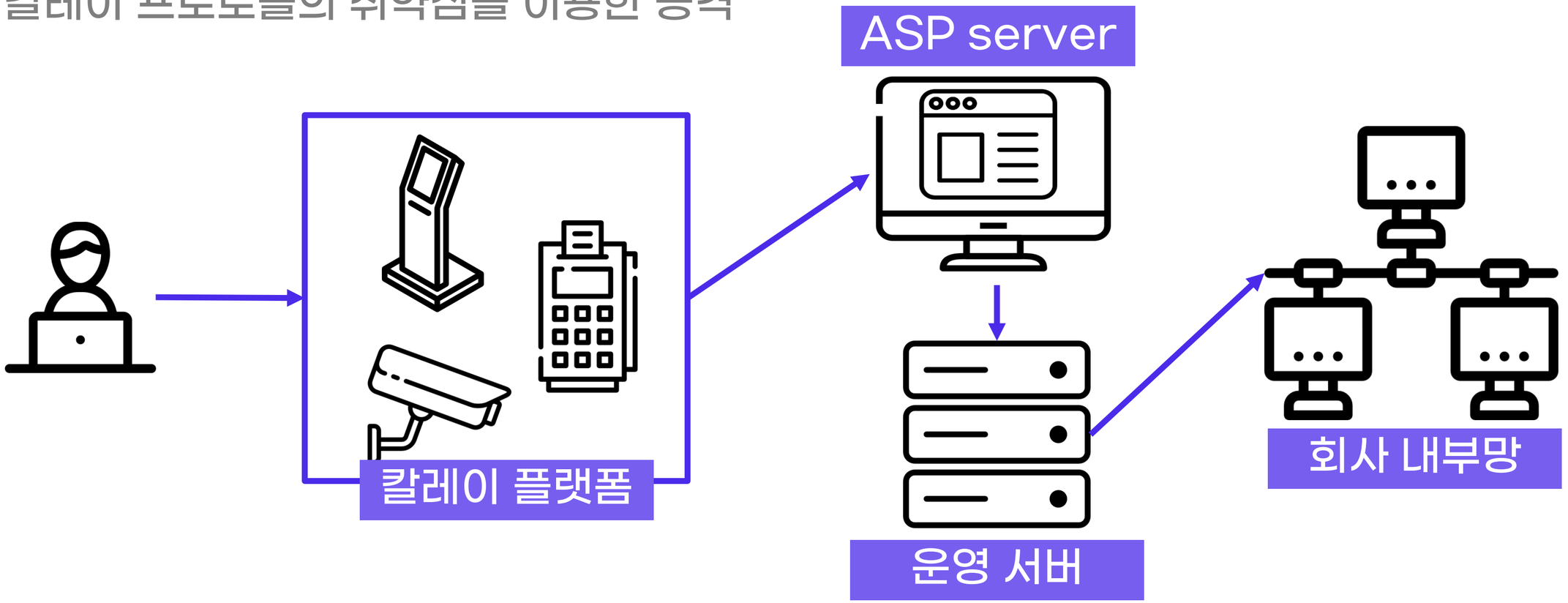
실무형 프로젝트 주제 회의
K-Shield 주니어 보안사고 분석대응 7기

2021.09.11
5팀 R&B

APT 시나리오 1

칼레이 프로토콜의 취약점을 이용한 공격

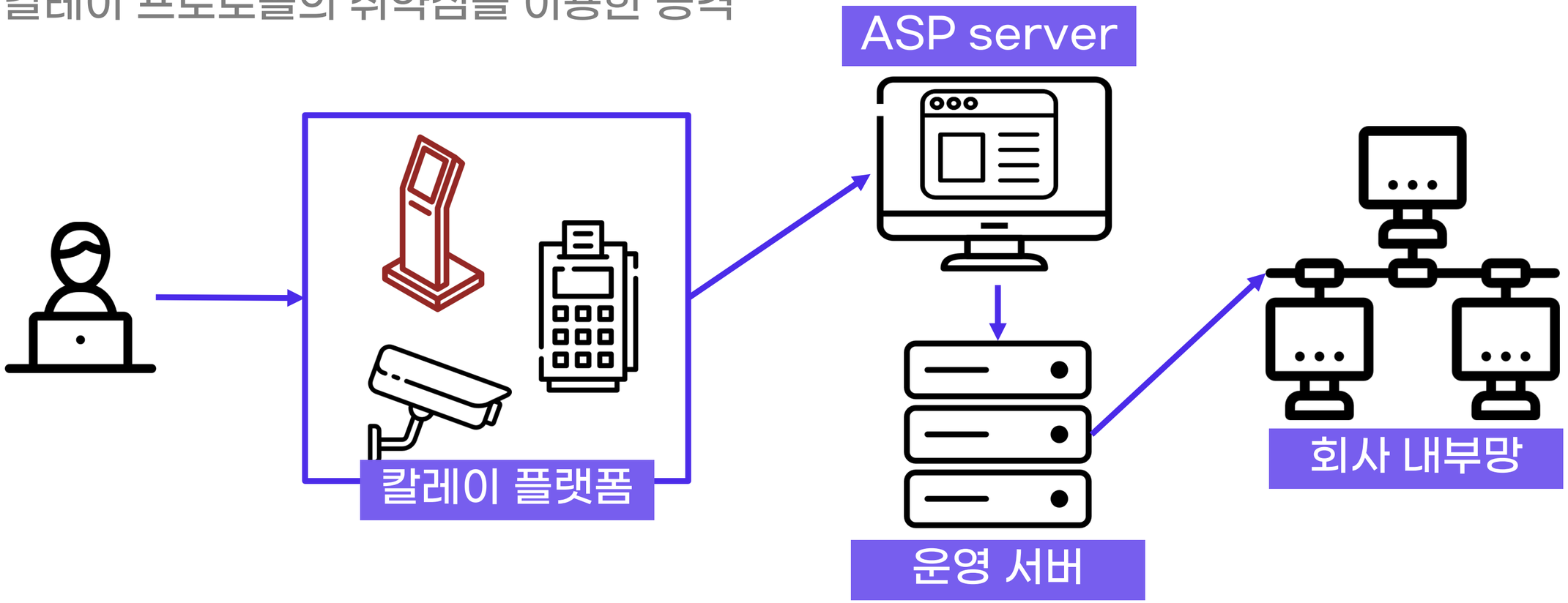
CVE-2021-28372
칼레이 프로토콜을 제대로 처리하지 않아 발생하는 취약점



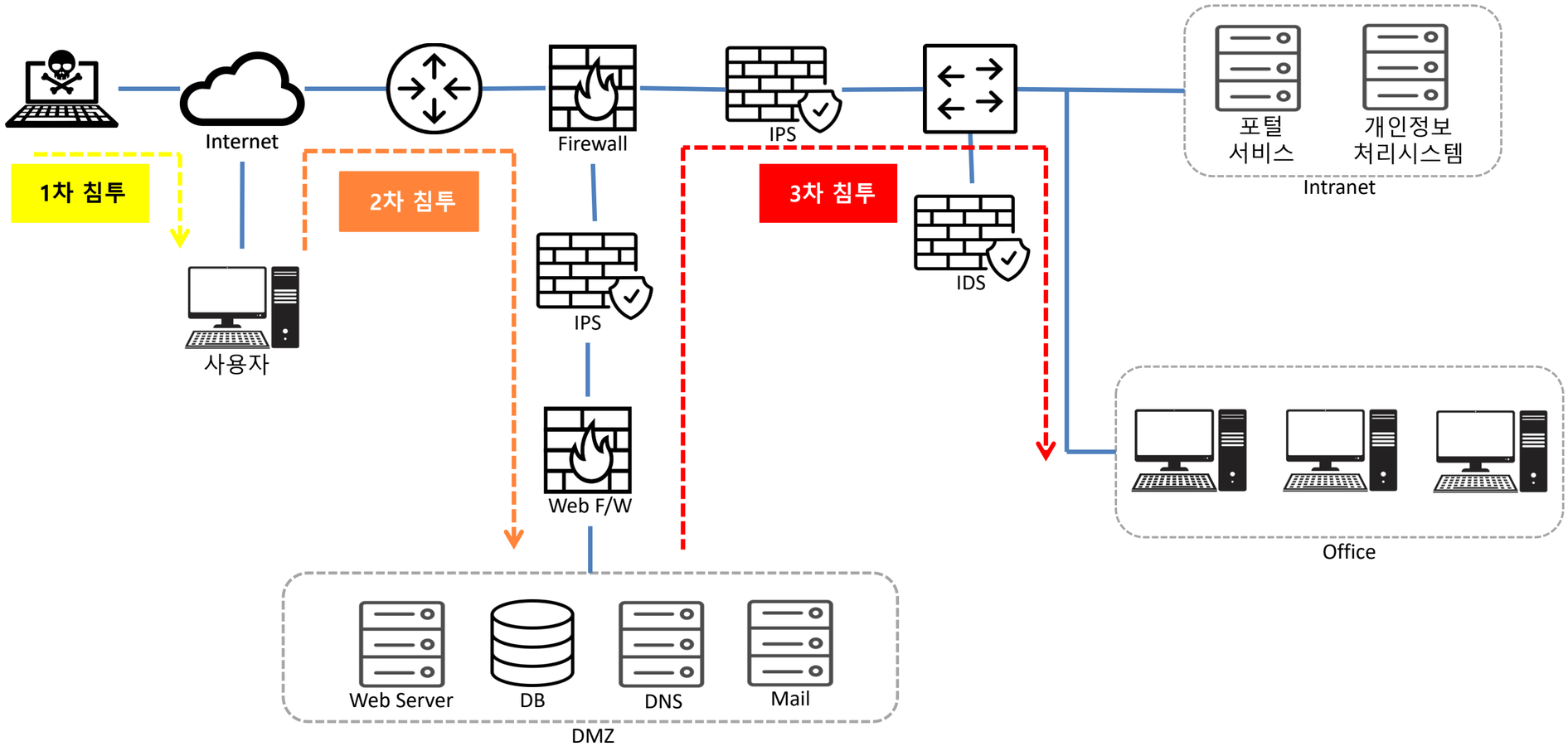
APT 시나리오 1

칼레이 프로토콜의 취약점을 이용한 공격

CVE-2021-28372
칼레이 프로토콜을 제대로 처리하지 않아 발생하는 취약점

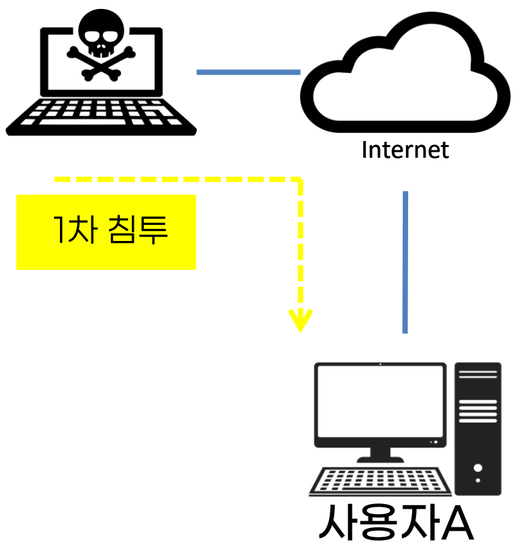


APT 시나리오 2


Internet
Firewall
IPS
포털
서비스
개인정보
처리시스템
Intranet
1차 침투
2차 침투
3차 침투
IPS
IDS
사용자
Web F/W
Office
Web Server
DB
DNS
Mail
DMZ

APT 시나리오 2

사용자 A는 자가격리로 인해 재택근무를 하는 상황



1차 침투 : 초기 침투(Drive-by Compromise)

1. 워터링 홀 역할을 하는 조작된 사이트를 통해 전달
2. 조작된 웹사이트와 익스플로잇 킷을 통해 피해자 시스템을 감염
3. 웹사이트의 악성 광고를 통해 확산
4. 조작된 웹사이트와 Google Ads를 사용하여 피해자가 설치 프로그램을 다운로드
5. Windows 및 macOS용 VST(Virtual Studio Technology)의
   불법 복제 복사본과 함께 번들로 제공
6. YouTube 비디오 다운로더 애플리케이션을 미끼로 사용하여 피해자들에게
   토렌트 파일 공유 웹사이트를 통해 악성코드 배포

APT 시나리오 2

2차 침투

1) 내려받은 파일을 실행하면

파일에서 암호화된 매크로 복호화 및 실행

2) 악성 셸코드를 로드하여 메모리에서 실행

- Command and Scripting Interpreter

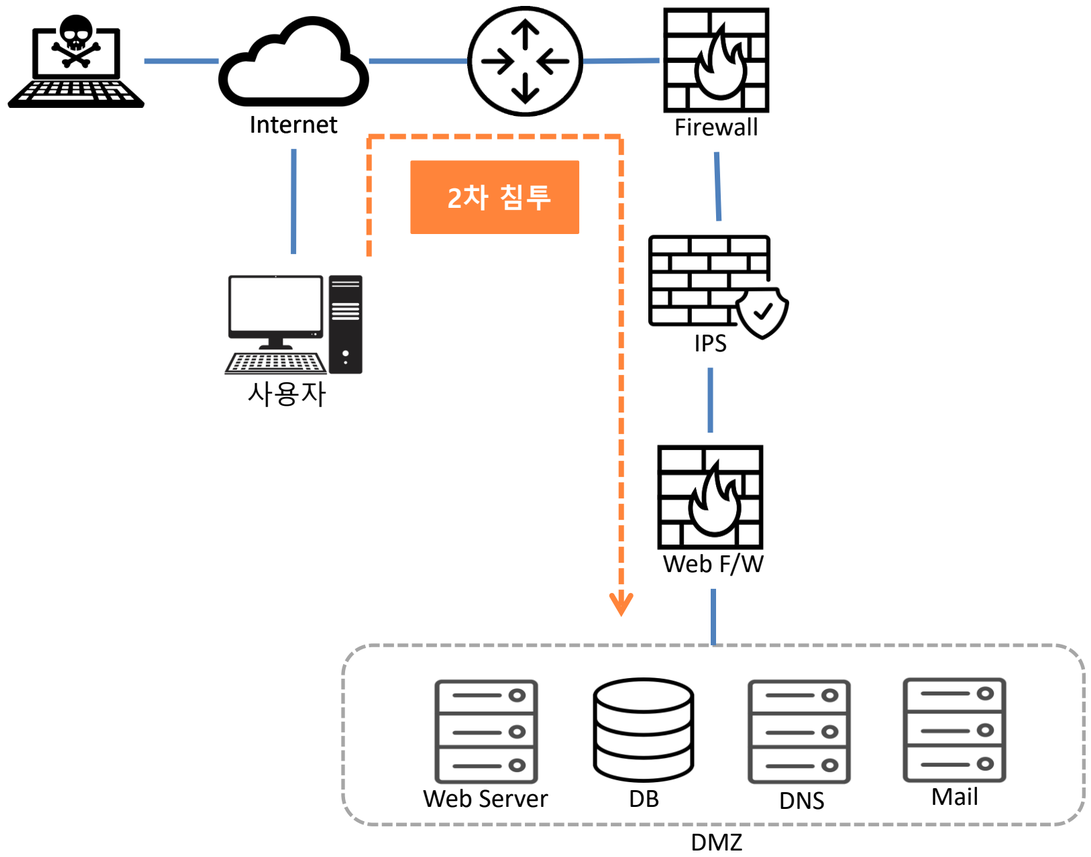
: Windows Command Shell

3) 지속성을 설정하기 위해 재부팅 시 파일이

실행되도록 레지스트리 키를 생성

- Boot or Logon Autostart Execution

: Registry Run Keys / Startup Folder



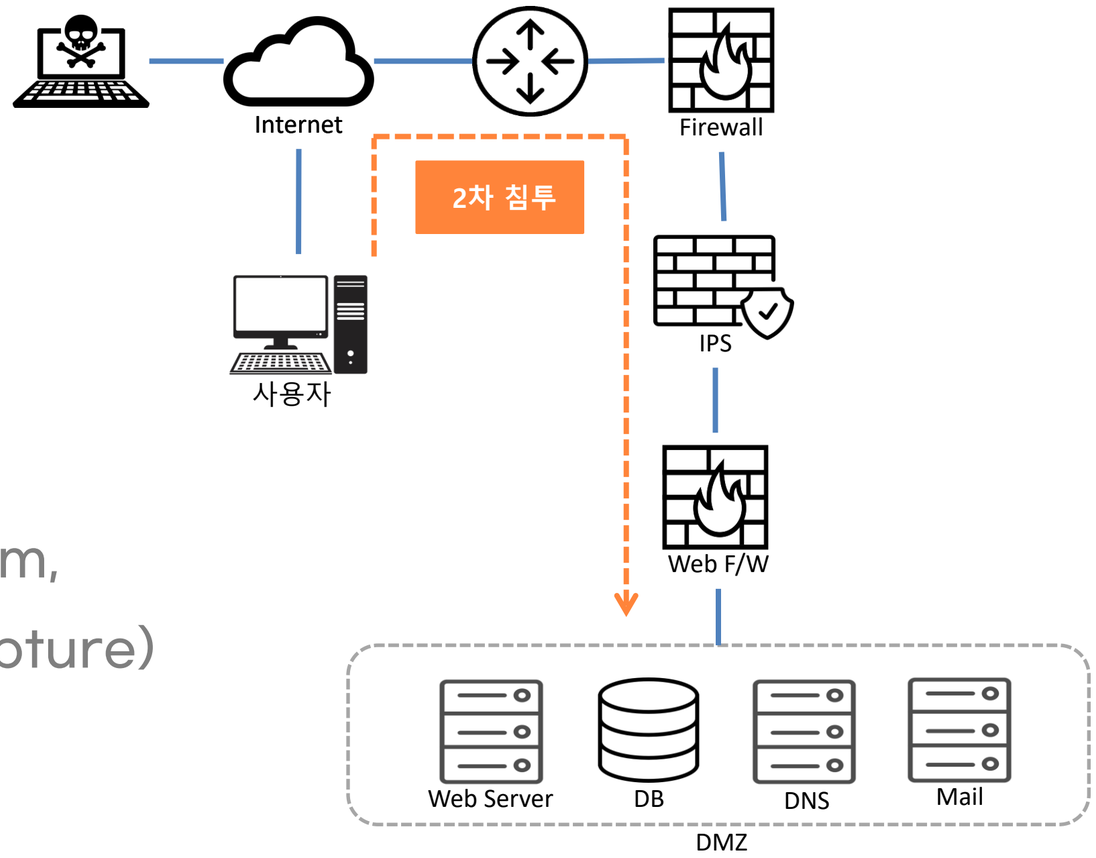
APT 시나리오 2

2차 침투

4) 명령 코드 및 데이터 다운로드(C&C)

5) A는 웹서버에 로그인하여 '업무 보고서'라는
문서 파일을 자신에게 메일 전송

6) 정보 수집
(Audio Capture, Data from Local System,
Input Capture:Keylogging, Screen Capture)



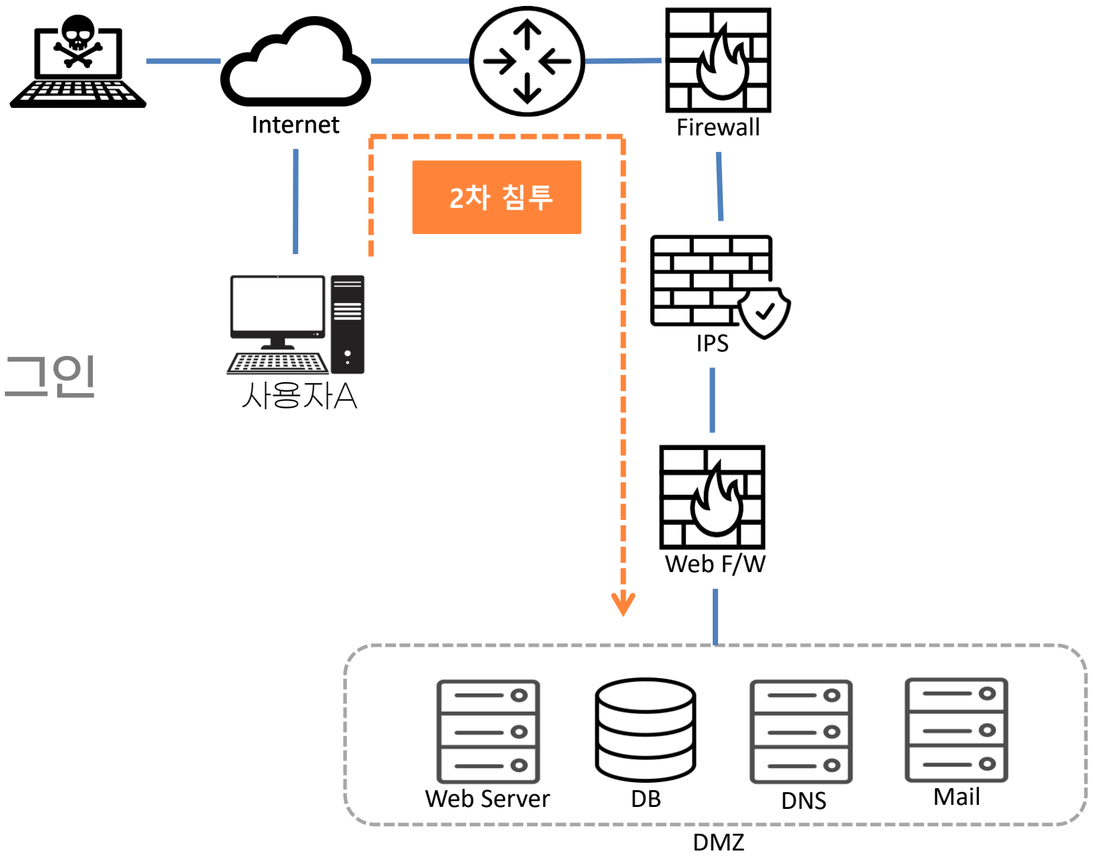
APT 시나리오 2

2차 침투

7) 수집한 정보를 공격자에게 전송
(Exfiltration Over C2 Channel)

8) 공격자는 획득한 A의 ID와 PW를 통해 웹서버 로그인

9) 공격자는 '업무 보고서' 문서 파일에 악성코드를
포함시켜 수정(Spearphishing)

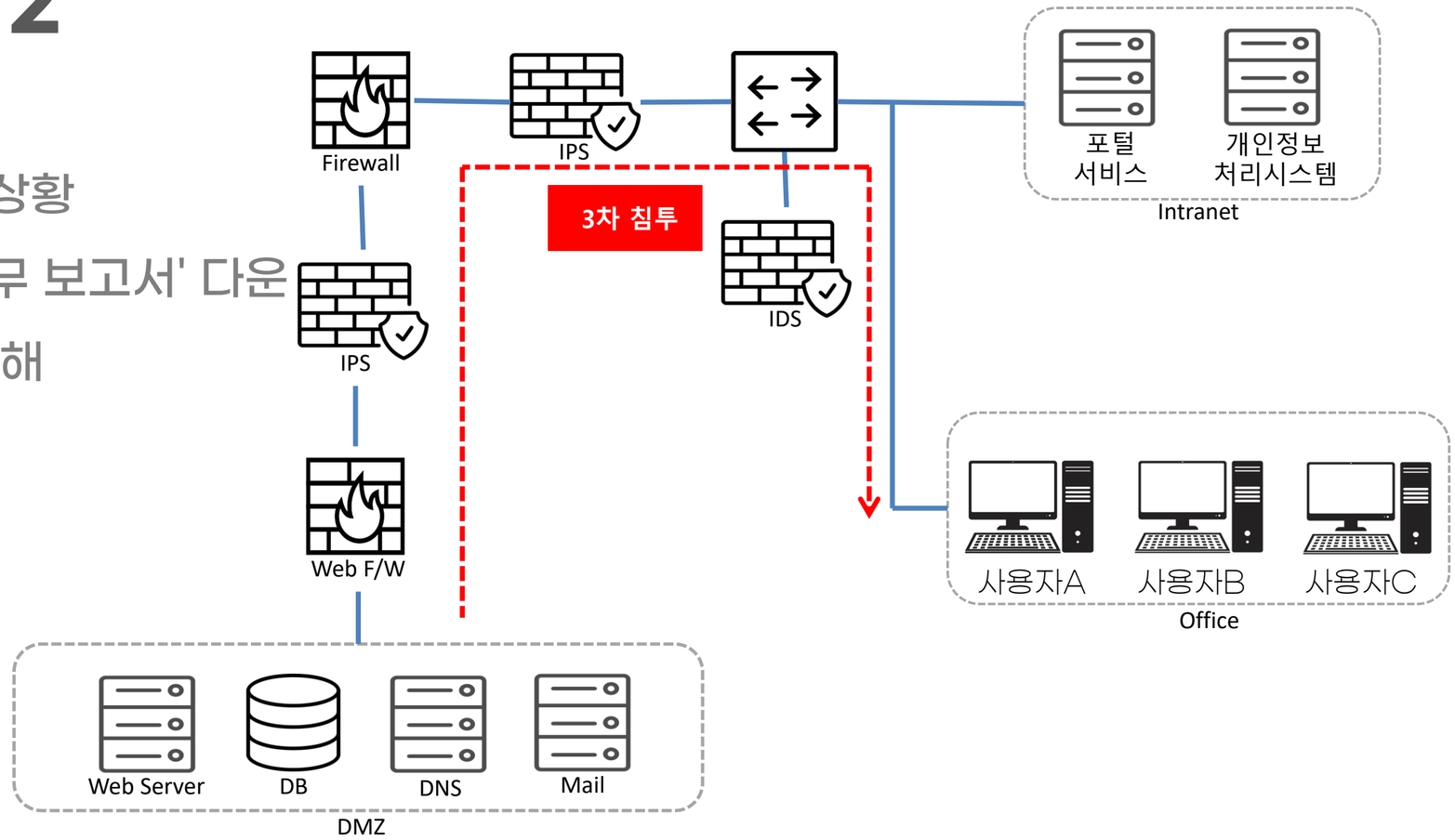


APT 시나리오 2

3차 침투

사용자A는 회사로 복귀한 상황

- A는 자신에게 보냈던 '업무 보고서' 다운
- '업무 보고서' 실행으로 인해
  악성 코드 감염



APT 시나리오 2

Defense Evasion(우회)

Living off the Land

Living off the Land

시스템에 이미 설치되어 있는 Tool을 사용해서 해킹 공격을 하는 기법

1) Anti-Virus Software 탐지를 피할 수 있음

2) Fileless 형태

Lateral Movement (측면 이동)

1) Exploitation of Remote Services

2) Lateral Tool Transfer

< 최종 목표 >

1) 중요 데이터 탈취 후 흔적 삭제

2) 중요 데이터 랜섬웨어 후 금전 요구

3) 시스템 및 네트워크 자원 파괴

EDR 시스템 Detection Module 구현

정적 탐지 Yara 규칙 적용

동적 탐지 악성 행위 로깅

1) Sysmon - MITRE ATT&CK 프레임워크 매핑

Fileless Attack Detection

1) Windows API 분석 2) 이벤트 실행 순서 추적

Living off the Land Detection

1) Powershell 스크립트 분석 2) WMI 분석

EDR 시스템 Defense Module 구현

- 악성 행위 차단
- 경고 및 결과 Report 제공 기능

^
진
단
v

Living off the Land Attack

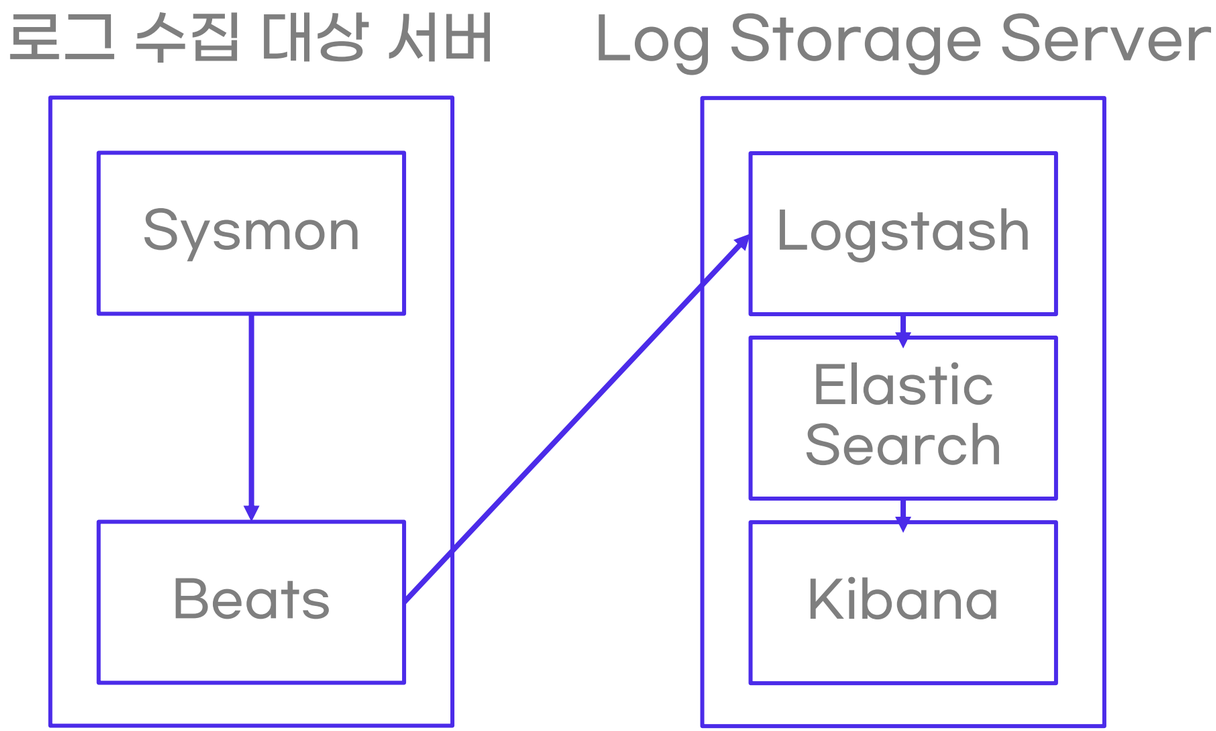
Fileless Attack

- Windows Regitstry Manipulation
- Memory Code Injection
- Script-Based techniques

EDR 시스템 GUI

Elastic (ELK) Stack 사용

- 악성 행위 로그 모니터링
- 로그 시각화
- 탐지 / 차단 결과 통계화



감사합니다!