동남권(부울경) 스피어피싱 대응 훈련 운영계획(안)

2023. 10. 31.(화) 팀장 : 이동화 (☎1102)
디지털안전본부 보안인재단 보안인재정책팀 담당 : 김광복 (☎1321)

□ 개요

○ **(추진배경)** 지역거점 훈련장 완공에 따라, 동남권(부울경) 구·재직자 대상 실전형 훈련 제공으로 지역 사이버보안 인재 양성 및 훈련장 홍보 추진

○ **(추진일정)** '23. 11. 20. ~ 12. 10.(온라인 3주), 12. 21.(오프라인 1일)

○ **(훈련과정)** 스피어피싱 대응 훈련(기본, 심화1(HWP), 심화2(MS Office))

○ **(협력방안)** 부산정보산업진흥원, 지역센터와 협력하여 홍보 및 모집 추진

* 오프라인 미니 챌린지 행사 일정에 맞춰 부울경 지역 또는 전국 단위 언론보도 추진

□ 세부 운영프로그램

온라인 훈련	**스피어피싱 대응 훈련 과정** **(1주차)** 스피어피싱 기본 ➡ **(2주차)** 스피어피싱 심화1(HWP) ➡ **(3주차)** 스피어피싱 심화2(MS Office) · **(일정)** 11.20.(월)~12.10(일), 3주 간, 온라인 훈련과정 자율 수강 · **(대상)** 동남권(부울경) 지역 관련업계 재직자, 구직자(대학생 포함) 약 150명 **※ 수료생 상위 30명 오프라인 미니 챌린지 선발**
오프라인 대회	**스피어피싱 대응 미니 챌린지** · **(일시)** 12.21.(목), 09:30~16:00 · **(장소)** 부산 지역거점 실전형 사이버훈련장(동서대 센텀캠퍼스 7F) · **(대상)** 스피어피싱 대응 훈련과정 우수 훈련생 30명(5인 1팀, 총 6팀 구성) · **(방식)** 팀 간 CTF 기반 악성 문서(HWP, MS Office 등) 식별 및 분석

□ 향후계획

○ 동남권(부울경) 지역 훈련생(약 150명) 모집(~11.15)

○ 동남권(부울경) 스피어피싱 대응 훈련 입과 안내(~11.17)

붙임1 동남권(부울경) 스피어피싱 대응 미니 챌린지 개최계획

2023. 10. 31.(화) 팀장 : 이동화 (☎1102)
디지털안전본부 보안인재단 보안인재정책팀 담당 : 김광복 (☎1321)

□ 개요

○ **(일시)** 12월 21일(목), 09:30~16:00(1부: OT, 2부:미니 챌린지 및 간담회)

○ **(장소)** 부산 지역거점 실전형 사이버훈련장(동서대 센텀캠퍼스 7F)

○ **(대상)** 스피어피싱 대응 훈련과정 우수생 30명 선발(5인 1팀, 총 6팀 구성)

※ (11.20~12.10, 온라인 훈련) 부울경 지역 관련업계 재직자, 구직자 등 약 150명 참여

○ **(운영방식)** 팀 간 CTF 기반 악성 문서 식별 및 분석

□ 세부 일정(안)

구 분	시 간		주요 내용
1부 (OT)	09:30~10:30	'60	• 오리엔테이션, 팀 아이스브레이킹
2부 (미니 챌린지, 간담회)	10:30~12:00	'90	• 팀 간 CTF 기반 악성 문서 식별 및 분석
	12:00~13:00	'60	• 훈련생 중식
	13:00~14:20	'80	• 팀 간 CTF 기반 악성 문서 식별 및 분석
	14:20~15:10	'50	• 챌린지 대회 문제풀이
	15:10~15:40	'30	• 부울경 미니챌린지 참여자 대상 간담회
	15:40~16:00	'20	• 챌린지 대회 시상식

□ 시상 계획

구 분	계(팀)	상 금
한국인터넷진흥원장상	1	50만원
부산정보산업진흥원장상	1	40만원
지역정보보호센터장상(동남센터, 울산센터)	4	30만원
계	**6**	**210만원**

※ 상금 및 운영 비용은 운영사 측 폐강된 훈련과정 운영비에서 활용

붙임2 스피어피싱 대응 과정별 세부 훈련내용

□ 스피어피싱 대응 기본과정(1주차)

연번	제목	훈련내용
1	MITRE ATT&CK 프레임워크와 위협 탐지	- MITRE ATT&CK 프레임워크 개요 - MITRE ATT&CK 지식 기반의 구성요소 - 위협에 대한 탐지, 차단, 대응 기술과 전략의 발전 방향
2	파일리스(Fileless) 공격	- 파일리스 공격의 개념 - LoL(Livin Off the land), LoL Binaries - 프로세스 인젝션
3	스피어 피싱 이메일 분석	- 이메일 기반 공격 기법과 유형 - 이메일 전송 과정과 헤더 구조 - 이메일 헤더 분석을 통한 이상징후 식별 방법
4	악성 문서파일 분석을 위해 알아야할 필수 지식	- PE-COFF 파일의 구본 구조 - 프로세스의 가상 주소 공간 - 악성 첨부파일 유형과 구성요소 - 악성 문서파일의 분석 절차
5	쉘코드 분석	- 쉘코드 개요와 분석 목표 - 쉘코드가 사용하는 주요 API - 쉘코드의 바인딩(Binding) API 해시 - 쉘코드에서 임포트하는 API 확인 방법 - 쉘 코드 분석 절차와 디버깅 방법
6	악성 HWP 문서 분석	- HWP 문서 개요와 기본 구조 - HWP 문서 파일 트리아지 (이상징후 식별) - HWP 문서 파일 분석 절차 - 포스트 스크립트 개요
7	악성 MS 오피스 문서 분석	- MS 오피스 문서파일 트리아지 (이상징후 식별) - VBA 매크로 개요와 특징 - DDE/DDEAUTO 개요와 특징

□ 스피어피싱 대응 심화1(HWP) 과정(2주차)

연번	제목	훈련내용
1	악성 HWP 문서의 유형별 분석 전략	- 악성 HWP 문서의 공격 방식에 따른 유형 분류와 시나리오 - 악성 HWP 문서의 유형별 식별 방법
2	포스트스크립트 유형 악성 HWP 문서 파일 분석	- BAT 파일을 이용한 파워쉘 스크립트 실행 코드 패턴
3	익스플로잇 유형 악성 HWP 문서 파일 분석	- 한컴 오피스의 그라데이션 오버플로우 취약점 - 포스트 스크립트의 프로세스 인젝션 루틴 패턴
4	오브젝트 유형 악성 HWP 문서 파일 분석	- OLE 객체로 임베드된 오브젝트의 특징과 분석 방법
5	매크로 유형 악성 HWP 문서 파일 분석 #1	- 매크로 유형 HWP 파일의 특징과 분석 방법

□ 스피어피싱 대응 심화2(MS Office) 과정(3주차)

연번	제목	훈련내용
1	악성 MS 오피스 문서의 유형별 분석 전략	- 악성 MS 오피스 문서의 공격 방식에 따른 유형 분류와 시나리오 - 악성 MS 오피스 문서의 유형별 식별 방법
2	VBA 스크립트 유형 악성 MS 오피스 문서 파일 분석	- 엑셀의 VHS(Very Hidden Sheet) 기능을 이용한 스크립트 은닉 - MSHTA와 자바스크립트를 이용한 공격 루틴 - 파워쉘을 이용한 쉘코드 로딩 루틴
3	DDE 유형 악성 MS 오피스 문서 파일 분석	- 파워쉘 스크립트 실행 루틴 - REGSVR32 및 VBA 스크립트를 이용한 프로세스 인젝션 루틴
4	OLE 오브젝트 유형 악성 MS 오피스 문서 파일 분석	- VBA 기반의 파워쉘 스크립트를 이용한 쉘코드 실행 루틴 - 윈도우 Startup Folder 대상 자바스크립트 모듈 생성 루틴
5	익스플로잇 유형 악성 MS 오피스 문서 파일 분석	- CVE-2017-11882 취약점을 이용한 원격코드 실행 - CVE-2021-40444 취약점을 이용한 자바스크립트 코드 실행