악성코드의 종류 및 특징

1 악성코드의 종류 및 특징

악성코드의 대략적인 분류

1 악성코드의 종류 및 특징

1 바이러스

바이러스

악의적인 목적으로 자기자신 또는 일부 데이터를 상대방에게 복제 · 감염 · 전파함

컴퓨터 바이러스

컴퓨터 바이러스(Computer Virus, 문화어 : 콤퓨터 비루스)는 스스로를 복제하여 컴퓨터를 감염시키는 컴퓨터 프로그램이다. 복제 기능이 없는 다른 종류의 악성 코드, 애드웨어, 스파이웨어와 혼동하여 잘못 쓰이는 경우도 있다. 바이러스는 한 컴퓨터에서 다른 컴퓨터로(일부 형식의 실행 코드로) 확산할 수 있다. 이를테면 사용자는 인터넷이나 네트워크를 통하여, 또는 플로피 디스크, CD, DVD, USB 드라이브와 같은 이동식 매체를 통하여 바이러스를 전파할 수 있다. 바이러스는 네트워크 파일 시스템이나, 다른 컴퓨터를 통해 접근하는 파일 시스템 상의 파일을 감염시킴으로써 다른 컴퓨터로의 확산 가능성을 높일 수 있다.

1 악성코드의 종류 및 특징

1 바이러스

⚙ 바이러스의 종류와 특징

1. 1세대 원시형 바이러스
2. 2세대
3. 3세대
4. 4세대
5. 5세대

부팅 단계에서 POST(Power On Self Test)가 완료되고,
BIOS가 CMOS의 설정을 읽어서 시스템을 구동시킨 후,
디스크의 MBR(Master Boot Record) 정보를 참고하여 부트 프로그램을 메모리에 적재함

↓

1세대 바이러스 중 부트 바이러스는 이 단계에서 MBR과 함께 메모리에 적재되어
다른 프로그램으로 자신을 전염시킴

예 부트 바이러스

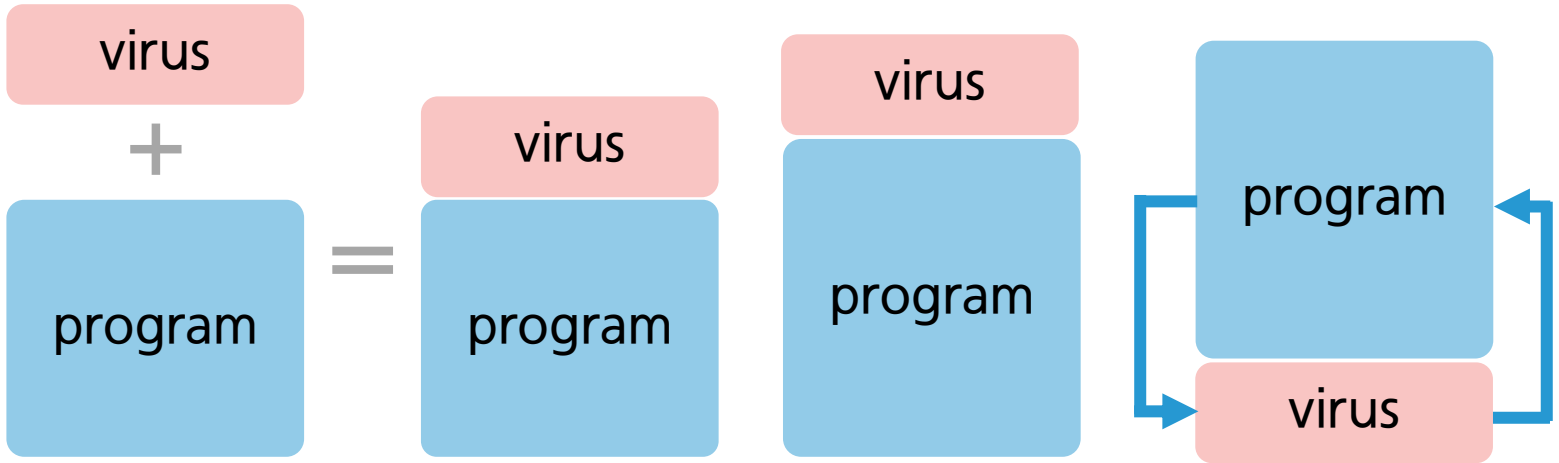
브레인 바이러스, 몽키 바이러스, 미켈란젤로 바이러스 등이 있음

1 바이러스

바이러스의 종류와 특징

1. 1세대 원시형 바이러스
2. 2세대
3. 3세대
4. 4세대
5. 5세대

- 파일 바이러스는 파일에 감염되어, 파일이 실행될 때 바이러스 코드가 실행됨
- 바이러스는 파일의 앞이나 뒤에 위치함



1 바이러스

바이러스의 종류와 특징

1. 1세대
2. 2세대 암호형 바이러스
3. 3세대
4. 4세대
5. 5세대

01 바이러스 제작자가 백신이나 바이러스 분석을 회피하기 위하여 코드를 암호화하는 방법을 사용하여 진단을 우회함

02 바이러스가 메모리에 적재될 때 복호화 되기 때문에 메모리를 분석하여 바이러스를 분석함

예 암호형 바이러스

슬로우, 캐스캐이드, 원더러, 버글러 등이 있음

1 바이러스

⚙ 바이러스의 종류와 특징

1. 1세대
2. 2세대
3. 3세대 은폐형 바이러스
4. 4세대
5. 5세대

- 바이러스가 감염 즉시 활동하게 될 경우 충분히 전파되기 어렵기 때문에 감염되고 잠복기를 가진 후 활동을 시작함

POINT 잠복기에는 바이러스가 활동하지 않으므로 감염 여부를 파악하기 난해함

예 은폐형 바이러스

브레인, 조시, 512, 4096 바이러스 등이 있음

1 바이러스

⚙ 바이러스의 종류와 특징

1. 1세대
2. 2세대
3. 3세대
4. 4세대 다형성 바이러스
5. 5세대

- 백신 프로그램이 특정 식별자를 이용하여 바이러스를 진단하는 기능을 우회하기 위해 만들어진 바이러스
- 다형성 바이러스는 코드 조합을 다양하게 할 수 있는 조합(mutation) 프로그램을 암호형 바이러스에 덧붙여 감염

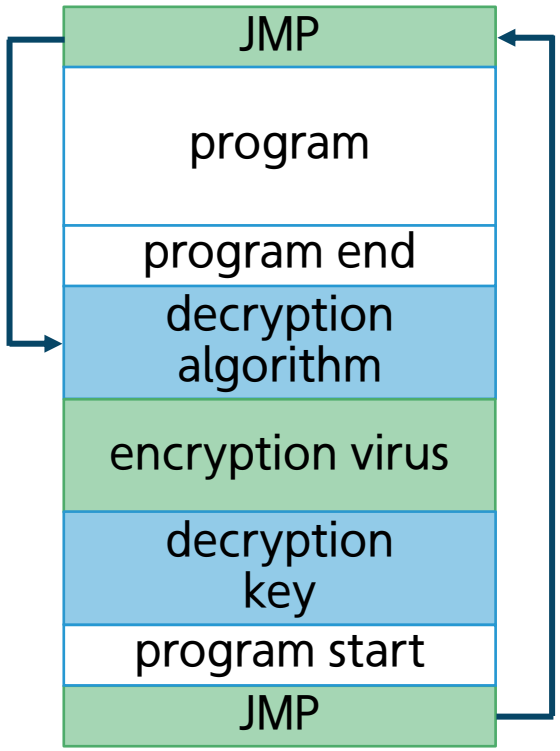
실행될 때마다 바이러스 코드 자체를 변경시켜 식별자로 구분하기 어렵게 함

1 바이러스

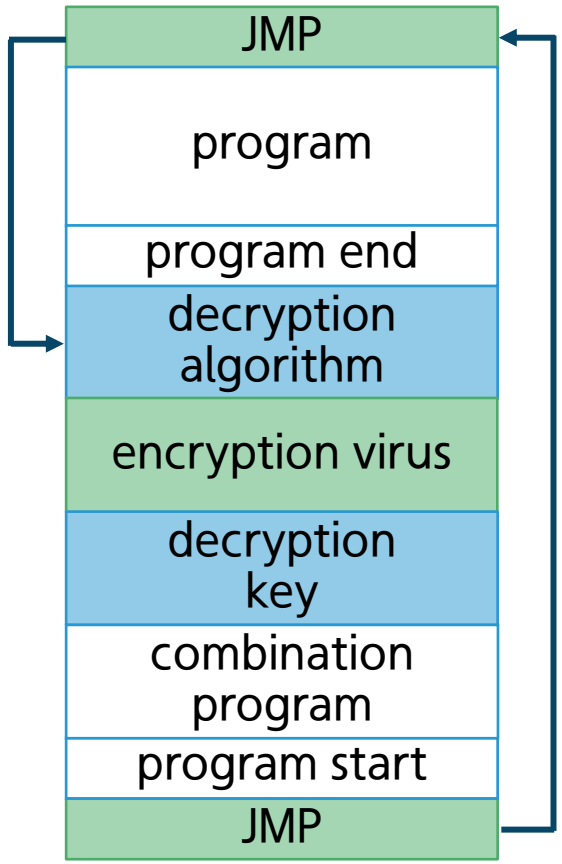
바이러스의 종류와 특징

1. 1세대
2. 2세대
3. 3세대
4. 4세대 다형성 바이러스
5. 5세대

[encryption virus]



[polymorphic virus]



1 바이러스

⚙ 바이러스의 종류와 특징

1. 1세대
2. 2세대
3. 3세대
4. 4세대
5. 5세대 매크로 바이러스

- 실행 파일에 감염되는 바이러스가 아닌, 엑셀, 워드 등의 문서에서 사용되는 매크로 기능을 사용하는 바이러스

POINT 문서 파일을 열어보기만 해도 감염됨

예 매크로 바이러스

워드 컨셉트, Wazzu, 엑셀-라룩스 바이러스 등이 있음

1 악성코드의 종류 및 특징

1 바이러스

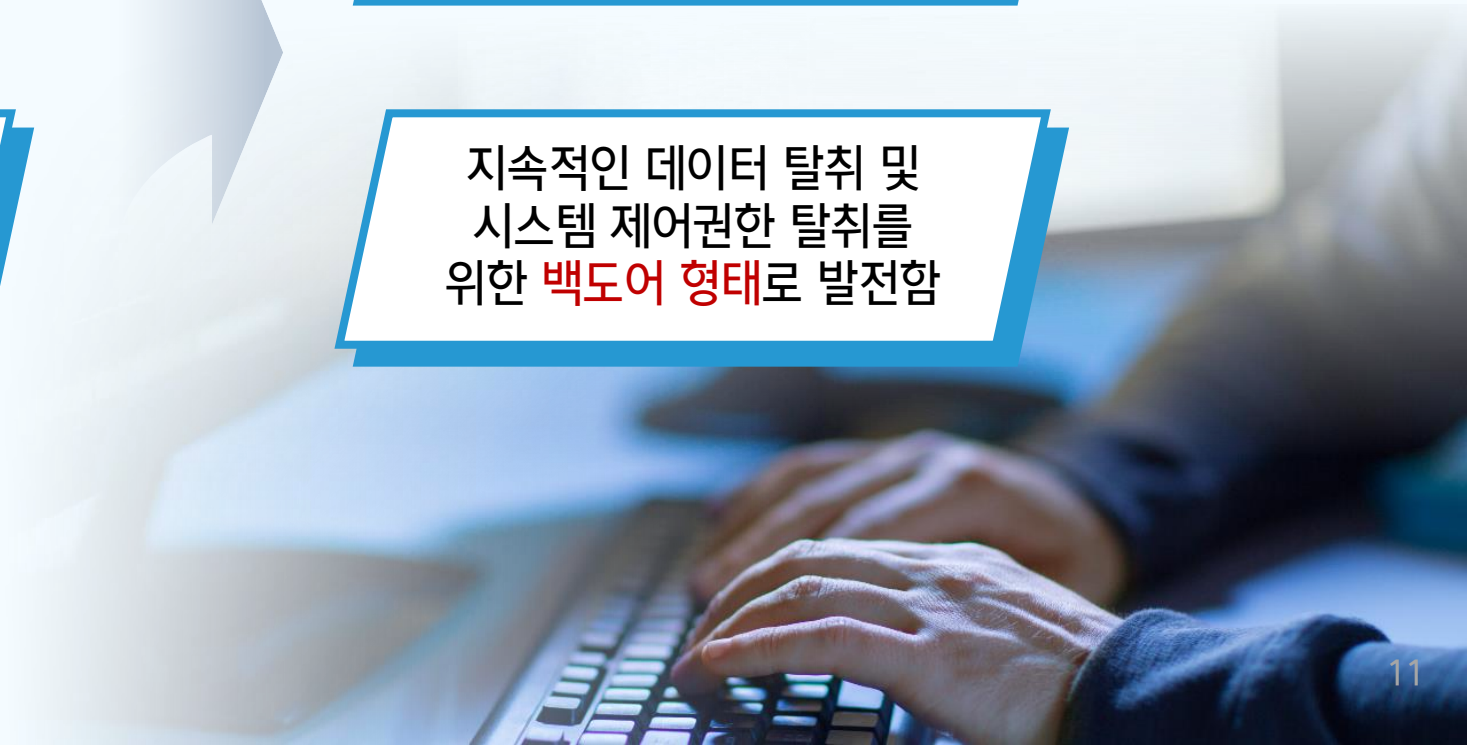
⚙ 바이러스 발전 형태

매크로 바이러스

인터넷, 메일 등을 통해 전파되는 스크립트 형태의 바이러스로 발전함

단순히 시스템을 파괴하기 위한 목적

지속적인 데이터 탈취 및 시스템 제어권한 탈취를 위한 백도어 형태로 발전함



2 웜

웜

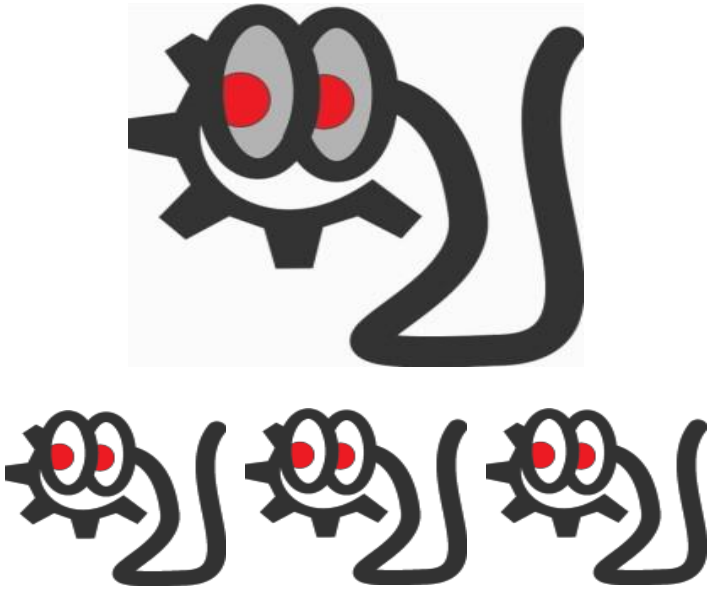
악의적인 목적으로 자신을 스스로 복제 · 전파함

웜

컴퓨터 웜(Computer Worm)은 스스로 복제하는 컴퓨터 프로그램이다. 컴퓨터 바이러스와 비슷하다. 바이러스가 다른 실행 프로그램에 기생하여 실행되는 데 반해 웜은 독자적으로 실행되며 다른 실행 프로그램이 필요하지 않다. 웜은 종종 컴퓨터의 파일 전송 기능을 착취하도록 설계된다. 컴퓨터 바이러스와 웜의 중요한 차이점은 바이러스는 스스로 전달할 수 없지만 웜은 가능하다는 점이다. 웜은 네트워크를 사용하여 자신의 복사본을 전송할 수 있으며, 어떠한 중재 작업 없이 그렇게 할 수 있다. 일반적으로 웜은 네트워크를 손상시키고 대역폭을 잠식하지만, 바이러스는 컴퓨터의 파일을 감염시키거나 손상시킨다. 바이러스는 보통 네트워크에 영향을 주지 않으며 대상 컴퓨터에 대해서만 활동한다.

② 웜

웜 배포 수단




ICQ
Offline
MSN
Mobile wit…enger.
AOL
Offline
Yahoo!
Offline
Jabber
Offline
GoogleTalk
Offline


Email

2 웜

최초의 웜

컴퓨터 바이러스

웜은 1978년 제록스 파크(Xerox PARC)의 두 명의 연구자에 의해 최초로 구현되었다. 개발자인 존 쇼크(John Shoch)와 존 허프(Jon Hupp)는 원래 네트워크에서 놀고 있는 프로세서들을 찾아 그들에게 업무를 할당하고 연산처리를 공유하여 전체적인 네트워크의 효율을 높이도록 웜을 설계했다.
많은 주목을 받았던 최초의 웜은 당시 코넬 대학교의 대학원 학생이었던 로버트 터팬 모리스(Robert Tappan Morris)가 개발했던 모리스 웜이다.
이 웜은 1988년 11월 2일에 배포되었는데, 그때 당시 인터넷에 연결된 수많은 컴퓨터들을 빠른 속도로 감염시켰다. 이 웜은 BSD 유닉스와 그것으로부터 파생된 운영 체제들의 많은 버그들을 통해 확산되었다. 모리스는 미국의 컴퓨터 범죄와 남용에 관한 법(Computer Crime and Abuse Act)에 따라 유죄가 선고되어 3년의 집행유예와 400시간의 사회 봉사, 10,000달러가 넘는 벌금을 받았다.

2 웜

웜의 역사

Morris Worm(모리스 웜)

- 최초의 웜(코넬대학교 모리스에 의해 작성)

ILOVEU(러브레터)

- 2000년 필리핀에서 발견됨
- 'ILOVEU'라는 이메일 제목과 'LOVE-LETTER-FOR-YOU.txt' 라는 첨부파일이 추가되어 있는 것이 특징임
- 감염자 아웃룩의 주소록에 있는 계정을 통해 추가 메일이 발송됨

Code Red(코드 레드)

- 2001년 7월 13일 처음 관찰된 웜 바이러스로, 마이크로소프트 인터넷 정보 서비스(IIS)의 버퍼 오버플로 취약점을 이용
- 감염된 후 20일~27일 동안 잠복한 후, 미국 백악관 홈페이지 등 몇몇 IP에 서비스 거부 공격(DoS)을 하는 루틴도 포함됨

2 웜

웜의 역사

Nimda(님다)

- 2001년 9월 최초 발생된 웜
- 전세계적으로 동시에 발생함
  - 단, 22분만에 확산되어 막대한 경제적 피해가 발생함
  - 주로 이메일을 통해 감염됨

그 이외에도 블래스터 웜, 슬래머 웜 등 현재도 지속적으로 웜 발생

3 트로이 목마

트로이 목마

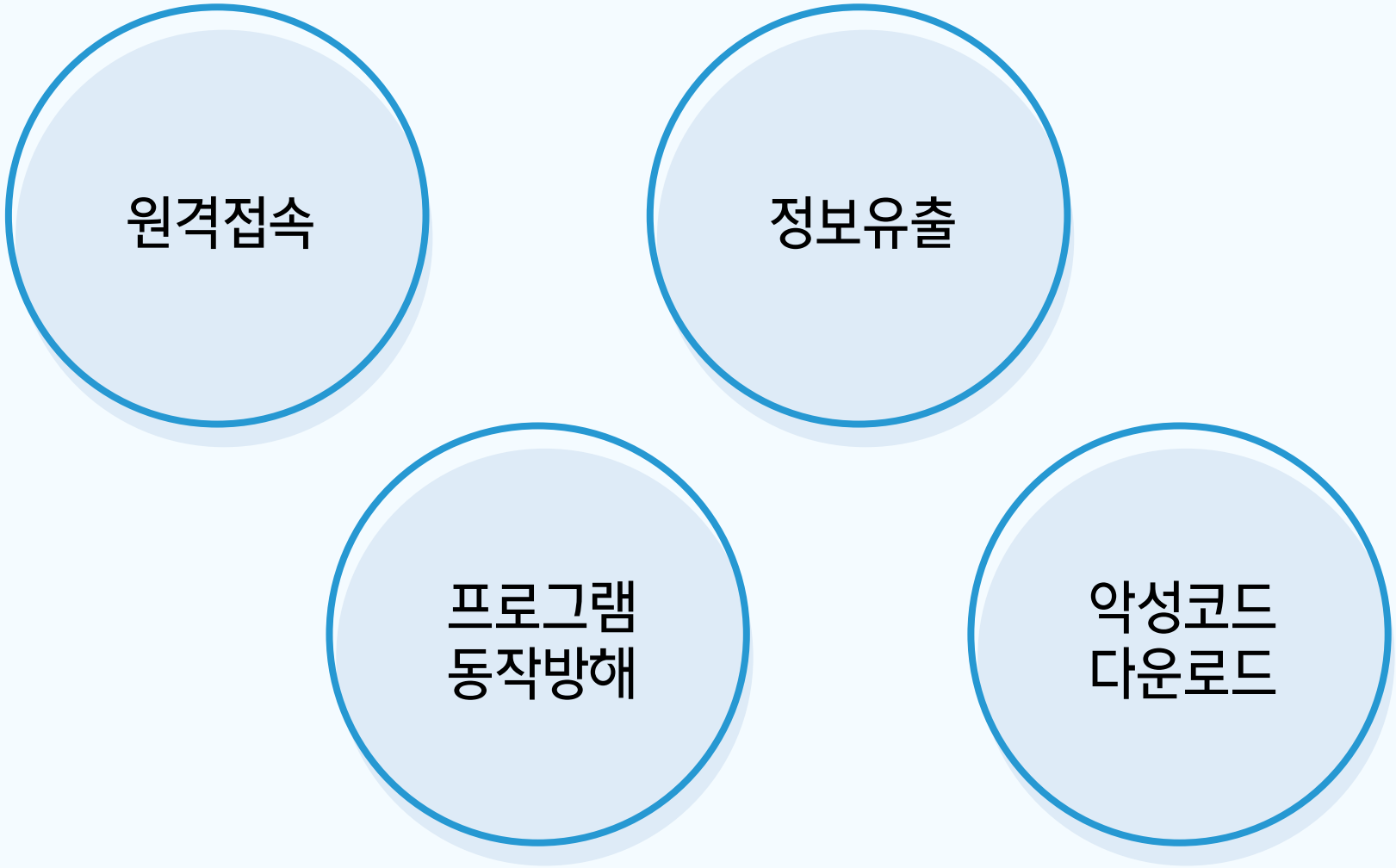
정상처럼 위장, 백그라운드로 악의적인 동작

WIKIPEDIA
The Free Encyclopedia

트로이 목마 (컴퓨팅)

트로이 목마(Trojan horse)는 악성 루틴이 숨어 있는 프로그램으로, 겉보기에는 정상적인 프로그램으로 보이지만 실행하면 악성 코드를 실행한다. 이 이름은 트로이 목마 이야기에서 따온 것으로, 겉보기에는 평범한 목마 안에 사람이 숨어 있었다는 것에 비유한 것이다.
예를 들어, 인터넷에서 게임 프로그램이라고 소개한 프로그램을 실행했더니 시스템 파일을 지워버리는 경우가 있을 수 있다. 또한 백도어를 열어 다른 곳에서 컴퓨터를 원격으로 조종할 수도 있다.

③ 트로이 목마



3 트로이 목마

대표적인 트로이 목마 프로그램

Netbus	▪ 넷버스, 12345번 포트 사용
Back Orifice	▪ 백오리피스, 31337번 포트 사용
Schoolbus	▪ 스쿨버스, 54321번 포트 사용
Executor	▪ 80번 포트 사용 ▪ 감염된 컴퓨터의 시스템 파일을 삭제 ▪ 시스템을 파괴하는 트로이 중의 하나
Silencer	▪ 1001번 포트 사용 ▪ 시스템 드라이브 등 하드디스크를 모두 파괴
Striker	▪ 2565번 포트 사용

➔ 그 이외에도 다양한 트로이목마 프로그램이 존재함

4 스파이웨어

최근에는 개인정보 탈취 등의 목적으로 많이 유포

스파이웨어

사용자의 동의 없이 컴퓨터의 정보를 수집, 전송하는 악성 프로그램

WIKIPEDIA
The Free Encyclopedia

스파이웨어

스파이웨어(Spyware)는 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어로, 신용 카드와 같은 금융 정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집한다. 처음에는 미국의 인터넷 전문 광고 회사인 라디에이트가 시작하였으나 그 뒤로 아이디, 암호 등을 알아낼 수 있도록 나쁜 용도로 변형되었다. 국립국어원에서는 스파이웨어를 정보 빼내기 프로그램으로 순화한 바 있다.

5 랜섬웨어

랜섬웨어

컴퓨터 시스템을 감염시켜 접근을 제한하고 인증에 대한 비용을 요구하는
악성 소프트웨어의 한 종류

- 대표적인 랜섬웨어(ransomware)
  - 워너크라이(WannaCry)
  - 록키(Locky)
  - 크립트XXX(CryptXXX)
  - 케르베르(CERBER)
  - 크립토락커(CryptoLocker)
  - 테슬라크립트(TeslaCrypt)

5 랜섬웨어

크립토락커(CryptoLocker)

- 2013년 9월 5일경부터 본격적으로 배포되기 시작한 것으로 여겨짐
- 이메일 첨부 등의 수단으로 감염되며, 감염되었을 경우 로컬 및 연결된 네트워크의 드라이브에 저장된 파일들을 2048비트 RSA 공개키 방식의 공개키로 암호화하며, 복호화하기 위한 개인키는 크립토라커를 조종하는 서버에만 저장함
- 크립토라커는 데이터를 복호화하고 싶으면 특정 시간까지 돈을 지불하라(추적을 피하기 위해 주로 비트코인 등의 수단을 사용한다)고 요구하고, 제한시간이 지나면 암호키를 삭제할 것이라고 협박함
- 크립토라커 프로그램 자체는 쉽게 제거 가능하나, 크립토라커가 행한 암호화를 깨는 것은 현실적으로 불가능하다고 알려졌음
- 국내에도 많이 유포되었고, 한국어 사이트도 오픈하였음

5 랜섬웨어

크립토락커 감염 화면

6 백도어

백도어

통상적으로는 인증을 우회할 목적으로 삽입 또는 탑재하는 악의적인 프로그램

WIKIPEDIA
The Free Encyclopedia

백도어

컴퓨터 시스템(또는 암호화 시스템, 알고리즘)의 백도어(BackDoor)는 일반적인 인증을 통과, 원격 접속을 보장하고 Plaintext에의 접근을 취득하는 등의 행동을 들키지 않고 행하는 방법을 일컫는다.
백도어는 설치된 프로그램의 형태를 취하기도 하고, 기존 프로그램 또는 하드웨어의 변형일 수도 있다.

7 루트킷(Rootkit)

루트킷

- 공격 이후 공격프로세스를 은닉할 목적으로 실행되는 프로그램
- 루트 권한을 획득한 공격자가 심어놓은 프로그램을 숨기기 위한 목적으로 사용되는 프로그램

- 1994년 처음 등장함
- 루트 권한을 가진 공격자가 로그인 하는 사용자들의 암호를 알아내기 위해 사용되는 일련의 위조 프로그램들 및 그 프로그램을 숨기기 위한 프로그램을 총칭하는 명칭
- 이후 백도어 프로세스나 파일 등의 흔적을 관리자가 볼 수 없도록 하는 프로그램에 대한 명칭으로 사용됨
- 루트킷은 펌웨어, 가상화 계층, 부트로더, 커널, 라이브러리 등 다양한 곳에서 동작함