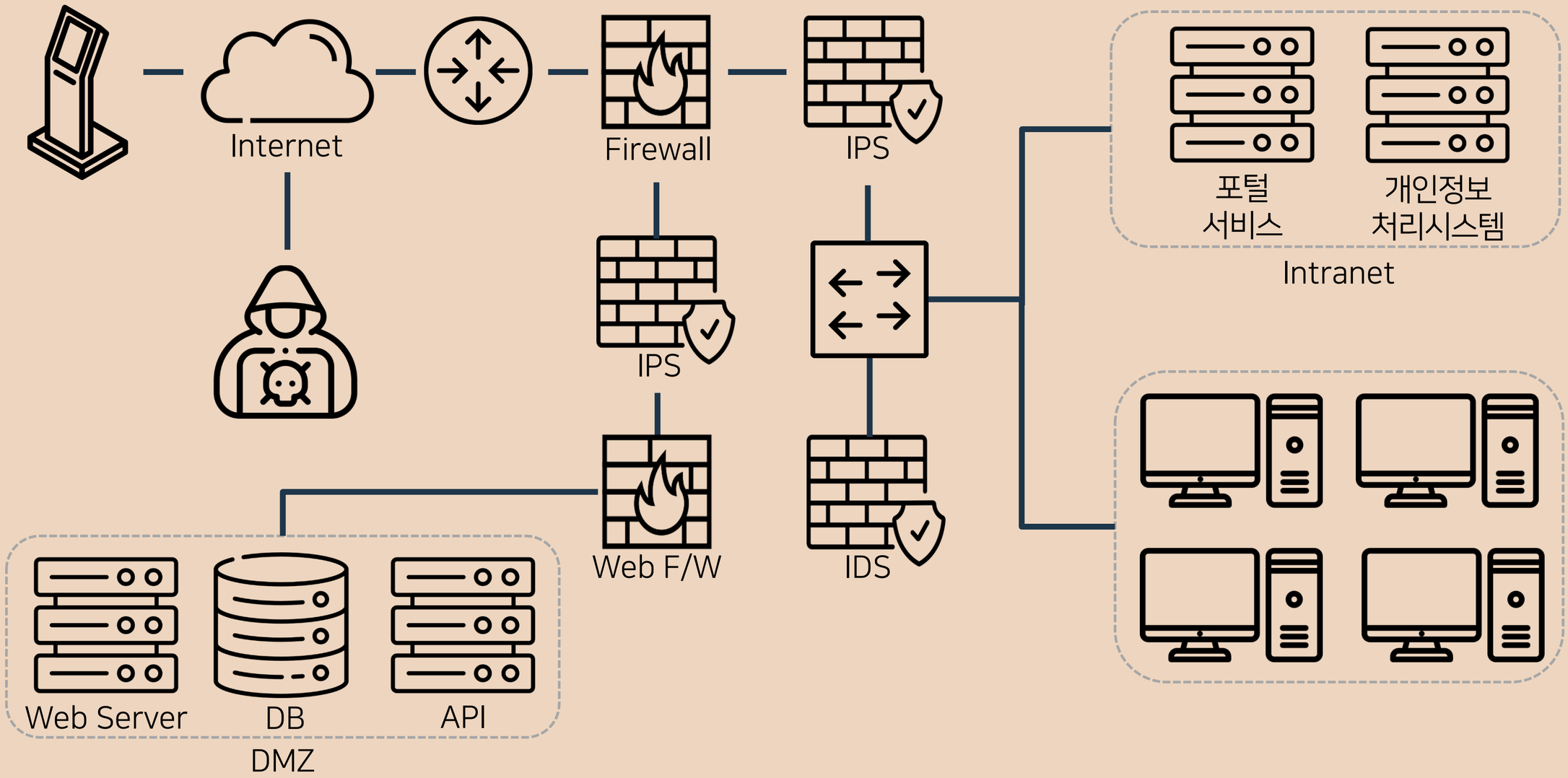
실무형 프로젝트 회의

K-Shield 주니어 보안사고 분석대응 7기

2021. 09. 18

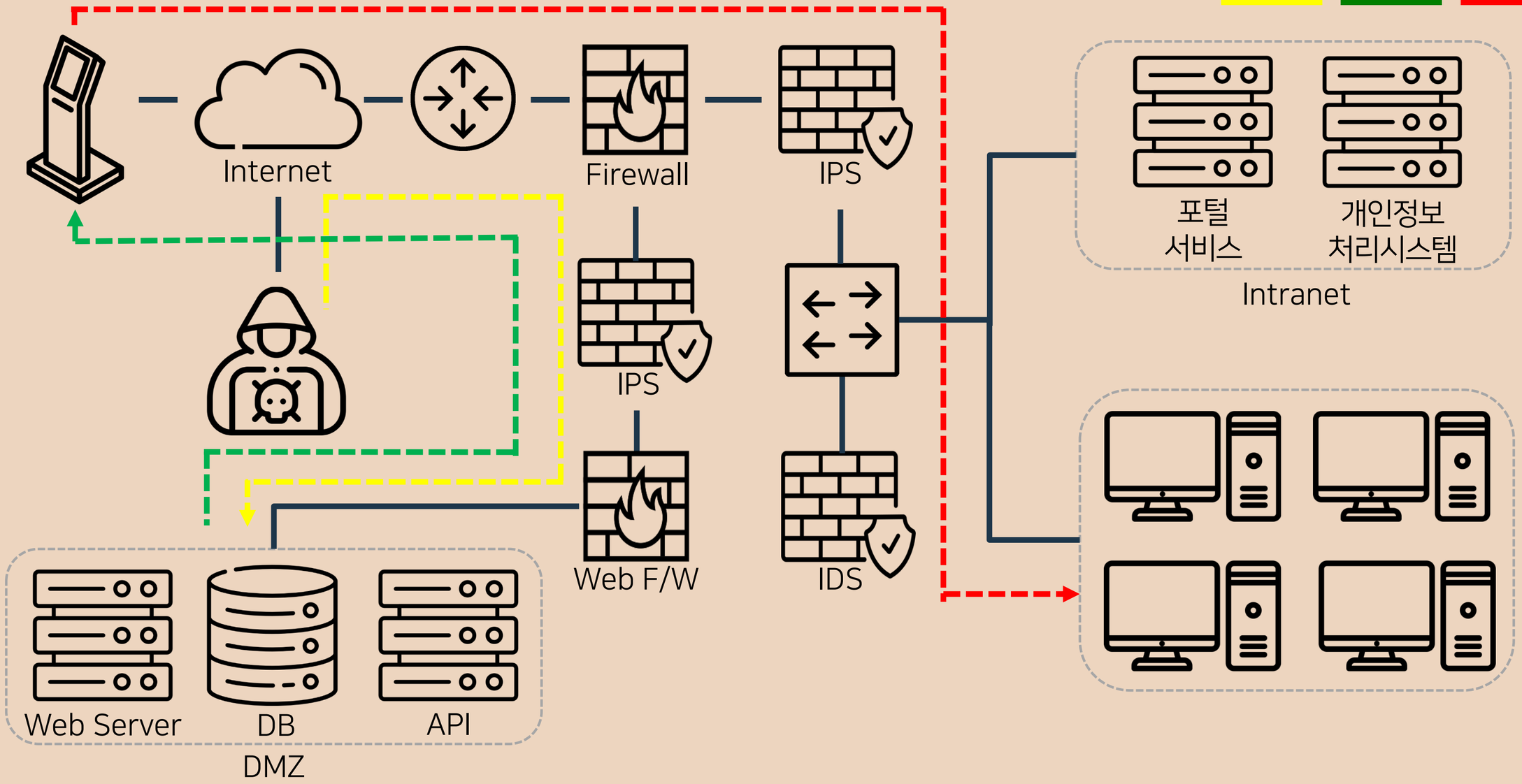
5조 R&B

APT 공격 시나리오

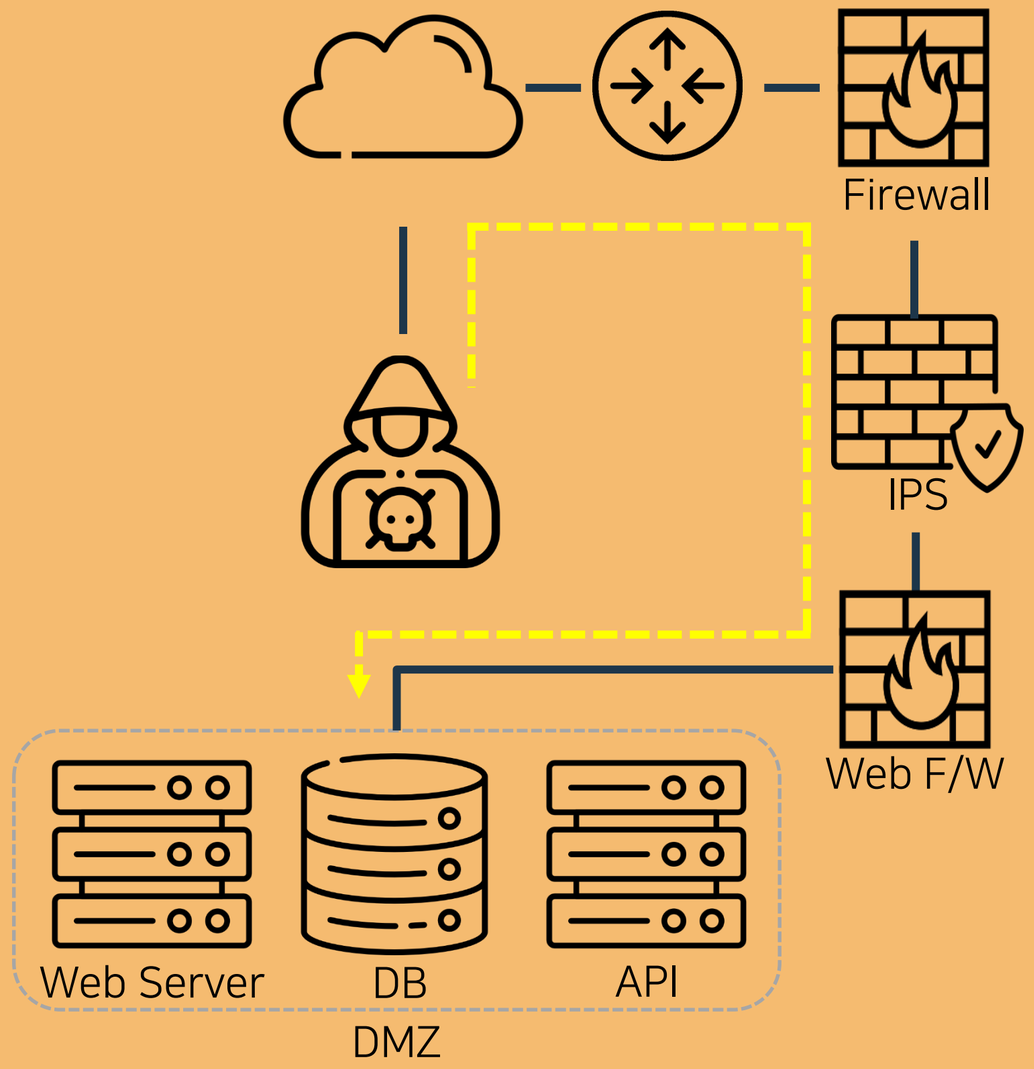

Internet
Firewall
IPS
IPS
IPS
Web F/W
IDS
포털
서비스
개인정보
처리시스템
Intranet
Web Server
DB
API
DMZ

APT 공격 시나리오

1차 2차 3차



침투 과정

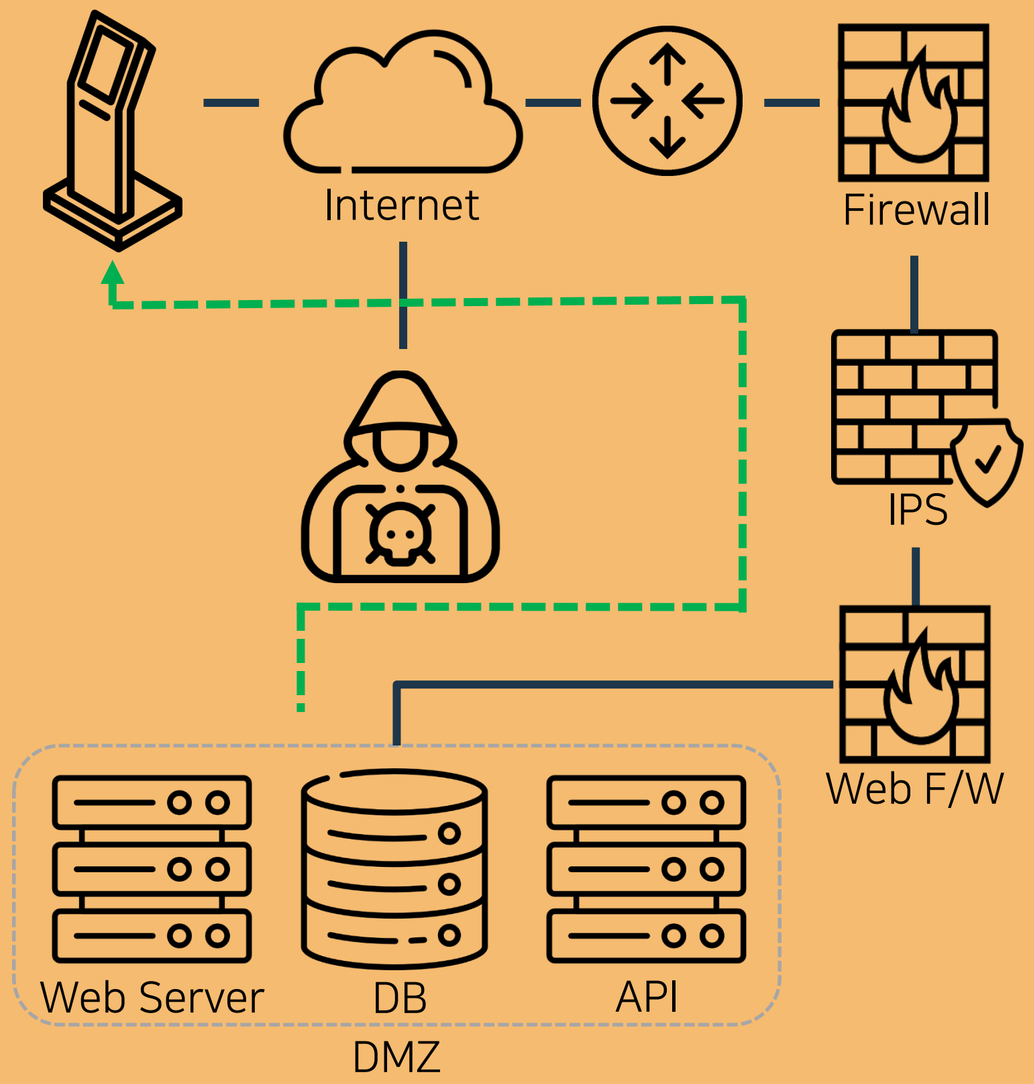


1차 침투 : 공격자 -> API 서버

코드 주입 / 리플레이 요청 /
요청 조작 / 사용자 인증 파괴 /
API 후킹

*API후킹 : 응용 프로그램에서
발생하는 API에 대한 정상적인 호출을
중간에 가로채서, 프로그래머가 의도한
특정 목적을 달성하는 해킹 기법

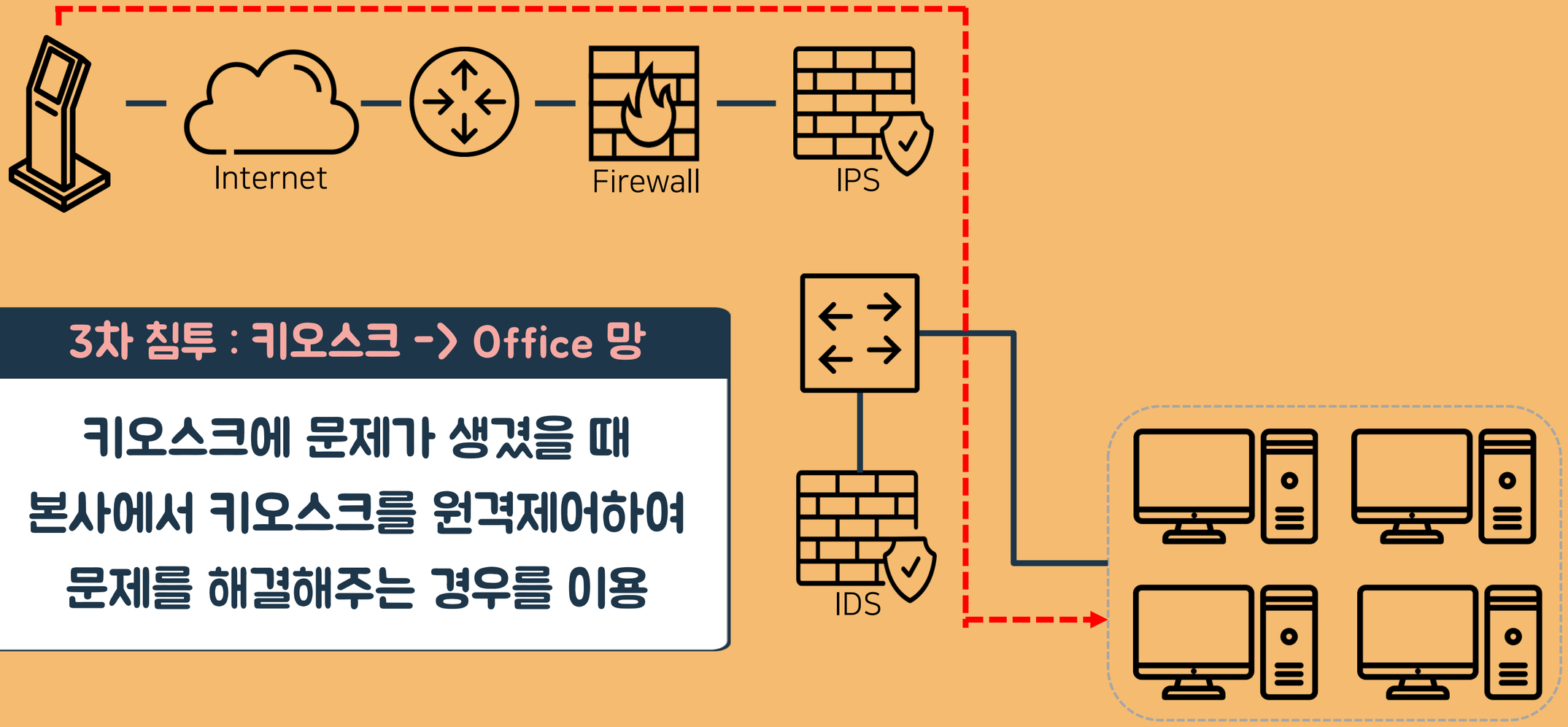
침투 과정



2차 침투 : API 서버 -> 키오스크

오염된 API를 통하여
키오스크 감염

침투 과정

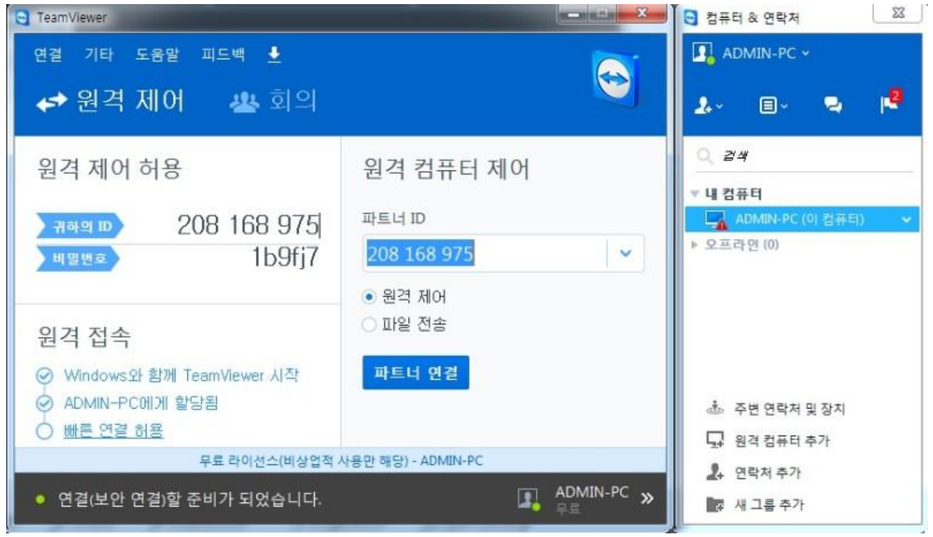


3차 침투 : 키오스크 -> Office 망

키오스크에 문제가 생겼을 때
본사에서 키오스크를 원격제어하여
문제를 해결해주는 경우를 이용

원격 제어 침투 방법

취약한 원격 PC 제어 프로그램을 악용(ex. 팀뷰어)



포스단말기 해킹한 후 개인정보,
금융정보 탈취
-> 탈취한 이메일 주소, 비밀번호로
팀뷰어 로그인 창에 '빈어택' 방식 이용

*BIN Attack (Bank Identification Number)
: 신용카드 번호와 카드 유효기간을 해킹해
무단으로 결제하거나 고객 정보를 빼내는 행위

키오스크 API

1) 키오스크 매니저(KIOSK Manager) : 키오스크에서 사용할 메뉴와 파일, 이미지 등을 다운로드하며 프로그램과 설정 파일을 관리	3) 디바이스 제어 프로그램: 기기와 응용 프로그램 간의 통신을 담당하며 각종 디바이스 에러 처리, 복구 등의 작업 수행
2) 전문제어 프로그램: 거래가 발생하면 점포 서버와 주문을 주고받으며 주문 처리, 결제, 개점, 마감 작업 등을 수행	4) 응용 프로그램: 실제 사용자로부터 주문을 받아 결제 처리 실행 관리자를 위한 관리 프로그램도 제공

키오스크 API 서버 구축

REST

Representational State Transfer

1) 네트워크를 통해서 컴퓨터끼리
통신할 수 있게 해주는 아키텍처 스타일

2) 웹 최적화, 데이터 포맷이 JSON

-> 브라우저들 간에 호환성이 좋고
성능과 확장성이 뛰어남

3) 표준화된 메시징 시스템 존재

4) 통신 장애가 있을 경우 재시도밖에 안 됨

SOAP

Simple Object Access Protocol

1) 보안이나 메시지 전송 등에 있어서
REST보다 더 많은 표준들이 정해져
있기 때문에 조금 더 복잡

2) 보안 수준이 엄격

-> SSL 지원, WS-Security라는
자체 표준 보안 기능 존재

3) 통신 할 때 처음부터 끝까지 신뢰성 제공

키오스크 API 서버 구축

차이점	REST	SOAP
유형	아키텍처 스타일	프로토콜
기능	데이터 위주; 데이터를 위해서 리소스에 접근	기능 위주; 구조화된 정보 전송
데이터 포맷	다양한 포맷 사용 (일반 텍스트, HTML, XML, JSON)	XML
보안	SSL, HTTPS	SSL, WS-Security
대역폭	상대적으로 리소스가 적게 필요하고, 무게가 가벼움	상대적으로 더 많은 리소스와 대역폭이 필요
데이터 캐시	사용 가능	사용 불가
페이로드 처리	미리 알릴 필요 없음	엄격한 통신 규약을 갖고 있으며, 모든 메시지는 보내기 전에 알려져야 함
ACID 준수	ACID 준수와 관련된 내용이 없음	자체적인 ACID 기준 존재, 데이터 손상 줄임

EDR 진행 상황

김가영

Yara 룰 설정 방법

이유림 / 정민지

1) ELK 사용법

2) ELK 서버 구축 방법

3) Sysmon

- Winlogbeats

4) Logstash Filter

5) Kibana Visulize

안병휘 / 박민주 / 이안나

기존 EDR의 Fileless / LtoL 공격 탐지 방법 조사

1) Windows Registry Manipulation 탐지 방법

2) Memory Code Injeciton 탐지 방법

3) Script-Based Techniques 탐지 방법

감사합니다