시나리오 제목

한 통의 전화가 부른 디지털 ARMAGEDDON
(전화 피싱과 이중 협박 랜섬웨어 대응 훈련 시나리오)

시나리오 단계

9

시나리오 목적

전화 피싱과 이중 협박 랜섬웨어 APT 공격을 통해 소셜엔지니어링을 대응하고, 침해 탐지, 포렌식 분석, 사고 대응 역량을 학습한다.

시나리오 줄거리

<배경 설정>

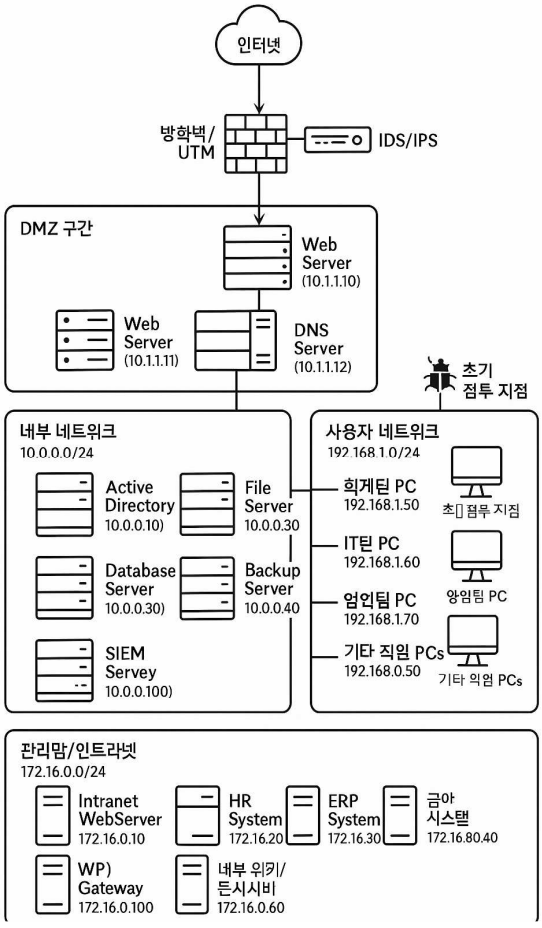
- 피해 기업명: ABC테크
  - 100명 규모의 IT 서비스 기업
  - 업무: 고객 데이터 관리와 웹 서비스 제공
  - 환경: VPN과 Microsoft 365 활용 중

- 공격 그룹명: APT 해커 그룹
  - 목적: 금전적 이익, 한국 IT 기업 표적
  - 전술: 전화 기반 사회공학 기법, 다단계 침투, 이중 협박 랜섬웨어

<시나리오 전개>

- 목요일 오후 2시, 회계팀 A과장에게 "보안팀" 사칭 전화가 온다. 공격자는 'ABC 테크'의 내부 조직도를 활용해 신뢰를 얻고, A과장이 MFA 해제와 TeamViewer 설치하게 한다.
- 이후 Microsoft 365 계정을 장악하고 Active Directory(AD)를 해킹, EternalBlue로 서버 확산, 인트라넷(HR, ERP, 급여) 데이터 탈취, 다크웹 유출, 랜섬웨어로 이중 협박을 가한다.
- 금요일, 파일 암호화와 "PAY OR WE PUBLISH" 메시지로 서비스가 중단되고, 고객 항의와 언론 취재가 이어진다.

시나리오 네트워크 구성도



교육적 시사점

- 소셜엔지니어링, 이중 협박, 인트라넷 보안의 중요성을 강조
- 직원 교육, Zero Trust, 개인정보보호법 준수 등 통합 대응 역량 함양

단계 번호		1
단계 명		전화 피싱 – 신뢰 구축
주요 목표		피해자(A과장) 신뢰 획득 및 정보 수집
유형	**공격**	정찰, 전달
	방어	
주요 활동		1. IT 헬프데스크 직원으로 신분 위장 2. 회사 조직도와 내부 정보를 활용한 신뢰성 확보 3. "보안 점검" 명목으로 정당성 부여 4. 피해자의 업무 패턴 및 시스템 사용 현황 파악 5. MFA 및 계정 정보에 대한 사전 조사 6. 대화 중 피해자 개인정보(예: 부서, 최근 이메일) 유출 유도 7. 긴급성 강조로 피해자 압박 및 의사결정 촉진 8. 후속 공격을 위한 심리적 취약점 식별
주요 사용 도구 및 기술		• VoIP(발신번호 조작) • OSINT(LinkedIn, 회사 홈페이지) • 사회공학적 심리 조작
예상 결과물 및 상태		• 피해자 신뢰 확보 • 시스템 정보 획득 • 2단계 준비

단계 번호		2
단계 명		자격 증명 탈취
주요 목표		MFA 우회 및 원격 접근 권한 획득
유형	**공격**	취약점 악용, 설치
	방어	
주요 활동		1. "보안 점검" 명목으로 MFA 인증 코드 요청 2. 실시간으로 피해자 계정 로그인 시도 3. TeamViewer 등 원격 프로그램 설치 유도 4. 피해자 PC에 대한 완전한 원격 제어 권한 확보 5. 브라우저 저장된 패스워드 및 쿠키 정보 수집 6. 추가 소프트웨어(예: 키로거) 은밀 설치 7. 피해자 파일 시스템 탐색 및 민감 파일 식별 8. 내부 네트워크 연결 상태 확인 및 초기 스캔
주요 사용 도구 및 기술		• TeamViewer • 브라우저 패스워드 추출 • Microsoft 365 접근
예상 결과물 및 상태		• Microsoft 365 계정 장악 • 원격 제어 • 내부망 진입 발판

단계 번호		3
단계 명		AD 침투 및 권한 상승
주요 목표		내부망 진입 및 도메인 관리자 권한 획득
유형	**공격**	취약점 악용, 설치
	방어	
주요 활동		1. VPN 연결 또는 내부망 직접 접근 2. Active Directory 환경 정찰 및 분석 3. Mimikatz를 통한 메모리 덤프 및 해시 추출 4. Pass-the-Hash 공격을 통한 권한 상승 5. 도메인 관리자 계정 탈취 6. AD 그룹 정책 및 사용자 목록 검토 7. 취약한 계정(예: 서비스 계정) 추가 식별 8. 권한 상승 후 초기 명령 실행 테스트
주요 사용 도구 및 기술		• Mimikatz • PowerShell Empire • BloodHound • PsExec
예상 결과물 및 상태		• AD 서버 접근 • 관리자 계정 탈취 • 네트워크 토폴로지 파악

단계 번호		4
단계 명		네트워크 횡적 이동
주요 목표		네트워크 확산 및 핵심 서버 장악
유형	**공격**	명령, 제어
	방어	
주요 활동		1. SMB 취약점(EternalBlue) 악용한 확산 2. 각 서버의 역할 및 중요도 분석 3. 데이터베이스 서버 및 파일 서버 접근 4. 백업 시스템 무력화 5. 보안 솔루션 우회 및 무력화 6. 네트워크 트래픽 모니터링으로 추가 취약점 탐색 7. 원격 명령 실행을 통한 파일 전송 및 실행 8. 횡적 이동 경로 은폐를 위한 로그 조작
주요 사용 도구 및 기술		• EternalBlue • PsExec • Nmap • Cobalt Strike
예상 결과물 및 상태		• 주요 서버 장악 • 자산 목록 확보 • 탐지 회피

단계 번호		5
단계 명		인트라넷 데이터 탈취
주요 목표		민감 시스템 접근 및 데이터 탈취
유형	**공격**	명령, 제어
	방어	
주요 활동		1. 인트라넷 웹서버 취약점 스캐닝 및 공격 2. SQL Injection을 통한 HR 시스템 침투 3. ERP 시스템 내 고객 정보 및 재무 데이터 탈취 4. 급여 시스템 접근을 통한 직원 개인정보 수집 5. 내부 위키 및 문서서버의 기밀문서 다운로드 6. 데이터 유출을 위한 외부 C&C 서버 연결 설정 7. 탈취 데이터 분류 및 우선순위화 8. 인트라넷 트래픽 분석으로 추가 시스템 발견
주요 사용 도구 및 기술		• Burp Suite • SQLmap • PHP 웹쉘 • DNS Tunneling
예상 결과물 및 상태		• 개인정보/기밀문서 탈취 • 유출 채널 확보

단계 번호		6
단계 명		데이터 유출 및 랜섬웨어 준비
주요 목표		데이터 외부 전송 및 랜섬웨어 배포 준비
유형	**공격**	목표달성
	방어	
주요 활동		1. 탈취한 데이터를 암호화하여 외부 서버로 전송 2. Tor 네트워크를 활용한 익명 통신 채널 구축 3. 다크웹에 유출 데이터 일부 공개 (압박 용도) 4. 내부 시스템 백도어 설치로 지속적 접근 보장 5. 추가 공격을 위한 네트워크 토폴로지 완전 매핑 6. 랜섬웨어 배포 이전 최종 정보 수집 7. 유출 데이터 무결성 검증 및 백업 8. C&C 서버와의 안정적 연결 테스트
주요 사용 도구 및 기술		• Tor • 7-Zip • 다크웹 파일 공유 • Nmap
예상 결과물 및 상태		• 데이터 유출 완료 • 백도어 설치 • 랜섬웨어 준비

단계 번호		7
단계 명		랜섬웨어 배포 및 이중 협박
주요 목표		데이터 암호화 및 이중 협박 실행
유형	**공격**	목표달성
	방어	
주요 활동		1. REvil 랜섬웨어 페이로드 동시 배포 2. 백업 파일 삭제 및 복구 불가 처리 3. 중요 데이터베이스 및 파일 암호화 4. 랜섬 노트 생성 및 배치 (데이터 유출 경고 포함) 5. 이중 협박: 암호화 복구비 + 데이터 비공개 보장료 6. 암호화 키 및 복구 지시사항 준비 7. 네트워크 공유 드라이브 전체 암호화 8. 시스템 재부팅 후 랜섬웨어 활성화
주요 사용 도구 및 기술		• REvil • AES-256 • 스케줄 태스크 • 네트워크 드라이브 암호화
예상 결과물 및 상태		• 데이터 암호화 • 서비스 중단 • 이중 협박 랜섬 노트 표시

단계 번호		8
단계 명		사고 탐지 및 침해 분석
주요 목표		보안 사고 인지 및 침입 경로 분석
유형	**공격**	
	방어	탐지, 분석
주요 활동		1. SIEM 다중 알람 및 이상 트래픽 탐지 2. 랜섬웨어 감염과 데이터 유출 동시 발견 3. 네트워크 로그 분석 및 다단계 침입 경로 역추적 4. 인트라넷 시스템 침해 흔적 포렌식 분석 5. 데이터 유출 규모 및 유형 파악 6. 피해 현황 조사 및 법적 대응 필요성 검토 7. 확대된 사고 대응팀 구성 (법무팀, PR팀 포함) 8. 메모리 및 디스크 포렌식으로 증거 수집
주요 사용 도구 및 기술		• Splunk/ELK • Wireshark • EDR(CrowdStrike) • Volatility
예상 결과물 및 상태		• 침입 경로/유출 규모 보고서 • 대응팀 구성 • 법적 신고 준비

단계 번호		9
단계 명		통합 격리, 복구, 사후 조치
주요 목표		위협 차단, 시스템 복구, 재발 방지
유형	**공격**	
	방어	대응
주요 활동		1. 감염된 모든 시스템 완전 네트워크 격리 2. 침해된 모든 계정 비활성화 및 패스워드 강제 재설정 3. 백업을 통한 순차적 데이터 복원 (무결성 검증 포함) 4. 인트라넷 및 웹 애플리케이션 보안 패치 및 재구축 5. 개인정보보호위원회 신고 및 고객 통지 절차 이행 6. 전 직원 대상 심화 보안 교육 실시 (소셜엔지니어링 중점) 7. Zero Trust 모델 기반 보안 정책 전면 개편 8. 24시간 SOC 구축 및 모니터링 체계 강화
주요 사용 도구 및 기술		• VLAN/ACL • Veeam • OWASP ZAP • Okta • SOAR
예상 결과물 및 상태		• 위협 제거 • 시스템 복구 • Zero Trust 구축 • 사고 대응 매뉴얼