid"] – 대상 사용자 SID /Event/EventData/Data[@Name="TargetUserName"] – 대상 사용자 이름 /Event/EventData/Data[@Name="TargetDomainName] – 대상 도메인 이름 /Event/EventData/Data[@Name="FailureReason"] – 로그온 실패사유 * RDP 접속의 경우, 로그온 타입이 ‘10’으로 찍힌다.		

10.3.2. Microsoft-Windows-TerminalServices-LocalSessionManager

Provider	Microsoft-Windows-TerminalServices-LocalSessionManager	추가설정	-
이벤트 ID	21	운영체제	Win7 / Win10
발생조건	로그온 성공 시		
주요 속성 (XPath)	/Event/UserData/EventXML/User – 로그온한 사용자 /Event/UserData/EventXML/SessionID – 세션 ID /Event/UserData/EventXML/Address – 원본 네트워크 주소(원격지 주소)		

Provider	Microsoft-Windows-TerminalServices-LocalSessionManager	추가설정	-
이벤트 ID	22	운영체제	Win7 / Win10
발생조건	로그온 성공(셸 시작) 시		
주요 속성 (XPath)	/Event/UserData/EventXML/User – 로그온한 사용자 /Event/UserData/EventXML/SessionID – 세션 ID /Event/UserData/EventXML/Address – 원본 네트워크 주소(원격지 주소)		

Provider	Microsoft-Windows-TerminalServices-LocalSessionManager	**추가설정**	-
이벤트 ID	23	**운영체제**	Win7 / Win10
발생조건	세션 로그오프		
주요 속성 (XPath)	/Event/UserData/EventXML/User – 로그오프한 사용자 /Event/UserData/EventXML/SessionID – 세션 ID		

Provider	Microsoft-Windows-TerminalServices-LocalSessionManager	**추가설정**	-
이벤트 ID	24	**운영체제**	Win7 / Win10
발생조건	세션 연결 끊김		
주요 속성 (XPath)	/Event/UserData/EventXML/User – 로그오프한 사용자 /Event/UserData/EventXML/SessionID – 세션 ID /Event/UserData/EventXML/Address – 원본 네트워크 주소(원격지 주소)		

Provider	Microsoft-Windows-TerminalServices-LocalSessionManager	**추가설정**	-
이벤트 ID	25	**운영체제**	Win7 / Win10
발생조건	세션 재연결		
주요 속성 (XPath)	/Event/UserData/EventXML/User – 로그오프한 사용자 /Event/UserData/EventXML/SessionID – 세션 ID /Event/UserData/EventXML/Address – 원본 네트워크 주소(원격지 주소)		

10.3.3. Microsoft-Windows-TerminalServices-RemoteConnectionManager

Provider	Microsoft-Windows-TerminalServices-RemoteConnectionManager	추가설정	-
이벤트 ID	1149	운영체제	Win7 / Win10
발생조건	사용자 인증 성공(접속성공) 시		
주요 속성 (XPath)	/Event/UserData/EventXML/Param1 – 사용자명 /Event/UserData/EventXML/Param2 – 도메인 /Event/UserData/EventXML/Param3 – 원본 네트워크 주소(원격지 주소)		

Provider	Microsoft-Windows-TerminalServices-RemoteConnectionManager	추가설정	-
이벤트 ID	261	운영체제	Win7 / Win10
발생조건	RDP 포트 연결 시도 시(단순 TCP 연결시에도 기록)		
주요 속성 (XPath)	없음		

11. 어플리케이션 에러

11.1. 분석 개요

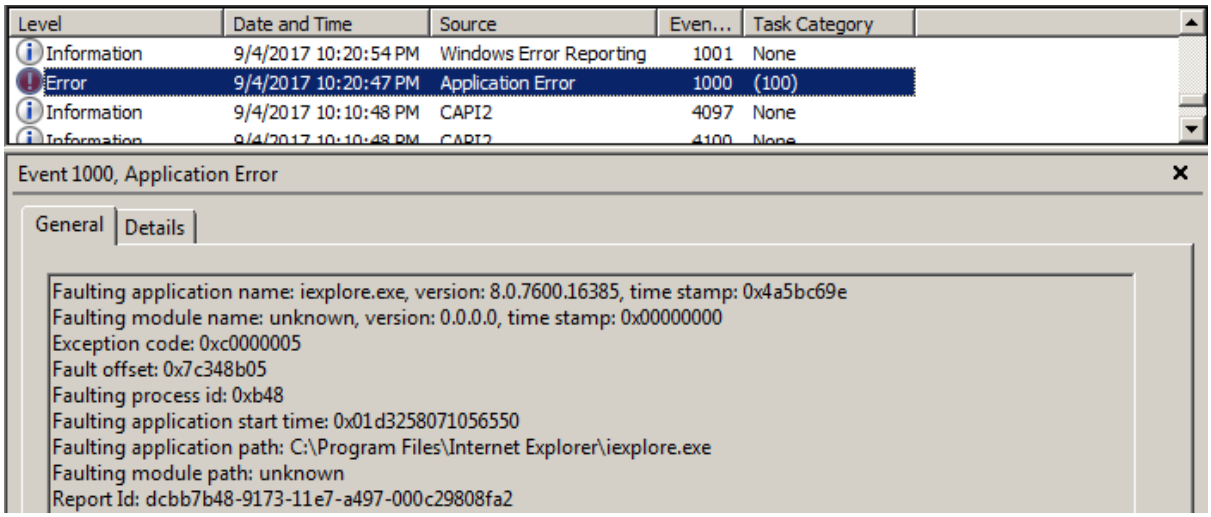
웹 브라우저 또는 문서 편집기 등의 메모리 핸들링 취약점을 이용한 익스플로잇이 동작되었을 경우, 어플리케이션 에러에 관한 정보가 이벤트 로그에 기록될 수 있다. 악성 프로세스가 식별되었을 경우, 해당 시간과 근접한 어플리케이션 에러 이벤트 등을 확인하여 원인이 된 어플리케이션을 추정할 수 있다.

구분	시나리오	이벤트 ID	비고
어플리케이션 에러 발생여부 확인	악성코드	1000, 1001	

11.2. 이벤트 상세 분석

11.2.1. Application Error

어플리케이션 에러 발생 시, 이벤트 ID 1000(Application Error)를 가진 이벤트가 기록된다. 해당 이벤트를 통해 오류가 발생한 프로세스 및 모듈의 버전, 타임스탬프, 오류 오프셋 등 상세한 정보를 확인할 수 있다.

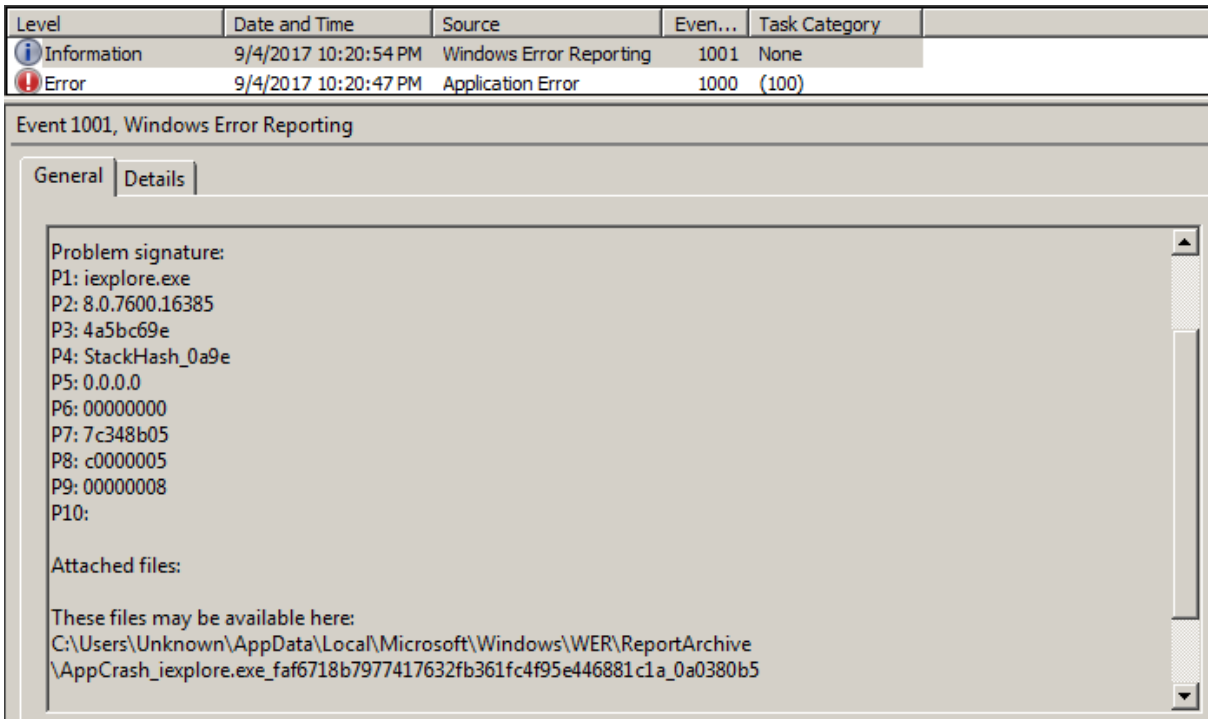


<그림 41> Application Error – Internet Explorer 크래시 예시

11.2.2. Windows Error Reporting

Microsoft에서 에러 정보를 수집하여 제품을 개선하기 위한 WER(Windows Error Reporting)에 의해 생성되는 이벤트 로그 또한 에러에 대한 정보를 제공하므로 어플리케이션 취약점 공격 수행 여부를 추정할 수 있다. 그러나 이벤트 로그만을 가지고

에러가 발생한 프로세스의 전체 경로를 확인하는 것은 불가능하며, 이벤트 내 남아있는 ReportArchive 파일의 경로를 통해 프로세스명(실행파일명) 정도만 확인할 수 있다.



<그림 42> WER – Internet Explorer 크래시 예시

11.2.3. 이외 활용가능한 이벤트

Microsoft-Windows-WER-Diag 의 일부 이벤트를 통해 에러 여부를 확인할 수 있으나, 알 수 있는 정보는 매우 제한적이다.

11.3. 주요 이벤트 ID 목록

Provider	Application Error	**추가설정**	-
이벤트 ID	1000	**운영체제**	Win7 / Win10
발생조건	어플리케이션 에러 발생 시		
주요 속성 (XPath)	/Event/EventData/Data[1] – 프로세스 이름 /Event/EventData/Data[2] – 프로세스 버전 /Event/EventData/Data[3] – 프로세스 타임스탬프 /Event/EventData/Data[4] – 오류 발생 모듈 이름 /Event/EventData/Data[5] – 오류 발생 모듈 버전 /Event/EventData/Data[6] – 오류 발생 모듈 타임스탬프 /Event/EventData/Data[7] – 예외 코드 /Event/EventData/Data[8] – 오류 오프셋 /Event/EventData/Data[9] – 오류 발생 프로세스 ID /Event/EventData/Data[10] – 오류 발생 프로세스의 시작 시간 /Event/EventData/Data[11] – 오류 발생 프로세스의 전체 경로 /Event/EventData/Data[12] – 오류 발생 모듈의 전체 경로 /Event/EventData/Data[13] – 보고서 ID		

Provider	Windows Error Reporting	**추가설정**	-
이벤트 ID	1001	**운영체제**	Win7 / Win10?
발생조건	어플리케이션 에러 발생 시		
주요 속성 (XPath)	/Event/EventData/Data[1] – 오류 버킷 /Event/EventData/Data[2] – 유형 /Event/EventData/Data[3] – 이벤트 이름 /Event/EventData/Data[4] – 응답 /Event/EventData/Data[5] – 캐비닛 ID		

12. 소프트웨어 설치

12.1. 분석 개요

시스템에 침투한 공격자는 자료 유출 등을 위해 FTP 서버 또는 클라이언트 프로그램을 설치하여 사용하기도 한다, 또한 직원의 비인가 소프트웨어 설치여부 적발 시에도 소프트웨어 설치 시 기록되는 이벤트 로그를 통해 식별할 수 있다.

구분	시나리오	이벤트 ID	비고
소프트웨어의 설치여부 확인(MSI 기반 인스톨러)	악성코드 /기업보안	1033,1034,1035	설치/제거/변경
소프트웨어의 설치여부 확인(비-MSI 기반 인스톨러)	악성코드 /기업보안	903,905,907	설치/제거/변경
소프트웨어의 설치여부 추정 (비-MSI 기반 인스톨러, Windows 10)	악성코드 /기업보안	28115	설치 한정
소프트웨어의 설치여부 확인(EXE 기반 인스톨러)	악성코드 /기업보안	4657	레지스트리 감사

12.2. 이벤트 상세 분석

12.2.1. MSI 기반 인스톨러에 의한 소프트웨어 설치/변경/제거

MSI 기반 인스톨러에 의한 소프트웨어 설치/제거/수정 시 이벤트 ID 1033,1034,1035(MsiInstaller)가 생성되며, 해당 이벤트를 통해 설치된 소프트웨어의 이름, 버전, 언어, 제조 업체 등을 확인할 수 있다.

또한, 설치/변경/제거 시 이벤트 ID 904/905/908 (Microsoft-Windows-Application-Experience)을 가진 이벤트 로그가 생성될 수 있다. 이 이벤트에서도 마찬가지로 설치된 소프트웨어의 이름, 버전, 언어, 제조 업체 등을 확인할 수 있다.

12.2.2. 비-MSI 기반 인스톨러에 의한 소프트웨어 설치/변경/제거 추정

비-MSI 기반 인스톨러에 의한 소프트웨어 설치/제거/수정 시, 이벤트 ID 903, 905, 907 (Microsoft-Windows-Application-Experience)를 가진 이벤트 로그가 생성된다. 이 이벤트에서도 마찬가지로 설치된 소프트웨어의 이름, 버전, 언어, 제조 업체 등을 확인할 수 있다.

12.2.3. Windows 10 - Microsoft-Windows-Shell-Core

Windows 10에서 프로그램 설치 시, 설치된 프로그램과 관련된 바로가기를 시작 메뉴에 등록하며 수행되는 앱 확인 프로그램 캐시에 추가하게 되며, 이러한 과정에서 이벤트 ID 28115(Microsoft-Windows-Shell-Core)를 가진 이벤트가 기록된다. 이를 통해 프로그램의 설치여부를 추측할 수 있다.

12.2.4. 레지스트리 감사 설정을 통한 소프트웨어 설치/변경/제거 확인

레지스트리 감사 설정을 통해 프로그램 설치 시 생성되는 Uninstall 키 (HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Uninstall)의 변경이력을 감사하도록 하여 설치된 프로그램을 식별할 수 있다. (Microsoft-Windows-Security-Auditing / 4657)

12.2.5. 이외 활용가능한 단서

이외에도, 제품 설치 시 윈도우 서비스가 추가되는 경우(웹 서버, DBMS 등) 서비스 등록에 관한 이벤트를 통해 추정할 수 있다. 또한 필터 드라이버가 사용되는 솔루션(원격제어 솔루션, 정보보호 솔루션 등)의 경우 해당 제품의 필터 드라이버가 최초 로드된 시점으로 설치시점을 추정할 수 있으나, 이를 위해서는 장기간의 로그 보존이 필요하다.

12.3. 상황별 조사가능 범위

유형	프로세스 추적 감사	레지스트리 감사	식별가능 정보
MSI	X	X	설치/변경/제거(MSIInstaller) 설치/변경/제거(Microsoft-Windows-Application-Experience)
Non-MSI	X	X	설치/변경/제거(Microsoft-Windows-Application-Experience)
MSI/Non-MSI (Windows 10)	X	X	설치(Microsoft-Windows-Shell-Core)
MSI/Non-MSI	O	X	설치 추정(실행파일명 내 특정 키워드 포함여부) 설치 추정(서비스 추가 이벤트를 통한 추정)
MSI/Non-MSI	X	O	설치/변경/제거(Uninstall 키 감사)

12.4. 주요 이벤트 ID 목록

12.4.1. MsiInstaller

Provider	MsiInstaller	추가설정	-
이벤트 ID	1033	운영체제	Win7 / Win10
발생조건	MSI 기반 소프트웨어 설치 시		
주요 속성 (XPath)	/Event/EventData/Data[1] – 설치된 제품의 이름 /Event/EventData/Data[2] – 설치된 제품의 버전 /Event/EventData/Data[3] – 설치된 제품의 언어 /Event/EventData/Data[4] – 설치 성공 또는 오류 상태 /Event/EventData/Data[5] – 제조 업체		

Provider	MsiInstaller	추가설정	-
이벤트 ID	1034	운영체제	Win7 / Win10
발생조건	MSI 기반 소프트웨어 제거 시		
주요 속성 (XPath)	/Event/EventData/Data[1] – 제거된 제품의 이름 /Event/EventData/Data[2] – 제거된 제품의 버전 /Event/EventData/Data[3] – 제거된 제품의 언어 /Event/EventData/Data[4] – 제거 성공 또는 오류 상태 /Event/EventData/Data[5] – 제조 업체		

Provider	MsiInstaller	추가설정	-
이벤트 ID	1035	운영체제	Win7 / Win10
발생조건	MSI 기반 소프트웨어 재구성(Repair) 시		
주요 속성 (XPath)	/Event/EventData/Data[1] – 재구성된 제품의 이름 /Event/EventData/Data[2] – 재구성된 제품의 버전 /Event/EventData/Data[3] – 재구성된 제품의 언어 /Event/EventData/Data[4] – 재구성 성공 또는 오류 상태 /Event/EventData/Data[5] – 제조 업체		

12.4.2. Microsoft-Windows-Application-Experience

Provider	Microsoft-Windows-Application-Experience	추가설정	-
이벤트 ID	903	운영체제	Win7 / Win10
발생조건	비-MSI 기반 소프트웨어 설치 시		
주요 속성 (XPath)	/Event/UserData/ProgramChangeInfoEvent/Name - 프로그램 이름 /Event/UserData/ProgramChangeInfoEvent/Version - 프로그램 버전 /Event/UserData/ProgramChangeInfoEvent/Publisher - 프로그램 제조사 /Event/UserData/ProgramChangeInfoEvent/Language - 프로그램 언어 /Event/UserData/ProgramChangeInfoEvent/ProgramID - 프로그램 ID		

Provider	Microsoft-Windows-Application-Experience	추가설정	-
이벤트 ID	904	운영체제	Win7 / Win10
발생조건	MSI 기반 소프트웨어 설치 시		
주요 속성 (XPath)	/Event/UserData/ProgramChangeInfoEvent/Name - 프로그램 이름 /Event/UserData/ProgramChangeInfoEvent/Version - 프로그램 버전 /Event/UserData/ProgramChangeInfoEvent/Publisher - 프로그램 제조사 /Event/UserData/ProgramChangeInfoEvent/Language - 프로그램 언어 /Event/UserData/ProgramChangeInfoEvent/ProgramID - 프로그램 ID /Event/UserData/ProgramChangeInfoEvent/MsiProductCode - MSI 제품코드 /Event/UserData/ProgramChangeInfoEvent/MsiPackageCode - MSI 패키지코드		

Provider	Microsoft-Windows-Application-Experience	추가설정	-
이벤트 ID	905	운영체제	Win7 / Win10
발생조건	소프트웨어 변경(Repair) 시		
주요 속성 (XPath)	/Event/UserData/ProgramChangeInfoEvent/Name - 프로그램 이름 /Event/UserData/ProgramChangeInfoEvent/Version - 프로그램 버전 /Event/UserData/ProgramChangeInfoEvent/Publisher - 프로그램 제조사 /Event/UserData/ProgramChangeInfoEvent/Language - 프로그램 언어		

	/Event/UserData/ProgramChangeInfoEvent/ProgramID – 프로그램 ID

Provider	Microsoft-Windows-Application-Experience	**추가설정**	-
이벤트 ID	907	**운영체제**	Win7 / Win10
발생조건	비-MSI 기반 소프트웨어 제거 시		
주요 속성 (XPath)	/Event/UserData/ProgramChangeInfoEvent/Name – 프로그램 이름 /Event/UserData/ProgramChangeInfoEvent/Version – 프로그램 버전 /Event/UserData/ProgramChangeInfoEvent/Publisher – 프로그램 제조사 /Event/UserData/ProgramChangeInfoEvent/Language – 프로그램 언어 /Event/UserData/ProgramChangeInfoEvent/ProgramID – 프로그램 ID		

Provider	Microsoft-Windows-Application-Experience	**추가설정**	-
이벤트 ID	908	**운영체제**	Win7 / Win10
발생조건	MSI 기반 소프트웨어 제거 시		
주요 속성 (XPath)	/Event/UserData/ProgramChangeInfoEvent/Name – 프로그램 이름 /Event/UserData/ProgramChangeInfoEvent/Version – 프로그램 버전 /Event/UserData/ProgramChangeInfoEvent/Publisher – 프로그램 제조사 /Event/UserData/ProgramChangeInfoEvent/Language – 프로그램 언어 /Event/UserData/ProgramChangeInfoEvent/ProgramID – 프로그램 ID /Event/UserData/ProgramChangeInfoEvent/MsiProductCode – MSI 제품코드 /Event/UserData/ProgramChangeInfoEvent/MsiPackageCode – MSI 패키지코드		

12.4.3. Microsoft-Windows-Shell-Core

Provider	Microsoft-Windows-Shell-Core	추가설정	-
이벤트 ID	28115	운영체제	Win10
발생조건	앱 확인 프로그램 캐시 내 응용 프로그램의 바로가기 추가 시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="Name"] – 바로가기 이름 /Event/EventData/Data[@Name="AppID"] – 원본 경로 /Event/EventData/Data[@Name="Flags"] – 플래그		

12.4.4. Microsoft-Windows-Security-Auditing (레지스트리 감사)

Provider	Microsoft-Windows-Security-Auditing	추가설정	필요
이벤트 ID	4657	운영체제	Win7 / Win10
발생조건	레지스트리 값 생성 또는 수정 시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="ObjectName"] – 개체 이름 /Event/EventData/Data[@Name="ObjectValueName"] – 개체 값 이름 /Event/EventData/Data[@Name="HandleId"] – 핸들 ID /Event/EventData/Data[@Name="OperationType"] – 작업 유형 /Event/EventData/Data[@Name="OldValueType"] – 이전 값 형식 /Event/EventData/Data[@Name="OldValue"] – 이전 값 /Event/EventData/Data[@Name="NewValueType"] – 새 값 형식 /Event/EventData/Data[@Name="NewValue"] – 새 값 /Event/EventData/Data[@Name="ProcessId"] – 프로세스 ID /Event/EventData/Data[@Name="ProcessName"] – 프로세스* * 설치프로그램 경로 또는 msiexec.exe 경로		
비고	아래 키에 대한 레지스트리 감사 설정 필요 HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Uninstall		

13. 윈도우 방화벽 정책

13.1. 분석 개요

시스템에 침투한 공격자는 악성 프로그램이 외부 C&C 서버와 통신하거나 정보를 유출할 수 있도록 운영체제에 설정된 방화벽에 예외처리 룰을 추가하거나 기존 방화벽 룰을 삭제하기도 한다. 이러한 악성프로그램의 행위를 파악하기 위해 방화벽 이벤트를 이용하여 방화벽 정책 현황을 확인할 수 있다.

구분	시나리오	이벤트 ID	비고
공격자에 의한 방화벽 룰 변경 여부	악성코드	2004 2005	
공격자에 의한 방화벽 비활성화 또는 룰 삭제 여부	악성코드	2003 2006	

<표 22> 윈도우 방화벽 이벤트를 통해 알 수 있는 정보

13.2. 이벤트 상세 분석

13.2.1. 방화벽 활성화/비활성화

방화벽 정책을 활성화 또는 비활성화 할 경우 이벤트 ID 2003이 발생하며, 정책 구분값(SettingValue)을 통해 활성화/비활성화 여부를 확인할 수 있다.

SettingValue	내용
01000000	활성화
00000000	비활성화

<표 23> 방화벽 활성화/비활성화 속성

13.2.2. 방화벽 룰 생성/수정

방화벽 룰을 새로 생성하거나, 기존 방화벽 룰 변경하게 되면 이벤트 ID 2004, 2005가 발생한다. 해당 이벤트의 주요 속성값을 이용하여 방화벽 정책 현황을 확인할 수 있다.

구분	속성값	내용
Direction	1	인바운드
	2	아웃바운드
Action	2	차단
	3	허용
Protocol	6	TCP
	17	UDP
	256	모두

<표 24> 방화벽 룰 생성/수정 주요 속성

13.2.3. 방화벽 룰 삭제

기존 방화벽 룰을 삭제할 경우 이벤트 ID 2006이 발생하며, 방화벽 룰 아이디 값을 이용하여 삭제가 가능하다.

13.3. 주요 이벤트 ID 목록

Provider	Microsoft-Windows-Windows Firewall With Advanced Security	**추가설정**	불필요
이벤트 ID	2004, 2005	**운영체제**	Win7 / Win10
발생조건	방화벽 룰 추가/변경시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="RuleId"] – 방화벽 룰 아이디 /Event/EventData/Data[@Name="RuleName"] – 방화벽 룰 이름 /Event/EventData/Data[@Name="ApplicationPath"] – 응용프로그램 /Event/EventData/Data[@Name="Direction"] – 방향 /Event/EventData/Data[@Name="Protocol"] – 프로토콜 /Event/EventData/Data[@Name="Action"] – 동작 /Event/EventData/Data[@Name="LocalPorts"] – 로컬 PORT /Event/EventData/Data[@Name="RemotePorts"] – 원격 PORT /Event/EventData/Data[@Name="LocalAddresses"] – 로컬 IP /Event/EventData/Data[@Name="RemoteAddresses"] – 원격 IP /Event/EventData/Data[@Name="ModifyingApplication"] – 방화벽 수정 프로그램 이름		

Provider	추가설정	이벤트 ID	발생조건
Microsoft-Windows-Windows Firewall With Advanced Security	불필요	2003	방화벽 켜기/끄기
Microsoft-Windows-Windows Firewall With Advanced Security	불필요	2006	방화벽 정책 삭제
Microsoft-Windows-Windows Firewall With Advanced Security	불필요	2010	네트워크 프로필 정보 수정

14. 문서 인쇄

14.1. 분석 개요

기밀 정보를 유출하고자 하는 악의적인 내부자는, 중요 자료를 인쇄하여 유출할 수 있다. 문서 인쇄 관련 이벤트 로그를 모니터링 하는 것은 이러한 시도를 탐지하는 데 도움을 줄 수 있으나, 문서 인쇄 이력을 확인할 수 있는 이벤트 로그 항목은 기본적으로 비활성화 되어있어 사전에 별도의 설정을 해두어야 한다.

'Microsoft-Windows-PrintService/Admin' 항목은 기본적으로 활성화 되어있으나, 해당 항목에는 성공한 인쇄 작업의 로그는 기록되지 않기 때문에 모든 문서의 인쇄 기록을 확인하기는 어렵다.

'Microsoft-Windows-PrintService/Operational' 항목은 기본적으로 비활성화 되어있어 별도의 활성화가 필요하지만, 활성화 하는 경우 프린터의 추가 및 삭제, 문서 인쇄 기록과 같은 활동을 이벤트 로그로 기록할 수 있어 인쇄를 통한 기밀정보 유출 시도를 탐지하는 데 유용하게 사용될 수 있다.

구분	시나리오	이벤트 ID	추가설정
기본 프린터 변경이력을 통한 주 사용 프린터 확인	기업보안	823	
프린터 추가 / 삭제 이력 확인	기업보안	823	필요
문서 출력이력 확인	기업보안	307 외 다수	필요

14.2. 이벤트 상세 분석

14.2.1. 기본 설정 프린터 변동이력

기본 프린터 설정 시 이벤트 ID 823을 가지는 이벤트 로그가 등록되며, 해당 항목을 통해 피조사자가 자주 사용하는 프린터나 과거에 기본으로 설정되었던 프린터 등을 식별할 수 있다.

14.2.2. 프린터 설치 / 삭제 이력 탐지

새 프린터가 설치되어 프린터 항목으로 등록될 때, 이벤트 ID 300이 발생하며 추가된 프린터의 이름을 확인할 수 있다. 프린터 삭제 시 이벤트 ID 302(삭제 예약), 301(삭제 완료) 가 차례로 발생하며 삭제 대상 프린터 이름을 확인할 수 있다.

14.2.3. 문서 인쇄 이력

문서가 한 번 인쇄될 때 이벤트 ID 800, 308, 309, 801, 842, 812, 805, 307 등 다양한 이벤트가 생성되며, 각 이벤트들에 유의미한 정보(파일명, 부수, 사용자, 프린터 등)가 분산되어 저장된다. 이러한 특성 상 문서 인쇄에 관한 상세한 정보를 얻기 위해서는 각 이벤트를 1회의 인쇄 행위로 묶어 볼 수 있는 방법이 필요하다.

문서 인쇄 시 인쇄 스풀러의 한 개 Thread에서 이벤트 ID 801, 842, 812, 805, 307을 생성하며, 생성된 이벤트에는 인쇄 스풀러의 프로세스 ID와 스레드 ID가 함께 기록된다. 이러한 특성을 이용하여, 유의미한 정보가 별도의 이벤트 ID를 가진 이벤트들에 분리되어 있더라도 /Event/System/Execution 태그의 ProcressID 및 ThreadID 속성을 통해 각 이벤트를 연결지을 수 있다.

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
 <System>
  <Provider Name="Microsoft-Windows-PrintService" Guid="{747EF6FD-E535-4D16-B510-
      42C90F6873A1}" />
  <EventID>307</EventID>
  . . . 중략 . . .
  <Execution ProcessID="1772" ThreadID="7944" />
  <Channel>Microsoft-Windows-PrintService/Operational</Channel>
  <Computer>Unknown</Computer>
</System>
 <UserData>
  <DocumentPrinted xmlns:auto-ns3="http://schemas.microsoft.com/win/2004/08/events"
      xmlns="http://manifests.microsoft.com/win/2005/08/windows/printing/spooler/core/events">
   <Param1>2</Param1>
   <Param2>공중전화번호책.pdf</Param2>
  . . . 중략 . . .
 </DocumentPrinted>
</UserData>
</Event>
```

<표 25> 문서 인쇄 이벤트의 ProcessID, ThreadID

이러한 특성을 이용하여 각 이벤트를 묶었을 때, 주요 이벤트 로그는 아래 표 와 같다.

이벤트 ID	특징
801	작업 ID
842	프린터명
812	**스풀 파일 경로**
805	인쇄부수, 해상도 등
307	**인쇄한 사용자, 인쇄된 문서 이름, 인쇄된 프린터**, 프린터 위치 등의 정보

<표 26> 이벤트 ID별 확인 가능한 문서 인쇄 정보

이벤트 ID 812 에서는 인쇄 스풀 파일의 경로를 획득할 수 있으며, 피조사자의 PC 내 해당 파일이 존재할 경우 해당 파일을 열어 확인하고, 삭제된 경우 해당 파일의 복구를 시도하여 인쇄된 문서를 확인할 수 있다.

이벤트 ID 307 에서는 인쇄한 사용자, 인쇄된 문서 이름, 인쇄된 프린터, 프린터 위치 등 인쇄에 관한 중요한 정보를 확인할 수 있다.

위치	인쇄한 사용자	문서번호	문서이름	프린터 이름	프린터 포트	페이지 수	부수	스풀 파일 경로	Time Created(Local)
\\김용현-인트라넷	X1210018	2	보물지도.hwp	SINDOH A401_407 Series PCL5e	IP_192_168_192_100	1	1	C:\Windows\system32\spool\PRINTERS\00002.SHD	2017-09-07 11:09:01.483346+09:00

Showing 1 to 1 of 1 rows

<그림 43> 문서 인쇄 목록 예시

14.3. 주요 이벤트 ID 목록

Provider	Microsoft-Windows-PrintService	**추가설정**	-
이벤트 ID	823	**운영체제**	Win7 / Win10
발생조건	기본 프린터 변경		
주요 속성 (XPath)	/Event/UserData/ChangingDefaultPrinter/NewDefaultPrinter – 새 프린터명		

Provider	Microsoft-Windows-PrintService	**추가설정**	필요
이벤트 ID	300	**운영체제**	Win7 / Win10
발생조건	새 프린터 추가		
주요 속성 (XPath)	/Event/UserData/PrinterCreated/Param1 – 추가된 프린터명		

Provider	Microsoft-Windows-PrintService	**추가설정**	필요
이벤트 ID	302	**운영체제**	Win7 / Win10
발생조건	프린터 삭제 Pending		
주요 속성 (XPath)	/Event/UserData/PrinterDeletionPending/Param1 – 삭제대상 프린터명		
Provider	Microsoft-Windows-PrintService	**추가설정**	필요

이벤트 ID	301	운영체제	Win7 / Win10
발생조건	프린터 삭제		
주요 속성 (XPath)	/Event/UserData/PrinterDeletion/Param1 – 삭제대상 프린터명		

Provider	Microsoft-Windows-PrintService	추가설정	필요
이벤트 ID	801	운영체제	Win7 / Win10
발생조건	작업 인쇄		
주요 속성 (XPath)	/Event/UserData/JobDiag/JobId – 작업 ID		

Provider	Microsoft-Windows-PrintService	추가설정	필요
이벤트 ID	842	운영체제	Win7 / Win10
발생조건	인쇄 작업 전송		
주요 속성 (XPath)	/Event/UserData/PrintDriverSandboxJobPrintProc/JobId – 작업 ID /Event/UserData/PrintDriverSandboxJobPrintProc/Processor - /Event/UserData/PrintDriverSandboxJobPrintProc/Printer - /Event/UserData/PrintDriverSandboxJobPrintProc/Driver - /Event/UserData/PrintDriverSandboxJobPrintProc/IsolationMode - /Event/UserData/PrintDriverSandboxJobPrintProc/ErrorCode – 에러코드		

Provider	Microsoft-Windows-PrintService	추가설정	필요
이벤트 ID	812	운영체제	Win7 / Win10
발생조건	파일 작업 실행		
주요 속성 (XPath)	/Event/UserData/FileOpFailed/Source – 스풀 파일 경로 /Event/UserData/FileOpFailed/ErrorCode – 오류 코드		

Provider	Microsoft-Windows-PrintService	추가설정	필요
이벤트 ID	805	운영체제	Win7 / Win10
발생조건	작업 렌더링		
주요 속성 (XPath)	/Event/UserData/RenderJobDiag/JobId – 작업 ID /Event/UserData/RenderJobDiag/GdiJobSize – 작업 사이즈 /Event/UserData/RenderJobDiag/Quality – 인쇄 품질 /Event/UserData/RenderJobDiag/Copies – 인쇄 부수		

Provider	Microsoft-Windows-PrintService	추가설정	필요
이벤트 ID	307	운영체제	Win7 / Win10
발생조건	문서 인쇄 성공 시		
주요 속성 (XPath)	/Event/UserData/DocumentPrinted/Param1 – 문서번호 /Event/UserData/DocumentPrinted/Param2 – 문서 이름* /Event/UserData/DocumentPrinted/Param3 – 인쇄한 사용자 /Event/UserData/DocumentPrinted/Param4 – 위치 /Event/UserData/DocumentPrinted/Param5 – 프린터 이름 /Event/UserData/DocumentPrinted/Param6 – 프린터 포트** /Event/UserData/DocumentPrinted/Param7 – 크기(작업 사이즈) /Event/UserData/DocumentPrinted/Param8 – 페이지 수 * Windows 8 이상인 경우 로컬 그룹 정책 편집을 통해 별도 설정 필요 (‘이벤트 로그에서 작업 이름 허용’ 항목) ** 경우에 따라 파일의 경로가 기록되기도 한다(PDF 변환용 가상프린터 등)		

15. 윈도우 계정관리

15.1. 분석 개요

악성코드 감염 등을 통해 시스템 침투에 성공한 공격자는 원격접속(RDP) 등 재침입을 위해 추가 계정을 생성할 수 있다. 따라서 침해사고 발생 시 윈도우 계정의 추가/삭제/수정 여부를 확인해야 한다.

구분	시나리오	이벤트 ID	비고
백도어 계정 생성 여부	악성코드	4720	
계정 비밀번호 변경 여부	악성코드	4724	

<표 27> 윈도우 계정 관리 이벤트를 통해 알 수 있는 정보

15.2. 이벤트 상세 분석

15.2.1. 윈도우 계정 추가

신규 계정을 추가할 경우 이벤트 ID 4720가 발생한다. 해당 이벤트를 통해 계정명, 홈 디렉토리, 도메인, 생성시간 등을 확인할 수 있다.

15.2.2. 비밀번호 변경

특정 계정의 비밀번호를 변경하면 이벤트 ID 4724가 발생한다. 사용하지 않는 계정의 비밀번호를 임의로 변경하여 사용하는 경우 해당 이벤트를 통해 비밀번호 변경여부를 확인할 수 있다.

15.3. 주요 이벤트 ID 목록

Provider	추가설정	이벤트 ID	발생조건
Microsoft-Windows-Security-Auditing	불필요	4720	계정 추가
Microsoft-Windows-Security-Auditing	불필요	4726	계정 삭제
Microsoft-Windows-Security-Auditing	불필요	4724	비밀번호 변경

16. 무선 네트워크 연결

16.1. 분석 개요

무선랜카드를 통해 네트워크에 연결하면 접속 이력이 윈도우 이벤트에 기록된다. 연결 이벤트를 통해 무선 AP SSID, 연결 시간 등 상세 정보를 확인할 수 있다.

구분	시나리오	이벤트 ID	비고
보안 정책 우회를 위한 비인가 네트워크 연결 정보	기업보안	8001	

<표 28> 무선 네트워크 이벤트를 통해 알 수 있는 정보

16.2. 이벤트 상세 분석

16.2.1. 무선 네트워크 접속

이벤트 ID 8000을 통해 무선 네트워크 접속 시도가 있었음을 알 수 있다. 이후 연결에 성공하는 경우 이벤트 ID 8001이 발생하고, 연결에 실패하면 이벤트 ID 8002가 발생한다. 연결에 성공한 AP의 상세 정보는 이벤트 ID 8001을 통해 확인할 수 있으며, 연결이 종료되는 경우 이벤트 ID 8003이 발생한다.

16.3. 주요 이벤트 ID 목록

Provider	Microsoft-Windows-WLAN-AutoConfig	**추가설정**	불필요
이벤트 ID	8001	**운영체제**	Win7 / Win10
발생조건	접속 성공시		
주요 속성 (XPath)	/Event/EventData/Data[@Name="SSID"] - SSID 이름 /Event/EventData/Data[@Name="PHYType"] - 계층타입 /Event/EventData/Data[@Name="AuthenticationAlgorithm"] - 인증방법 /Event/EventData/Data[@Name="CipherAlgorithm"] - 암호 알고리즘		

Provider	추가설정	이벤트 ID	발생조건
Microsoft-Windows-WLAN-AutoConfig	불필요	8000	연결 시도
Microsoft-Windows-WLAN-AutoConfig	불필요	8002	연결 실패
Microsoft-Windows-WLAN-AutoConfig	불필요	8003	연결 종료

V. 결론

지금까지 EVTX 파일 구조 및 목적별 분석방법, 시나리오별 주요 이벤트 로그 분석 절차를 제시하였다. 윈도우 이벤트 로그를 통해 침해사고 대응, 기업 보안 감사 등 다양한 관점에서의 분석이 가능하기 때문에 사건 해결에 매우 중요한 증거가 된다. 이처럼 윈도우 이벤트 로그는 디지털 포렌식 관점에서 중요한 증거이지만 태생적으로 세 가지 한계가 존재한다.

첫째. 기본적인 로깅 설정 이벤트만 기록된다.

운영체제 설치 후 별도로 설정하지 않으면 기본적으로 설정된 이벤트만 기록된다. 윈도우 이벤트 로그중 일부는 기록되지 않도록 설정되어 추가적으로 설정해야만 기록되거나, 감사 정책이 활성화 되어야 기록되는 이벤트가 다수 존재한다.

둘째. 기본 로그 저장 공간이 충분하지 않다.

각 로그별로 저장되는 용량의 경우 Security, System 로그의 경우 20MB 이며, 그외 대부분의 응용프로그램 로그는 1MB 용량까지만 저장되도록 기본 설정되어 있다. 로그 저장 공간이 최대치에 도달하게 되면, 기본적으로 기존 로그부터 삭제되고, 운영체제 활용 빈도에 따라 다르지만 수개월 이내 이벤트만 저장되어 있는 경우도 있다.

셋째. 기록된 로그 훼손이 쉽다.

윈도우 이벤트 로그는 사용자가 명령어나 삭제 기능을 통해 임의로 삭제할 수 있고 삭제된 경우 복구기법이 존재하지만 환경에 따라 실제 복구는 쉽지 않다.

이러한 한계 때문에, 사고 발생 이전에 충분한 로깅 설정이 되어있지 않은 경우 보안사고가 발생하여 윈도우 이벤트 로그를 분석할 시 유의미한 결과를 얻지 못할 수 있다.

그럼에도 불구하고 이러한 한계는 작은 노력을 통해 극복할 수 있다. 평소 침해사고, 정보유출과 같은 보안 사고가 언젠가는 반드시 발생할 것이라는 가정 하에 보안 사고에 대비하여 분석에 필요한 이벤트가 기록되도록 감사 로그 설정 및 사용하지 않는 이벤트를 활성화하고, 이벤트 로그 저장 용량도 충분히 설정해야 한다. 또한 주기적인 백업을 통해 삭제에 대비하는 것도 필요하다.

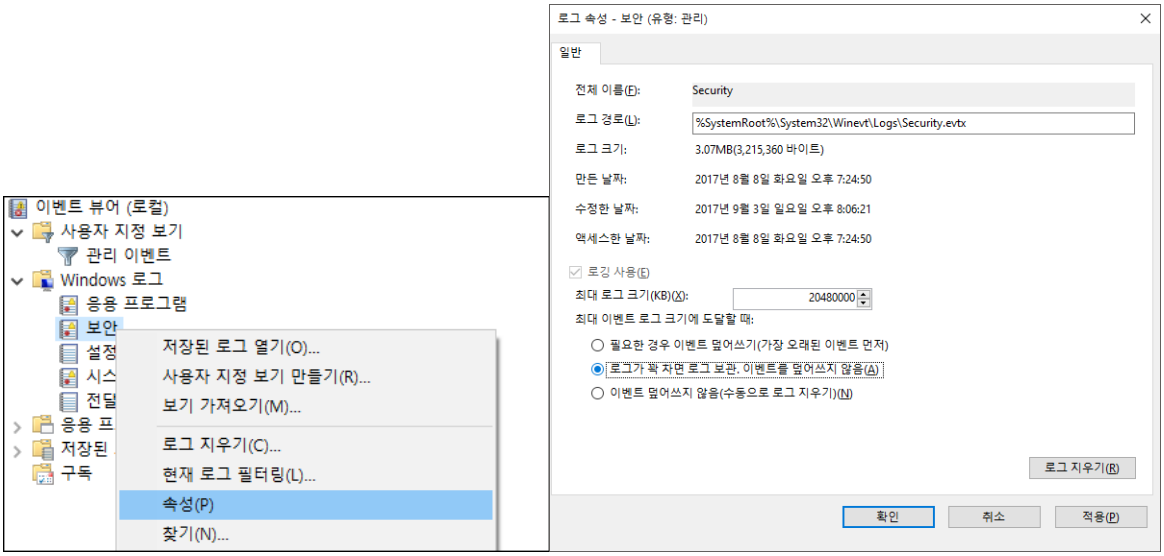
본 분석보고서와 윈도우 이벤트 로그 분석 프로그램을 통해 윈도우 이벤트 로그에 대한 디지털 포렌식 분석 기법 개발에 이바지할 수 있기를 기대한다.

VI. 부록

1. 이벤트 로그 최대 저장 용량 설정

일부 이벤트 로그는 System.evtx, Security.evtx, Application.evtx 에 통합 저장되고, 적은 기본 저장용량으로 인해(20MB) 사고 시점으로부터 오랜 기간이 지난 후 디지털 포렌식 분석을 진행한다면 유의미한 결과를 도출하기 어려울 수 있다.

따라서 이벤트 로그의 적절한 최대 저장 용량을 설정하여 실제 분석 시 유의미한 데이터를 얻을 수 있도록 사전에 대비하여야 한다.



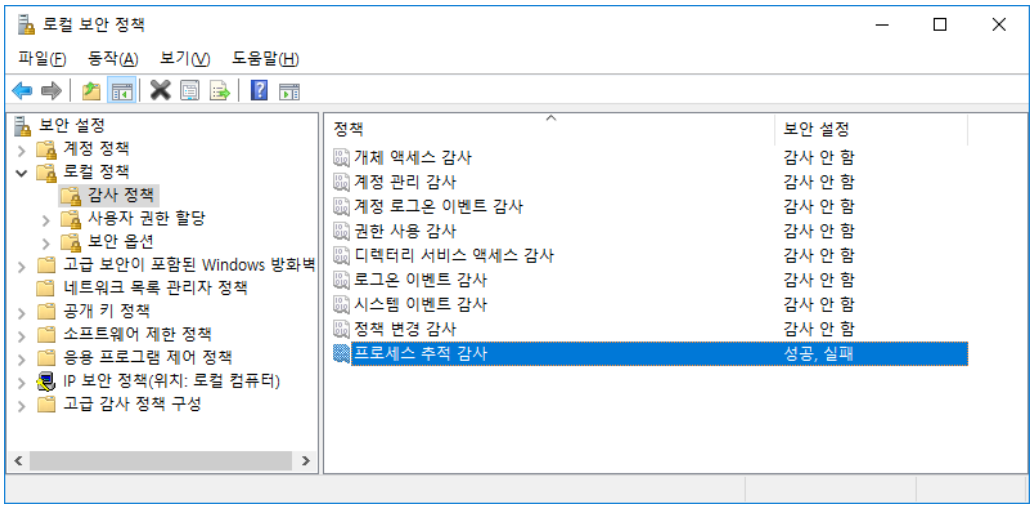
<그림 44> 이벤트 로그 최대 크기 설정

별도의 설정을 하지 않은 상태에서의 Application, Security, System 로그의 최대 저장 기본값은 20,480KB, '응용 프로그램 및 서비스 로그' 항목 내 이벤트 로그의 최대 저장 기본값은 1,024KB이며, 장기간의 로그를 보존하기 위해 이를 충분히 늘리는 것이 좋다.

또한, 이벤트 로그가 최대 크기에 도달했을 시, 로그를 삭제하지 않고 보관하도록 설정하여 오래된 보안사고도 분석할 수 있도록 대비하는 것이 필요하다. 그러나 큰 조직의 경우 장기간에 걸친 로그 생성에 따른 이벤트 로그 백업본으로 인해 가용 디스크 공간에 대한 이슈가 발생할 수 있다. 따라서 이벤트 로그 용량을 크게 설정하고 오래된 로그를 삭제하는 방법이나, 윈도우 이벤트 로그 구독 기능을 활용한 중앙관리시스템의 구축을 대안으로 생각해볼 수 있을 것이다.

2. 감사 항목 설정

감사 항목을 설정하기 위해서는 '제어판' -> '시스템 및 보안' -> '관리 도구' -> '로컬 보안 정책' -> '로컬 정책' 항목에서 활성화 가능하다.



<그림 45> 프로세스 추적 감사

각 감사 항목의 용도는 아래와 같다.

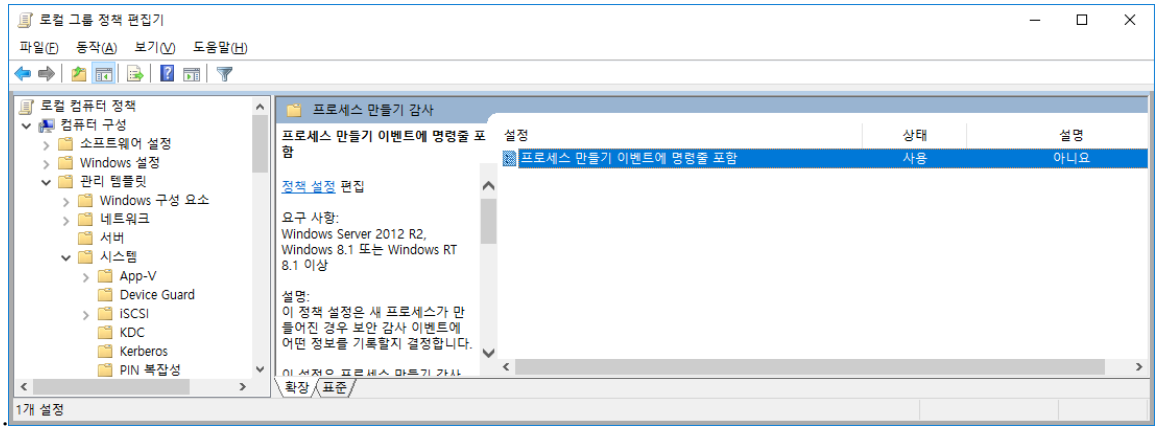
감사 항목	설명
개체 액세스 감사	파일, 폴더, 레지스트리 키, 프린터 등 감사 요구 사항을 지정하는 SACL이 있는 개체에 액세스하는 사용자의 이벤트를 감사
계정 관리 감사	컴퓨터의 각 계정 관리 이벤트를 감사
계정 로그온 이벤트 감사	다른 컴퓨터에서의 각 사용자 로그온/로그오프 인스턴스 감사
권한 사용 감사	권한을 사용하는 사용자의 각 인스턴스를 감사
디렉터리 서비스 액세스 감사	연결된 SACL(시스템 액세스 제어 목록)이 있는 Active Directory 디렉터리 서비스 개체에 대한 사용자 액세스를 감사
로그온 이벤트 감사	감사 이벤트를 기록하는 컴퓨터에 대한 사용자 로그온, 로그오프 또는 네트워크 연결의 각 인스턴스를 감사
시스템 이벤트 감사	사용자가 컴퓨터를 다시 시작하거나 종료할 경우 또는 컴퓨터 보안이나 보안 로그에 영향을 주는 이벤트가 발생할 경우에 감사
정책 변경 감사	모든 사용자 권한 할당 정책, Windows 방화벽 정책, 감사 정책 또는 신뢰 정책 변경 사항을 감사
프로세스 추적 감사	프로그램 활성화, 프로세스 종료, 핸들 복제 및 간접적 개체 액세스 등의 이벤트에 대한 자세한 추적 정보를 감사

<표 29> 감사 항목 및 용도

3. 프로세스 명령줄 감사 설정

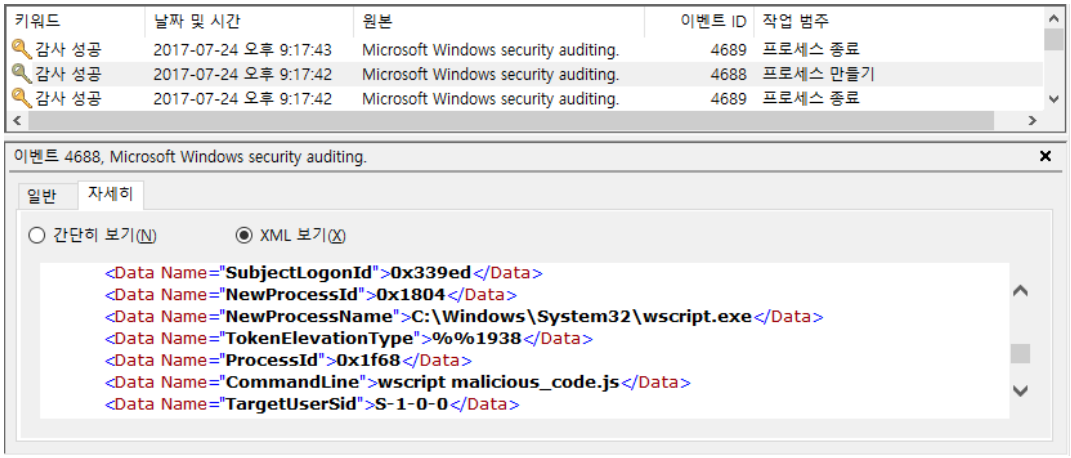
프로세스 추적 감사 기능 활성화 시 생성되는 프로세스 생성 이벤트(Microsoft-Windows-Security-Auditing / 4688)에서는 단순히 프로세스의 경로만 확인할 수 있기 때문에, 해당 프로세스가 어떠한 파라미터를 통해 실행되었는지까지는 확인할 수 없다. 따라서 악성코드 또는 시스템에 침투한 공격자에 의해 추가로 실행된 프로세스가 정확히 어떤 동작을 하였는지 등을 확인하기 어려운 경우가 있다.

윈도우 8.1 이상부터 도입된 **'프로세스 만들기 이벤트에 명령줄 포함'** 그룹 정책을 이용하면 프로세스가 실행될 때 사용된 명령줄을 함께 기록하여 보다 상세한 정보를 확인할 수 있다.



<그림 46> '프로세스 만들기 이벤트에 명령줄 포함' 정책

단, 이러한 정책을 활성화 하는 경우 아이디 및 패스워드, API 키 등이 명령행 인자로 전달되어 실행되는 프로그램들의 인자 또한 이벤트 로그에 기록될 수 있음을 유의하여야 한다.



<그림 47> wscript.exe에 의한 스크립트 실행 예시

만약 윈도우 7에서 프로세스 실행 시 사용된 명령줄을 확인하고자 한다면, Microsoft에서 제공하는 Sysmon(https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon)을 활용, Sysmon에 의해 생성되는 이벤트 로그를 확인하여야 한다.

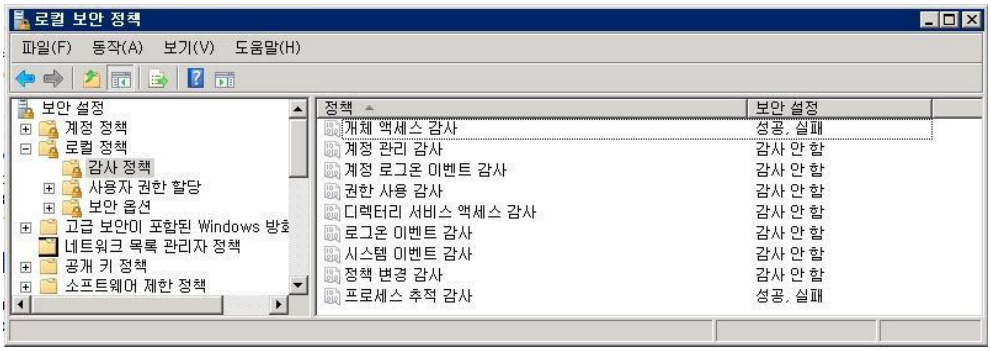
4. 개체 액세스 감사를 이용한 파일시스템/레지스트리 변경 로깅

파일시스템 및 레지스트리의 생성/수정/삭제 이력이 기록되도록 설정되어 있다면, 악성코드에 의한 지속실행 기법 사용여부 식별, 직원의 비인가 프로그램 설치 및 사용여부 적발, 열람한 문서 및 일시 확인 등 다양한 곳에 활용할 수 있다. 그러나 이러한 용도로 쓸 수 있는 개체 액세스 감사 기능은 기본적으로 비활성화 된 상태이며, 별도 활성화가 필요하다.

모든 파일시스템 및 레지스트리 관련 이벤트가 감사되도록 설정하면 좋겠지만, 파일시스템 및 레지스트리의 변경은 수시로 일어나는 관계로 이러한 모든 이력을 기록하는 경우 다른 중요한 이벤트 로그들까지 덮어쓰게 만들거나 디스크 용량을 고갈시키게 될 것이다.

따라서 로그의 보관성 측면에서나 분석의 용이성 측면에서 반드시 필요하며, 생성 / 수정 / 삭제 이벤트를 통해 유의미한 정보를 얻어낼 수 있는 경로만을 선별하여 기록하도록 설정하는 것이 중요하다.

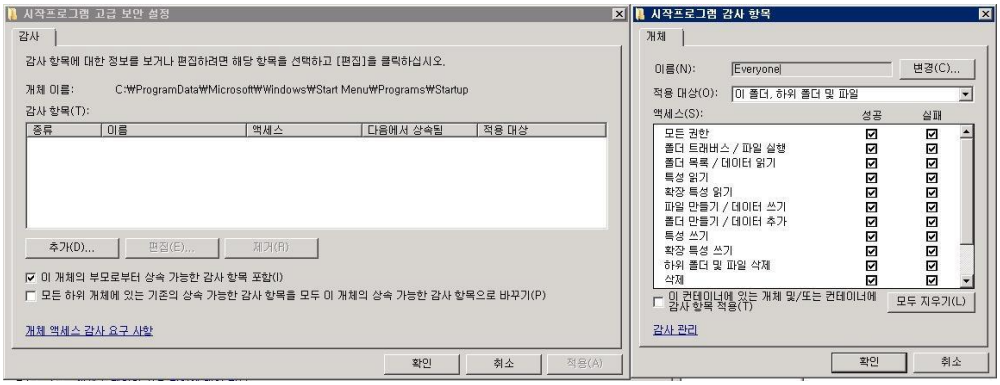
파일시스템 및 레지스트리 관련 이력을 이벤트 로그로 남기기 위해서는, 앞서 소개한 감사 항목 설정을 통해 '개체 액세스 감사' 설정을 활성화한 후, 아래 절차에 따라 감사 대상을 지정하여야 한다.



<그림 48> 감사로그 설정

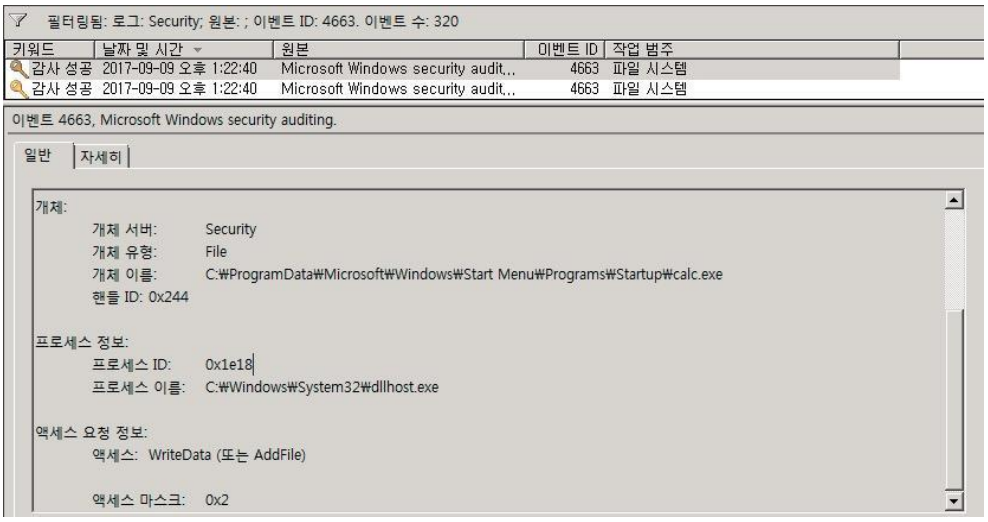
4.1. 파일시스템

탐색기를 이용하여 감사하고자 하는 디렉토리로 이동, 대상 디렉토리를 우클릭하여 '속성(R)' 을 클릭하여 디렉토리 속성 다이얼로그를 띄운 후 '보안'탭의 '고급(V)'을 클릭하여 고급 보안 설정 다이얼로그를 띄운다. 이후 '감사' 탭에 진입하여 적절한 감사 항목을 설정한다.



<그림 49> 파일 시스템 접근 로그 설정

위와 같은 설정을 마치고 나면, 해당 디렉토리 이하의 열람/수정/삭제 발생 시 관련 이벤트가 생성됨을 확인할 수 있다.

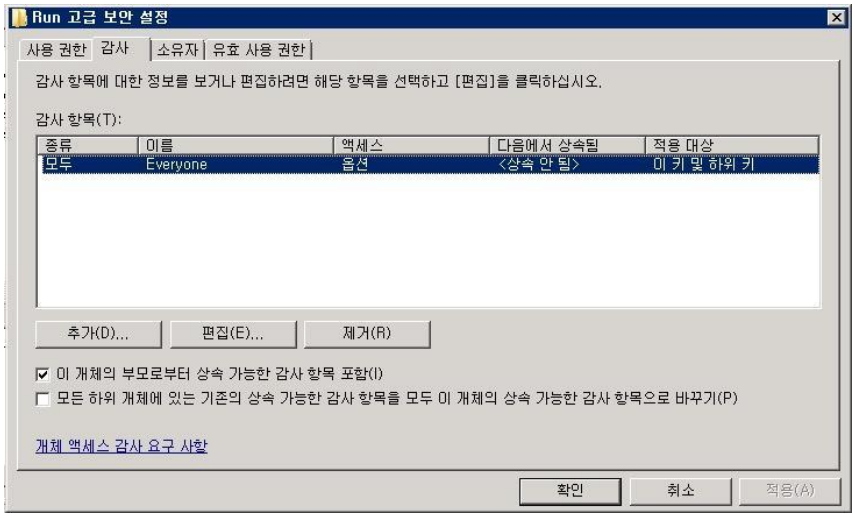


<그림 50> 파일 시스템 접근 시 감사 로그 기록

4.2. 레지스트리

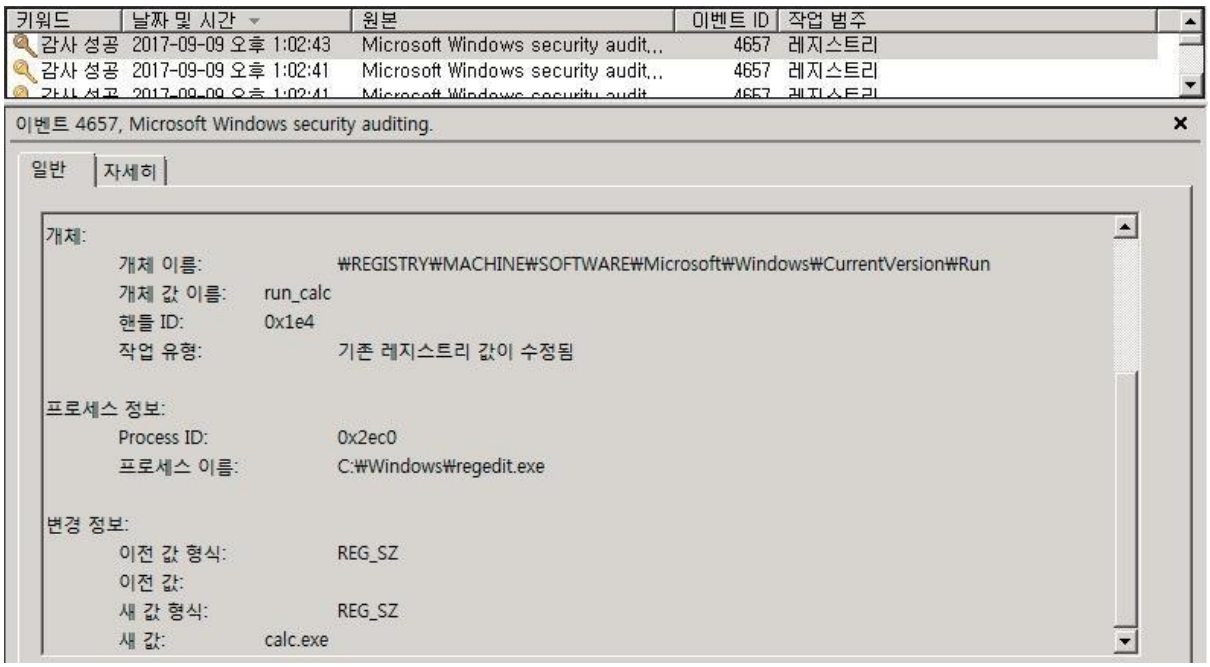
레지스트리 편집기를 이용하여 감사하고자 하는 키로 이동, 대상 키를 우클릭하여 '사용 권한(P)...' 을 클릭한 후 '고급'을 클릭하여 '감사' 탭으로 이동하여 감사 설정을 수행한다.

<그림 51> 레지스트리 접근 로그 설정1



<그림 52> 레지스트리 접근 로그 설정2

위와 같은 설정을 마치고 나면, 해당 키 이하의 레지스트리에 관한 열람/수정/삭제 발생 시 관련 이벤트가 생성됨을 확인할 수 있다.

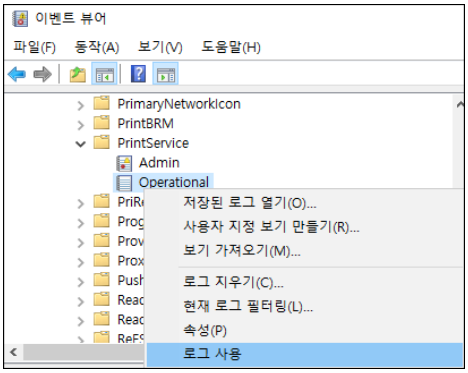


<그림 53> 레지스트리 접근 시 감사 로그 기록

5. 기타 비활성 이벤트 로그 항목 활성화

문서 인쇄 로깅, USB 장치 연결이력과 같은 행위도 이벤트 로그로 남길 수는 있다. 그러나 분석 시 유용한 일부 이벤트 로그는 기본적으로 활성화 되어있지 않거나 최대 저장용량이 적어 유의미한 이벤트 로그가 덮어쓰여질 수 있다. 따라서 포렌식 준비도 관점에서 사고 발생 이전에 해당 이벤트 항목들을 활성화하고, 저장 용량을 증가시키는 것이 권장된다.

활성화 설정은 이벤트 뷰어의 '응용 프로그램 서비스 로그' 항목 아래 각 이벤트 항목에서 우클릭 후 '로그 사용'을 클릭하여 활성화할 수 있다.



<그림 54> 문서 인쇄 이벤트 기록을 위한 예시

항목	설명
Microsoft-Windows-DriverFrameworks-UserMode	장치 연결 관련 (외장 저장매체 등)
Microsoft-Windows-PrintService	문서 인쇄*
Microsoft-Windows-Application-Experience	응용 프로그램 사용정보
Microsoft-Windows-TerminalServices-LocalSessionManager	원격접속(RDP) 기록
Microsoft-Windows-TerminalServices-RemoteConnectionManager	원격접속(RDP) 기록
Microsoft-Windows-WER-Diagnostics	어플리케이션 에러
Microsoft-Windows-WLAN-AutoConfig	무선 네트워크 연결
Microsoft-Windows-DNS-Client	DNS 요청 및 응답 등
Microsoft-Windows-NetworkProfile	네트워크 프로파일 관련
Microsoft-Windows-OfflineFiles	Offline Files 서비스 관련
Microsoft-Windows-Windows Defender	안티바이러스 로그 (Windows Defender)

<표 30> 주요 비활성 이벤트 로그 목록

* Windows 8 이상인 경우, 로컬 그룹 정책 편집을 통해 '이벤트 로그에서 작업 이름 허용' 항목을 활성화하여야 인쇄된 문서 이름이 기록된다.

6. 참고문서

1. 금융보안원. 금융회사 침해사고 준비도 가이드 : https://www.fsec.or.kr/common/proc/fsec/bbs/147/fileDownLoad/863.do
2. 김진국. 정보 유출 사고와 포렌식 준비도 : https://github.com/proneer/Slides/blob/master/Events/(KDFS2014)%20%EC%A0%95%EB%B3%B4%20%EC%9C%A0%EC%B6%9C%20%EC%82%AC%EA%B3%A0%EC%99%80%20%ED%8F%AC%EB%A0%8C%EC%8B%9D%20%EC%A4%80%EB%B9%84%EB%8F%84%20(Information%20Leakage%20and%20Readiness).pdf
3. 신용학. 윈도우 이벤트 로그 파일 (EVTX) 삭제 및 위변조에 대한 디지털 포렌식 복구 기술 연구 : https://www.riss.kr/search/detail/DetailView.do?p_mat_type=be54d9b8bc7cdb09&control_no=8551b7650d92effeffe0bdc3ef48d419
4. Dimitris Margaritis. Microsoft Sysmon Deployment : https://securitylogsdotorg.files.wordpress.com/2017/01/sysmon-2017-16-1.pdf
5. FORENSIC-PROOF(PRONEER). 윈도우 7 장치 연결/해제 이벤트 로그 (Windows 7 Device Tracking Event Log) : http://forensic-proof.com/archives/5945
6. Joachim Metz. Windows XML Event Log (EVTX) format : https://github.com/libyal/libevtx/blob/master/documentation/Windows%20XML%20Event%20Log%20(EVTX).asciidoc
7. JPCERT. Detecting Lateral Movement through Tracking Event Logs : https://www.jpcert.or.jp/english/pub/sr/ir_research.html
8. KALI-KM Security Study - 이벤트 로그의 개념
   A. http://kali-km.tistory.com/entry/Windows-Event-Log-1
   B. http://kali-km.tistory.com/entry/Windows-Event-Log-2---주요-이벤트-로그
9. Microsoft Technet - 감사 정책 : https://technet.microsoft.com/ko-kr/library/dd547945.aspx
10. NSA. Spotting the Adversary with Windows Event Log Monitoring : https://www.iad.gov/iad/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm
11. Quentin Jerome. Carving EVTX : https://rawsec.lu/blog/posts/2017/Jun/23/carving-evtx/