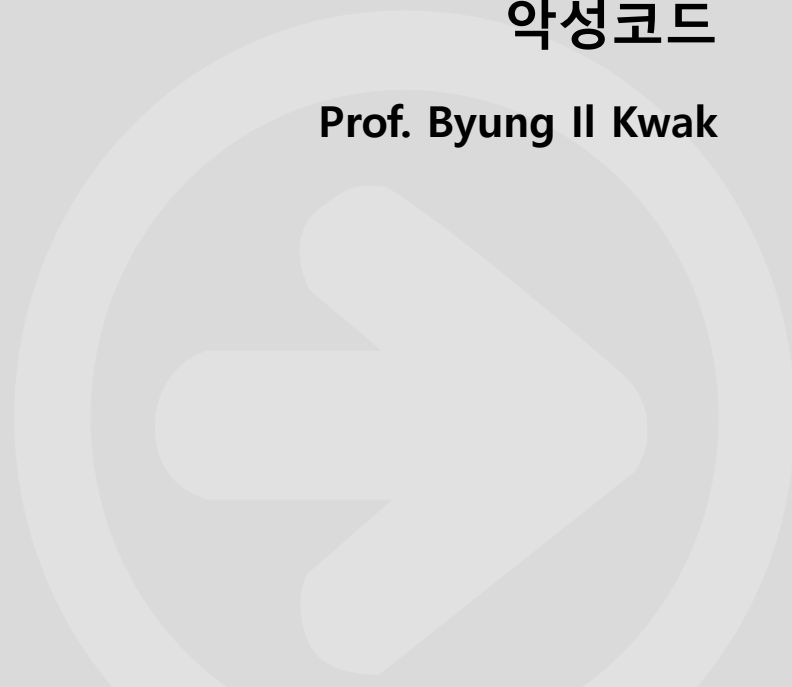




# 정보보호론 #9

악성코드

Prof. Byung Il Kwak



- 시스템 구성과 프로그램 동작
- 버퍼 오버플로 공격
- 포맷 스트링 공격
- 메모리 해킹

- ❑ 악성 코드
- ❑ 바이러스
- ❑ 웜
- ❑ 트로이 목마
- ❑ PUP
- ❑ 악성 코드 탐지 및 대응책

# CONTENTS

---

▣ 악성 코드

## ▣ 악성 코드의 역사

### ▣ 컴퓨터 바이러스 개념의 등장

- 데이비드 제럴드의 공상 과학 소설 《When Harlie Was One》(1972)에 처음 등장
- 1984년에 프레드 코헨이 컴퓨터 바이러스의 개념을 정립함

### ▣ 최초의 바이러스와 웜

- 일반적으로 1986년에 등장한 브레인 바이러스를 최초의 바이러스로 인정
- 최초의 웜은 1988년 미국의 네트워크를 마비시킨 '모리스 웜' 사건의 원인인 모리스 웜

## ▣ 악성 코드의 역사

### ▣ 매크로 바이러스의 출현

- 1999년에 매크로 바이러스로 잘 알려진 멜리사 바이러스 출현
- 매크로: 엑셀이나 워드에서 특정 기능을 자동화한 프로그램
- 시스템 프로그램 같은 고난이도 기술만 웬이나 바이러스 제작에 이용되는 것이 아님을 일깨워준 계기

### ▣ 웬에 의한 대규모 피해 발생

- 2001년 7월 13일 25만 대 이상의 컴퓨터가 8시간 만에 코드레드 웬에 감염.
- 윈도우 2000과 윈도우 NT 서버를 경유지로 미국 백악관 공격
- 국내도 최소 3만 대 이상의 시스템이 피해를 입은 것으로 추정

## ▣ 악성 코드 분류

악성 코드	설명
바이러스	<ul style="list-style-type: none"><li>• 사용자의 컴퓨터(네트워크로 공유된 컴퓨터 포함) 내에서 프로그램이나 실행 가능한 부분을 몰래 변형하여 자신 또는 자신의 변형을 복사하는 프로그램이다.</li><li>• 가장 큰 특성은 복제와 감염이며, 다른 네트워크의 컴퓨터로 스스로 전파되지는 않는다.</li></ul>
웜	<ul style="list-style-type: none"><li>• 인터넷 또는 네트워크를 통해 컴퓨터에서 컴퓨터로 전파되는 악성 프로그램이다.</li><li>• 윈도우 또는 응용 프로그램의 취약점을 이용하거나 이메일 또는 공유 폴더를 통해 전파되며, 최근에는 공유 프로그램(P2P)을 통해 전파되기도 한다.</li><li>• 바이러스와 달리 스스로 전파된다.</li></ul>
트로이 목마	<ul style="list-style-type: none"><li>• 바이러스나 웜처럼 컴퓨터에 직접적인 피해를 주지는 않지만, 악의적인 공격자가 침투하여 사용자의 컴퓨터를 조종하는 프로그램이다.</li><li>• 고의적으로 만들어졌다는 점에서 프로그래머의 실수인 버그와는 다르다.</li><li>• 자기 자신을 다른 파일에 복사하지 않고 인터넷 또는 네트워크를 통해 전파되지 않는다는 점에서 컴퓨터 바이러스나 웜과 구별된다.</li></ul>
PUP	<ul style="list-style-type: none"><li>• 잠재적으로 원하지 않는, 즉 불필요한 프로그램이란 의미로, 사용자에게 치명적인 피해를 주지는 않지만 불편함을 주는 악성 코드다.</li><li>• 프로그램 설치 시 사용자에게 직간접적인 동의를 구하지만 용도를 파악하기 어렵게 한다.</li><li>• 스파이웨어나 광고가 포함된 악성 코드 제거 프로그램, 웹 사이트 바로가기 생성 프로그램 등이 있다.</li></ul>

### 동작에 의한 악성 코드 분류

# 악성 코드

## ■ 악성 코드 분류

악성 코드	설명
다운로더 (downloader)	<ul style="list-style-type: none"> <li>• 네트워크를 통해 어떤 데이터나 프로그램 등을 내려받는 것이 목적으로, 내려받은 데이터나 프로그램이 추가 공격을 위한 악성 코드가거나 악성 코드 작성자의 명령 집합인 경우다.</li> <li>• 무언가를 내려받는 것 자체는 흔한 동작이라 백신 모니터링 시 간과하기 쉽다.</li> </ul>
드롭퍼 (dropper)	<ul style="list-style-type: none"> <li>• 외부에서 파일을 내려받는 다운로드와 달리 드로퍼는 자신 안에 존재하는 데이터로부터 새로운 파일을 생성하여 공격을 수행하는 것이 목적이다.</li> <li>• 드로퍼가 생성하는 파일은 압축되어 있어 실행해보지 않고서는 확인하기 어렵다.</li> </ul>
런처(launcher)	<ul style="list-style-type: none"> <li>• 다운로드나 드로퍼 등으로 생성된 파일을 실행하기 위해 관련 기능을 포함하고 있다.</li> </ul>
애드웨어 (adware)	<ul style="list-style-type: none"> <li>• 광고가 포함된 소프트웨어로, 자체에 광고를 포함하거나 같이 묶어서 배포한다.</li> <li>• 압축 또는 동영상 재생 프로그램과 같은 프리웨어 설치 시에 동의 항목에 포함되어 설치 및 실행되는 경우가 많다.</li> <li>• 사용자의 인식 없이 설치된 애드웨어는 인터넷 시작 페이지 변경하기, 광고와 관련된 알림 창 띄우기, 바탕화면에 광고 페이지의 바로가기 지속 생성하기 등을 목적으로 한다.</li> </ul>
스파이웨어 (spyware)	<ul style="list-style-type: none"> <li>• 개인이나 기업의 정보를 몰래 수집하여 동의 없이 다른 곳에 보내는 것이 목적이다.</li> <li>• 자신의 존재를 숨긴 채 사용자의 컴퓨터 조작 방해하기, 사용자의 컴퓨터 지켜보기, 사용자의 정보(인터넷 검색 흔적, 사용자 로그인 정보, 은행이나 신용 계좌 정보 등) 수집하기 등을 한다.</li> <li>• 스파이웨어는 패스워드 스틸링, 키로거 등으로 세분화될 수 있다.</li> </ul>

악성 코드	설명
랜섬웨어 (ransomware)	<ul style="list-style-type: none"> <li>• 인질의 몸값을 나타내는 'ransom'과 'software'의 합성어로, 최근 급격히 퍼지고 있는 악성 코드다. 사용자에게 의해 랜섬웨어가 실행되면 파일 암호화가 진행되어 사용자가 실행하거나 읽을 수 없게 한다. 즉 자료를 인질로 잡고 돈을 요구한다.</li> <li>• 한 번 암호화된 파일은 복구가 거의 불가능하므로 백업과 같은 사전 대비가 가장 중요하다.</li> </ul>
백도어 (backdoor)	<ul style="list-style-type: none"> <li>• 원래 시스템의 유지·보수나 유사시 문제 해결을 위해 시스템 관리자가 보안 설정을 우회한 다음 시스템에 접근할 수 있도록 만든 도구인 백도어를 악의적인 목적을 지닌 공격자가 시스템에 쉽게 재침입하는 데 이용하는 경우를 의미한다.</li> <li>• 백도어의 기능은 비인가된 접근을 허용하는 것으로, 공격자가 사용자 인증 등의 절차를 거치지 않고 프로그램이나 시스템에 접근할 수 있도록 지원한다. 시스템에 침입한 공격자는 재접속을 위해 백도어를 설치하기도 하지만, 프로그래머가 관리 목적으로 만들었다가 제거하지 않은 백도어를 찾아 악용하기도 한다.</li> </ul>
익스플로잇 (exploit)	<ul style="list-style-type: none"> <li>• 운영체제나 특정 프로그램의 취약점을 이용하여 공격하는 악성 코드다.</li> <li>• 기존의 익스플로잇 코드는 공격자가 직접 공격을 수행했으나 최근에는 악성 코드로 제작 및 배포하여 자동으로 공격 확산을 수행하는 경우가 많다.</li> </ul>
봇(bot)	<ul style="list-style-type: none"> <li>• DDoS 공격 시 지정된 공격을 수행하도록 하는 악성 코드다.</li> <li>• 수많은 봇이 모여 대규모 DDoS 공격을 수행하는 봇넷을 구성한다.</li> </ul>
스케어웨어 (scareware)	<ul style="list-style-type: none"> <li>• 'scare(겁주다)'와 'software'의 합성어로, 사용자를 놀라게 하거나 겁을 주어 원하는 목적을 달성한다.</li> <li>• 악성 코드에 감염되지 않았는데도 악성 코드를 탐지했다고 겁을 주고 자사의 안티바이러스 제품으로 제거해야 한다는 식으로 구매를 유도한다.</li> </ul>

## 목적에 의한 악성 코드 분류



## ■ 악성 코드 분류

### ■ 악성 프로그램 감염 증상

대분류	소분류	설명
시스템	시스템 설정 정보 변경	레지스트리 키 값을 변경하여 시스템 정보를 변경한다.
	FAT 파괴	시스템의 파일 시스템을 파괴한다.
	CMOS 변경	CMOS 내용을 변경하여 부팅 시 오류를 발생시킨다.
	CMOS 정보 파괴	CMOS의 일부를 파괴한다.
	기본 메모리 감소	시스템의 기본 메모리를 줄인다.
	시스템 속도 저하	시스템의 속도를 저하시킨다.
	프로그램 자동 실행	레지스트리 값을 변경하여 시스템 부팅 시 특정 프로그램을 자동으로 실행한다.
	프로세스 종료	특정 프로세스를 강제로 종료시킨다.
	시스템 재부팅	시스템을 재부팅시킨다.
네트워크	메일 발송	특정 사용자에게 메일을 발송한다.
	정보 유출	사용자의 정보를 네트워크를 통해 공격자의 컴퓨터로 전송한다.
	네트워크 속도 저하	감염된 컴퓨터가 속한 네트워크가 느려진다.
	메시지 전송	네트워크를 통해 다른 컴퓨터로 메시지를 전달한다.
	특정 포트 오픈	특정 백도어 포트를 연다.
하드디스크	하드디스크 포맷	하드디스크를 포맷한다.
	부트 섹터 파괴	하드디스크의 특정 부분을 파괴한다.
파일	파일 생성	특정 파일(주로 백도어 파일)을 생성한다.
	파일 삭제	특정 파일이나 디렉터리를 삭제한다.
	파일 감염	특정 파일을 바이러스에 감염시킨다.
	파일 손상	특정 파일에 바이러스가 겹쳐 쓰기 형태로 감염되어 손상된다.
	파일 암호화	파일이 임의로 암호화되어 접근할 수 없다.
특이점	이상 화면 출력	출력 화면에 특정 내용이 나타난다.
	특정 음 발생	컴퓨터에서 특정 음이 발생한다.
	메시지 상자 출력	출력 화면에 특정 메시지 상자가 나타난다.
	증상 없음	특이한 증상이 없다.

# CONTENTS

---

## ▣ 바이러스

## ▣ 1세대 원시형 바이러스

### ▣ 바이러스

- 가장 기본적인 형태의 악성 코드로 사용자 컴퓨터(네트워크로 공유된 컴퓨터 포함)에서 프로그램이나 실행
- 가능한 부분을 몰래 수정하여 자신 또는 자신의 변형을 복사함
- 원시형 바이러스
  - 처음 컴퓨터 바이러스가 등장한 시점의 가장 원시적인 형태. (단순하게 자기 복제 기능과 데이터 파괴 기능만을 가짐)

### ▣ 부트 바이러스

- 플로피디스크나 하드디스크의 부트 섹터에 감염되는 바이러스
- MBR과 함께 PC 메모리에 저장되어 부팅 시 자동으로 동작하여 부팅 후에 사용되는 모든 프로그램을 감염
- 부트 바이러스를 이해하려면 컴퓨터의 부팅 순서를 알아야 함

## □ 1세대 원시형 바이러스

### ▣ 파일 바이러스

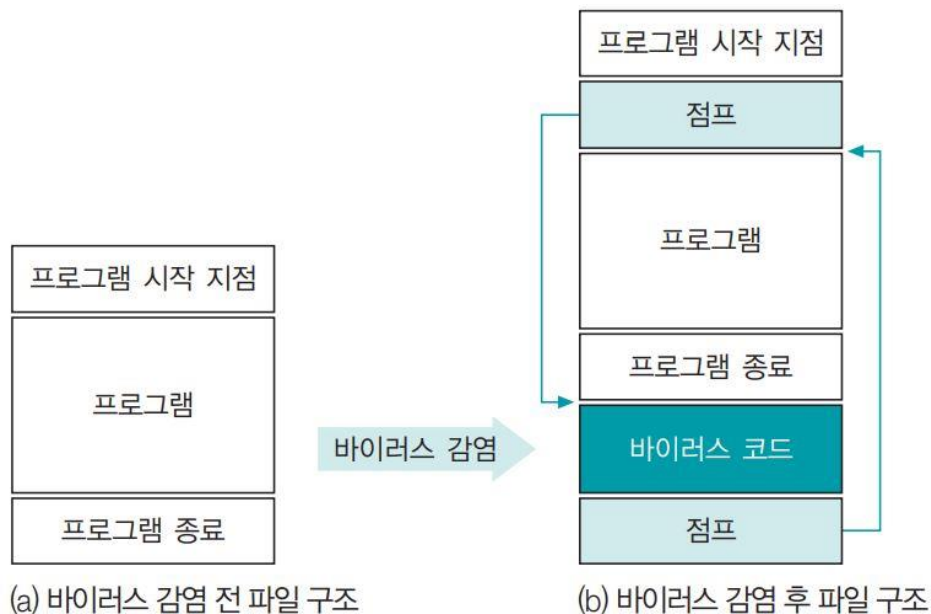
- 파일을 직접 감염시켜 바이러스 코드를 실행시키는 것
- 하드디스크 부팅이 일반화되면서 부트 바이러스의 대안으로 등장
- COM, EXE와 같은 실행 파일과 오버레이 파일, 디바이스 드라이버 등에 감염
- 전체 바이러스의 80% 이상을 차지
- 파일 바이러스의 감염 위치
  - 프로그램을 덮어쓰는 경우
  - 프로그램 앞부분에 실행 코드를 붙이는 경우,
  - 프로그램 뒷부분에 바이러스 코드를 붙이는 경우



## □ 1세대 원시형 바이러스

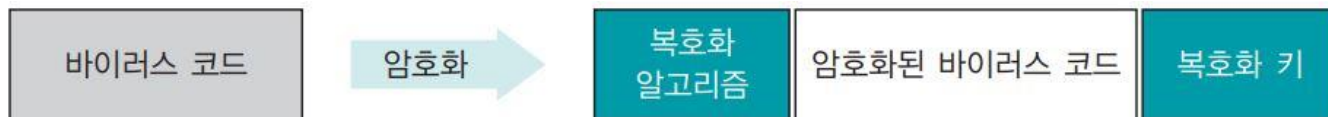
### ▣ 파일 바이러스

- 바이러스가 프로그램 뒷부분에 위치한다면 백신의 바이러스 스캔으로부터 자신의 존재를 숨기기 위함
  - 파일 바이러스의 종류에는 예루살렘 바이러스, 선데이, 스코피온, 크로, FCL, CIH 바이러스 등이 존재



## □ 2세대 암호형 바이러스

- 암호형 바이러스는 바이러스 코드를 쉽게 파악하여 제거할 수 없도록 암호화한 바이러스
- 바이러스 동작 시 메모리에 올라오는 과정에서 암호화가 풀리므로 백신은 이를 이용하여 메모리에 실행되어 올라온 바이러스와 감염 파일을 분석하고 치료
- 암호형 바이러스에 슬로, 캐스케이드, 원더러, 버글러 등이 있음



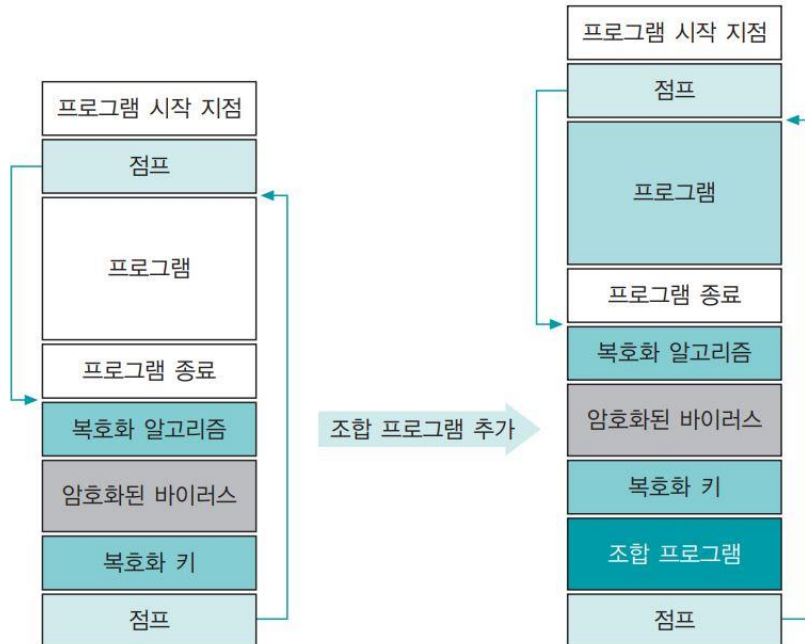
암호화된 바이러스 코드

## □ 3세대 은폐형 바이러스

- 바이러스에 감염된 파일이 일정 기간 잠복기를 가지도록 제작
- 은폐형 바이러스에는 브레인, 조시, 512, 4096 등이 있음

## 4세대 다형성 바이러스

- 백신 프로그램은 바이러스 파일 안의 특정한 식별자로 바이러스 감염 여부 판단
- 이 기능을 우회하기 위해 사용하는 것이 다형성 바이러스
- 코드 조합을 다양하게 할 수 있는 조합 프로그램을 암호형 바이러스에 덧붙여 감염시키므로 프로그램이 실행될 때마다 바이러스 코드 자체를 변경하여 식별자를 구분하기 어렵게 함
- 다형성 바이러스는 제작하기도 어렵고 진단하기도 어려움



다형성 바이러스

## □ 5세대 매크로 바이러스

### ▣ 매크로 바이러스

- MS 오피스 프로그램의 매크로 기능으로 감염되는 바이러스
- 워드 콘셉트, 엑셀-라룩스, 멜리사 바이러스 등이 있음

### ▣ 비주얼 베이직 스크립트(VBS)로 많이 제작됨.

### ▣ 매크로 바이러스의 증상

- 문서가 정상적으로 열리지 않거나 암호가 설정되어 있음
- 문서 내용에 깨진 글자나 이상한 문구가 포함되어 있음
- 매크로 메뉴가 실행할 수 없게 잠겨 있음
- 엑셀이나 워드 작업 중 VB편집기의 디버그 모드가 실행됨



MS 엑셀에서의 매크로 사용 설정



## ▣ 차세대 바이러스

- ▣ 스크립트 형태의 바이러스가 더욱 활성화되어 대부분 네트워크와 메일을 이용하여 전파
- ▣ 단순히 데이터를 파괴하고 다른 파일을 감염시키는 것에서 나아가 사용자 정보를 빼내거나 시스템 장악을 위한 백도어 기능을 가진 웜의 형태로 진화

# CONTENTS

---



## □ 웜의 개념

- 원래 '벌레'와 '증식'을 뜻하는 말
- IT 분야에서는 인터넷 또는 네트워크를 통해 컴퓨터에서 컴퓨터로 전파되는 프로그램을 의미
- 스스로를 증식하는 것이 목적이므로 파일 자체에 이런 기능이 있거나 운영체제에 자신을 감염시킴
- 1999년 인터넷 웜이 출현하면서 일반인에게 웜이라는 용어가 알려지기 시작
- 오늘날의 웜은 이메일의 첨부 파일 형태로 확산되거나, 운영체제 또는 프로그램의 보안 취약점을 이용하여 스스로 침투하는 형태
- 다른 파일을 감염시키는 컴퓨터 바이러스의 기능을 가진 복합적인 형태의 웜도 존재

## □ 웜의 개념

### ▣ 매스메일러형 웜

- 자기 자신을 포함하는 대량 메일을 발송하여 확산되는 것
- 제목 없는 메일이나 특정 제목의 메일을 전송하고 사용자가 이를 읽었을 때 감염
- 주요 특징과 증상
  - 메일로 전파되며 감염된 시스템이 많으면 **SMTP 서버**(TCP 25 번 포트)의 **네트워크 트래픽이 증가**
  - 출처나 내용이 확인되지 않은 메일을 열었을 때 확산되는 경우가 많음
  - 베이글 웜은 웜 파일을 실행할 때 "Can't find a viewer associated with the file"과 같은 가짜 오류 메시지를 출력
  - 넷스카이 웜은 윈도우 시스템 디렉터리 밑에 CSRSS.exe 실행 파일을 만듦
  - 변형된 종류에 따라 시스템에 임의의 파일을 생성

## □ 시스템 공격형 웜

- 운영체제 고유의 취약점을 이용하여 내부 정보를 파괴하거나, 컴퓨터를 사용할 수 없는 상태로 만들거나, 외부의 공격자가 시스템 내부에 접속할 수 있도록 악성 코드를 설치하는 형태
- 간단한 비밀번호 크래킹 알고리즘을 포함하고 있어 비밀번호가 취약한 시스템을 공격하는 웜도 있음
- 주요 특징과 증상
  - 전파할 때 과다한 TCP/135,445 트래픽이 발생
  - windows, windows/system32, winnt, winnt/system32 폴더에 SVCHOST.EXE 파일을 설치
  - 공격 성공 후 UDP/5599 등의 특정 포트를 열어 외부 시스템과 통신
  - 시스템 파일 삭제 또는 정보 유출(게임 CD의 시리얼 키 등)이 가능

## ▣ 네트워크 공격형 웜

- ▣ 특정 네트워크나 시스템에 대해 SYN 플러딩이나 스머프와 같은 서비스 거부(DoS) 공격을 수행하는 것
- ▣ 네트워크 공격형 웜은 분산 서비스 거부 공격을 위한 봇 형태로 발전
- ▣ 주요 증상
  - 네트워크가 마비되거나 급격히 느려짐
  - 네트워크 장비가 비정상적으로 동작
- ▣ 네트워크 공격 유형의 웜은 적은 수의 시스템이 감염되어도 파급 효과가 크므로 **안정적인 네트워크 설계와 시스템 취약점에 대한 지속적인 패치 관리가 중요함**

# CONTENTS

---

▣ 트로이 목마

## ▣ 트로이 목마의 개요

### ▣ 악성 루틴이 숨어 있는 프로그램

- 겉보기에는 정상이지만 사용자가 실행 시 악성 코드가 수행
- 사회공학 기법 형태로 퍼짐
- 어떤 악성 코드도 포함될 수 있어 시스템 파괴, 스파이웨어 나 랜섬웨어로의 동작 등 어떤 형태든 가능하지만 주로 백도어로 사용됨
- 다른 파일에 삽입되거나 스스로 전파되지 않음

### ▣ 백도어

- 백도어는 프로그램이 개발된 후 완전히 삭제되어야 하지만 제품이 출시될 때 그대로 남아 있는 경우도 있음
  - MS 오피스의 엑셀에 간단한 자동차 게임을 숨겨놓거나 한글 프로그램에 테트리스를 숨겨놓는 경우
  - 개발자가 장난삼아 만들어 두기도 함



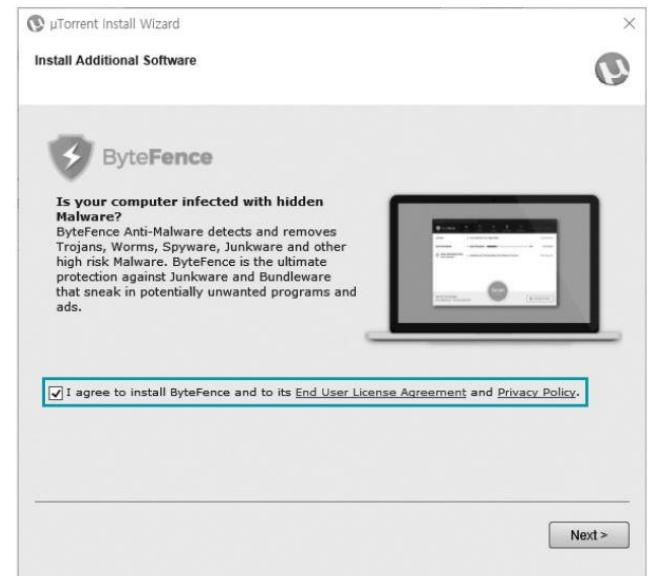
# CONTENTS

---

 PUP

## ❑ PUP의 개요

- ❑ 사용자에게 직간접적으로 동의를 구하지만 용도를 파악하기 어려운 상태에서 설치되는 프로그램
- ❑ 설치되는 경우
  - 포르노 또는 크랙 사이트 등에 접속시 설치 되는 경우
  - 악성 코드에 의해 설치되는 경우
  - 특정 프로그램을 설치할 때 함께 설치되는 경우
  - 설치를 진행하는 과정에서 특정 프로그램이 부가적으로 설치되는 경우
- ❑ PUP는 악성 코드라고 단언하기에 애매한 면이 있지만 사용자에게 불편함을 줌



uTorrent 설치 시 함께 설치되는 BytesFence

# CONTENTS

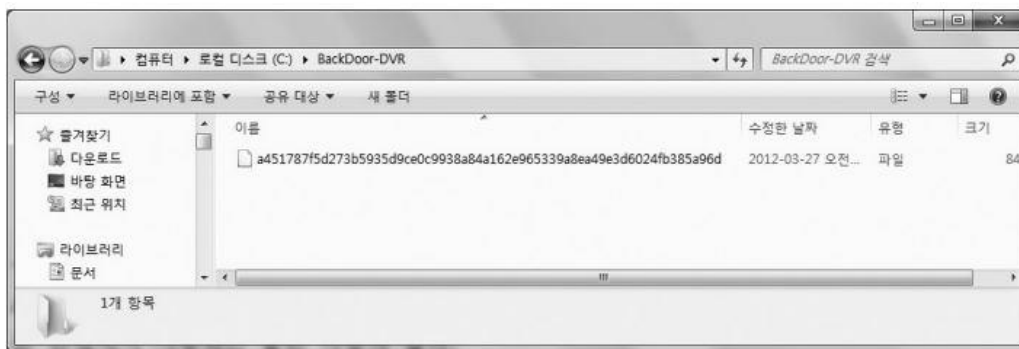
---

- ❑ 악성 코드 탐지 및 대응책

# ➔ 악성 코드 탐지 및 대응책

## ❑ 악성 코드 탐지 예시

- ❑ 임의의 악성 코드인 BackDoor-DVR를 실행해 악성코드 탐지용 툴로 탐지
- ❑ 악성코드 탐지용 툴
  - 윈도우 7 악성 코드: **Win-Trojan.Pearmor**
  - Process Explorer
  - Total Commander: <http://www.ghisler.com>
  - CPorts: <http://www.nirsoft.net/utis/cports.html>



BackDoor-DVR 실행 파일

# 악성 코드 탐지 및 대응책

## □ 네트워크 상태 점검하기

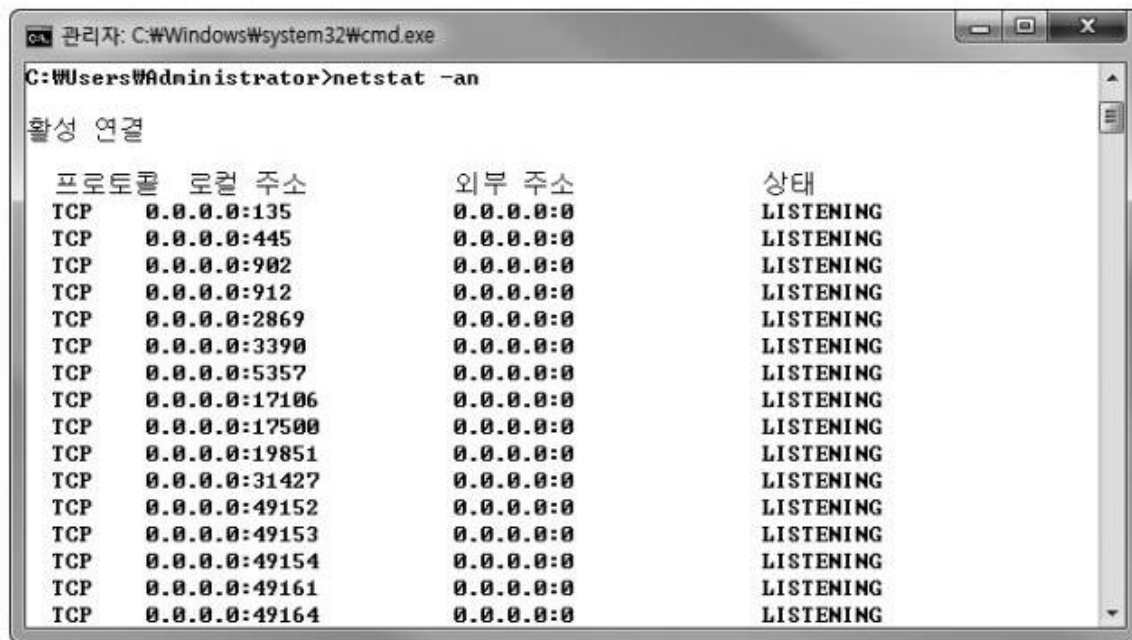
- ▣ 상당수의 악성 코드는 외부에 있는 해커나 악성 코드 작성자와 통신을 하기 위해 서비스 포트를 생성

포트 번호	악성 코드	포트 번호	악성 코드
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

# 악성 코드 탐지 및 대응책

## ▣ 네트워크 상태 점검하기

- ▣ 시스템에서는 netstat 명령으로 열려 있는 포트를 확인할 수 있음



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

활성 연결

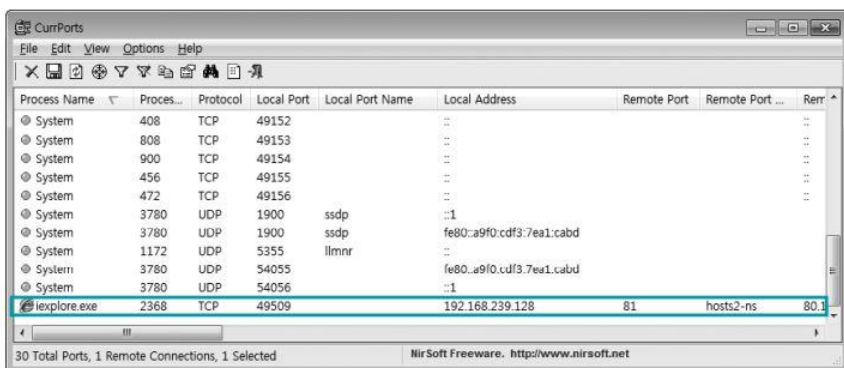
프로토콜  로컬 주소          외부 주소          상태
TCP       0.0.0.0:135      0.0.0.0:0          LISTENING
TCP       0.0.0.0:445      0.0.0.0:0          LISTENING
TCP       0.0.0.0:902      0.0.0.0:0          LISTENING
TCP       0.0.0.0:912      0.0.0.0:0          LISTENING
TCP       0.0.0.0:2869     0.0.0.0:0          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
```

netstat -an 실행 결과

# ➔ 악성 코드 탐지 및 대응책

## ▣ 네트워크 상태 점검하기

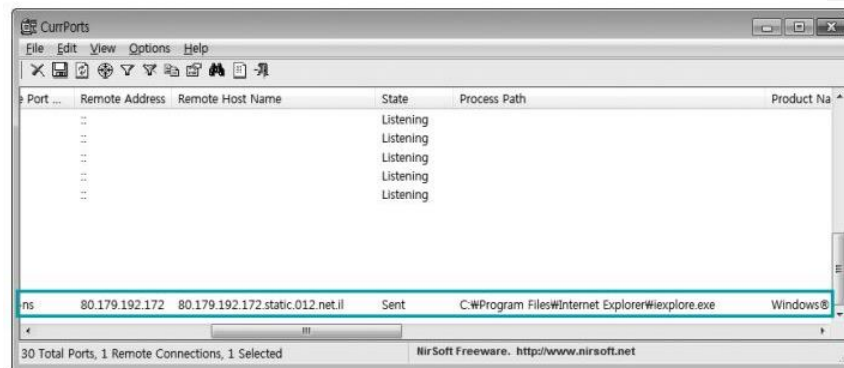
- ▣ 악성 코드가 사용하는 포트를 netstat 명령만으로 확인하기 어려운 경우 CPorts 같은 프로그램으로 서비스 포트별로 사용하는 응용 프로그램을 확인 가능
- ▣ BackDoor-DVR 실행한 뒤 CPorts에서 활성화된 네트워크 항목을 살펴보면 특이한 연결을 발견할 수 있음



Process Name	Process...	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port ...	Rem...
System	408	TCP	49152					
System	808	TCP	49153					
System	900	TCP	49154					
System	456	TCP	49155					
System	472	TCP	49156					
System	3780	UDP	1900	ssdp				
System	3780	UDP	1900	ssdp	fe80::a9f0:cd3:7ea1:cabd			
System	1172	UDP	5355	llmnr				
System	3780	UDP	54055		fe80::a9f0:cd3:7ea1:cabd			
System	3780	UDP	54056					
iexplore.exe	2368	TCP	49509		192.168.239.128	81	hosts2-ns	80.1

30 Total Ports, 1 Remote Connections, 1 Selected  
NirSoft Freeware. <http://www.nirsoft.net>

Cports 실행 결과1



Port ...	Remote Address	Remote Host Name	State	Process Path	Product Na
			Listening		
			Listening		
			Listening		
			Listening		
			Listening		
			Listening		
ns	80.179.192.172	80.179.192.172.static.012.net.il	Sent	C:\Program Files\Internet Explorer\iexplore.exe	Windows®

30 Total Ports, 1 Remote Connections, 1 Selected  
NirSoft Freeware. <http://www.nirsoft.net>

Cports 실행 결과2

# → 악성 코드 탐지 및 대응책

## □ 정상적인 프로세스와 비교

- 윈도우와 유닉스 시스템 등의 정상적인 프로세스를 외워두면 비정상적인 프로세스 식별에 도움
  - 모든 프로세스를 외울 수 없음
  - 다만, 정상 프로세스를 화이트리스트 기반으로 작성해 둔다면, 비정상 프로세스 식별에 도움이 될 수 있음
- 윈도우에서는 [Ctrl]+[Alt]로 작업 관리자 실행하여 현재 실행 중인 프로세스 확인 가능
- 중간 과정 없이 [Ctrl] + [Shift] + [esc] 를 누르면 작업 관리자를 통해 프로세스를 바로 확인 가능



윈도우에서 동작 중인 프로세스 확인



# 악성 코드 탐지 및 대응책

## □ 정상적인 프로세스와 비교

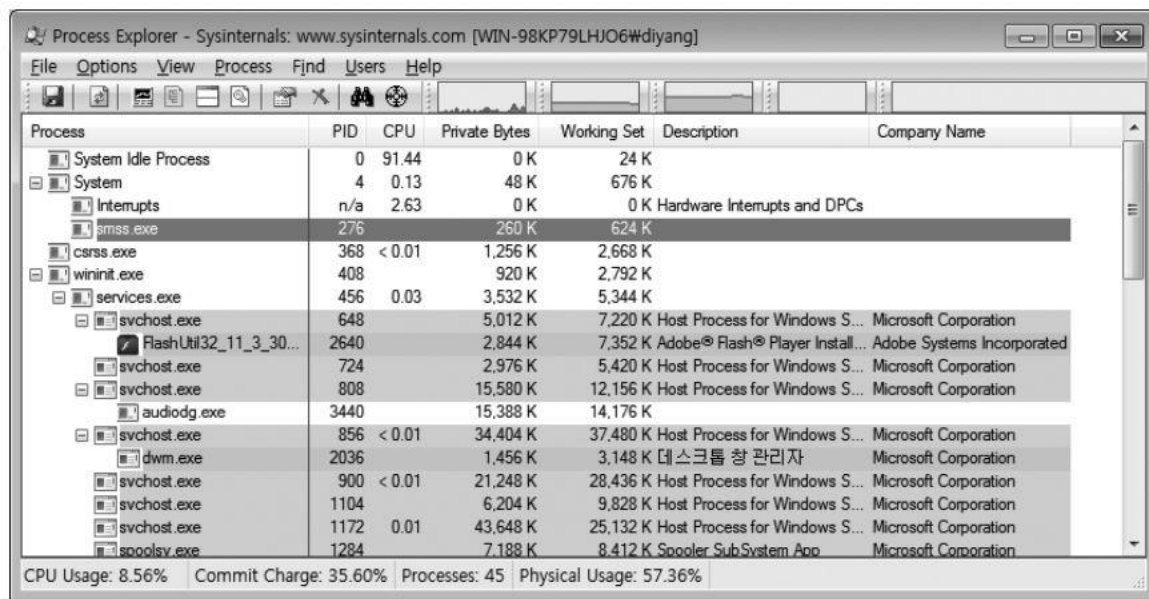
- ▣ 윈도우 시스템이 동작하기 위한 기본 프로세스
- ▣ 이 중에서 악성 코드가 주로 사용하는 서비스명은 **csrss**와 **svchost**

프로세스명	설명
<b>csrss.exe</b> (client/server runtime subsystem: win 32)	윈도우 콘솔 관리자, 스레드 생성 및 삭제, 32비트 가상 MS-DOS 모드 지원
explorer.exe	작업 표시줄이나 바탕화면과 같은 사용자 셸 지원
lsass.exe (local security authentication server)	winlogon 서비스에 필요한 인증 프로세스 담당
mstask.exe (window task scheduler)	시스템 백업이나 업데이트와 관련된 작업의 스케줄러
smss.exe (session manager subSystem)	사용자 세션을 시작하는 기능 담당
spoolsv.exe (printer spooler service)	프린터와 팩스의 스푼링 기능 담당
<b>svchost.exe (service host process)</b>	<b>DLL(Dynamic Link Libraries)에 의해 실행되는 기본 프로세스</b>
services.exe (service control manager)	시스템 서비스를 시작 및 정지하고 그것들 간에 상호작용하는 기능 수행
system	커널 모드 스레드 대부분의 시작점이 되는 프로세스
system idle process	각 CPU마다 하나씩 실행되는 스레드로 CPU의 잔여 프로세스 처리량을 %로 나타낸 값
taskmgr.exe (task manager)	작업 관리자 자신을 나타냄.
winlogon.exe (windows logon process)	사용자의 로그인.로그오프를 담당하는 프로세스.
winmgmt.exe (window management service)	장치 관리 및 계정 관리, 네트워크 동작 관련한 스크립트를 위한 프로세스
msdtc.exe (distributed transaction coordinator)	웹 서버와 SQL 서버 구동 시에 다른 서버와 연동하기 위한 프로세스
ctfmon.exe (alternative user input services)	키보드, 음성, 손으로 적은 글 등 여러 가지 텍스트 입력에 대한 처리를 지원하는 프로세스
dfsrv.exe (distributed file system)	분산 파일 시스템(DFS)을 지원하기 위해 백그라운드로 실행되는 프로세스

# 악성 코드 탐지 및 대응책

## □ 정상적인 프로세스와 비교

- ▣ 좀 더 자세한 프로세스 정보 확인을 위해 Process Explorer 사용



The screenshot shows the Process Explorer window from Sysinternals. The title bar reads 'Process Explorer - Sysinternals: www.sysinternals.com [WIN-98KP79LHJO6#diyang]'. The menu bar includes File, Options, View, Process, Find, Users, and Help. The toolbar contains icons for file operations and process management. The main window displays a list of processes with columns for Process, PID, CPU, Private Bytes, Working Set, Description, and Company Name. The processes listed include System Idle Process, System, Interrupts, smss.exe, csrss.exe, wininit.exe, services.exe, svchost.exe, FlashUtil32\_11\_3\_30..., audiodg.exe, dwm.exe, and spoolsv.exe. The status bar at the bottom shows CPU Usage: 8.56%, Commit Charge: 35.60%, Processes: 45, and Physical Usage: 57.36%.

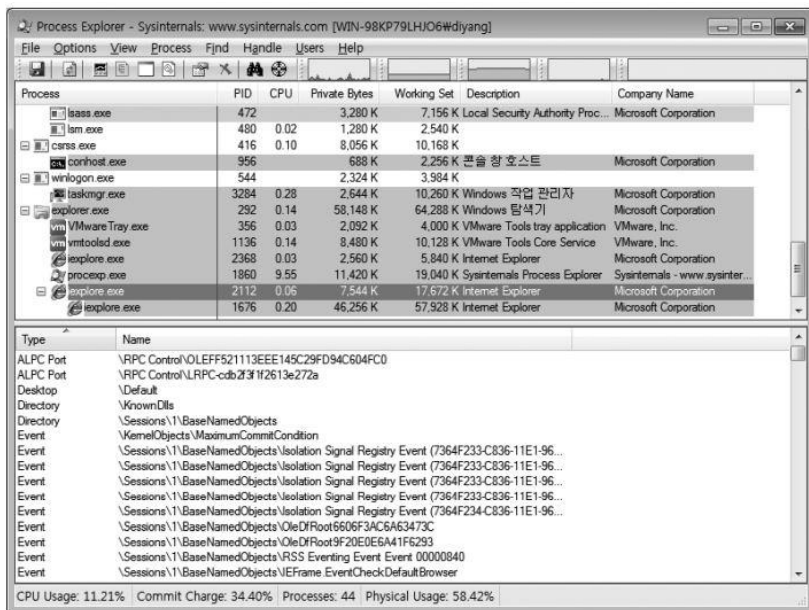
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	91.44	0 K	24 K		
System	4	0.13	48 K	676 K		
Interrupts	n/a	2.63	0 K	0 K	0 K Hardware Interrupts and DPCs	
smss.exe	276		260 K	624 K		
csrss.exe	368	< 0.01	1,256 K	2,668 K		
wininit.exe	408		920 K	2,792 K		
services.exe	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 창 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

Process Explorer를 이용한 프로세스 확인

# 악성 코드 탐지 및 대응책

## □ 정상적인 프로세스와 비교

- 2368번 프로세스를 Process Explorer를 통해 확인수 있는 'C:\User\Wdiyang\AppData\Roaming\Bifrost\logg.dat'를 제외하고는 의심할 만한 값이 없음
- 정상적인 인터넷 익스플로러를 실행하여 상세 창에서 해당 프로세스를 살펴보면, 비정상적인 인터넷 익스플로러 프로세스와 상당히 다름

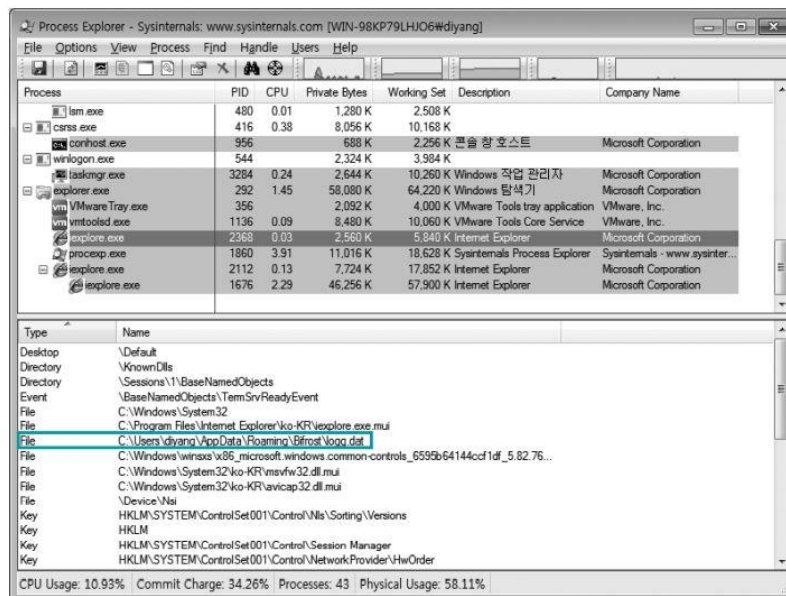


Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
lsass.exe	472		3,280 K	7,156 K	Local Security Authority Proc...	Microsoft Corporation
lsm.exe	480	0.02	1,280 K	2,540 K		
csrss.exe	416	0.10	8,056 K	10,168 K		
conhost.exe	956		688 K	2,256 K	콘솔 호스트	Microsoft Corporation
winlogon.exe	544		2,324 K	3,984 K		
taskmgr.exe	3284	0.28	2,644 K	10,260 K	Windows 작업 관리자	Microsoft Corporation
explorer.exe	292	0.14	58,148 K	64,288 K	Windows 탐색기	Microsoft Corporation
VMwareTray.exe	356	0.03	2,092 K	4,000 K	VMware Tools tray application	VMware, Inc.
vmtoolsd.exe	1136	0.14	8,480 K	10,128 K	VMware Tools Core Service	VMware, Inc.
explore.exe	2368	0.03	2,560 K	5,840 K	Internet Explorer	Microsoft Corporation
process.exe	1860	9.55	11,420 K	19,040 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
explore.exe	2112	0.06	7,544 K	17,672 K	Internet Explorer	Microsoft Corporation
explore.exe	1676	0.20	46,256 K	57,928 K	Internet Explorer	Microsoft Corporation

Type	Name
ALPC Port	\RPC Control\OLEFF521113EEE145C29F04C604FC0
ALPC Port	\RPC Control\LRPC-cdb3f1f2613e272a
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
Event	\Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (7364F233-C836-11E1-96...
Event	\Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (7364F233-C836-11E1-96...
Event	\Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (7364F233-C836-11E1-96...
Event	\Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (7364F233-C836-11E1-96...
Event	\Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (7364F233-C836-11E1-96...
Event	\Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (7364F233-C836-11E1-96...
Event	\Sessions\1\BaseNamedObjects\OLEDFRoot660F3AC6A63473C
Event	\Sessions\1\BaseNamedObjects\OLEDFRoot9F20E6A41F6293
Event	\Sessions\1\BaseNamedObjects\RSS Eventing Event Event 00000840
Event	\Sessions\1\BaseNamedObjects\IEFrame EventCheckDefaultBrowser

CPU Usage: 11.21% Commit Charge: 34.40% Processes: 44 Physical Usage: 58.42%

### 경로 이상



Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
lsass.exe	480	0.01	1,280 K	2,508 K		
csrss.exe	416	0.38	8,056 K	10,168 K		
conhost.exe	956		688 K	2,256 K	콘솔 호스트	Microsoft Corporation
winlogon.exe	544		2,324 K	3,984 K		
taskmgr.exe	3284	0.24	2,644 K	10,260 K	Windows 작업 관리자	Microsoft Corporation
explorer.exe	292	1.45	58,080 K	64,220 K	Windows 탐색기	Microsoft Corporation
VMwareTray.exe	356		2,092 K	4,000 K	VMware Tools tray application	VMware, Inc.
vmtoolsd.exe	1136	0.09	8,480 K	10,060 K	VMware Tools Core Service	VMware, Inc.
explore.exe	2368	0.03	2,560 K	5,840 K	Internet Explorer	Microsoft Corporation
process.exe	1860	3.91	11,016 K	18,628 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
explore.exe	2112	0.13	7,724 K	17,852 K	Internet Explorer	Microsoft Corporation
explore.exe	1676	2.29	46,256 K	57,900 K	Internet Explorer	Microsoft Corporation

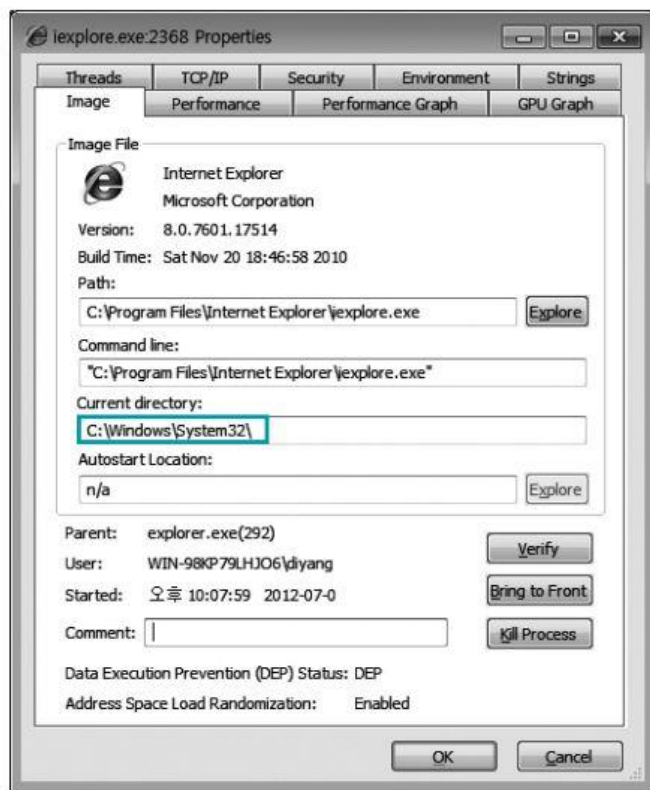
Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\BaseNamedObjects\TermSrvReadyEvent
File	C:\Windows\System32
File	C:\Program Files\Internet Explorer\ko-KR\explore.exe.mui
File	C:\Users\Wdiyang\AppData\Roaming\Bifrost\logg.dat
File	C:\Windows\winsock\6595b64144cd1df_5.82.76...
File	C:\Windows\System32\ko-KR\msvfw32.dll.mui
File	C:\Windows\System32\ko-KR\avicap32.dll.mui
File	\Device\Nai
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKLM\SYSTEM\ControlSet001\Control\NetworkProvider\HwOrder

CPU Usage: 10.93% Commit Charge: 34.26% Processes: 43 Physical Usage: 58.11%

# 악성 코드 탐지 및 대응책

## □ 정상적인 프로세스와 비교

- 2개의 iexplore.exe 프로세스 속성 창을 비교해보면 Current directory 값만 다를 뿐 나머지는 모두 같음



비정상 프로세스



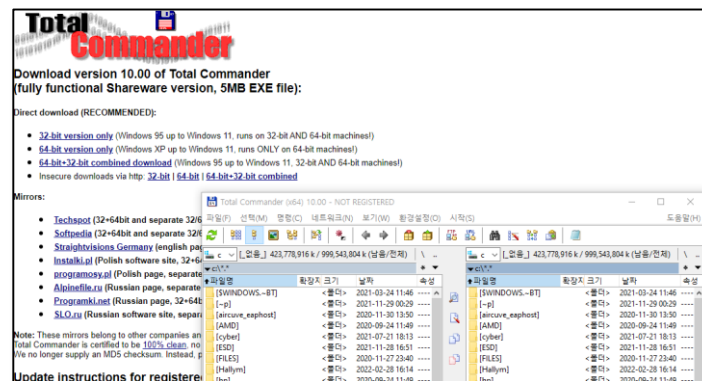
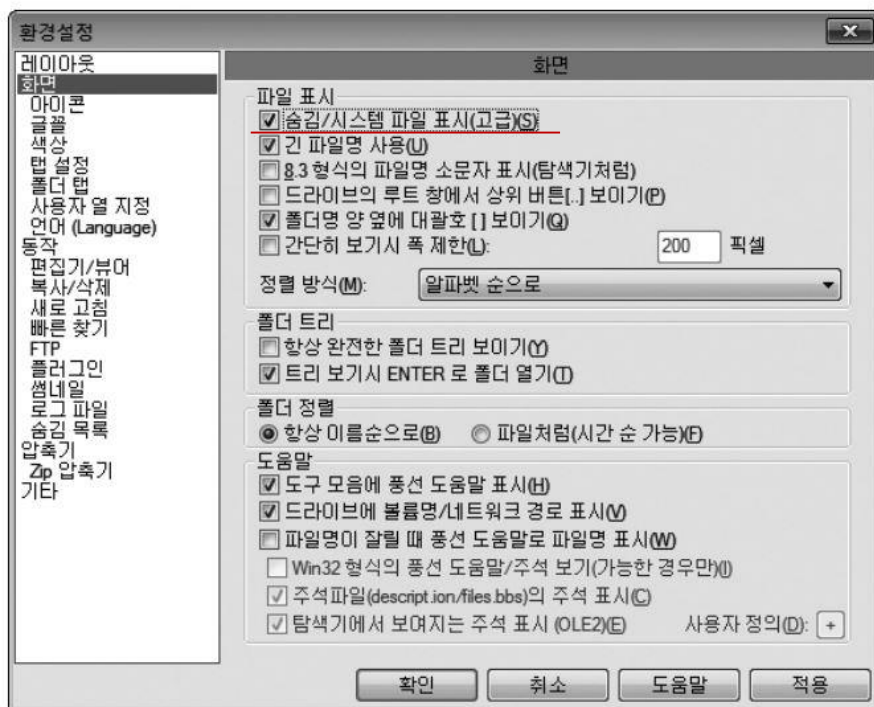
정상 프로세스

# 악성 코드 탐지 및 대응책

## 악성 코드의 실제 파일 확인하기

악성 코드의 실제 파일을 확인하는데 total commander와 같은 툴을 사용

먼저 [환경설정]- [옵션]-[화면]에서 [숨김/시스템 파일 표시] 옵션을 활성화함

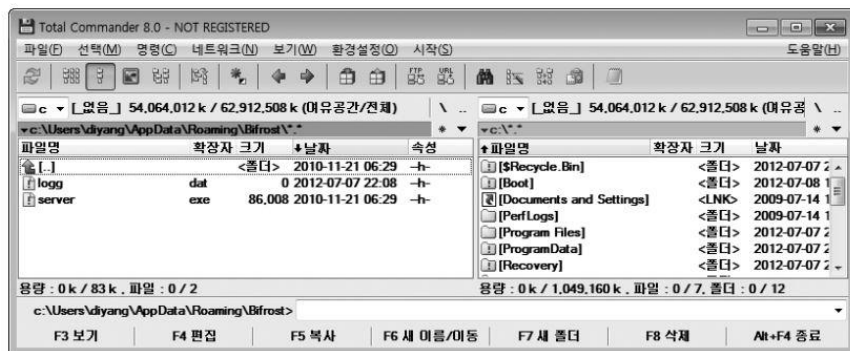




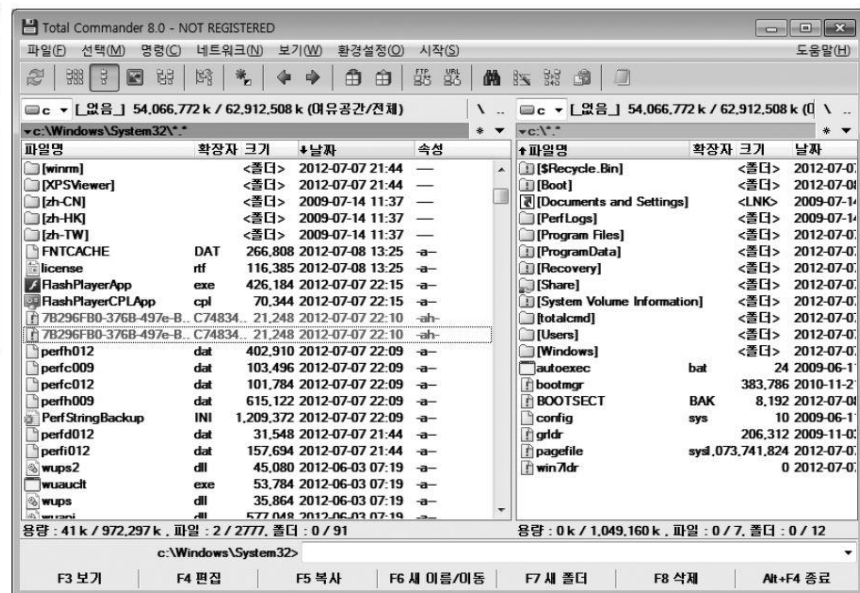
# 악성 코드 탐지 및 대응책

## ❑ 악성 코드의 실제 파일 확인하기

- ❑ 파일을 찾을때 Process Explorer에서 확인한 파일명을 검색하는 방법을 사용할 수 있음
- ❑ 'BackDoor-DVR'의 경우 Bifrost 폴더를 먼저 검색
- ❑ 파일 확인 과정에서 'C:\Windows\system32' 폴더를 필수 확인



Bifrost 폴더 확인

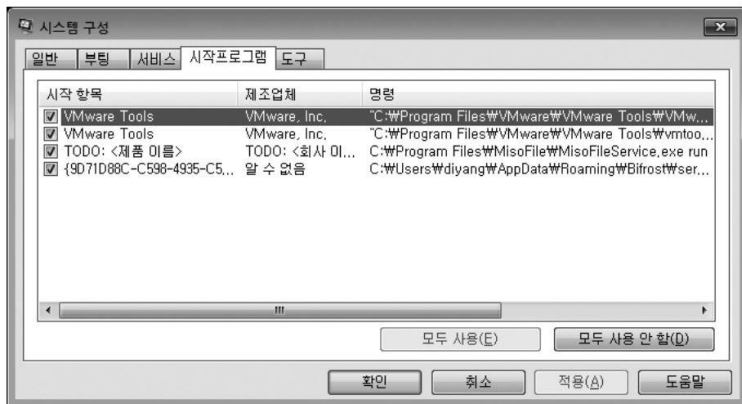


'C:\Windows\system32' 폴더 확인

# 악성 코드 탐지 및 대응책

## ■ 악성 코드의 실제 파일 확인하기

- 악성코드의 내용이 레지스터에 기록될 수 있으므로 악성 코드를 삭제할 때는 레지스터에서도 관련 내용을 확인
- 시작 프로그램 목록은 'msconfig' 명령을 통해 확인 할 수 있음



시작 프로그램 확인

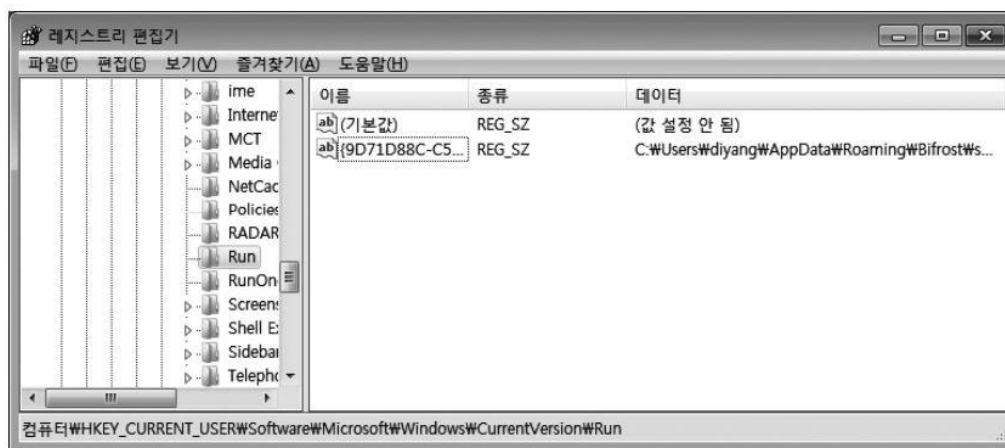


'C:\Program FilesWMisoFile' 폴더 확인

# ➔ 악성 코드 탐지 및 대응책

## ❑ 악성 코드 제거하기

- ① 악성 코드 프로세스 중지하기
  - 2368 프로세스를 'Kill Process Tree([Shift]+[Delete] )'로 중지
- ② 악성 코드 파일 삭제하기
  - Bifrost 폴더에서 확인한 파일을 삭제
  - C:\Windows\system32 폴더에서 확인한 파일을 삭제
  - C:\Program Files\MisoFile 폴더에서 확인한 파일을 삭제
- ③ 레지스트리 삭제하기
  - 시작 프로그램에서 확인한 사항을 삭제
  - 'regedit'로 레지스트리 경로를 확인한 뒤 레지스트리에서 해당 항목을 삭제



레지스트리에서 해당 레지스트리 값 확인



- ❑ 악성 코드
- ❑ 바이러스
- ❑ 웜
- ❑ 트로이 목마
- ❑ PUP
- ❑ 악성 코드 탐지 및 대응책

# 참고문헌

- ▣ 정보 보안 개론 - 한권으로 배우는 핵심 보안 이론, 양대일, 한빛 아카데미

# Q & A

