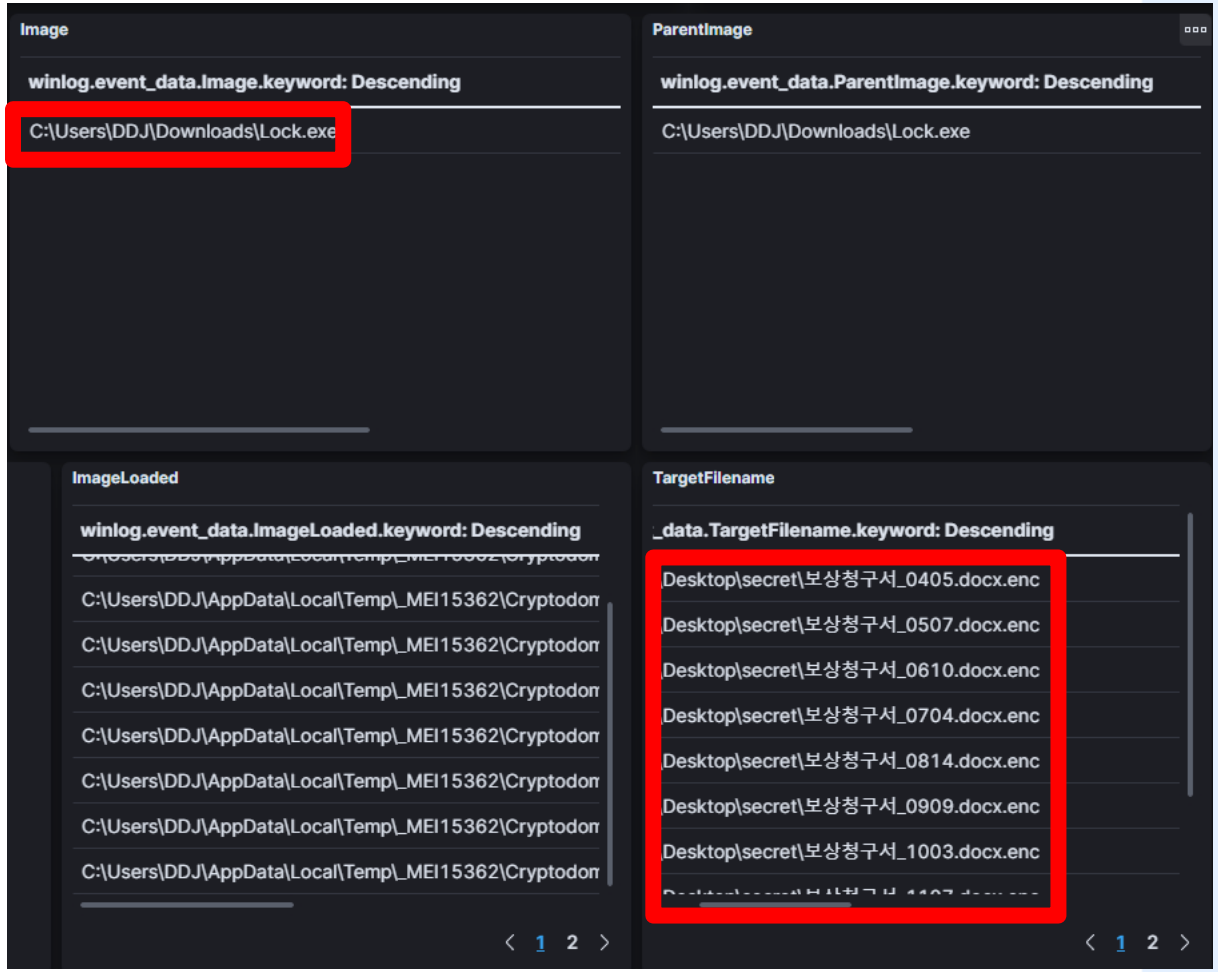
K-Shield Jr.

03
EDR 시스템

K-Shield Jr.

EDR 시스템을 이용하여 분석

DDJ : 피해자 PC 2 최기밀



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 최기밀

프로세스 id

winlog.event_data.ProcessId.keyword: Descending	Count
4456	43

부모 프로세스 id

winlog.event_data.ParentProcessId.keyword: Descending	Count
1536	1

프로토콜

Lock.exe의 PID 확인

프로세스 id

winlog.event_data.ProcessId.keyword: Descending	Count
1536	11

부모 프로세스 id

winlog.event_data.ParentProcessId.keyword: Descending	Count
4244	1

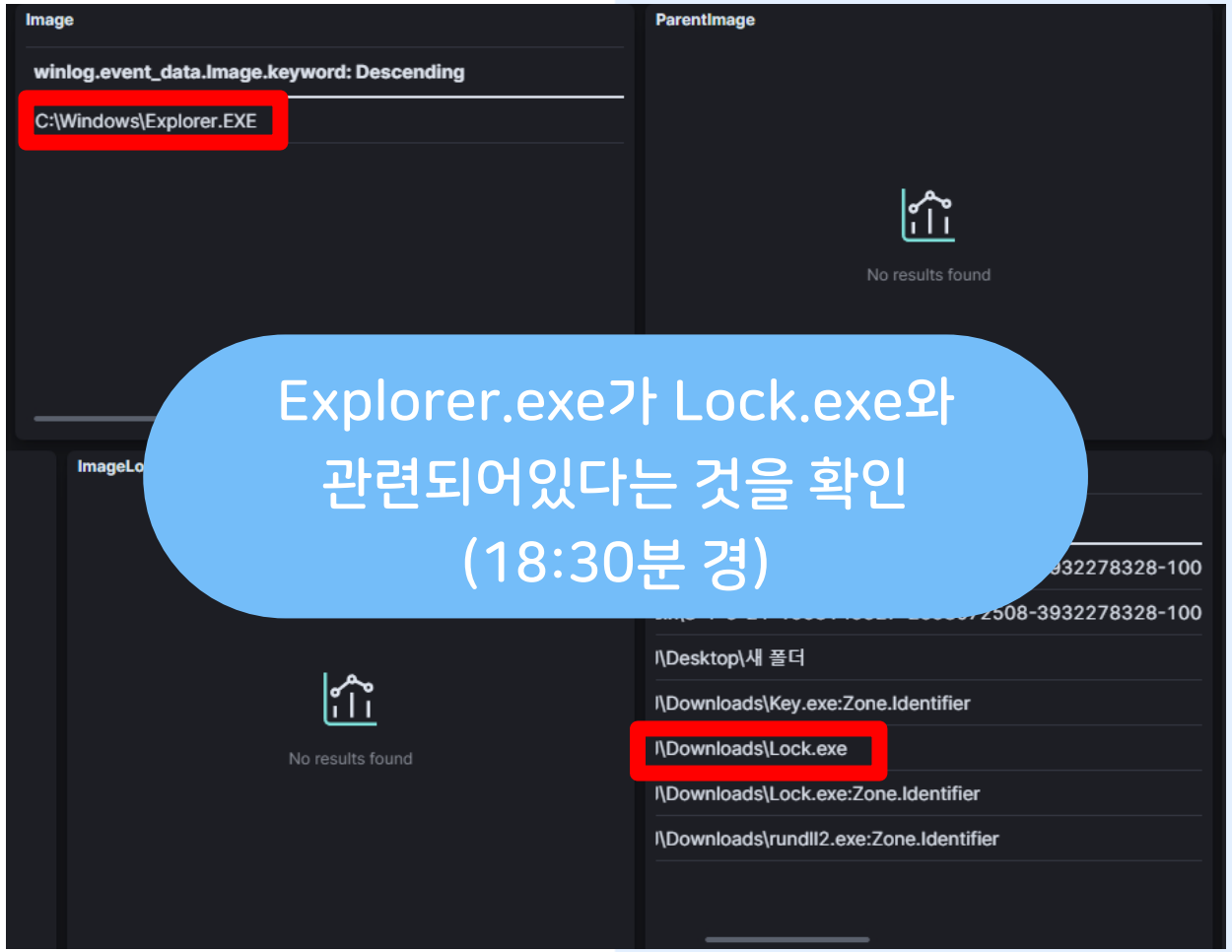
프로토콜

1536의 PID의 PPID 확인

K-Shield Jr.

EDR 시스템을 이용하여 분석

PID 1536으로 검색



K-Shield Jr.

EDR 시스템을 이용하여 분석

Lock.exe 분석

프로세스 id

winlog.event_data.ProcessId.keyword: Descending	Count
5604	529
7152	528
664	9
8784	7

PID

부모 프로세스 id

winlog.event_data.ParentProcessId.keyword: Descending	Count
1268	1
4244	1
664	1
8784	1

PPID

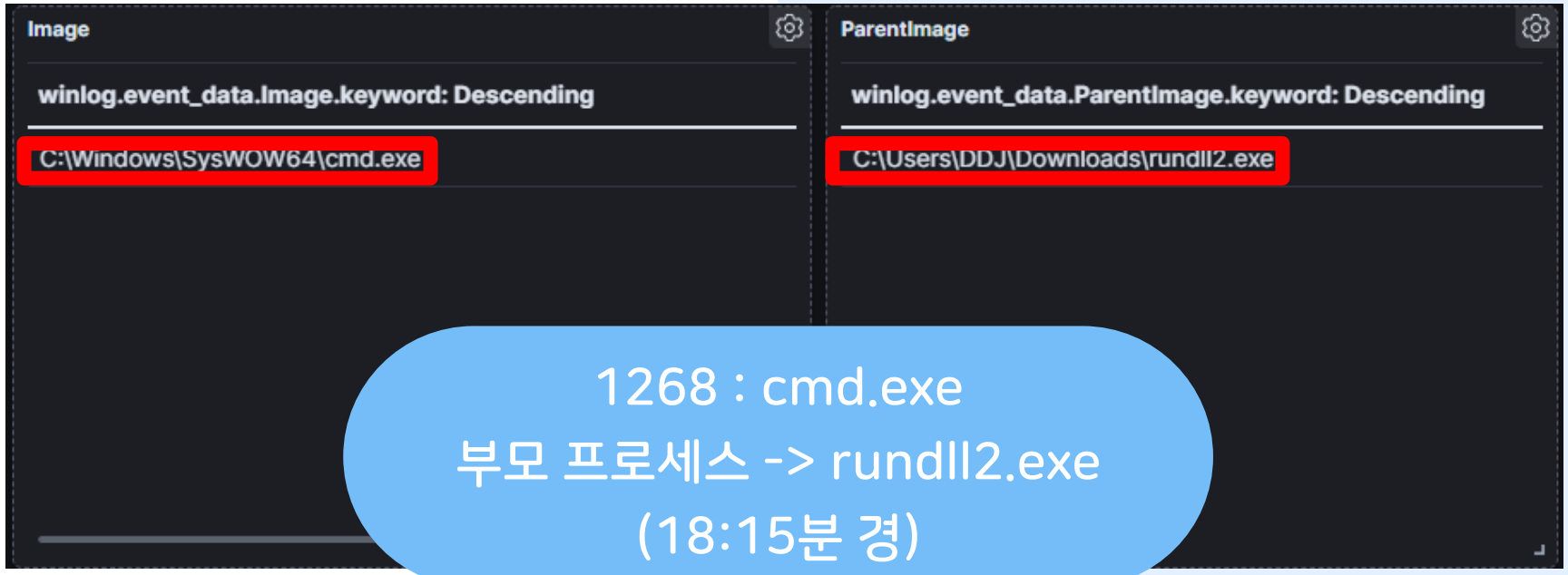
1268 4244 ~~664~~ ~~8784~~

Explorer.exe의
부모 프로세스

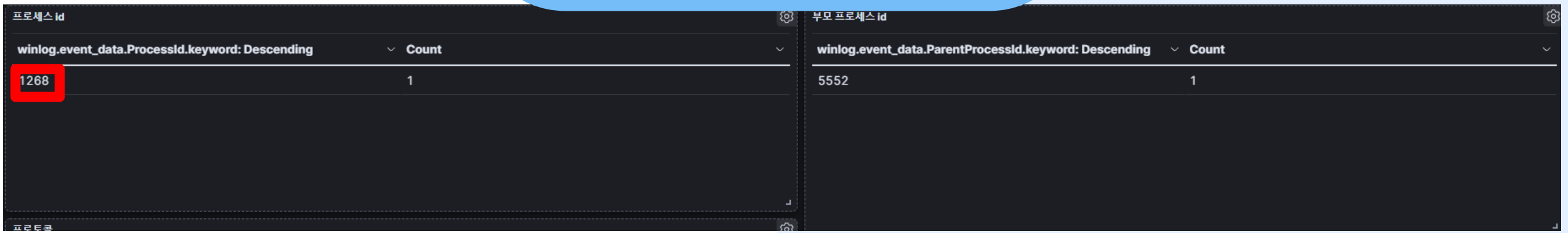
K-Shield Jr.

EDR 시스템을 이용하여 분석

1268 검색



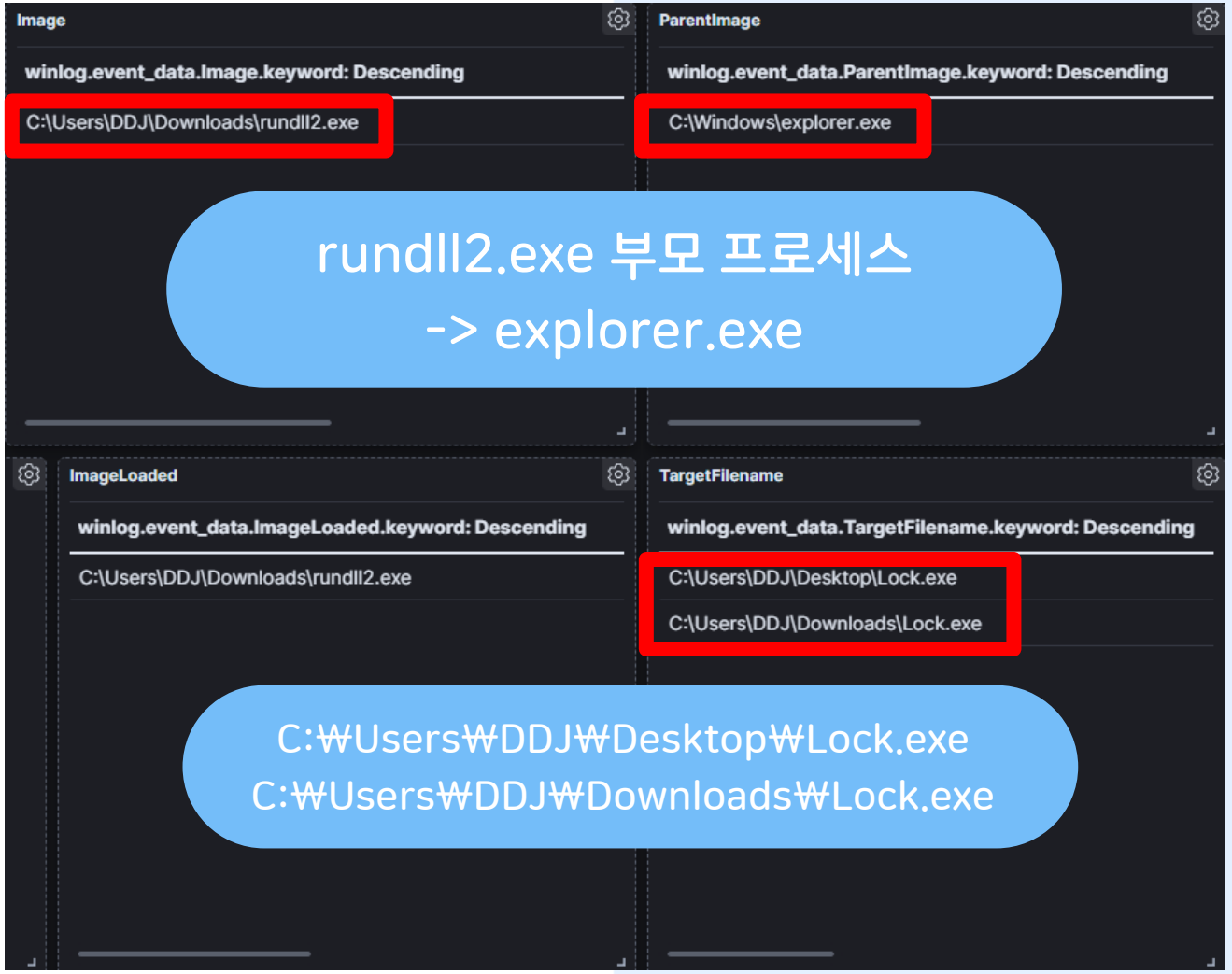
1268 : cmd.exe
부모 프로세스 -> rundll2.exe
(18:15분 경)



K-Shield Jr.

EDR 시스템을 이용하여 분석

1268 검색



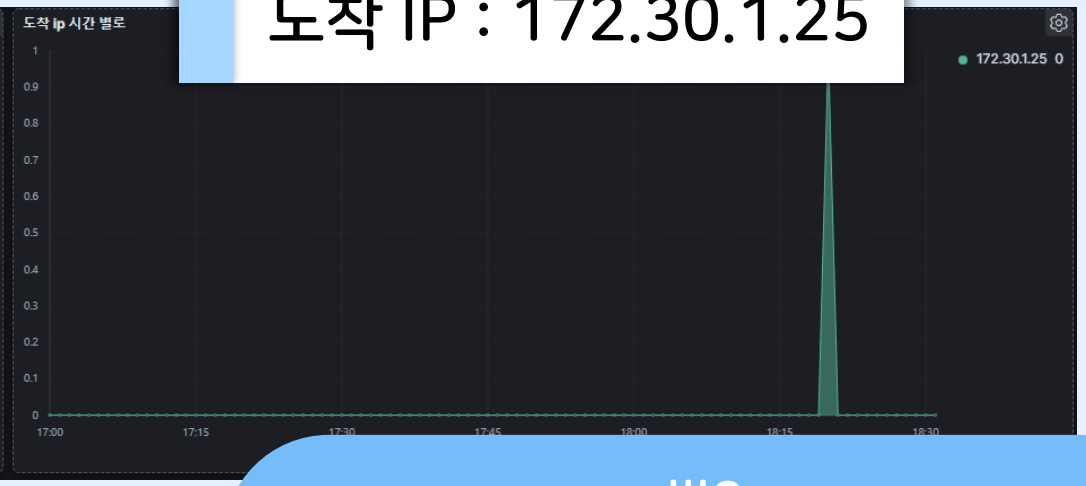
K-Shield Jr.

EDR 시스템을 이용하여 분석

1268 검색

소스 IP : 172.30.1.35

도착 IP : 172.30.1.25



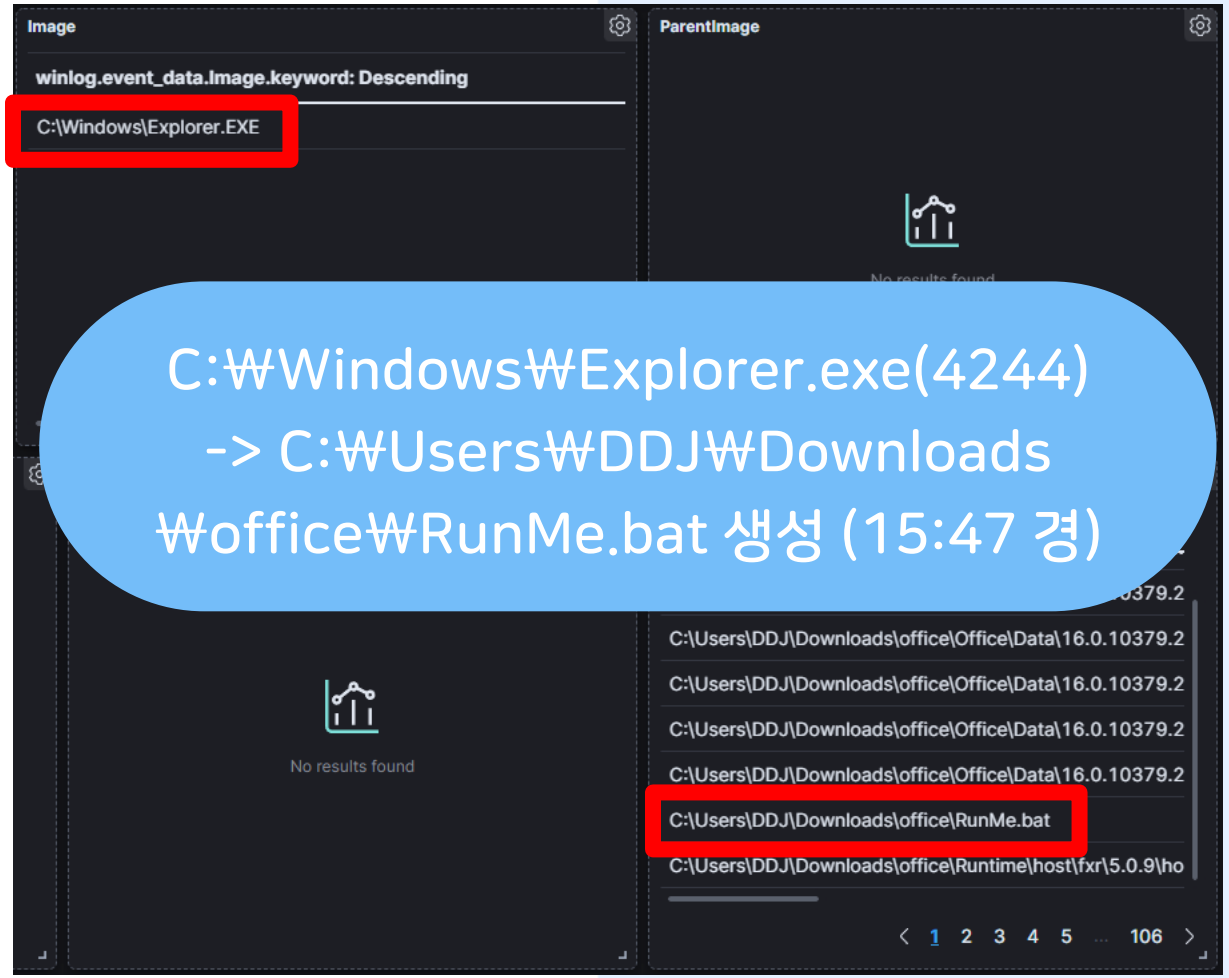
rundll2.exe
: 네트워크 연결한 것도 확인

포트 번호까지 알 수 있음

K-Shield Jr.

EDR 시스템을 이용하여 분석

Explorer.exe 분석

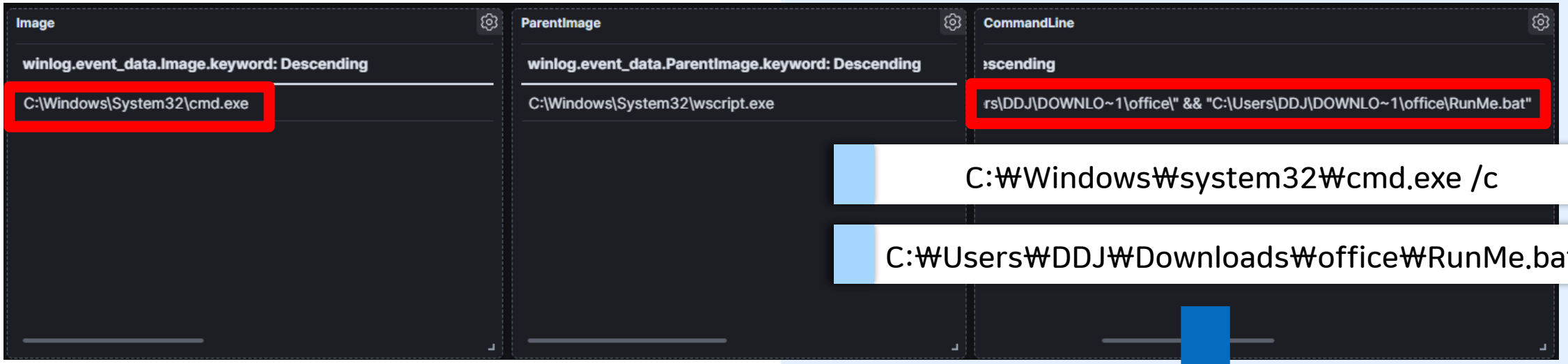


C:₩Windows₩Explorer.exe(4244)
-> C:₩Users₩DDJ₩Downloads
₩office₩RunMe.bat 생성 (15:47 경)

K-Shield Jr.

EDR 시스템을 이용하여 분석

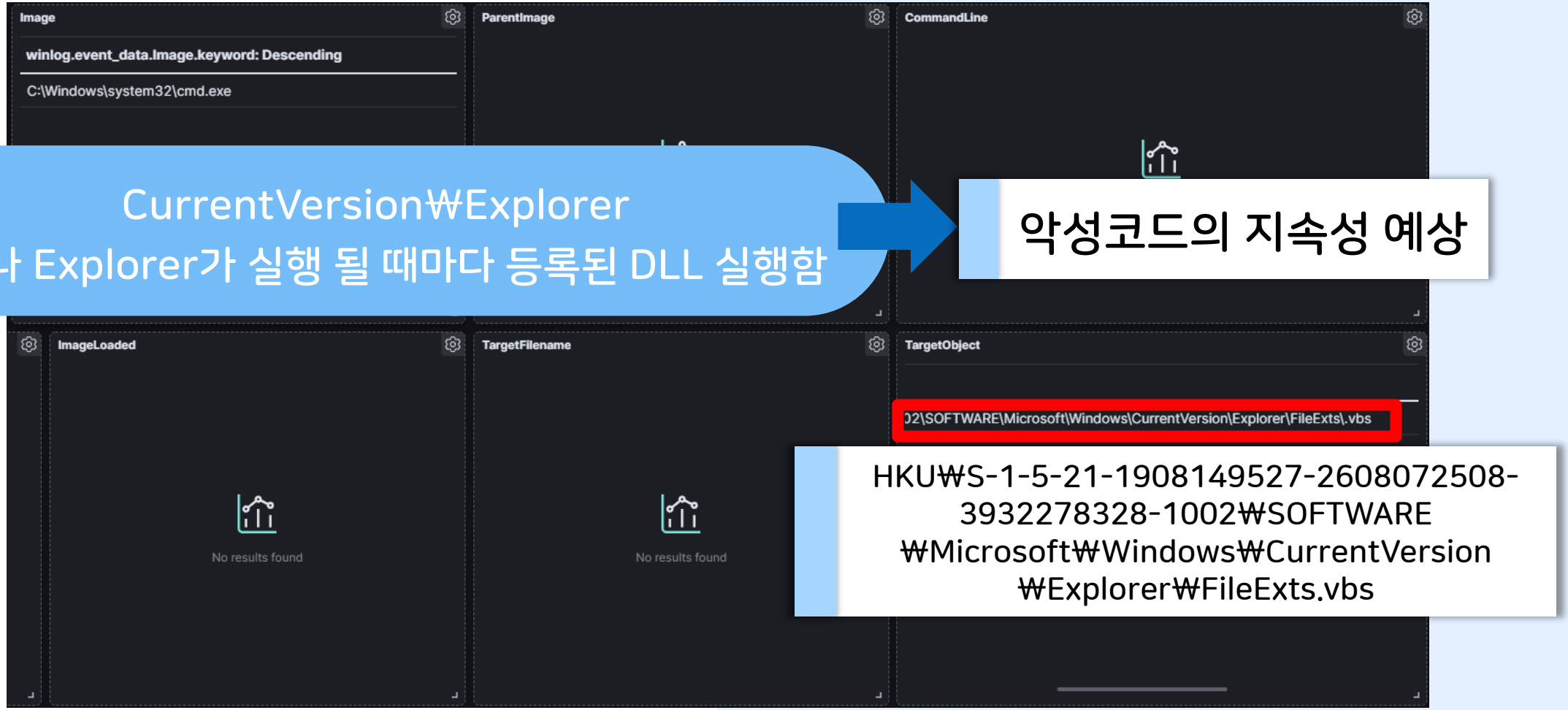
cmd.exe 분석



K-Shield Jr.

EDR 시스템을 이용하여 분석

cmd.exe 분석



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

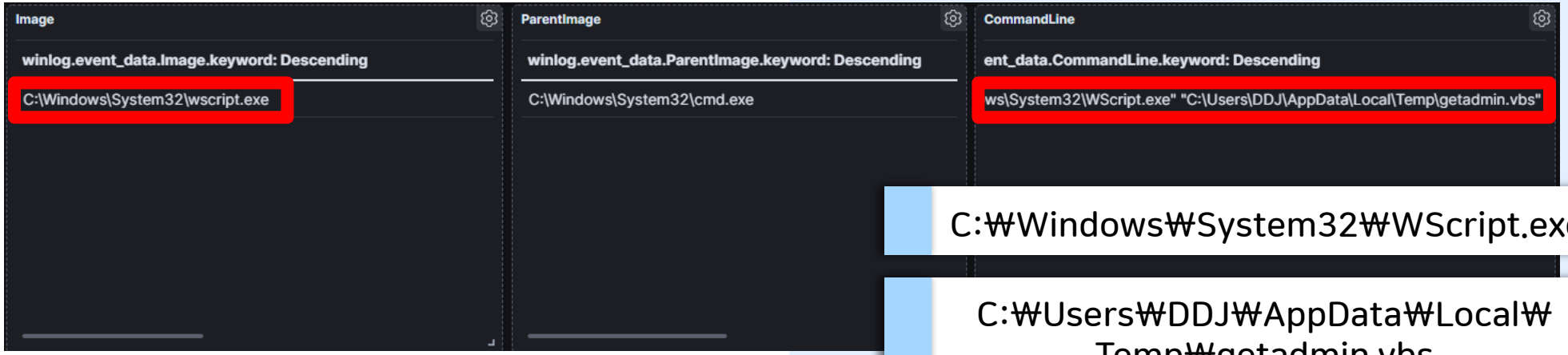
악성코드의 지속성 예상

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

K-Shield Jr.

EDR 시스템을 이용하여 분석

wscript.exe 분석



C:₩Windows₩System32₩WScript.exe

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

getadmin.vbs를 실행

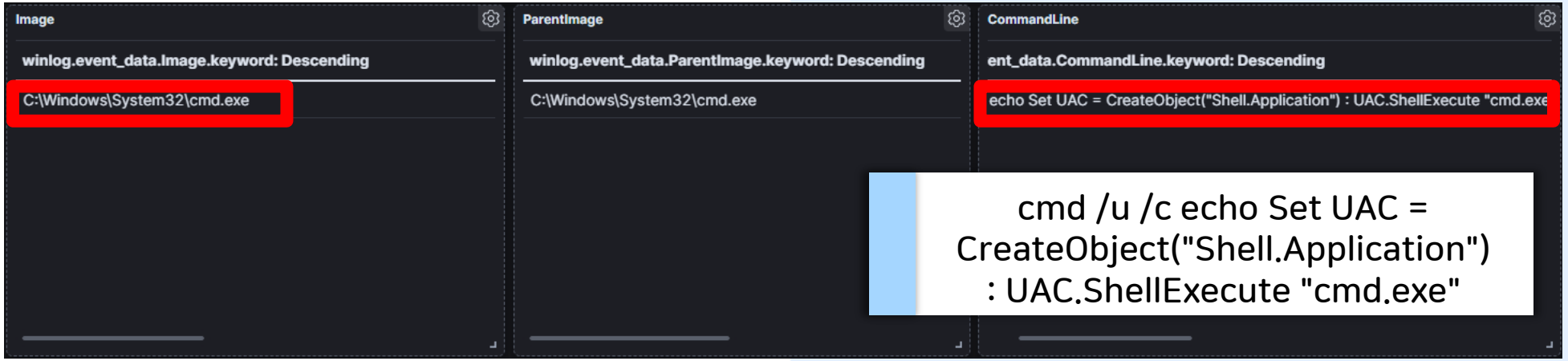
wscript.exe의 부모 프로세스

C:₩Windows₩System32₩cmd.exe

K-Shield Jr.

EDR 시스템을 이용하여 분석

Explorer.exe 분석

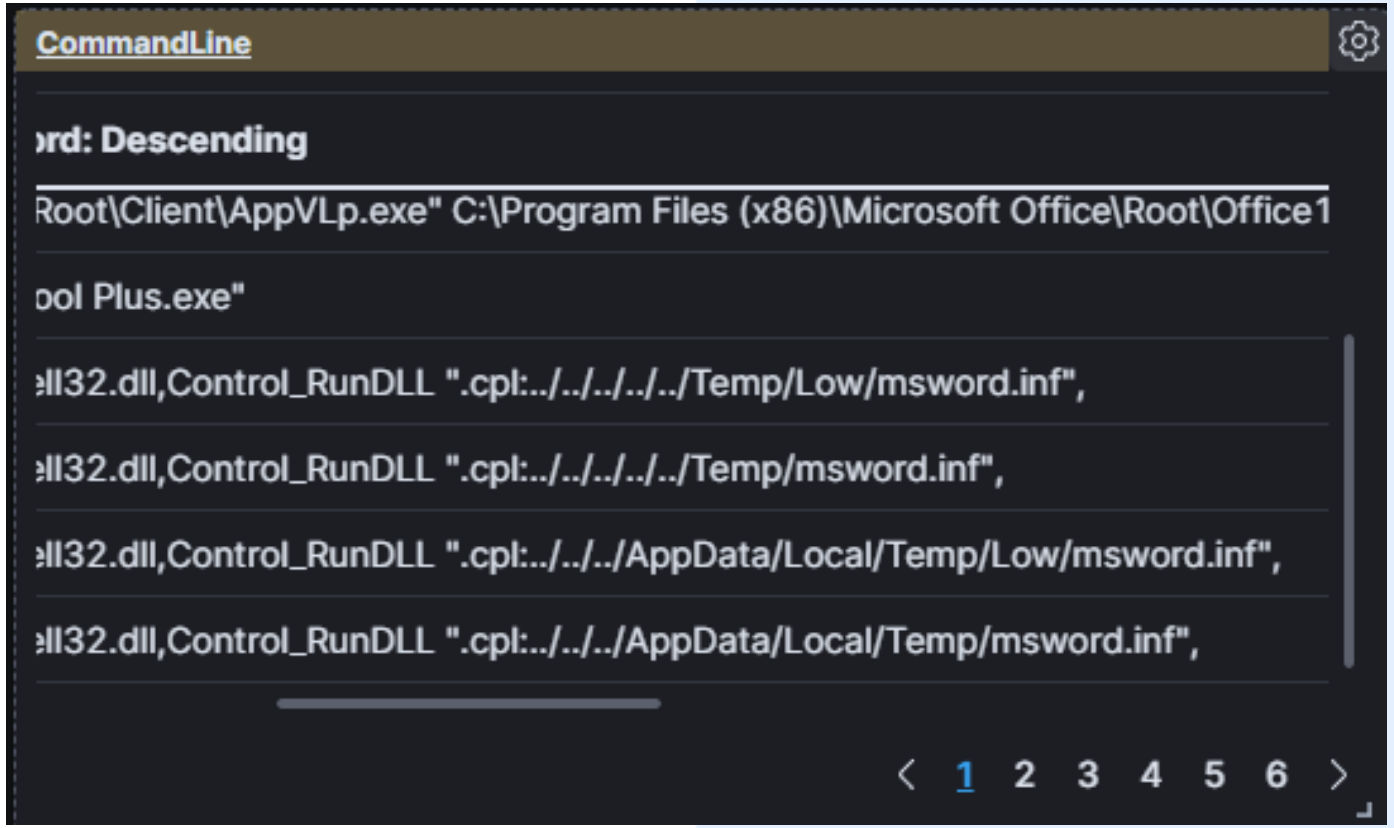


배치 파일 관리자 실행을 권유하지 않고
강제로 관리자로 실행시키는 코드

K-Shield Jr.

EDR 시스템을 이용하여 분석

경로 순회 공격 발견



K-Shield Jr.

EDR 시스템을 이용하여 분석

rundll2.exe 부모 프로세스 추적

Image	ParentImage	CommandLine
winlog.event_data.Image.keyword: Descending	winlog.event_data.ParentImage.keyword: Descending	winlog.event_data.CommandLine.keyword: Descending
C:\Windows\SysWOW64\rundll32.exe	C:\Windows\SysWOW64\control.exe	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL ".cpl:../../../

프로세스 id

winlog.event_data.ProcessId.keyword: Descending	Count
10064	1
1744	1
2780	1
6320	1

부모 프로세스 id

winlog.event_data.ParentProcessId.keyword: Descending	Count
3260	1
3772	1
7332	1
9800	1

프로토콜

K-Shield Jr.

EDR 시스템을 이용하여 분석

3260, 3772, 9800 검색

악성코드는 WINWORD.exe
관계되어있다는 것을 확인 가능

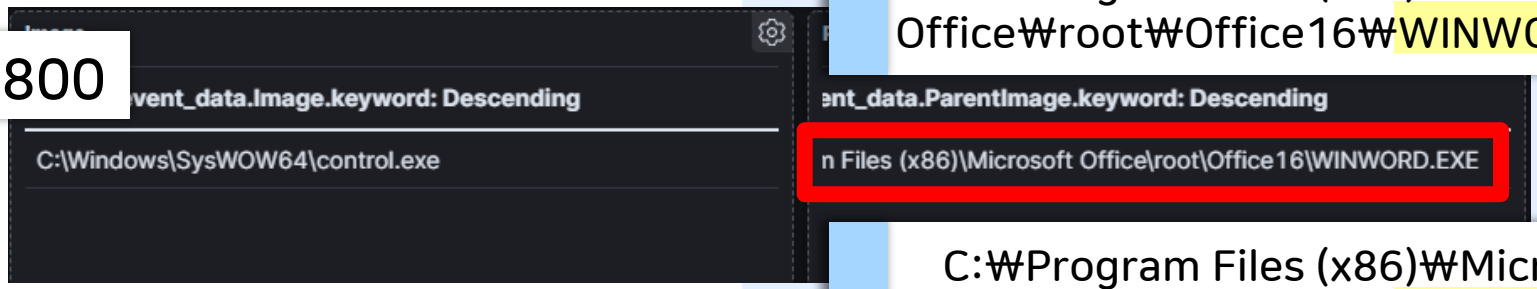
3260

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

3772

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

9800



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

K-Shield Jr.

04
프로젝트 이후 계획

K-Shield Jr.

프로젝트 이후 해보고 싶은 것

K-Shield Jr. 가 끝난 뒤

- 완성하지 못한 시나리오 토플로지 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