

# 포렌식관점의 MS EXCHANGE 서버 취약점 공격 및 분석

내이름은코난,탐정이조

# 목차

- 01 프로젝트 개요
- 02 팀 구성 및 역할
- 03 진행 일정
- 04 프로젝트 수행 결과
- 05 공격 프로파일
- 06 산출물
- 07 QnA

# 01

## 프로젝트 개요

프로젝트 주제 선정 배경

프로젝트 목적

## 선정 배경



### MS 익스체인지 서버, 록빗 랜섬웨어 감염

“해커는 처음에 손상된 익스체인지 서버에 웹셸을 배포한 후 네트워크에서 호스팅 되는 시스템을 암호화하기 전에 Active Directory 관리자 권한을 탈취하여 약 1.3TB의 데이터를 훔쳤다.”  
< cctv뉴스, 2022-10-13>

### AD 환경 랜섬웨어 감염 사례

“AD는 다수의 시스템을 관리하는 데 효율적이지만, 미숙한 계정 관리로 인해 관리자 권한이 탈취된다면 전체 내부망이 장악...”  
<보안뉴스, 2021-06-04>

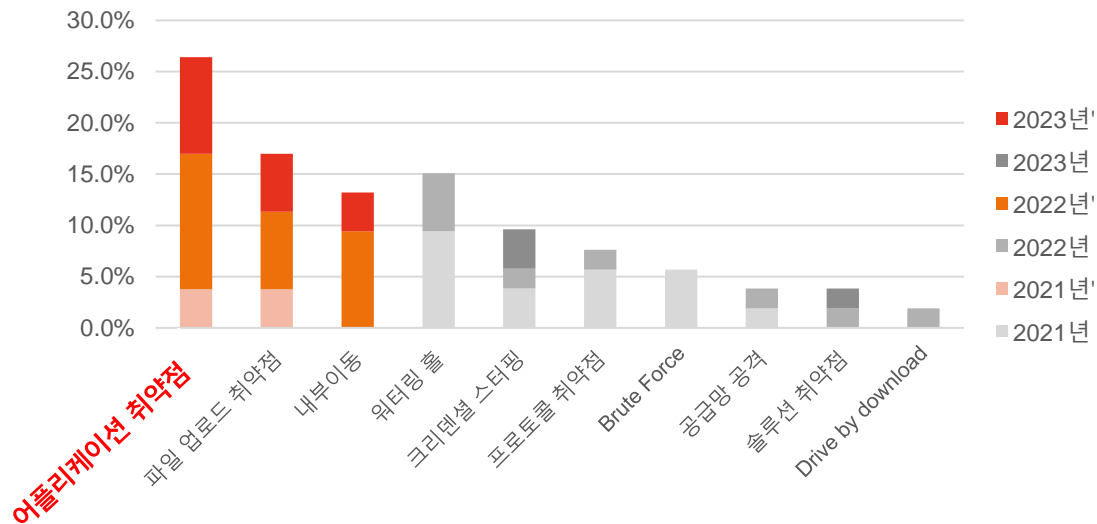
### “MS Exchange Server를 악용한 사이버 공격”

“자동화된 스캔 작업을 통해 해커는 해킹한 Exchange에 웹 셸(web shell)을 삽입해, 공격 대상으로 삼은 기기를 정찰하고 같은 네트워크를 사용하는 다른 여러 컴퓨터에도 이동할 수 있도록 했다.” <와이어드뉴스, 2021-03-06>

## 선정 배경 -침해사고 통계

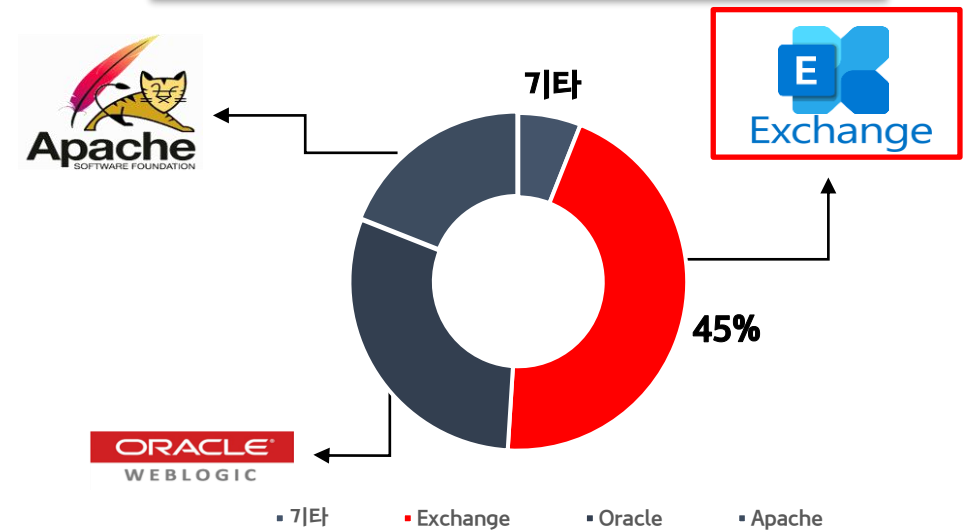
최근 3년간 발생한 침해사고의 통계 결과, 초기침투 단계에서 어플리케이션 취약점을 이용한 공격이 매년 크게 증가 하고 있다. 초기침투에 사용된 대표적인 어플리케이션으로는 **Exchange**, WebLogic, Apache 등 이 확인되었다.

초기침투 (통계)



- 내부 계열사 및 고객사를 통한 초기 침투 증가
- 23년' 어플리케이션 취약점을 이용한 공격 대폭 증가

어플리케이션 취약점



[최근 3년 주요 어플리케이션 취약점]

- 최근 3년간 주요 어플리케이션 취약점 전체 45%가 **MS Exchange**

## 프로젝트 목적

### 공격 시나리오 재구성



#### Exchange

- SSRF 취약점  
➢ (CVE-2021-26855)
- 임의 파일 쓰기 취약점  
➢ (CVE-2021-27065)



#### Active Directory

- OU 사용자 관리  
➢ 사용자 정보 수집
- 랜섬웨어 배포  
➢ Petya

### 포렌식관점의 분석



#### 단계별 분석

- 1) 초기 정찰
- 2) 초기 침투
- 3) 거점 확보
- 4) 내부 정찰 및 확산(1)
- 5) 내부 정찰 및 확산(2)
- 6) 연결 유지
- 7) 목표 달성



#### 대응방안 도출

- 대응방안 제시
- 솔루션 제공

# 02

## 팀 구성 및 역할

공격팀

구축 및 분석팀

## 소개

### 공격팀

조장



민작은바위

프로젝트 총괄



이 석

AD 공격  
DB 관리자 PC 공격



류태영

AD 공격  
DB 서버 공격



이성제

AD 공격  
Exchange 공격



장서현

AD 공격  
Exchange 공격

### 구축및분석팀

발표자



정대로

AD 구축  
DB 서버 구축



김민재

AD 구축  
Exchange 구축



박종원

DB 서버 구축  
DB 관리자 PC 구축



서민성

AD 구축  
DB 서버 구축



서경범

AD 구축  
DB 관리자 PC 구축



# 03

## 프로젝트 진행일정

## 프로젝트 진행 일정



사전  
이론학습

( 11/14 ~ 11/25 )



시나리오  
구성

( 11/23 ~ 11/25 )



인프라 구축

( 11/25 ~ 11/28 )



시나리오  
구체화

( 11/28 ~ 11/29 )



취약점 테스트

( 11/29 ~ 12/02 )



중간발표 준비  
&  
구축 테스트

( 12/02 ~ 12/08 )

## 프로젝트 진행 일정



중간 발표

12/09



공격진행

12/12 ~ 12/14



분석 및  
대응방안 작성

12/15 ~ 12/19



보고서 작성  
&  
PPT 제작

12/19 ~ 12/21



최종발표  
리허설

12/22 ~ 12/27



최종발표 및  
수료식

12/28

# 04

## 프로젝트 수행 결과

시나리오 개요

프로젝트 수행 절차 및 방법

타임라인

공격 시연 영상

대응방안 및 솔루션

## 시나리오 개요

### 기업정보



업체 명 : Marry with me  
업 종 : 결혼 정보 업체

| Inbound | Outbound |
|---------|----------|
| O       | X        |

| 운영중인 서비스 |                  |           |
|----------|------------------|-----------|
| Exchange | Active Directory | DB(MySQL) |
| DMZ      | 내부               | 폐쇄망       |

#### 설 명

- 2023년 12월 15일 직원들에 의해 랜섬웨어에 감염 사실 확인.
- 이를 보고 받은 보안 담당자는 정보 유출 및 추가 피해 가능성을 식별하기 위해 조사 요청.

### 공격 흐름 요약

- Exchange 대외 서비스 (OWA) 를 운영
- 공격자는 OSINT(shodan, censys) 를 통해 IP 대역대를 확인
- 취약점 스캔을 통해 취약한 Exchange 서버를 확인
- 공격자는 "Marry with me" 직원의 비즈니스 이메일 계정을 획득
- 이메일을 악용하여 내부 Exchange 서버에 침투
- Exchange 서버에서 AD(Active Directory) 서버 자격 증명 탈취
- AD에 접근한 공격자는 데이터베이스 관리자의 권한을 이용하여 정보 탈취
- 공격자는 AD 서버에서 랜섬웨어를 OU Zone에 배포 및 실행

## 프로젝트 수행 절차 및 방법

### 분석 대상 정보

#### 공격자 정보

| 분류    | 역할             | OS         | 버전                      |
|-------|----------------|------------|-------------------------|
| 공격자 1 | 취약점 스캔 및 직접 침투 | Kali Linux | kali-linux-2023.2-amd64 |
| 공격자 2 | 내부 확산 및 정보 탈취  | Kali Linux | kali-linux-2023.2-amd64 |

#### 구축 인프라 정보

| 분류               | 역할           | OS                  | 버전                                        |
|------------------|--------------|---------------------|-------------------------------------------|
| Exchange         | OWA / 메일 사서함 | Windows Server 2016 | Microsoft Exchange 2016 cu19<br>KB4588884 |
| Active Directory | OU 연결 자원 관리  | Windows Server 2016 | Standard Evaluation                       |
| DB 관리자 PC        | 데이터베이스 관리    | Windows Server 2016 | Standard Evaluation                       |
| Database         | 고객 데이터베이스 저장 | Ubuntu 20.04 LTS    | MySQL 8.0                                 |

# 프로젝트 수행 절차 및 방법

## 분석 도구

### 시스템 분석

| 도구명                   | 버전      | 설명              |
|-----------------------|---------|-----------------|
| analyzeMFT            | v2.20   | MFT 분석          |
| REGA                  | v1.5.3  | 레지스트리 분석        |
| Events Log Explorer   | V 5.4.1 | 이벤트 로그 분석       |
| Volatility            | v2.6    | 휘발성 데이터 수집 & 분석 |
| NTFS Log Tracker      | v1.71   | 파일 로그 확인        |
| Autoruns              | v14.09  | 자동으로 실행 프로그램 확인 |
| Tcpviewer             | v4.17   | 네트워크 패킷 분석      |
| tcpdump               | v4.1.2  | 네트워크 패킷 캡처      |
| gplist                | v2021   | 정책 정보 확인        |
| LogonSessions         | v2023   | 활성 로그인 세션 확인    |
| netusers              | v1.79   | 시스템 계정정보 확인     |
| DB Browser for SQLite | v3.12.2 | 파일 로그 확인        |
| Procmon               | v2.95   | 프로세스 모니터링       |
| LastActivityViewer    | v1.37   | 실행 목록 확인        |

### Windows Artifact 분석

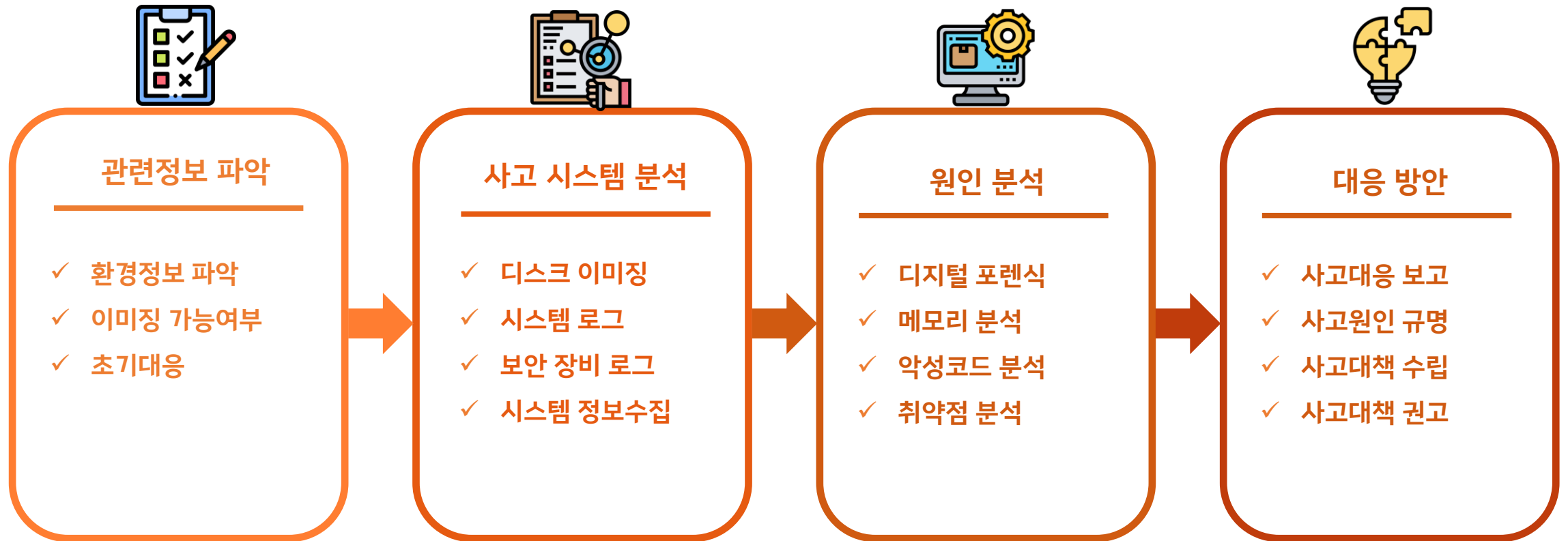
| 도구명                   | 버전    | 설명                |
|-----------------------|-------|-------------------|
| BrowsingHistoryViewer | v2.51 | 인터넷 사용 기록 분석      |
| ChromeCacheViewer     | v2.36 | Chrome Cache 분석   |
| ChromeCookiesViewer   | v1.70 | Chrome Cookies 분석 |
| ChromeHistoryViewer   | v1.50 | Chrome History 분석 |
| IECacheViewer         | v1.58 | IE Cache 분석       |
| IECookiesViewer       | v1.79 | IE Cookies 분석     |
| MZCacheViewer         | v2.20 | Firefox Cache 분석  |
| WinPrefetchViewer     | v1.37 | Prefetch 분석       |

### Disk 분석

| 도구명        | 버전      | 설명           |
|------------|---------|--------------|
| FTK Imager | v4.7.1  | 디스크 이미징 & 분석 |
| HxD        | v2.3    | 헥스 에디터       |
| Autopsy    | v4.21.0 | 디스크 이미지 분석   |

## 프로젝트 수행 절차 및 방법

### 분석 프로세스





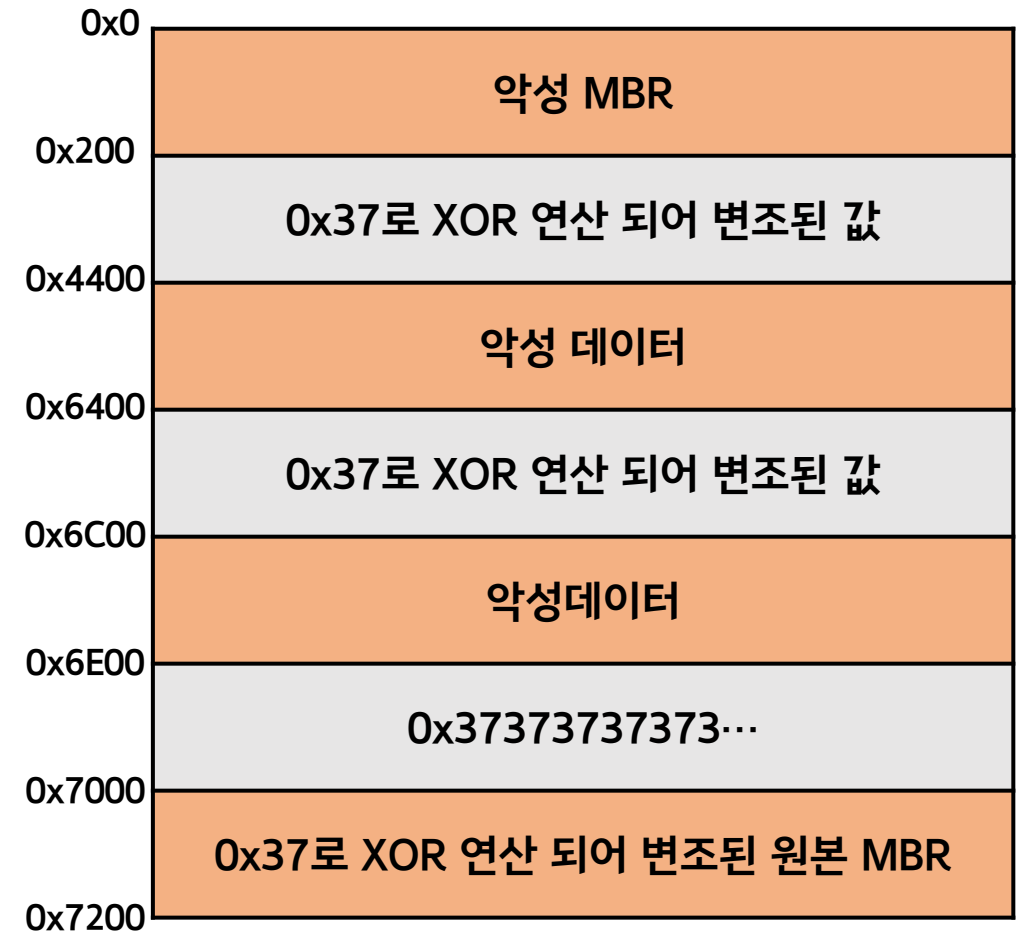
## 프로젝트 수행 절차 및 방법

### 랜섬웨어 (Petya)



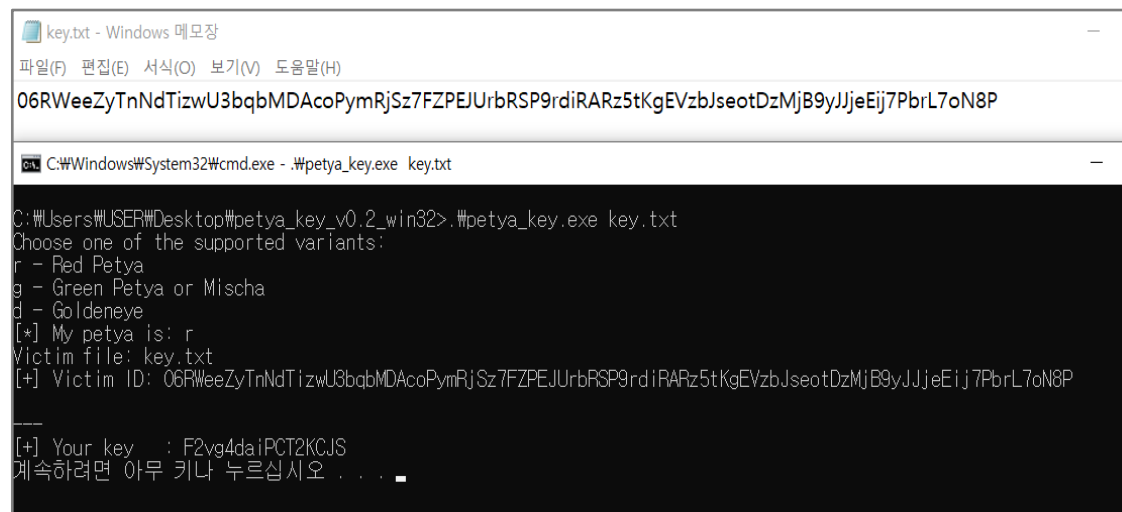
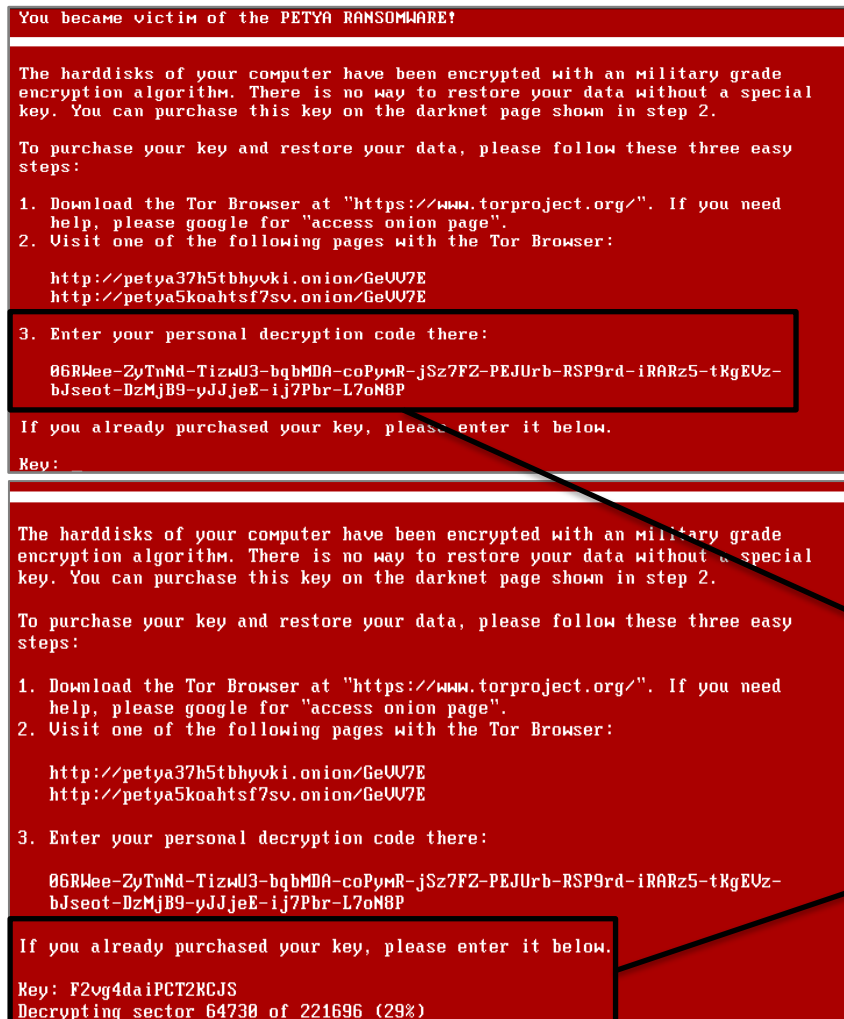
- Petya 는 2016년에 처음 발견된 암호화 악성 코드
- Microsoft Windows 기반 시스템을 표적으로 삼아 마스터 부트 레코드를 감염시켜 하드 드라이브의 파일 시스템 테이블을 암호화하고 Windows 부팅을 방해하는 페이로드를 실행

### 감염 후 구조



# 프로젝트 수행 절차 및 방법

## 랜섬웨어 복구 (Petya)



3. Enter your personal decryption code there:

**06RWee-ZyTnNd-TizwU3-bqbMDA-coPymR-jSz7FZ-PEJurb-RSP9rd-iRARz5-tKgEUz-bJseot-DzMjB9-yJJjeE-ij7Pbr-L7oN8P**

암호화 키

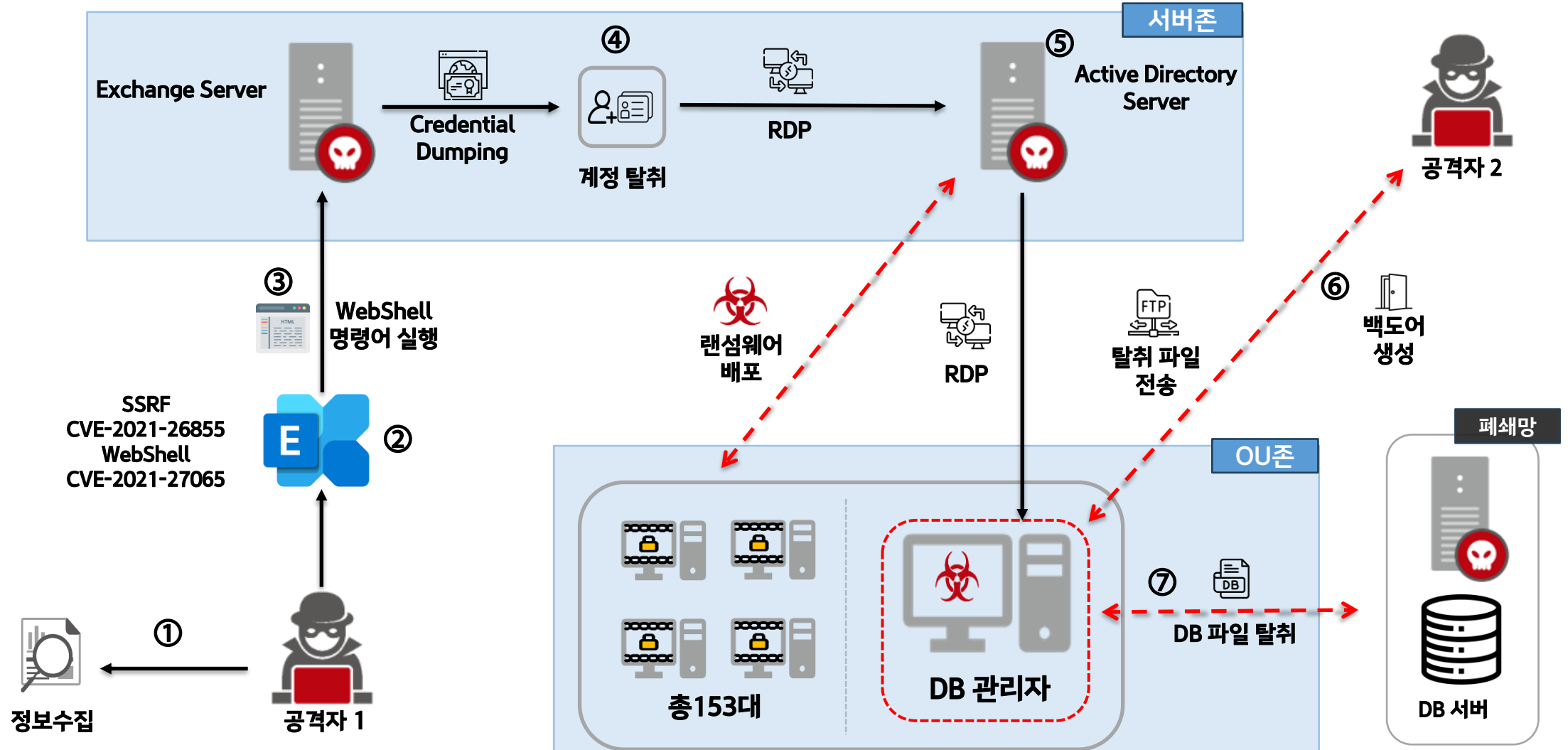
If you already purchased your key, please enter it below.

**Key: F2vg4daiPCT2KCJS**  
**Decrypting sector 64730 of 221696 (29%)**

복호화 키

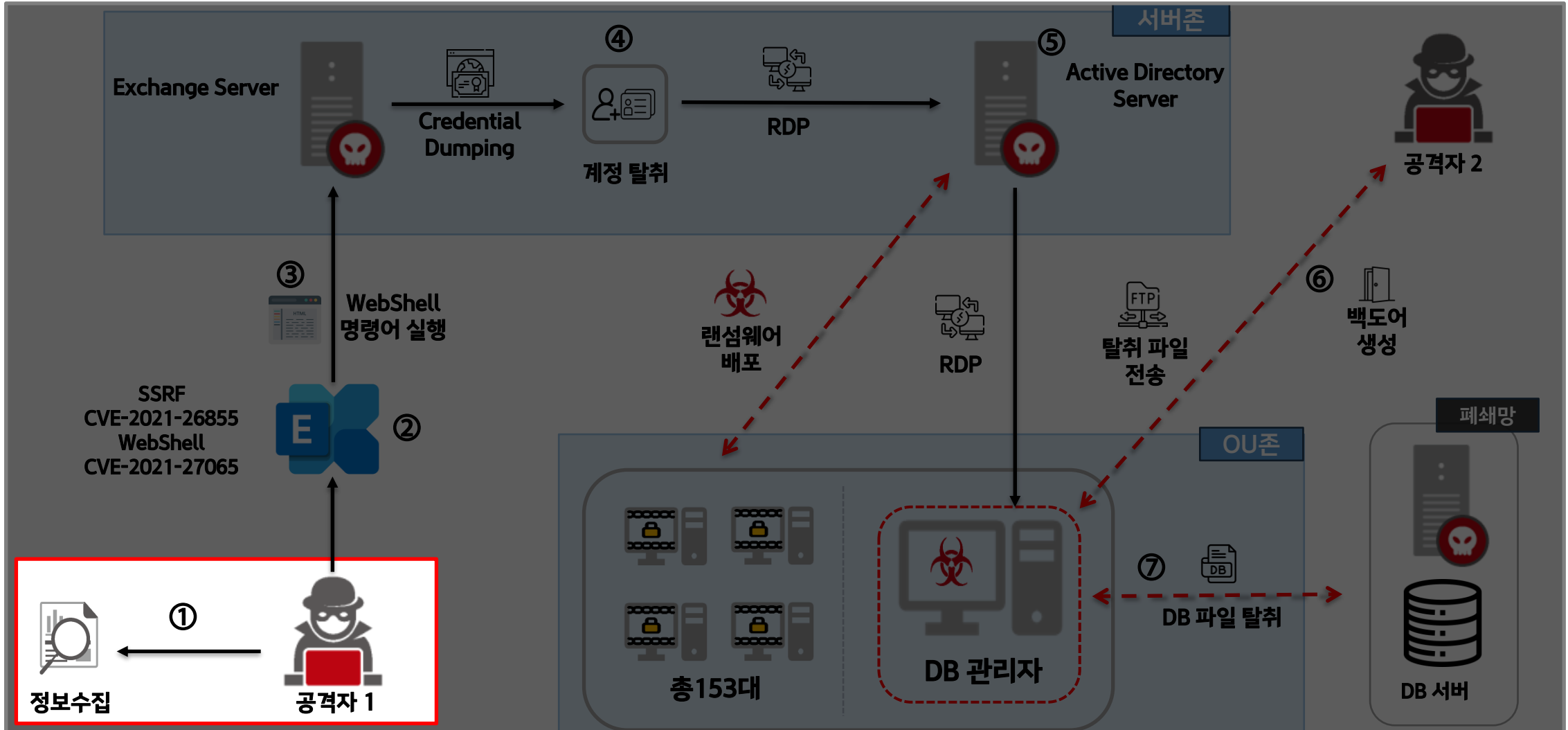
## 프로젝트 수행 절차 및 방법

### 공격 시나리오



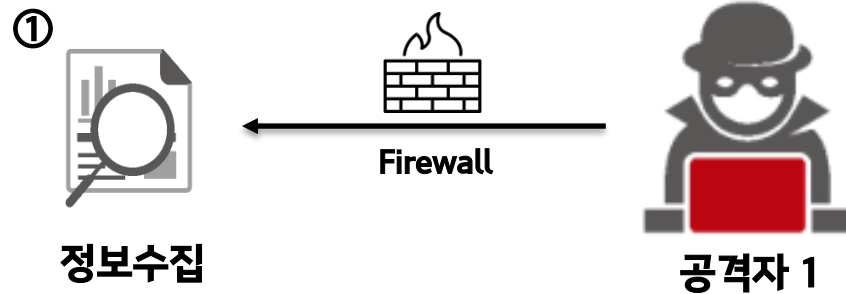
## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ① 초기 정찰



## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ① 초기 정찰



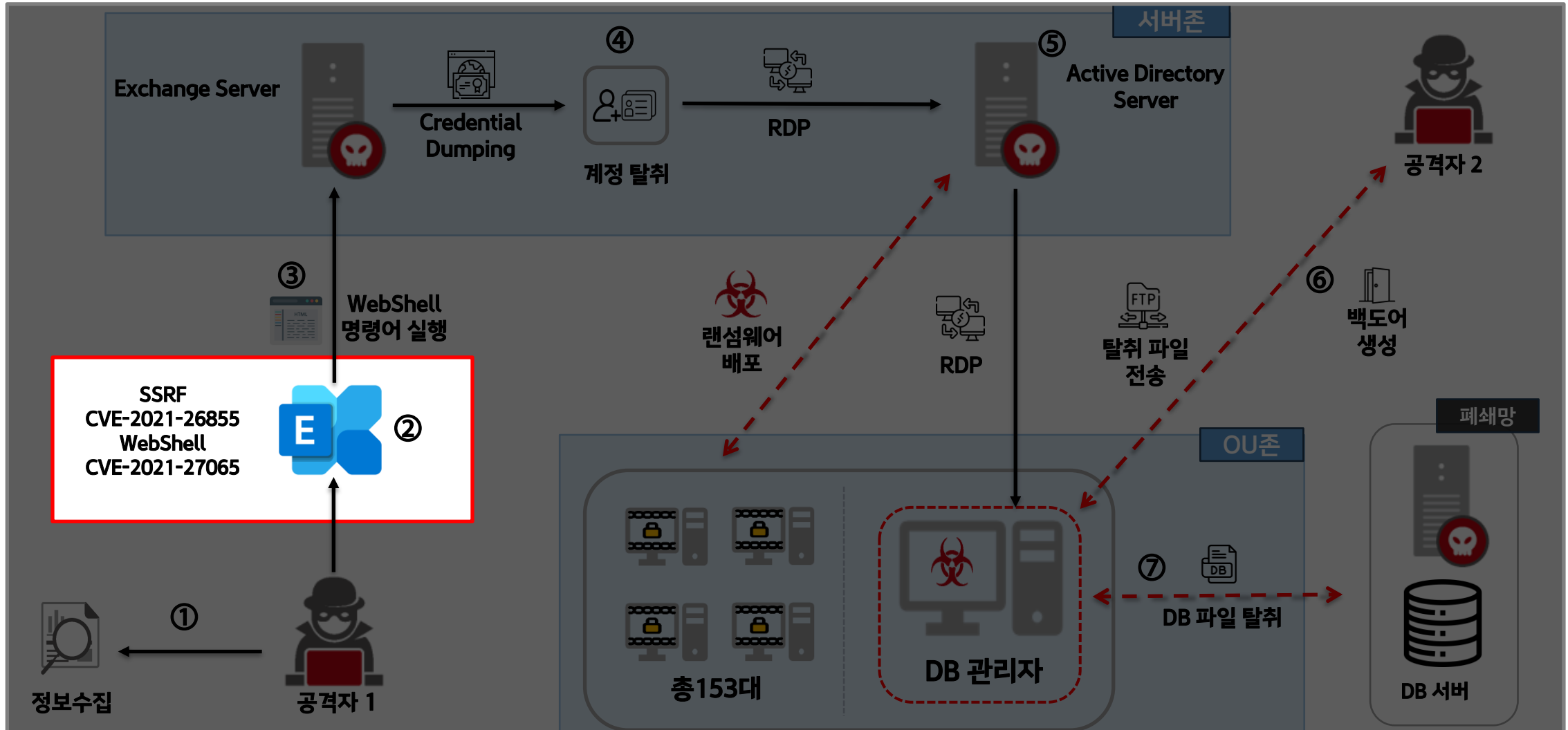
#### 초기 정찰

- 공격자가 Marry with me의 IP 대역대를 탐색
- 현재 서버 중 하나가 취약한 Exchange 서버를 사용 중임을 확인

| 이름            | 설명                            | 비고        | 증거 |
|---------------|-------------------------------|-----------|----|
| Firewall.pcap | nikto 실행 로그<br>포트 및 취약점 스캔 기록 | Wireshark | ②  |
| W3SVC1        |                               | 웹 로그      |    |

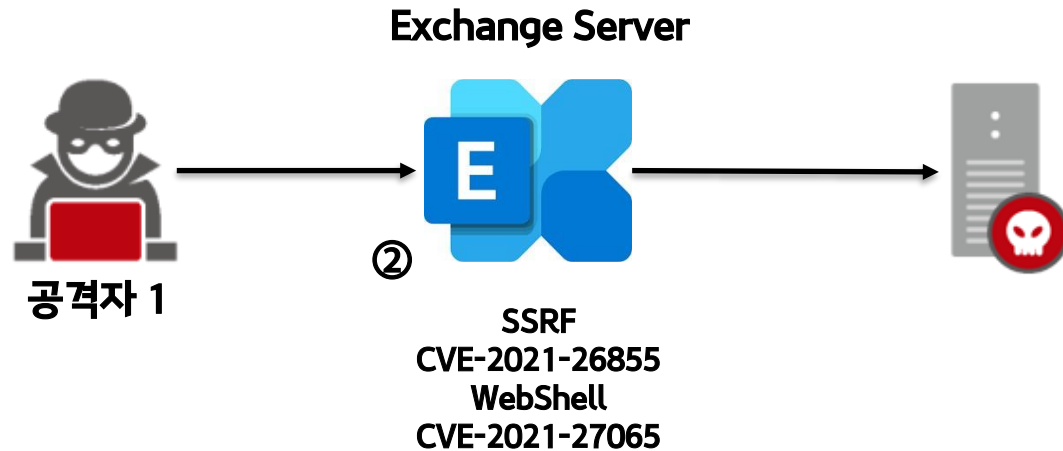
## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ② 초기 침투



## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ② 초기 침투



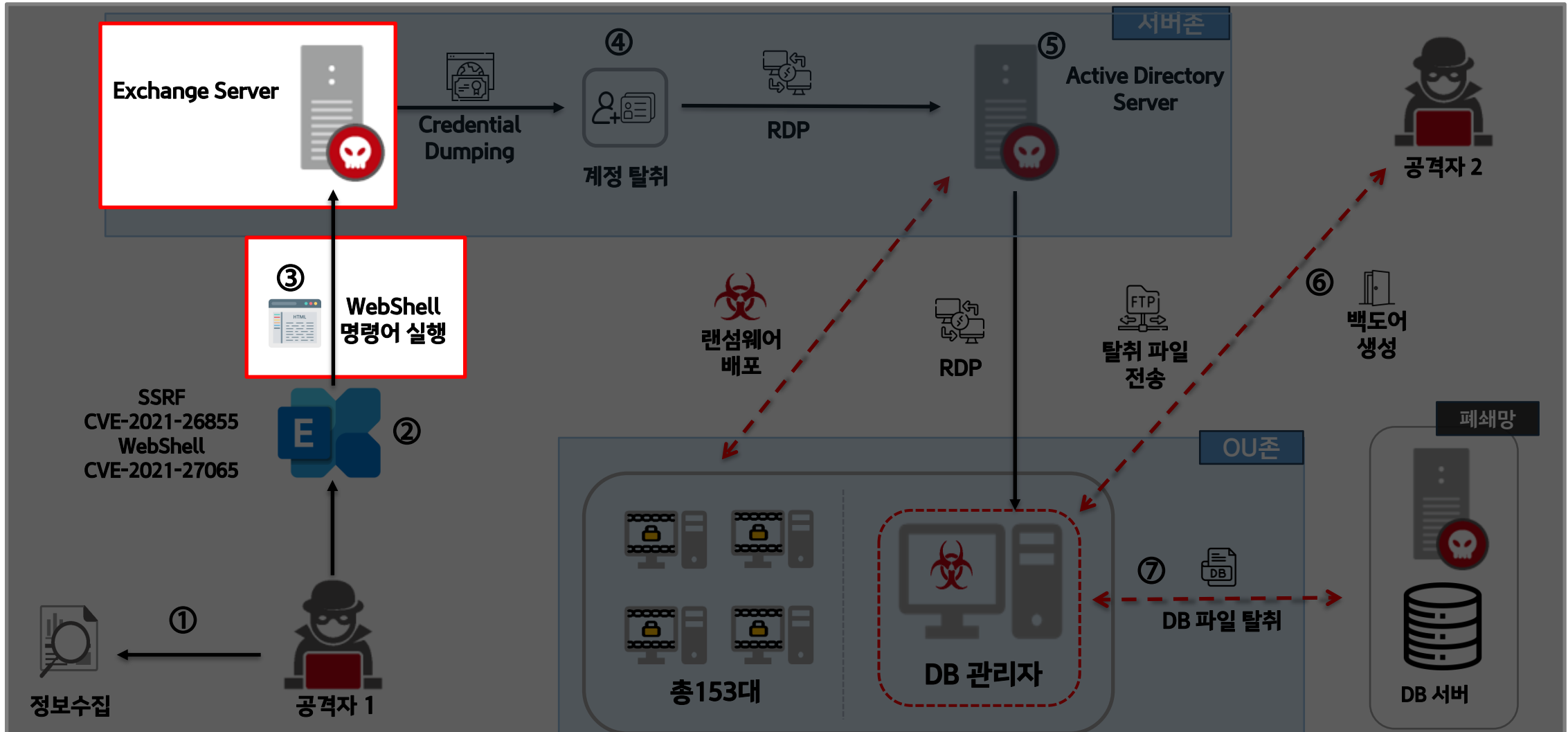
#### 초기 침투

- 공격자가 CVE-2021-26855(SSRF)취약점과 CVE-2021-27065(파일 업로드) 취약점을 이용하여 침투

| 분석 대상                    | 설명         | 비고                 | 증거 |
|--------------------------|------------|--------------------|----|
| HttpProxy.log            | 인증 우회 취약점  | Exchange 서버 로그     | ①  |
| ECP Server.log           | 파일 업로드 취약점 | Exchange 서버 로그     | ②  |
| Exchange Management.evtx |            | Event Log Explorer |    |

## 프로젝트 수행 절차 및 방법

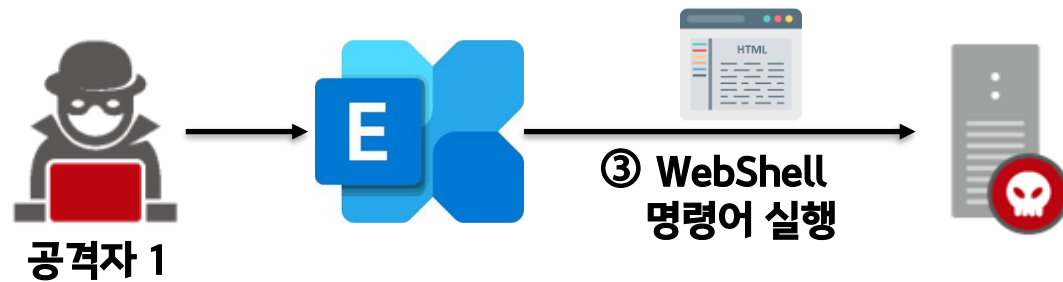
### 공격 시나리오 ③ 거점 확보





## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ③ 거점 확보



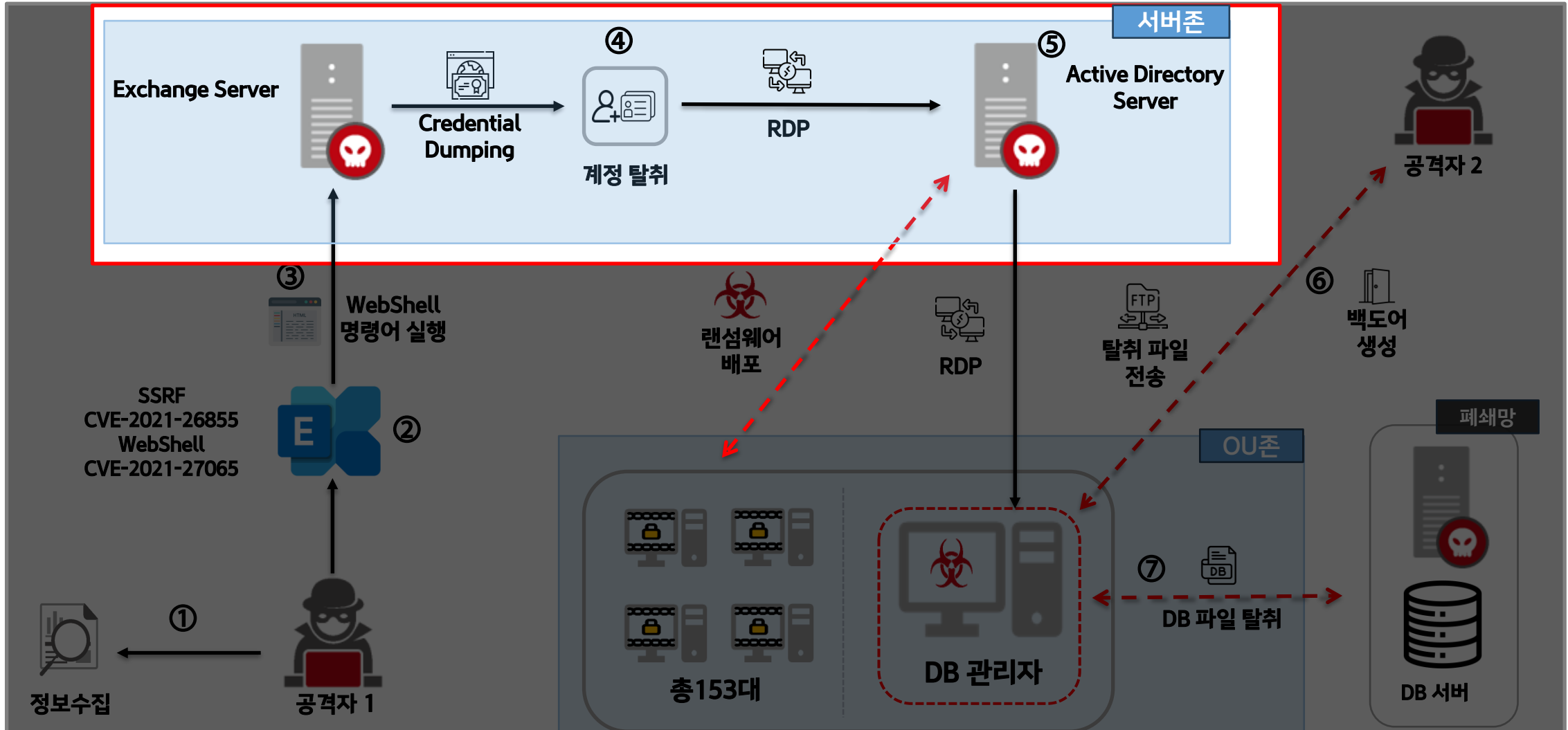
#### 거점 확보

- WebShell 통해 방화벽 및 실시간 모니터링 비활성화, 계정 생성, 공격 도구 및 백도어 파일 다운로드 및 압축해제, frpc실행 명령어 실행

| 분석 대상                | 설명                     | 비고                                | 증거 |
|----------------------|------------------------|-----------------------------------|----|
| Powershell.<br>evtx  | 방화벽 및 실시간<br>모니터링 비활성화 | Event Log<br>Explorer             | ⤵  |
| Application.<br>evtx | Hack 계정 생성             | Event Log<br>Explorer, Volatility | ⤵  |
| Powershell.<br>evtx  | 파일 다운로드 및<br>압축해제      | Event Log<br>Explorer             | ⤵  |
| MFT                  |                        | Volatility, Analyzer<br>MFT       |    |
| process 정보           | frpc 사용                | Volatility                        | ⤵  |

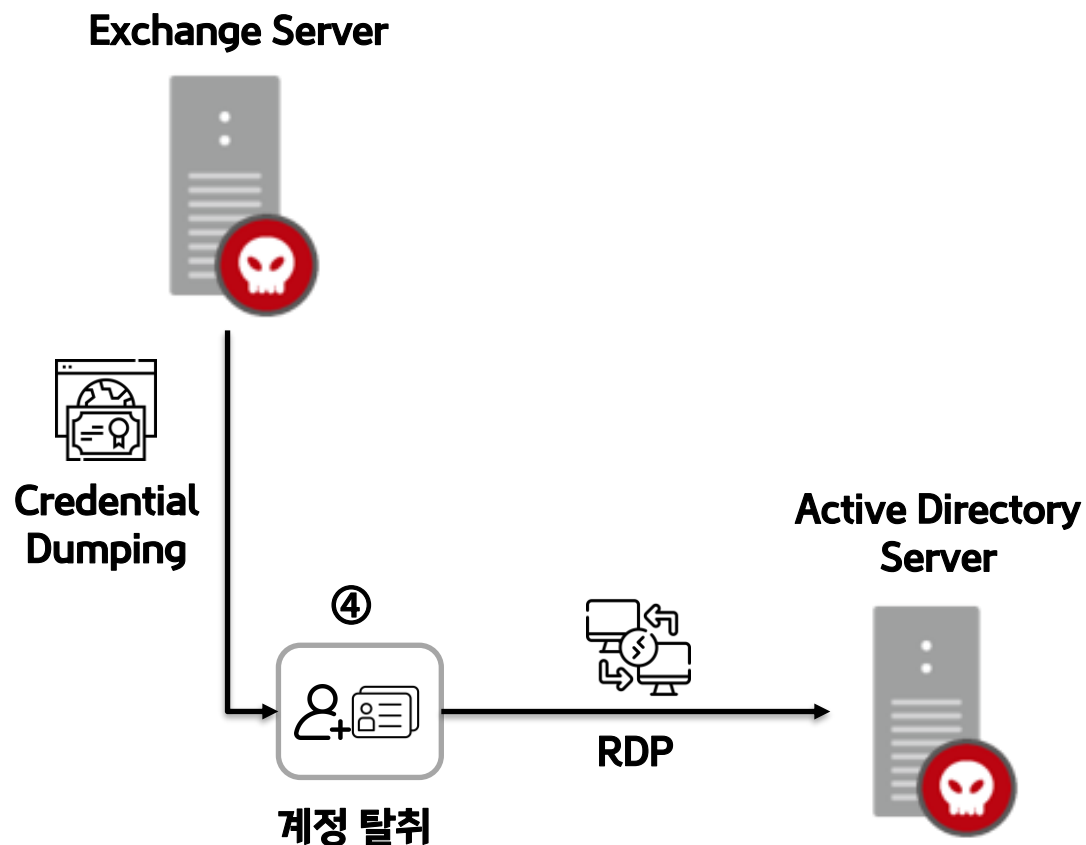
## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ④ 내부 정찰 및 확산 (1)



## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ④ 내부 정찰 및 확산 (1)



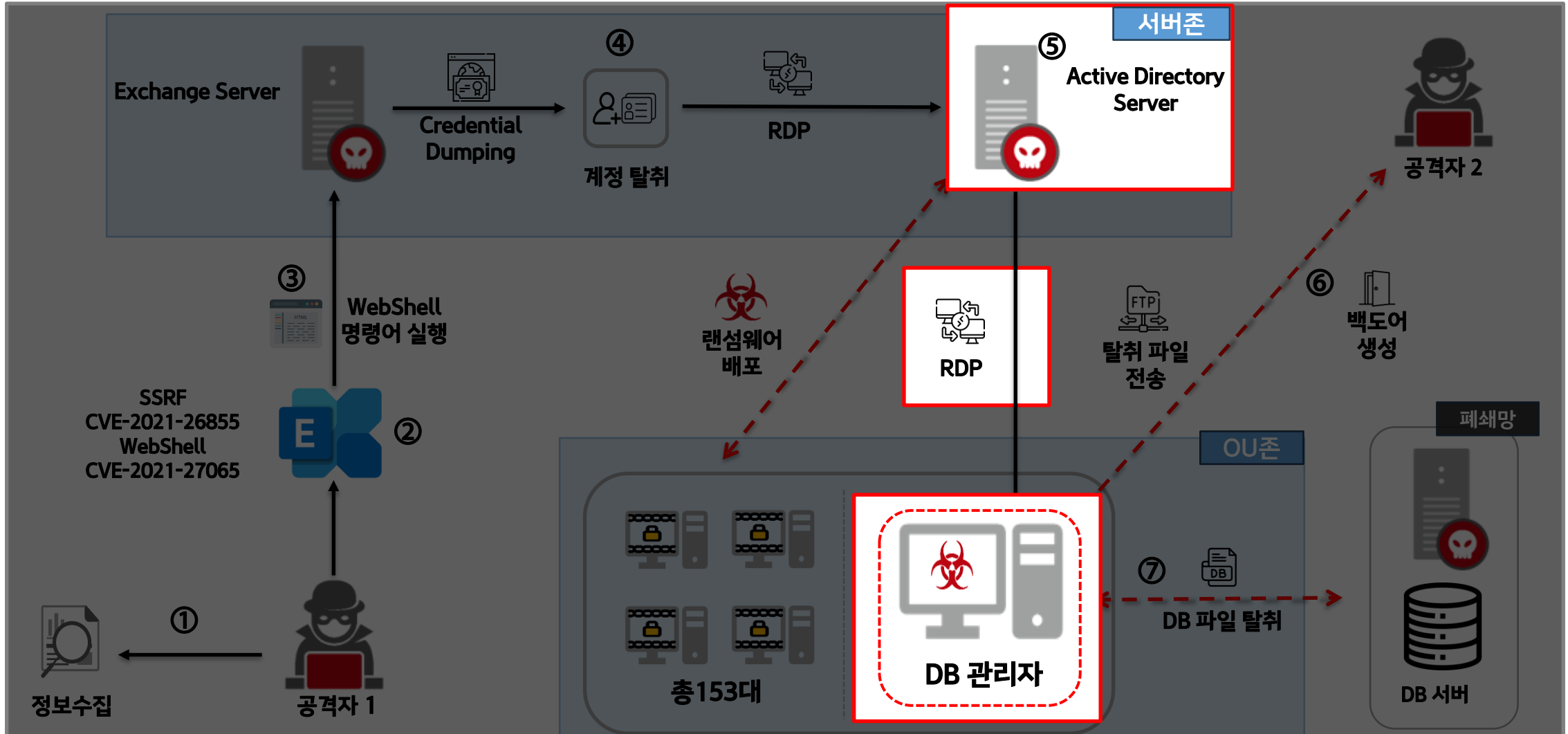
#### 내부 정찰 및 확산 (1)

- hydra를 실행하여 무차별 대입 공격 (실패)
- mimikatz를 실행하여 Credential Dumping
- RDP를 이용하여 Active Directory Server로 이동

| 이름             | 설명                    | 비고                       | 증거 |
|----------------|-----------------------|--------------------------|----|
| Registry       | start.bat 실행 기록       | REGA                     | ⤵  |
| Security .evtx | 로그인 실패 기록             | Event Log Explorer       |    |
| MFT            | mimikatz 압축 해제, 실행 흔적 | Volatility, Analyzer MFT | ⤵  |
| Registry       | RDP 흔적                | REGA                     | ⤵  |

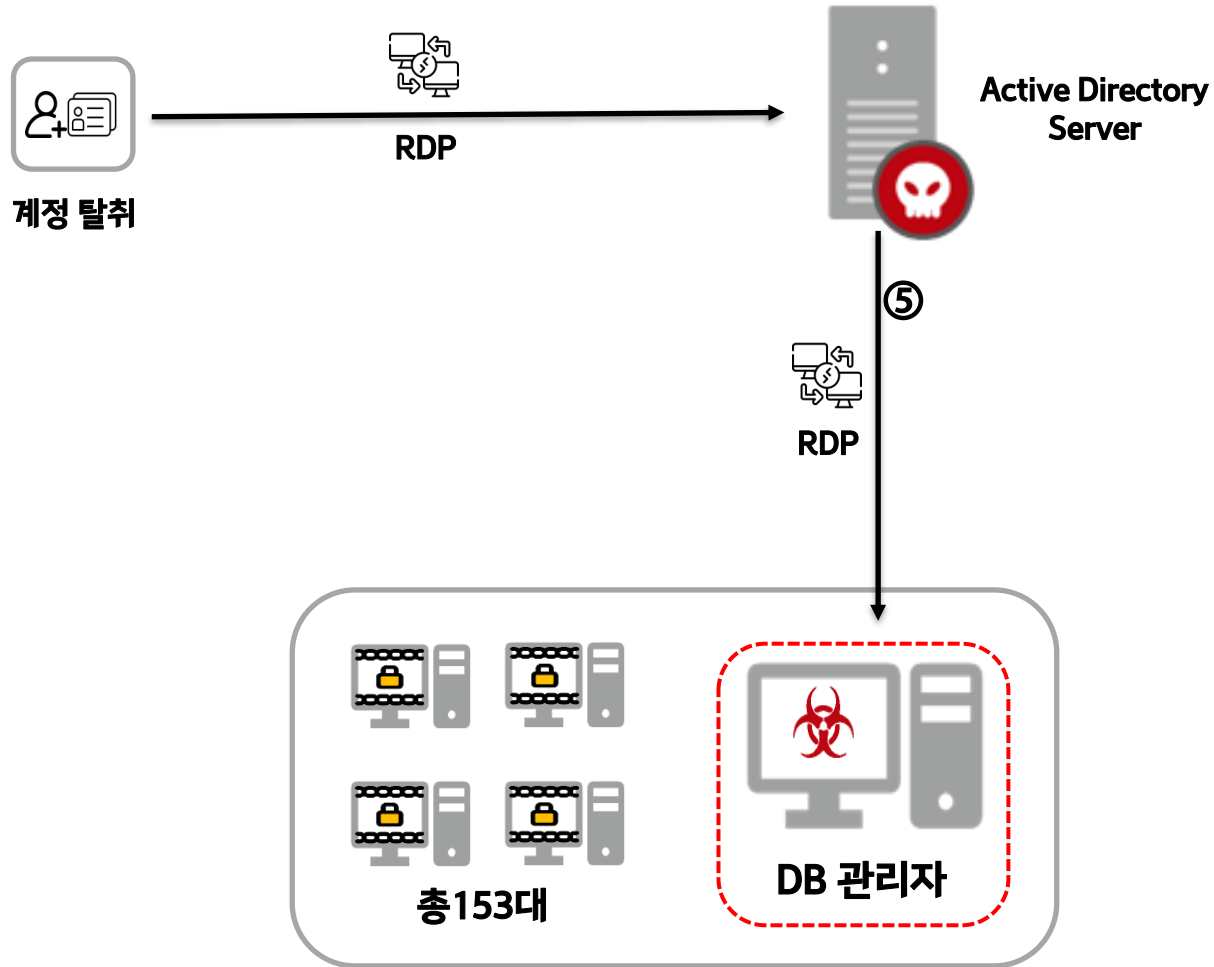
## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ⑤ 내부 정찰 및 확산 (2)



## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ⑤ 내부 정찰 및 확산 (2)



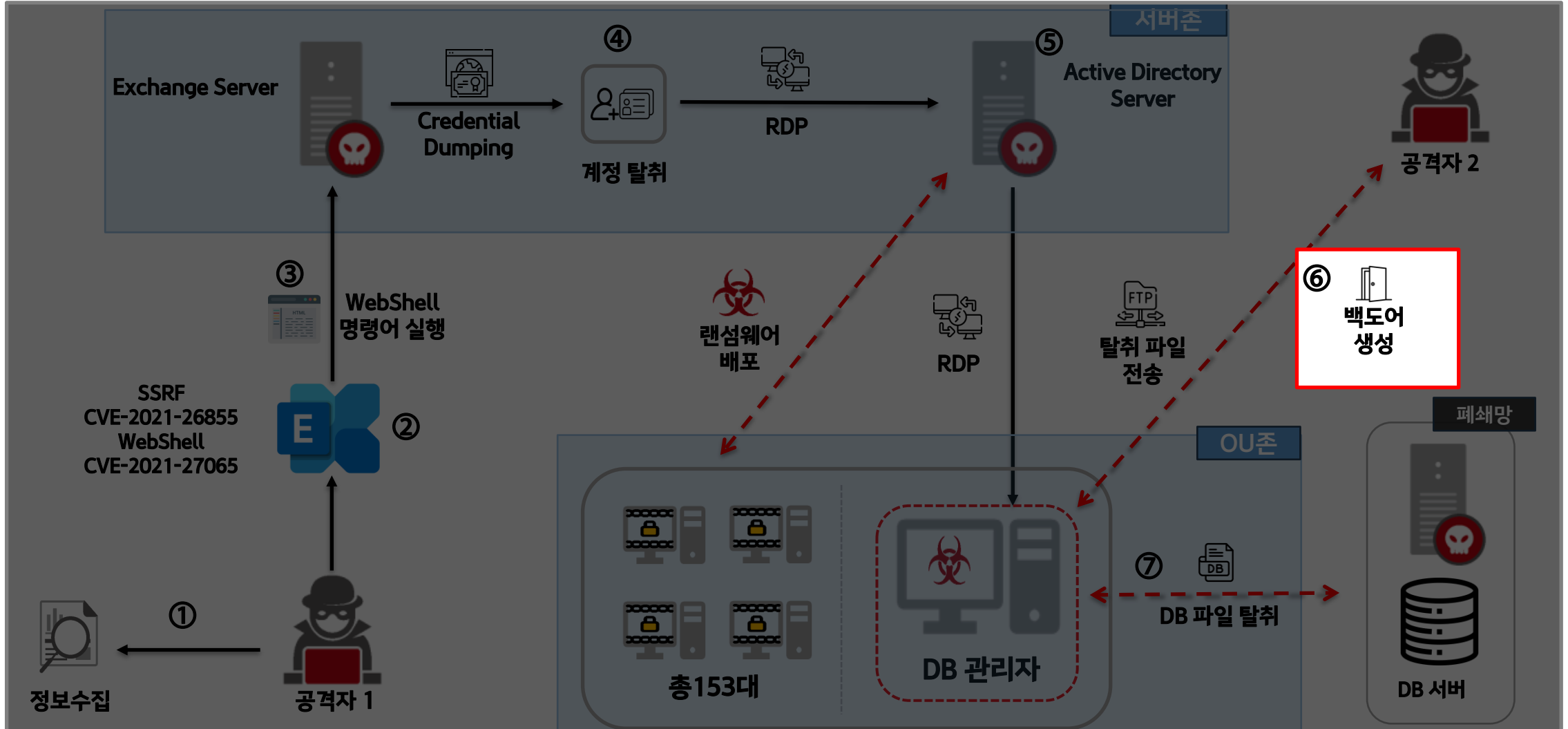
### 내부 정찰 및 확산 (2)

- Active Directory Server까지 장악한 공격자는 DB관리자 PC의 실시간 보호 비활성화, 정책 배포, 파일 다운, 게더링, 방화벽 비활성화 정책 배포, OU계정 비밀번호 변경, RDP연결

| 이름                      | 설명                           | 비고                       | 증거 |
|-------------------------|------------------------------|--------------------------|----|
| Powershell.evtx         | Windows Defender 실시간 보호 비활성화 | Event Log Explorer       | ⤵  |
| MFT                     | attack.zip 파일 다운로드           | Volatility, Analyzer MFT | ⤵  |
| Windows Powershell.evtx | Powershell로 게더링 스크립트 실행      | Event Log Explorer       | ⤵  |
| Registry                | 게더링 result.txt 열람로그 확인       | REGA                     |    |
| Registry.pol            | 방화벽 비활성화 정책 배포               | Policy Log               | ⤵  |
| Security Auditing.evtx  | OU 계정 비밀번호 변경                | Event Log Explorer       | ⤵  |
| Powershell.evtx         | RDP 연결                       | Event Log Explorer       | ⤵  |

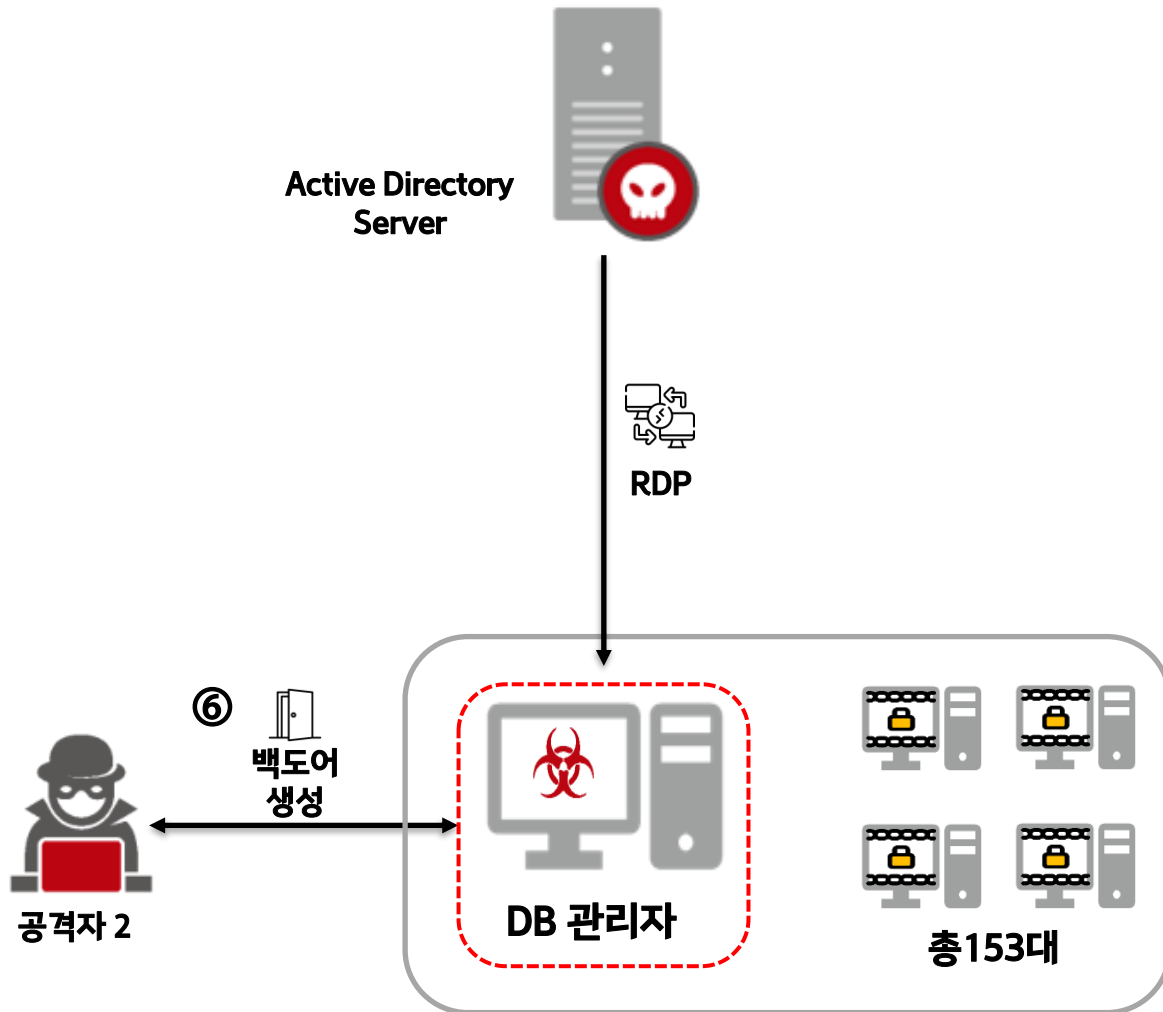
## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ⑥ 연결 유지



## 프로젝트 수행 절차 및 방법

### 공격 시나리오 ⑥ 연결 유지



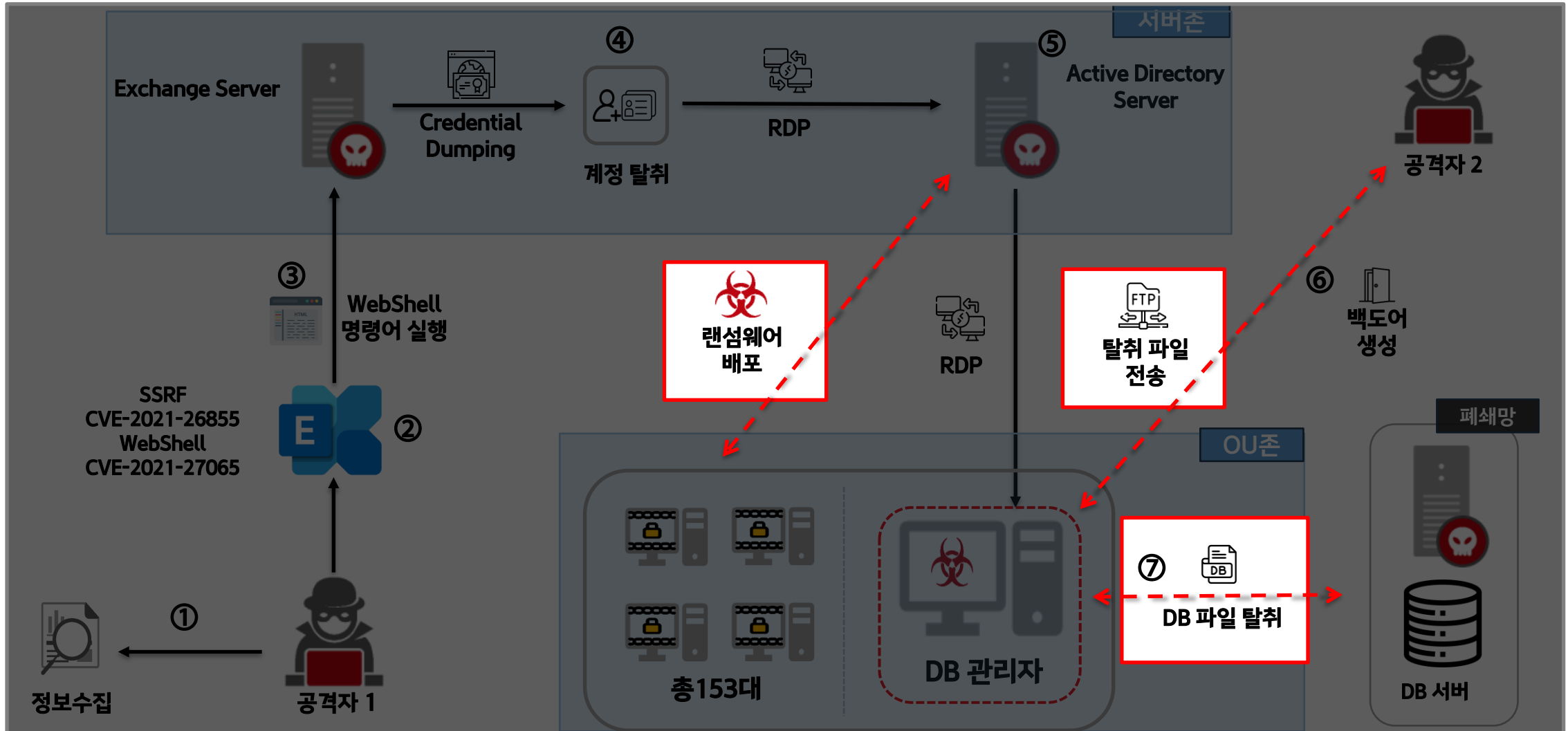
#### 연결 유지

- 백도어(update.exe)악성코드 실행

| 분석 대상      | 설명     | 비고               | 증거 |
|------------|--------|------------------|----|
| update.exe | 백도어 생성 | REGA,<br>TCPView | ⤵  |

## 프로젝트 수행 절차 및 방법

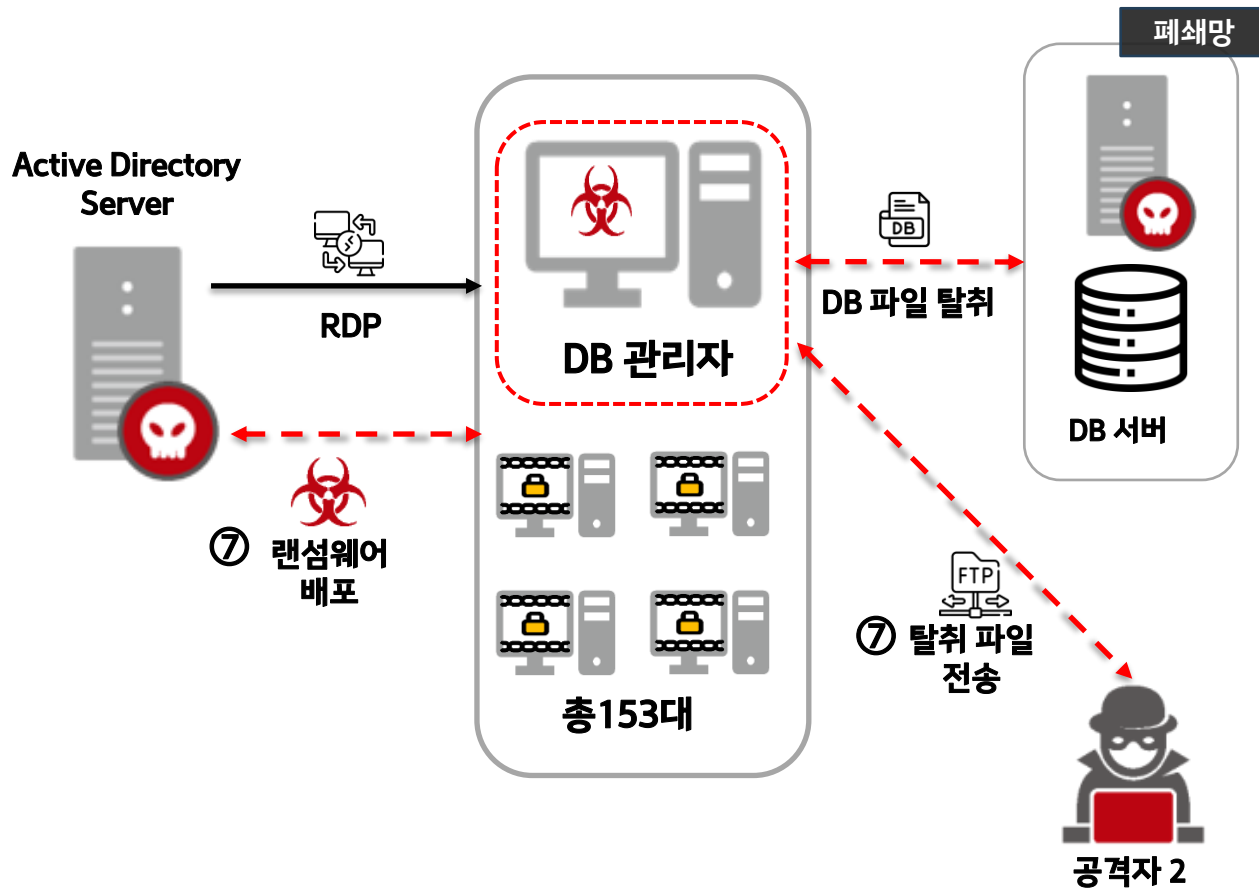
### 공격 시나리오 ⑦ 목표달성





# 프로젝트 수행 절차 및 방법

## 공격 시나리오 ⑦ 목표달성



### 목표달성

- DB서버 접속
- 파일 탈취 및 탈취 파일 공격자에게 전송
- 랜섬웨어 배포

| 분석 대상            | 설명                        | 비고                       | 증거 |
|------------------|---------------------------|--------------------------|----|
| filezilla.log    | FileZilla 접속 및 IP주소 연결 확인 | FileZilla 로그             | ⑦  |
| MFT              | 세션 파일 접근 시간 확인            | Volatility, Analyzer MFT |    |
| Auth.log         | auth.log의 접근된 시간          | vim                      |    |
| filezilla.log    | 탈취한 파일 및 탈취 시간            | FileZilla 로그             | ⑦  |
| regripper_result | Readme.msi파일 이동           | Volatility               | ⑦  |
| Hello.exe        | Hello.exe 실행 로그 확인        | REGA                     |    |

# 타임 라인

Exchange 서버



취약점 스캔  
2023-12-14 20:50:02



cve-2021-26855 &  
cve-2021-27065  
WebShell 업로드  
2023-12-14 20:52:05



악성 파일  
방화벽 & Defender OFF  
계정 생성 및 attack.zip 다운로드  
2023-12-14 20:52:19



frpc.exe  
frpc.exe를 이용해 RDP  
접속  
2023-12-14 20:52:43



payload.exe  
Reverse Connection  
2023-12-14 20:53:58



Petya  
Readme.msi(랜섬웨어) 배포  
2023-12-14 21:06:06



AD 정책  
방화벽 &  
Defender OFF 정책 배포  
2023-12-14 21:03:45



gathering  
OU 정보 수집  
2023-12-14  
21:00:05



악성 파일  
attack.zip 다운로드  
2023-12-14 20:59:09



RDP  
RDP 접속  
2023-12-14 20:58:05



mimikatz.exe  
계정정보 덤프  
2023-12-14 20:55:55  
Active Directory  
서버



RDP  
RDP 접속  
2023-12-14  
21:06:24



DB 관리자



update.exe  
Reverse Connection  
2023-12-14 21:07:21



db\_backup.sql  
DB 접속 후 DB 탈취  
2023-12-14  
21:09:15



공격 흔적 삭제  
2023-12-14 21:10:21



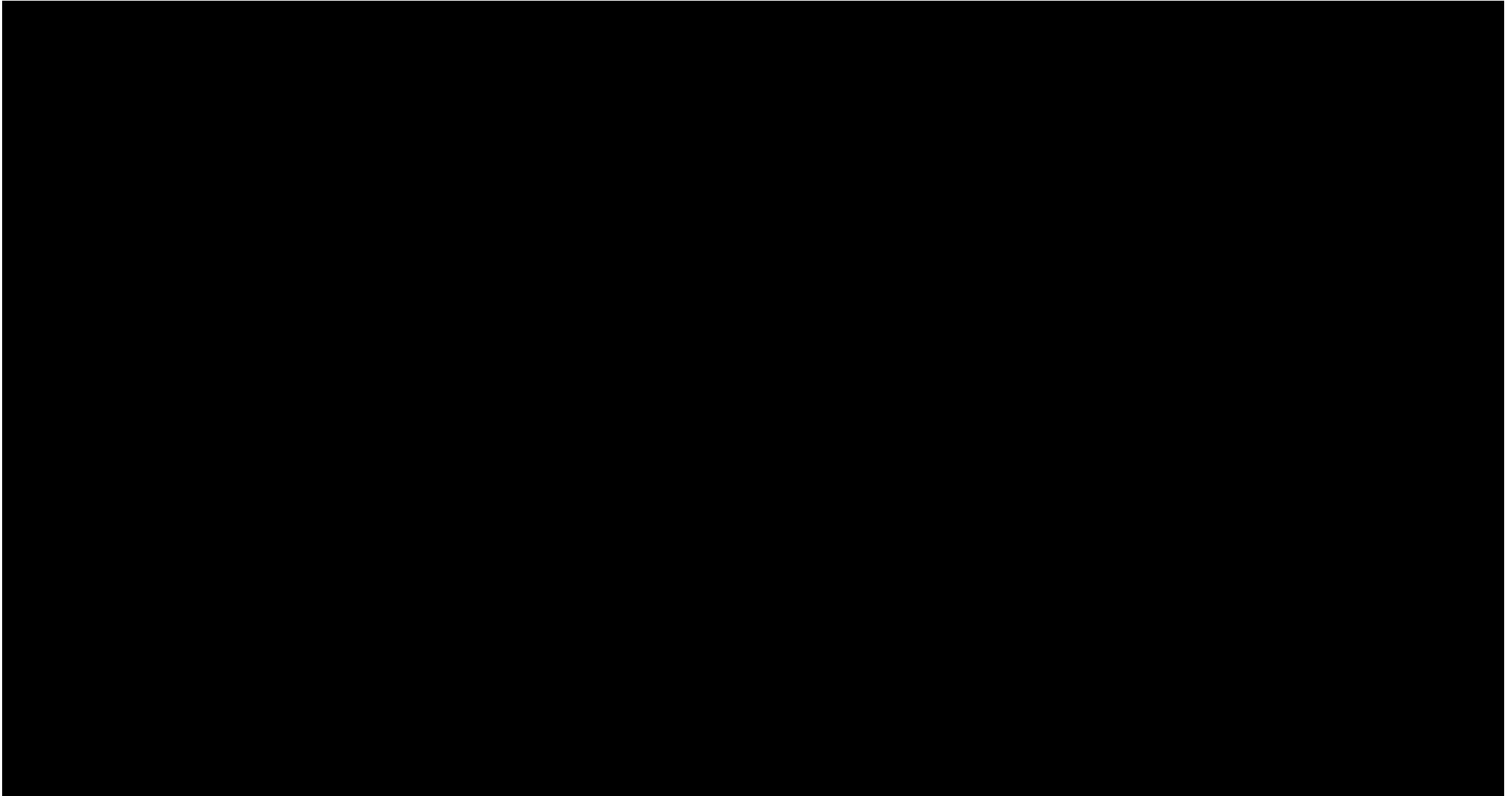
Active Directory  
서버



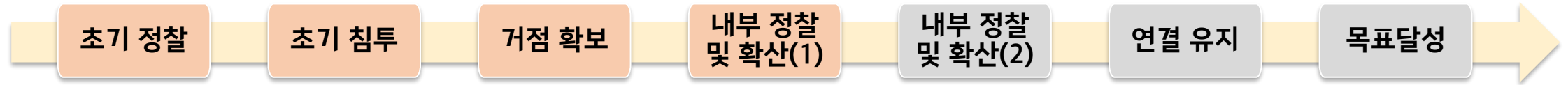
Petya  
hello.exe 랜섬웨어 실행  
2023-12-14 21:12:44

## 공격 시연 영상

---

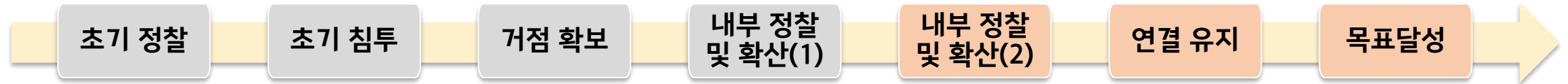


## 대응방안 및 솔루션



| 구분 | Attack Cycle        | 행위                 | 공격                               | 대응방안                       | 솔루션                     | TID                     |
|----|---------------------|--------------------|----------------------------------|----------------------------|-------------------------|-------------------------|
| 1  | 초기 정찰               | 취약점 스캐닝            | 스캐닝 자동화 도구                       | 불필요한 포트 비활성화               | WAF (웹 방화벽)<br>보안관제 서비스 | T1590<br>T1595          |
| 2  | 초기 침투               | RCE 취약점            | CVE-2021-26855<br>CVE-2021-27065 | KB패치, CU패치<br>OWA 외부 접근 차단 | 취약점 진단 서비스              | T1078<br>T1133<br>T1659 |
| 3  | 거점 확보               | WebShell 명령어 실행    | Webshell.aspx                    | 웹 디렉토리 실행 권한 설정            | 웹셸 탐지 솔루션               | T1548                   |
|    |                     | 악성코드 실행            | payload.exe                      | 아웃바운드 정책 설정                | 백신 프로그램<br>EDR          | T1484                   |
| 4  | 내부 정찰<br>및<br>내부 확산 | Credential Dumping | mimikatz                         | 비밀번호 정책 강화<br>WDigest 비활성화 | .                       | T1570<br>T1592          |
|    |                     | 무차별 대입 공격          | hydra                            | Trust to Trust 접근 정책 강화    | 접근 통제 솔루션               | T1110<br>T1212          |

## 대응방안 및 솔루션



| 구분 | Attack Cycle | 행위          | 공격                | 대응방안               | 솔루션            | TID                     |
|----|--------------|-------------|-------------------|--------------------|----------------|-------------------------|
| 5  | 내부 정찰 및 확산   | AD OU 정보 수집 | gather_script.ps1 | .                  | .              | T1003                   |
|    |              | DB 접근       | WinSCP            | 2차 인증 사용<br>DB 암호화 | DB 접근제어 솔루션    | T1072                   |
|    |              | 내부 장악       | 그룹 정책 활용          | .                  | .              | T1484                   |
| 6  | 연결 유지        | 악성코드 삽입     | update.exe        | 아웃바운드 정책 설정        | 백신 프로그램<br>EDR | T1543                   |
| 7  | 목표달성         | 정보 유출       | FileZilla         | FTP 포트 비활성화        | DLP            | T1041                   |
|    |              | 랜섬웨어        | Petya             | .                  | 백신 프로그램<br>EDR | T1489<br>T1490<br>T1529 |

# 05

## 공격 프로파일

MITRE ATT&CK

# MITRE ATT&CK

## MITRE ATT&CK Tactics

| Reconnaissance                    | Resource Development   | Initial Access           | Execution                 | Persistence                     | Privilege Escalation              | Defense Evasion                   | Credential Access                  | Discovery                    | Lateral Movement                | Command and Control        | Exfiltration                 | Impact                  |
|-----------------------------------|------------------------|--------------------------|---------------------------|---------------------------------|-----------------------------------|-----------------------------------|------------------------------------|------------------------------|---------------------------------|----------------------------|------------------------------|-------------------------|
| Active Scanning                   | Acquire Access         | Content Injection        | Software Deployment Tools | Create or Modify System Process | Abuse Elevation Control Mechanism | Abuse Elevation Control Mechanism | Brute Force                        | Account Discovery            | Exploitation of Remote Services | Application Layer Protocol | Exfiltration Over C2 Channel | Account Access Removal  |
| Gather Victim Host Information    | Acquire Infrastructure | External Remote Services |                           | External Remote Services        | Domain Policy Modification        | Domain Policy Modification        | Exploitation for Credential Access | File and Directory Discovery | Lateral Tool Transfer           | Content Injection          |                              | Inhibit System Recovery |
| Gather Victim Network Information | Compromise Accounts    | Valid Accounts           |                           | Server Software Component       | Valid Accounts                    | Exploitation for Defense Evasion  | OS Credential Dumping              | Group Policy Discovery       | Remote Services                 | Proxy                      |                              | Service Stop            |
|                                   | Stage Capabilities     |                          |                           | Valid Accounts                  |                                   | Impair Defenses                   |                                    |                              | Software Deployment Tools       | Remote Access Software     |                              | System Shutdown/Reboot  |
|                                   |                        |                          |                           |                                 |                                   | Valid Accounts                    |                                    |                              |                                 |                            |                              |                         |

※ MITRE ATT&CK Framework는 공격자의 초기 정보 수집 및 계획 행위부터 공격의 최종실행에 이르기까지 사이버공격 라이프 사이클의 각 단계에 따른 사이버 범죄 전술, 기법 등을 분류하여 정리한 것입니다.

# MITRE ATT&CK

## MITRE ATT&CK Tactics

| Reconnaissance                    | Resource Development   | Initial Access           | Execution                 | Persis          |
|-----------------------------------|------------------------|--------------------------|---------------------------|-----------------|
| Active Scanning                   | Acquire Access         | Content Injection        | Software Deployment Tools | Create o System |
| Gather Victim Host Information    | Acquire Infrastructure | External Remote Services |                           | External Serv   |
| Gather Victim Network Information | Compromise Accounts    | Valid Accounts           |                           | Server S Comp   |
|                                   | Stage Capabilities     |                          |                           | Valid A         |



# 06

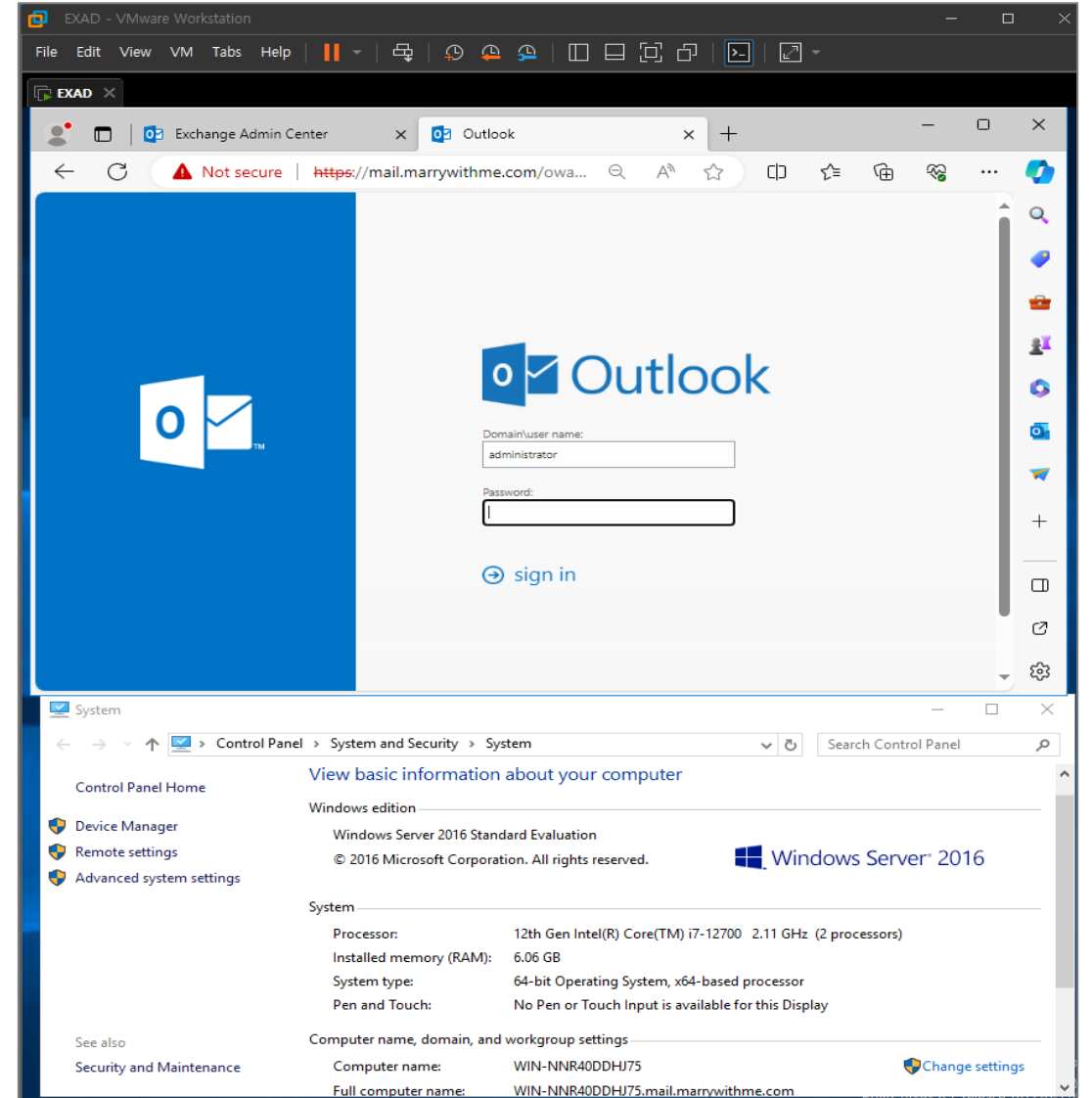
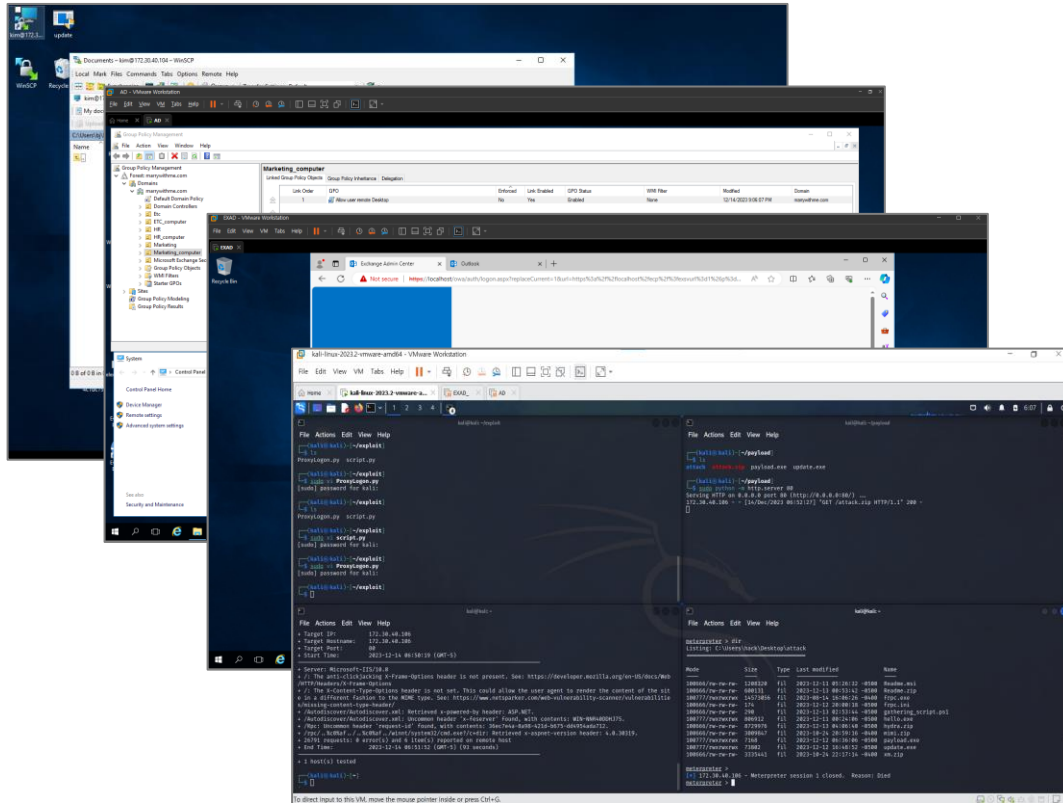
## 산출물

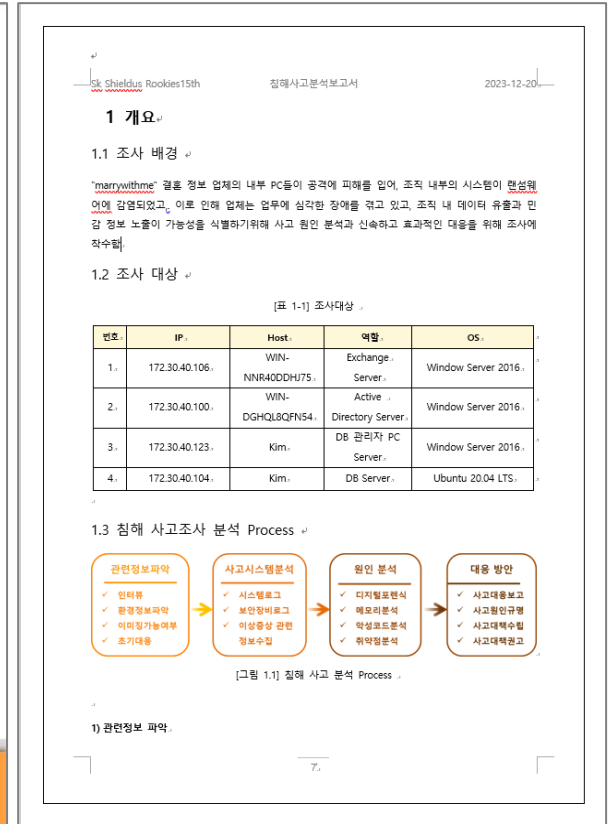
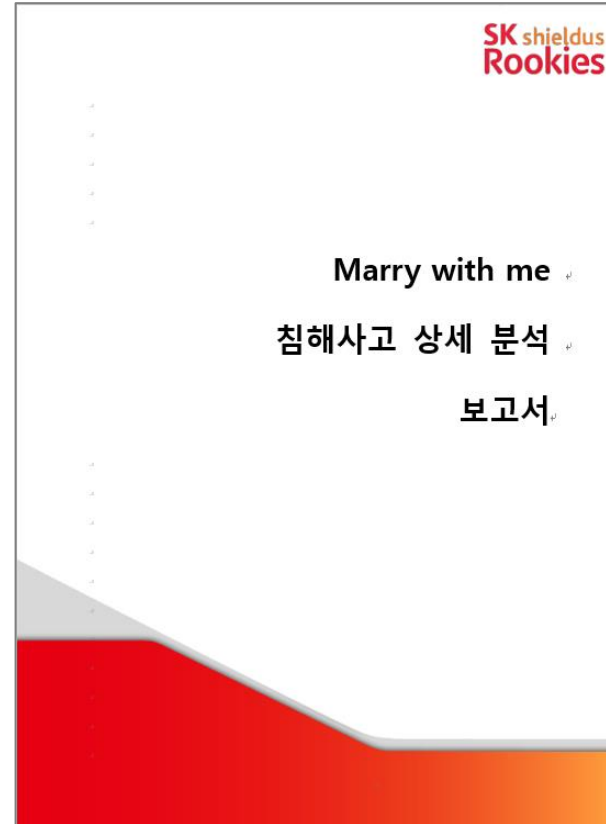
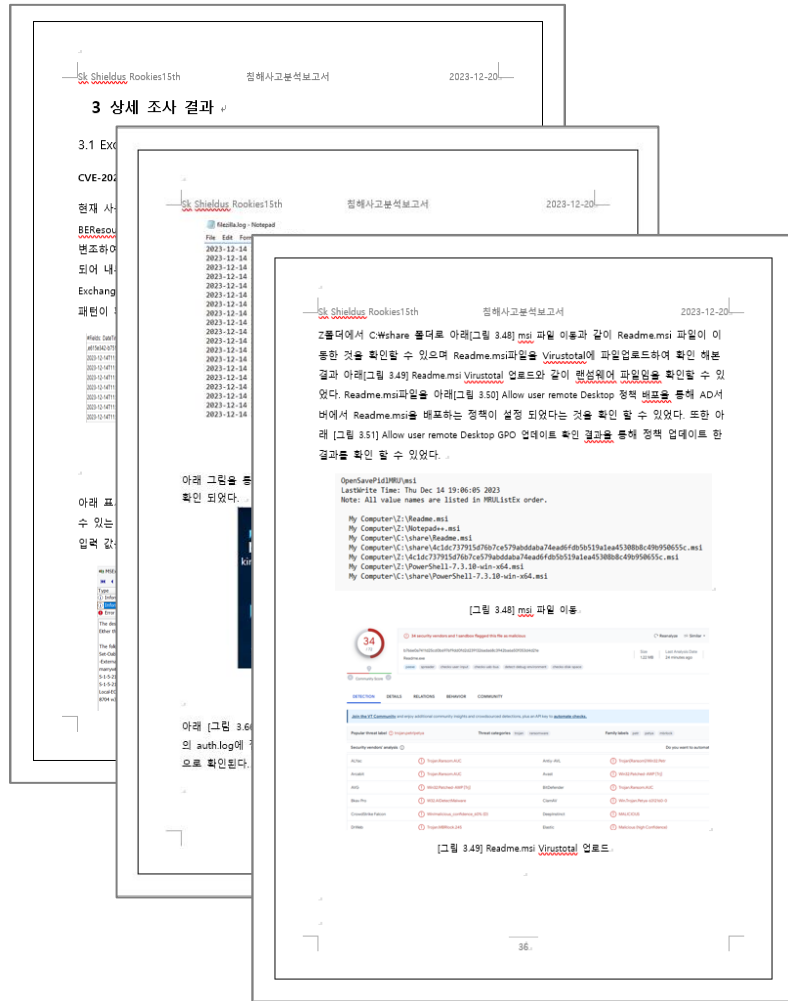
보고서

구축 이미지

공동 작업물

# 산출물 구축 이미지





## Notion-공동 작업물

SAW: Microsoft Exchange 2016 cu19 KB4588884

## AD 사용자 정보 게더링하기

AD에서 POWERSHELL을 켜 후,

## 정책할당 후 랜섬웨어 삽입

```
gpupdate /force gpresult -r
{05A6454F-288D-478E-A947-35F0385E4E0C}
```

## 악성코드분석



2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527 2528 2529 2530 2531 2532 2533 2534 2535 2536 2537 2538 2539 2540 2541 2542 2543 2544 2545 2546 2547 2548 2549 2550 2551 2552 2553 2554 2555 2556 2557 2558 2559 2560 2561 2562 2563 2564 2565 2566 2567 2568 2569 2570 2571 2572 2573 2574 2575 2576 2577 2578 2579 2580 2581 2582 2583 2584 2585 2586 2587 2588 2589 2590 2591 2592 2593 2594 2595 2596 2597 2598 2599 2600 2601 2602 2603 2604 2605 2606 2607 2608 2609 2610 2611 2612 2613 2614 2615 2616 2617 2618 2619 2620 2621 2622 2623 2624 2625 2626 2627 2628 2629 2630 2631 2632 2633 2634 2635 2636 2637 2638 2639 2640 2641 2642 2643 2644 2645 2646 2647 2648 2649 2650 2651 2652 2653 2654 2655 2656 2657 2658 2659 2660 2661 2662 2663 2664 2665 2666 2667 2668 2669 2670 2671 2672 2673 2674 2675 2676 2677 2678 2679 2680 2681 2682 2683 2684 2685 2686 2687 2688 2689 2690 2691 2692 2693 2694 2695 2696 2697 2698 2699 2700 2701 2702 2703 2704 2705 2706 2707 2708 2709 2710 2711 2712 2713 2714 2715 2716 2717 2718 2719 2720 2721 2722 2723 2724 2725 2726 2727 2728 2729 2730 2731 2732 2733 2734 2735 2736 2737 2738 2739 2740 2741 2742 2743 2744 2745 2746 2747 2748 2749 2750 2751 2752 2753 2754 2755 2756 2757 2758 2759 2760 2761 2762 2763 2764 2765 2766 2767 2768 2769 2770 2771 2772 2773 2774 2775 2776 2777 2778 2779 2780 2781 2782 2783 2784 2785 2786 2787 2788 2789 2790 2791 2792 2793 2794 2795 2796 2797 2798 2799 2800 2801 2802 2803 2804 2805 2806 2807 2808 2809 2810 2811 2812 2813 2814 2815 2816 2817 2818

국립현대미술관 URL: [www.museum.go.kr](http://www.museum.go.kr) 찾기



VT ENTERPRISE를 사용하여 해시, 도메인, IP 주소, URL을 검색하거나 주  
가 검색으로 및 위험 점진 가시성을 확보하세요.

4c15c717916d7a27e579ab3d8a74a96f8b525f9a45308b8c49b950a55

최저 가격을 자율적으로 구현하는 **비즈니스 모델** 및 **가전정보보호정책**의 적용과 비교 분석의 성공 여부를 보완 커뮤니케이션을 통해 공유하는 데 중점을 둡니다. 가전 정보를 자율적으로 수집하고, VirusTotal을 권하는 자율적인 내용의 대외 책임을 지고 있습니다. **최대 이익**

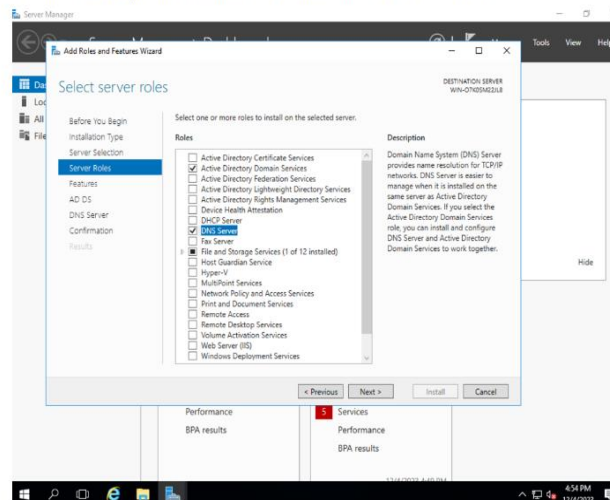
## AD 구축 및 부모 Exchange 설정

출처:

<https://hope.pe.kr/761>

3040103

1. Active Directory Domain Services랑 DNS Server 체크 추가후 인스톨하면 끝



2. 깃발에서 promote domain control 클릭후 새로운 포레스트를 만듬 (marrywithme.com)




커버 추가 댓글 추가

## 분석 도구 및 Dump 파일

## Windows 분석 도구

 Windows\_Artifact\_Script.zip 29781.2KB

로그(이벤트로그익스플로어)

 [elex\\_fe\\_setup.zip](#) 10834.4KB

## IP정리

AD: 172.30.40.100

EXAD:172.30.40.106

공격자 1: 172.30.40.125

공격자 2: 172.30.40.97

DB 관리자:172.30.40.123

## Dump 파일

AD

# 07

## 자체 평가 의견

## 자체 평가 의견

### 프로젝트를 통한 경험

- ▶ 모든 조원들이 열정적으로 참여하여 짧은 기간에 성공적으로 프로젝트를 마무리 할 수 있었다.
- ▶ 오류와 어려움이 있었지만, 함께 검색하고 노력하여 프로젝트를 완성하는 과정에서 협동심을 기를 수 있었다.
- ▶ 서로에게 질문하고 도움을 주고받으며 프로젝트를 진행하는데 큰 도움이 되었다.

### 공통의견

- ▶ 사전 학습을 2주 동안 진행하다 보니 프로젝트 진행 기간이 많이 짧았다.
- ▶ 네트워크 및 자원부족으로 인해 잦은 오류가 많았다.
- ▶ 발표가 총 20분이라 모든 것을 보여드리지 못해 아쉽다.

# 감사합니다



내이름은코난,탐정이조

# QnA



내이름은코난,탐정이조