**<Security Factorial 프로젝트 계획서>**

팀명: S!\_악성분석단

|  |  |
| --- | --- |
| 프로젝트 주제명 | **문서형 악성코드 솔루션 방안 탐지** |
| 프로젝트 분야 | 악성코드(문서형) 분석 |
| 프로젝트 기간 | 2023.04.07. ~ 2023.06.31. |
| 참여 인원 | 김정호, 김지태, 신정훈, 이정민, 양인규, 조승현, 최기상 |
| 지도 멘토 | - |
| 환경구성 (개발/인적) | 문서형 악성코드에 관심 있는 사람 |
| 프로젝트 개요 (배경, 주요 내용 요약) | 산업과 인터넷의 연계에 따라 다양한 악성 행위들이 인터넷 상에서 발견되고 있다. 해당 악성 행위들 중 대표적인 것들로는 스펨 메일이 있으며, “채용공고 입사지원 드립니다.” 와 “합격을 축하드립니다.”와 같은 매력적인 제목을 사용하여 사용자로 하여금 누르도록 유도하고 특정 파일을 다운받게 하여 사용자의 PC를 감염시키도록 한다.  파일 종류 중 대다수는 docx, pdf와 같은 문서형이며 이에 따른 피해 역시 만연하다.  피해 사례를 줄이고 사용자로 하여금 악성코드의 위험성을 재인식하고자 문서형 악성코드 분석 및 솔루션을 제안하고자 한다. |
| 프로젝트 목적 | 문서형 악성코드가 만연함에 따라 대응 방안 및 탐지 방안 관련 솔루션 제시 |
| 프로젝트 수행 방법 | 프로젝트 수행 방법은 다음과 같이 3단계로 분류된다.  **첫 번째**, 문서형 악성코드 관련 배경 지식 습득   * 문서형 악성코드에서 사용되는 스크립트 언어인 VBA(Visual Basic for Application)에 대한 공부를 진행 * 문서마다 가지고 있는 고유 구조체에 대하여 공부 * 문서형 악성코드 특징과 관련 논문 읽고 문서형 악성코드 종류 파악   **두 번째**, 문서형 악성코드 분석 및 시현   * 배경지식 기반 문서형 악성코드 보고서 훑고 시현 * 문서형 악성코드 실행에 따른 컴퓨터 아티팩트 분석 * (시간이 남을 시)스크립트 형 악성코드뿐만 아닌 문서의 취약점을 바탕으로 시현된 악성 코드 대해서 분석 예정   **세 번째**, 분석 기반 솔루션 제안 및 분석 보고서 게시   * 문서형 악성 코드에 대한 솔루션 제안 관련 논문 쓰기 * 동아리 블로그에 분석한 문서형 악성 코드 보고서 게시 |
| 프로젝트 기대효과 | ‘문서형 악성코드 솔루션 방안 탐지’ 라는 주제로 진행하기 위해 문서형 악성코드 분석, 악성 행위로 인한 아티팩트 연구 그리고 해결책 고안과 같은 행위를 수행해야 한다.  따라 다음 행위를 통해 얻을 수 있는 기대효과로는 다음과 같겠다.   1. 문서형 악성코드 분석에 따른 쉘 스크립트 사용법 및 API 종류 습득 2. 윈도우 아티팩트 종류 습득 및 역추적 고안에 따른 CS 지식 습득   사회적으로 기대할 수 있는 효과는 다음과 같다.   1. 솔루션 제시에 따른 문서형 악성코드 대응 방안 증가 2. 사용자의 인식 향상 및 감염 사례의 감소에 따른 사회적 문제 해소 |
| 프로젝트 수행 시 문제점 (내외부 요인 기술) | 해당 프로젝트 진행에 앞서 우려되는 부분은 문서형 악성코드를 분석해본 경험이 없다는 것이다.  이러한 이유로 선행 연구에 있어 어떠한 Task를 미리 진행해야 하는지, 해당 Task에 따른 산출물이 어떠한 것이 나올 수 있는지에 대한 시간 소요가 클 것이라 예상된다. |
| 필요 자원 | 문서형 악성코드 샘플 및 문서형 악성코드 분석 관련 도서 |

※ 작성 분량 제한 없습니다. 최대한 구체적으로 작성 부탁드립니다.