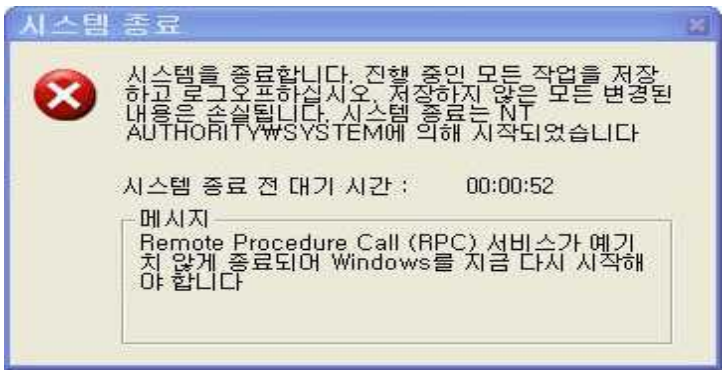
제16장 해킹/바이러스

1. 바이러스

1. 바이러스 구분

	트로이목마	컴퓨터 바이러스	웜(worm)
복제 능력	없음	있음	매우 강함
감염 능력	없음	있음	매우 강함
감염 대상	**없음**	**있음**	**없음**
전파 경로	사용자가 내려 받음 (수동적 존재)	사용자가 감염된 파일을 옮김 (스스로 복제 및 변형)	네트워크를 통해 전파 (스스로 복제품 전파)
형태	**유용한 프로그램으로 위장** (유틸리티로 착각하도록 함)	부트섹터나 파일 등에 기생 (감염 대상이 필요)	독립적인 실체로 존재 (감염 대상 불필요)
주 특징	컴퓨터 성능 저하 좀비 컴퓨터	해당 파일시스템 손상 해당 컴퓨터 손상	네트워크 성능 저하 (대역폭 잠식)

- **컴퓨터 바이러스**는 다른 실행 프로그램에 **기생**하여 실행된다.
- **웜**은 **독자적**으로 실행된다. 웜은 다른 실행 프로그램이 필요하지 않다.
- 웜은 이메일, 메신저 등의 주소록을 뒤지고 스스로를 첨부해 네트워크를 통해 퍼진다.
- 웜은 외국에서 발견되고 몇 시간 만에 한국에서도 발견될 정도로 전염성이 강하다.
- 바이러스처럼 개인 PC를 손상시키는 웜이 등장하면서 '**웜바이러스**'라는 신조어도 생겼다.
- 블래스터(blaster) 웜이 감염된 경우(윈도우 NT계열을 통해 급속하게 확산된 웜)



2. 바이러스 분류

◈ 감염 부위에 따른 분류

부트 바이러스 (boot virus)	• 컴퓨터를 가동되면 **부트섹터**에 위치하는 바이러스 프로그램이다. • 예 : 뇌(brain), 원숭이(monkey), anti-cmos
파일 바이러스 (file virus)	• **실행 가능한 프로그램**에 감염되는 바이러스를 말한다. • 이때 감염되는 대상은 확장자가 exe 같은 실행파일이 대부분이다. • 예 : 예루살렘, 일요일, 전갈(scorpion), 까마귀(crow)
부트/파일 바이러스 (multipartite virus)	• 부트/파일 바이러스는 부트섹터와 파일에 모두 감염된다. • 예 : 침입자(invader), 안락사(euthanasia), 에볼라(ebola)
매크로 바이러스 (macro virus)	• 매크로는 하나의 명령으로 여러 명령을 수행하기 위한 기능이다. • Visual Basic을 이용하면 매크로는 간단하게 변조될 수 있다. • 매크로 기능을 사용하는 응용프로그램의 **데이터에 감염**된다. • 마이크로소프트사의 엑셀, 워드 등은 매크로 기능을 제공 • 실행 프로그램 파일이 아닌, 작성된 데이터 파일에 감염된다. • 데이터 파일인 *.DOC, *.DAT와 같은 파일에 감염된다. • 매크로를 사용하는 문서를 읽을 때 감염된다. • 매크로 바이러스로 W97M.Joke, 사이버넷 등이 있다. • 사이버넷은 다변형 바이러스이다. • 사이버넷에 감염된 파일은 파일명이 계속 바뀌는 현상이 발생 • 사이버넷에 감염된 워드와 엑셀 파일은 삭제되기도 한다. • "V3 매크로"는 매크로바이러스만 치료할 수 있는 백신 프로그램

◈ 운영체계에 따른 분류

① 윈도우 바이러스

• 윈도우 바이러스 1994년 처음 등장하였다.

• 윈도우 바이러스는 97년부터 컴퓨터를 이용하는 최대 바이러스로 부상했다.

② 자바 바이러스

• 최초 자바 바이러스는 1998년 여름 발견되었다.

• 이들 바이러스 역시 자바가 디스크에 접근할 때 자바 애플리케이션을 감염시킨다.

• 예 : Java/BeanHive, Java/StrangeBrew

◈ **세대별 분류**

① 제1세대 원시형 바이러스(primitive virus)

- 실력이 뛰어나지 않은 프로그래머가 만들어 프로그램 구조가 단순하여 분석이 쉽다.
- 원시형 바이러스는 **코드 변형** 없이 **고정된 크기**를 가진다.
- 주로 기억장소에 상주해서 부트 영역이나 파일을 감염시킨다.
- **예** : 돌(stoned) 바이러스, 예루살렘(jerusalem) 바이러스 - 기존의 도스용 바이러스

② 제2세대 암호화 바이러스(encryption virus)

- 바이러스 프로그램 일부 또는 대부분을 **암호화**시켜 저장한다.
- 암호화는 백신 프로그램이 진단할 수 없도록 하기 위함이다.
- **예** : 폭포(cascade) 바이러스, 느림보(slow) 바이러스 등

③ 제3세대 은폐형 바이러스(stealth virus)

- 자신을 **은폐**하고, 사용자나 백신 프로그램에 **거짓 정보를 제공**한다,**(백신 프로그램을 속인다)**
- 거짓 정보를 제공하기 위해서 다양한 기법을 사용한다,
- 기억장소에 존재하면서 감염된 파일 길이가 증가하지 않은 것처럼 보이게 하고
- 백신 프로그램이 감염된 부분을 읽으면, **감염 전**의 **내용**을 보여준다.**(바이러스가 없는 것처럼 위장)**
- **예** : 조쉬(joshi), 방랑자.1347(wanderer.1347), 프로도(frodo) 바이러스 등

④ 제4세대 갑옷형 바이러스(armour virus)

- **백신 개발**을 **지연**시키기 위하여 **다양한 암호 기법**을 사용하는 바이러스이다.
- 제2세대, 3세대 바이러스들은 백신이 바이러스를 진단하기 어렵게 하는 것이 목표였다.
- 그러나, 백신 프로그램의 발달로 이런 목표가 무산되었다.
- 해서, 바이러스 제작자들은 백신 프로그램 제작자에게 공격의 화살을 돌림
- 백신 프로그램으로부터 자신을 숨기기보다는 바이러스 분석을 어렵게 한다.**(백신 개발 지연)**
- 백신 프로그램이 분석하기 어렵도록 여러 단계의 암호화 기법 등을 이용한다.
- 갑옷형 바이러스의 일종인 다형성(polymorphic) 바이러스는 암호화 기법을 사용한다.
  → 암호화를 푸는 부분이 항상 일정하지 않다.
  → 암호화를 푸는 부분이 감염될 때마다 달라지고
  → 한 개의 바이러스가 몇 억가지 이상의 변형을 만드는 경우도 있다.

⑤ 제5세대 매크로 바이러스(macro virus)

- 매크로를 사용하는 프로그램의 **데이터를 감염**시키는 바이러스이다.
- 매크로 바이러스는 운영체제와 관계없이 응용프로그램 내부에서 동작한다.
- **예** : MS사 제품(워드, 엑셀, 파워포인트), 비지오(Visio), 오토캐드(AutoCAD) 등

기출문제 분석

1. 다음 설명에 해당하는 악성 소프트웨어를 옳게 짝지은 것은? [2017년 법무부 9급]

ㄱ. 시스템 및 응용 소프트웨어의 취약점을 악용하거나 전자우편 또는 공유 폴더를 이용하며, 네트워크를 통해서 컴퓨터에서 컴퓨터로 빠르게 전파된다.

ㄴ. 사용자 컴퓨터 내에서 자신 또는 자신의 변형을 다른 실행 프로그램에 복제하여 그 프로그램을 감염시킨다.

ㄷ. 겉으로 보기에는 유용해 보이지만 정상적인 프로그램 속에 숨어있는 악성 소프트웨어로, 사용자가 프로그램을 실행할 때 동작한다.

	ㄱ	ㄴ	ㄷ
①	웜	바이러스	트로이목마
②	바이러스	웜	봇
③	바이러스	웜	트로이목마
④	웜	바이러스	봇

♤ **악성 소프트웨어**

ㄱ. 네트워크를 통해서 컴퓨터에서 컴퓨터로 빠르게 전파된다. - **웜**

ㄴ. 다른 실행 프로그램에 복제하여 그 프로그램을 감염시킨다. - **바이러스**

ㄷ. 정상적인 프로그램 속에 숨어있는 악성 소프트웨어 - **트로이목마**

정답 : ①

2. MS 오피스와 같은 응용프로그램의 문서 파일에 삽입되어 스크립트 형태의 실행 환경을 악용하는 악성코드는? [2015년 지방 9급]

① 애드웨어 ② 트로이 목마

③ 백도어 ④ 매크로 바이러스

♤ **매크로 바이러스**

- 매크로 바이러스는 매크로 기능을 사용하는 응용프로그램의 데이터에 감염된다.
- 마이크로소프트사의 엑셀, 워드 등은 매크로 기능을 제공

정답 : ④

3. 겉으로는 유용한 프로그램으로 보이지만 사용자가 의도하지 않은 악성 루틴이 숨어 있어서 사용자가 실행시키면 동작하는 악성 소프트웨어는? [2021년 국가 9급]

① 키로거 ② 트로이목마 ③ 애드웨어 ④ 랜섬웨어

♤ **악성 소프트웨어**

- 트로이목마는 겉으로 보기에는 유용해 보이지만 정상적인 프로그램 속에 숨어있는 악성코드이다.
- 트로이목마는 사용자가 프로그램을 실행할 때 동작한다.

정답 : ②

4. 다음 바이러스 발전 단계에 따른 분류에 대한 설명으로 옳지 않은 것은? [2016년 서울 9급]

① 원시형 바이러스는 가변 크기를 갖는 단순하고 분석하기 쉬운 바이러스이다.
② 암호화 바이러스는 바이러스 프로그램 전체 또는 일부를 암호화시켜 저장하는 바이러스이다.
③ 갑옷형 바이러스는 백신 개발을 지연시키기 위하여 다양한 암호화 기법을 사용하는 바이러스이다.
④ 매크로 바이러스는 매크로를 사용하는 프로그램 데이터를 감염시키는 바이러스이다.

♤ **컴퓨터 바이러스 분류 – 세대별 분류**

- 원시형 바이러스는 가변 크기를 갖는 단순하고 분석하기 쉬운 바이러스이다.(×)
  → 원시형 바이러스는 코드 변형 없이 고정된 크기를 가진다.

정답 : ①

5. 바이러스 중에서 감염될 때마다 구현된 코드의 형태가 변형되는 것은? [2019년 서울 9급]

① Polymorphic virus ② Signature virus
③ Generic decryption virus ④ Macro virus

♤ **바이러스 종류**

- 다형성 바이러스(polymorphic virus) : 감염될 때마다 자신의 모습을 변형한다.
- 서명 바이러스(signature virus) : 서명 바이러스는 바이러스 종류에 없는 것으로
- 일반 해독 바이러스(generic decryption virus) : 역시, 바이러스 종류에 없는 것으로
- 매크로 바이러스(macro virus) : 매크로 언어로 기록된 바이러스이다.(데이터 파일에 감염)

정답 : ①

6. 최근 발생한 보안 위협에 대한 설명으로 옳은 것은? [2020년 국회 9급]

① 블루킵(bluekeep): 원격 데스크톱 서비스를 인증 없이 조작할 수 있는 취약점
② 다크웹(dark web): 피싱 메일을 통해 유포되며 금융정보 탈취를 시도하는 악성코드
③ 딥페이크(deepfake): 특정 웹브라우저를 통해 익명성이 보장되는 인터넷 영역
④ 이모텟(emotet): 한글로 작성된 메일 내부에 정상파일로 위장한 랜섬웨어
⑤ 소디노키비(sodinokibi): 인공지능을 기반으로 실제처럼 조작한 음성, 영상 등을 통칭함

♤ **보안 위협**

◈ **블루킵(bluekeep)**

- 블루킵 취약점은 윈도우 원격 데스크톱 서비스(RDS)에서 발견되었다.
- 블루킵은 윈도우의 원격 데스크톱 서비스를 **정상적 인증 없이 조작할 수 있는 취약점**이다.
- 마이크로소프트사는 블루킵을 예방할 수 있는 패치를 발표하였다.(2019년 5월)
- 블루킵은 CVE-2019-0708이라는 번호가 붙은 유명 취약점이다.
- 블루킵은 웜의 방식으로 증식할 수 있다.

◈ **다크웹(dark web)**

표면웹(surface web)	• 구글, 네이버 같은 일반 검색엔진으로 검색이 가능한 웹 • 광고를 해서 이름을 알리는 일반적인 보통의 웹이다.
딥웹(deep web)	• 구글, 네이버 같은 일반 검색엔진으로 검색이 불가능한 웹 • 광고를 하지 않아서 아는 사람들만 갈 수 있는 웹이다.
다크넷(darknet)	• 다크넷은 비표준 통신 프로토콜과 포트를 사용하는 네트워크이다. • 다크넷은 특정 소프트웨어나 네트워크 허가나 설정이 있어야 접속할 수 있는 오버레이 네트워크(overlay network) 이다. • 예 : P2P 접속으로 파일을 공유하는 친구 간 네트워크 • 예 : 토르(tor) 같은 사생활 보호 네트워크
다크웹(dark web)	• 다크넷 중에서 웹만을 따로 다크웹(dark web)이라고 한다. • 다크웹을 딥웹이라고 잘못 부르는 경우가 많다.

- **다크웹**은 쉽게 추적할 수 없는 암호화된 지하 네트워크이다.
- **다크웹**은 사이트 주소도 일반 웹사이트 도메인과 다른 형태를 갖고 있다.
- **다크웹**은 철저한 익명화를 특징으로 하고, 온라인 상거래는 가상화폐를 사용하고 있다.
- **다크웹**은 불특정 다수의 사람들에게 익명과 자유를 제공하는 **긍정적인 영향**이 있는 대신 각종 범죄자들이 모이는 **부정적인 영향**도 유발시킨다.
- **다크웹**은 위조지폐, 무기 암거래, 청부살인, 공문서 위조, 마약 거래, 아동 포르노 거래와 같은 위험한 범죄를 저지르는 범죄자들은 숨어들어 악용하기도 한다.
- 베리마켓이라는 **다크웹**에서 비트코인으로 마약을 거래한 사람들이 체포된 적이 있다.

◈ **딥페이크(deepfake)**

- 영어단어 **fake**는 가짜의, 거짓된, 모조품 등의 뜻을 가진다.
- 딥페이크는 인공지능 기술을 활용해 기존에 있던 인물의 얼굴이나 특정한 부위를 영화의 컴퓨터 그래픽(CG)처리처럼 합성한 영상편집물을 말한다.
- 예 : 힐러리 클린턴에 도널드 트럼프의 얼굴을 바꿔치기한 영상
- 개인과 집단의 이익 목적을 실현하기 위해 딥페이크를 악용할 수 있다.
- 딥페이크는 정치적으로 악용될 수 있다.(거짓 정보를 통해 대중을 선동하고 불안 조장)

// MBC 뉴스에서 딥페이크 기술을 이용한 아이유와 방탄소년단 사건

2020년 4월 20일 방영된 MBC 뉴스데스크에서 딥페이크 기술의 악용에 대한 보도를 하는 과정에서 방탄소년단에게는 성룡의 얼굴, 아이유에게는 로버트 다우니 주니어를 합성한 영상을 인용하였고 이를 트위터 등지의 방탄소년단 팬들과 아이유 팬들이 문제 제기를 하면서 논란이 되었다.

◈ **이모텟(emotet)**

- 이모텟은 **금융정보**를 탈취하기 위한 **악성코드**이다.(2014년 처음 발견)
- 이모텟은 주로 이메일을 통해 유포된다.
- 이모텟은 자기복제, 사용자 정보탈취, 다운로더 등 다양한 악성 행위를 수행한다.
- 최근, 피싱 메일을 통해 금융정보 탈취를 시도하는 이모텟이 대량으로 유포되었다.
- 출처가 불분명한 메일에 있는 첨부파일 및 링크는 접근을 피한다.
- 검증되지 않은 파일은 실행하기 전에 백신 프로그램으로 악성 여부를 점검한다.

◈ **소디노키비(sodinokibi)**

- 소디노키비는 기존 랜섬웨어의 텍스트 일부를 해커가 임의로 수정한 버전을 말한다.
- 즉, 소디노키비는 **랜섬웨어 변종**이다.
- 예 : 입사지원서 위장한 '소디노키비' 랜섬웨어 발견(이메일을 통해 유포)

↓

- 메일에 첨부된 입사지원서 파일은 '7z' 형식의 압축파일이다.
- 압축을 풀면, 실제 입사지원서 제출하는 위장된 '이력서.pdf', '포트폴리오.pdf'의 파일이 존재
- 첨부된 파일은 실제 PDF, HWP 문서파일이 아닌 **악성 실행파일(exe)**이다.
- 공격자는 문서파일 이름에 공백을 삽입해 수신자가 악성파일을 PDF나 HWP 문서로 착각하도록 유도한 것이다.
- 수신자가 파일을 여는 순간 해커가 만들어 둔 명령제어서버에 연결되고
- 소디노키비 랜섬웨어를 다운로드 실행 후 수신자 PC의 **주요 데이터를 암호화**한다.

정답 : ①

7. 리버스 엔지니어링을 어렵게 만드는 안티 리버싱 기술에 대한 설명으로 가장 옳지 않은 것은? [2020년 서울 7급]

① 원본 프로그램을 새로운 파일에 패킹된 형태로 압축하고 암호화하여 저장한다.
② 공격에 이용될 수 있는 코드를 최소화하기 위해 쓰레기(garbage) 코드를 모두 삭제한다.
③ 리버스 엔지니어링 수행을 위한 디버거 활동을 탐지하여 프로그램을 강제 종료한다.
④ 다단계 점프문을 섞어 코드를 치환하여 배치한다.

♤ **리버스 엔지니어링 / 안티 리버싱 기술**

• 공격에 이용될 수 있는 코드를 최소화하기 위해 **쓰레기(garbage) 코드를 모두 삭제**한다.(×)
→ **쓰레기(garbage) 코드를 삽입**해야 리버스 공격을 방지할 수 있다.

// 리버스 엔지니어링(reverse engineering)

• 리버싱(reverse+engineering)은 이미 완성된 소프트웨어를 역으로 분석하는 과정이다.
• 리버싱을 통해 사람이 알아 볼 수 있도록 기존의 원시코드를 복원하는 것이다.(디컴파일)

// 안티(anti) 리버싱

• 먼저, 영어단어 anti는 "~에 반대되는" 뜻도 있지만 "**~를 방지하는**"이라는 뜻도 있다.
• 전산에서 안티 리버싱. 안티 디버깅 등의 용어를 사용하고 있다..
• 안티 리버싱 : 암호화, 난독화, 쓰레기 코드 삽입, 제어흐름변환 등

정답 : ②

8. 다음 중 컴퓨터 바이러스에 대한 설명으로 가장 옳지 않은 것은?

① 원시형 : 단순하게 자기복제 기능과 데이터 파괴 기능만을 가지고 있다.
② 은폐형 : 바이러스 코드를 암호화하여 코드를 은닉한 바이러스이다.
③ 다형성 : 프로그램이 실행될 때마다 바이러스 코드를 변경한다.
④ 매크로 : 주로 오피스 프로그램의 매크로 기능을 통해 감염된다.

♤ **컴퓨터 바이러스**

• **은폐형** : 바이러스 코드를 **암호화**하여 코드를 은닉한 바이러스이다.(×) ← **갑옷형** 바이러스

// 은폐형 바이러스(stealth virus)

• 자신을 은폐하고, 사용자나 백신 프로그램에 **거짓 정보를 제공**한다,**(백신 프로그램을 속인다)**
• 거짓 정보를 제공하기 위해서 다양한 기법을 사용한다,
• 백신 프로그램이 감염된 부분을 읽으면, **감염 전**의 **내용**을 보여준다.**(바이러스가 없는 것처럼 위장)**
• **예** : 조쉬(joshi), 방랑자.1347(wanderer.1347), 프로도(frodo) 바이러스 등

정답 : ②