|  |  |  |
| --- | --- | --- |
| 머신러닝을 이용한 악성코드 탐지 프로그램 | 07-26  2017 | |
| 작성자 : 모의해킹 14기 권주승 김예지 박주연 이현준 | | **#SHUT DOWN** |

목차

[1. 프로젝트 개요 4](#_Toc488334743)

[1.1 프로젝트 정의 및 목표 4](#_Toc488334744)

[1.1.1 정의 4](#_Toc488334745)

[1.1.2 목표 4](#_Toc488334746)

[1.2 주제 선정 동기 4](#_Toc488334747)

[1.3 팀원 및 역할 5](#_Toc488334748)

[1.4 프로젝트 일정 5](#_Toc488334749)

[1.5 부분별 기대효과 5](#_Toc488334750)

[1.5.1 AS-IS 5](#_Toc488334751)

[1.5.2 TO-BE 5](#_Toc488334752)

[2. 악성코드 분석과정 5](#_Toc488334753)

[2.1 분석 환경 5](#_Toc488334754)

[2.2 정적 분석 5](#_Toc488334755)

[2.3 동적 분석 5](#_Toc488334756)

[3. 악성코드 탐지 프로그램 개발 5](#_Toc488334757)

[3.1 개발 환경 5](#_Toc488334758)

[3.2 머신러닝 5](#_Toc488334759)

[3.2.1 머신러닝 소개 5](#_Toc488334760)

[3.2.2 머신러닝 학습 알고리즘 6](#_Toc488334761)

[3.3 동작 원리 6](#_Toc488334762)

[3.3.1 MD5 해시값 비교 6](#_Toc488334763)

[3.3.2 VirusTotal 분석 6](#_Toc488334764)

[3.3.3 머신러닝 학습&탐지 6](#_Toc488334765)

[3.4 실행 결과 6](#_Toc488334766)

[3.5 산출물 6](#_Toc488334767)

[4. 프로젝트 결론 및 추후과제 6](#_Toc488334768)

[4.1 결론 6](#_Toc488334769)

[4.2 추후과제 6](#_Toc488334770)

[5. 참고자료 6](#_Toc488334771)

# **프로젝트 개요**

## **1.1 프로젝트 정의 및 목표**

### 1.1.1 정의

본 프로젝트는 한국정보기술연구원에서 진행하는 정보보안 전문가 모의해킹 14기 ‘Shutdown’ 팀의 프로젝트 결과 보고서이다. 본 보고서는 전 교육과정에 대한 실무 응용 능력과 국내 보안 기술 향상에 기여하고자 한다

본 프로젝트는 2017년 최근 가장 큰 이슈가 되고 있는 악성코드와 랜섬웨어를 미리 탐지하여 감염에 예방하고자 한다. 사이버 공격이 고도화 됨에 따라 악성코드가 지능적으로 발전하고 기존의 방식으로 탐지가 어려워져 감염 사례가 늘고 있는데 머신러닝기반으로 차세대 탐지 보안 솔루션을 제시

### 1.1.2 목표

일정 단계를 거쳐 악성코드와 랜섬웨어를 탐지하고

대응방안을 제시하여 최신 보안 취약점을 파악함으로써 보안 사고를 예방하는데 그 목적을 둔다.

## **주제 선정 동기**

## **팀원 및 역할**

## **프로젝트 일정**

## **부분별 기대효과**

### 1.5.1 AS-IS

### 1.5.2 TO-BE

# **악성코드 분석과정**

## **2.1 분석 환경**

## **2.2 정적 분석**

## **2.3 동적 분석**

# **악성코드 탐지 프로그램 개발**

## **3.1 개발 환경**

## **3.2 머신러닝**

### 3.2.1 머신러닝 소개

### 3.2.2 머신러닝 학습 알고리즘

## **3.3 동작 원리**

### 3.3.1 MD5 해시값 비교

### 3.3.2 VirusTotal 분석

### 3.3.3 머신러닝 학습&탐지

## **3.4 실행 결과**

## **3.5 산출물**

# **프로젝트 결론 및 추후과제**

## **4.1 결론**

## **4.2 추후과제**

# **참고자료**