어떻게 들어왔는가?

안랩 A-FIRST

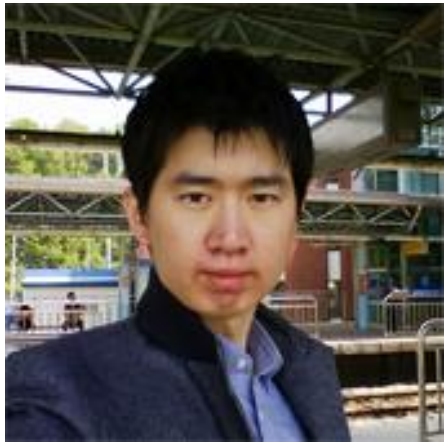
오정훈

Jh.oh@ahnlab.com

Who am I ??

A·FIRST

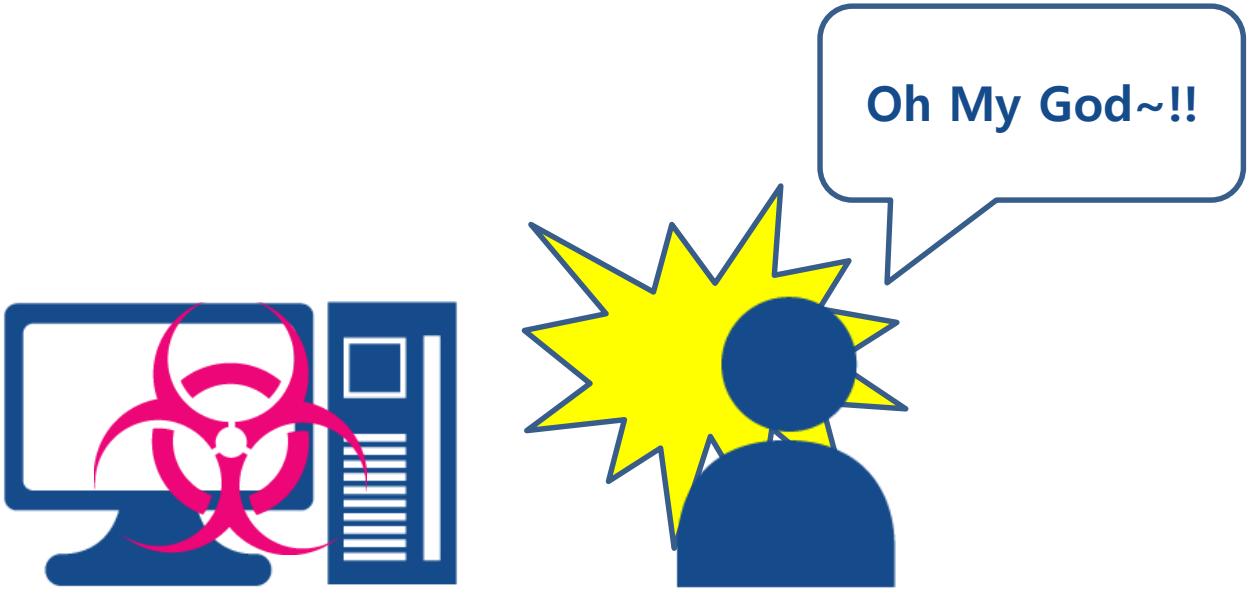
- 이름 : 오정훈(jh.oh@ahnlab.com)



- 소속 : 안랩 A-FIRST
- 업무 : 침해 사고 분석
- 경력
  - 고려대 정보보호대학원 디지털포렌식연구센터(2010.01 ~ 2011.12)
  - 안랩 A-FIRST(2012.01 ~ 현재)
  - DFRWS 2011 Speaker : Advanced Evidence Collection and Analysis of Web Browser Activity
  - 2012 미국방성 Digital Forensic Challenge : Overall Civilian Winner
  - WISA 2012 Speaker : Advanced Evidence Collection and Analysis of Web Browser Activity
  - FIRST 2014 Speaker : A Forensic Analysis of APT Lateral Movement in Windows Environment
  - 2014 Forensic Insight 공개 세미나 Speaker : APT 내부망 감염 기법 분석
- 도구 : NTFS Log Tracker, RP Log Tracker (https://sites.google.com/site/forensicnote/)

왜? 어떻게 들어왔는지 알아야 하나?

시스템에서 악성코드를 발견하였다면...



시스템에서 악성코드를 발견하였다면...

어떻게 하시나요??

일반적인 대응…

일반적인 대응…

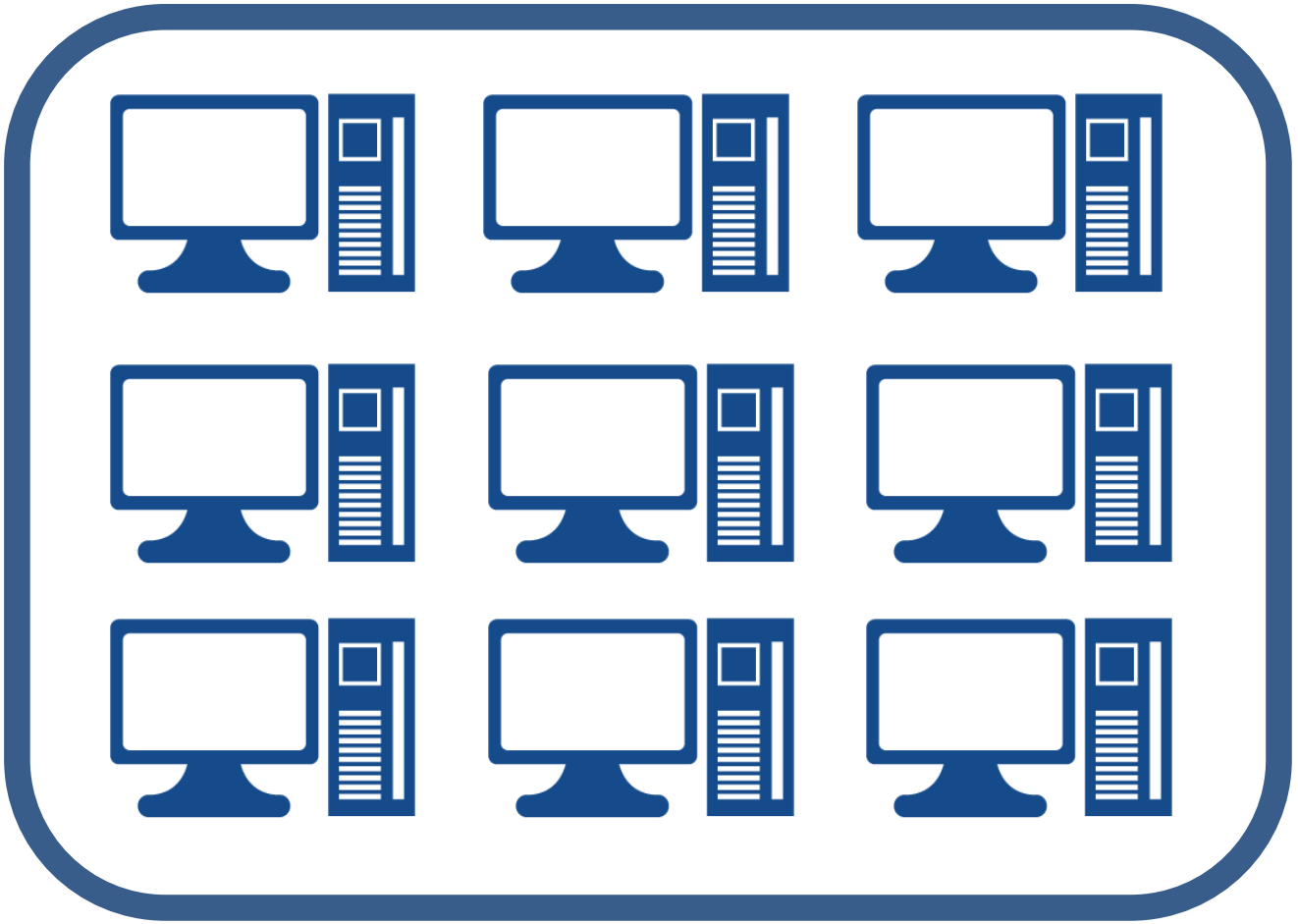
포멧 or 시스템 교체

일반적인 대응…

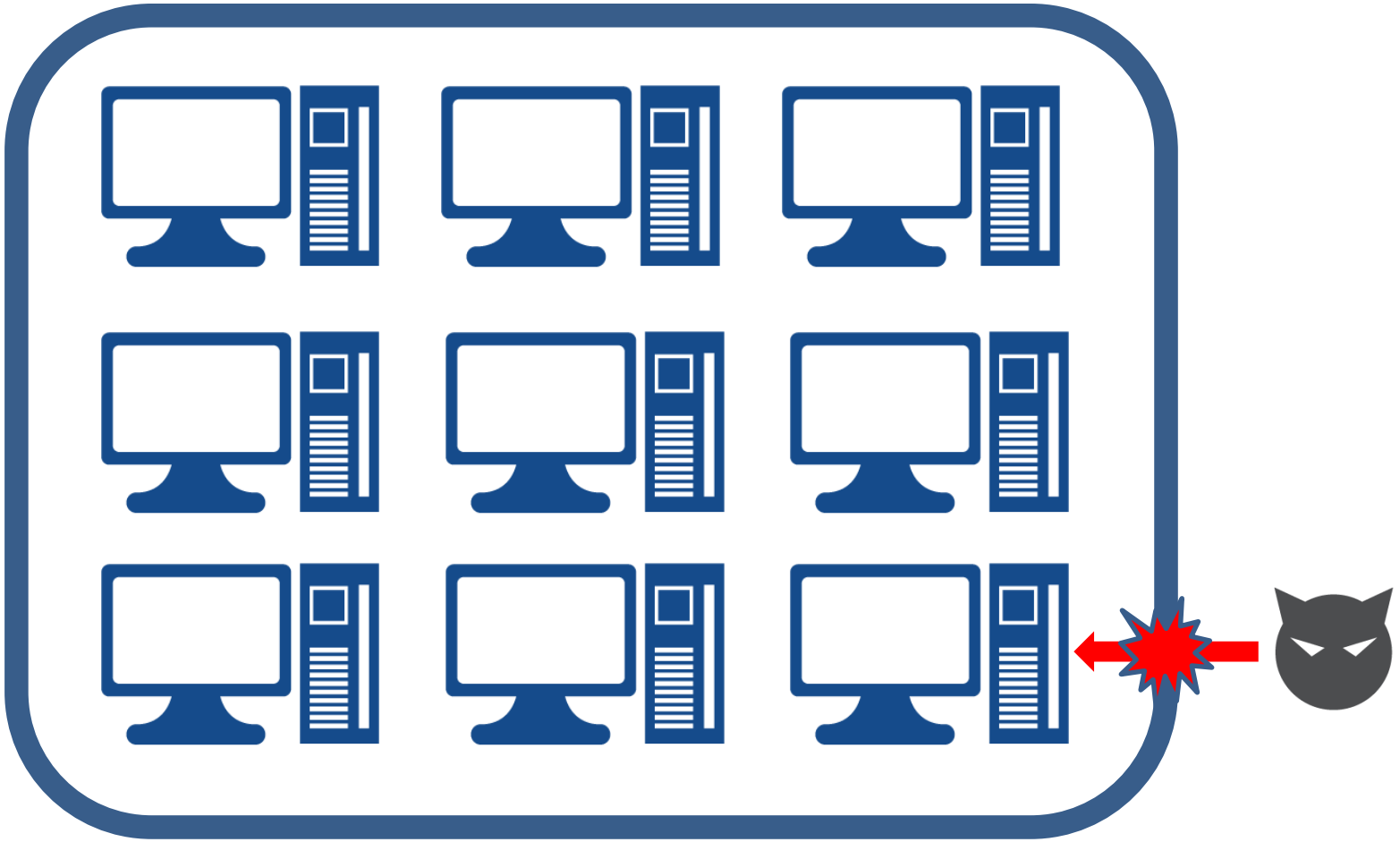
일반적인 대응…

실제 상황 …

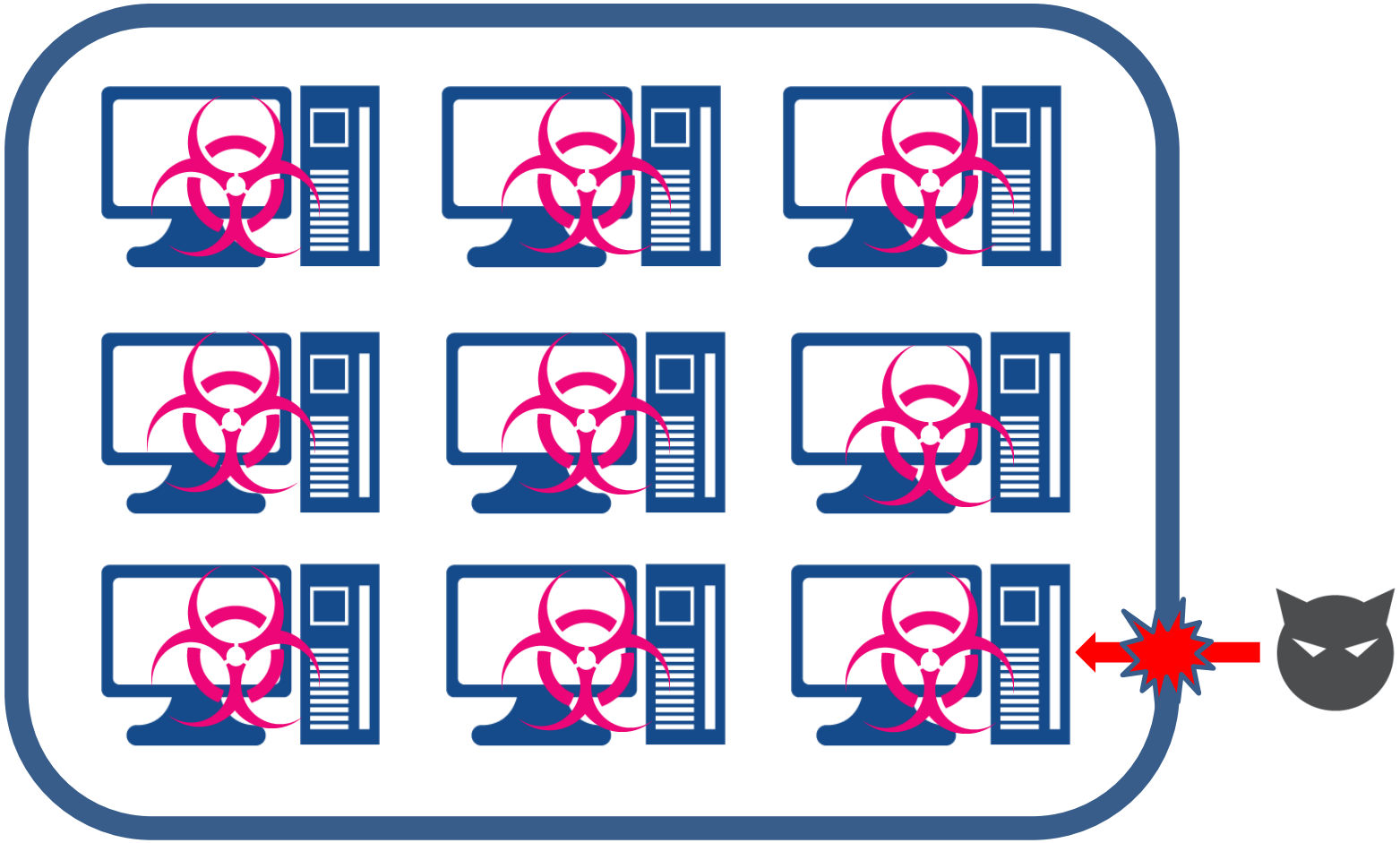
실제 상황 …



실제 상황 …



실제 상황 …



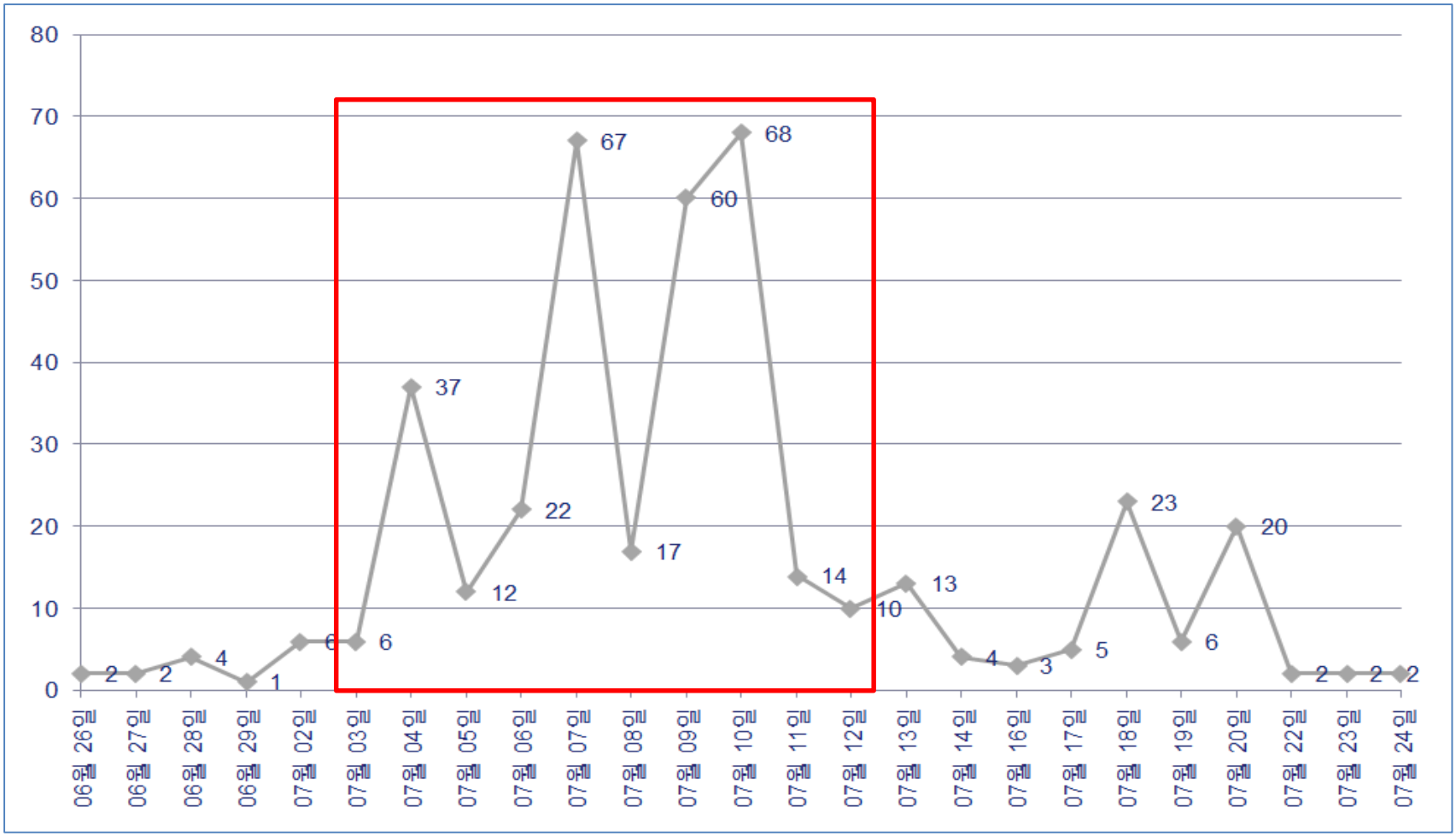
공격자 vs 관리자 ??

감염 vs 치료

공격자 vs 관리자 ??

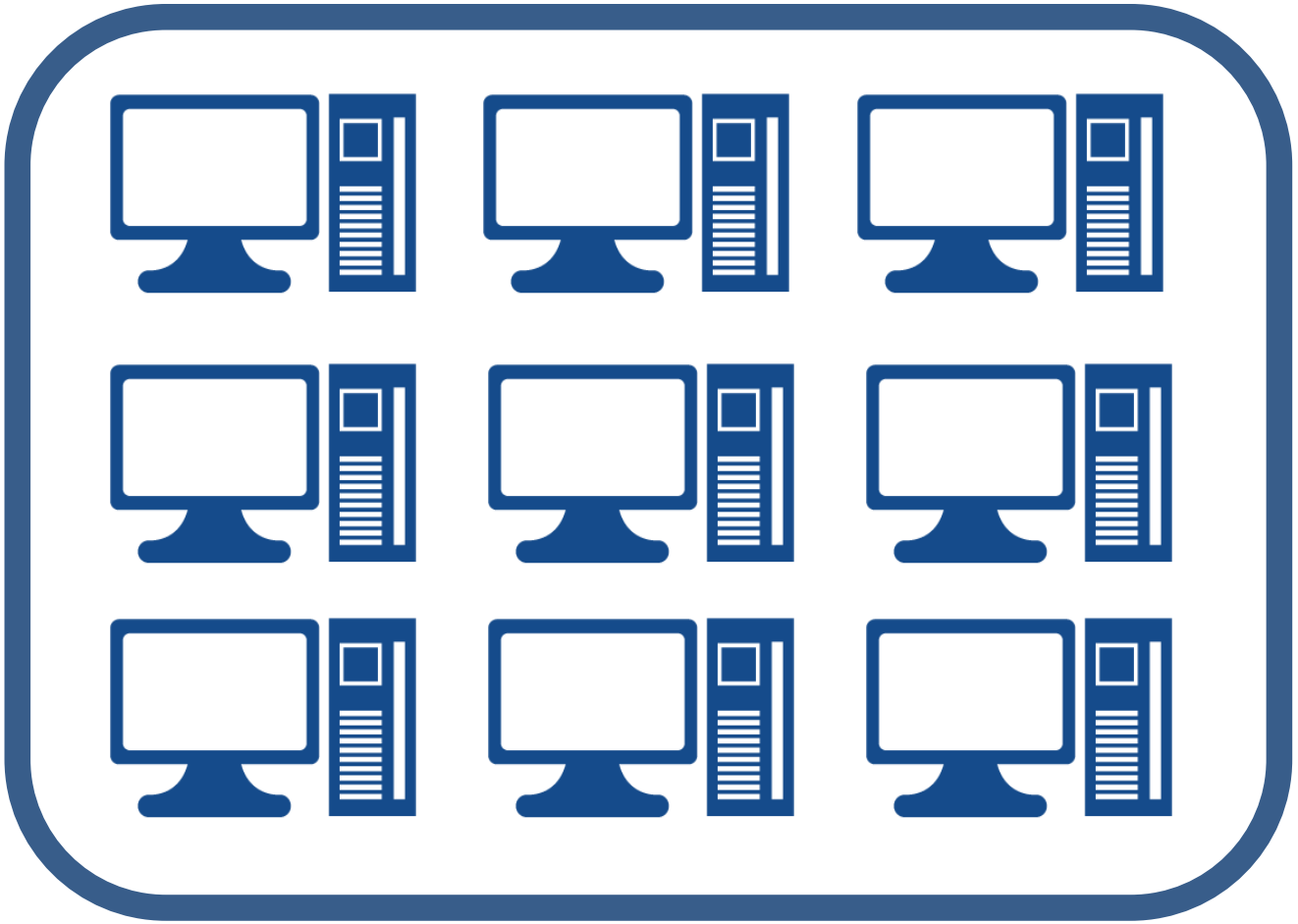
공격자 vs 관리자 ??

공격자 vs 관리자 ??


80
70
60
50
40
30
20
10
0
2
2
4
1
6
6
37
12
22
67
17
60
68
14
10
13
4
3
5
23
6
20
2
2
2
06월 26일
06월 27일
06월 28일
06월 29일
07월 02일
07월 03일
07월 04일
07월 05일
07월 06일
07월 07일
07월 08일
07월 09일
07월 10일
07월 11일
07월 12일
07월 13일
07월 14일
07월 16일
07월 17일
07월 18일
07월 19일
07월 20일
07월 22일
07월 23일
07월 24일

어떤 CEO 께서는...

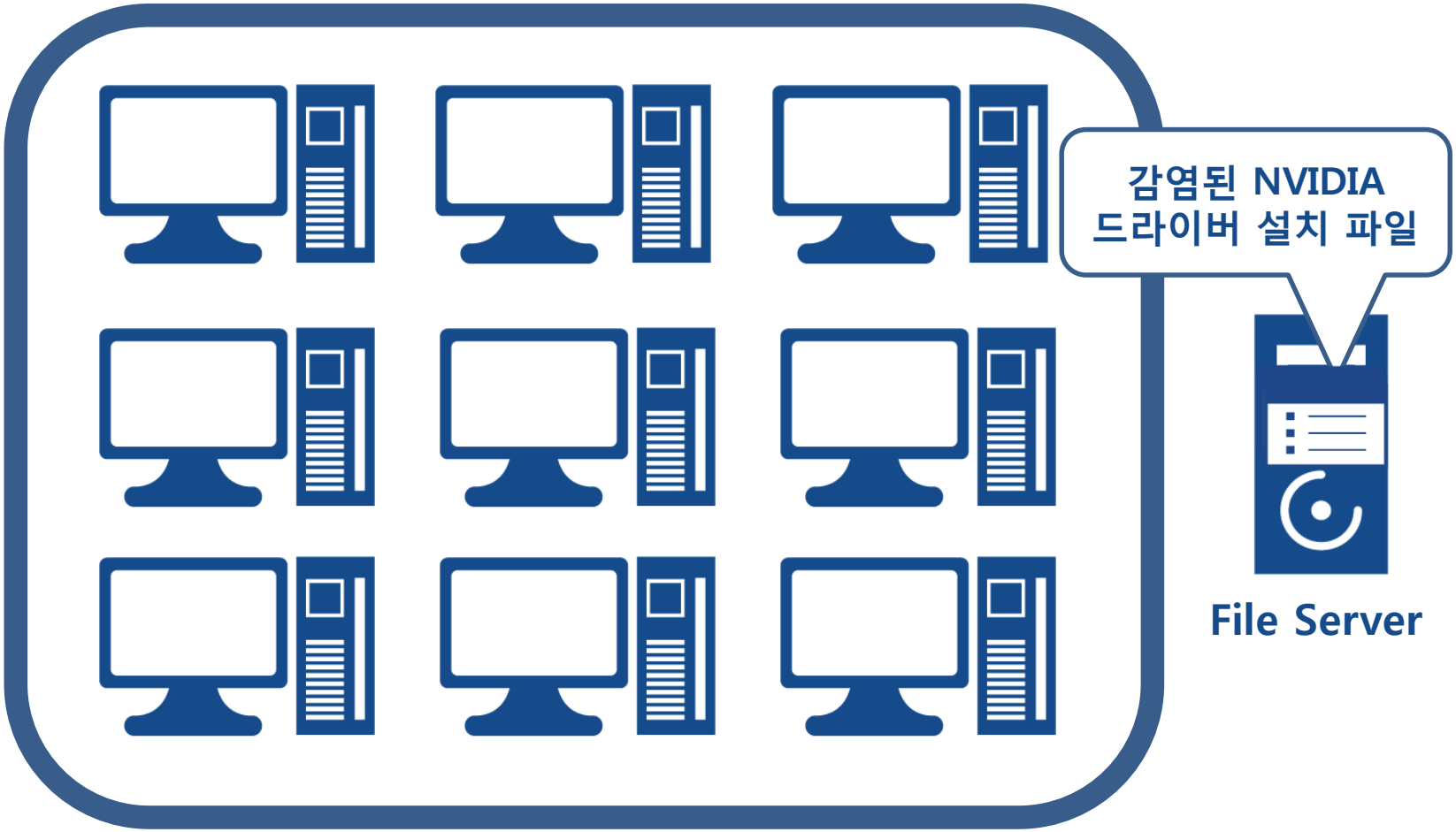
모든 시스템 재설치...



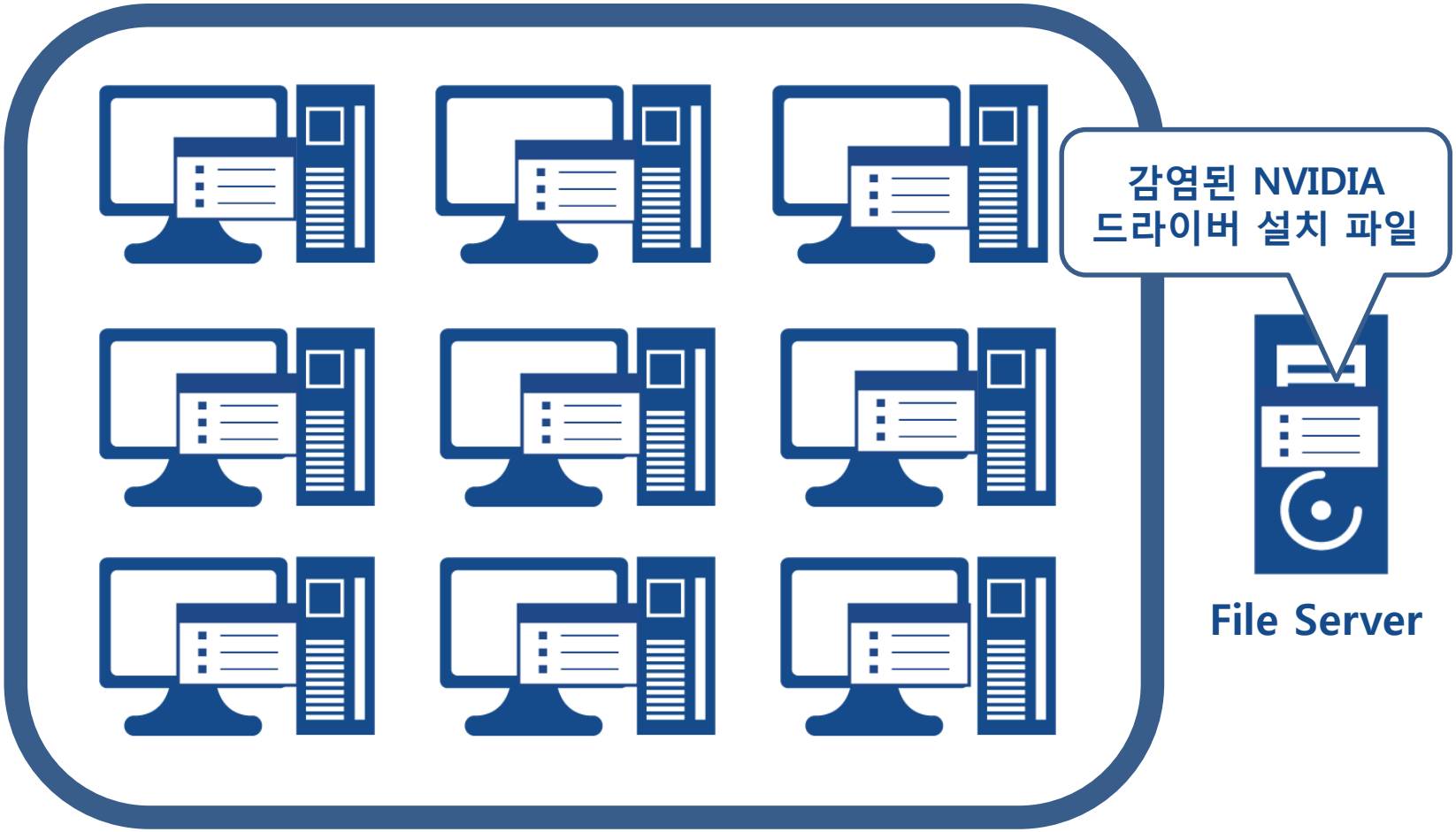
재감염...;;

왜 계속 감염되지 ??

왜 계속 감염되지 ??

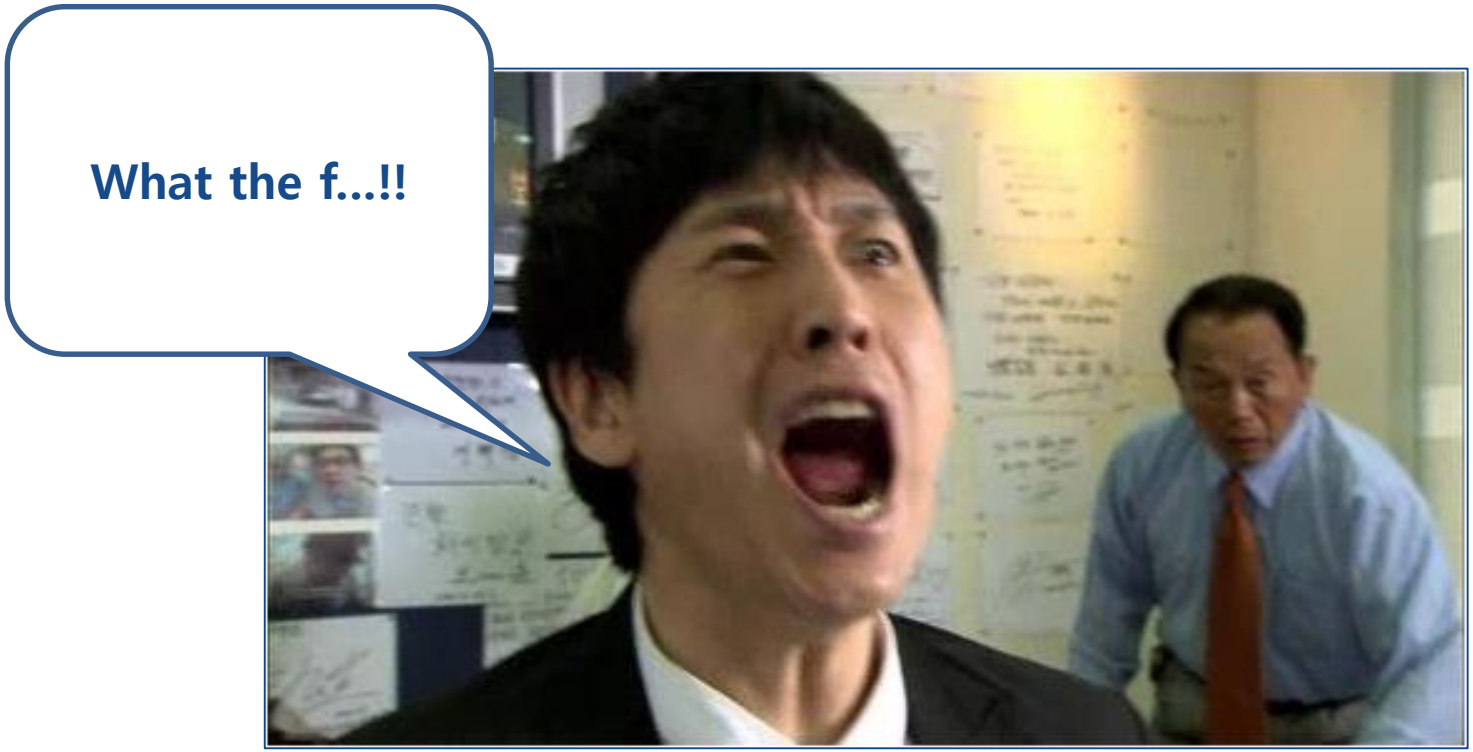


왜 계속 감염되지 ??



왜 계속 감염되지 ??

만약 최초 유입 경로를 찾지 못했다면...

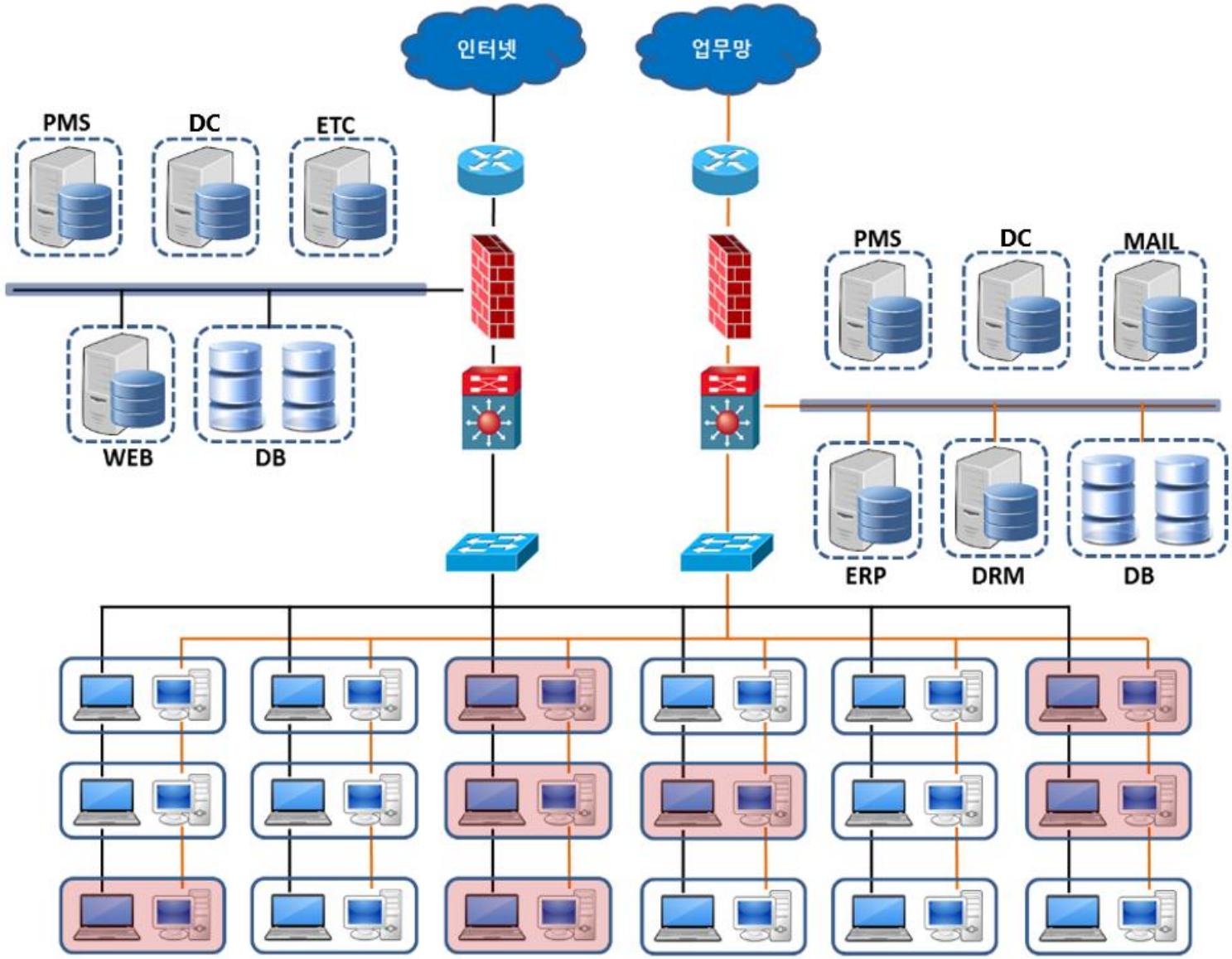


따라서 …

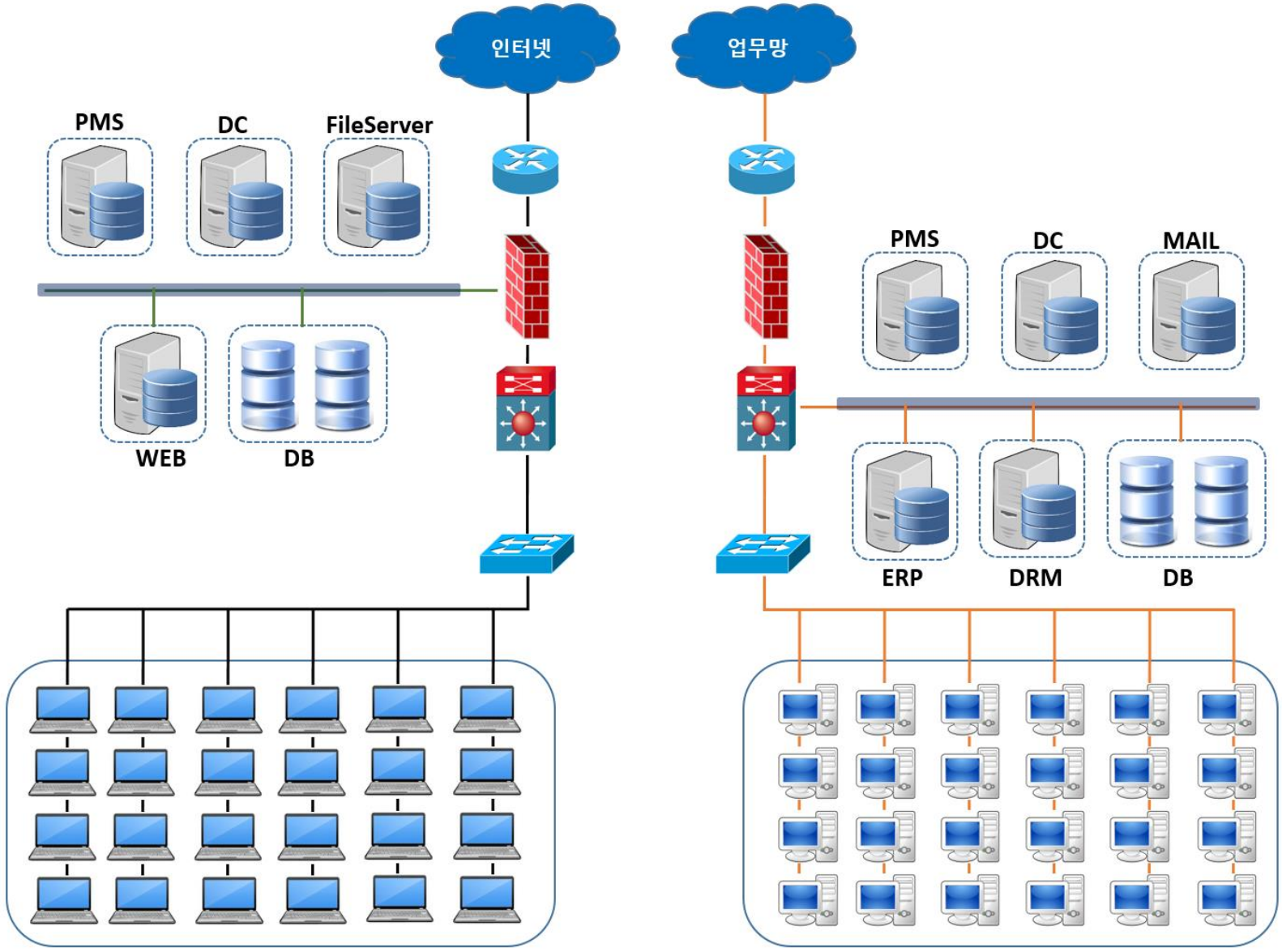
No Initial Breach Point, No Win …

일반적인 APT 공격 과정

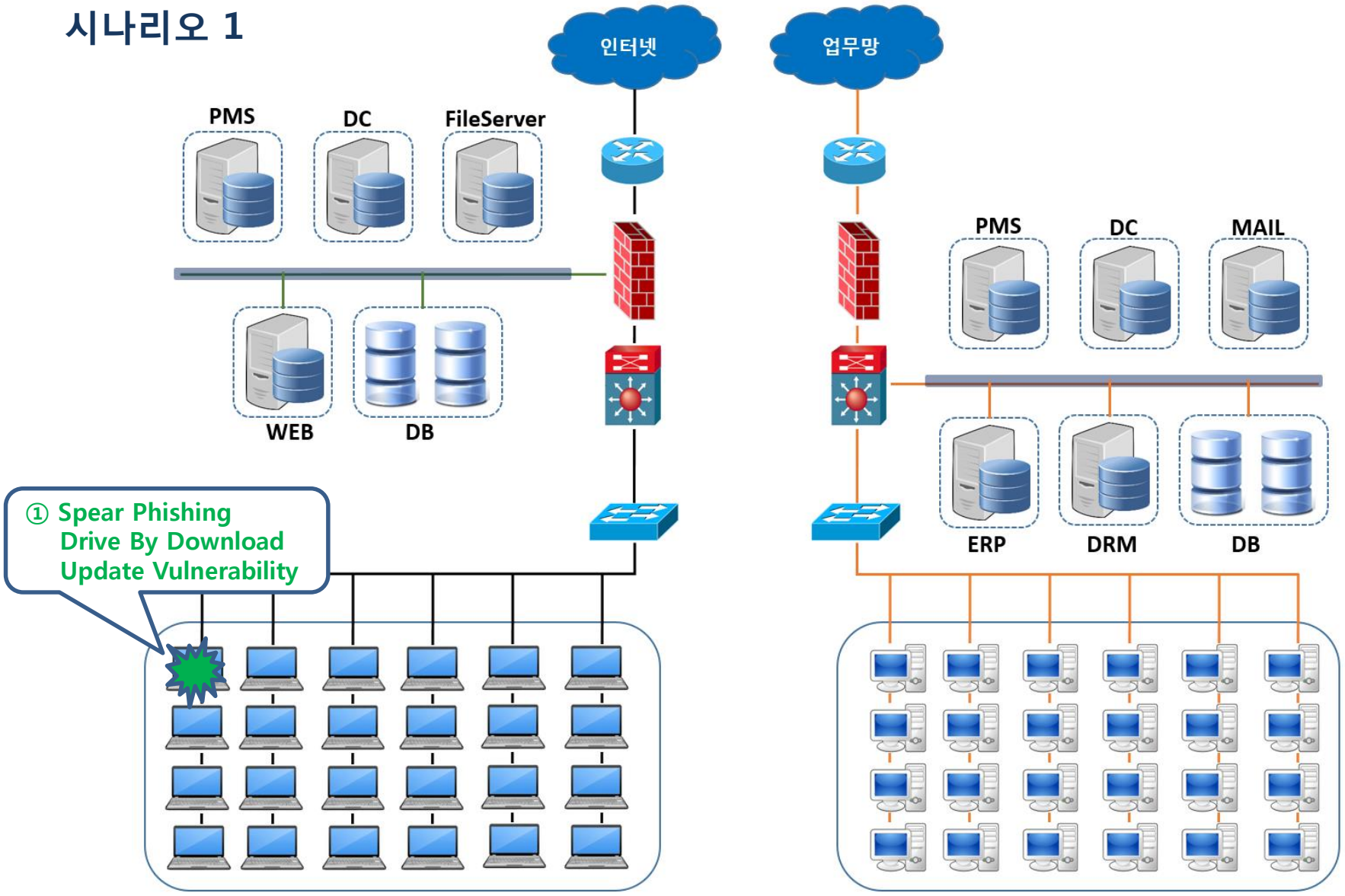
일반적인 APT 공격 과정



일반적인 APT 공격 과정

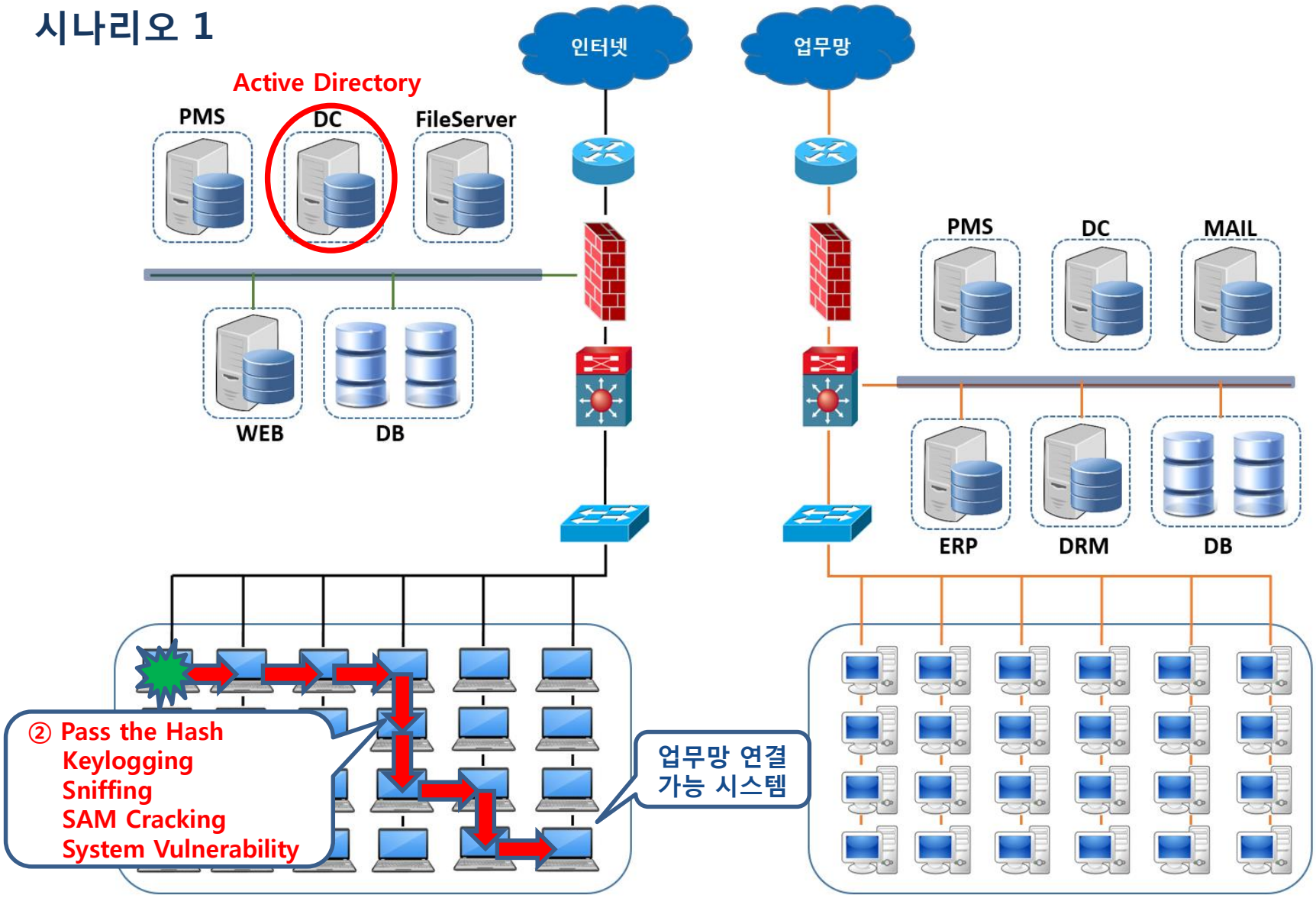


시나리오 1

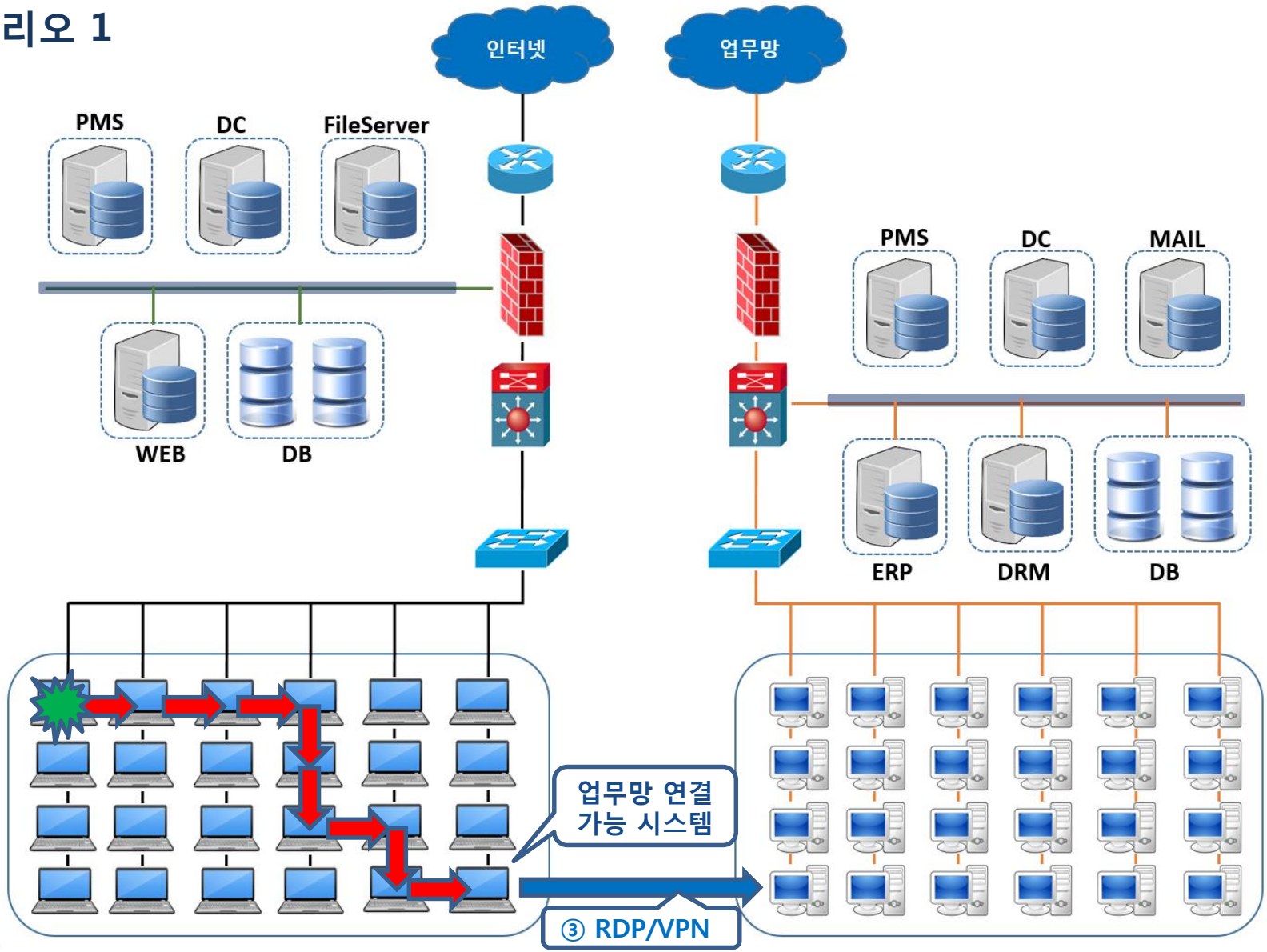

인터넷
업무망
PMS
DC
FileServer
WEB
DB
PMS
DC
MAIL
ERP
DRM
DB
① Spear Phishing
Drive By Download
Update Vulnerability

일반적인 APT 공격 과정

시나리오 1

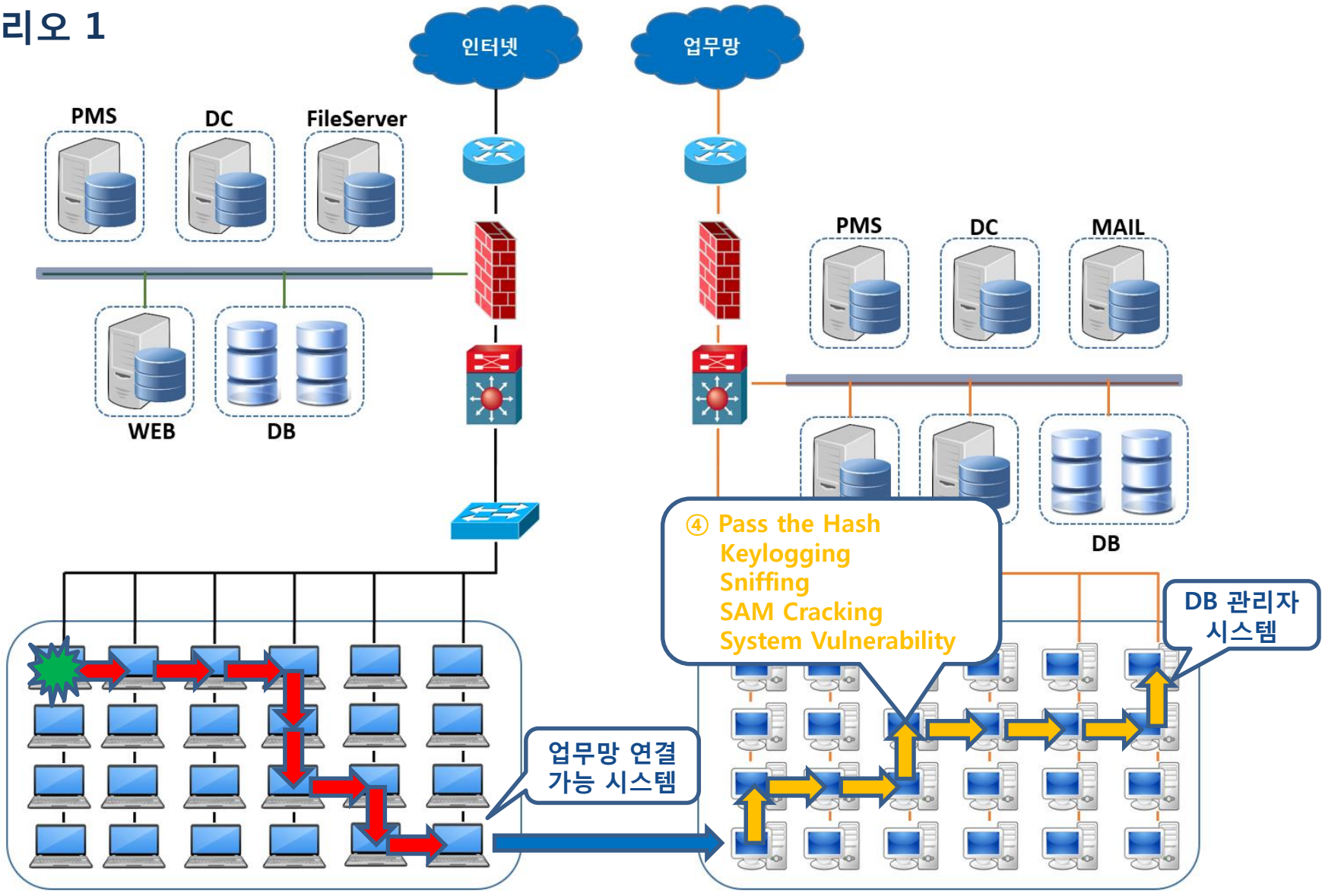


시나리오 1


인터넷
업무망
PMS
DC
FileServer
WEB
DB
PMS
DC
MAIL
ERP
DRM
DB
업무망 연결
가능 시스템
③ RDP/VPN

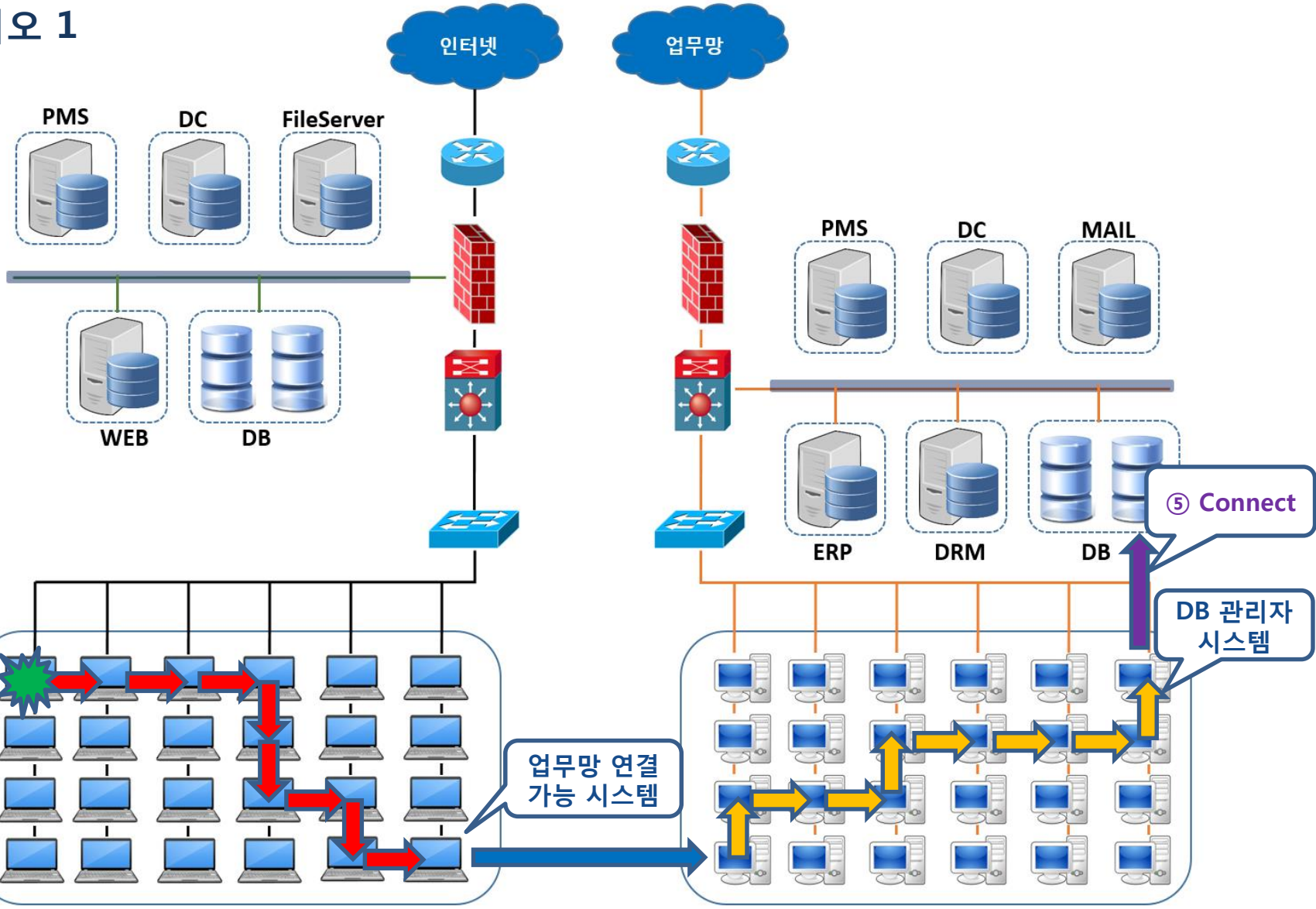
일반적인 APT 공격 과정

시나리오 1

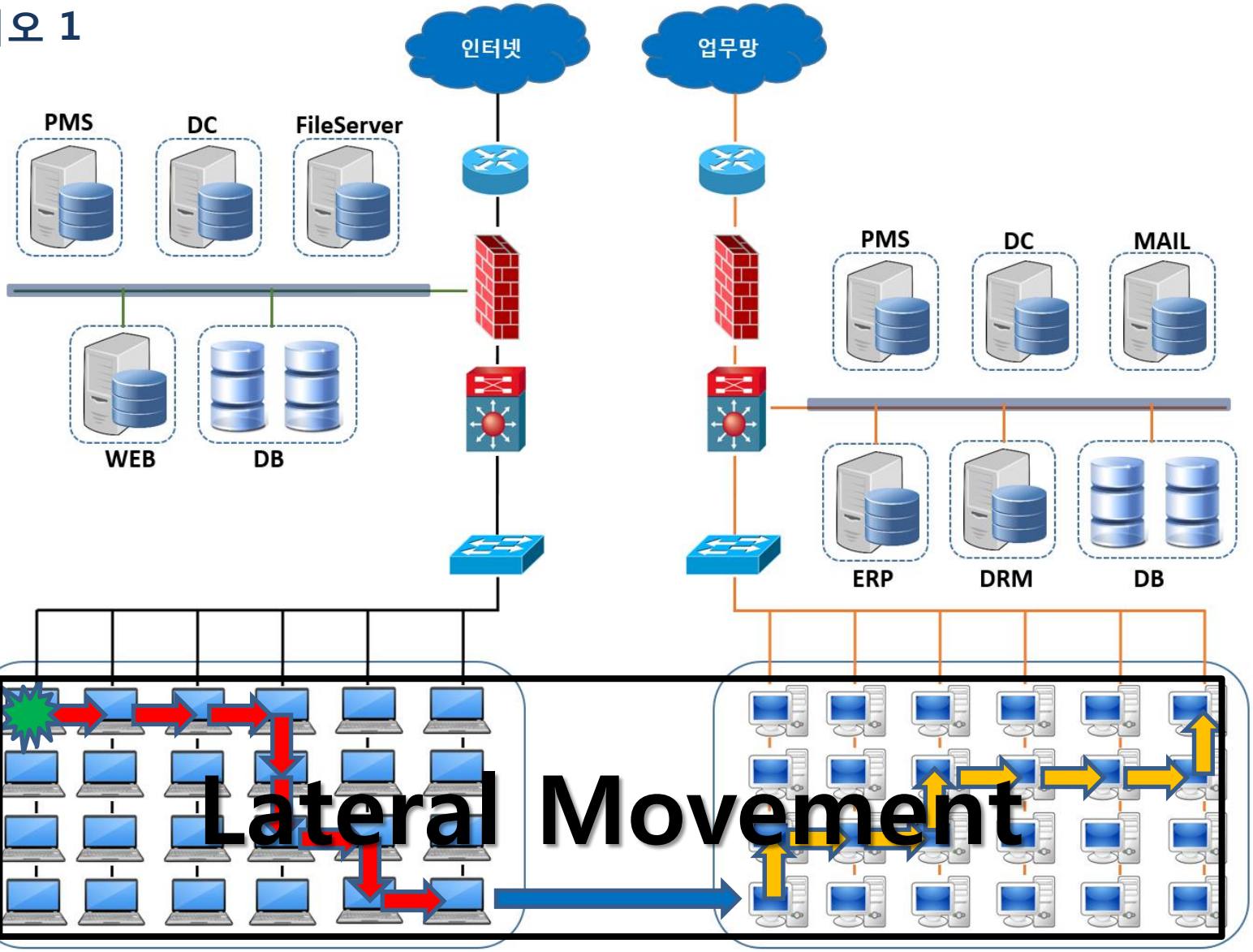


일반적인 APT 공격 과정

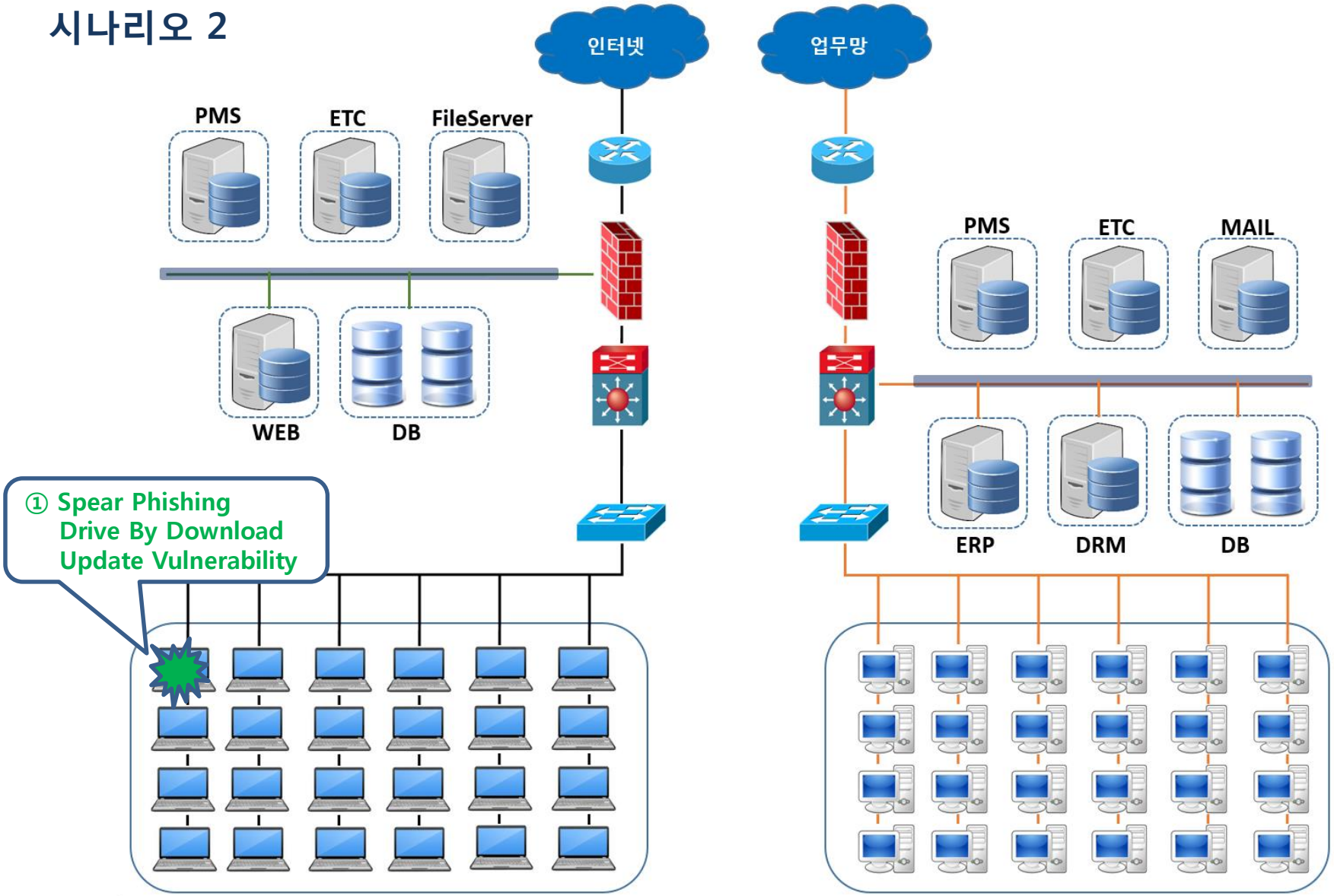
시나리오 1



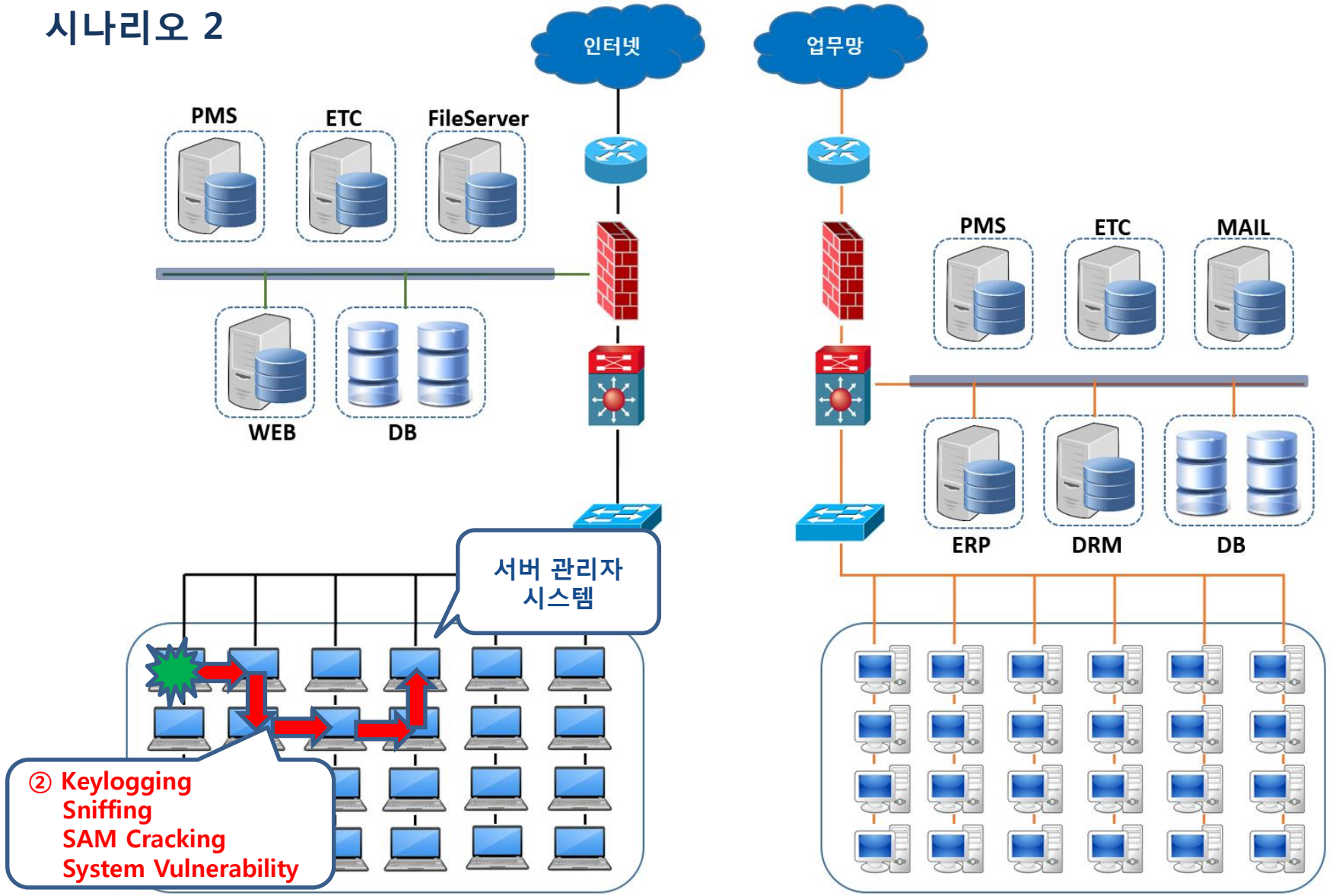
시나리오 1


인터넷
업무망
PMS
DC
FileServer
WEB
DB
PMS
DC
MAIL
ERP
DRM
DB
Lateral Movement

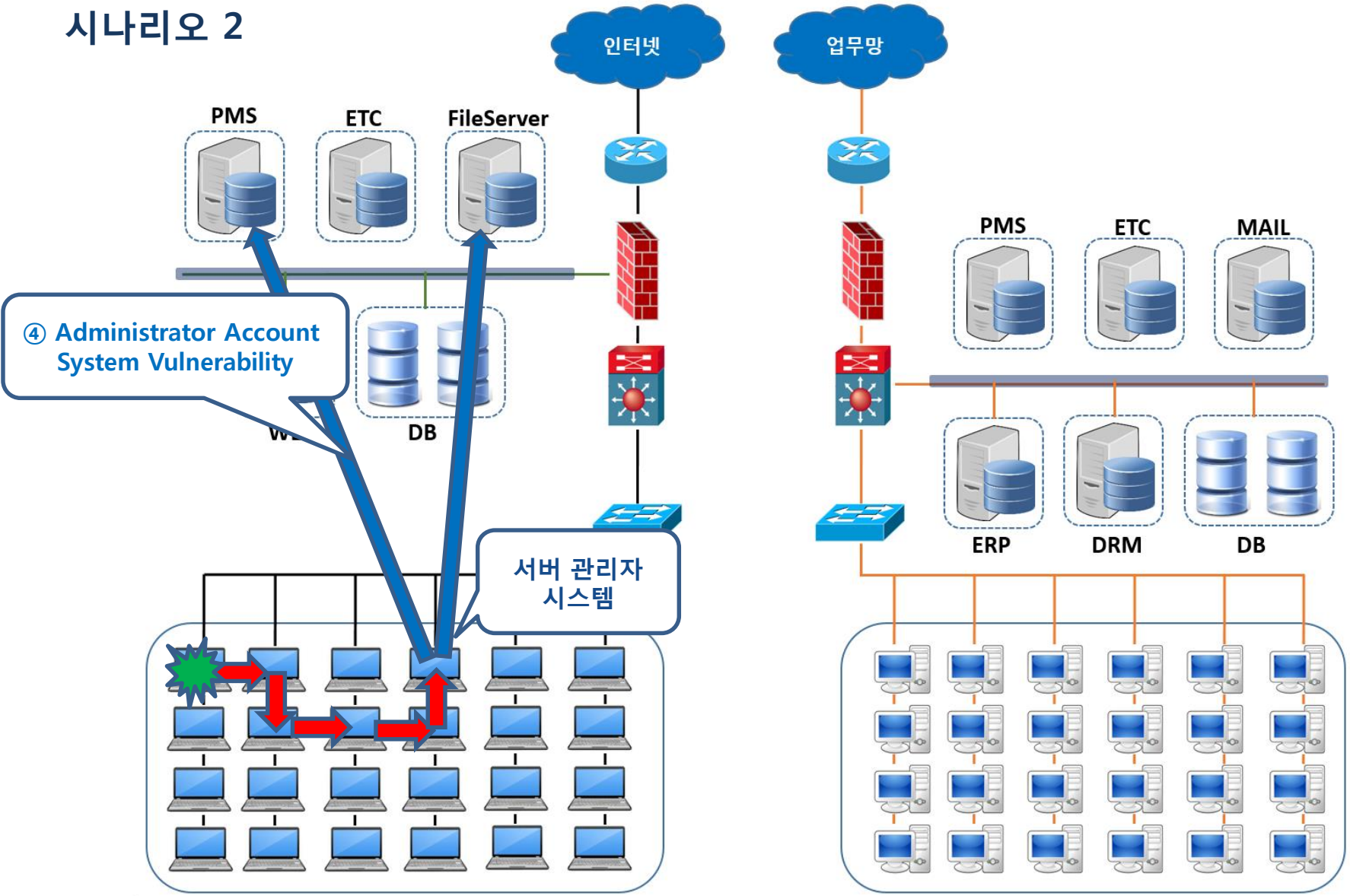
시나리오 2


인터넷
업무망
PMS
ETC
FileServer
WEB
DB
PMS
ETC
MAIL
ERP
DRM
DB
① Spear Phishing
Drive By Download
Update Vulnerability

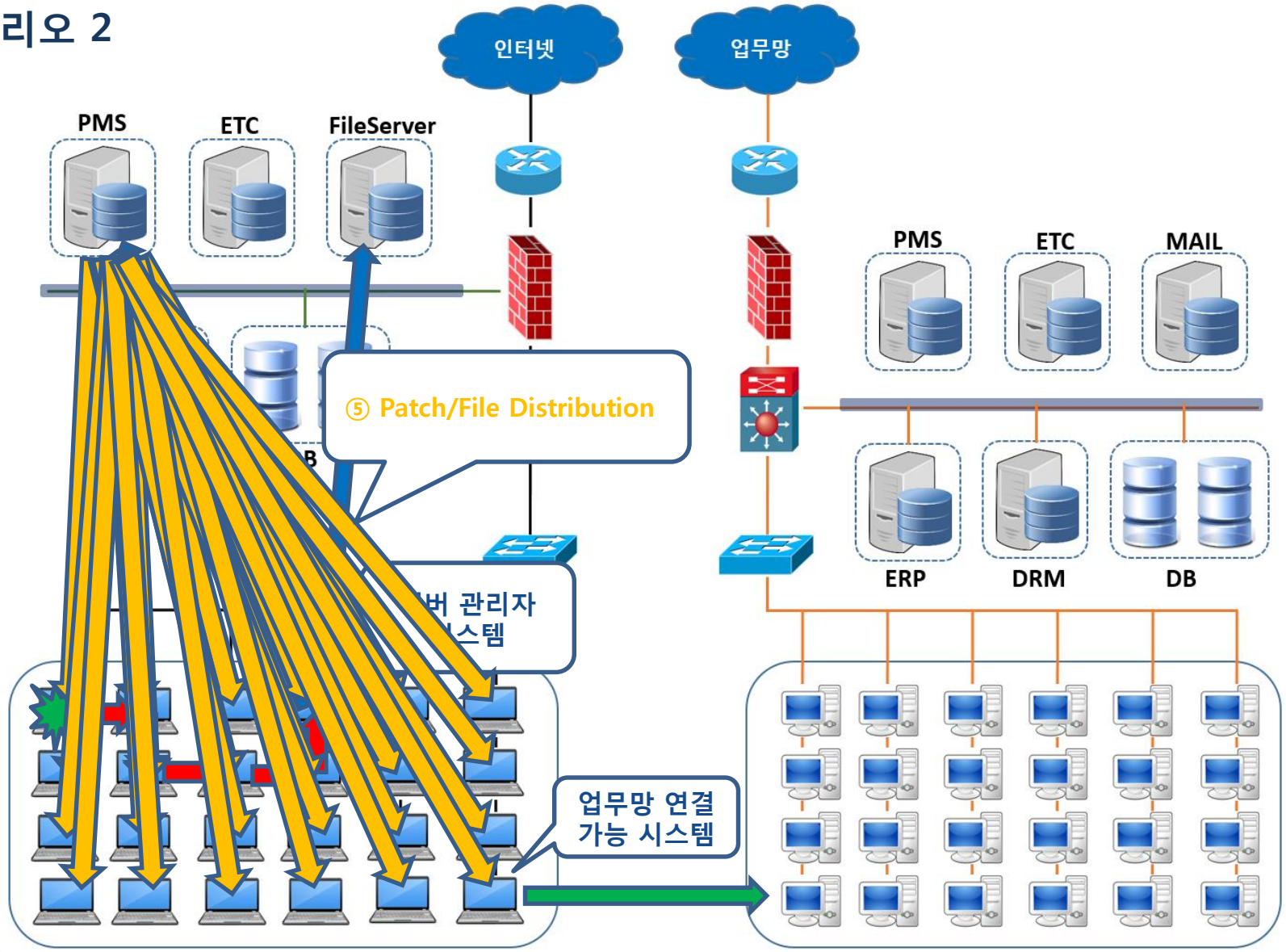
시나리오 2


인터넷
업무망
PMS
ETC
FileServer
WEB
DB
PMS
ETC
MAIL
ERP
DRM
DB
서버 관리자
시스템
② Keylogging
Sniffing
SAM Cracking
System Vulnerability

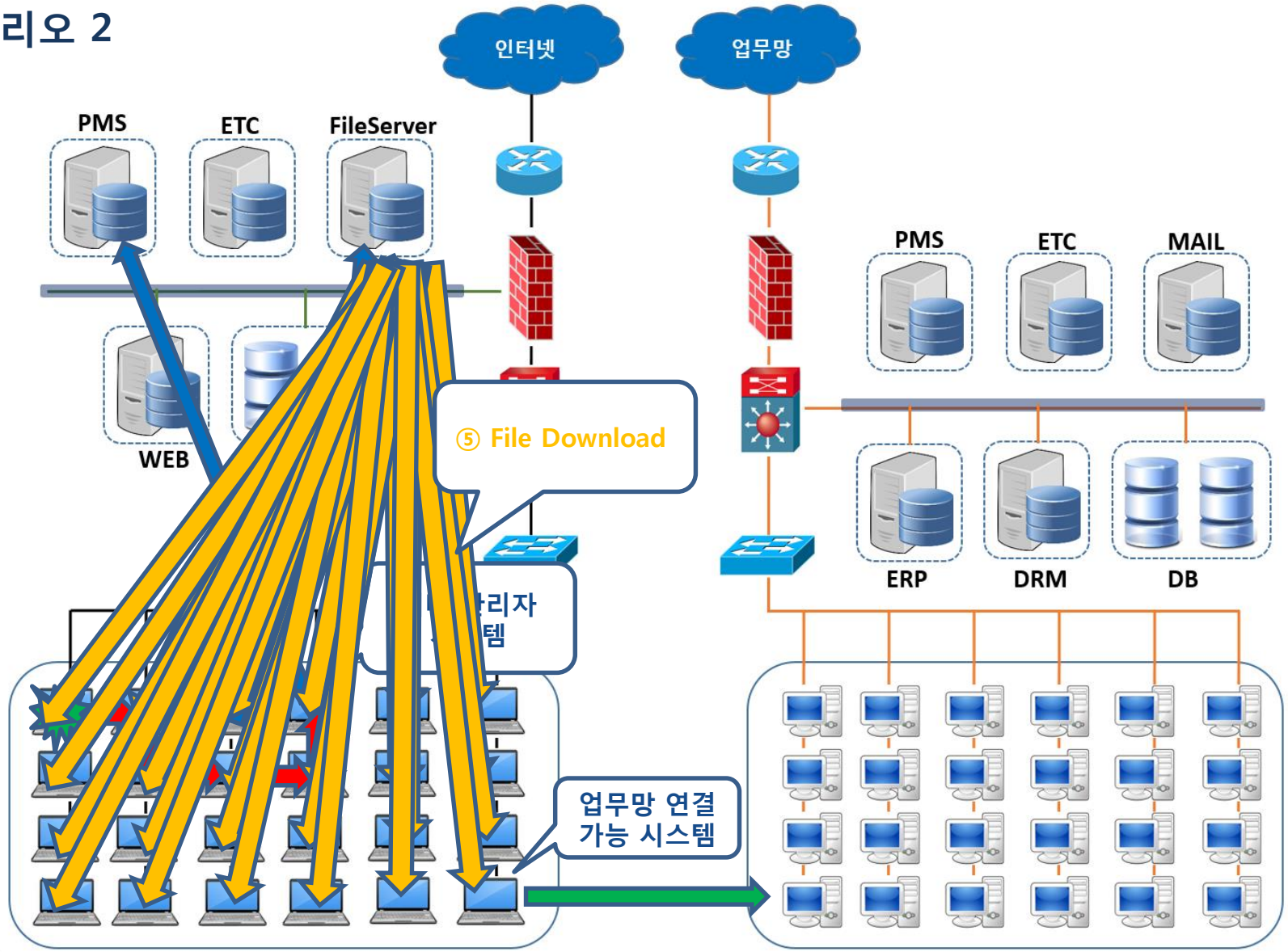
시나리오 2


인터넷
업무망
PMS
ETC
FileServer
DB
④ Administrator Account
System Vulnerability
서버 관리자
시스템
PMS
ETC
MAIL
ERP
DRM
DB

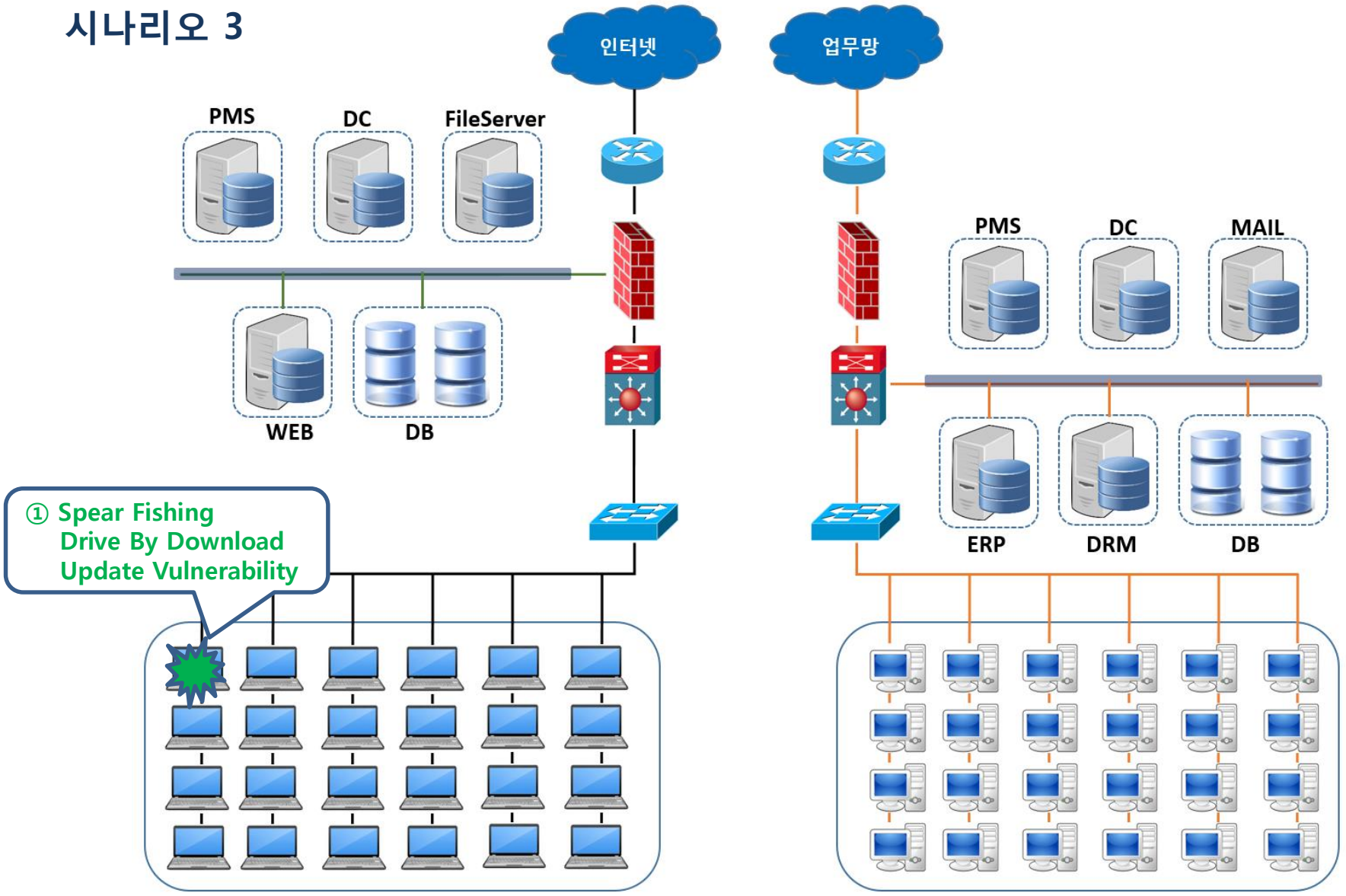
시나리오 2


인터넷
업무망
PMS
ETC
FileServer
PMS
ETC
MAIL
⑤ Patch/File Distribution
ERP
DRM
DB
업무망 연결
가능 시스템

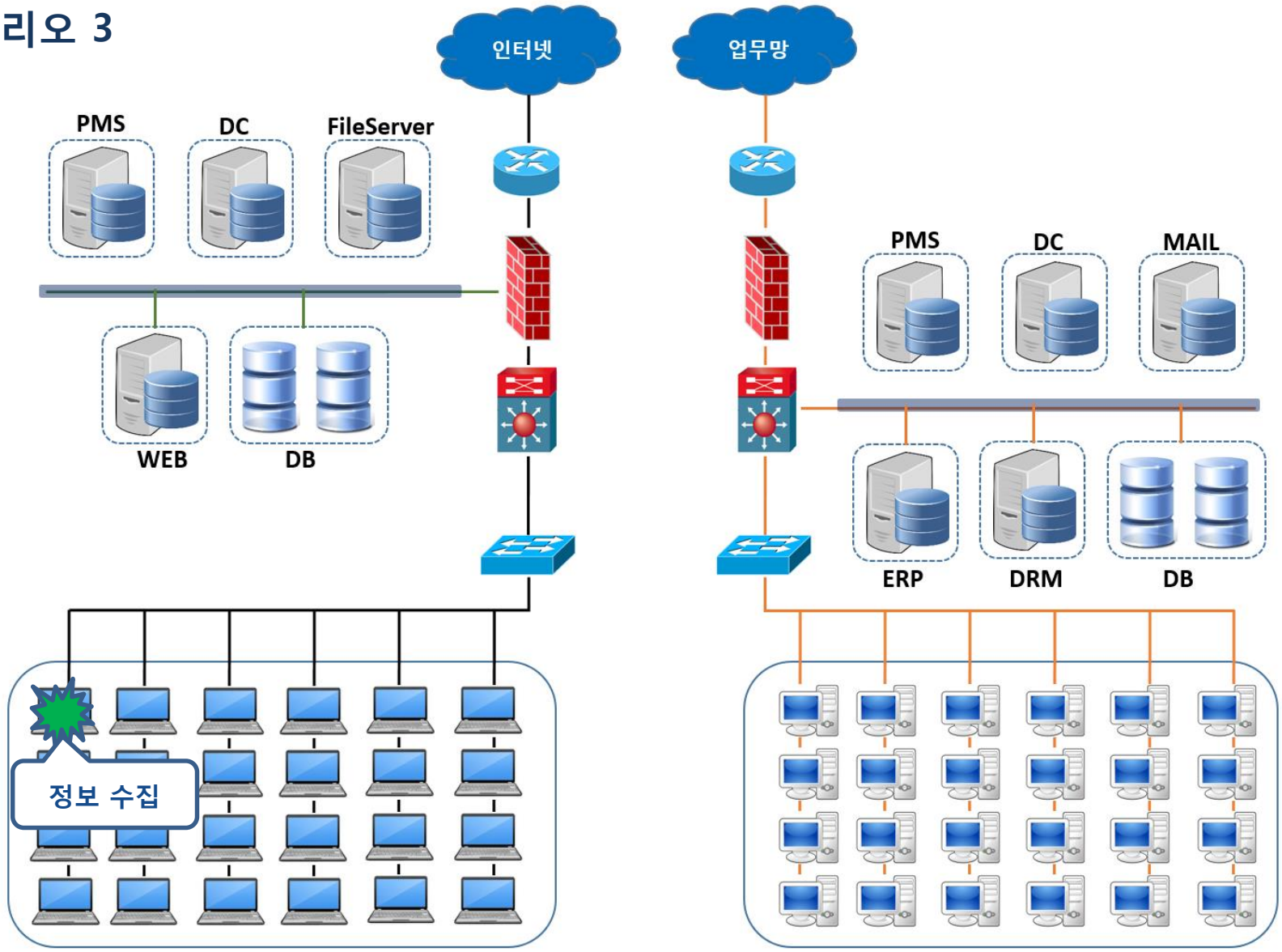
시나리오 2


인터넷
업무망
PMS
ETC
FileServer
WEB
PMS
ETC
MAIL
ERP
DRM
DB
⑤ File Download
업무망 연결
가능 시스템

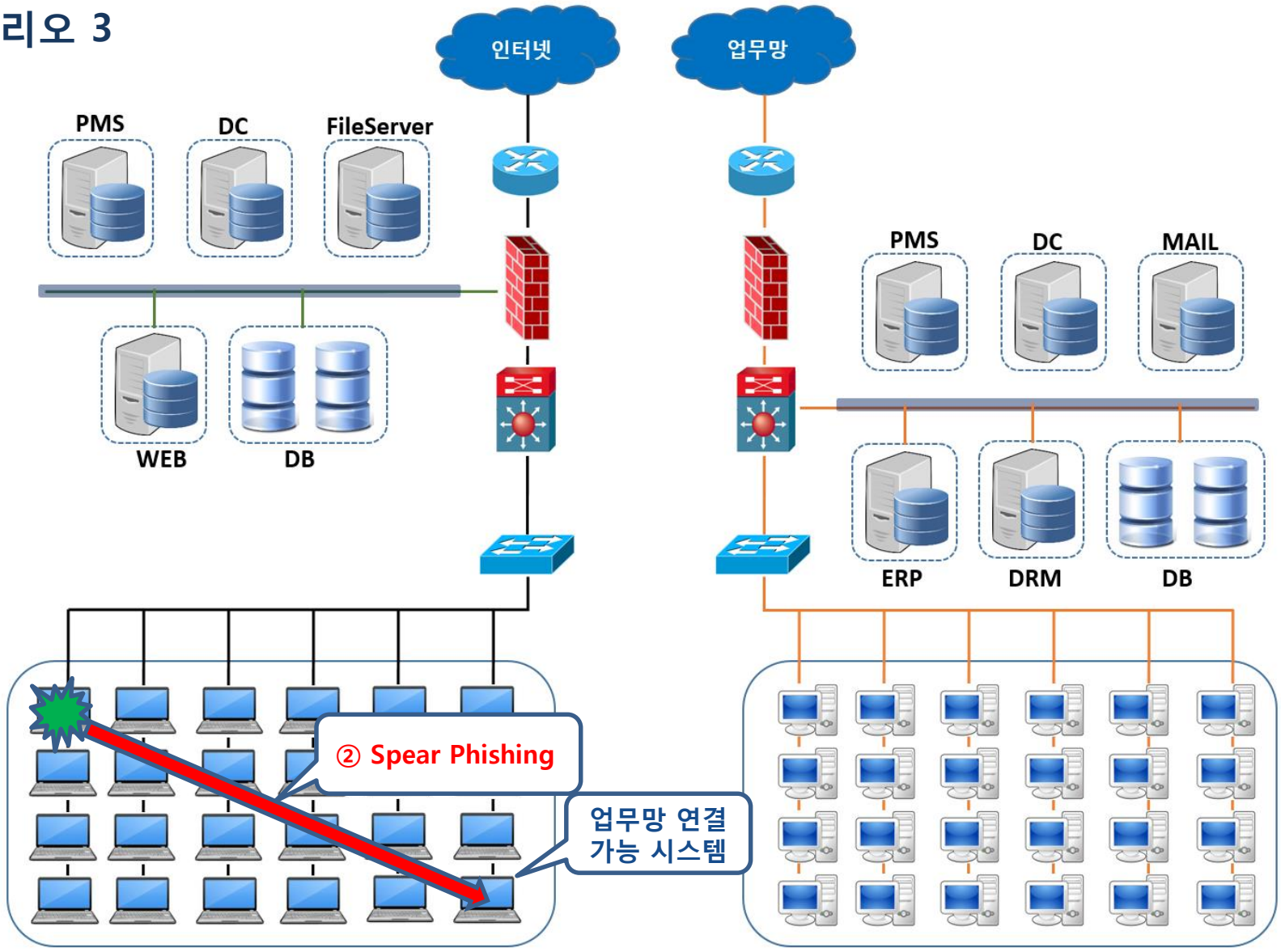
시나리오 3


인터넷
업무망
PMS
DC
FileServer
WEB
DB
PMS
DC
MAIL
ERP
DRM
DB
① Spear Fishing
Drive By Download
Update Vulnerability

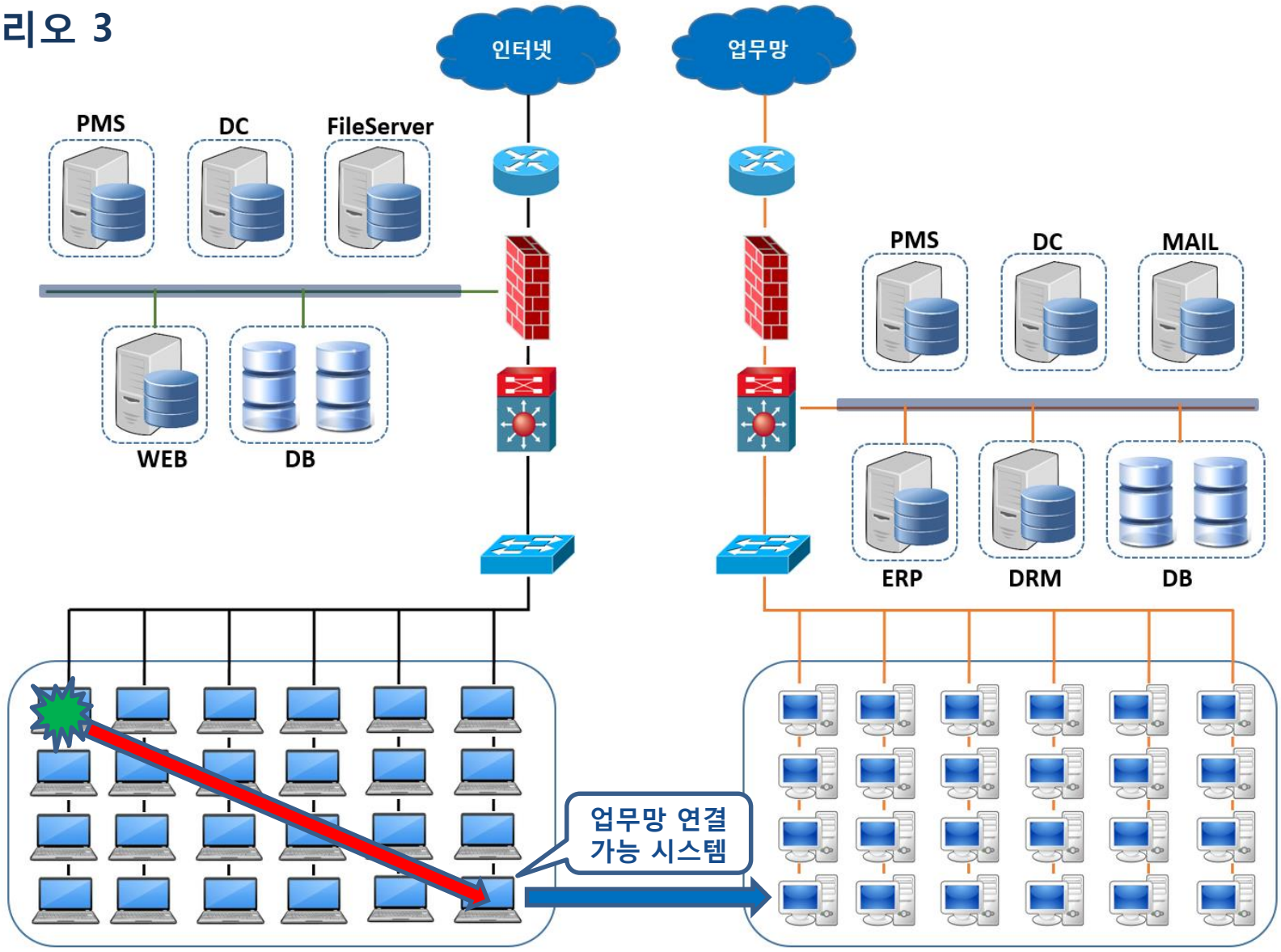
시나리오 3



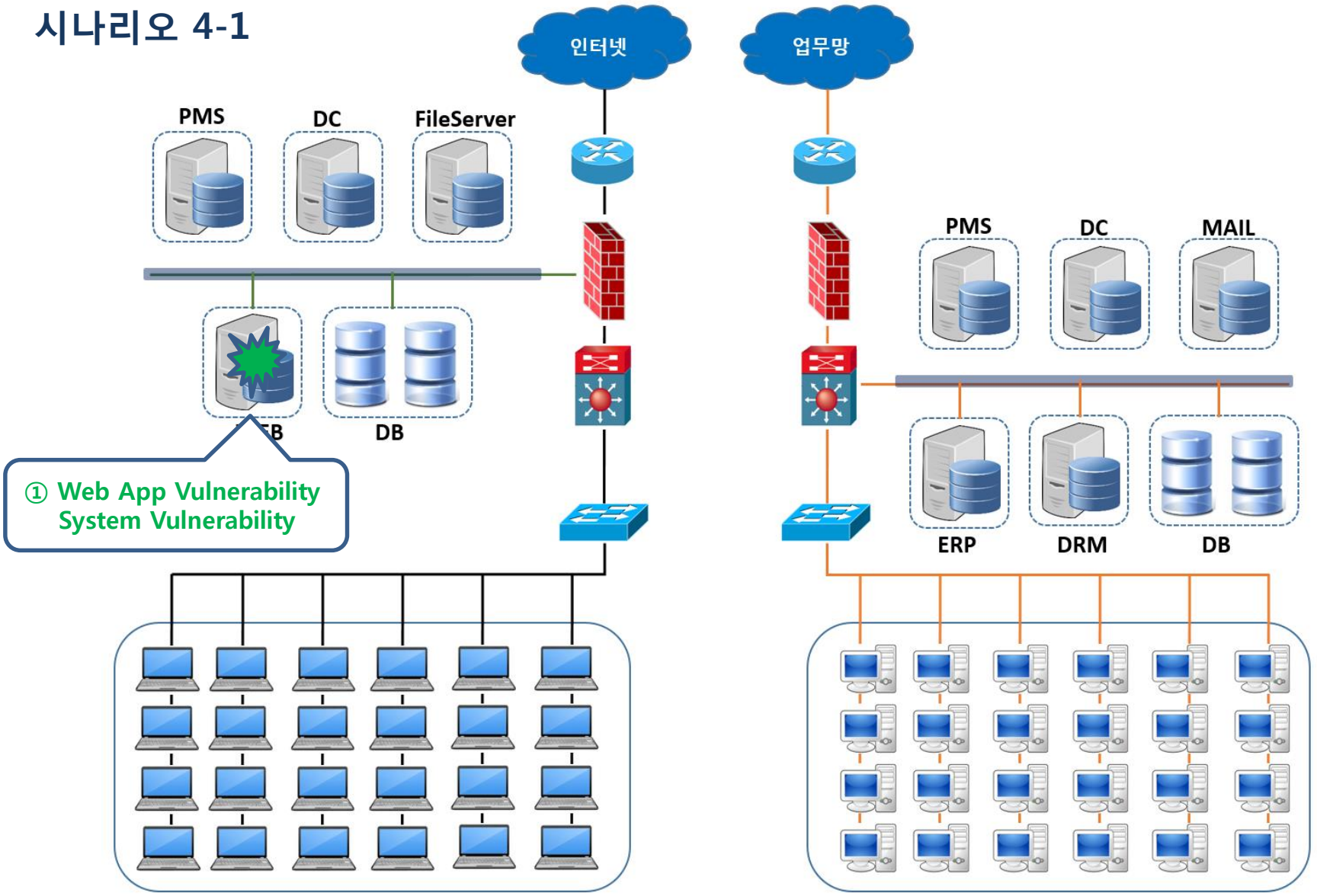
시나리오 3


인터넷
업무망
PMS
DC
FileServer
WEB
DB
PMS
DC
MAIL
ERP
DRM
DB
② Spear Phishing
업무망 연결
가능 시스템

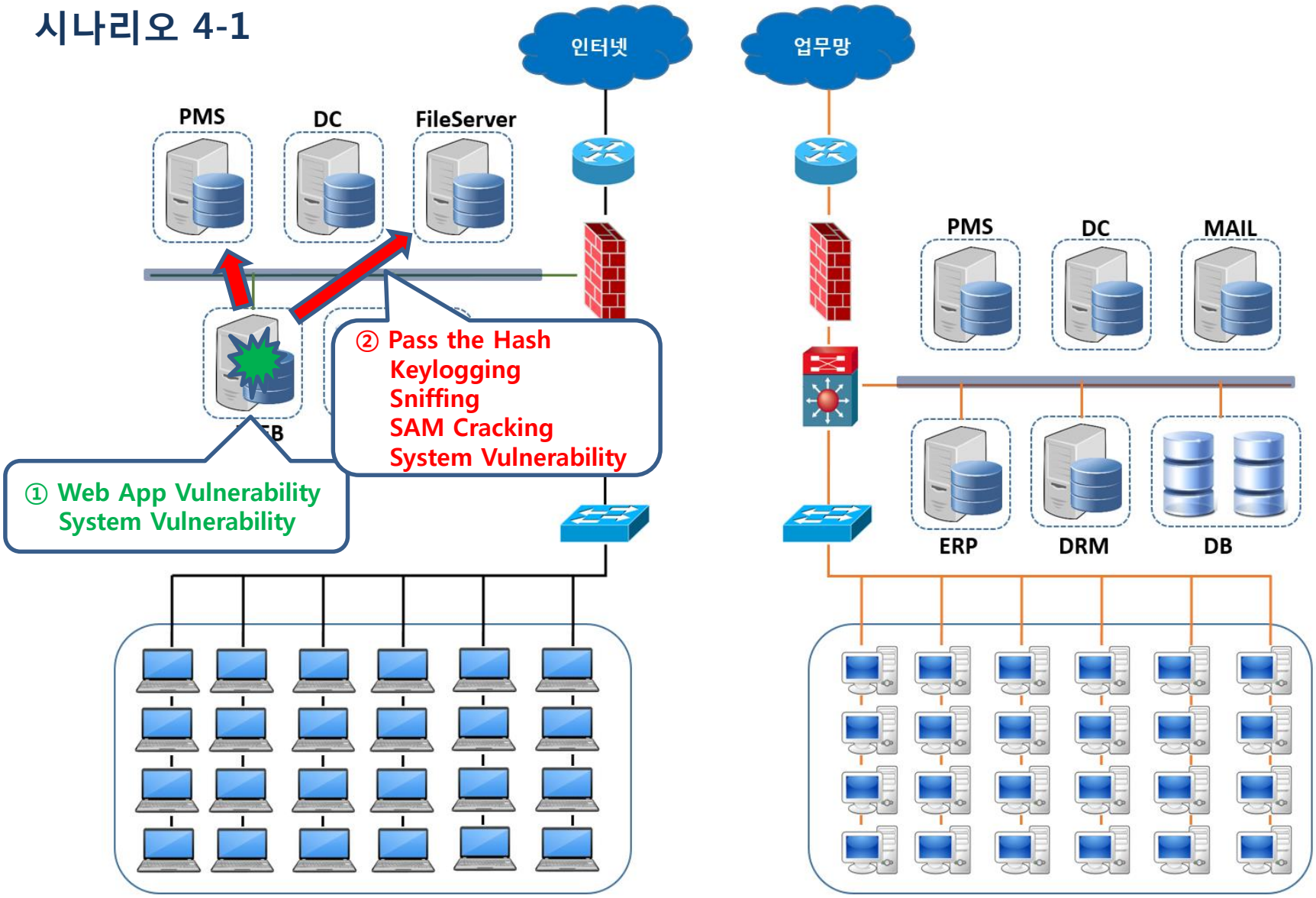
시나리오 3


인터넷
업무망
PMS
DC
FileServer
WEB
DB
PMS
DC
MAIL
ERP
DRM
DB
업무망 연결
가능 시스템

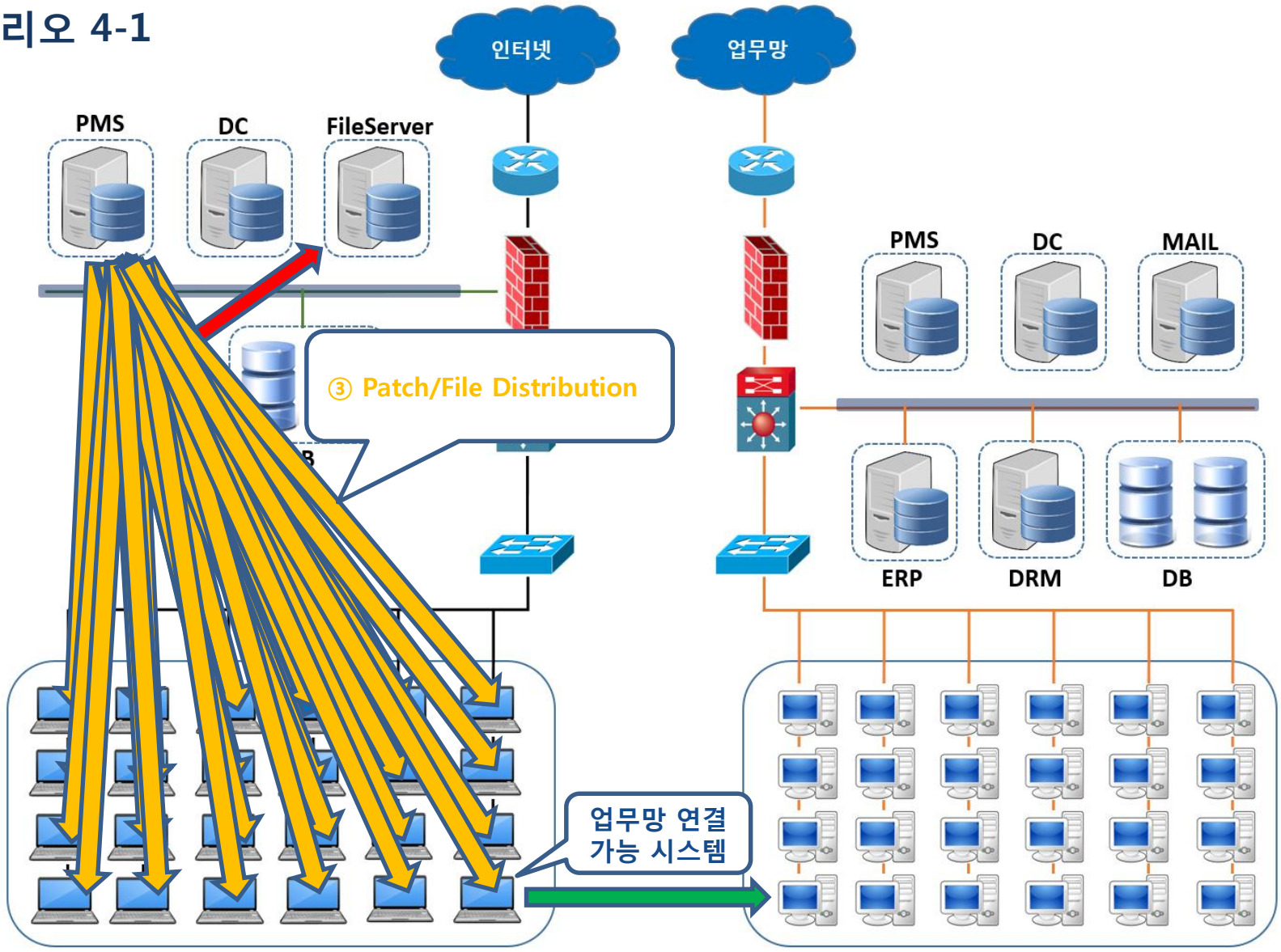
시나리오 4-1


인터넷
업무망
PMS
DC
FileServer
DB
① Web App Vulnerability
System Vulnerability
PMS
DC
MAIL
ERP
DRM
DB

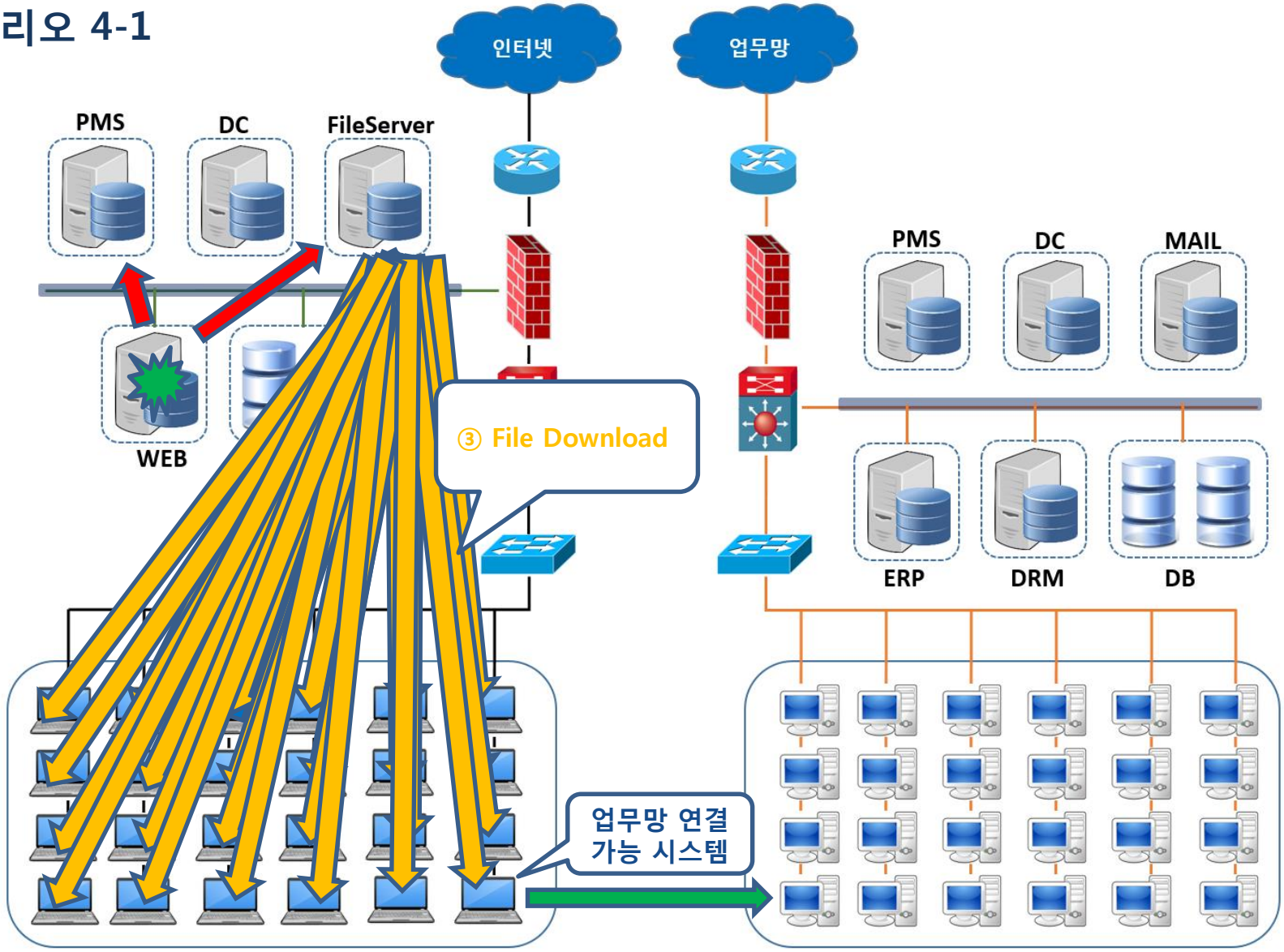
시나리오 4-1


인터넷
업무망
PMS
DC
FileServer
PMS
DC
MAIL
ERP
DRM
DB
② Pass the Hash
Keylogging
Sniffing
SAM Cracking
System Vulnerability
① Web App Vulnerability
System Vulnerability

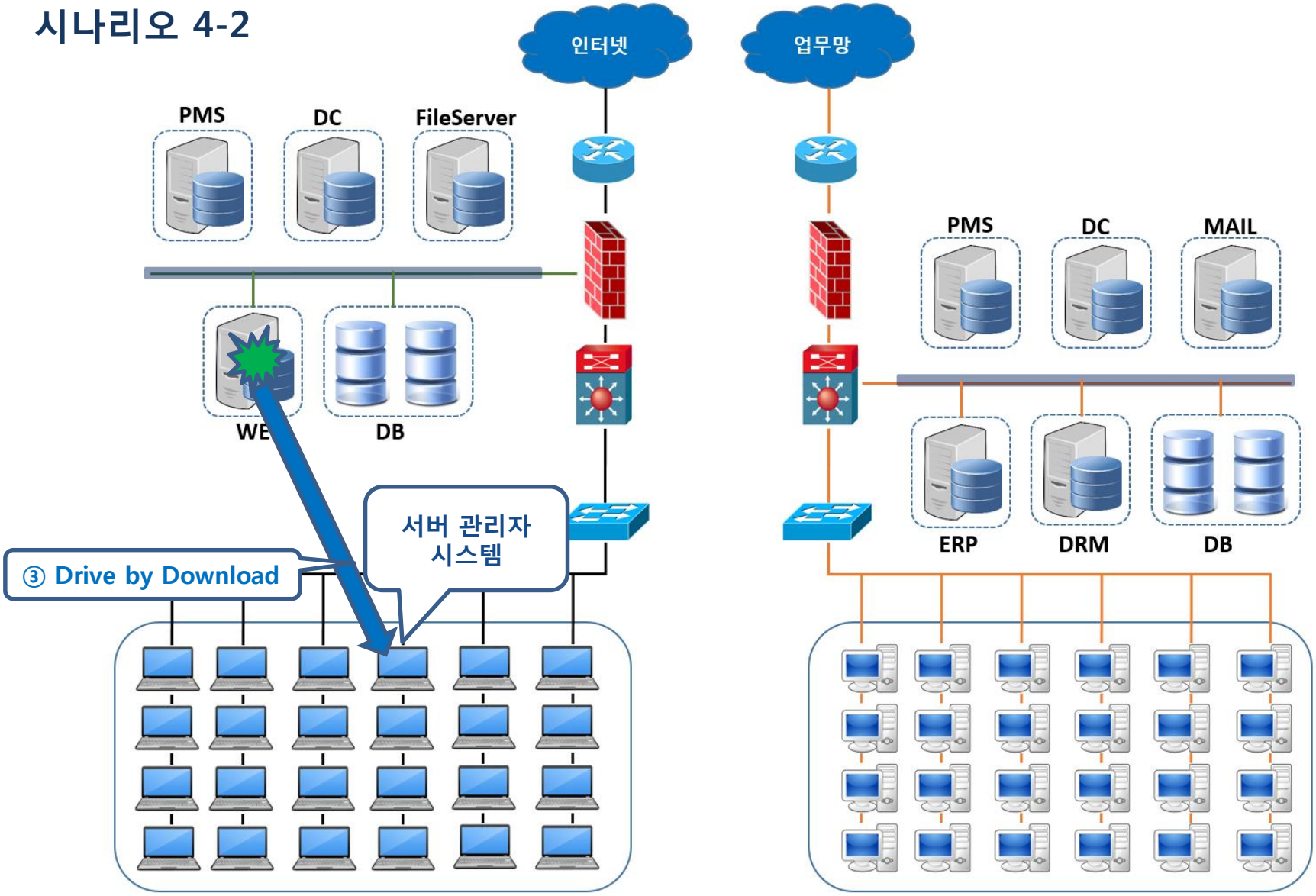
시나리오 4-1


인터넷
업무망
PMS
DC
FileServer
③ Patch/File Distribution
PMS
DC
MAIL
ERP
DRM
DB
업무망 연결
가능 시스템

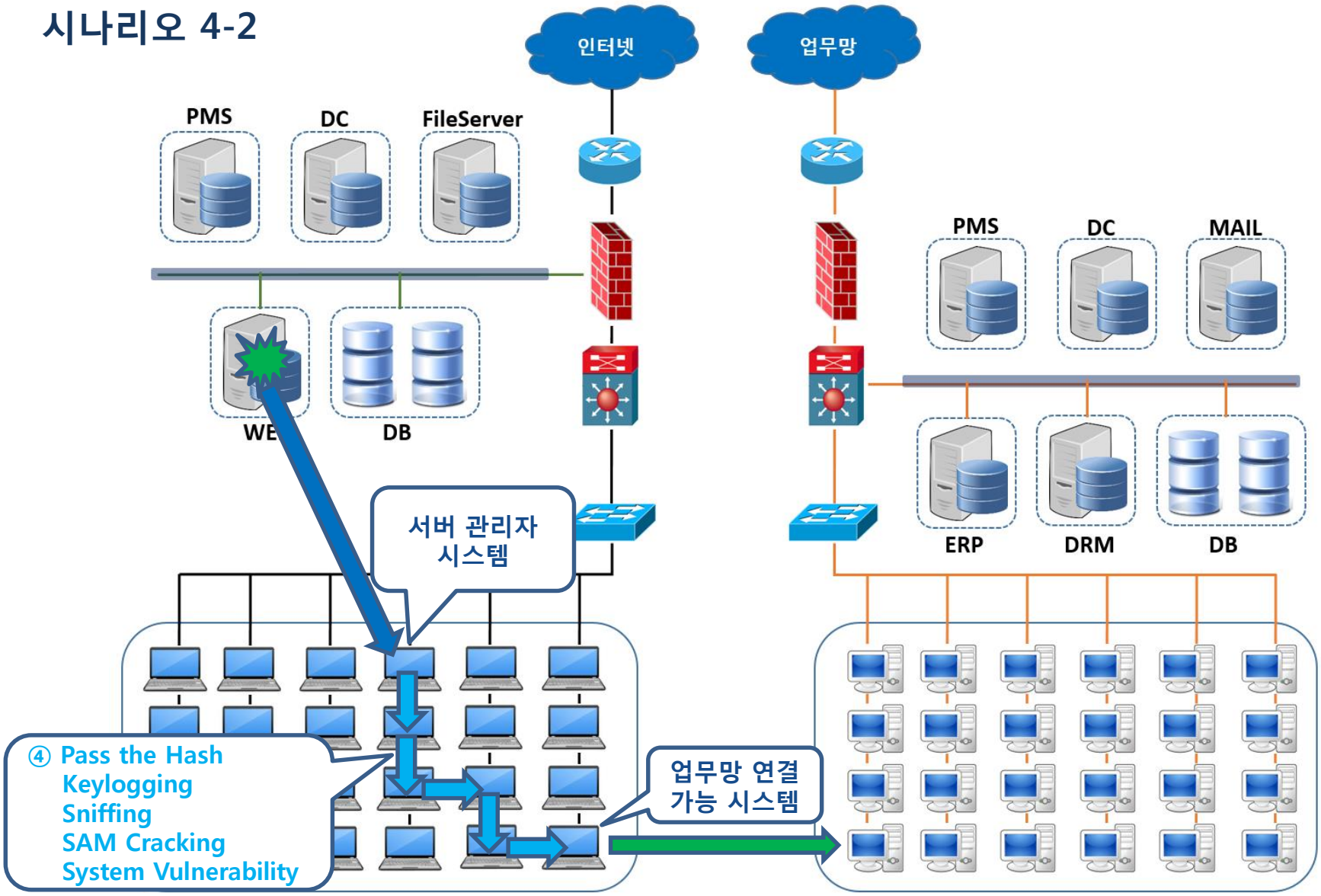
시나리오 4-1


인터넷
업무망
PMS
DC
FileServer
WEB
③ File Download
PMS
DC
MAIL
ERP
DRM
DB
업무망 연결
가능 시스템

시나리오 4-2


인터넷
업무망
PMS
DC
FileServer
WE
DB
PMS
DC
MAIL
ERP
DRM
DB
서버 관리자
시스템
③ Drive by Download

시나리오 4-2


인터넷
업무망
PMS
DC
FileServer
WE
DB
PMS
DC
MAIL
ERP
DRM
DB
서버 관리자
시스템
④ Pass the Hash
Keylogging
Sniffing
SAM Cracking
System Vulnerability
업무망 연결
가능 시스템

Lateral Movement 기법

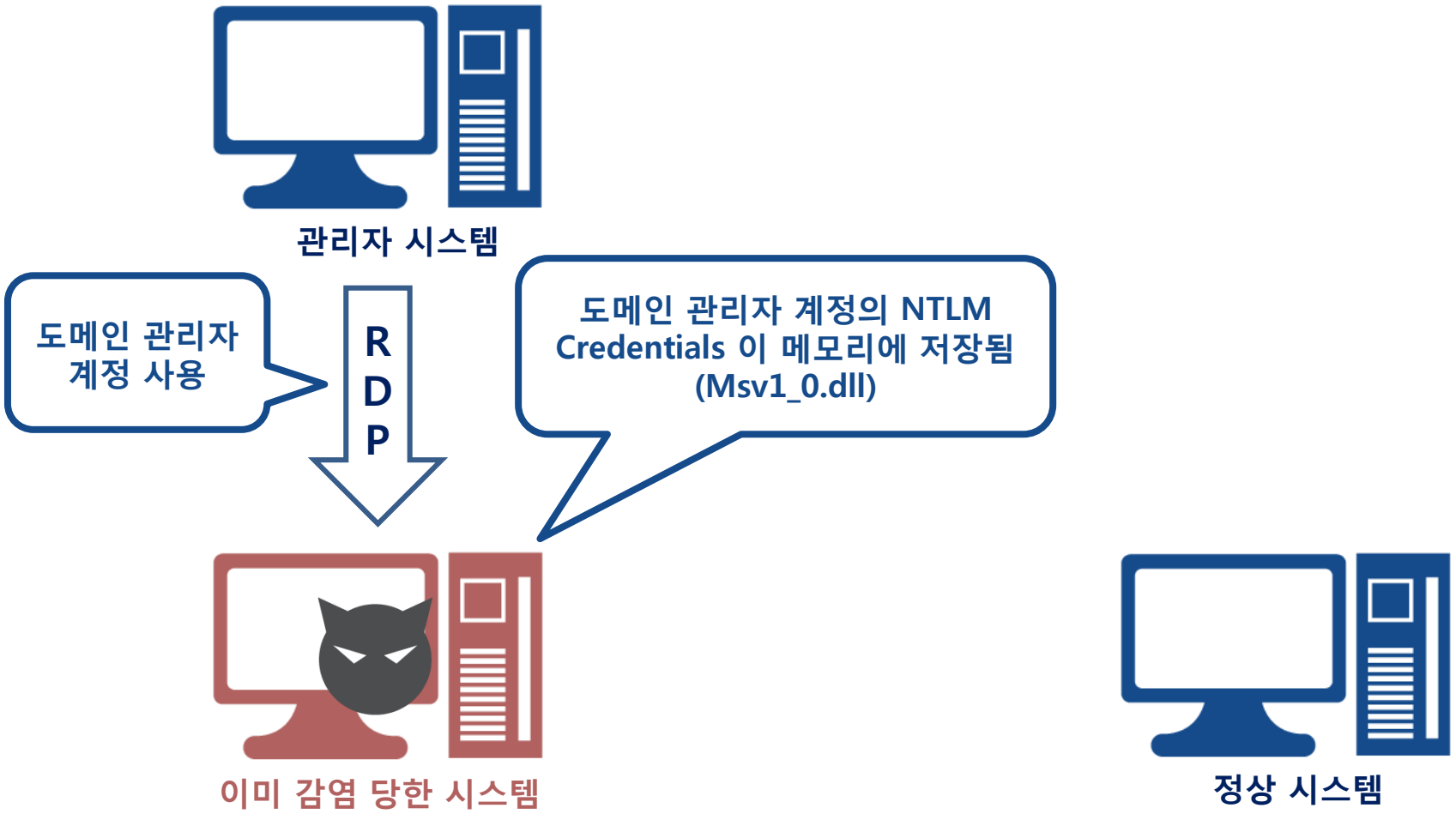
- Keylogging
- Sniffing Passwords(ARP Hijack/MIM)
- Dump Passwords(LSA Secret, Protected Storage2 & Credential Manger)
- SAM Cracking(Brute Force, Rainbow Crack)
- Pass the Hash
- Pass the Pass
- Patch/File Server
- Spear Phishing
- System Vulnerability
- …

Lateral Movement 기법

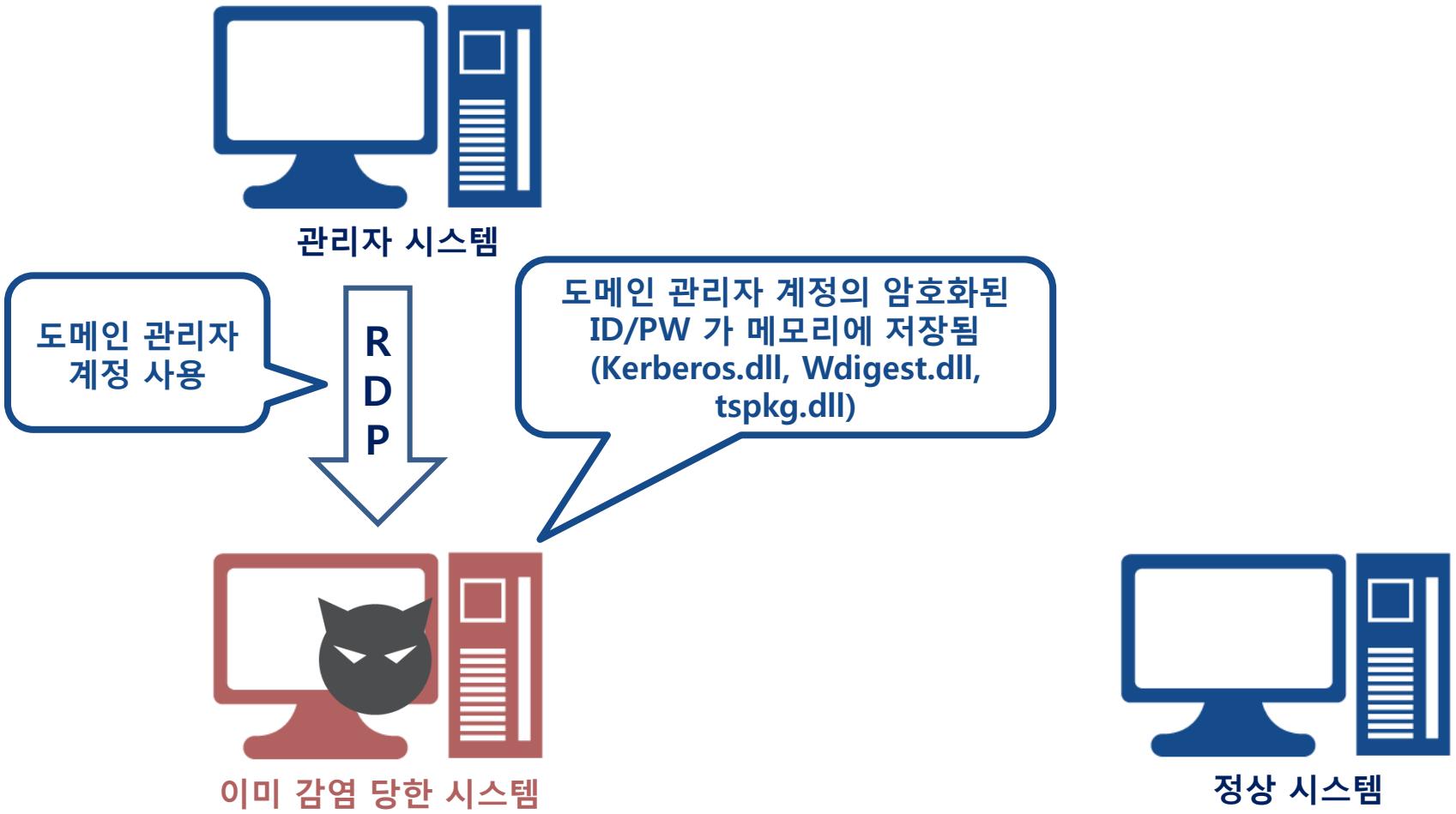
- Keylogging
- Sniffing Passwords(ARP Hijack/MIM)
- Dump Passwords(LSA Secret, Protected Storage2 & Credential Manger)
- SAM Cracking(Brute Force, Rainbow Crack)
- Pass the Hash
- Pass the Pass
- Patch/File Server
- Spear Phishing
- System Vulnerability
- …

Active Directory 환경에서의 Pass the Hash 공격

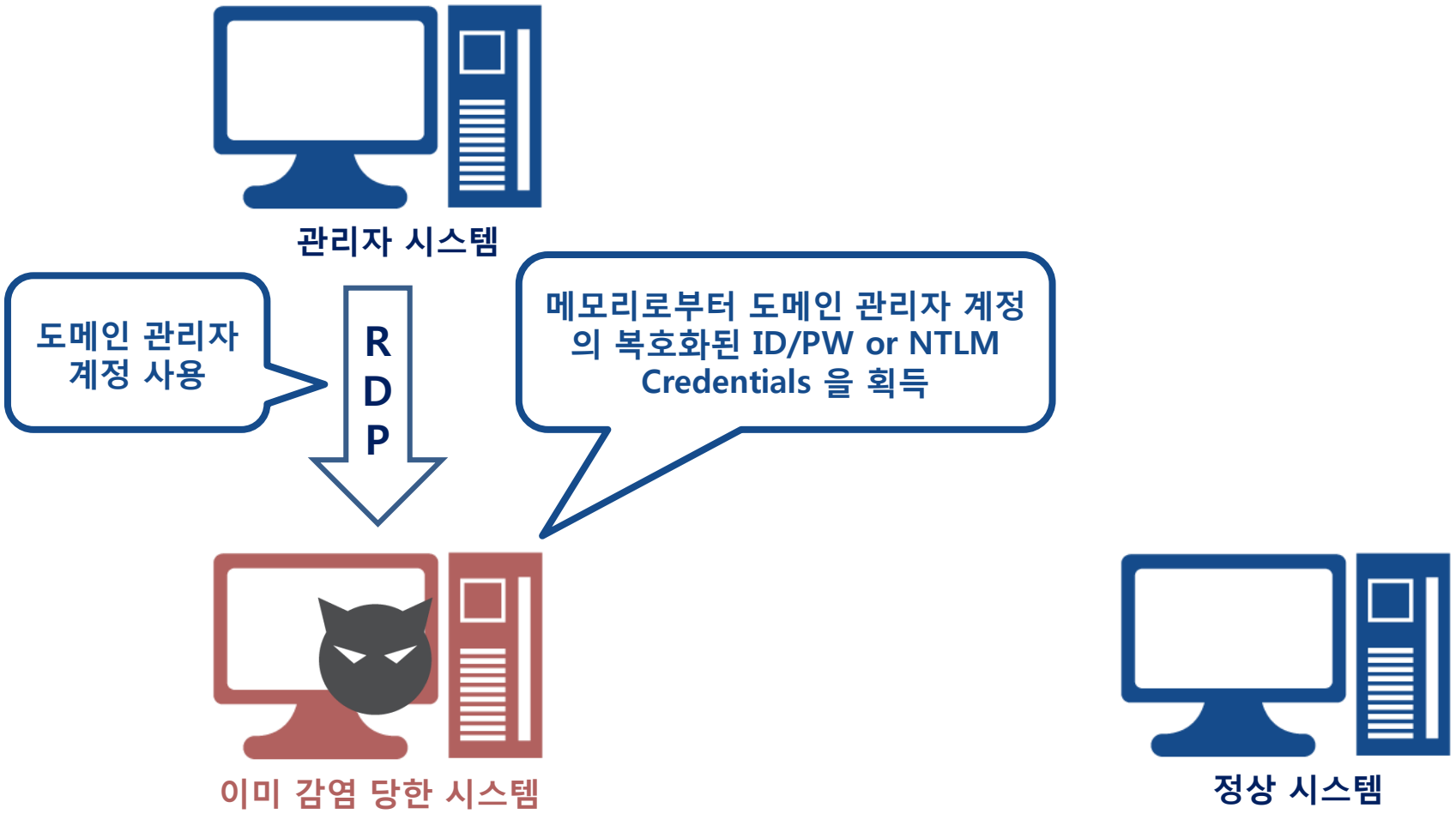
Active Directory 환경에서의 Pass the Hash 공격



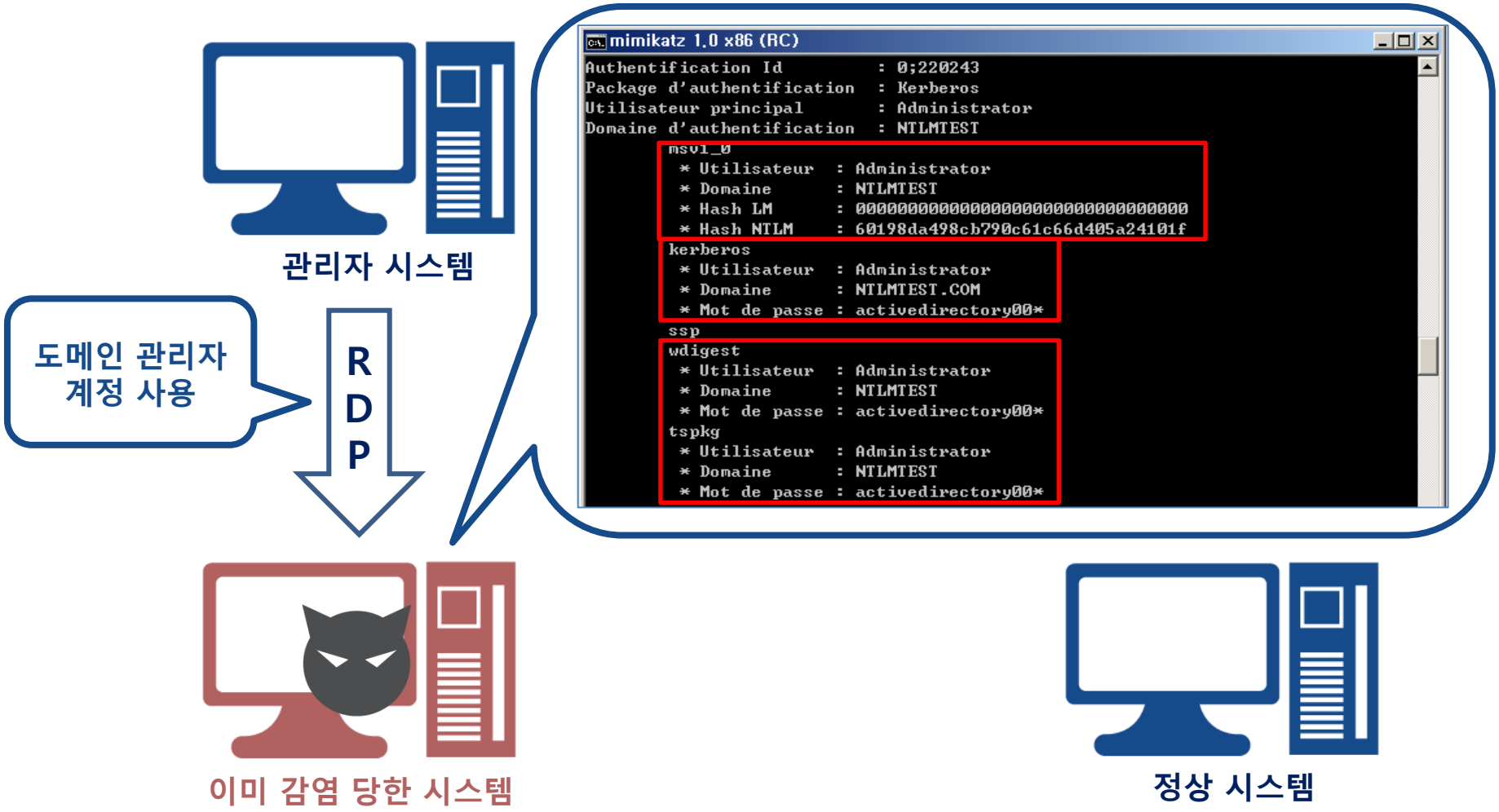
Active Directory 환경에서의 Pass the Hash 공격



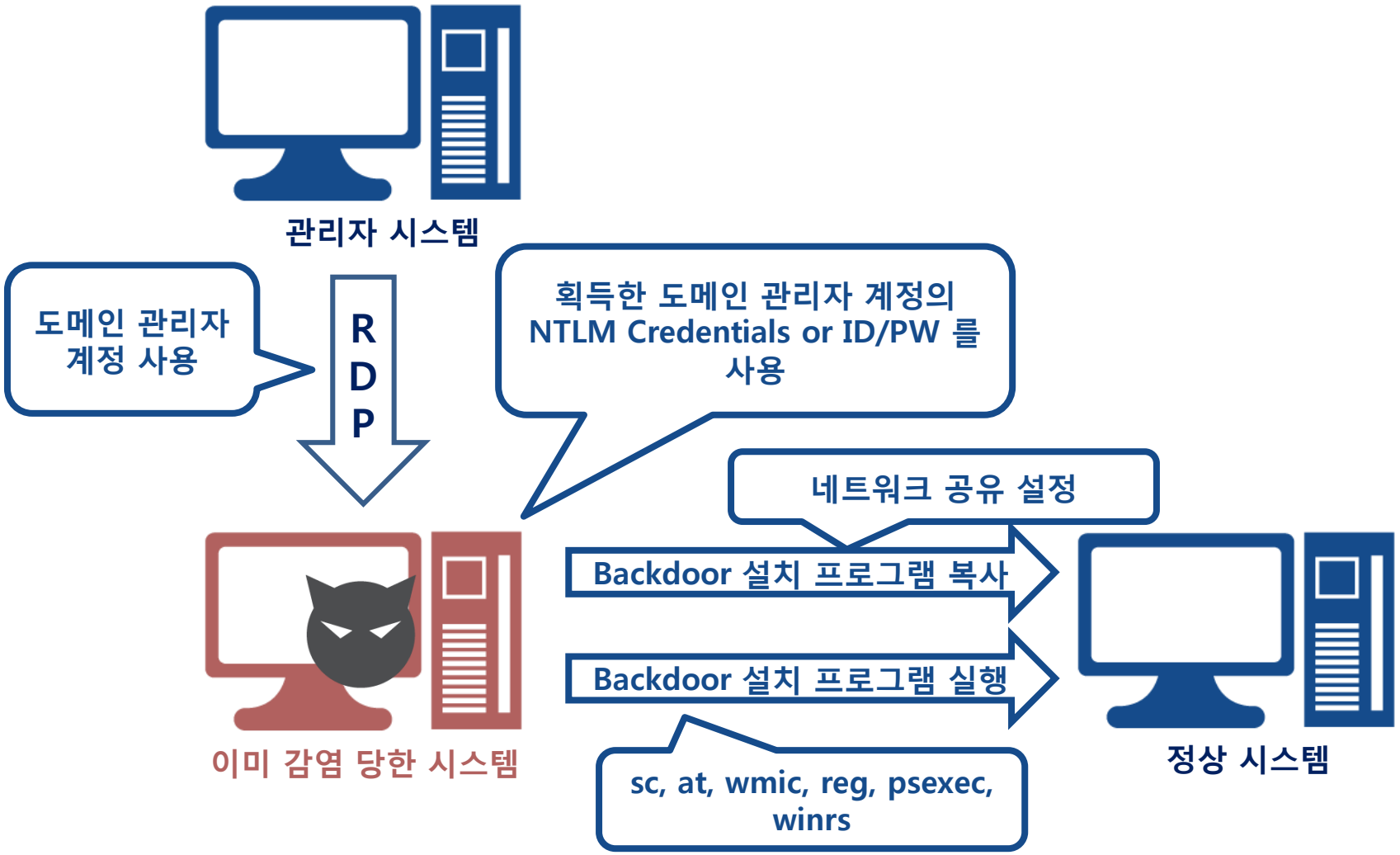
Active Directory 환경에서의 Pass the Hash 공격



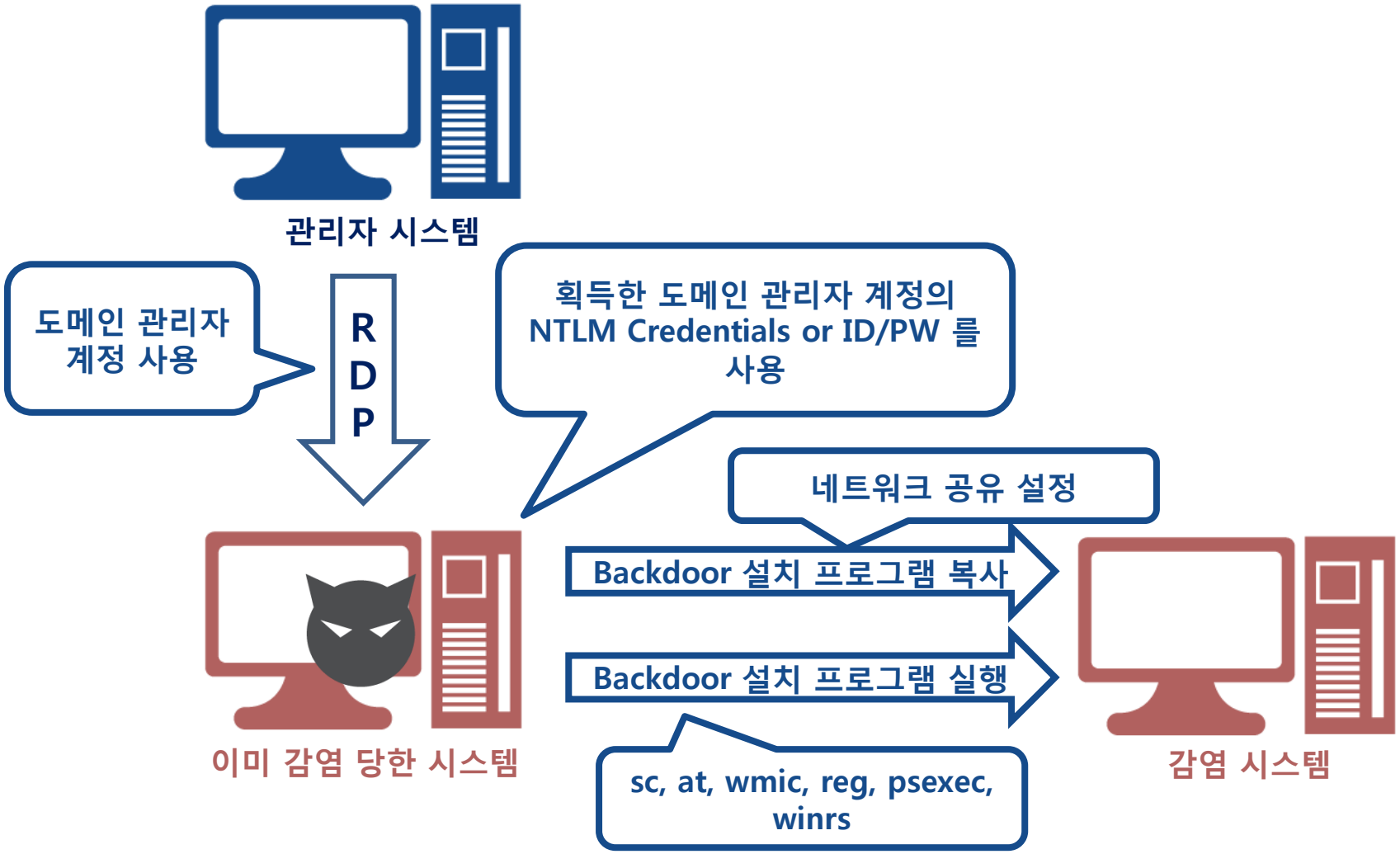
Active Directory 환경에서의 Pass the Hash 공격



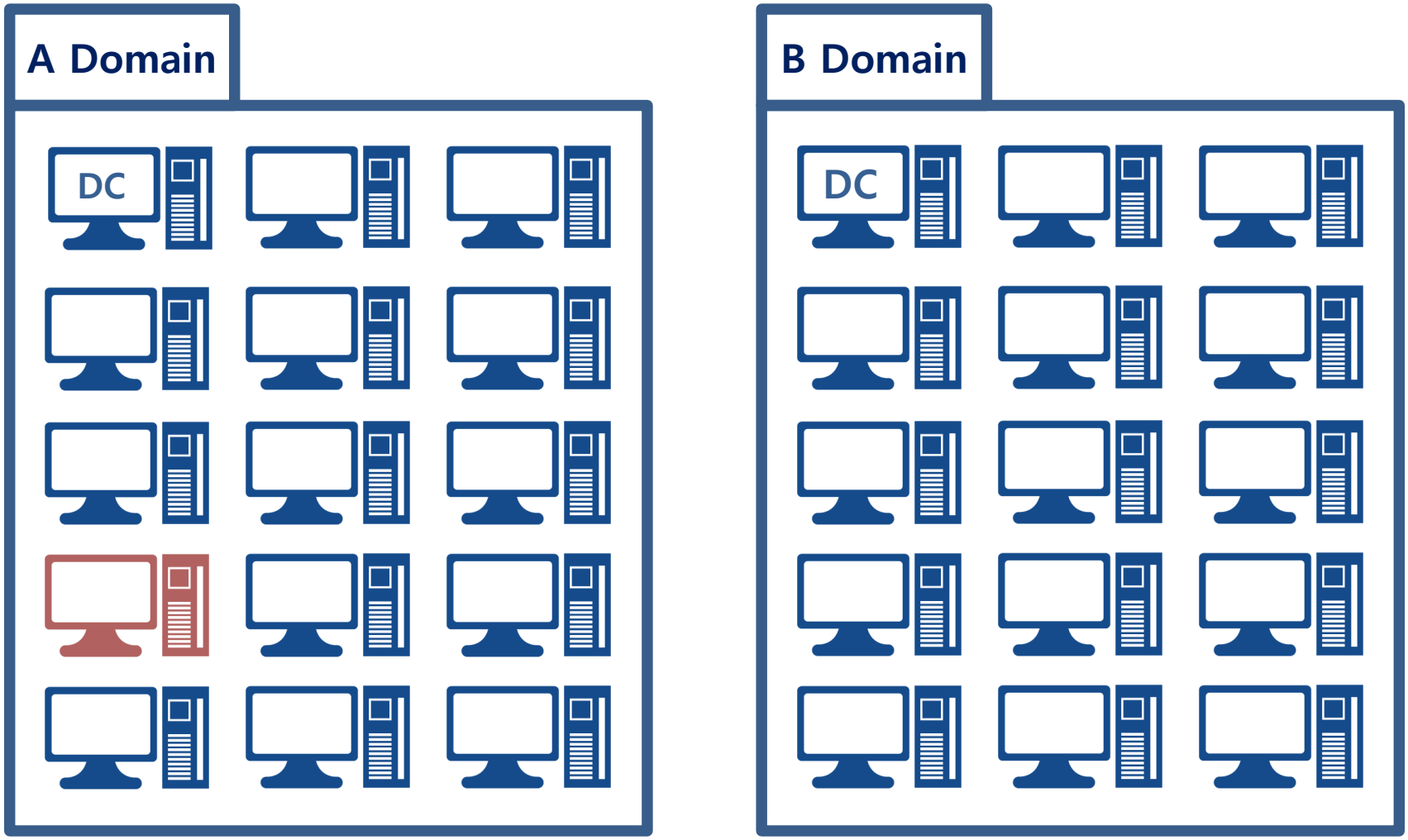
Active Directory 환경에서의 Pass the Hash 공격



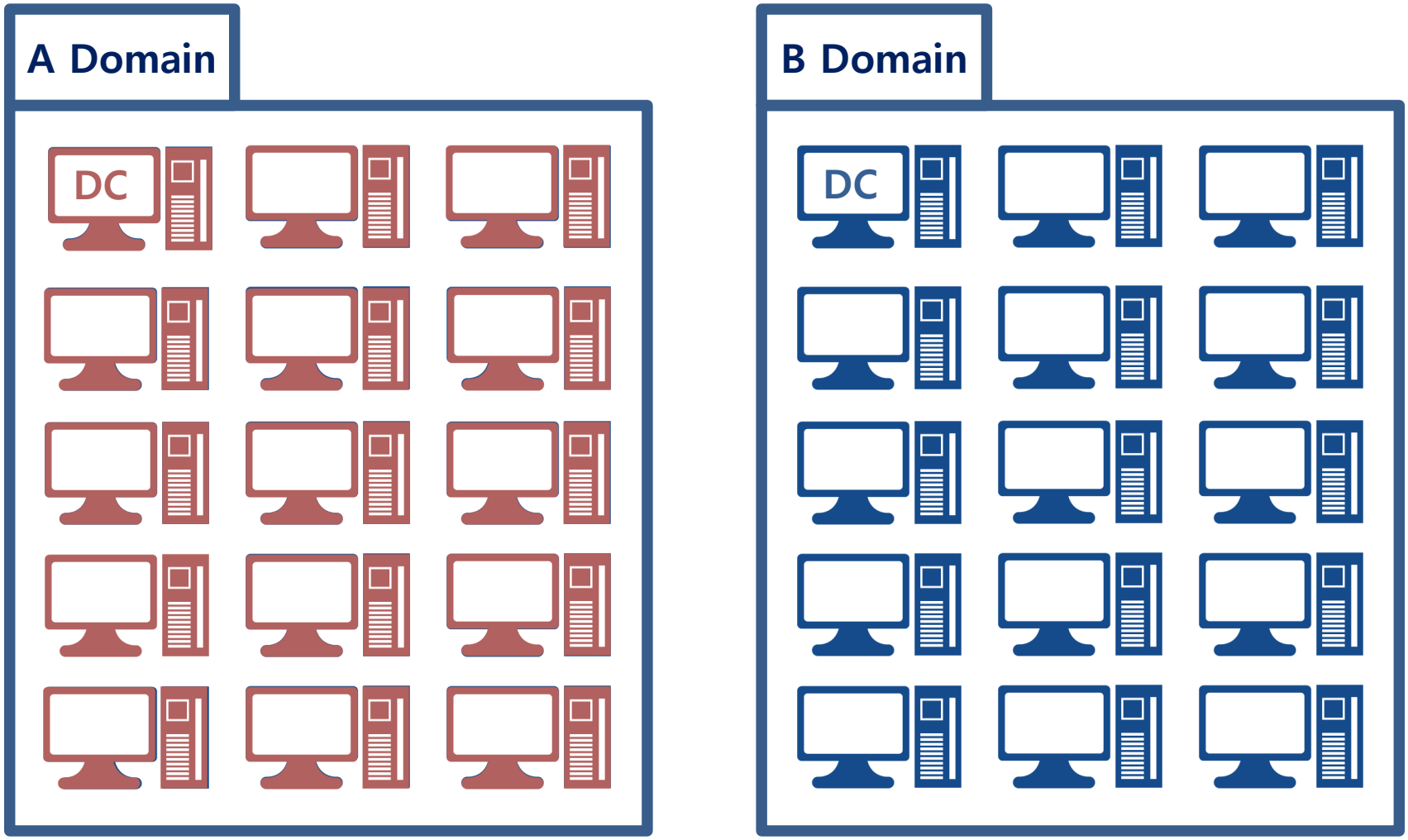
Active Directory 환경에서의 Pass the Hash 공격



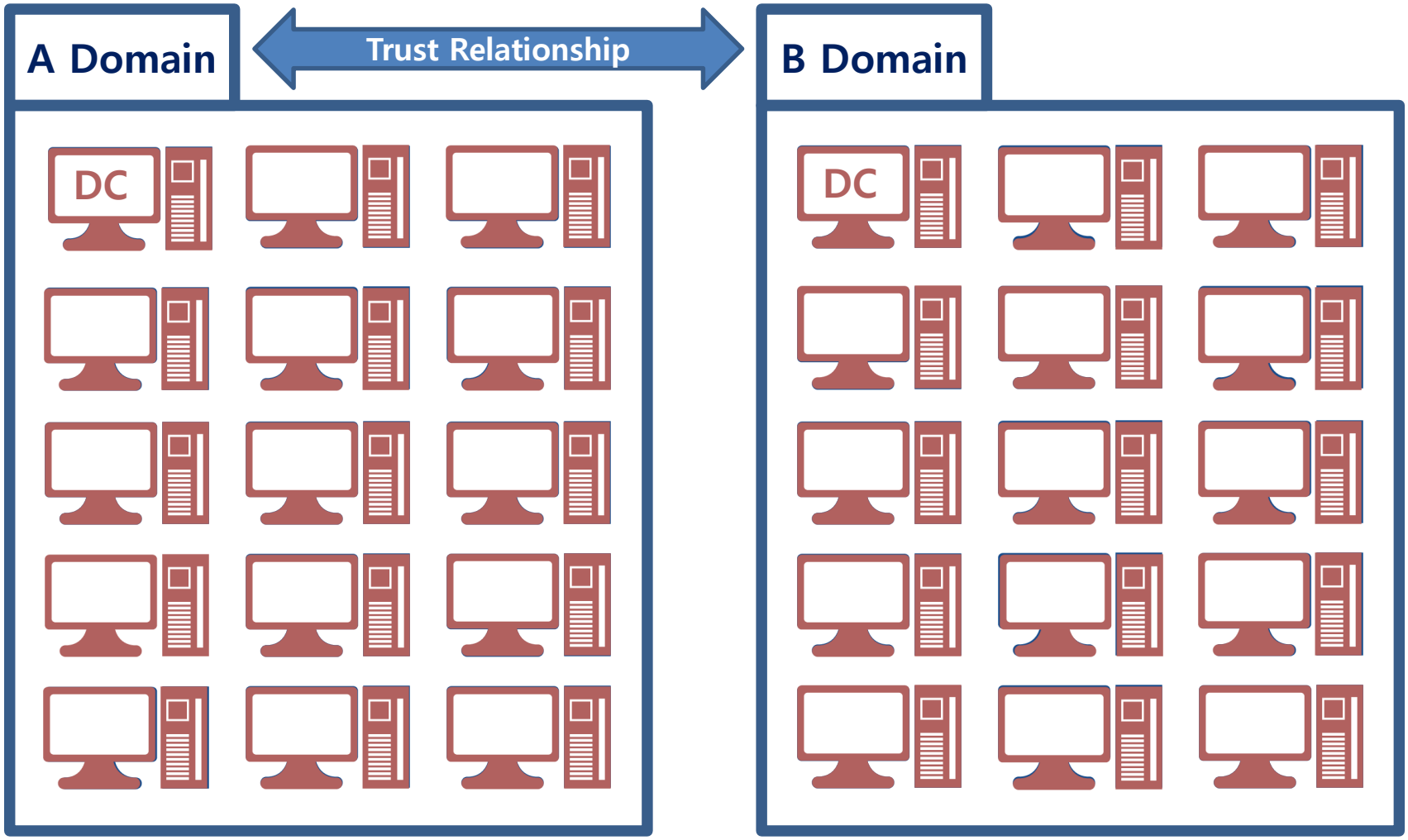
Active Directory 환경에서 Pass the Hash 공격이 위험한 이유



Active Directory 환경에서 Pass the Hash 공격이 위험한 이유



Active Directory 환경에서 Pass the Hash 공격이 위험한 이유



In Mind of Administrator...

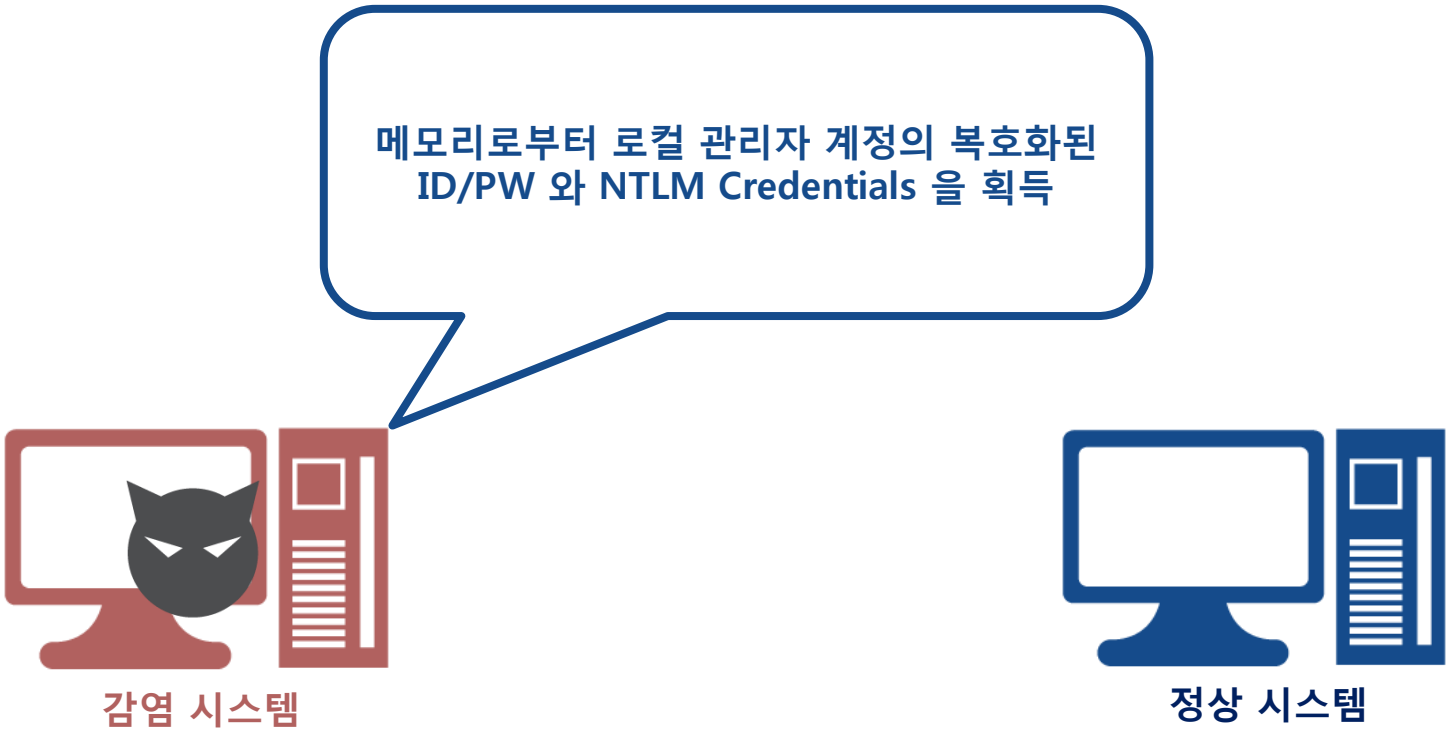
Non-Active Directory 환경에서의 Pass the Hash 공격

모든 시스템이 동일한
로컬 관리자 계정을 사용

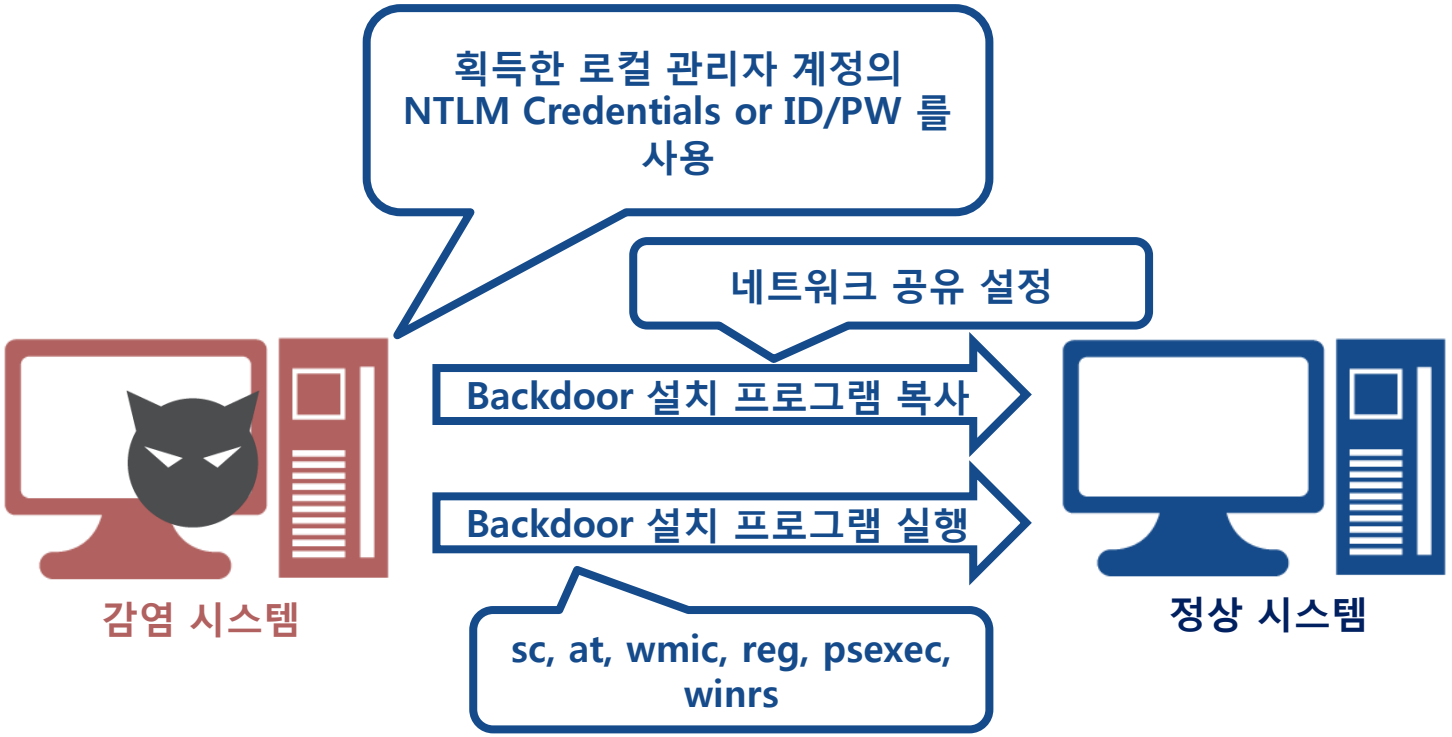
감염 시스템

정상 시스템

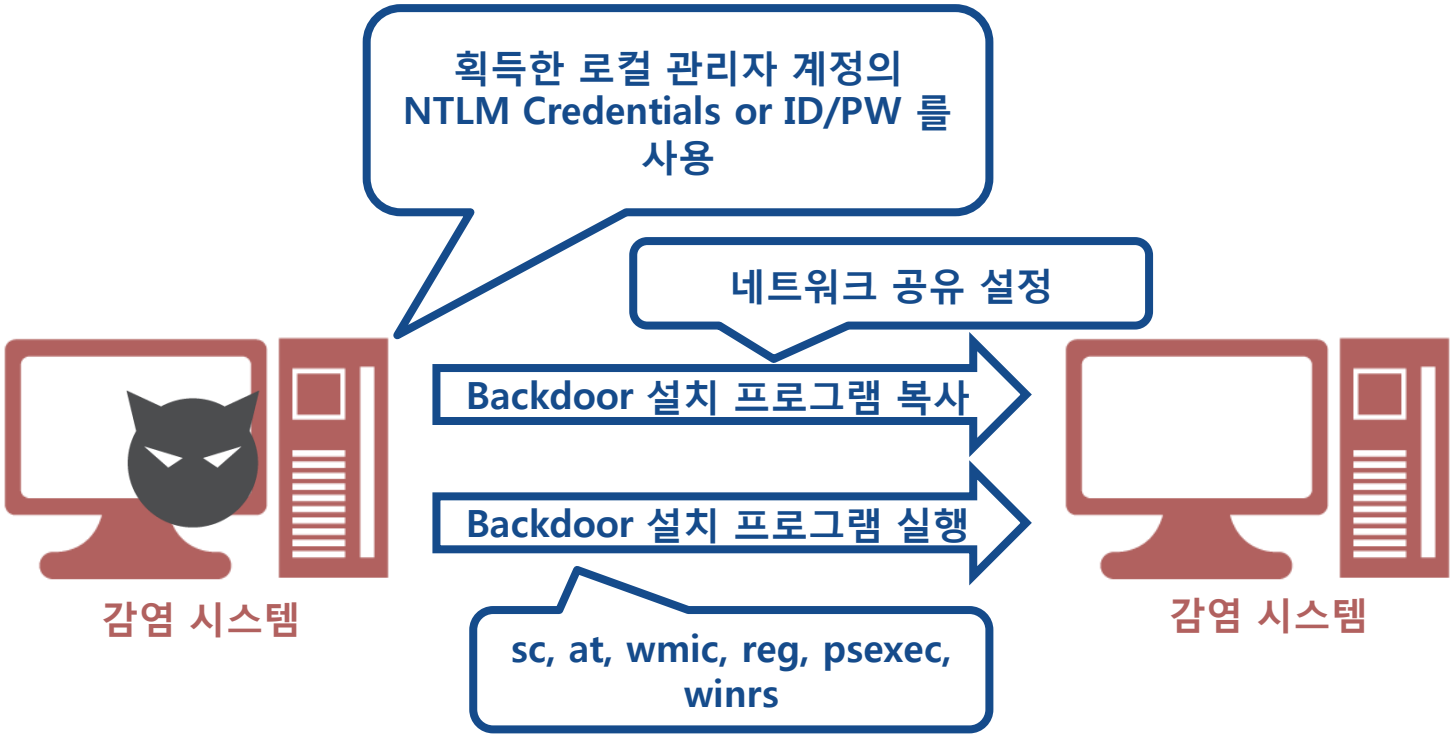
Non-Active Directory 환경에서의 Pass the Hash 공격



Non-Active Directory 환경에서의 Pass the Hash 공격



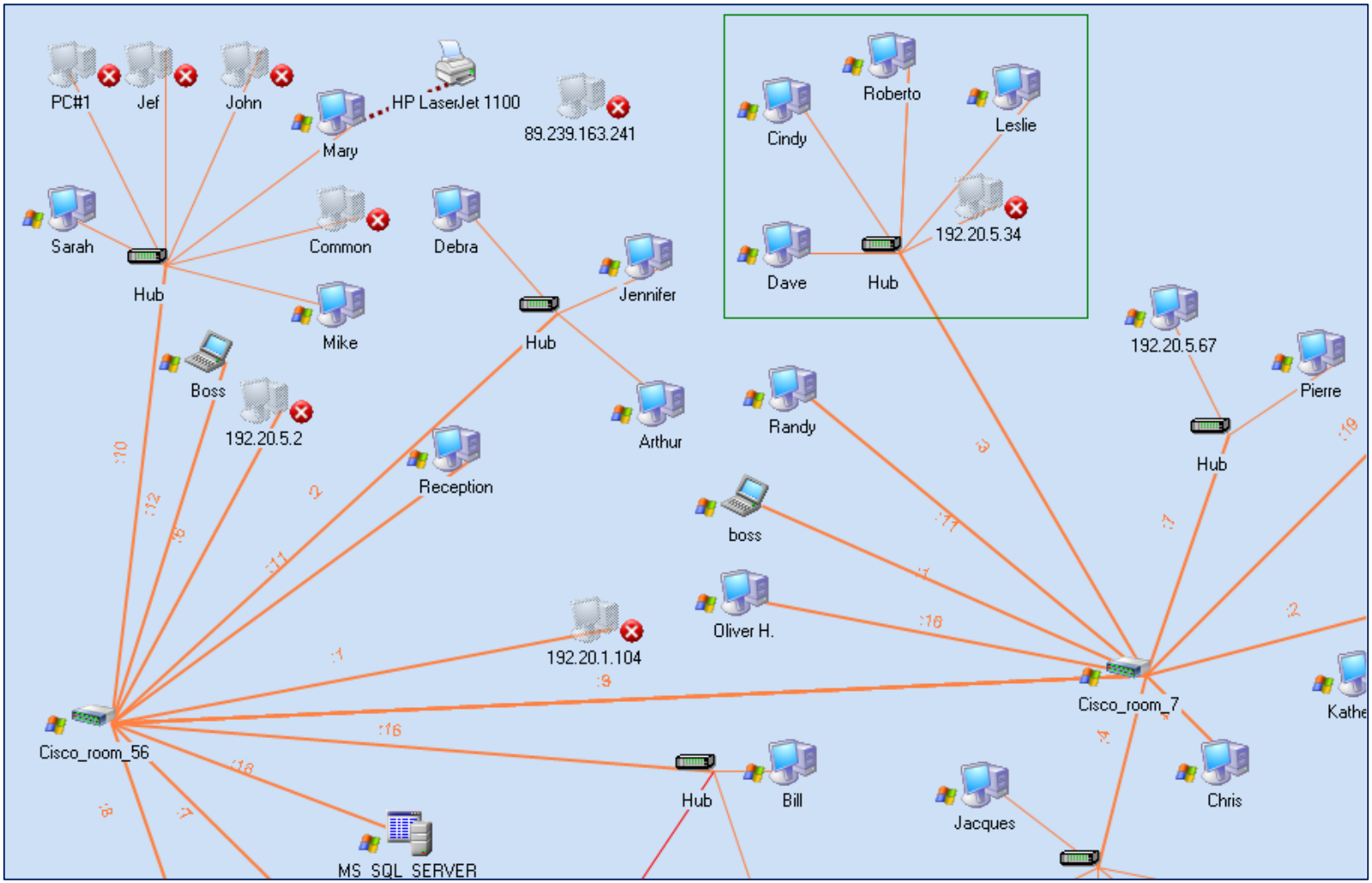
Non-Active Directory 환경에서의 Pass the Hash 공격



최초 유입 경로 분석

가장 먼저 수행해야 할 작업은??

- 네트워크 구성 파악



네트워크 구성 파악을 안하고 시작하면...

분석 시작 시스템 지정~!!

- 이상 징후가 발견된 시스템부터…
  - 악성코드
  - 공격 흔적
  - 비정상적인 시스템 접근
  - …

- 전혀 알 수 없을 경우…
  - 유출된 정보를 저장하고 있는 시스템
  - 위 시스템에 접근할 수 있는 시스템
  - 보안 솔루션 로그의 이상 징후
  - …

시스템 분석 유형

- **상세 분석**
  - 아무 단서가 없는 상황에서 시스템 전체를 분석
  - 의심스러운 악성코드/흔적을 찾아 공격 시간대를 알아내는 것이 목적
  - 타임라인 분석 기법 사용
  - Lateral Movement 기법 파악, 유입 경로 파악
  - 비할당 영역 분석을 위해 디스크 이미징이 필요함
  - 추후 분석에 사용할 수 있도록 최대한 많은 정보를 모아야 함

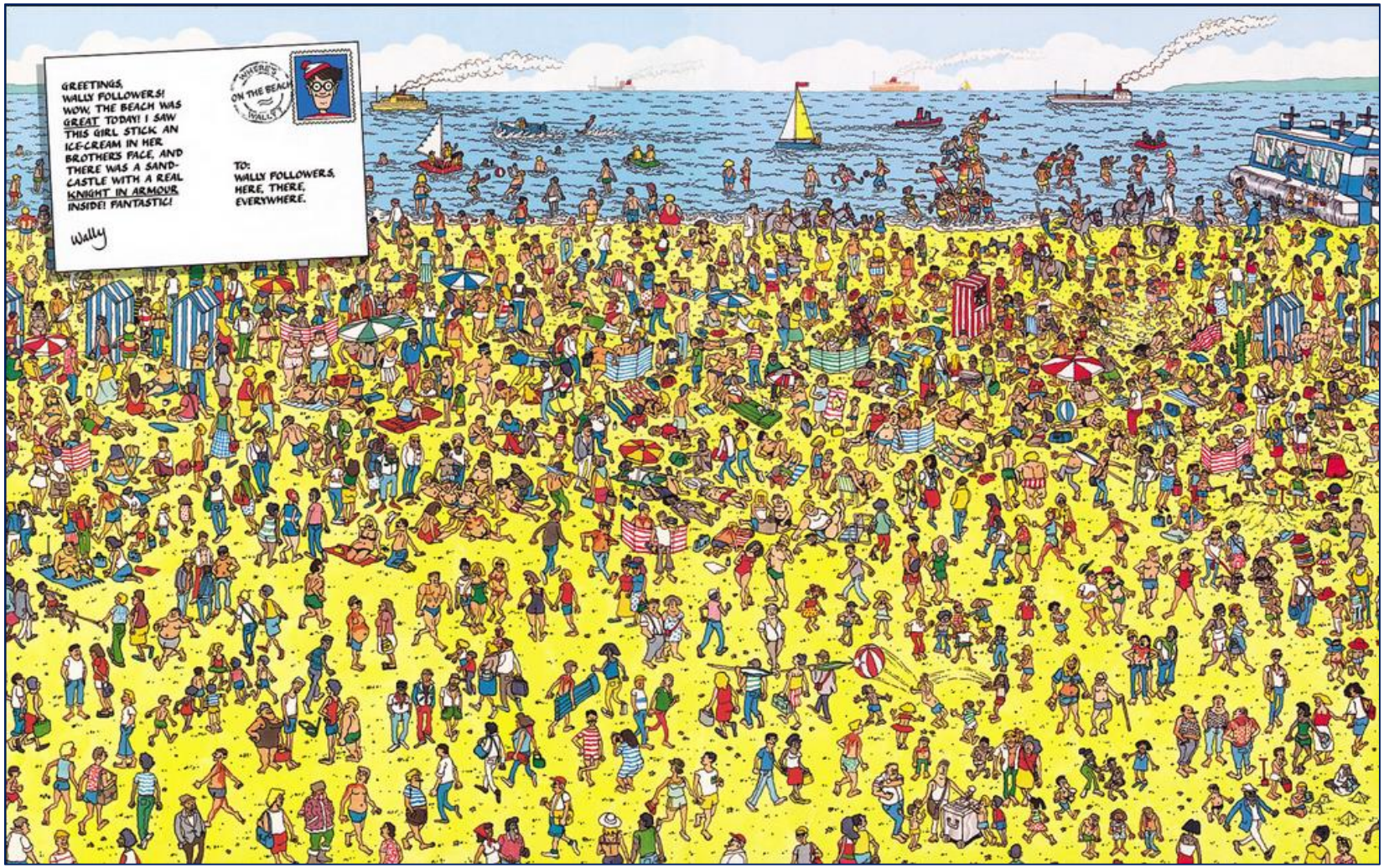
- **포인트 분석**
  - 이미 공격 시간대와 악성 코드 및 여러 정보를 확보한 상태의 분석
  - 특정 시간대의 특정 아티팩트만을 분석
  - 디스크 이미징이 필요 없음
  - 스크립트 혹은 수집 Agent 를 통해 주요 아티펙트들만 수집

시스템 상세 분석

- **STEP 1. 시스템 내 악성코드 or 공격 흔적 찾기**
  - 의심스러운 파일 실행 흔적
  - 의심스러운 Reloading Point
  - 파일 시스템 내 숨겨진 악성코드
  - 의심스러운 다운로드 흔적
  - …

시스템 상세 분석

- **STEP 1. 시스템 내 악성코드 or 공격 흔적 찾기**



시스템 상세 분석

- **STEP 2. 타임라인 분석**
  - 타임라인 : 여러 아티팩트를 시간 정보를 기준으로 하나로 통합

시스템 상세 분석

- **STEP 2. 타임라인 분석**
  - 타임라인 : 여러 아티팩트를 시간 정보를 기준으로 하나로 통합

date	time	MACB	sourcetype	type	short
39649	0.06115	MACB	Email PST	Email Read	Message 114: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MACB	XP Prefetch	Last run	EXCEL.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:27:40	.AC.	NTFS $MFT	$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCEL.EXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launch	UEME_RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCEL.EXE
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:043	MACB	NTFS $MFT	$SI [MACB] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/Desktop.LNK
7/20/2008	1:28:03	MACB	FileExts key	Extension Change	File extension .xls opened by EXCEL.EXE
7/20/2008	1:28:03	MACB	NTFS $MFT	$SI [MACB] time	C:/windows/system32/winsvchost.exe
7/20/2008	1:28:03		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7/20/2008	1:27:40		Memory Process	Process Started	winsvchost.exe|1556|1032||0x02476768
7/20/2008	1:27:40		Memory Socket	Socket Opened	4|134.182.111.82:443|Protocol: 6 (TCP)|0x8162de98|||
7/20/2008	1:27:40		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:03	.A..	Shortcut LNK	Access	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:04	MAC.	NTFS $MFT	$SI [MAC.] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist01200807202008
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist01200807202008
7/20/2008	1:28:04	MACB	RecentDocs key	File opened	Recently opened file of extension: .xls - value: m57biz.xls

시스템 상세 분석

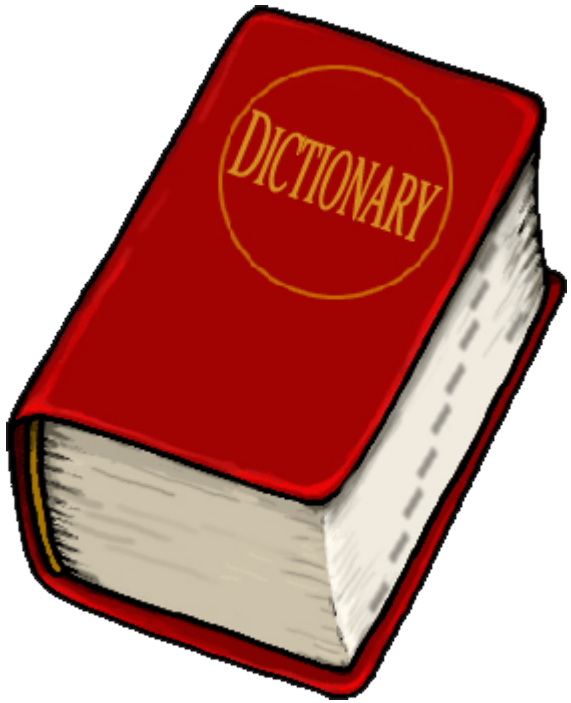
- STEP 2. 타임라인 분석

타임라인만 보면 되는거 아닌가??

시스템 상세 분석

- STEP 2. 타임라인 분석

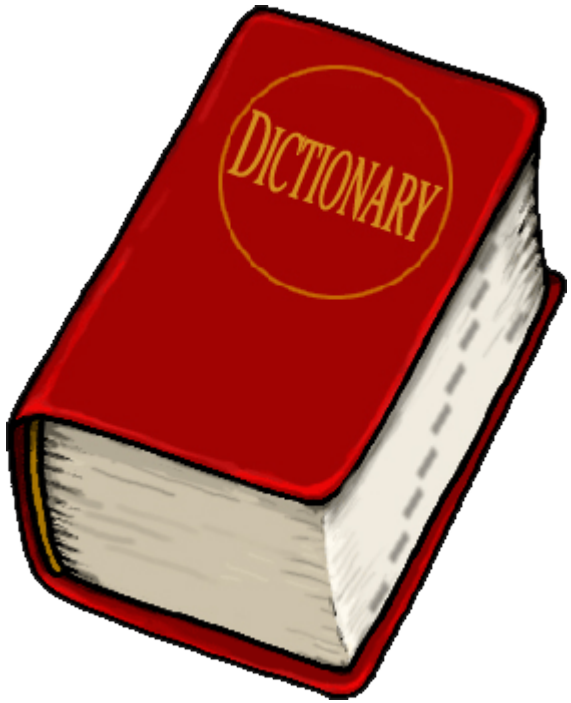
타임라인 분석 = 사전 찾기



시스템 상세 분석

- STEP 2. 타임라인 분석

의심스러운 이벤트 시간 = 색인



시스템 상세 분석

- **STEP 2. 타임라인 분석**
  - 분석 도구 : Plaso(http://plaso.kiddaland.net)

두 가지 분석 목표~!!

1. 최초 침입 시스템 찾기

2. 침입 포인트 찾기

분석 전략

1. 모든 시스템을 상세 분석할 순 없음

- 상세 분석 대상 시스템 지정
  - ✓ 최초로 공격이 탐지된 시스템, 주요 데이터가 저장된 시스템
  - ✓ 최초 침입 시스템
  - ✓ 주요 관리자/게이트웨이 시스템
  - ✓ 분석이 막혔을 때….

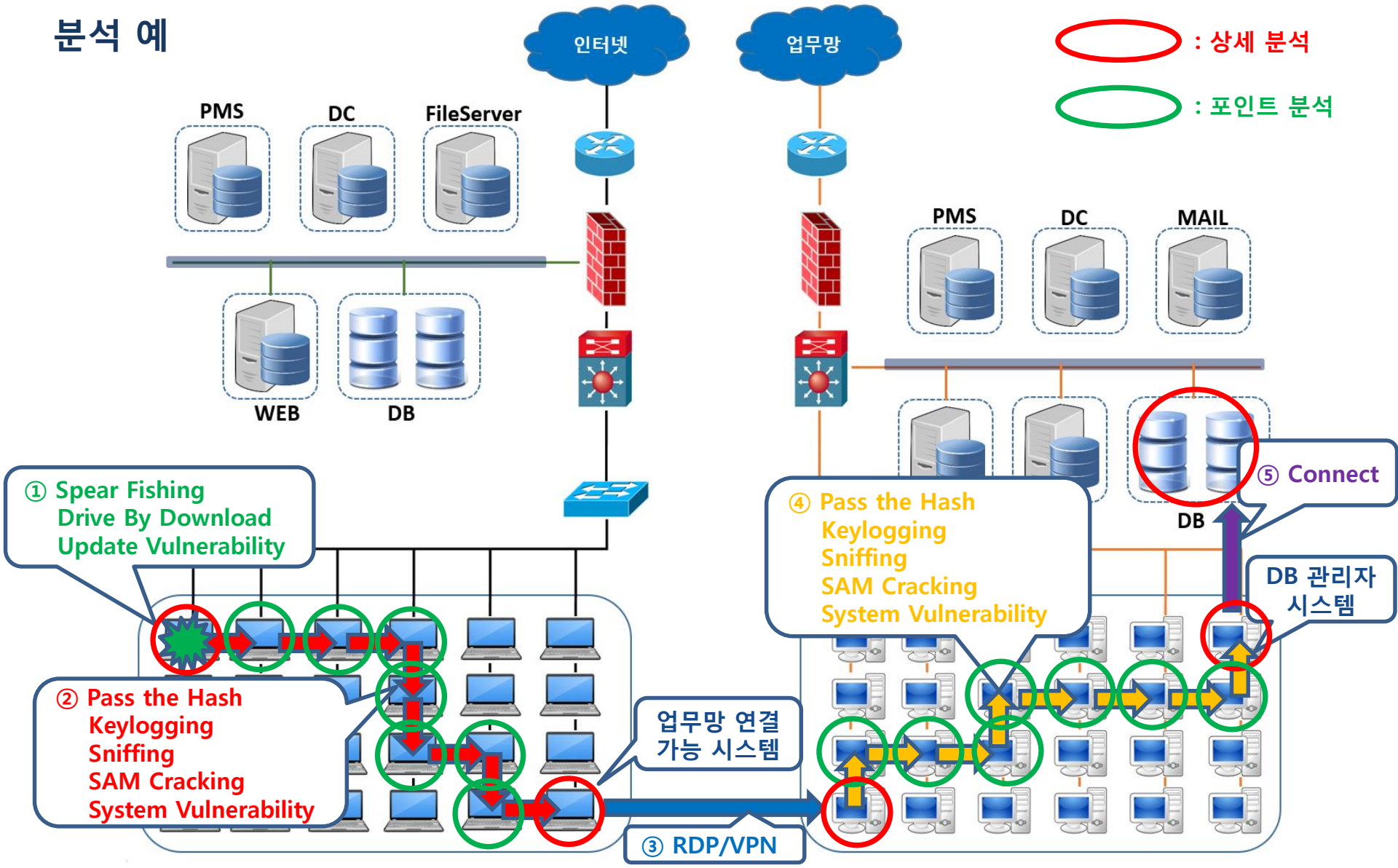
2. 최대한 많은 시스템의 아티팩트 및 정보 수집이 필요

- 앞으로 어떤 시스템을 분석하게 될지 모름
- 포인트 분석에 사용 : 주로 **Lateral Movement 역추적**이 목적
- 수집 도구 : FPLive_win v1.1, OpenIOC Editor/Finder

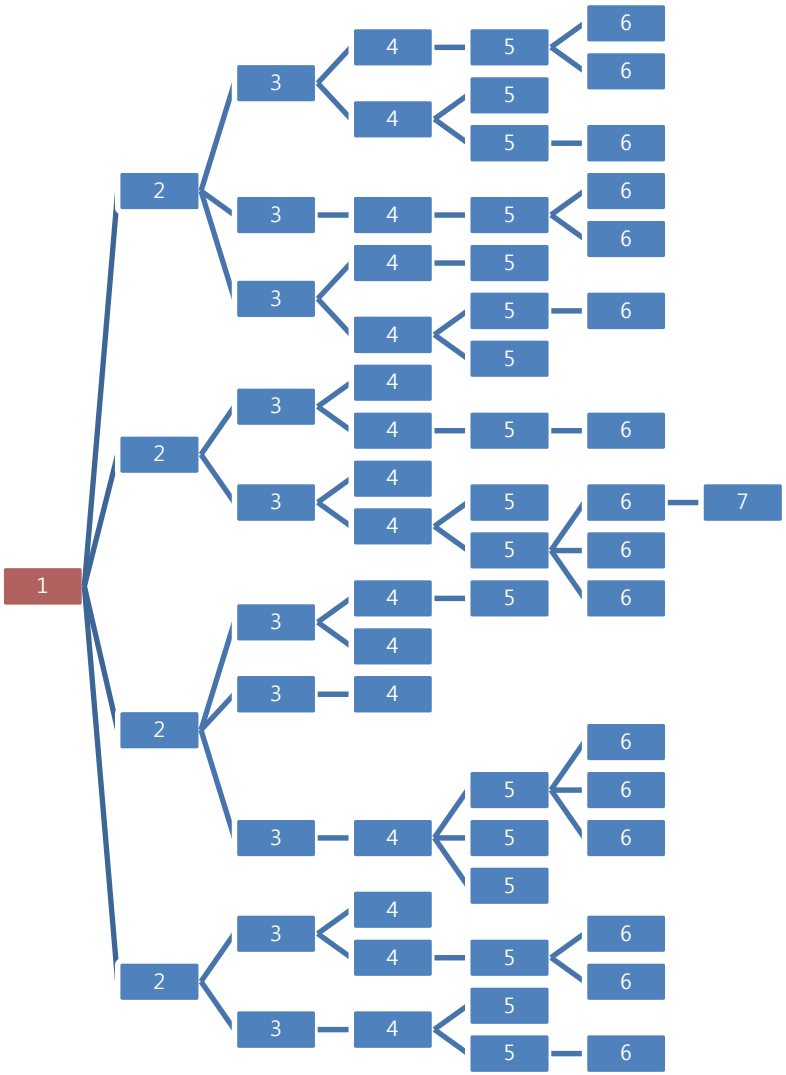
3. 절대 중간에 분석을 멈추면 안됨

- 분석 중간에 전혀 다른 시스템에서 악성코드 및 공격 징후가 발생할 수 있음
- 타 팀 혹은 상급자가 해당 이벤트를 긴급하게 요청;;
- 악성코드 치료 및 대응은 일단 유입 경로 파악 및 제거 후 수행함

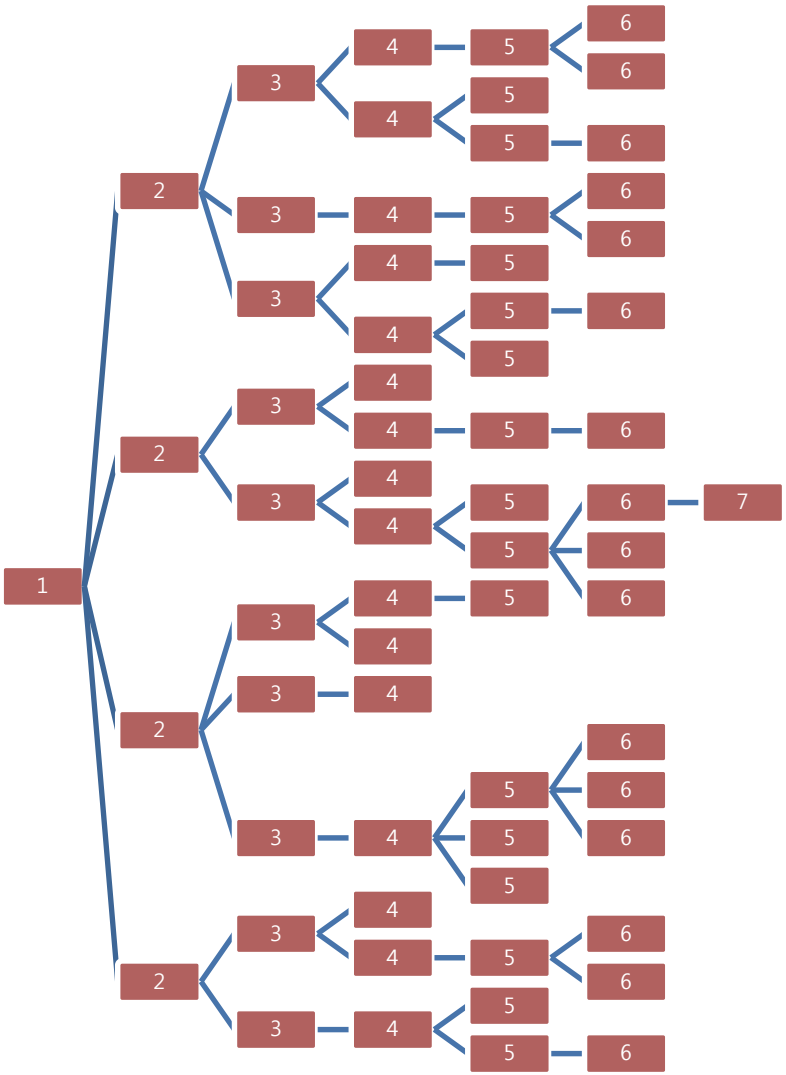
분석 예


인터넷
업무망
: 상세 분석
: 포인트 분석
PMS
DC
FileServer
WEB
DB
PMS
DC
MAIL
DB
① Spear Fishing
Drive By Download
Update Vulnerability
② Pass the Hash
Keylogging
Sniffing
SAM Cracking
System Vulnerability
④ Pass the Hash
Keylogging
Sniffing
SAM Cracking
System Vulnerability
⑤ Connect
DB 관리자
시스템
업무망 연결
가능 시스템
③ RDP/VPN

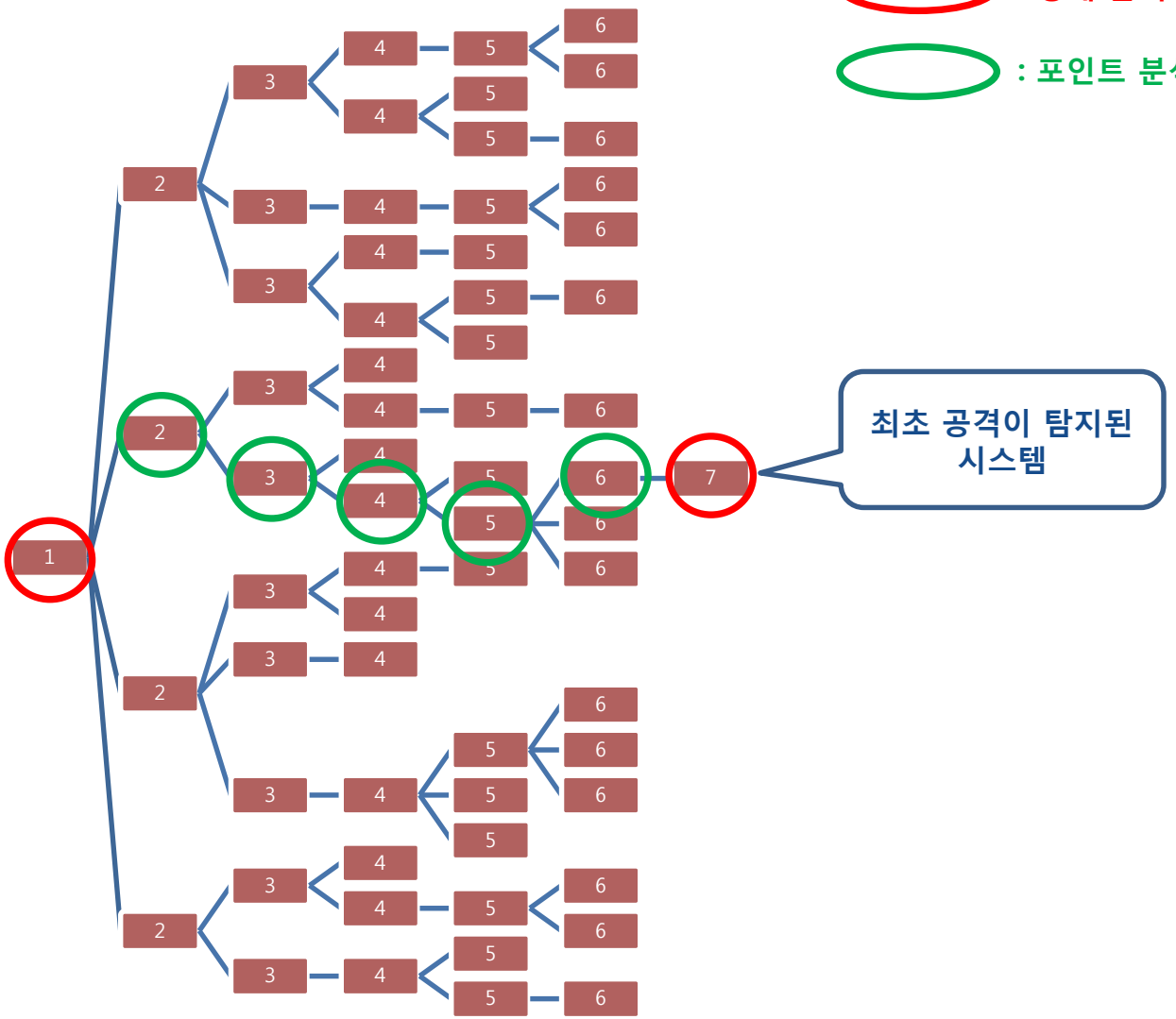
모든 시스템이 감염된 상황이라면~!!?



모든 시스템이 감염된 상황이라면~!!?



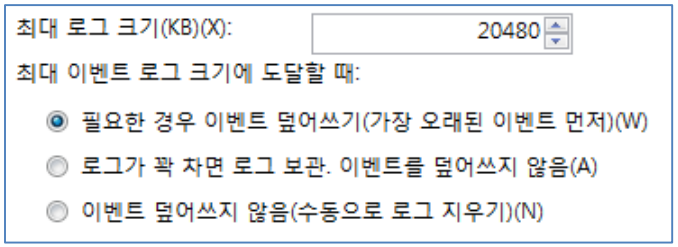
모든 시스템이 감염된 상황이라면~!!?



현실적 어려움

1. 아티팩트의 용량

- Windows Event Log 의 Default Size 는 512KB(XP), 20MB(Win7)…
- 장시간의 로그가 저장되어 있지 않음
- 오래된 로그를 덮어써버림
- **대응** : 포렌식 준비도 관점에서 용량 재설정 및 백업



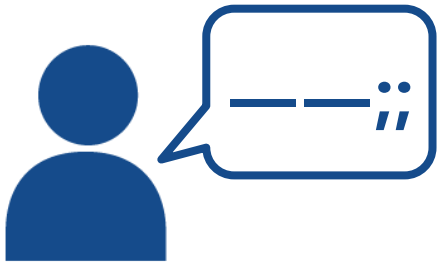
2. 공격자의 Anti Forensic 행위

- 공격자가 자신의 흔적을 지우려는 행위(로그 삭제, 파일 완전 삭제, 파일 시스템 파괴…)

- **대응** : 비할당영역에서 삭제 데이터 복구, 파일 완전 삭제 흔적 추적($LogFile, $UsnJrnl), 파일 시스템 구조 복구…

아무런 흔적이 없음...

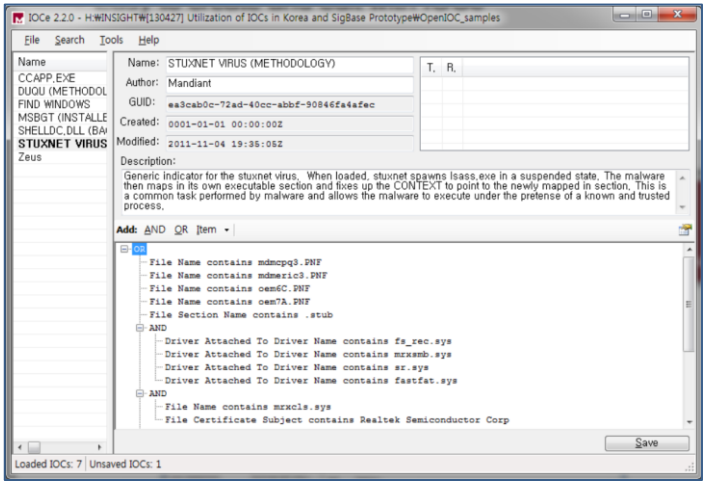
- 공격 시점이 너무 오래된 흔적이 남아 있지 않음
- 초기 대응 미숙으로 인한 흔적 삭제
- 삭제된 데이터 복구 실패



- 분석 실패?!!

아무런 흔적이 없음…

- **대응 1** (Lateral Movement 역추적에 실패한 경우)
  - IOC(Indicator of Compromise) 를 통한 최초 감염 시스템 추적
    - ✓ 감염 시기가 가장 빠른 시스템을 파악
    - ✓ 해당 시스템에 대한 상세 분석 및 또 다른 IOC 획득을 통한 분석 포인트 재획득
    - ✓ 도구(OpenIOC)
      - IOC Editor(http://www.mandiant.com/resources/download/ioc-editor/)



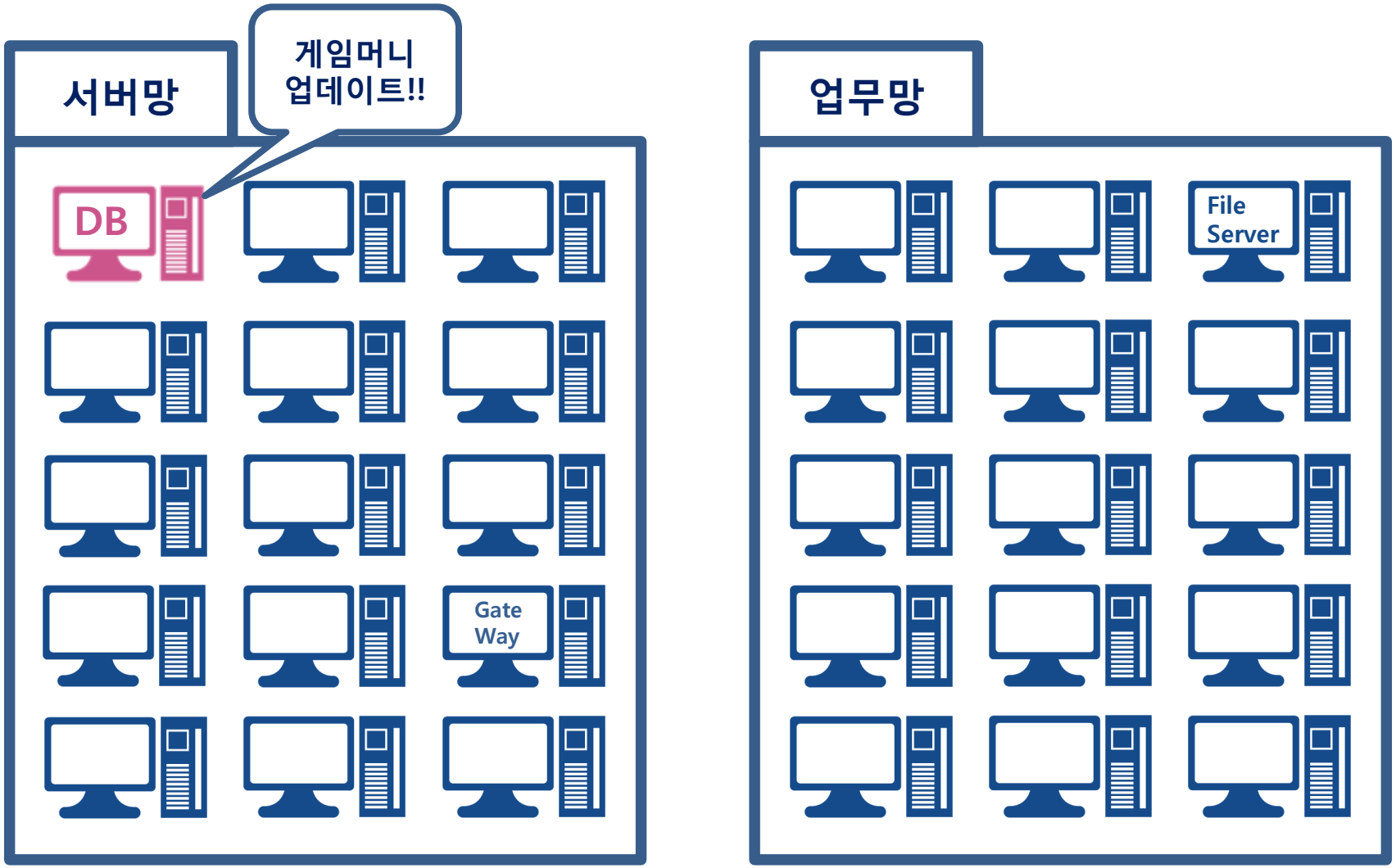
      - IOC Finder(http://www.mandiant.com/resources/download/ioc-finder/)

```
C:\lab>mandiant_ioc_finder collect -o result1 -d c:
05-27-2013 17:47:33 Setting up dependencies...
05-27-2013 17:47:33 Starting collection...
05-27-2013 17:47:33 Running built-in collection script at ./lib/script.xml...
05-27-2013 17:47:34 Auditing (w32system) started at 05-27-2013 17:47:34
```

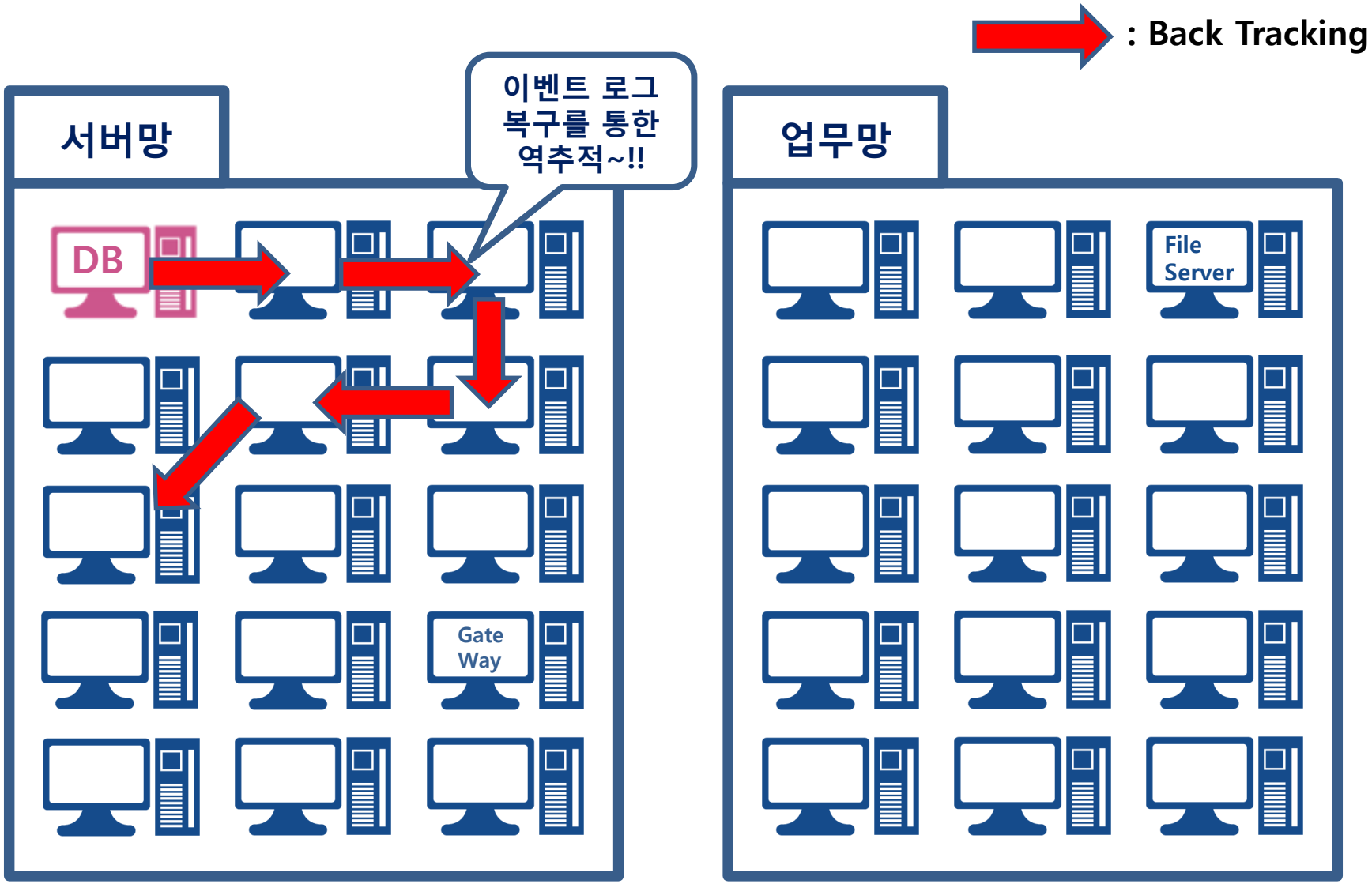
아무런 흔적이 없음…

- **대응 2** (유입 경로 찾기에 실패한 경우)
  - 외부 공격자와의 연결 지점은 반드시 있음
    - ✓ 일반적으로 백도어 Proxy 기능을 통한 쉘 연결 유지
      - ➔ 어딘가 외부와 연결이 가능한 시스템에 백도어가 설치되어 있음
    - ✓ 현재 연결을 다 차단함으로써 재침투 유도… ➔ 유입 경로 재분석
      - 발견된 모든 백도어의 동시 삭제
      - AV 의 실시간 차단 기능 사용

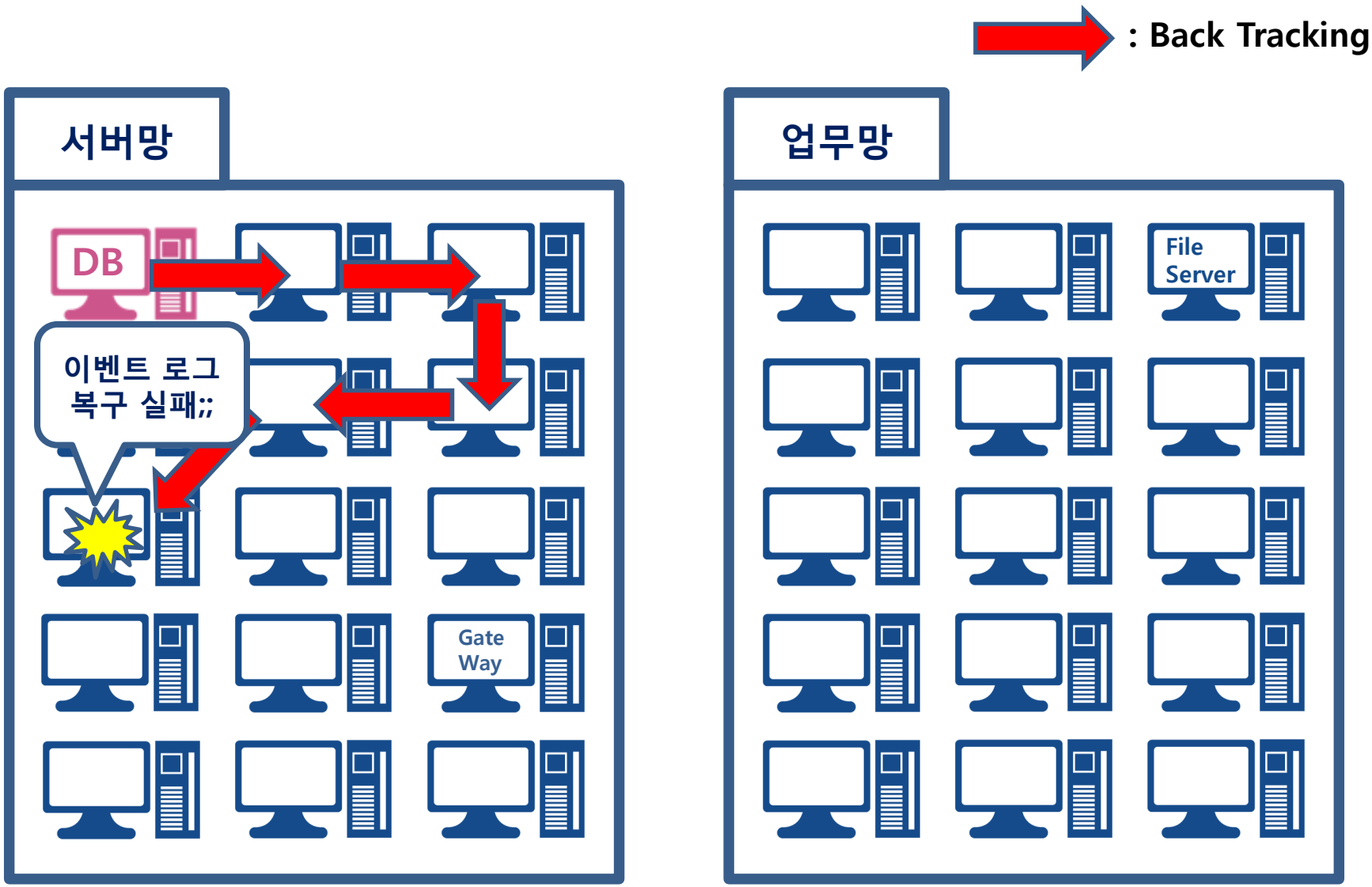
Case Study : 국내 온라인 게임사의 APT 대응



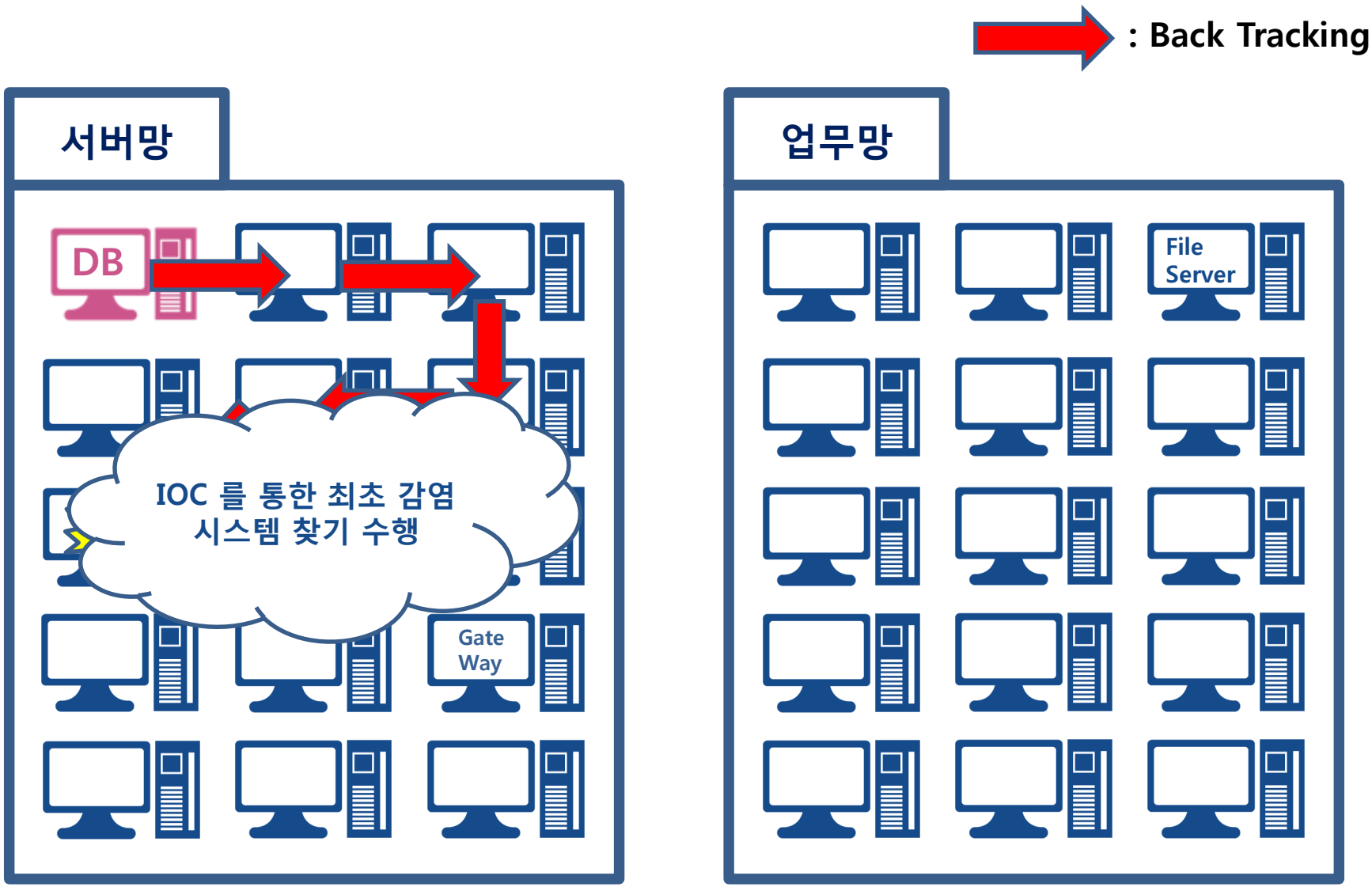
Case Study : 국내 온라인 게임사의 APT 대응



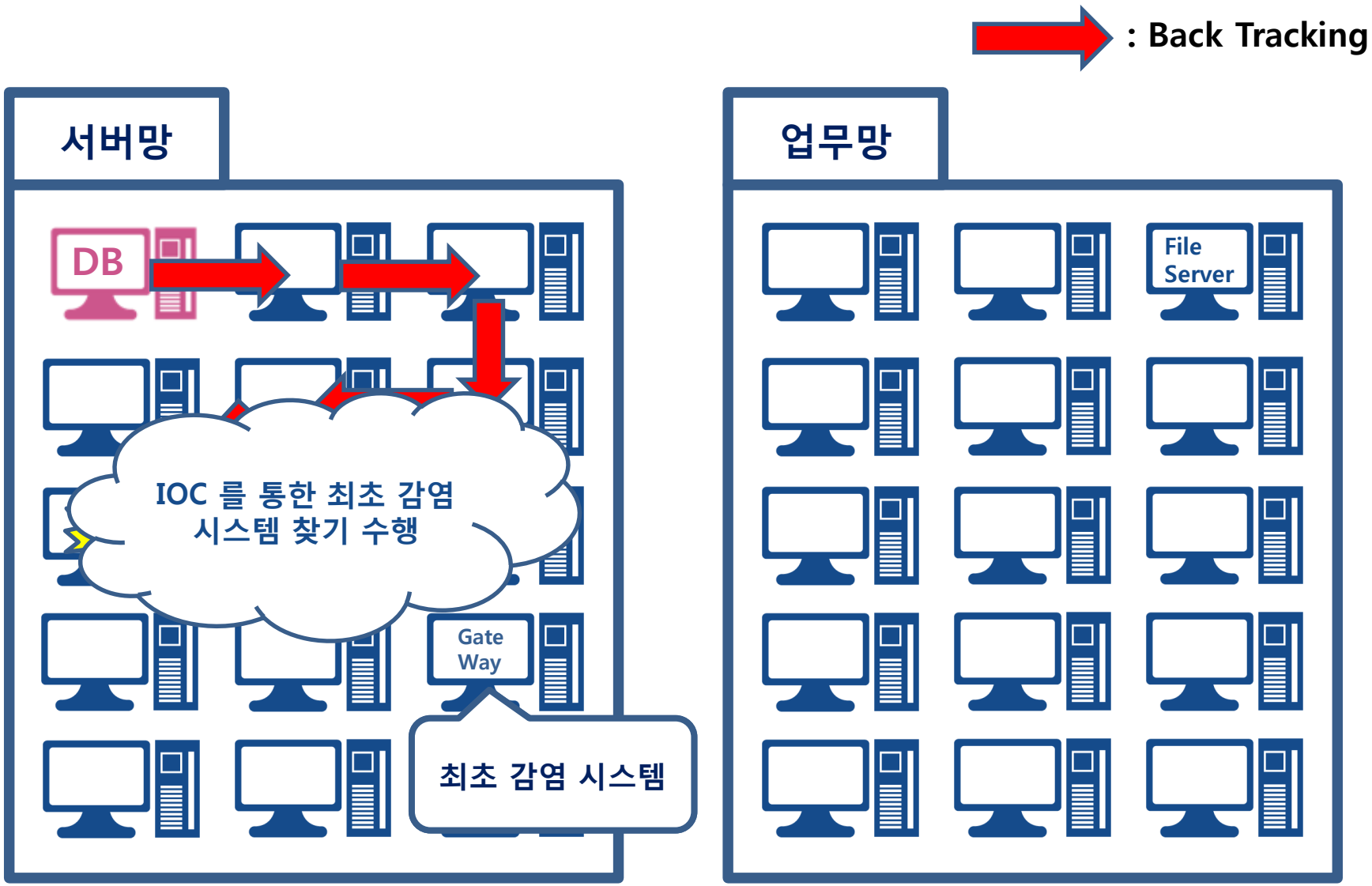
Case Study : 국내 온라인 게임사의 APT 대응



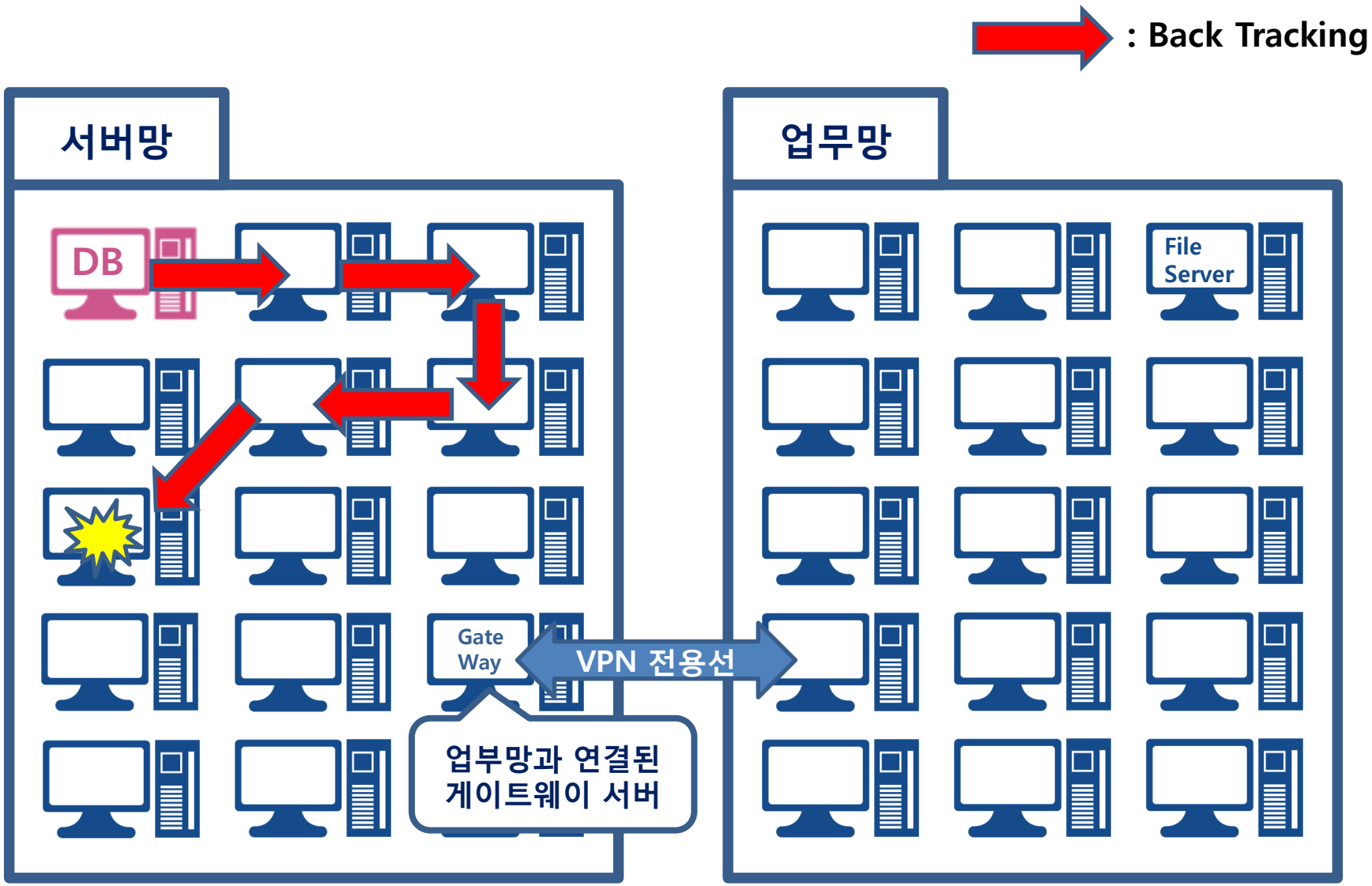
Case Study : 국내 온라인 게임사의 APT 대응



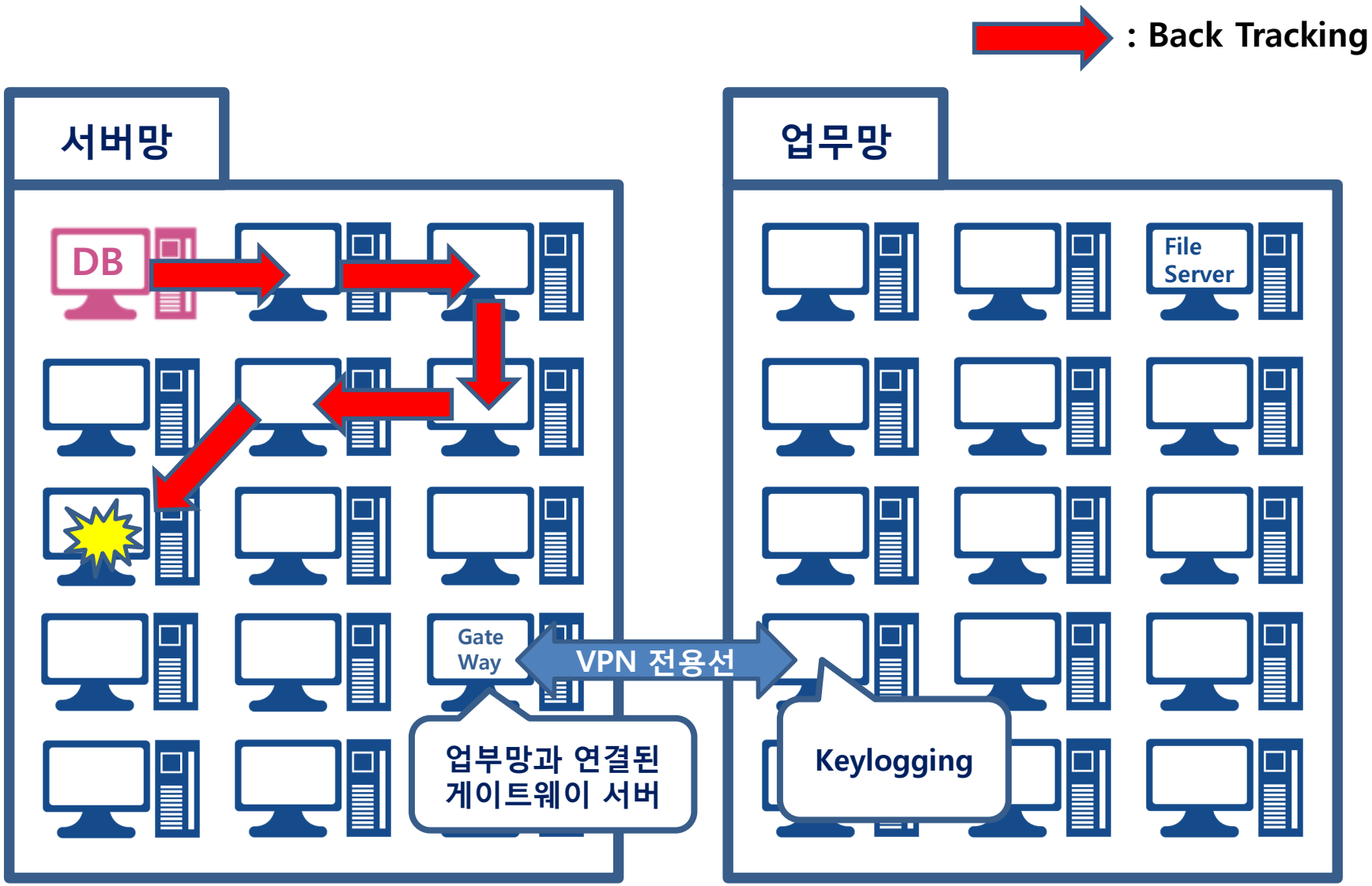
Case Study : 국내 온라인 게임사의 APT 대응



Case Study : 국내 온라인 게임사의 APT 대응

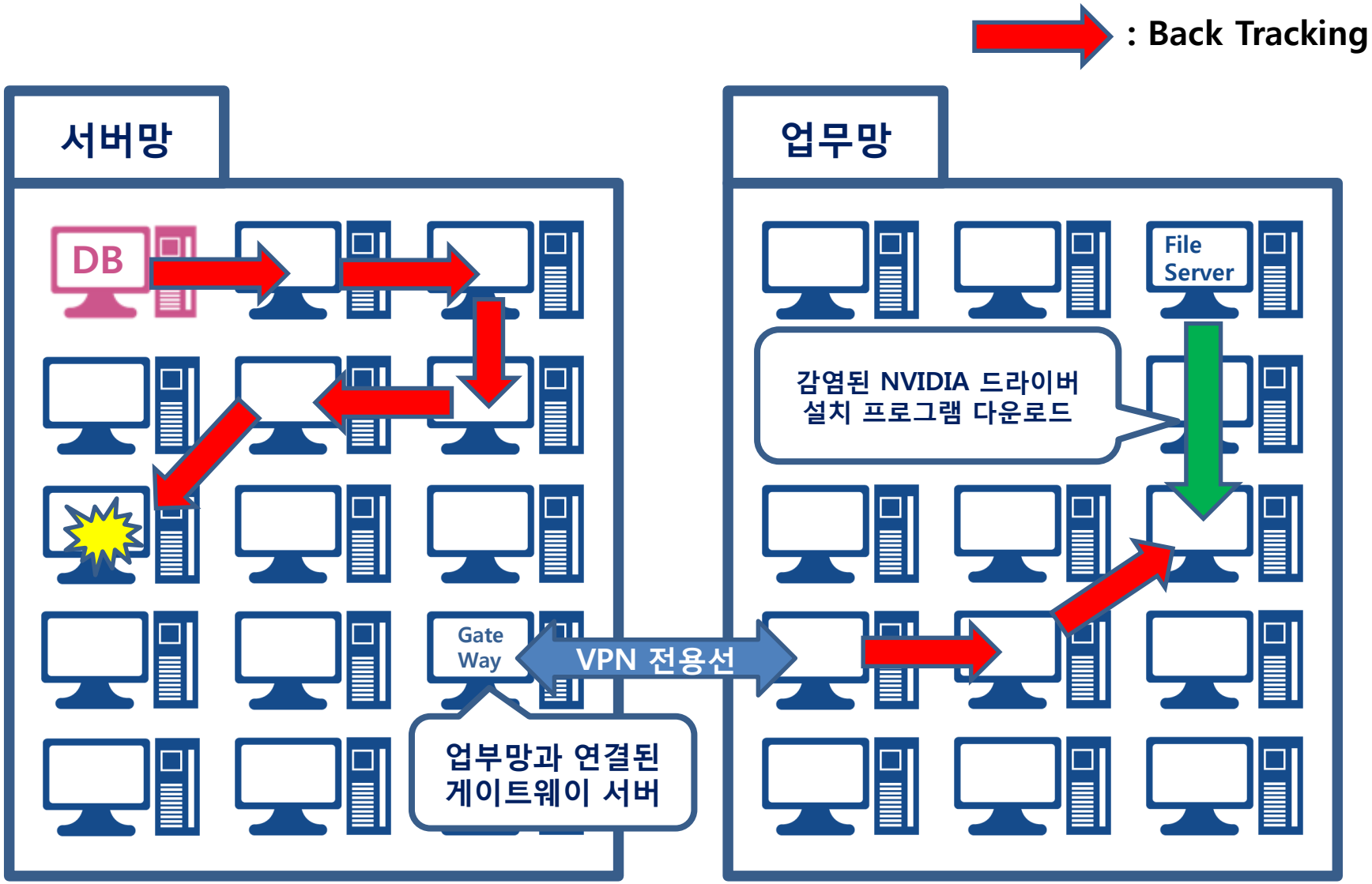


Case Study : 국내 온라인 게임사의 APT 대응



Case Study : 국내 온라인 게임사의 APT 대응

Case Study : 국내 온라인 게임사의 APT 대응



다시 한번…

왜? 유입 경로를 파악해야 하는가?


I’m Sick…

님하... 그만... ㅠ.ㅠ

No Initial Breach Point, No Win …

점심하러 가시죠?~^^