랜섬웨어 분석과 가상화폐 분석 추적 실무 과정

2일 교육과정 커리큘럼

INSEC security

랜섬웨어 분석과 가상화폐 분석 추적 실무 과정 (2일)

교육일정	교육내용	교육시간
1일차	**최신 악성코드 및 랜섬웨어 동향** - 랜섬웨어 피해 사례 [국내 및 해외] - 다크웹 / 랜섬웨어 / 사이버 위협 동향	10:00 ~ 10:50
	랜섬웨어 분석 도구 - IDA Pro - 조샌드박스(Joe Sandbox)	11:00 ~ 11:50
	최신 랜섬웨어 분석1 – 크립토락커(CryptoLocker) 랜섬웨어 분석 - 안드로이드 SDK 설치 - 안드로이드 에뮬레이터 구축 - 네트워크 패킷 분석 도구 설치 및 ADB 환경 설정	13:00 ~ 13:50
	최신 랜섬웨어 분석2 – 크립토월(CryptoWall) 랜섬웨어 분석 - 디컴파일(Decompile) 분석 방법 - 퍼미션(Permission) 데이터 분석 - /data/data 디렉토리 데이터 분석 - 오픈 소스 도구를 활용한 바이너리 XML 분석	14:00 ~ 14:50
	최신 랜섬웨어 분석3 – 로키(Locky) 랜섬웨어 분석 - 모바일 랜섬웨어 주요 특징 및 파일 암호화 코드 루틴 분석 - 디컴파일을 통한 안드로이드 내부 코드 정적 분석 실습 - 전문 상세 분석 도구를 활용한 랜섬웨어 샘플 분석 실습	15:00 ~ 15:50
	최신 랜섬웨어 분석4 –펫야(Petya) 랜섬웨어 분석 - 문자 메시지, 통화 기록, 녹음 파일, GPS 정보, 주소록 정보 탈취 특징 이해 - 정보 유출 유형 코드 루틴 분석 - 정보 유출 유형 퍼미션 특징 이해 - 전문 상세 분석 도구를 활용한 스파이웨어 샘플 분석 실습	16:00 ~ 16:50
	최신 랜섬웨어 분석5 – 세르베르(Cerber) 랜섬웨어 분석 - 프로가드(Proguard)로 난독화 된 악성코드 유형 분석 - APKProtect로 난독화 된 악성코드 유형 분석 - 전문 상세 분석 도구를 활용한 난독화 악성코드 분석 실습	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** OllyDBG, IDA Pro, PEiD, Process Monitor, ProcDot, Hex Decompiler UPX, PEView, Autoruns, Process Explorer, Joe Sandbox, Metadefender	

*** 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.**

상담문의 : 02-851-5687

랜섬웨어 분석과 가상화폐 분석 추적 실무 과정 (2일)

교육일정	교육내용	교육시간
2일차	**최신 랜섬웨어 분석6 – 낫 펫야(NotPetya) 랜섬웨어 분석** – 랜섬웨어 실행 및 감염 – 랜섬웨어 동작 방식 및 분석 – 랜섬웨어 관련 가상화폐 주소 추출 및 수집 – 랜섬웨어 관련 가상화폐 주소 분석 및 추적	10:00 ~ 10:50
	최신 랜섬웨어 분석7 – 워너크라이(WannaCry) 랜섬웨어 분석 – 랜섬웨어 실행 및 감염 – 랜섬웨어 동작 방식 및 분석 – 랜섬웨어 관련 가상화폐 주소 추출 및 수집 – 랜섬웨어 관련 가상화폐 주소 분석 및 추적	11:00 ~ 11:50
	최신 랜섬웨어 분석8 – 갠드크랩(GandCrab) 랜섬웨어 분석 – 랜섬웨어 실행 및 감염 – 랜섬웨어 동작 방식 및 분석 – 랜섬웨어 관련 가상화폐 주소 추출 및 수집 – 랜섬웨어 관련 가상화폐 주소 분석 및 추적	13:00 ~ 13:50
	최신 랜섬웨어 분석9 – 메이즈(Maze) 랜섬웨어 분석 – 랜섬웨어 실행 및 감염 – 랜섬웨어 동작 방식 및 분석 – 랜섬웨어 관련 가상화폐 주소 추출 및 수집 – 랜섬웨어 관련 가상화폐 주소 분석 및 추적	14:00 ~ 14:50
	최신 랜섬웨어 분석10 – 콘티(Conti) 랜섬웨어 분석 – 랜섬웨어 실행 및 감염 – 랜섬웨어 동작 방식 및 분석 – 랜섬웨어 관련 가상화폐 주소 추출 및 수집 – 랜섬웨어 관련 가상화폐 주소 분석 및 추적	15:00 ~ 15:50
	최신 랜섬웨어 분석11 – 다크사이드(DarkSide) 랜섬웨어 분석 – 랜섬웨어 실행 및 감염 – 랜섬웨어 동작 방식 및 분석 – 랜섬웨어 관련 가상화폐 주소 추출 및 수집 – 랜섬웨어 관련 가상화폐 주소 분석 및 추적	16:00 ~ 16:50
	최신 랜섬웨어 분석12 – 락빗(Lockbit) 랜섬웨어 분석 – 랜섬웨어 실행 및 감염 – 랜섬웨어 동작 방식 및 분석 – 랜섬웨어 관련 가상화폐 주소 추출 및 수집 – 랜섬웨어 관련 가상화폐 주소 분석 및 추적	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** OllyDBG, IDA Pro, PEiD, Process Monitor, ProcDot, Hex Decompiler UPX, PEView, Autoruns, Process Explorer, Joe Sandbox, Metadefender	

*** 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.**

상담문의 : 02-851-5687

(주)인섹시큐리티 공인 교육센터

교육센터 지점별 안내 [서울 독산 / 제주 함덕] 바로가기

교육일정 안내 바로가기

교육문의 : 02-851-5687

INSEC security