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

2021.09.07
5팀 R&B

주제 : APT 공격 - EDR 탐지

APT 공격과 EDR 탐지로 팀을 나눠 진행할 생각

APT 공격 팀

이찬진(PL)
김지예
장민경
김은주

EDR 탐지 팀

이안나(PL)
김가영
안병휘
박민주
이유림
정민지

APT 환경

* 필요한 서버

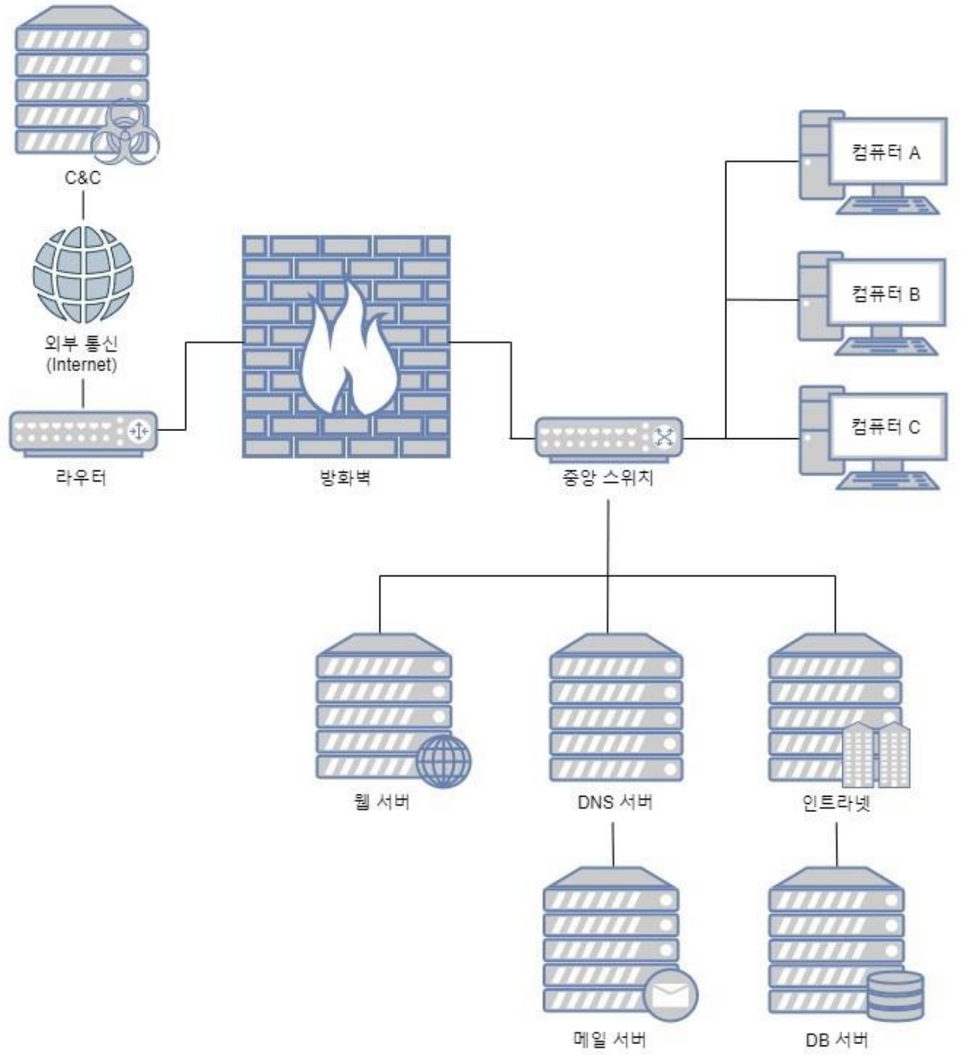
1) 웹 서버

2) DNS 서버 - 메일 서버

3) 인트라넷 - DB 서버

4) 방화벽

5) C&C 서버



APT 시나리오

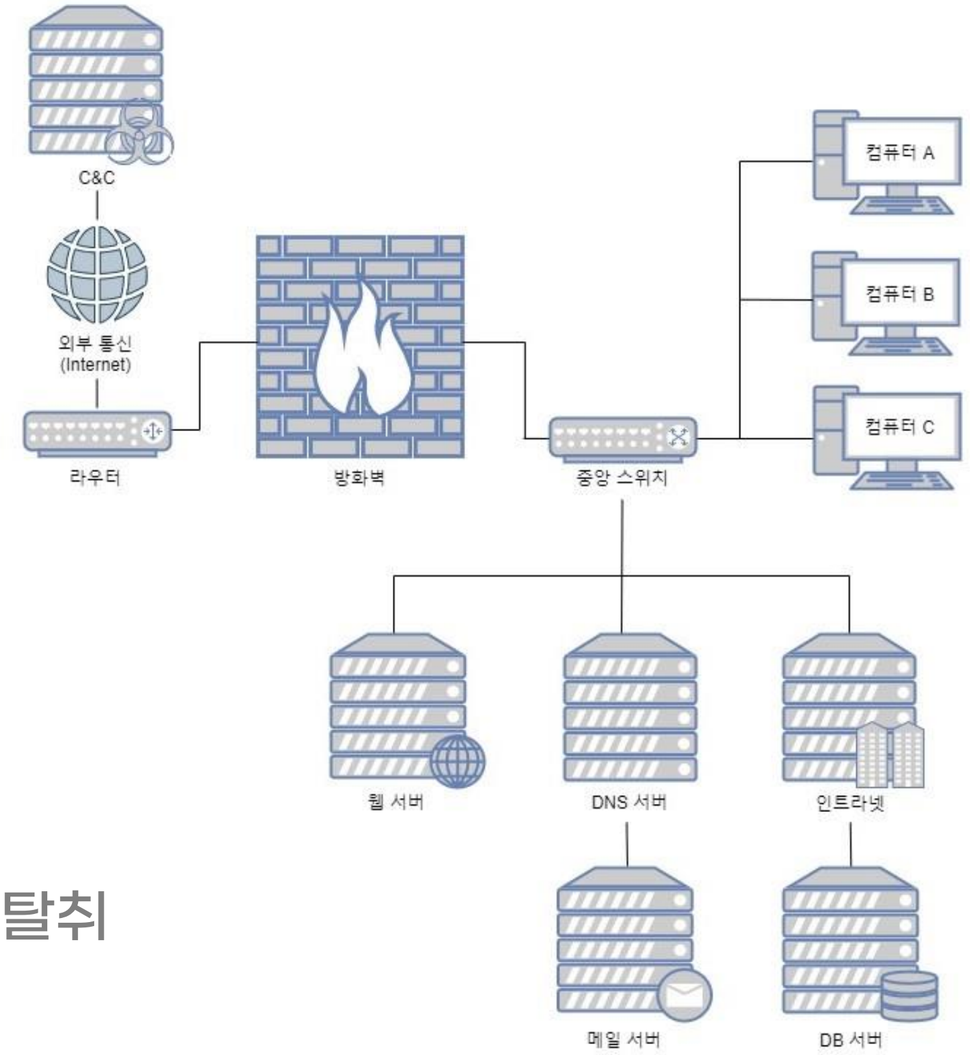
최종 목표

접근 권한이 부장 이상이어야 가능한 폴더에 있는 기밀 문서 탈취

사원을 목표로 악성코드 유포 진행

-> 악성코드 실행 시 사원의 권한을 획득한다 가정

-> 사원의 권한에서 관리자의 권한으로 설정을 바꾸어 DB에 접근 후 기밀 문서 탈취



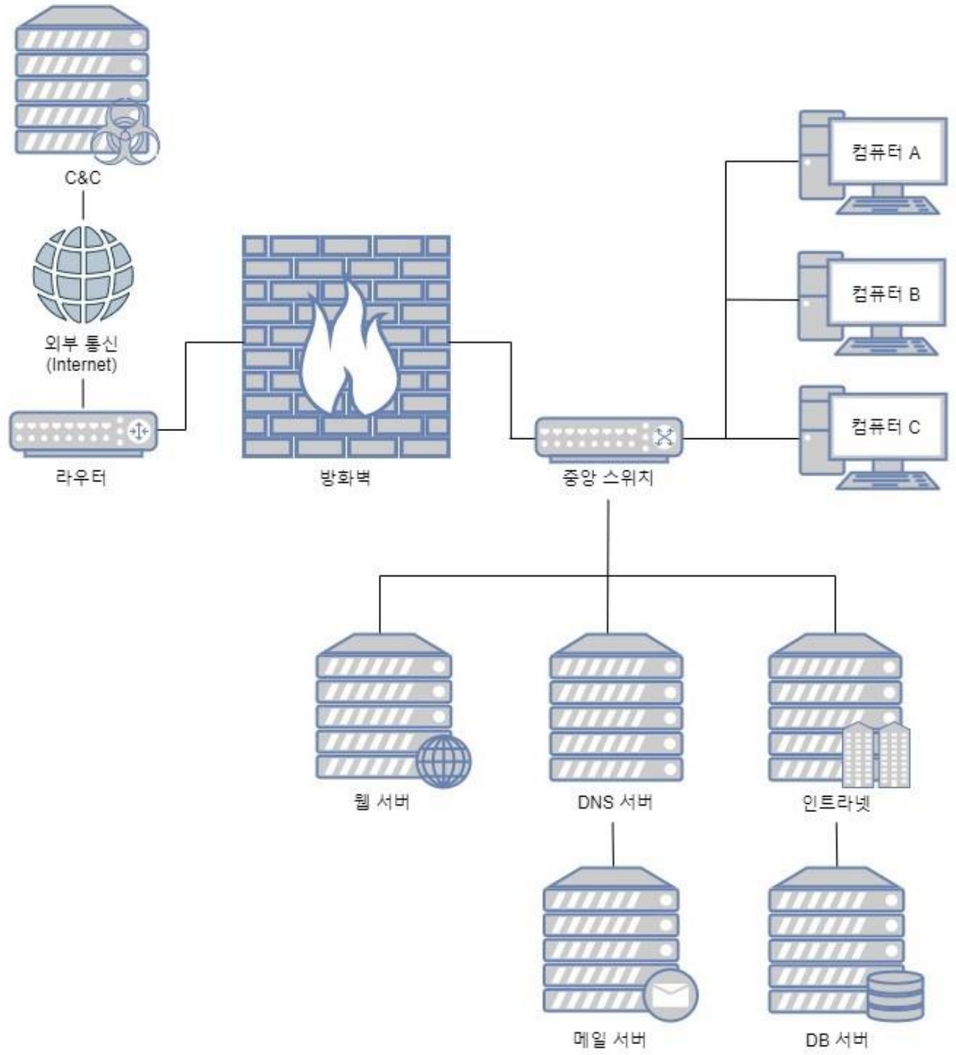
APT 공격 팀

WBS 참고

No.	구 분		항 목	세부사항
1	주제선정		주제 선정	아이디어 도출 및 정리
				보완사항 도출 및 의견 수렴
	보고		주간보고	주간 이슈사항 보고 및 회의
			최종보고	사업 최종 결과보고서 제출
2	공통 학습		서버	서버 역할 및 구축 관련 스터디
			악성코드	악성코드 종류 및 기존의 사례 스터디
3	환경구축	웹 서버	웹 서버 구축	워드 프레스 이용하여 구축
		메일 서버	네임 서버 구축	DNS 서버 구축
			메일 서버 구축	회사 내부 메일 서버 구축
		회사 내부망	인트라넷 구축	회사 내부에서 사용할 환경 구축
			DB 서버 구축	회사 내부 데이터 저장할 DB 구축
		방화벽	내부->외부 설정	내부망에서 외부망으로 접근 설정
			외부->내부 설정	외부망에서 내부망으로 접근 설정
		C&C 서버	C&C 서버 구축	악성코드 제어 서버 구축
4	공격 사전 준비	악성코드	악성코드 제작	스피어피싱에 사용할 악성코드 제작
			악성코드 유포	스피어피싱을 통한 악성코드 유포
		실행 및 유지	악성코드 유지	C&C 서버와 악성코드 연결 유지
		우회	안티 바이러스 우회	백신 프로그램을 피할 방법 고안
			OS 패치 방지	윈도우 업데이트와 같은 OS 패치를 방지
5	모의 해킹	침투	공격 대상자 PC 접속	악성코드를 이용하여 공격 대상자의 권한으로 접속
		검색 및 수집	상위 권한 검색 및 수집	높은 권한의 관리자를 찾기 위해 검색 및 수집
		유출(공격)	권한 탈취	관리자의 권한을 탈취
			데이터 탈취	목표한 데이터를 공격자 PC로 가져오기
		보고	결과 보고	프로그램 사양서, 코드 정의서, 소스코드
6	지원	테스트	중간 테스트	진행 중간에 총 3번의 테스트 진행
			최종 테스트	중간 발표/최종 발표 전 총 2차례 진행

EDR 시스템

악성코드가 포함된 메일을 열었을 때,
그것을 감지하고 위험 신호를 보내는
EDR 시스템을 구축할 예정



EDR 시스템 개발 과정 소개

후킹된 정보를 바탕으로 분석

Windows API 후킹

YARA 룰 탐지

분석 알고리즘 설계

모니터링 보고서 작성

EDR 탐지 팀

WBS 참고

No.	구 분		항 목	세부사항
1	사업관리		주제 선정	아이디어 도출 및 정리
				보완사항 도출 및 의견수렴
	보고		주간 보고	주간 이슈사항 보고 및 회의
			최종 보고	최종 결과보고서 제출
2	자료조사		Windows API	API 동작 및 후킹 과정
			APT	APT 공격 기술 자료 수집(MITRE ATT&CK 참고)
				공격 기술에 대응하는 악성 코드의 API 행위 분석
			기존 EDR 솔루션	기존 솔루션과의 차이점 조사
	개발 환경 구축			C 개발 환경 구축, Github repository 생성
	개발	API 추출	프로세스 핸들 구현	프로세스 핸들 구현
				핸들을 통해 프로세스 모듈 가져오기
			메모리 추출	프로세스 정보수집
				메모리 위치에 접근하여 추출
		분석 및 진단	YARA 룰 탐지	YARA 룰 매치 및 탐지에 따른 적절한 조치
			진단 알고리즘 설계	공격 매커니즘에 따른 알고리즘 설계
			분석 및 진단 시스템 구현	임의 코드 실행 진단
				코드 컴파일 작업 진단
				파일 작업 수행(생성, 수정, 삭제) 진단
				지속성 메커니즘
				UAC 우회 진단
				프로세스 메모리 덤핑
				키로깅 작업
				로그 수정 진단
			분석 결과	레포트 제공 시스템 구현
		대응	대응 시스템	분석 결과에 따른 조치 구현
		보고	최종 보고	최종 프로그램, 소스 코드
3	지원	테스트	중간 테스트	진행 중간에 총 3번의 테스트 진행
			최종 테스트	중간 발표/최종 발표 전 총 2차례 진행
			사후관리	사후관리

감사합니다!