

과정명	
11차시	악성코드 분석

### <1> 악성코드 분석 환경 구축

#### [1] 악성코드

- 악성코드는 악의적인 목적을 위해 작성된 컴퓨터 프로그램 또는 소프트웨어를 말함
- 1990년대까지만 해도 주로 컴퓨터 바이러스가 이러한 악성코드 대부분을 차지 했으나 네트워크의 발전과 더불어 이메일이나 웹을 통한 감염이 증가하면서 최근에는 감염 방법이나 증상들이 다양한 악성코드가 발생함
- 악성코드가 악성 행위를 하기 위해서는 공격 대상이 되는 컴퓨터 혹은 모바일 기기에 설치되어야 하는데, 이를 위해 악성코드를 설치하기 위한 다양한 수단을 사용함

#### [2] 악성코드의 종류와 특징

- 악성코드는 하는 행위와 전파 및 실행 방법에 따라 다양한 형태로 구분됨
  - (1) 트로이 목마
    - 개인정보 유출을 목적으로 다른 프로그램 내부에 기생하며 동작하는 악성코드
    - 자기 복제 능력이 없고 다른 프로그램을 감염 시키지 않기 때문에 트로이 목마 프로그램만 삭제하면 피해는 없음
    - 주로 이메일의 링크를 클릭하거나 인터넷 검색을 통해 내려 받는 불법 소프트웨어가 실행 또는 설치될 때 전파됨
    - PC 내 저장된 중요한 정보를 외부의 공격자에게 유출하는 것이 주 목적
    - 최근의 악질적인 트로이 목마는 프로그램을 삭제하면 컴퓨터를 무한 리부팅하게 하는 등 시스템을 망가뜨리는 자폭 기능을 가지고 있기도 함
  - (2) 웜
    - 독자적으로 실행되며 자기 스스로를 다른 시스템으로 전파시키는 악성코드
    - 막대한 시스템 과부하를 일으켜 바이러스를 능가하는 피해를 줄 수 있음
    - 확산속도가 매우 빨라 단시간 내 대규모 피해를 입히는게 가능함
  - (3) 스파이웨어
    - 다른 사람의 컴퓨터에 잠입하여 개인정보를 빼내거나 광고용으로 사용되는 소프트웨어
    - 사용자 컴퓨터의 자원을 잠식함
  - (4) 악성 봇
    - 사용자의 컴퓨터를 제어하도록 만들어 주는 프로그램
    - 감염된 컴퓨터에서 일반 프로세스처럼 존재하지만 공격자가 원격으로 제어
    - 악성행위로는 바이러스 전파, 스팸메일 전송, DDoS 공격 등이 있음
  - (5) 스텝스넷
    - 산업 자동화 제어 시스템을 겨냥해 제작된 악성코드
    - 산업설비에 침투하여 제동장치 오작동 등의 치명적인 타격을 입힐 수 있음
  - (6) 백도어
    - 시스템 접근 시 정상 절차 없이 접근하도록 돕는 도구
    - 최초 침입 후 재침입 시의 통로로 활용됨
  - (7) Key-logger
    - 키보드로부터 입력을 감시하고 기록하여 공격자에게 전송
    - 아이디나 패스워드 등의 데이터가 탈취될 수 있음

(8) 애드웨어(Adware)

- 다른 프로그램이 실행될 때 자동으로 광고가 표시되는 악성코드
- 방치할 경우 컴퓨터를 사용할 수 없을 정도로 불편하게 만들거나 애드웨어인 척 하는 트로이 목마의 기능이 있을 수도 있기 때문에 가능한 제거해야 함

(9) 랜섬웨어

- 기업을 타겟으로 사회공학적인 방법을 이용 및 스크립트 실행을 유도하여 문서를 모두 암호화하고 복호화를 대가로 금전이나 비트코인을 유도하게 하는 프로그램

(10) 바이러스

- 악성코드 중 가장 오래된 종류 중 하나로 자기자신을 다른 프로그램의 내부에 복제하는 악성코드
- 독립적인 실행 파일이 있지 않고 다른 프로그램 내부에 들어가 있음
- 자신의 숙주 프로그램 실행 시 자신도 같이 실행되는 방식으로 악질적인 바이러스인 경우에는 자기 복제뿐만 아니라 다른 파일을 삭제하거나 시스템을 망가뜨리는 등의 악성 행위를 수행하기도 함
- 최근에는 맥 운영체제, 리눅스, 안드로이드를 대상으로 하는 바이러스 증가
- 공격 대상에 따라 부트 바이러스, 파일 바이러스, 부트/파일 바이러스, 매크로 바이러스로 구분

부트 바이러스	<ul style="list-style-type: none"><li>◆ 운영체제가 실행되기 전 먼저 실행되어 운영체제가 정상적으로 부팅되지 못하도록 하거나 시스템 파일을 감염시켜 시스템을 매우 느리게 만듦</li><li>◆ 플로피 디스크가 사용되던 1990년대에 주로 활약하던 바이러스</li><li>◆ 브레인, 몽키, 미켈란젤로 바이러스 등</li></ul>
파일 바이러스	<ul style="list-style-type: none"><li>◆ 바이러스가 메모리에 상주하면서 실행되는 모든 파일에 자신을 복제하여 감염시키는 바이러스</li><li>◆ 일반적으로 바이러스라고 지칭하는 실행 파일 감염 바이러스</li><li>◆ 예루살렘, 일요일, 전갈, 까마귀 등</li></ul>
부트/파일 바이러스	<ul style="list-style-type: none"><li>◆ 부트 섹터와 실행 파일 두 개 모두를 노리는 바이러스</li><li>◆ 침입자, 안락사, 에볼라 등</li></ul>
매크로 바이러스	<ul style="list-style-type: none"><li>◆ 감염 대상이 오피스 파일</li><li>◆ 매크로 = 문서 파일에 포함된 소스코드의 한 종류</li><li>◆ 오피스 프로그램이 매크로가 포함된 문서 파일을 읽어 들이면 매크로도 같이 읽고 매크로의 지시에 따라 연산을 하거나 다른 파일을 읽고 쓰거나 다른 프로그램을 실행을 함</li><li>◆ 매크로 바이러스는 오피스 파일 내 매크로에 악성코드를 넣어 악의적인 행동을 하도록 함</li></ul>

- PC가 바이러스에 감염되면 보통 CPU 용량 부족, 하드디스크 I/O 증가, 하드디스크 용량 부족, 파일크기나 시간의 변경 등의 현상이 발생함. 하지만 이러한 증상의 원인이 반드시 바이러스라고 단정 지을 수는 없으며 바이러스에 의한 피해 유무를 파악하려면 백신 프로그램을 실행시켜 확인해야 함

[3] 악성코드 분석 방법

- 악성코드 분석 방법은 악성코드를 실행하지 않고 분석하는 정적 분석, 악성코드를 직접 실행하여 분석하는 동적 분석 그리고 완전 자동화 분석으로 분류할 수 있다.

(1) 정적 코드 분석

- 분석 중 악성코드를 실행하지 않는 기법으로 프로그래밍 코드레벨의 지식을 요구함
- 정적 분석의 시작은 실행 프로그램 파일에서 소스를 역추출하는 작업으로, 실행파일에서 소스를 추출하는 방법을 디스어셈블링 또는 리버싱이라고 함
- 역추출되는 소스는 해커가 원래 개발했던 고급 언어가 아닌 기계어나 어셈블리어 같은 저급 언어로 소스 분석이 쉽지 않음

(2) 동적 코드 분석

- 악성코드를 실행시켜 행위를 분석하는 과정으로 악성코드가 실행될 때 생기는 변화를 확인함
- 시스템 감염으로 시스템 상의 손상을 유발할 수 있으므로 안전한 환경에서 수행되어야 하는데 이러한 특성 때문에 VMWare와 같은 가상 머신을 많이 이용함

### (3) 완전 자동화 분석

- 하루에도 수 만개씩 쏟아지는 악성코드를 전문 분석가들이 하나씩 분석할 수 없어 사용

## [4] 악성코드 수집 사이트

- 하루에도 수십 만 개가 유입되는 악성코드를 수집하여 통계, 분석하는 경로를 통해 상세한 악성코드 분석이 가능하도록 함

### (1) 바이러스 쉼어

- 윈도우 실행 악성 코드, 안드로이드 악성 앱 등 다양한 파일의 공유
- 토렌트 및 압축 파일로 다량의 악성코드 샘플을 공유하여 최근 배포되고 있는 악성코드 동향을 파악할 때 통계를 내어 활용 가능

### (2) 멀웨어 트래픽 분석 사이트

- 사이트에서 배포되고 있는 악성코드에 대한 네트워크 분석과 다운로드되는 파일들에 대한 분석 사례를 보여줌
- 네트워크 패킷 파일, 샘플파일, 피들러 분석결과를 다운로드하고 직접 실행해보며 분석 가능

### (3) 제로서트

- 사이트를 크롤링해 페이지 내에 악성코드가 포함되는지의 여부를 판단
- 실시간으로 배포되고 있는 악성코드 파일을 신속하게 파악할 수 있고, 해당 배포 파일이 악성코드일 경우 배포 사이트에 보안적인 이슈가 발생했다는 의미이기도 하므로 신속한 조치를 하는데 많은 도움이 됨
- 각 분석된 페이지는 공격자가 어떤 패커를 사용하고 있는지 알려주고, 바이러스 토탈 등의 대외적인 서비스와 연계되며 배포된 파일의 샘플 다운로드가 가능

## [5] 취약점

- 공격자의 시스템 침투를 위한 교두보가 되는 약점으로, 취약점 공격을 위해 공격자는 시스템의 약점에 접속할 수 있는 적어도 하나의 툴이나 기법이 필요함
- 취약점은 시스템의 민감성 또는 시스템의 결함, 결함에 대한 접근, 결함에 대한 익스플로잇 가능성의 세 가지 관점에서 볼 수 있음

### (1) 취약점 공격 방법

#### 1) 시스템 취약점 공격 방법

- 시스템의 프로그램 취약점을 이용한 해킹 기법인 버퍼 오버플로우나 포맷 스트링과 같은 방식들을 이용하여 취약한 시스템을 공격하여 해당 시스템에 접속, 관리자 권한을 획득하는 것

버퍼 오버플로우	<ul style="list-style-type: none"> <li>◆ 데이터의 형태와 길이에 대한 불명확한 정의로 인한 문제점 중 '길이에 대한 명확하지 않은 정의'를 악용한 덮어쓰기로 발생</li> <li>◆ 정상적인 경우에는 사용되지 않아야 할 주소 공간에 공격자가 임의의 코드를 덮어쓰는 것</li> </ul>
포맷 스트링	<ul style="list-style-type: none"> <li>◆ 데이터의 형태와 길이에 대한 불명확한 정의로 인한 문제점 중 '데이터 형태에 대한 명확하지 않은 정의'를 이용한 공격</li> <li>◆ C언어의 경우 %s와 같은 문자열을 가리켜 포맷 스트링이라고 하는데 포맷 스트링 공격은 이 포맷 스트링인 %s의 값을 바꾸는 것</li> </ul>

#### 2) 네트워크 취약점 공격 방법

- 네트워크 취약점이나 컴퓨터 네트워크의 취약한 사설망에 불법적으로 접근하거나, 정보 시스템에 유해한 영향을 끼치는 공격방식으로 ARP스푸핑, DNS 스푸핑, DDoS 등이 있음

ARP스푸핑	<ul style="list-style-type: none"> <li>근거리 통신망 하에 Mac Address를 이용하여 상대방의 데이터 패킷을 중간에 가로채는 중간자 공격 기법</li> <li>과정               <ol style="list-style-type: none"> <li>① 공격자는 공격 대상 시스템에 주로 통신하는 시스템 감시</li> <li>② 공격자가 대상 시스템에 주로 통신하는 시스템의 MAC 주소가 공격자 시스템 MAC 주소라고 알림</li> <li>③ 대상 시스템은 공격자 시스템으로 프레임을 만들어 전송</li> <li>④ 공격자를 프레임을 읽어보고 실제 목적지로 패킷 전송</li> </ol> </li> </ul>
DNS스푸핑	<ul style="list-style-type: none"> <li>DNS 서버보다 빠르게 공격 대상에게 DNS 리스폰 패킷을 보내, 공격 대상이 잘못된 IP주소로 웹 접속을 하도록 유도하는 공격</li> <li>과정               <ol style="list-style-type: none"> <li>① 공격자가 DNS 클라이언트가 DNS 서버에 보내는 쿼리를 가로챈</li> <li>② 공격자가 준비한 DNS에서 대상 시스템이 보낸 DNS 쿼리에 대한 응답을 자신이 생성한 위조 웹 서버의 주소로 먼저 알림</li> <li>③ 클라이언트는 공격자에게서 받은 DNS를 받고 실제 DNS 서버가 보낸 응답을 버림</li> <li>④ 클라이언트 컴퓨터가 위조된 웹 사이트에 접속</li> </ol> </li> </ul>
DDoS	<ul style="list-style-type: none"> <li>수십~수백만 대의 PC를 원격 조종하여 특정 웹사이트에 동시 접속시켜 단시간 내에 과부하를 일으키는 공격</li> <li>단순한 서버 마비로 인한 업무 연속성 중단이 목적</li> </ul>

## <2> 악성코드 분석 도구 운용

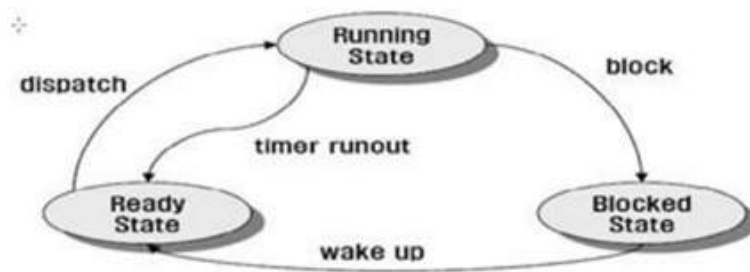
### [1] 시스템 분석 도구 운용

#### (1) PE 파일

- 유닉스 COFF를 기반으로 윈도우 3.1로부터 지원된 실행파일 형식으로 의식성이 있으며, 플랫폼에 독립적인 파일
- 일부 악성코드는 PE 파일을 사용하거나 변조하기 때문에 PE 파일의 전체적인 구조 및 PE 헤더에 대한 이해가 있어야 악성코드의 분석이 가능함
- PE 파일의 종류로는 실행 계열인 EXE, SCR, 라이브러리 계열인 DLL, OCX, CPL, DRV, 드라이브 계열인 SYS, VXD, 오브젝트 파일 계열인 OBJ 등이 있음
- 크게 PE 헤더와 PE 바디로 구성. PE 헤더는 파일을 실행하기 위한 전반적인 정보가 구조체 형식으로 저장되어 있으며, PE 바디는 코드 섹션, 데이터 섹션, 리소스 섹션으로 나누어져 파일의 실제 코드, 데이터, 리소스 등의 내용들이 존재함

#### (2) 프로세스

- 프로세스는 레지스터, 스택, 포인트, 프로그램, 데이터 등의 집합체로 실행 중인 프로그램 인스턴스를 의미함



#### (3) 악성코드 분석 툴

##### 1) 프로세스 모니터

- 각 프로세스 별로 파일이나 레지스트리 등에 어떤 동작을 수행하는지 확인하여 악성코드가 레지스트리에 어떤 동작을 하는지 실시간으로 모니터링하기 위해 사용하는 프로그램

##### 2) 오토런즈(Autoruns)

- 운영체제에 등록된 시작 프로그램 중 기존과 다른 의심되는 프로그램이 등록되었는지 확인 가능한 프로그램

- 운영체제에서 기본적으로 제공하는 msconfig와 달리 오토런즈는 별도 설치가 필요한 대신 알려진 모든 윈도우 시작 프로그램 표시, 시작 프로그램의 전자서명된 인증서 검증, 검증된 마이크로소프트 서비스 숨기기 등 여러 다양하고 편리한 기능을 제공함

### 3) 작업관리자

- 악성코드 실행 확인을 위해 현재 실행되는 프로세스 확인
- 이전과 다른 독특한 이름의 프로세스가 실행되고 있다면 그 이름을 검색하여 악성코드인지 판단이 가능하며, 네트워크 자원이나 CPU 자원을 많이 소모하는 프로세스도 악성코드일 가능성이 큼

## [2] 루트킷, 스크립트 분석 도구 운용

### (1) 루트킷

- 자신 또는 다른 소프트웨어의 존재를 숨기고 허가되지 않은 컴퓨터나 소프트웨어의 영역에 접근할 수 있게 설계된 프로그램
- 루트킷의 설치의 자동 혹은 공격자가 루트 권한이나 관리자 접근을 획득하였을 때 가능
- 루트킷의 기능으로는 프로세스나 스레드 감추기, 파일과 폴더 감추기, 프로세스 보안 설정 변경 및 제거, 레지스트리/서비스 숨기기, 네트워크 정보 숨기기, 스니핑 및 시스템 제어 등이 있음
- 루트킷은 사용자 모드와 커널모드로 구분할 수 있음

사용자 모드 루트킷	<ul style="list-style-type: none"> <li>◆ 특정 프로세스에 사용한 인젝션 된 DLL 파일들을 교체하거나 IAT 후킹, API Entry 패치 방법들을 사용해서 원하는 정보들을 숨기는 동작</li> </ul>
커널 모드 루트킷	<ul style="list-style-type: none"> <li>◆ 윈도우 Native API 커널드라이브와 Win32 응용 프로그램 간의 데이터를 조작함으로써 공격자를 숨김</li> </ul>

- 루트킷의 종류로는 Hacker Defender, Vanquish, FU, NT Rootkit, AFX rootkit이 있으며, 현재 공개된 대부분의 루트킷은 이 루트킷들의 변종

Hacker Defender	<ul style="list-style-type: none"> <li>◆ 가장 광범위하게 사용되며 다양한 변종이 존재</li> <li>◆ 프로세스, 네트워크, 시작프로그램, 레지스트리, 서비스 등을 숨기는 가장 많은 기능 제공</li> </ul>
Vanquish	<ul style="list-style-type: none"> <li>◆ DLL 인젝션 기법 사용</li> <li>◆ 프로세스, 네트워크, 레지스트리, 서비스를 숨기는 기능 및 로그인 정보 기록 기능 제공</li> </ul>
FU	<ul style="list-style-type: none"> <li>◆ EPROCESS의 링크 조작을 통한 프로세스 숨기기 기능 제공</li> </ul>
NT Rootkit	<ul style="list-style-type: none"> <li>◆ 초기 윈도우 루트킷</li> </ul>
AFX rootkit	<ul style="list-style-type: none"> <li>◆ 코드 인젝션과 API 후킹 사용</li> <li>◆ 프로세스, 모듈, 핸들, 파일, 포트, 레지스트리 등을 숨기는 기능 제공</li> </ul>

- 루트킷 분석 도구는 다양하나 가장 강력하고 기능이 많은 두 가지는 GMER과 ICESword임

GMER	<ul style="list-style-type: none"> <li>◆ 빠른 속도로 루트킷 검색</li> <li>◆ 다양한 탐색 및 제거 기능 제공</li> </ul>
IceSword	<ul style="list-style-type: none"> <li>◆ 개인 블로그를 통해 배포되는 강력한 안티 루트킷 도구</li> <li>◆ 분석을 위한 정보를 제공하여 사용자에게 루트킷을 제거하도록 유도</li> </ul>

### (2) 스크립트

- 스크립트 언어는 고수준의 프로그래밍 언어로 응용소프트웨어를 제어하는 빠르고 단순하게 작성된 언어를 말함
- 스크립트 언어는 대부분 특별한 환경의 제약 없이 실행이 가능해 악성코드를 실행할 주체가 되는데 이를 악성 스크립트라고 함
- 악성 스크립트는 주로 난독화 기법을 사용해 바로 분석이 어렵고 이를 이용해 공격이 가능한 웹 익스플로잇 킷 형태로 배포됨
- 악성 스크립트의 분석 도구에는 동적 환경에서 파이썬 도구를 이용한 샌드박스 분석과 스크립트를 실행하여 분석할 수 있는 에뮬레이터 형태의 도구가 있음

### [3] 악성코드 제거

- 악성코드는 프로세스를 종료시킨 다음 악성코드가 생성한 레지스트리 값과 악성코드 파일들을 삭제하면 제거가 가능함
- 최근의 악성코드는 자기보호로직이 점점 더 강력해져서 때에 따라 제거가 안되거나 본인이 제거되면 운영체제가 동작하지 못하도록 할 수 있기 때문에 악성코드 제거 전에는 먼저 자료 백업을 받아 두고 시작하는 것이 권장됨
- 악성코드 제거 방법
  - 1) 프로세스 종료 후 삭제
    - 프로세스 익스플로러에서 악성코드로 의심되는 프로세스를 선택하여 프로그램에서 제공하는 프로세스 종료 기능을 통해 악성코드 프로세스 강제종료
    - 여러 개의 악성코드가 서로를 감시해서 하나의 프로세스가 종료되어도 다시 재실행되는 로직이 존재할 수 있으므로 관련 악성코드 프로세스는 모두 종료
  - 2) 파일 삭제와 레지스트리 키/값 삭제
    - 악성코드 프로세스 종료 후 해당 악성코드 파일을 삭제함. 파일이 삭제되지 않는다면 파일 이름을 변경하고 운영체제를 다시 시작함
    - 악성코드의 동작과 관련된 레지스트리 값 중 악성코드가 생성한 키/값은 삭제해야 하나, 운영체제나 기존 응용 프로그램의 동작에 필요한 레지스트리 값을 삭제해서는 안됨
  - 3) 안전모드 부팅 후 삭제
    - 프로세스가 종료되지 않고 파일 이름도 변경되지 않는 경우 사용
    - 안전모드로 부팅하면 대부분의 루트킷이 동작하지 않음
    - 윈도우 시작 시 F8키를 눌러 윈도우 시작 모드를 키고 안전 모드를 선택 해 안전 모드 부팅 후 문제의 악성코드 파일을 삭제하고 운영체제를 재시작하는 순서로 실행