



K-Shield Jr.

# 03 EDR 시스템



K-Shield Jr.

# EDR 시스템을 이용하여 분석

DDJ : 피해자 PC 2 초기밀

winlog.event\_data.Image.keyword: Descending

C:\Users\DDJ\Downloads\Lock.exe

winlog.event\_data.ParentImage.keyword: Descending

C:\Users\DDJ\Downloads\Lock.exe

ImageLoaded

winlog.event\_data.ImageLoaded.keyword: Descending

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

C:\Users\DDJ\AppData\Local\Temp\ME15362\Cryptodon

TargetFilename

\_data.TargetFilename.keyword: Descending

Desktop\secret\보상청구서\_0405.docx.enc

Desktop\secret\보상청구서\_0507.docx.enc

Desktop\secret\보상청구서\_0610.docx.enc

Desktop\secret\보상청구서\_0704.docx.enc

Desktop\secret\보상청구서\_0814.docx.enc

Desktop\secret\보상청구서\_0909.docx.enc

Desktop\secret\보상청구서\_1003.docx.enc

C:\Users\DDJ\Downloads  
Lock.exe(4456)가 문서를  
암호화함 (18:35분 경)

C:\Users\DDJ\Desktop\secret\보상청구서\_0405.docx.enc  
C:\Users\DDJ\Desktop\secret\보상청구서\_0507.docx.enc  
C:\Users\DDJ\Desktop\secret\보상청구서\_0610.docx.enc  
C:\Users\DDJ\Desktop\secret\보상청구서\_0704.docx.enc  
C:\Users\DDJ\Desktop\secret\보상청구서\_0814.docx.enc  
C:\Users\DDJ\Desktop\secret\보상청구서\_0909.docx.enc  
C:\Users\DDJ\Desktop\secret\보상청구서\_1003.docx.enc  
C:\Users\DDJ\Desktop\secret\보상청구서\_1107.docx.enc  
C:\Users\DDJ\Desktop\secret\의료자문 동의서\_백병원.docx.enc  
C:\Users\DDJ\Desktop\secret\의료자문 동의서\_세브란스.docx.enc



문서 파일이 Lock.exe에게  
암호화 되었음



K-Shield Jr.

# EDR 시스템을 이용하여 분석

## DDJ : 피해자 PC 2 초기밀

프로세스 Id		부모 프로세스 Id	
winlog.event_data.ProcessId.keyword: Descending	Count	winlog.event_data.ParentProcessId.keyword: Descending	Count
4456	43	1536	1

프로토콜

Lock.exe의 PID 확인

프로세스 Id		부모 프로세스 Id	
winlog.event_data.ProcessId.keyword: Descending	Count	winlog.event_data.ParentProcessId.keyword: Descending	Count
1536	11	4244	1

프로토콜

1536의 PID의 PPID 확인



K-Shield Jr.

# EDR 시스템을 이용하여 분석

## PID 1536으로 검색

The screenshot displays the EDR interface with search results for PID 1536. The 'Image' column shows 'C:\Windows\Explorer.EXE' highlighted with a red box. The 'ParentImage' column shows 'No results found'. The 'ImageLocation' column shows 'No results found'. The 'ProcessName' column lists several files, with '\Downloads\Lock.exe' highlighted by a red box. A blue callout bubble is overlaid on the center of the screenshot.

winlog.event\_data.Image.keyword: Descending

C:\Windows\Explorer.EXE

No results found

No results found

No results found

\Desktop\새 폴더

\Downloads\Key.exe:Zone.Identifier

\Downloads\Lock.exe

\Downloads\Lock.exe:Zone.Identifier

\Downloads\rundll2.exe:Zone.Identifier

Explorer.exe가 Lock.exe와  
관련되어있다는 것을 확인  
(18:30분 경)



K-Shield Jr.

# EDR 시스템을 이용하여 분석

## Lock.exe 분석

프로세스 Id	부모 프로세스 Id
winlog.event_data.ProcessId.keyword: Descending	winlog.event_data.ParentProcessId.keyword: Descending
Count	Count
5604	1268
7152	4244
664	664
8784	8784

PID

PPID

1268

4244

~~664~~~~8784~~

Explorer.exe의  
부모 프로세스



# EDR 시스템을 이용하여 분석

## 1268 검색

Image

winlog.event\_data.Image.keyword: Descending

C:\Windows\SysWOW64\cmd.exe

ParentImage

winlog.event\_data.ParentImage.keyword: Descending

C:\Users\DDJ\Downloads\rundll2.exe

1268 : cmd.exe  
부모 프로세스 -> rundll2.exe  
(18:15분 경)

프로세스 Id	Count	부모 프로세스 Id	Count
1268	1	5552	1



# EDR 시스템을 이용하여 분석

## 1268 검색

The screenshot displays the EDR system's search results for keyword 1268. The interface is divided into four panels, each showing a list of events sorted by keyword in descending order.

- Image Panel:** Shows the file path `C:\Users\DDJ\Downloads\rundll2.exe` highlighted with a red box.
- ParentImage Panel:** Shows the file path `C:\Windows\explorer.exe` highlighted with a red box.
- ImageLoaded Panel:** Shows the file path `C:\Users\DDJ\Downloads\rundll2.exe` highlighted with a red box.
- TargetFilename Panel:** Shows two file paths highlighted with a red box: `C:\Users\DDJ\Desktop\Lock.exe` and `C:\Users\DDJ\Downloads\Lock.exe`.

A blue callout box in the center states: `rundll2.exe` 부모 프로세스 -> `explorer.exe`.

A blue callout box at the bottom lists the target file paths: `C:\Users\DDJ\Desktop\Lock.exe` and `C:\Users\DDJ\Downloads\Lock.exe`.



K-Shield Jr.

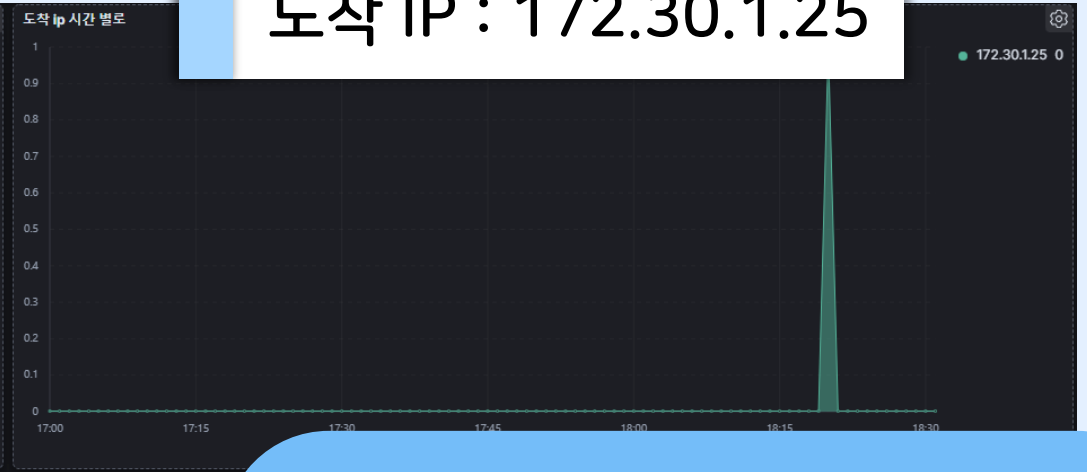
# EDR 시스템을 이용하여 분석

## 1268 검색

소스 IP : 172.30.1.35



도착 IP : 172.30.1.25



rundll2.exe

: 네트워크 연결한 것도 확인

소스 포트	도착 포트	프로토콜
winlog.event_data.Sour... Count	winlog.event_data.Destina... Count	winlog.event_data.Protocol.keyword: Descending Count
50804 1	443 1	tcp 1

포트 번호까지 알 수 있음





# EDR 시스템을 이용하여 분석

## Explorer.exe 분석

winlog.event\_data.Image.keyword: Descending

C:\Windows\Explorer.EXE

C:\Windows\Explorer.exe(4244)  
-> C:\Users\DDJ\Downloads  
office\RunMe.bat 생성 (15:47 경)

C:\Users\DDJ\Downloads\office\Office\Data\16.0.10379.2  
C:\Users\DDJ\Downloads\office\Office\Data\16.0.10379.2  
C:\Users\DDJ\Downloads\office\Office\Data\16.0.10379.2  
C:\Users\DDJ\Downloads\office\Office\Data\16.0.10379.2  
C:\Users\DDJ\Downloads\office\RunMe.bat  
C:\Users\DDJ\Downloads\office\Runtime\host\fxr\5.0.9\ho

< 1 2 3 4 5 ... 106 >



K-Shield Jr.

# EDR 시스템을 이용하여 분석

## cmd.exe 분석

Image	ParentImage	CommandLine
winlog.event_data.Image.keyword: Descending	winlog.event_data.ParentImage.keyword: Descending	Ascending
C:\Windows\System32\cmd.exe	C:\Windows\System32\wscript.exe	rs\DDJ\DOWNLO~1\office\ && "C:\Users\DDJ\DOWNLO~1\office\RunMe.bat"

C:\Windows\system32\cmd.exe /c

C:\Users\DDJ\Downloads\office\RunMe.bat

C:\Users\DDJ\AppData\Local\Temp  
getadmin.vbs 생성됨(15:48 경)



K-Shield Jr.

# EDR 시스템을 이용하여 분석

## cmd.exe 분석

winlog.event\_data.Image.keyword: Descending  
C:\Windows\system32\cmd.exe

CurrentVersion\Explorer  
: IE나 Explorer가 실행 될 때마다 등록된 DLL 실행함

악성코드의 지속성 예상

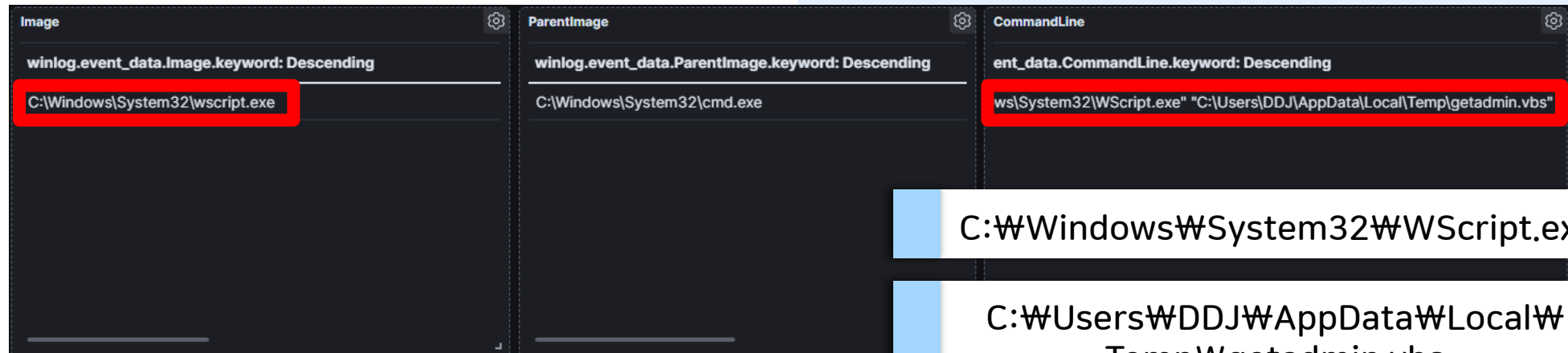
02\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts.vbs

HKU\WS-1-5-21-1908149527-2608072508-3932278328-1002\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts.vbs



# EDR 시스템을 이용하여 분석

## wscript.exe 분석



C:\Windows\System32\WScript.exe

C:\Users\DDJ\AppData\Local\Temp\getadmin.vbs

wscript.exe의 부모 프로세스

C:\Windows\System32\cmd.exe

getadmin.vbs를 실행



# EDR 시스템을 이용하여 분석

## Explorer.exe 분석

The screenshot displays three panels of event data from an EDR system. The 'Image' panel shows 'winlog.event\_data.Image.keyword: Descending' with 'C:\Windows\System32\cmd.exe' highlighted in a red box. The 'ParentImage' panel shows 'winlog.event\_data.ParentImage.keyword: Descending' with 'C:\Windows\System32\cmd.exe'. The 'CommandLine' panel shows 'ent\_data.CommandLine.keyword: Descending' with 'echo Set UAC = CreateObject("Shell.Application") : UAC.ShellExecute "cmd.exe"' highlighted in a red box. A callout box on the right contains the command: 'cmd /u /c echo Set UAC = CreateObject("Shell.Application") : UAC.ShellExecute "cmd.exe"'.

배치 파일 관리자 실행을 권유하지 않고  
강제로 관리자로 실행시키는 코드



K-Shield Jr.

# EDR 시스템을 이용하여 분석

## 경로 순회 공격 발견

```
CommandLine
Sort: Descending
Root\Client\AppVLp.exe" C:\Program Files (x86)\Microsoft Office\Root\Office1
ool Plus.exe"
dll32.dll,Control_RunDLL ".cpl:../../../../Temp/Low/msword.inf",
dll32.dll,Control_RunDLL ".cpl:../../../../Temp/msword.inf",
dll32.dll,Control_RunDLL ".cpl:../../../../AppData/Local/Temp/Low/msword.inf",
dll32.dll,Control_RunDLL ".cpl:../../../../AppData/Local/Temp/msword.inf",
```

< 1 2 3 4 5 6 >



# EDR 시스템을 이용하여 분석

## rundll2.exe 부모 프로세스 추적

**Image**  
winlog.event\_data.Image.keyword: Descending  
C:\Windows\SysWOW64\rundll32.exe

**ParentImage**  
winlog.event\_data.ParentImage.keyword: Descending  
C:\Windows\SysWOW64\control.exe

**CommandLine**  
winlog.event\_data.CommandLine.keyword: Descending  
"C:\Windows\system32\rundll32.exe" Shell32.dll,Control\_RunDLL ".cpl:../..../.."/>

프로세스 Id	부모 프로세스 Id
winlog.event_data.ProcessId.keyword: Descending	winlog.event_data.ParentProcessId.keyword: Descending
Count	Count
10064	3260
1744	3772
2780	7332
6320	9800



# EDR 시스템을 이용하여 분석

3260, 3772, 9800 검색

악성코드는 WINWORD.exe  
관계되어있다는 것을 확인 가능

3260

event\_data.Image.keyword: Descending

C:\Windows\system32\wuauclt.exe

C:\Windows\SysWOW64\control.exe

ata.ParentImage.keyword: Descending

§ (x86)\Microsoft Office\root\Office16\WINWORD.EXE

C:\Program Files (x86)\Microsoft  
Office\root\Office16\WINWORD.EXE

3772

event\_data.Image.keyword: Descending

C:\Windows\SysWOW64\control.exe

C:\Windows\SysWOW64\rundll32.exe

ParentImage

ata.ParentImage.keyword: Descending

§ (x86)\Microsoft Office\root\Office16\WINWORD.EXE

C:\Program Files (x86)\Microsoft  
Office\root\Office16\WINWORD.EXE

9800

event\_data.Image.keyword: Descending

C:\Windows\SysWOW64\control.exe

ent\_data.ParentImage.keyword: Descending

n Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

C:\Program Files (x86)\Microsoft  
Office\root\Office16\WINWORD.EXE





# 04 프로젝트 이후 계획



## 프로젝트 이후 해보고 싶은 것

K-Shield Jr. 가 끝난 뒤

완성하지 못한 시나리오 토폴로지 수정

분석한 결과에 대한 레포트 파일 작성 시스템 구현

프로세스 위협 점수를 매긴 뒤 그에 따른 알림 시스템 구현

기존에 분석이 되어있는 위협들에 대해 자동으로 탐지하는 시스템 구현