

정보보호와 시스템보안

악성코드, 바이러스 & 웜

전은아

목차

1. 악성코드
2. 바이러스
3. 웜
4. 기타 악성코드
5. 악성코드 탐지 및 대응책

학습목표

- 악성코드의 종류와 그 특성을 알아본다.
- 바이러스의 동작 원리를 이해한다.
- 웜의 동작 원리를 이해한다.
- 기타 악성코드의 종류를 알아본다.

01 악성코드

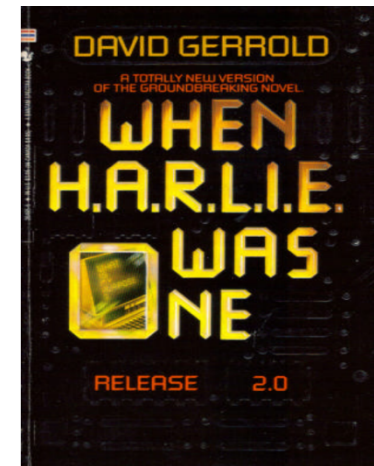
■ 악성코드의 정의

- 제작자가 의도적으로 사용자에게 피해를 주고자 만든 모든 악의적 목적을 가진 프로그램 및 매크로, 스크립트 등 컴퓨터상에서 작동하는 모든 실행 가능한 형태

■ 악성코드의 역사 : 바이러스의 역사

■ 바이러스 개념의 정립

- 1972년 : 컴퓨터 바이러스의 개념이 처음 등장
- 소설가인 데이비드 제럴드의 공상과학소설 『When Harlie was One』 (Nelson Doubleday, 1972)
 - ‘다른 컴퓨터에 계속 자신을 복제한 후 감염된 컴퓨터의 운영체제에 영향을 미쳐 점차 시스템을 마비시키는 장치를 한 과학자가 제작해 배포한다’는 내용이 소개
- 1984년 : 프레드 코헨(Fred Cohen)이 컴퓨터 바이러스의 개념 정립
We define a computer 'virus' as a program can 'infect' other programs by modifying them to include a possibly evolved copy of itself.



[그림 1] When Harlie was One의 표지

■ 최초의 바이러스

- 일반적으로 1986년에 발견된 **브레인 바이러스(Brain Virus)**를 **최초의 바이러스로 인정**
 - 파키스탄에서 프로그래머로 일하던 알비 형제가 자신들의 소프트웨어가 불법 복제되는 것에 대한 불만으로 바이러스를 만들어서 뿌렸다고 함.

01 악성코드

■ 악성코드의 역사

■ 최초의 웜

- 1988 : 미국의 네트워크를 마비시켰던 '모리스 웜' 사건의 원인이었던 모리스 웜이 최초의 웜으로 알려져 있음.

■ 매크로 바이러스 출현

- 1999년 : 매크로 바이러스로 잘 알려진 멜리사(Melissa) 바이러스가 출현.
 - 고난이도 기술만이 웜/바이러스 제작에 이용될 수 있다는 인식을 바꿔놓음.
 - 매크로(Macro)란 엑셀이나 워드에서 특정한 기능을 자동화 시켜놓은 일종의 프로그램

■ 웜에 의한 대규모 피해 발생

- 2001년 : 코드 레드(Code Red) 웜에 의해 8시간 만에 25만 대 이상의 컴퓨터가 감염
 - 이 웜은 윈도우 2000과 윈도우 NT 서버를 경유지로 이용해 미국 백악관을 공격하였는데, 국내도 최소 3만대 이상의 시스템이 피해를 입은 것으로 추정됨.

■ 인터넷 대란

- 2003년 : 인터넷 대란을 일으킨 SQL_Overflow(일명 슬래머) 웜이 등장
 - CAIDA에 따르면, 기준으로 2003년 1월 25일 05시 29분에 슬래머가 퍼지기 시작하여, 06시를 기준으로 전 세계의 74,855대 시스템이 그림과 같이 감염됨.
 - 8월에는 1~2분 간격으로 컴퓨터를 강제 재부팅시킴으로써 국내외적으로 큰 피해를 준 블래스터 웜(Blaster Worm)을 시작으로, 웰치아 웜(Welchia Worm), 엄청난 양의 스팸 메일을 집중 발송해 전 세계를 깜짝 놀라게 한 소빅.F 웜(Sobig.F Worm) 등이 발생

01 악성코드

■ 악성코드의 역사



[그림 2] 슬래머 웜의 전파

- 변종 웜의 발생
 - 2000년 중반에 들어서면서 웜의 다양한 변종이 지속적으로 등장해 컴퓨터 사용자를 괴롭힘.
 - 2005년 : 멀티미디어 메시징 서비스(MMS)를 이용해 감염된 휴대폰에 저장된 전화번호로 악성코드를 퍼뜨리는 휴대폰 악성코드 컴워리어(CommWarrior)가 등장
 - 플로피 디스크와 같은 저장 미디어나 인터넷 등을 통해서만 전파되던 악성코드가 **핸드폰 통신망을 통해 전파**되기에 이룸.
 - 악성코드는 수백만 종에 이르며, 악성코드로 인한 피해액은 수백억 달러에 이르고 그 액수도 해마다 커지고 있음.

01 악성코드

■ 악성코드의 분류

[표 1] 악성코드의 분류

| 이름(코드) | 설명 |
|----------|--|
| 바이러스 | <ul style="list-style-type: none">• 사용자 컴퓨터(네트워크로 공유된 컴퓨터 포함) 내에서 사용자 몰래 프로그램이나 실행 가능한 부분을 변형해 자신 또는 자신의 변형을 복사하는 프로그램이다.• 가장 큰 특성은 복제와 감염이다. 다른 네트워크의 컴퓨터로 스스로 전파되지는 않는다. |
| 웜 | <ul style="list-style-type: none">• 인터넷 또는 네트워크를 통해서 컴퓨터에서 컴퓨터로 전파되는 악성 프로그램이다.• 윈도우의 취약점 또는 응용 프로그램의 취약점을 이용하거나 이메일이나 공유 폴더를 통해 전파되며, 최근에는 공유 프로그램(P2P)을 이용하여 전파되기도 한다.• 바이러스와 달리 스스로 전파되는 특성이 있다. |
| 트로이 목마 | <ul style="list-style-type: none">• 바이러스나 웜처럼 컴퓨터에 직접적인 피해를 주지는 않지만, 악의적인 공격자가 컴퓨터에 침투하여 사용자의 컴퓨터를 조종할 수 있는 프로그램이다.• 고의적으로 만들어졌다는 점에서 프로그래머의 실수인 버그와는 다르다.• 자기 자신을 다른 파일에 복사하지 않는다는 점에서 컴퓨터 바이러스와 구별된다. |
| 인터넷 악성코드 | <ul style="list-style-type: none">• 인가되지 않은 성인 사이트나 크랙 사이트 등에 접속할 때 감염된다.• 예전에는 인터넷 악성코드로 끝나는 경우가 많았으나 최근에는 웜의 형태로 전이되고 있다. |
| 스파이웨어 | <ul style="list-style-type: none">• 자신이 설치된 시스템의 정보를 원격지의 특정한 서버에 주기적으로 보내는 프로그램이다.• 사용자가 주로 방문하는 사이트, 검색어 등 취향을 파악하기 위한 것도 있지만 패스워드 등과 같은 특정 정보를 원격지에 보내는 스파이웨어도 존재한다. |

01 악성코드

■ 악성코드의 분류

[표 2] 악성 프로그램으로 인해 발생할 수 있는 증상

| 대분류 | 소분류 | 설명 |
|-----------|--------------|--|
| 시스템 관련 | 시스템 설정 정보 변경 | 변경 레지스트리 키 값을 변경하여 시스템의 정보를 변경한다. |
| | FAT 파괴 | 시스템의 파일 시스템을 파괴한다. |
| | CMOS 변경 | CMOS 내용을 변경하여 부팅 때 에러를 발생시킨다. |
| | CMOS 정보 파괴 | CMOS의 일부를 파괴한다. |
| | 기본 메모리 감소 | 시스템의 기본 메모리를 줄인다. |
| | 시스템 속도 저하 | 시스템의 속도를 저하시킨다. |
| | 프로그램 자동 실행 | 레지스터리 값을 변경해 시스템을 부팅할 때 특정 프로그램을 자동으로 실행시킨다. |
| | 프로세스 종료 | 특정 프로세스를 강제로 종료시킨다. |
| | 시스템 재부팅 | 시스템을 재부팅시킨다. |
| 네트워크 관련 | 메일 발송 | 특정 사용자에게 메일을 발송한다. |
| | 정보 유출 | 사용자의 정보를 네트워크를 통해서 공격자 컴퓨터로 전송한다. |
| | 네트워크 속도 저하 | 감염된 컴퓨터가 속한 네트워크가 느려진다. |
| | 메시지 전송 | 메시지를 네트워크를 통해 다른 컴퓨터로 전달한다. |
| | 특정 포트 오픈 | 특정 백도어 포트를 연다. |
| 하드 디스크 관련 | 하드 디스크 포맷 | 하드 디스크를 포맷한다. |
| | 부트 섹터 파괴 | 하드 디스크의 특정 부분을 파괴한다. |
| 파일 관련 | 파일 생성 | 특정 파일(주로 백도어 파일)을 생성한다. |
| | 파일 삭제 | 특정 파일이나 디렉터리를 삭제한다. |
| | 파일 감염 | 바이러스가 특정 파일을 감염시킨다. |
| | 파일 손상 | 바이러스가 특정 파일에 겹쳐 쓰기 형태로 감염되면 파일이 손상된다. |
| 특이 증상 | 이상 화면 출력 | 출력 화면에 특정 내용이 나타난다. |
| | 특정음 | 발생 컴퓨터에서 특정음이 난다. |
| | 메시지 상자 출력 | 화면에 특정 메시지 상자가 나타난다. |
| | 증상 없음 | 특이한 증상이 없다. |

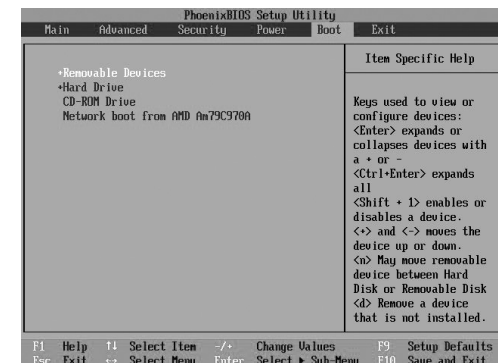
02 바이러스

■ 바이러스의 정의

- 악성코드 중에 가장 기본적인 형태
- 사용자 컴퓨터(네트워크로 공유된 컴퓨터 포함) 내에서 사용자 몰래 프로그램이나 실행 가능한 부분을 변형해 자신 또는 자신의 변형을 복사하는 프로그램을 말함
- 최초의 악성 코드가 만들어진 1980년대 이후에서 2000년대 초반까지 악성 코드의 주류를 차지

■ 1세대 : 원시형 바이러스

- 부트 바이러스
 - 플로피 디스크나 하드 디스크의 부트 섹터에 감염되는 바이러스로, 부팅할 때 자동으로 동작
 - 1단계 : POST
 - POST는 하드웨어 자체가 시스템에 문제가 없는지 기본 사항을 스스로 체크하는 과정
 - BIOS에 의해서 실행되는데, POST 도중 하드웨어에서 문제가 발견되면 사용자에게 여러 방법으로 그 문제를 알림.
 - 2단계 : CMOS
 - CMOS에서는 기본 장치에 대한 설정과 부팅 순서를 설정할 수 있음.
 - BIOS는 CMOS에서 이런 기본 설정 사항을 읽어 시스템에 적용



[그림 3] CMOS의 부팅 순서 결정

02 바이러스

■ 1세대 : 원시형 바이러스

• 3단계 : 운영체제 위치 정보 로드

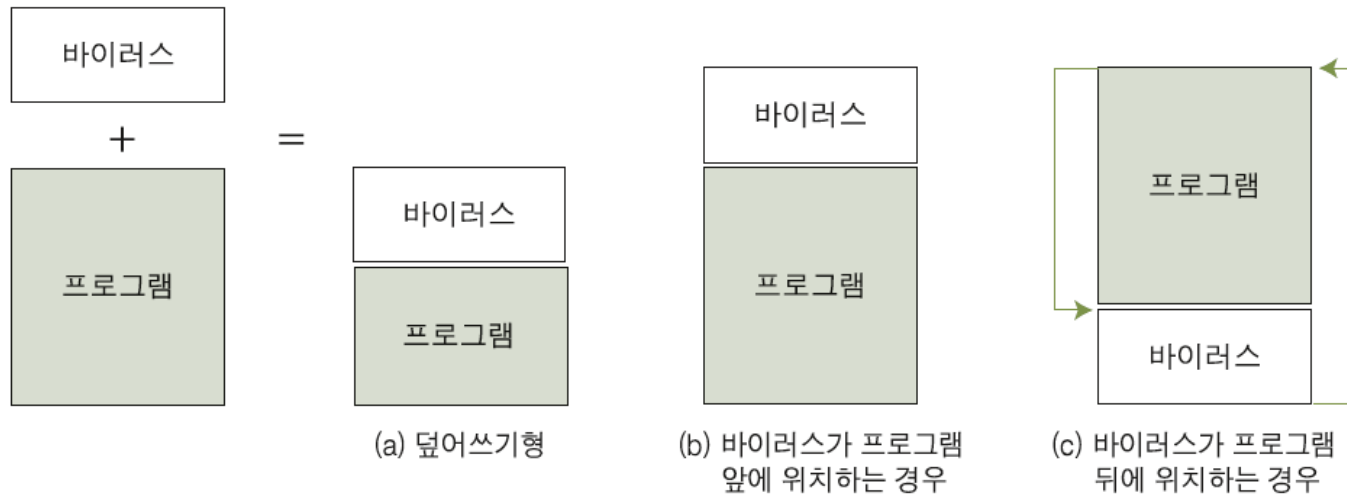
- 윈도우 2003 이전 : CMOS 정보를 읽어 부팅 매체를 확인한 뒤 부팅 매체의 MBR(Master Boot Record) 정보를 읽음.
 - » MBR은 운영체제가 어디에, 어떻게 위치해 있는지를 식별하여 컴퓨터의 주 기억장치에 적재될 수 있도록 하기 위한 정보로, 하드 디스크나 디스켓의 첫 번째 섹터에 저장되어 있음.
 - » MBR은 메모리에 적재될 운영체제가 저장된 파티션의 부트 섹터 레코드를 읽을 수 있는 프로그램
 - » 이때 부트 섹터 레코드는 운영체제의 나머지 부분을 메모리에 적재시키는 프로그램을 담고 있음.
- 윈도우 2008 이후 : 윈도우 부트 서브 시스템(Window Boot Manager)이 실행됨.
 - » 윈도우 부트 서브 시스템은 bootmgr.exe가 실행되고 부트 설정 데이터(BCD, Boot Configuration Data)를 읽어 실행 가능한 운영체제의 목록을 보여줌.
 - » 이것은 NTDLR이 boot.ini을 읽어 실행 가능한 운영체제의 목록을 보여주는 것과 같음.
- 부트 바이러스는 이 3단계에서 동작.
- 부트 바이러스에 감염된 플로피 디스크로 운영체제를 구동시키면 바이러스가 MBR과 함께 PC 메모리에 저장되고 부팅 후에 사용되는 모든 프로그램에 자신을 감염시킴.
- 부트 바이러스는 브레인, 몽키, 미켈란젤로 바이러스가 있음.

02 바이러스

■ 1세대 : 원시형 바이러스

■ 파일 바이러스

- 파일을 직접 감염시키는 바이러스
- 하드 디스크가 PC에서 일반화되면서 그 대안으로 나온 형태
- 일반적으로 COM이나 EXE와 같은 실행 파일과 오버레이 파일, 디바이스 드라이버 등에 감염
- 전체 바이러스의 80% 이상을 차지
- 바이러스에 감염된 실행 파일이 실행될 때 바이러스 코드를 실행.



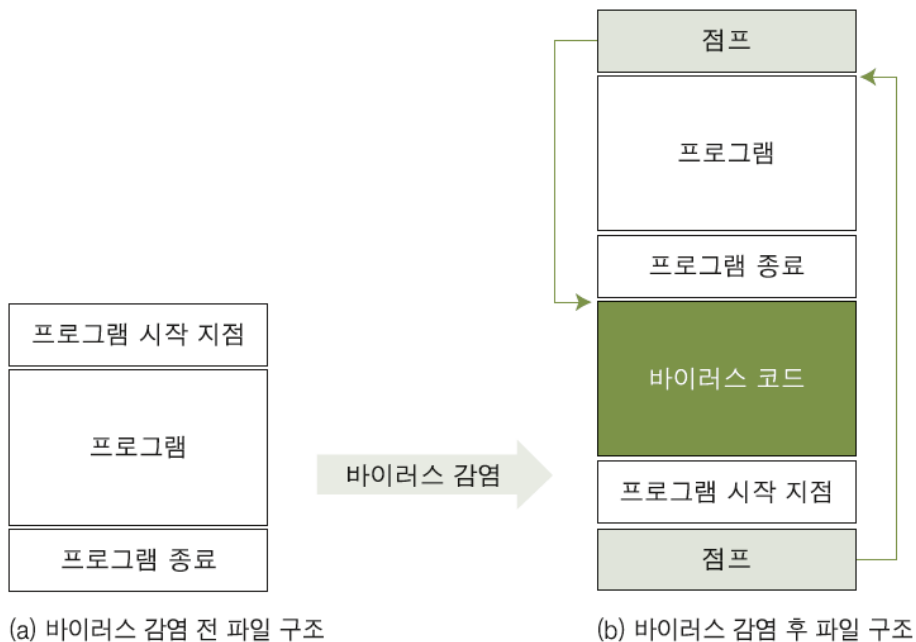
[그림 4] 파일 바이러스의 감염 위치

02 바이러스

■ 1세대 : 원시형 바이러스

■ 파일 바이러스

- 바이러스가 프로그램의 뒷부분에 위치하게 된 이유는 백신의 바이러스 스캔으로부터 자신의 존재를 숨기기 위해서임.



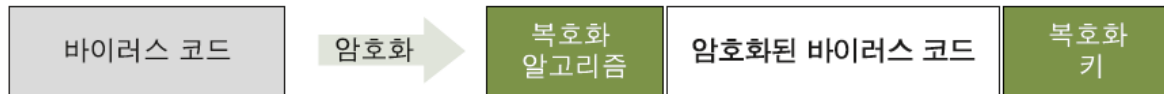
[그림 5] 바이러스가 프로그램 뒤에 있는 경우 실행 루틴

- 예루살렘 바이러스가 최초의 파일 바이러스로 알려져 있음
- 이외에도 썬데이, 스킴피온, 크로우, FCL 등이 있음. CIH 바이러스도 이에 해당됨.

02 바이러스

■ 2세대 : 암호형 바이러스

- 바이러스 코드를 쉽게 파악하고 제거할 수 없도록 암호화한 바이러스
- 바이러스 제작자들은 백신의 진단을 우회하기 위해 자체적으로 코드를 암호화하는 방법을 사용하여 백신 프로그램이 진단하기 힘들게 만들기 시작함.



[그림 6] 암호화된 바이러스 코드

- 바이러스가 동작할 때 메모리에 올라오는 과정에서 암호화가 풀림.
 - 이를 이용하여 메모리에 실행되어 올라온 바이러스를 거꾸로 분석하여 감염파일과 바이러스를 분석하고 치료
- 슬로우(Slow), 캐스케이드(Cascade), 원더러(Wanderer), 버글러(burglar) 등이 있음.

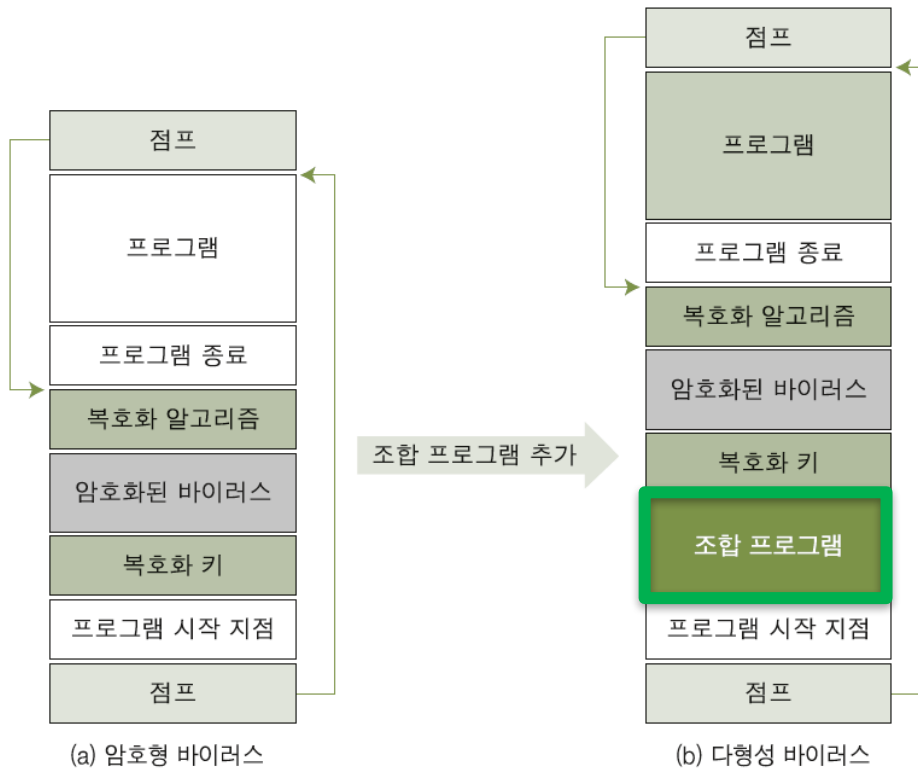
■ 3세대 : 은폐형 바이러스

- 바이러스에 감염된 파일들이 일정 기간의 잠복기를 가지도록 만들어진 바이러스
- 확산되기도 전에 바이러스가 활동하기 시작하면 다른 시스템으로 전파되기 힘들기 때문.
 - 이런 이유로 감염이 되더라도 실제로 바이러스가 동작하기 전까지 쉽게 그 존재를 파악하기 힘들었음.
- 브레인(Brain), 조시(Joshi), 512, 4096 바이러스 등이 있음.

02 바이러스

■ 4세대 : 다형성 바이러스

- 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.

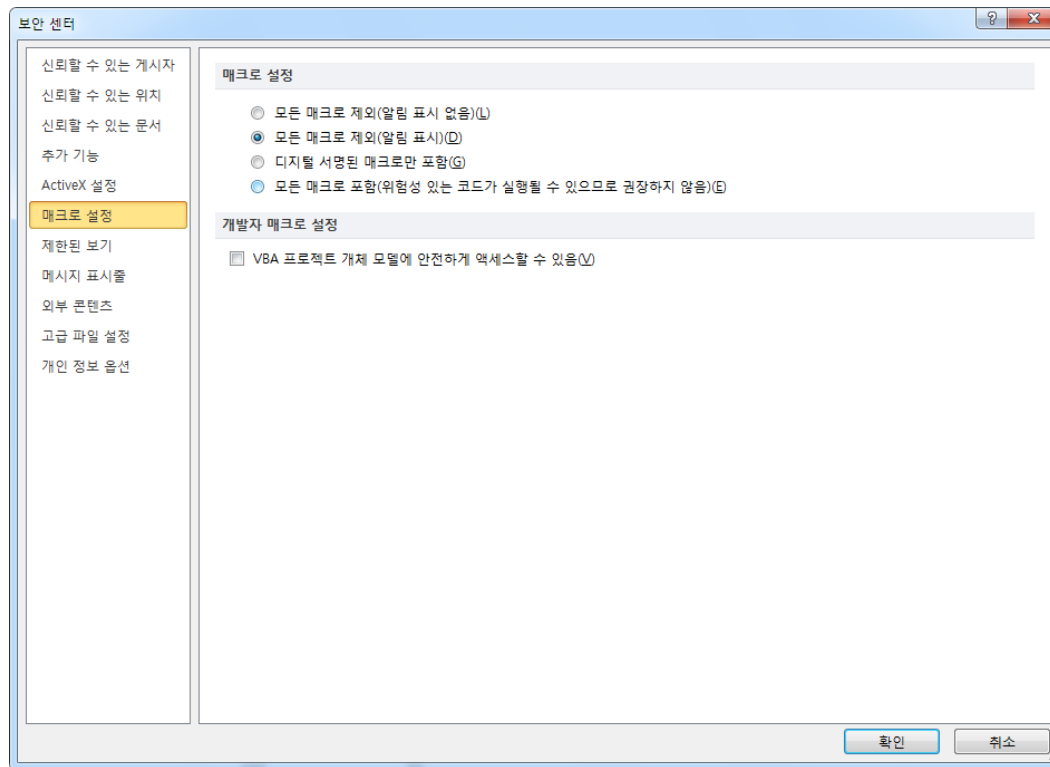


[그림 7] 다형성 바이러스

02 바이러스

■ 5세대 : 매크로 바이러스

- 기존의 바이러스는 실행할 수 있는 파일(COM이나 EXE)에 감염된 반면, 매크로 바이러스는 엑셀 또는 워드와 같은 문서 파일의 매크로 기능을 이용하기 때문에 워드나 엑셀 파일을 열 때 감염됨.
- 워드 컨셉트(Word Concept), 와쭈(Wazzu), 엑셀-라룩스(Laloux) 바이러스 등이 있음.



[그림 7] 다형성 바이러스

02 바이러스

■ 5세대 : 매크로 바이러스

- 매크로 바이러스의 증상
 - 문서가 정상적으로 열리지 않거나 암호가 설정되어 있음.
 - 문서 내용에 깨진 글자나 이상한 문구가 포함되어 있음.
 - 도구 메뉴 중 매크로 메뉴가 실행할 수 없게 잠겨 있음.
 - 엑셀이나 워드 작업 중 VB(Visual Basic) 편집기의 디버그 모드가 실행됨.

■ 차세대 바이러스

- 최근에는 매크로 바이러스에서 나타난 스크립트 형태의 바이러스가 더욱 활성화되고 있음.
- 대부분 네트워크와 메일을 이용하여 전파되는 방식
- 바이러스는 단순히 데이터를 파괴하고 다른 파일을 감염시키는 형태에서 벗어나, 사용자 정보를 빼내거나 시스템을 장악하기 위한 백도어 기능을 가진 웜의 형태로 진화하고 있음

03 웜

■ 웜의 등장

- 웜(Worm)은 인터넷 또는 네트워크를 통해서 컴퓨터에서 컴퓨터로 전파되는 프로그램을 의미
- 1999년 다른 사람의 이메일 주소를 수집하고 스스로 전달되는 형태의 인터넷 웜이 출현하면서 일반인에게 웜이라는 용어가 알려지기 시작
- 이메일에 첨부 파일 형태로 첨부되어 확산되거나, 운영체제나 프로그램의 보안 취약점을 이용하여 스스로 침투하는 것이 일반적
 - 현재는 mIRC 채팅 프로그램, P2P 파일 공유 프로그램, 이메일 관련 스크립트 기능, 네트워크 공유 기능 등의 허점을 이용하여 확산하고 증식하는 경우도 있어 피해와 부작용의 범위/크기가 계속 커지고 있음.

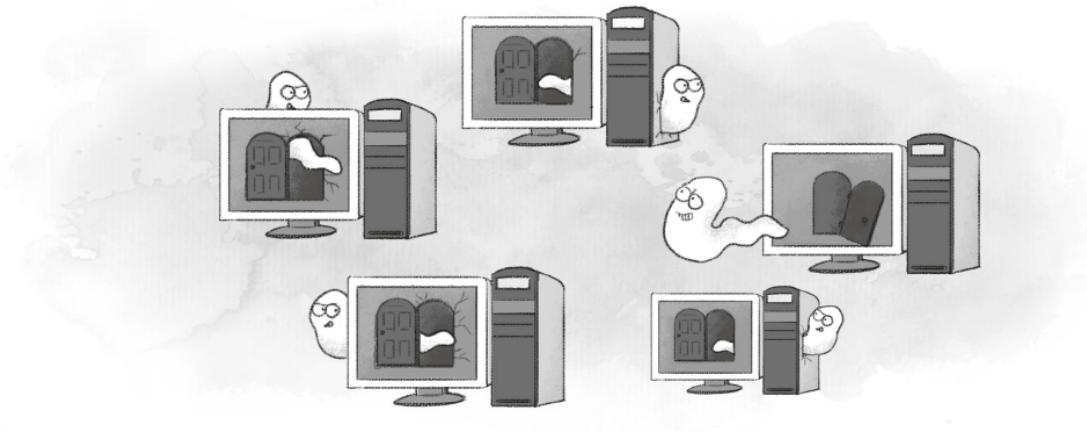
■ MASS Mailer형 웜

- MASS Mailer형 웜은 자기 자신을 포함하는 대량 메일 발송을 통해 확산
- 최근 발생한 웜 중 약 40%가 MASS Mailer 형에 해당.
- 제목이 없거나 특정 제목으로 전송되는 메일을 읽었을 때 감염
- 치료하지 않으면 시스템에 계속 기생하면서 시스템 내부에서 메일 주소를 수집해 계속 메일을 보냄.
- MASS Mailer형 웜의 주요 증상
 - 메일로 전파. 감염된 시스템이 많으면 SMTP 서버(TCP 25번 포트)의 네트워크 트래픽이 증가
 - 베이글은 웜 파일을 실행할 때 'Can't find a viewer associated with the file'과 같은 가짜 오류 메시지를 출력
 - 넷스카이는 윈도우 시스템 디렉터리 밑에 CSRSS.exe를 만들.
 - 변형된 종류에 따라 시스템에 임의의 파일을 생성
 - 확인되지 않은 메일을 열어볼 때 확산됨.
- MASS Mailer형 웜의 종류로는 베이글(Bagle), 넷스카이(Netsky), 두마루(Dumaru), 소빅(Sobig) 등이 있음.

03 웹

■ 시스템 공격형 웜

- 운영체제 고유의 취약점을 이용해 내부 정보를 파괴하거나, 컴퓨터를 사용할 수 없는 상태로 만들거나, 혹은 외부의 공격자가 시스템 내부에 접속할 수 있도록 백도어를 설치하는 웜
- 시스템 공격형 웜의 주요증상
 - 전파할 때 과다한 TCP/135,445 트래픽이 발생
 - windows, windows/system32, winnt, winnt/system32 폴더에 SVCHOST.EXE 등의 파일을 설치
 - 공격 성공 후 UDP/5599 등의 특정 포트를 열어 외부 시스템과 통신
 - 시스템 파일 삭제, 정보 유출(게임CD 시리얼 키 등)이 가능



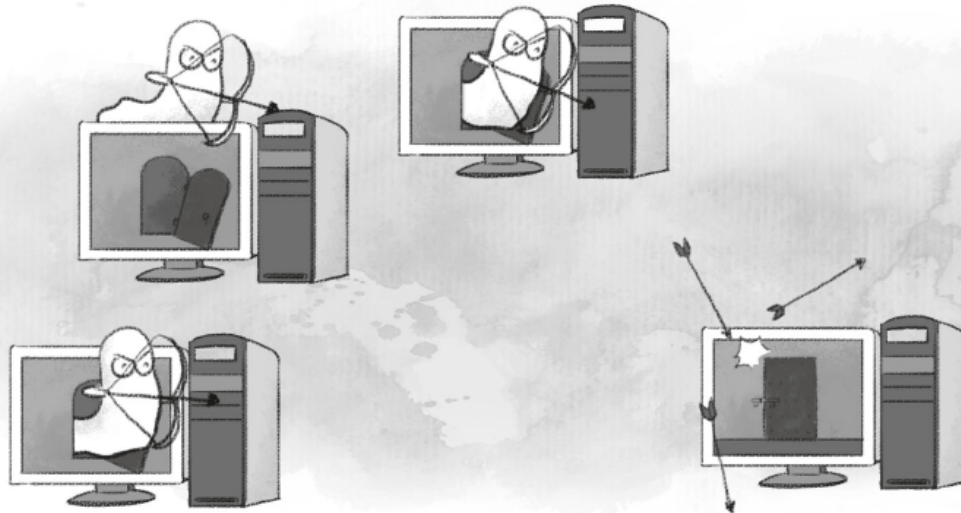
[그림 9] 취약한 시스템에 대한 웜의 공격

- 시스템 공격형 웜의 종류로는 아고봇(Agobot), 블래스터(Blaster.worm), 웰치아(Welchia) 등이 있음.

03 웹

■ 네트워크 공격형 웹

- 특정 네트워크나 시스템에 대해 Syn Flooding, Smurf와 같은 서비스 거부(DoS) 공격을 수행
- 네트워크 공격형 웹은 분산 서비스 거부(DDOS) 공격을 위한 봇(Bot)과 같은 형태로 발전하고 있음.
- 네트워크 공격형 웹의 주요 증상
 - 네트워크가 마비되거나, 급속도로 느려짐.
 - 네트워크 장비가 비정상적으로 동작



[그림 10] 웹에 의해 감염된 시스템에서의 네트워크 공격

- 네트워크 공격형 웹의 종류로는 저봇(Zerbo), 클레즈(Klez) 등이 있음.

04 기타 악성코드

■ 백도어와 트로이 목마

- 백도어(Backdoor)의 원래 의미는 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로
 - 다른 말로 Administrative hook이나 트랩 도어(Trap Door)라고도 함.
- 트로이 목마는 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 형태



[그림 11] 트로이 목마

04 기타 악성코드

■ 인터넷 악성코드

- 인터넷 악성코드의 증상
 - 인터넷 익스플로러의 시작 페이지가 계속 다른 곳으로 변경됨.
 - 인터넷 속도가 느려지거나 끊김.
 - 시스템의 비정상적인 작동으로 운영체제가 사용 불능의 상태가 됨.
- 인터넷 악성코드를 막는 방법
 - 익스플로러의 [도구]-[보안]-[사용자 지정수준] 메뉴를 클릭→ [보안 설정] 창에서 각 사항을 '확인'으로 설정
 - 해당 프로그램이 인터넷에서 자동으로 설치되는 것을 막고 사용자가 확인할 수 있음.

■ 스파이웨어

- 자신이 설치된 시스템의 정보를 원격지의 특정한 서버에 주기적으로 보내는 프로그램
- 사용자가 주로 방문하는 사이트, 검색어 등 취향을 파악하기 위한 것도 있었으나, 패스워드 등과 같은 특정 정보를 원격지에 보내는 스파이웨어도 있음.

05 악성코드 탐지 및 대응책

■ 네트워크 상태 점검하기

- 상당수의 백도어는 외부(해커, 악성코드 작성자)와의 통신을 위해 서비스 포트를 생성

[표 2] 주요 백도어 사용 포트

| 포트번호 | 트로이 목마 | 포트번호 | 트로이 목마 |
|------|-------------------------|------|--------------------|
| 21 | TrojanFore | 1080 | WinHole |
| 23 | Tiny Telnet Server[TTS] | 1090 | Xtreme |
| 25 | NaebiHappy | 1150 | Orion |
| 31 | Agent, ParadiseMasters | 1234 | Ultors Trojan |
| 41 | DeepThroat Foreplay | 1243 | Backdoor G |
| 80 | WWW Tunnel | 1245 | VooDoo Doll |
| 119 | Happy 99 | 1257 | Frenzy 2000 |
| 133 | Farnaz | 1272 | The Matrix |
| 137 | ChodeMSinit (UDP) | 1441 | Remote Storm |
| 514 | RPCBackdoor | 1524 | Trin00 |
| 555 | Seven Eleven | 1999 | Sub Seven |
| 666 | ServeU | 2140 | Deep Throat 1.3 |
| 667 | SniperNet | 2255 | Nirvana |
| 777 | AIM Spy | 2583 | WinCrash |
| 808 | WinHole | 2773 | Sub Seven Gold 2.1 |
| 999 | Deep Throat | 3459 | Eclipse 2000 |
| 1001 | Silencer | 5400 | Blade Runner |
| 1016 | Doly Trojan | 5880 | Y3K Rat |
| 1024 | NetSpy | 8787 | BackOrifice 2000 |

05 악성코드 탐지 및 대응책

■ 네트워크 상태 점검하기

- 시스템에서는 netstat와 같은 명령으로 열려 있는 포트를 확인할 수 있음.

```
관리자: C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat -an

활성 연결

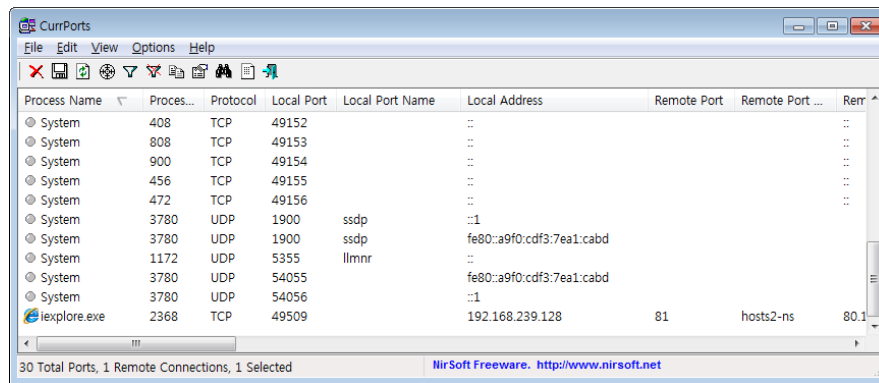
프로토콜  로컬 주소          외부 주소          상태
TCP       0.0.0.0:135      0.0.0.0:0          LISTENING
TCP       0.0.0.0:445      0.0.0.0:0          LISTENING
TCP       0.0.0.0:902      0.0.0.0:0          LISTENING
TCP       0.0.0.0:912      0.0.0.0:0          LISTENING
TCP       0.0.0.0:2869     0.0.0.0:0          LISTENING
TCP       0.0.0.0:3390     0.0.0.0:0          LISTENING
TCP       0.0.0.0:5357     0.0.0.0:0          LISTENING
TCP       0.0.0.0:17106    0.0.0.0:0          LISTENING
TCP       0.0.0.0:17500    0.0.0.0:0          LISTENING
TCP       0.0.0.0:19851    0.0.0.0:0          LISTENING
TCP       0.0.0.0:31427    0.0.0.0:0          LISTENING
TCP       0.0.0.0:49152    0.0.0.0:0          LISTENING
TCP       0.0.0.0:49153    0.0.0.0:0          LISTENING
TCP       0.0.0.0:49154    0.0.0.0:0          LISTENING
TCP       0.0.0.0:49161    0.0.0.0:0          LISTENING
TCP       0.0.0.0:49164    0.0.0.0:0          LISTENING
```

[그림 15] netstat -an 실행 결과

05 악성코드 탐지 및 대응책

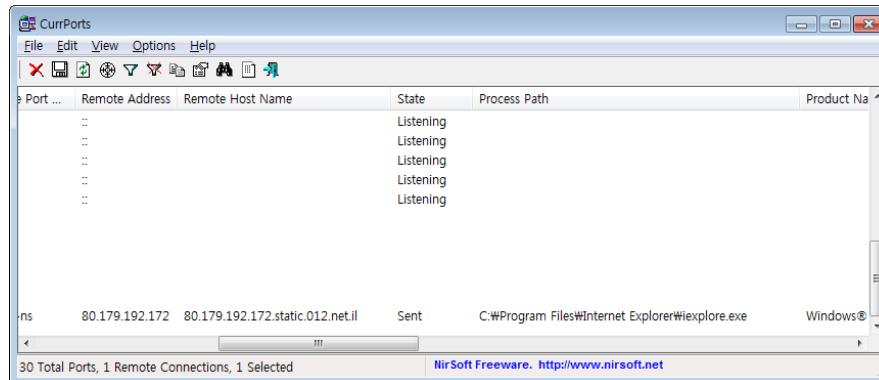
■ 네트워크 상태 점검하기

- 악성코드가 사용하는 포트를 확인하기 어려운 경우 CPorts와 같은 프로그램을 사용하여 서비스 포트별로 사용하는 응용 프로그램을 확인할 수 있음.
- BackDoor-DVR를 실행한 뒤 CPorts에서 활성화된 네트워크 항목을 살펴보면 특이한 연결이 존재



www.nirsoft.net/utils

(a)



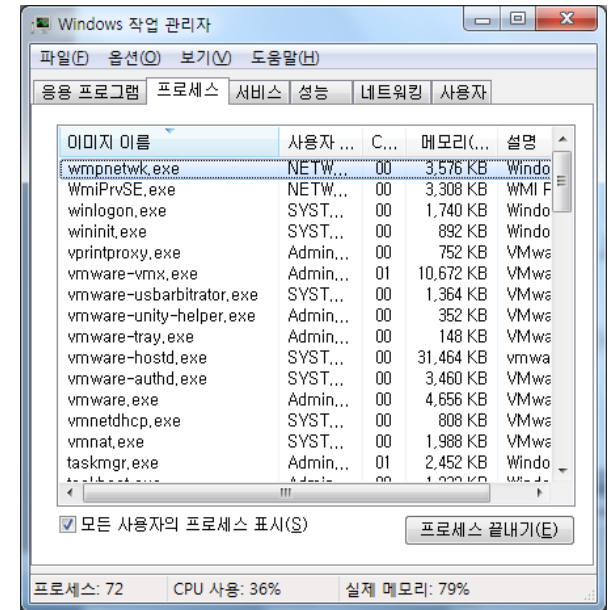
(b)

[그림 15] CPorts 실행 결과

05 악성코드 탐지 및 대응책

■ 정상적인 프로세스와 비교하기

- 윈도우와 유닉스 시스템 등의 정상적인 프로세스를 외워두면 비정상적인 프로세스를 식별하는 데 많은 도움이 됨.
- 윈도우 시스템이 동작하기 위한 기본 프로세스
 - Csrss.exe(Client/Server Runtime SubSystem : Win 32) : 윈도우 콘솔을 관장하고, 스레드를 생성·삭제하며 32비트 가상 MS-DOS 모드를 지원
 - Explorer.exe : 작업표시줄, 바탕화면과 같은 사용자 셸을 지원
 - Lsass.exe(Local Security Authentication Server) : Winlogon 서비스에 필요한 인증 프로세스를 담당
 - Mstask.exe(Window Task Scheduler) : 시스템에 대한 백업이나 업데이트 등에 관련된 작업의 스케줄러
 - Smss.exe(Session Manager SubSystem) : 사용자 세션을 시작하는 기능을 담당. 이 프로세스는 Winlogon, Win32(Csrss.exe)을 구동시키고, 시스템 변수를 설정. Smss는 Winlogon이나 Csrss가 끝나기를 기다려 정상적인 Winlogon, Csrss 종료시 시스템을 종료시킴.
 - Spoolsv.exe(Printer Spooler Service) : 프린터와 팩스의 스푼링 기능을 담당
 - Svchost.exe(Service Host Process) : DLL(Dynamic Link Libraries)에 의해 실행되는 프로세스의 기본 프로세스. 한 시스템에서 여러 개의 svchost 프로세스를 볼 수 있음.



[그림 16] 윈도우에서 동작 중인 프로세스 확인

05 악성코드 탐지 및 대응책

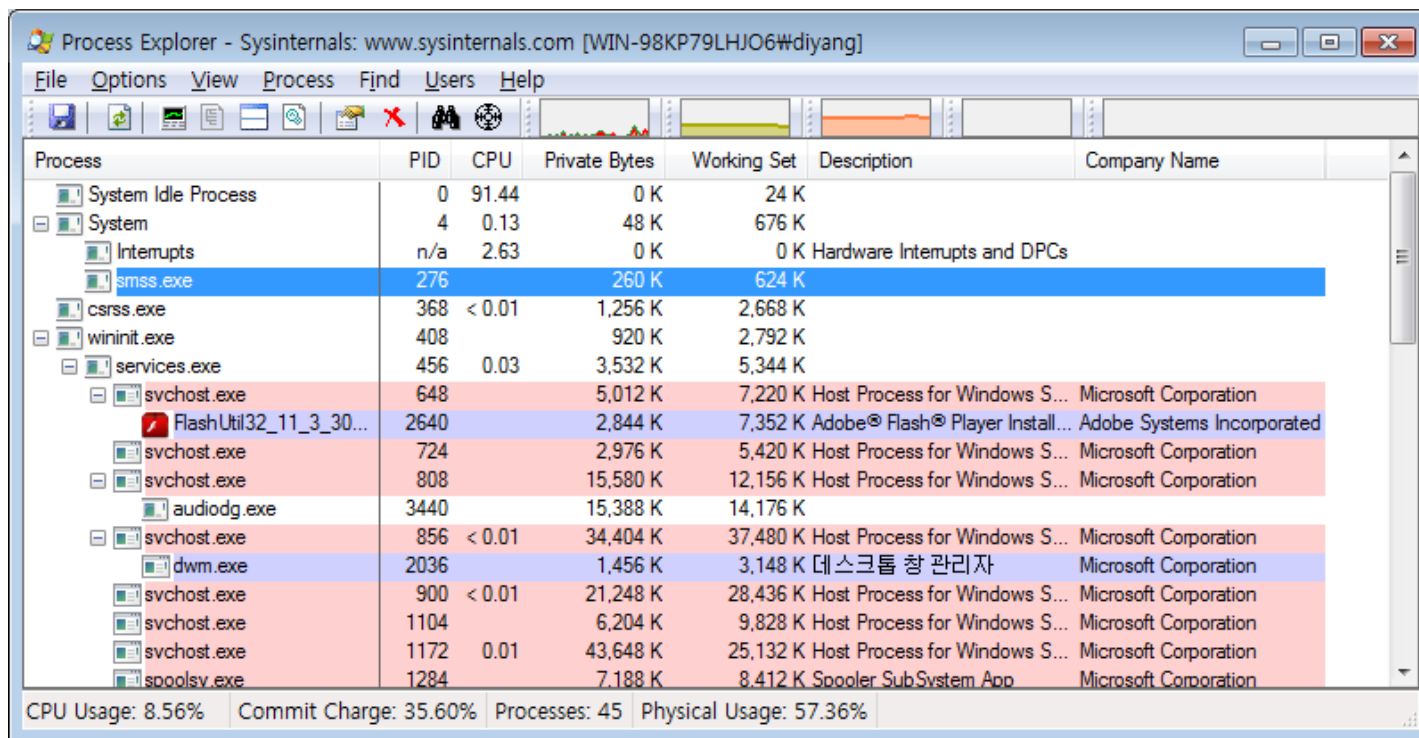
■ 정상적인 프로세스와 비교하기

- 웹/바이러스나 백도어가 주로 사용하는 서비스명은 Csrss와 Svchost
 - Services.exe (Service Control Manager) : 시스템 서비스를 시작/정지시키고, 그들간의 상호 작용하는 기능을 수행
 - System : 대부분의 커널 모드 스레드의 시작점이 되는 프로세스
 - System Idle Process : 각 CPU마다 하나씩 실행되는 스레드로서 CPU의 잔여 프로세스 처리량을 %로 나타낸 값
 - Taskmgr.exe(Task Manager) : 작업 관리자 자신
 - Winlogon.exe(Windows Logon Process) : 사용자 로그인/로그오프를 담당하는 프로세스. 윈도우의 시작/종료 시에 활성화되며 Ctrl+Alt+Delete 키를 눌렀을 경우에도 활성화됨.
 - Winmgmt.exe (Window Management Service) : 장치에 대한 관리 및 계정 관리, 네트워크 등의 동작에 관련한 스크립트를 위한 프로세스
 - msdtc.exe (Distributed Transaction Coordinator) : 웹 서버 및 SQL 서버 구동 시에 다른 서버와의 연동을 위한 프로세스
 - ctfmon.exe (Alternative User Input Services) : 키보드, 음성, 손으로 적은 글 등 여러 가지 텍스트 입력에 대한 처리를 할 수 있도록 지원하는 프로세스
 - dfssvc.exe (Distributed File System (DFS)) : 분산 파일 시스템(Distributed File System (DFS))에 대한 지원을 위해 백그라운드로 실행되고 있는 프로세스

05 악성코드 탐지 및 대응책

■ 정상적인 프로세스와 비교하기

- 좀더 자세한 프로세스 정보를 알고 싶은 경우에는 [Process Explorer](#)를 사용



| Process | PID | CPU | Private Bytes | Working Set | Description | Company Name |
|------------------------|------|--------|---------------|-------------|---------------------------------|----------------------------|
| System Idle Process | 0 | 91.44 | 0 K | 24 K | | |
| System | 4 | 0.13 | 48 K | 676 K | | |
| Interrupts | n/a | 2.63 | 0 K | 0 K | Hardware Interrupts and DPCs | |
| smss.exe | 276 | | 260 K | 624 K | | |
| csrss.exe | 368 | < 0.01 | 1,256 K | 2,668 K | | |
| wininit.exe | 408 | | 920 K | 2,792 K | | |
| services.exe | 456 | 0.03 | 3,532 K | 5,344 K | | |
| svchost.exe | 648 | | 5,012 K | 7,220 K | Host Process for Windows S... | Microsoft Corporation |
| FlashUtil32_11_3_30... | 2640 | | 2,844 K | 7,352 K | Adobe® Flash® Player Install... | Adobe Systems Incorporated |
| svchost.exe | 724 | | 2,976 K | 5,420 K | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | 808 | | 15,580 K | 12,156 K | Host Process for Windows S... | Microsoft Corporation |
| audiodg.exe | 3440 | | 15,388 K | 14,176 K | | |
| svchost.exe | 856 | < 0.01 | 34,404 K | 37,480 K | Host Process for Windows S... | Microsoft Corporation |
| dwm.exe | 2036 | | 1,456 K | 3,148 K | 데스크톱 환경 관리자 | Microsoft Corporation |
| svchost.exe | 900 | < 0.01 | 21,248 K | 28,436 K | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | 1104 | | 6,204 K | 9,828 K | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | 1172 | 0.01 | 43,648 K | 25,132 K | Host Process for Windows S... | Microsoft Corporation |
| spoolsv.exe | 1284 | | 7,188 K | 8,412 K | Spooler SubSystem App | Microsoft Corporation |

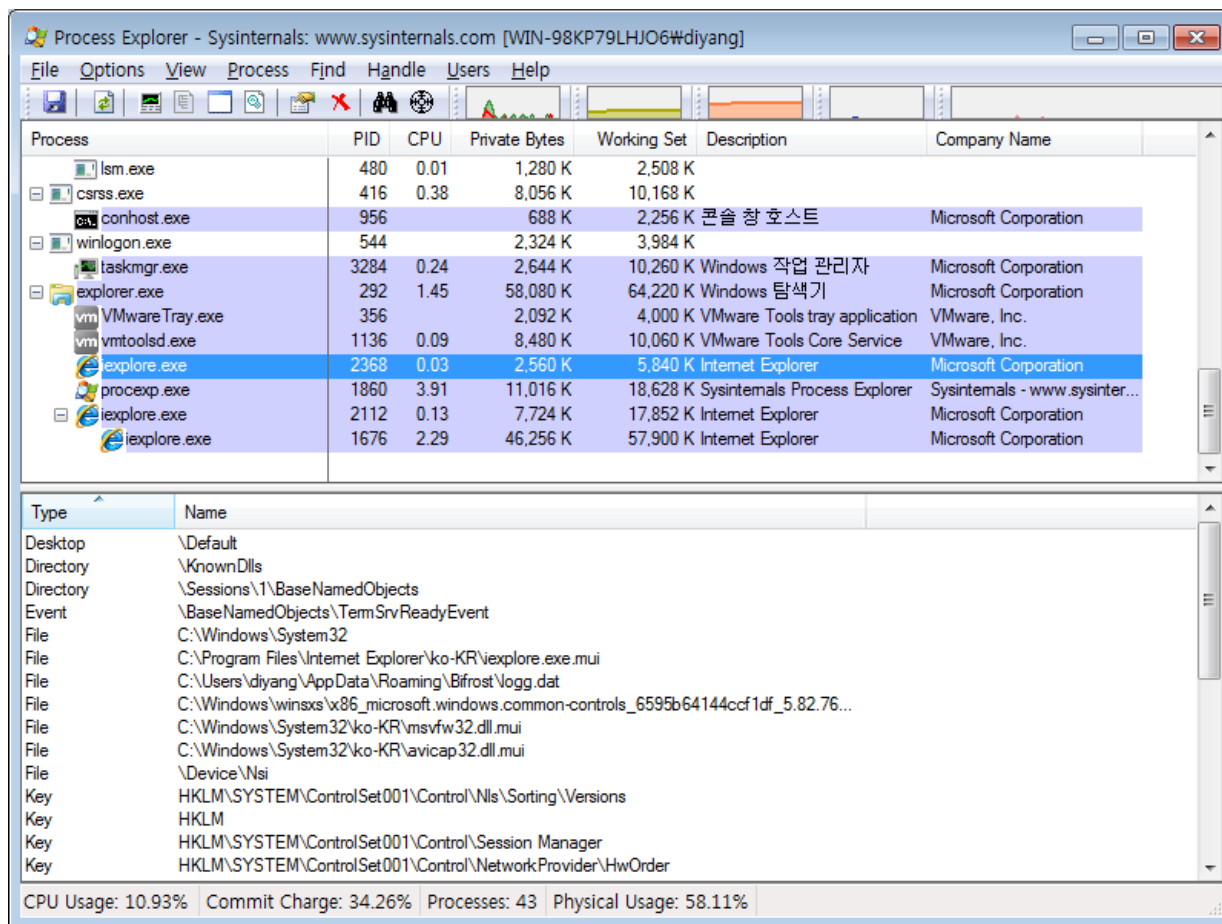
CPU Usage: 8.56% Commit Charge: 35.60% Processes: 45 Physical Usage: 57.36%

[그림 17] Process Explorer를 이용한 프로세스 확인

05 악성코드 탐지 및 대응책

■ 정상적인 프로세스와 비교하기

- Process Explorer에서 '[View]-[Show Lower Pane]' 옵션을 선택하면 해당 프로세스에 자세한 정보를 알 수 있음.

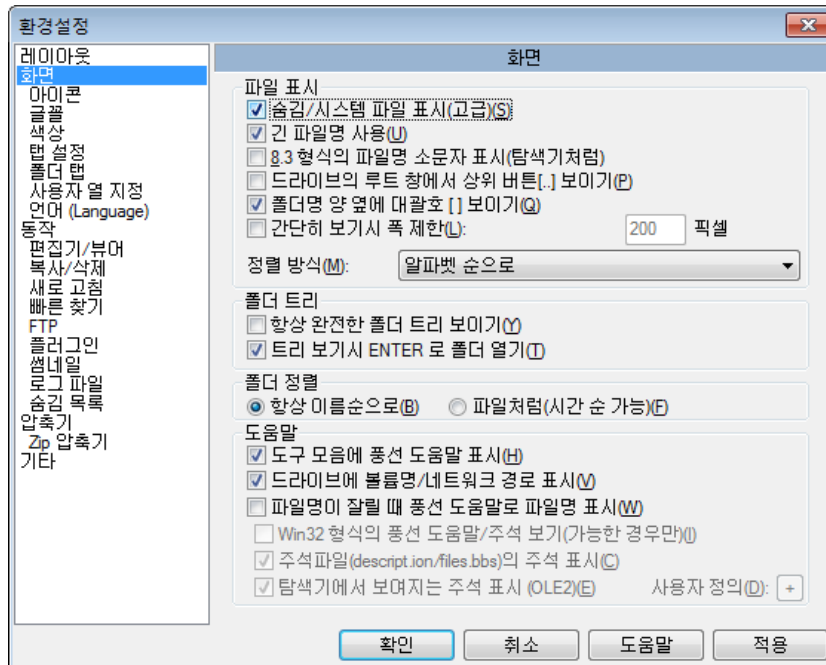


[그림 18] Process Explorer를 이용한 2368번 프로세스 확인

05 악성코드 탐지 및 대응책

■ 백도어의 실질적인 파일 확인하기

- 악성코드 파일을 확인할 때는 [total commander](#)와 같은 툴을 사용
- total commander를 이용해 백도어를 확인하기 전에 [환경설정]-[옵션]-[화면]에서 [숨김/시스템 파일 표시] 옵션을 활성화시켜야 함.

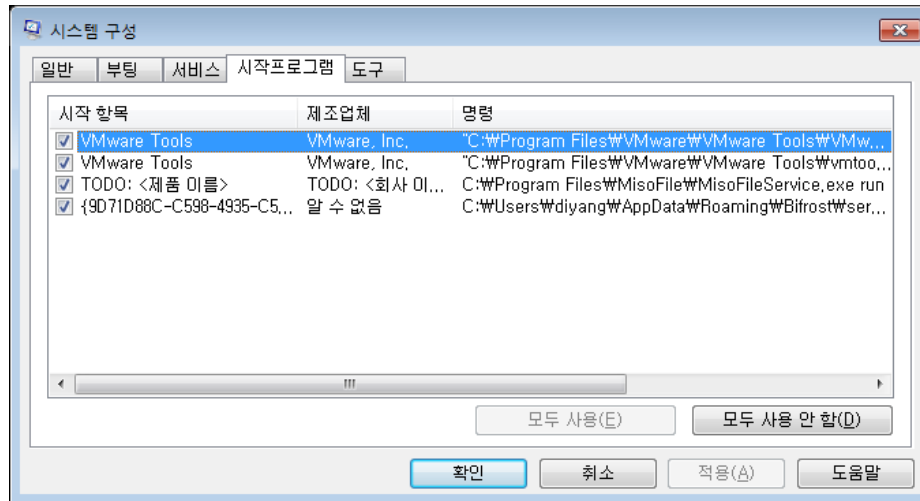


[그림 21] [숨김/시스템 파일 표시] 옵션을 활성화

05 악성코드 탐지 및 대응책

■ 시작 프로그램과 레지스트리 확인하기

- 윈도우 시스템은 시작 프로그램 등의 시스템 운영과 관련하여 리부팅되더라도 기본 설정값이 변하지 않도록 레지스트리에 여러 가지 값을 기록해 둡니다.
- 백도어 역시 이러한 레지스터를 이용하는 경우가 많기 때문에 백도어를 삭제할 때에는 레지스터에서도 이러한 내용을 확인해야 합니다.
- 시작 프로그램 목록은 'msconfig' 명령을 통해 확인



[그림 24] 시작 프로그램 확인

05 악성코드 탐지 및 대응책

■ 백도어 제거하기

■ 백도어를 삭제하는 절차

① 백도어 프로세스의 중지

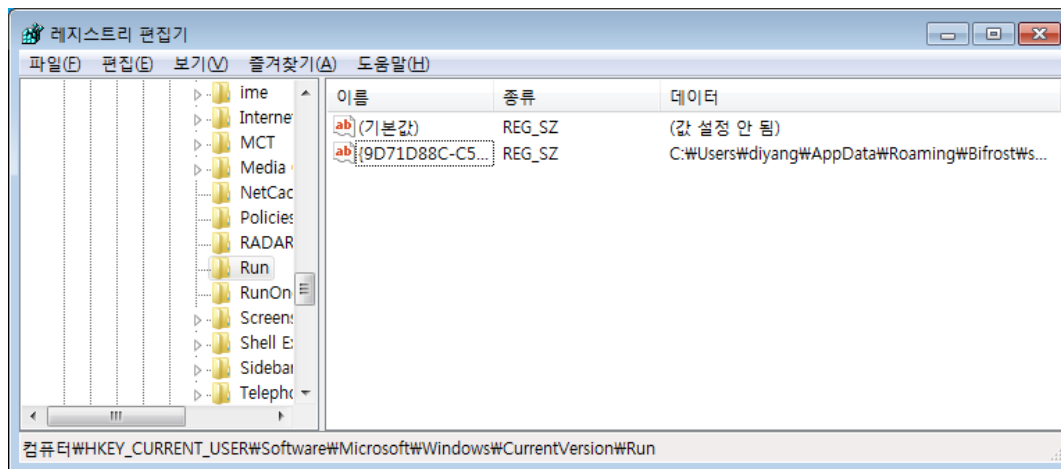
- xxxx 프로세스를 'Kill Process Tree(Shift Del)'로 중지시킴

② 백도어 파일의 삭제

- XXXX 폴더에서 확인한 파일을 삭제
- C:\Windows\system32 폴더에서 확인한 파일을 삭제
- C:\Program Files\XXXX 폴더에서 확인한 파일을 삭제

③ 레지스트리 삭제

- 시작 프로그램에서 확인한 사항을 삭제
- 'regedit'로 레지스트리 경로를 확인할 수 있는데, 레지스트리에서 해당 항목을 삭제함.



[그림 25] 레지스트리에서 해당 레지스트리 확인

Q&A