intro

악성코드 분석의 목표

- **악성코드 분석의 목표는 보통 네크워크 침입 대응에 필요한 정보를 알아내기 위함**
- **전반적으로 정확히 무슨 일이 발생했는지 감염된 시스템과 파일은 무엇인지 확실히 인지**
- 의심스러운 **특정 바이너리가 하는 행위와 네트워크에서 탐지하는 방법과 피해** 범위를 측정

악성코드 분석 기법

- **악성코드 분석을 수행하게 되면 거의 대부분은 대상자가 읽을 수 없는 형태의 악성코드 파일**

⇒ 의미를 알기위해서 여러가지 도구들과 기법을 활용

→ 많은양의 정보들 중 의미가 있는 정보들을 획득

- 악성코드에는 분석기법이 크게 2가지로 나뉨
  - **정적분석**
    - 악성코드를 실행하지 않고 분석
  - **동적분석**
    - 악성코드를 실행하면서 분석

⇒ 2가지에 따라서 기초 또는 고급으로 분류 할 수 있음

기초 정적 분석

- 명령어를 보지 않고 실행파일을 조사
  - **파일의 악성 여부를 확인**
  - **기능정보와 그 정보를 이용해서 간단한 네크워크 시그니처를 생성**

    → **직관적이고 신속히 수행이 가능**하지만 정교한 악성코드 분석에는

    비효율적, 중요한 행위를 놓칠 수 있음

기초 동적 분석

- 악성코드를 실행시킨 후 감염 흔적을 제거하거나 유효한 시그니처를 만들거나

  두 가지 모두를 위해 시스템의 행위 관찰(악성행위)

⇒ 악성코드를 안전하게 실행하기 위해서 자신의 환경을 피해가 없는

연구용으로 사용이 가능한 환경을 설정해야 함

→ 기초 정적 , 동적 분석은 프로그래밍 지식이 없는 사람들도 가능하지만

중요한 행위들을 놓칠 수 있음 - 모든 악성코드에 효과적이지 않음

고급 정적분석

- **프로그램의 명령어가 하는 작업이 무엇인지 파악할** 목적

  실행 파일을 디스어셈블러로 로드해서 악성코드의 내부를 역공학

- 명령어는 CPU가 실행 → 프로그램의 정확한 내용을 알 수 있음

  → 기초 정적 분석 보다 어렵고 디스어셈블리에 특화된 지식, 코드 구성

  윈도우 운영체제 개념을 요구한다

고급 동적 분석

- 디버거를 이용해서 동작하는 악성 실행 파일의 내부 상태를 점검
  - 실행파일에서 세부 정보들을 추출하는데 다른 방식을 제공

악성코드 유형

- **악성코드가 시도하는 행위를 먼저 추측하고 그런 가설을 확인**하는 방법으로 분석 속도를 높임 → 악성코드가 일반적으로 하는 행위를 알고 있다면 최선의 추측이 가능함

악성코드의 범주

- **백도어 (Backdoor)**
  - 공격자의 접근을 허용할 목적으로 컴퓨터에 설치하는 악성코드

    공격자가 부분 인증이나 무인증으로 컴퓨터에 접속해서 로컬 시스템 에서

    명령어 실행이 가능

- **봇넷 (Botnet)**
  - 공격자가 시스템에 접속 할 수 있다는 점에서 백도와 유사

    하지만 동일한 봇넷에 감염된 모든 컴퓨터가 하나의 C&C (명령 제어 서버) 로 부터 동일한 명령어를 수신
- **다운로더 (Downloader)**
  - 추가 악성코드를 다운로드하고 설치
- **정보 유출 악성코드 (Information - stealing malware)**
  - 피해자의 컴퓨터에서 정보를 수집해서 공격자에게 수신

    주로 온라인 뱅킹이나 이메일 같은 온라인 거래에 사용

    ex) Keylogger , sniffing, password hash collector
- **실행기 (launcher)**
  - 다른 악성프로그램을 실행 할 때 사용하는 악성 프로그램
    - 상위권한이나 은폐를 위해서 사용
- **루트킷 (root kit)**
  - 코드 내부에서 자신의 존재를 숨기는 악성코드
- **스케어 웨어 (scareware)**
  - 감염된 사용자가 뭔가를 구매하게 겁을 주는 악성코드
- **스팸 전송 악성코드 (spam-sending malware)**
  - 사용자의 장비를 감염시켜서 지속적으로 스팸을 보냄
- **웜/바이러스 (worm/virus)**
  - 자신을 복제해 추가적인 피해를 발생

악성코드 분석의 일반 규칙

1. **세부사항에 집착하지 말것**
   - 일반적인 악성코드는 크기가 방대해서 전부 다 이해 불가
   - **주요 특징에 초점을 둘것**

2. **작업은 여러가지 도구와 툴들이 있음**
    - 진전이 없으면 헤메지 말고 바로 다음 넘어갈 것
3. **고양이와 쥐 게임**
    - 새로운게 생기면 제작자는 분석 방법을 회피 할 수 있는 기법으로 공격

      이런 기법을 인지하고 이 과정에 대응이 가능해야함
