

악성코드

[참고자료 – 정보보안개론 한빛아카데미(주)]

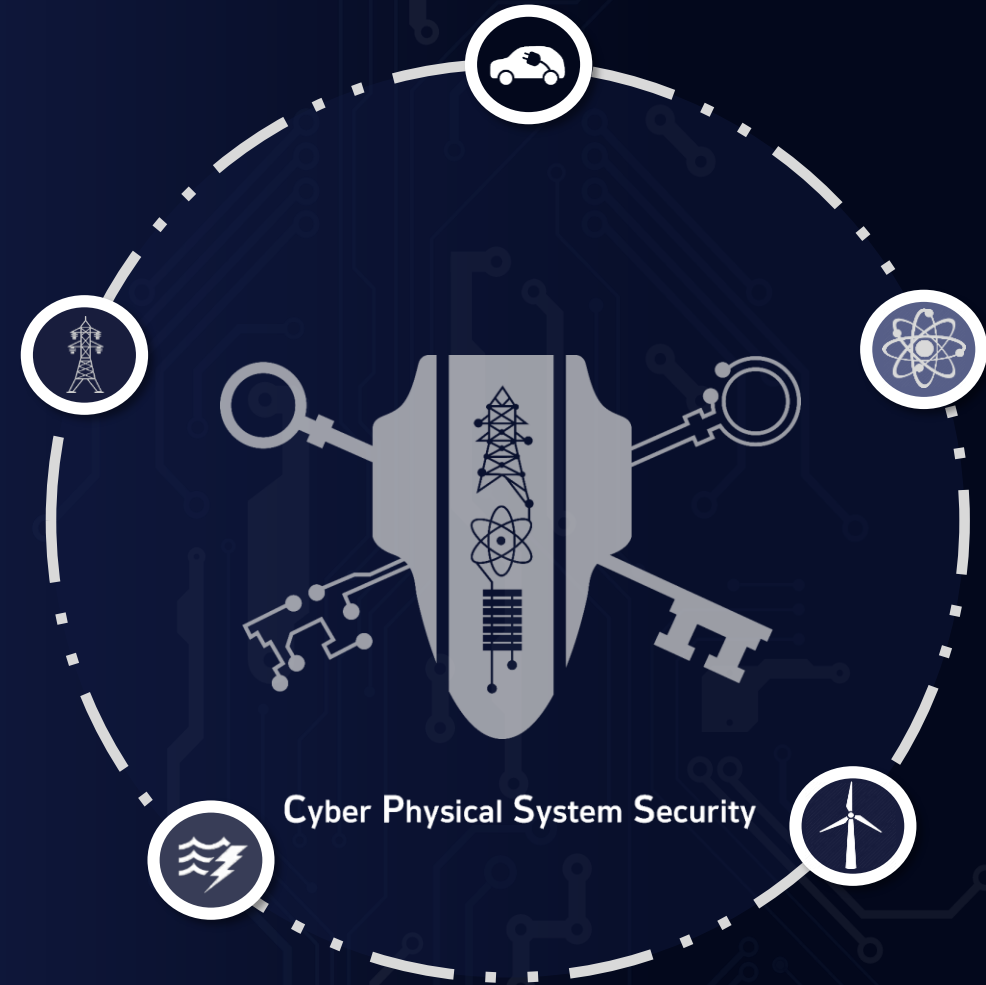
서정택

가천대학교 컴퓨터공학부 스마트보안전공 교수

가천대학교 CPS보안연구센터 센터장

한국정보보호학회 CPS보안연구회 위원장

seojt@gachon.ac.kr



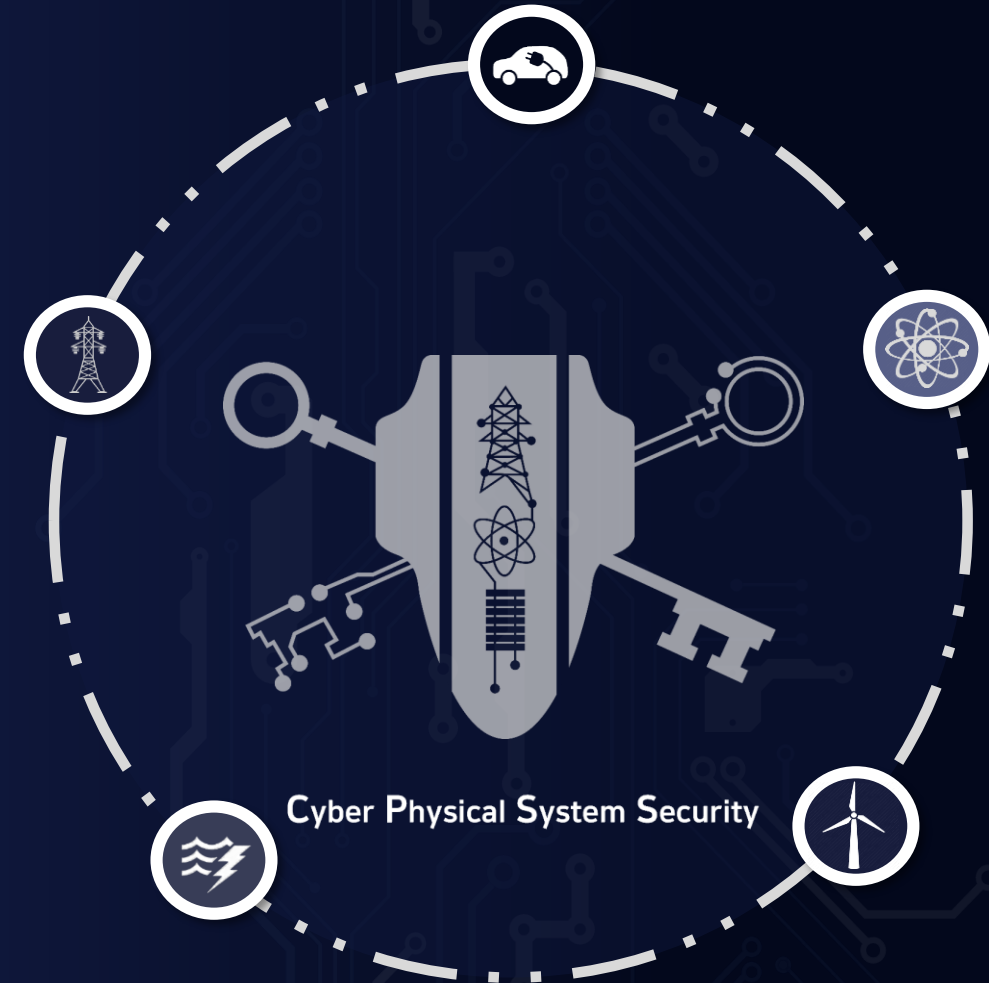
CONTENTS

01 악성코드

02 악성코드 종류

03 랜섬웨어

04 악성코드 탐지 및 대응책



01. 악성코드



악성코드

- 제작자가 의도적으로 사용자에게 피해를 주기 위해 만든, 모든 **악의적 목적**을 가진 프로그램 및 매크로, 스크립트로 컴퓨터에서 작동하는 실행 가능한 모든 형태

악성코드의 역사

- 컴퓨터 바이러스 개념
 - 데이비드 제럴드의 공상 과학 소설 《When Harlie Was One》(1972)에 맨 처음 등장
 - 1984년에 프레드 코헨이 컴퓨터 바이러스의 개념을 정립함
 - “자신의 사본을 포함하도록 다른 프로그램을 수정 및 진화시켜 감염시키는 프로그램”
- 최초의 바이러스와 웜
 - 최초의 바이러스는 1986년 등장한 브레인(Brain) 바이러스
 - 최초의 웜은 1988년 미국 네트워크를 마비시킨 모리스 웜
- 매크로 바이러스의 출현
 - 1999년에 매크로 바이러스로 잘 알려진 멜리사(Melissa) 바이러스 출현
 - 매크로(macro) : 엑셀이나 워드에서 특정한 기능을 자동화해 놓은 일종의 프로그램



그림 6-1 《When Harlie Was One》

악성코드 역사

● 웜에 의한 대규모 피해 발생

- 2001년 7월 13일 25만대 이상의 컴퓨터가 8시간 만에 코드레드(Code Red) 웜에 감염
- 윈도우 2000과 윈도우 NT 서버를 경유지로 미국 백악관 공격, 국내도 최소 3만 대 이상의 시스템 피해 추정

● 인터넷 대란

- 2003년 1월 25일 인터넷 대란을 일으킨 SQL_Overflow, 일명 슬래머 웜이 등장
- 05시 29분에 슬래머가 퍼진 후 06시를 기준으로 전 세계 74,855대 시스템이 감염됨
- 2003년 8월에는 1~2분 간격으로 컴퓨터를 강제 재부팅해 큰 피해를 준 블래스터 웜(Blaster worm)을 시작으로 웰치아 웜(Welchia worm), 엄청난 양의 스팸 메일을 집중 발송한 소빅.F 웜(Sobig.F worm) 등 발생

● 변종 웜의 발생

- 2005년 3월에 MMS로 감염된 휴대전화에 저장된 전화번호로 악성 코드를 퍼뜨리는 컴워리어(CommWarrior) 등장
- 저장 매체나 인터넷으로 전파되던 악성 코드가 휴대전화 통신망으로 전파되기 시작함

악성코드 분류 방법

동작 및 목적에 의한 분류

표 6-1 동작에 의한 악성 코드 분류

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

표 6-2 목적에 의한 악성 코드 분류

악성 코드	설명
다운로더(downloader)	<ul style="list-style-type: none"> • 네트워크를 통해 어떤 데이터나 프로그램 등을 내려받는 것이 목적으로, 내려받은 데이터나 프로그램이 추가 공격을 위한 악성 코드이거나 악성 코드 작성자의 명령 집합인 경우다. • 무언가를 내려받는 것 자체는 흔한 동작이라 백신 모니터링 시 간과하기 쉽다.
드롭퍼(dropper)	<ul style="list-style-type: none"> • 외부에서 파일을 내려받는 다운로더와 달리 드로퍼는 자신 안에 존재하는 데이터로부터 새로운 파일을 생성하여 공격을 수행하는 것이 목적이다. • 드로퍼가 생성하는 파일은 압축되어 있어 실행해보기 않고서는 확인하기 어렵다.
런처(launcher)	<ul style="list-style-type: none"> • 다운로드나 드로퍼 등으로 생성된 파일을 실행하기 위해 관련 기능을 포함하고 있다.
애드웨어(adware)	<ul style="list-style-type: none"> • 광고가 포함된 소프트웨어로, 자체에 광고를 포함하거나 같이 묶어서 배포한다. • 압축 또는 동영상 재생 프로그램과 같은 프리웨어 설치 시에 동의 항목에 포함되어 설치 및 실행되는 경우가 많다. • 사용자의 인식 없이 설치된 애드웨어는 인터넷 시작 페이지 변경하기, 광고와 관련된 알람 창 띄우기, 바탕화면에 광고 페이지의 바로가기가 지속 생성하기 등을 목적으로 한다.
스파이웨어(spyware)	<ul style="list-style-type: none"> • 개인이나 기업의 정보를 몰래 수집하여 동의 없이 다른 곳에 보내는 것이 목적이다. • 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. • 스파이웨어는 패스워드 스틸러, 키로거 등으로 세분화될 수 있다.
랜섬웨어(ransomware)	<ul style="list-style-type: none"> • 인질의 몸값을 나타내는 'ransom'과 'software'의 합성어로, 최근 급격히 퍼지고 있는 악성 코드다. • 사용자에게 랜섬웨어가 실행되면 파일 암호화가 진행되어 사용자가 실행하거나 읽을 수 없게 한다. • 즉 자료를 인질로 잡고 돈을 요구한다. • 한 번 암호화된 파일은 복구가 거의 불가능하므로 백업과 같은 사전 대비가 가장 중요하다.
백도어(backdoor)	<ul style="list-style-type: none"> • 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. • 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.
익스플로잇(exploit)	<ul style="list-style-type: none"> • 운영체제나 특정 프로그램의 취약점을 이용하여 공격하는 악성 코드다. • 기존의 익스플로잇 코드는 공격자가 직접 공격을 수행했으나 최근에는 악성 코드로 제작 및 배포하여 자동으로 공격 확산을 수행하는 경우가 많다.
봇(bot)	<ul style="list-style-type: none"> • DDoS 공격 시 지정된 공격을 수행하도록 하는 악성 코드다. • 수많은 봇이 모여 대규모 DDoS 공격을 수행하는 봇넷을 구성한다.
스케어웨어(scareware)	<ul style="list-style-type: none"> • 'scare(겁주다)'와 'software'의 합성어로, 사용자를 놀라게 하거나 겁을 주어 원하는 목적을 달성한다. • 악성 코드에 감염되지 않았는데도 악성 코드를 탐지했다고 겁을 주고 자사의 안티바이러스 제품으로 제거해야 한다는 식으로 구매를 유도한다.

악성코드 분류 방법

악성 프로그램 감염 증상

표 6-3 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.

02. 악성코드 종류

바이러스

1세대 원시형 바이러스(파일 바이러스)

- 파일을 직접 감염시켜 바이러스 코드를 실행시킴
- 하드디스크 부팅의 일반화로 부트 바이러스의 대안으로 등장
- COM, EXE와 같은 실행 파일과 오버레이 파일, 디바이스 드라이버 등에 감염
- 전체 바이러스의 80% 이상을 차지
- 파일 바이러스의 감염 위치
 - (a) 덮어쓰기형 : 정상 프로그램의 일부분을 바이러스로 덮음
 - (b) 바이러스가 프로그램 앞에 위치한 경우
 - (c) 바이러스가 프로그램에 뒤에 위치한 경우



그림 6-4 파일 바이러스의 감염 위치

바이러스

1세대 원시형 바이러스(파일 바이러스)

- 바이러스가 프로그램 뒷부분에 위치하는 것은 백신에 탐지되는 것을 피하기 위함
- 프로그램 뒷부분에 위치한 바이러스가 실행되는 형태
- 종류 : 예루살렘 바이러스(최초의 파일 바이러스), 선데이(sunday), 스코피온(scorpion), 크로(crow), FCL, CIH 바이러스

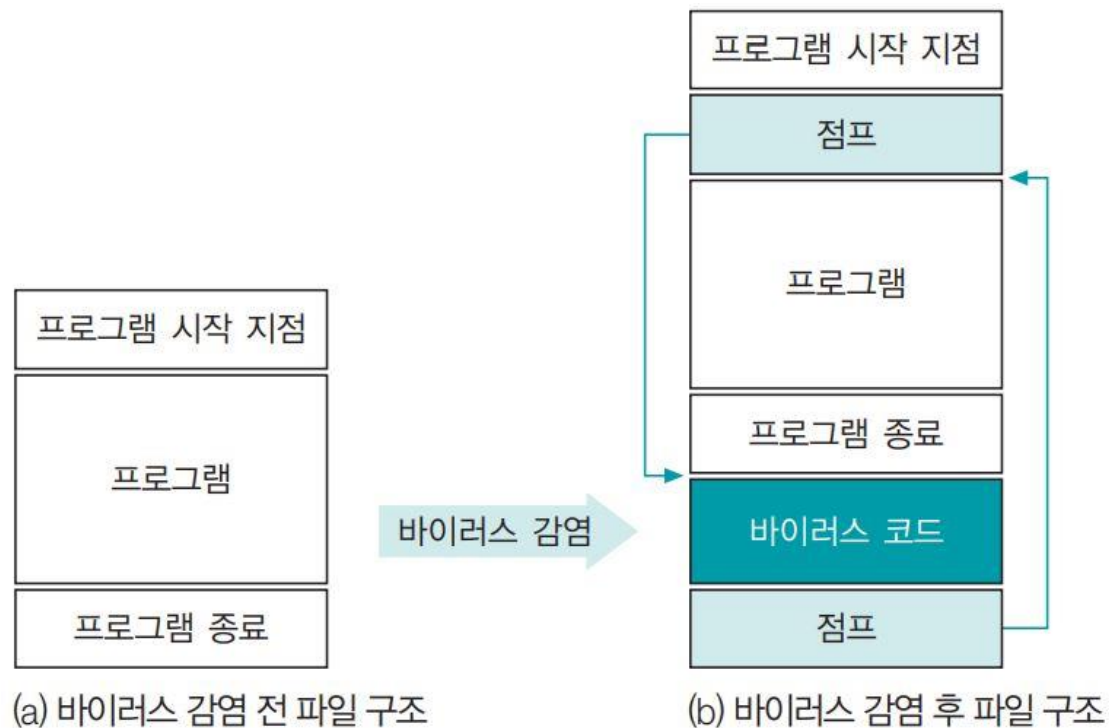


그림 6-5 바이러스가 프로그램 뒷부분에 위치할 때의 실행 과정

바이러스

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 치료함.
- 종류 : 슬로(slow), 캐스케이드(cascade), 원더러(wanderer), 버글러(burglar) 등

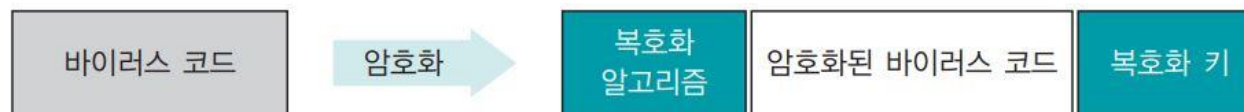


그림 6-6 암호화된 바이러스 코드

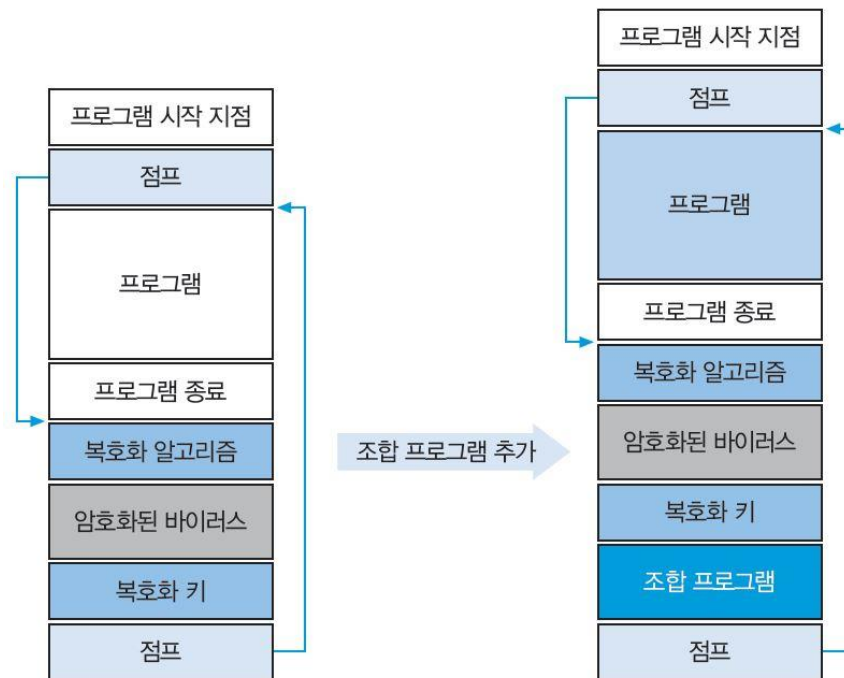
3세대 은폐형 바이러스

- 바이러스에 감염된 파일이 일정 기간 잠복기를 가지도록 만든 것으로, 이는 바이러스가 확산되기도 전에 활동하기 시작하면 다른 시스템으로 전파되기 힘들기 때문임.
- 종류 : 브레인, 조시(joshi), 512, 4096 바이러스 등

바이러스

4세대 다형성 바이러스

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



[그림 6-7] 다형성 바이러스

바이러스

5세대 매크로 바이러스

- MS 오피스 프로그램의 매크로 기능으로 감염되는 바이러스를 뜻하며, Visual Basic Script로 많이 제작됨
- 종류 : 워드 콘셉트(word concept), 와쭈(wazzu), 엑셀-라룩스(laloux), 멜리사 바이러스 등
- 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 VB(Visual Basic) 편집기의 디버그 모드가 실행됨

차세대 바이러스

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



웜

● 개념

- IT 분야에서 웜(worm)은 인터넷 또는 네트워크를 통해 컴퓨터에서 컴퓨터로 전파되는 프로그램
- 웜은 스스로를 증식하는 것이 목적이므로 파일 자체에 이런 기능이 있거나 운영체제에 자신을 감염시킴

● 매스메일러형 웜

- 자기 자신을 포함하는 대량 메일을 발송하여 확산되는 것
- 제목 없는 메일이나 특정 제목의 메일을 전송하고 사용자가 이를 읽었을 때 감염됨
- 매스메일러형 웜의 주요 특징과 증상
 - 메일로 전파. 감염된 시스템이 많으면 SMTP 서버(TCP 25번 포트)의 네트워크 트래픽이 증가함
 - 출처나 내용이 확인되지 않은 메일을 열었을 때 확산되는 경우가 많음
 - 베이글 웜은 웜 파일을 실행할 때 가짜 오류 메시지를 출력함
 - 넷스카이 웜은 윈도우 시스템 디렉터리 밑에 CSRSS.exe 실행 파일을 만듦
 - 변형된 종류에 따라 시스템에 임의의 파일을 생성함
- 종류 : 베이글(bagle), 넷스카이(netsky), 두마루(dumaru), 소빅(sobig) 등

웜

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 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
- 종류 : 아고봇, 블레스터 웜, 웰치아 등

웜

● 네트워크 공격형 웜

- 특정 네트워크나 시스템에 대해 SYN 플러딩이나 스머프와 같은 서비스 거부(DoS) 공격 수행
- 분산 서비스 거부(DDoS) 공격을 위한 봇(bot) 형태로 발전하고 있음.
- 주요 증상
 - 네트워크가 마비되거나 급격히 느려짐.
 - 네트워크 장비가 비정상적으로 동작함.
- 대표적인 네트워크 공격형 웜은 클레즈(klez).
- 이 유형의 웜은 적은 수의 시스템이 감염되어도 파급 효과가 크므로 안정적인 네트워크 설계와 시스템 취약점에 대한 지속적인 패치 관리가 중요함.

트로이 목마

개요

- 트로이 목마(Trojan horse)는 **악성 루틴이 숨어 있는 프로그램**
- 겉보기에는 정상적인 것 같지만 사용자가 실행하면 악성 코드 실행
- 사회공학 기법 형태로 퍼짐
- 어떤 악성 코드도 포함될 수 있어서 시스템 파괴, 랜섬웨어 등 어떤 형태로든 가능하지만 주로 백도어로 사용됨
- **다른 파일에 삽입되거나 스스로 전파되지 않음**
 - 트로이 목마와 혼용되는 백도어(backdoor)는 악성 코드를 지칭하는 말로 사용되는 경우가 많지만, 원래 의미는 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않아도 접근할 수 있게 만든 일종의 통로. 프로그램 개발 후 완전히 삭제되어야 하지만 그대로 남아 있는 경우도 있음.



그림 6-11 트로이 목마

PUP

개요

- PUP(Potentially Unwanted Program)는 사용자에게 직간접적으로 동의를 구하지만 용도를 파악하기 어려운 상태에서 설치되는 프로그램
- 설치되는 경우
 - 크랙 사이트 등의 불법 사이트 접속 시 설치
 - 악성 코드에 의해 설치
 - 특정 프로그램을 설치할 때 함께 설치
- 최근에는 특정 프로그램 설치 중에 함께 설치되는 경우가 많음
- 사용자에게 치명적인 악영향을 주는 것은 아니지만 귀찮을 정도로 광고를 지속적으로 보여주거나, 웹 브라우저의 시작 페이지를 특정 페이지로 강제로 변경, 사용하고 싶지 않은 백신을 강제로 사용하게 함.

악성코드 동향

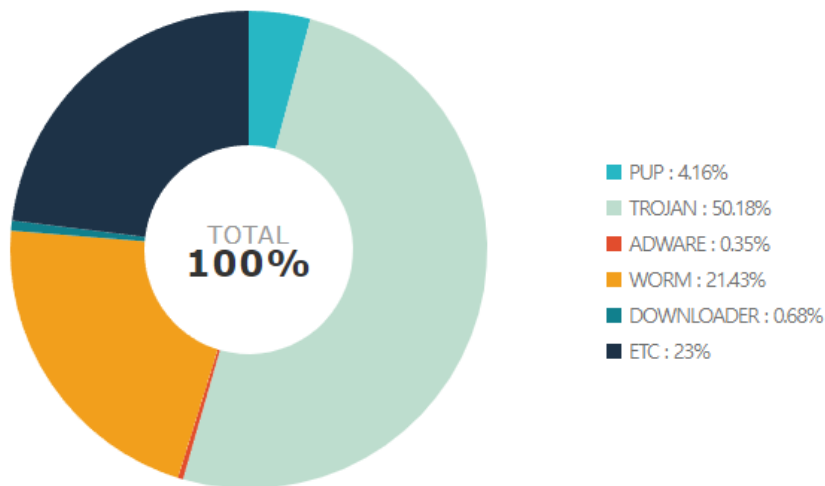
악성코드 유포율

- 21년 2월 기준으로 트로이목마 악성코드 유포율이 가장 높음
- 트로이목마 형태로 유포되어 공격자의 제작목적에 따라 악성행위 수행
 - 랜섬웨어, 드로퍼, 익스플로잇, 봇 등

악성코드 유형

가장 높은 비중을 차지한 악성코드 유형(%)

TROJAN 50.18%



출처 : Ahnlab, 22년 2월 기준으로 최근 1개월의 악성코드 유형별 유포율

03. 랜섬웨어



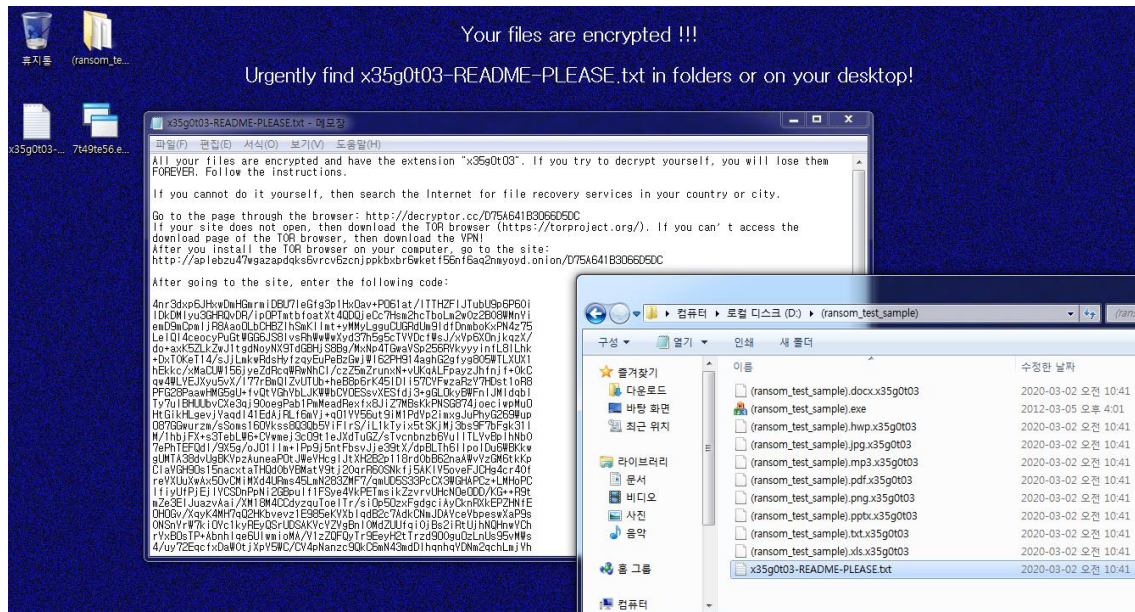
CPS Security Lab
Cyber Physical Systems Security Laboratory



랜섬웨어 개요 (1/2)

랜섬웨어란?

- 사용자의 파일, 자료, 데이터를 인질로 잡고 협박하는 악성코드로, 최근 가장 유행
- **인질의 몸값을 나타내는 'ransom'과 'software'의 합성어**
- **사용자에 의해 랜섬웨어가 실행되면 파일 암호화가 진행되어 사용자가 실행하거나 읽을 수 없게 함**
- 한 번 암호화된 파일은 복구가 거의 불가능하므로 백업과 같은 사전 대비가 가장 중요



출처 : ESTsecurity, Sodinokibi 랜섬웨어 감염 시스템 바탕화면 및 랜섬노트



출처 : checkmal blog, 다크사이드 랜섬웨어 감염 시스템 바탕화면

출처 : 이스트시큐리티 알약 블로그, "복호화를 위한 페이지 접속시 CAPTCHA코드를 삽입한 최신 Sodinokibi 랜섬웨어 발견". <https://blog.alyac.co.kr/2796>. 2020.03.
체크말블로그, "국가 기반 시설을 공격한 DarkSide 랜섬웨어 정보". <https://blog.naver.com/checkmal/222357247837>. 2021.05.

랜섬웨어 개요 (2/2)

특징

- **빠르게 신종 버전**이 발견되고 있으며, 이메일, 파일 공유, 소프트웨어 업데이트 등의 취약점을 이용하여 다양하게 유포
- 민감하고 중요한 정보를 다루는 병원, 기업체를 대상으로 집중 공격하여 큰 피해 규모가 발생하는 경우가 많음
- **ICS/OT 시스템에 랜섬웨어 감염 시, 대규모 피해 발생 피해 발생**
- **금융 추적이 어려운 암호화폐를 금전 지불 방법으로 지정해서 비교적 안전하게 금전 취득**
- 랜섬웨어 실행 시, 금전 지불 방법이 담긴 랜섬노트(ransom note)생성
 - 랜섬노트 데이터 : 암호화폐 지갑 주소, 복호화 키, 지불 방법 설명
- 랜섬웨어는 제작자마다 특정한 암호화 알고리즘을 통해 파일 암호화 수행
- 암호키 없이 개별적으로 복호화하는 것은 불가능에 가까움
 - 구형 버전, 제작자의 실수와 같은 경우 복호화가 가능
 - Window VSS(Volume Shadow Copy) 기능과 같은 복원 및 백업 기능을 무력화
- 대표적인 랜섬웨어 : GandCrab/BlueCrab/Sodinokibi, WannaCry, DrakSide



출처 : FINANCIAL TIMES, 콜로니얼 파이프라인 피해 규모

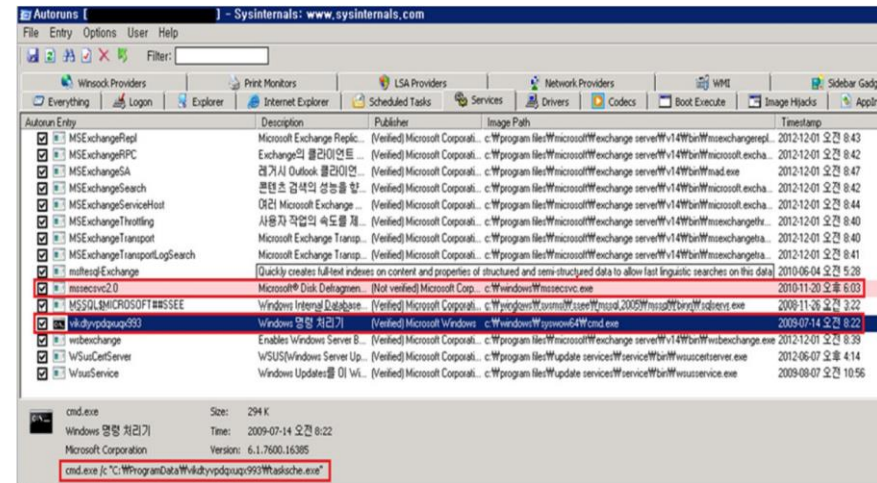
대표적인 랜섬웨어 (1/2)

워너크라이(WannaCry) 랜섬웨어

- 2017년 2월에 최초 발견된 랜섬웨어로, ***SMB 취약점을 이용하여 주변에 자체 전파하는 것이 특징**
 - SMB(Server Message Block) : 파일 · 장치를 공유하기 위해 사용되는 통신 프로토콜
 - SMB 취약점(CVE-2017-0144) : 원격에서 특수하게 조작된 SMB 메시지를 전송하여 원격에서 코드를 실행시킬 수 있는 취약점으로 이터널 블루(EternalBlue)로 명명
- 감염된 시스템은 SMB가 활성화되었다는 공통점이 있으며, 암호화된 파일은 '.wncry' 확장자로 변경
- 워너크라이는 윈도우 서비스로 등록되어 실행되며, 재부팅 시 자동 실행하도록 설정
 - msseccsvc.exe : 감염된 시스템의 취약점 스캔 및 암호화 악성코드 드롭퍼
 - tasksche.exe : 파일 암호화 악성코드 드롭퍼



출처 : KISA, 워너크라이 감염 시스템 배경화면 및 랜섬노트

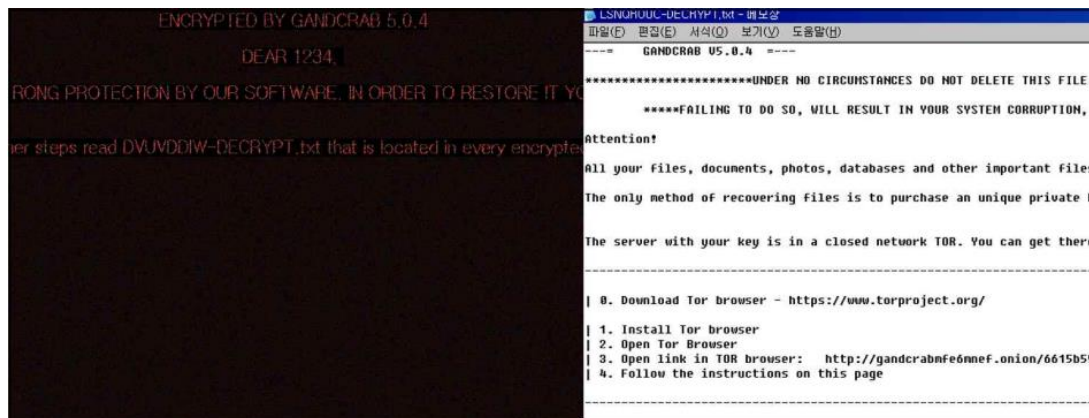


출처 : KISA, 워너크라이가 등록된 윈도우 서비스 화면

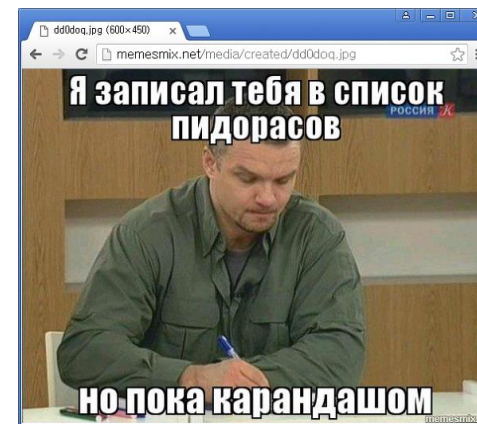
대표적인 랜섬웨어 (2/2)

● 갠드크랩(Gandcrab) 랜섬웨어

- 2018년 1월 발견되면 버전 1부터 5.3까지 발전하며 약 20억 달러 수익을 올림
 - 19년 6월 제작자가 은퇴를 발표하였으며, 21년 2월 국제공조로 인해 제작자 검거
- 암호화된 파일은 '.GDCB', '.KRAB' 등으로 확장자로 변경
- 위협이 되는 기업, 인물에 대해 악성코드 내에 명시 및 특정 백신 무력화**
 - 안랩에 대한 공격적인 행동을 보인
 - "Fortinet & ahnlab, mutex is also kill-switch not only lockfile ;)" 라는 문구를 악성코드 내에 포함
 - V3 제거 기능을 추가하거나 안랩을 러시아어로 욕하는 사진의 URL 포함



출처 : KISA, 갠드크랩 감염 시스템 배경화면 및 랜섬노트



출처 : ANLAB, 갠크크랩 내 안랩 욕설 URL

출처 : KISA, 워너크라이 분석 스페셜리포트

보안뉴스, "2조 3천억 번 갠드크랩 랜섬웨어 제작, 이젠 먹튀?" <https://www.boannews.com/media/view.asp?idx=80079&page=1&kind=1>

보안뉴스, "경찰서·헌법재판소·한국은행 사칭 '갠드크랩' 랜섬웨어 국내 유포자 검거", <https://www.boannews.com/media/view.asp?idx=95445&page=1&kind=1>

ANLAB ASEC, "변종 GandCrab v4.1.2 내부에 등장한 AhnLab 문구와 이미지", <https://asec.ahnlab.com/ko/1146/>

ICS/OT 환경의 랜섬웨어

사례 및 파급효과

- ICS/OT 시스템에 랜섬웨어 감염 시, 시스템 중단, 파괴 등의 대규모 피해 발생
- 21년 콜로니얼 파이프라인(Colonial Pipeline) 다크사이드(Darkside) 랜섬웨어 감염 사건
 - 콜로니얼 파이프라인은 미국 동부 해안 연료 수요량의 약 45% 담당
 - 랜섬웨어 감염으로 **파이프라인이 중단되어 휘발유 가격이 배럴당 3달러 상승**
- 19년 노르스크 하이드로(Norsk Hydro) 록커고가(LockerGoga) 랜섬웨어 감염
 - 노르스크 하이드로는 세계 4위의 합성 알루미늄 제조회사
 - 랜섬웨어 감염으로 **공장 생산 중단 및 폐쇄로 5,500만 달러의 대규모 피해 발생**

피해 조직	국가	피해 연도	공격 종류
콜로니얼 파이프라인(Colonial Pipeline)	미국	2021	랜섬웨어(Darkside)
솔 오리엔스(Sol Oriens)	미국	2021	랜섬웨어(REvil)
JBS 푸드(JBS Foods)	미국	2021	랜섬웨어(REvil)
혼다(Honda)	일본	2020	랜섬웨어(EKANS)
노르스크 하이드로(Norsk Hydro)	노르웨이	2019	랜섬웨어(LockerGoga)
레이크 시티(Lake City)	미국	2019	랜섬웨어(Ryuk)
우드 랜치 메디컬(Wood Ranch Medical)	미국	2019	랜섬웨어
사우디아라비아 석유화학공장	사우디	2017	지능형 지속 위협(APT; Advanced persistent threat) 공격(Triton)
우크라이나 지방 전력공급회사	우크라이나	2015/2016	APT 공격(Black Energy)
이란 부셰르 원자력 발전소	이란	2010	APT 공격(Stuxnet)

출처 : Deloitte, ICS/OT 관련 사이버침해사고 사례

04. 악성코드 탐지 및 대응책



실습 도구

- 윈도우 7 악성 코드: Win-Trojan.Pearmor
- Process Explorer
 - 시스템에서 실행 중인 프로세스 정보 수집을 위한 기능 제공
 - 프로세스 목록, 핸들값, 하위 프로세스 등
- Total Commander: <http://www.ghisler.com>
 - 윈도우의 파일 관리자 프로그램으로 FTP, 파일 비교, 압축 파일 처리, 파일비교 등의 기능 제공
- CPorts: <http://www.nirsoft.net/utills/cports.html>
 - 시스템에서 현재 열려 있는 모든 TCP/IP, UDP 포트 목록을 표시해주는 네트워크 모니터링 소프트웨어

실습 방법

네트워크 상태 점검하기

- 상당수의 악성 코드는 외부에 있는 해커나 악성 코드 작성자와의 통신을 위해 서비스 포트 생성
- 주요 악성 코드가 사용한 서비스 포트

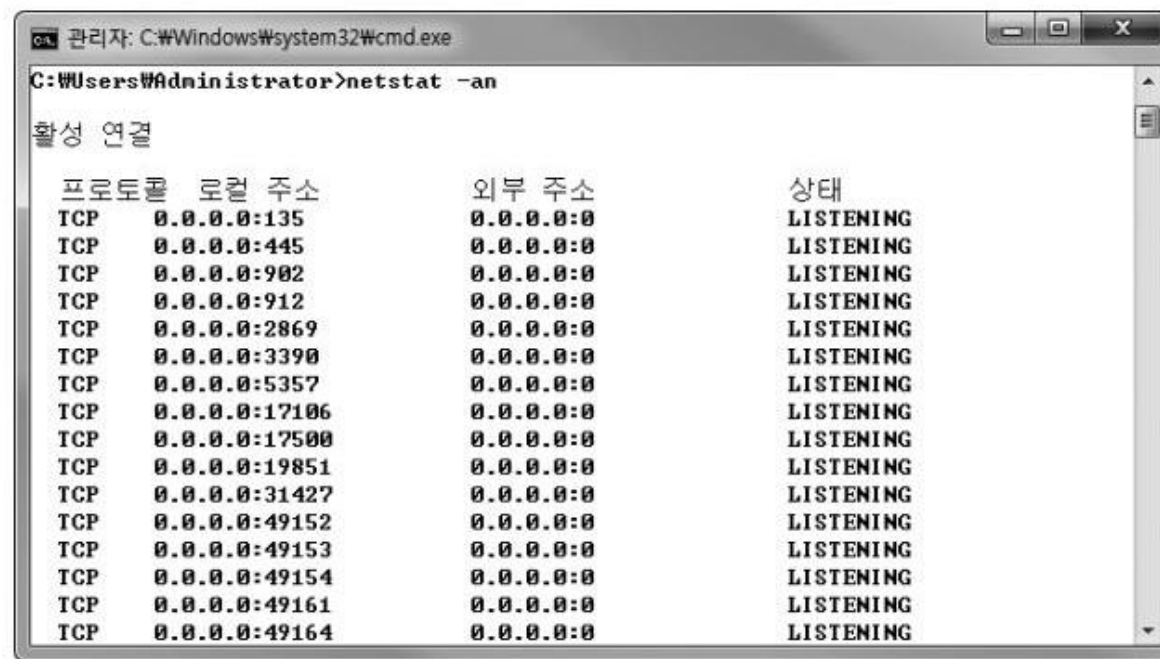
표 6-4 주요 악성 코드가 사용한 서비스 포트

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

실습 방법

네트워크 상태 점검하기

- 시스템에서는 netstat 명령으로 열려 있는 포트 확인 가능
- 프로세스 별로 열린 포트 확인 가능



```
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 6-14 netstat -an 실행 결과

실습 방법

네트워크 상태 점검하기

- 번호만으로 추측하기가 어려운 경우에는 CPorts 같은 프로그램으로 서비스 포트별로 사용하는 응용 프로그램 확인 가능
- BackDoor-DVR 실행한 뒤 CPorts에서 활성화된 네트워크 항목을 살펴보면 특이한 연결을 발견 가능
- 2368번 프로세스가 원격지의 80.79.192.72 시스템에 특정 패킷을 보내 네트워크 상태(State)가 Sent인 것을 확인 가능

CPorts application window showing active ports and connections. The table lists processes, their ports, protocols, and local addresses. A connection to 80.179.192.172 is highlighted.

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address
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	:::1			:::
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		:::1			:::
Internet Explorer.exe	2368	TCP	49509		192.168.239.128	81	hosts2-ns	80.179.192.172

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

CPorts application window showing connection details for the selected connection. The table lists port, remote address, remote host name, state, process path, and product name.

Port	Remote Address	Remote Host Name	State	Process Path	Product Name
			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>

그림 6-15 CPorts 실행 결과

실습 방법

● 정상적인 프로세스와 비교하기

- 윈도우와 유닉스 시스템 등의 정상적인 프로세스를 외워두면 비정상적인 프로세스 식별에 도움이 됨.
- 윈도우에서는 [Ctrl]+[Alt]로 작업 관리자 실행하여 현재 실행 중인 프로세스 확인 가능.



[그림 6-16] 윈도우에서 동작 중인 프로세스 확인

실습 방법

● 정상적인 프로세스와 비교하기

■ 윈도우 시스템이 동작하기 위한 기본 프로세스

- **csrss.exe(client/server runtime subsystem: win 32):** 윈도우 콘솔 관장, 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
- **svchost.exe(service host process): DLL(Dynamic Link Libraries)에 의해 실행되는 기본 프로세스**
- 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·로그오프 담당 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 입력 처리 지원 프로세스
- dfssvc.exe(distributed file system): 분산 파일 시스템(DFS)을 지원하기 위해 백그라운드로 실행되는 프로세스

■ 악성 코드가 주로 사용하는 서비스명은 **csrss와 svchost**

- 정상 프로세스명과 비슷하게 하여 정상 프로세스로 위장하는 경우도 존재

실습 방법

● 악성 코드의 실제 파일 확인하기

- 네트워크 상태와 프로세스 분석을 통해 파악한 악성 코드의 실제 파일을 확인하는데 total commander와 같은 툴 사용

● 시작 프로그램과 레지스트리 확인하기

- 윈도우는 시스템 운영과 관련된 것의 기본 설정 값이 재부팅 시에도 변하지 않도록 레지스트리에 여러 가지 값 기록
- 레지스트리를 악성 코드가 이용하는 경우가 많으므로 악성 코드를 삭제할 때는 레지스트리에서 관련 내용 확인 필요
 - 악성코드 지속성을 위한 시작 프로그램 설정
 - 백신 탐지 회피를 위한 악성 코드 데이터 저장
- 시작 프로그램 목록은 msconfig 명령으로 확인 가능.

● 악성 코드 제거하기

- 확인한 악성 코드를 삭제하는 절차
 - ① 악성 코드 프로세스 중지하기
 - ② 악성 코드 파일 삭제하기
 - ③ 레지스트리 삭제하기

Q&A

