

## CHAPTER 10

# 안티 바이러스

# 목차

- 바이러스와 악성코드
- 안티 바이러스의 이해
- 바이러스/악성코드의 탐지 원리



I

# 바이러스와 악성코드

## 1

## 컴퓨터 바이러스

- 컴퓨터 내 다른 프로그램이나 기억장치에 **자기 자신 또는 자기 자신의 변형을 복제 · 삽입해가며 감염(확산)**시키는 컴퓨터 프로그램
- 정보통신망 환경에서는 **네트워크 범위로까지 확산** 가능하며, 시대가 지나면서 바이러스의 기능도 점차 진화하는 경향
- 컴퓨터 바이러스의 **세대 구분**

1세대

원시형 바이러스

2세대

암호형 바이러스

3세대

은폐형 바이러스

4세대

다형성 바이러스

5세대

매크로 바이러스

## 컴퓨터 바이러스

### ■ 1세대 : 원시형 바이러스

- 컴퓨터 바이러스가 처음 등장했을 때와 같이 **원시적인 형태**
- **자기 복제** 기능이 주 기능
- 악의적인 목적으로 유포된 경우 컴퓨터 내 자료/정보를 **파괴하는 기능**도 포함

부트 바이러스

파일 바이러스

## 컴퓨터 바이러스

### 1세대 : 원시형 바이러스

#### 부트 바이러스

- 과거의 컴퓨터는 하드디스크 용량이 충분치 않았기 때문에 플로피 디스크 등 **외부의 보조기억장치에 운영체제를 보관**하고 이를 삽입하여 부팅
- 컴퓨터 사용 중 부트형 바이러스가 실행되면 **삽입된 운영체제 디스크에 감염** 발생
  - 주로 운영체제의 부팅 영역(Master Boot Record, MBR)을 감염
- 감염된 운영체제 디스크로 컴퓨터를 부팅하면 **운영체제와 함께 바이러스가 실행**되어 임의접근메모리(RAM)에 상시 상주하며, 이후 사용되는 모든 프로그램에도 **바이러스가 주입 · 감염**되는 방식

예

브레인

몽키

미젤란젤로 바이러스

...

1

## 컴퓨터 바이러스

- 1세대 : 원시형 바이러스

부트 바이러스

파일 바이러스

- 하드디스크의 사용이 보편화되면서 등장하여, 오늘날 대부분의 컴퓨터 바이러스는 파일 바이러스
- 주로 실행 파일(EXE, COM 등)에 감염되며, 실행 파일의 앞 부분이나 뒷 부분에 바이러스 코드를 붙이는 방식으로 감염
  - 안티 바이러스가 등장한 이후에는 안티 바이러스에 의한 탐지를 회피하기 위해 실행 파일의 뒷 부분에 바이러스 코드를 붙이는 방식 유행

예

예루살렘 바이러스 (최초의 파일 바이러스)	선데이	스콜피온	크로우
FCL	CIH(체르노빌) 바이러스	...	

## 컴퓨터 바이러스

### ■ 2세대 : 암호형 바이러스

- 원시형 바이러스는 **안티 바이러스에 의한 탐지가 용이한 만큼, 이를 회피하기 위해 바이러스 코드를 암호화하고 복호화 논리와 키를 같이 붙이는 방식으로 감염시키는 바이러스**
  - 단, 바이러스가 실행될 때 복호화 되기 때문에 **임의접근메모리(RAM)에 적재된 바이러스 탐지 가능**

### • 대표적인 예



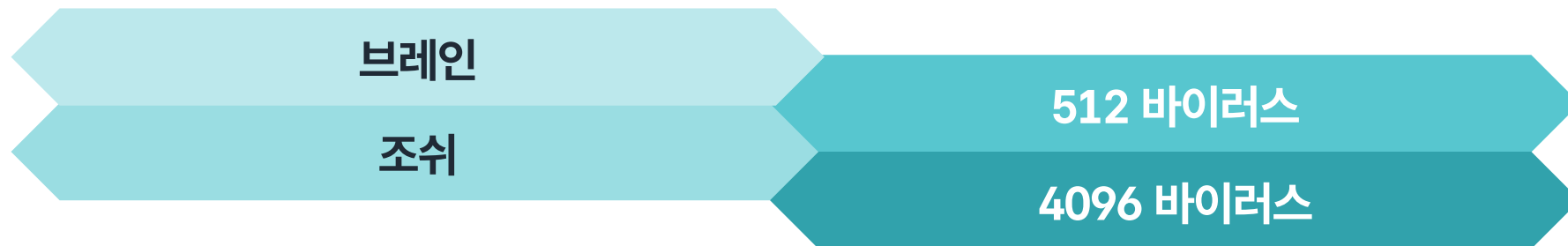


## 컴퓨터 바이러스

### ■ 3세대 : 은폐형 바이러스

- 바이러스에 감염되더라도 **일정 기간 잠복기**를 갖도록 만든 바이러스
  - 바이러스가 확산되기 전에 활성화되면 **안티 바이러스**에서 탐지할 수 있어 확산이 어렵기 때문
  - 안티 바이러스 내 실시간 감시 기능이 포함되면서 **잠복기 이후 활성화가 될 때 탐지** 가능

### • 대표적인 예



## 컴퓨터 바이러스

### ■ 4세대 : 다형형 바이러스

- 바이러스가 자기 자신의 코드를 지속적으로 변형해나가며 전파시키는 바이러스
  - 안티 바이러스가 탐지하는 바이러스 고유의 패턴(문자열, 식별자 등)을 변경하는 방식으로 탐지 원리를 우회
  - 특히, 암호형 바이러스나 은폐형 바이러스의 특성을 같이 갖는 경우  
안티 바이러스에 의한 탐지가 어려워지는 경향
- 대표적인 예

Polip

## 컴퓨터 바이러스

### ■ 5세대 : 매크로 바이러스

- Microsoft Office 제품군에는 **자동화**를 위한 편의 기능으로 매크로 기능을 제공

#### 장점

VBS(Visual Basic Script) 코드에 기반을 두고 있어  
컴퓨터 프로그램 수준의 자동화를 구현

#### 단점

이를 악용하여 운영체제의 API를 호출하는 등의  
방식으로 컴퓨터에 악영향을 초래

- 사무 현장에서 **매크로가 빈번하게 쓰이는 점을 악용한** 바이러스
  - 이로 인해 보안 정책상 매크로 기능 자체를 금지하던 곳들도 많았으나,  
생산성 측면에서 **매크로 기능 제한을 완화하는 경우가 우세**해지는 경향

- **대표적인 예**

워드 콘셉트

와쭈

엑셀 - 라룩스

멜리사 바이러스

## 악성코드

- 컴퓨터 바이러스는 태생적으로 **자기 자신을 복제**해가거나 그렇지 않더라도 **다른 파일들의 무결성을 훼손**하는 특성 보유
- 컴퓨터의 사양이 높아지고 정보통신망 환경이 보편화되면서 **전통적인 바이러스의 특성을 갖지 않으면서도 악성 기능을 수행하는 컴퓨터 프로그램**이 등장
  - 전통적인 바이러스의 특성이 도리어 **안티 바이러스에 의해 탐지될 수 있는 가능성을** 높게 만드는 원인으로 작용
  - 공격자 입장에서는 **악성 기능을 통해 악의적 목적을 달성**하는 것이 가장 중요하기 때문에 전통적인 바이러스의 특성을 유지해야 할 이유가 없음.

## 악성코드 (Malware)



종래의 컴퓨터 바이러스의 개념을 포함하며,  
악의적 목적을 가진 모든 종류의 실행 가능한  
컴퓨터 프로그램을 총칭

### ■ 악성코드의 법령상 정의

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률, 과학기술정보통신부)

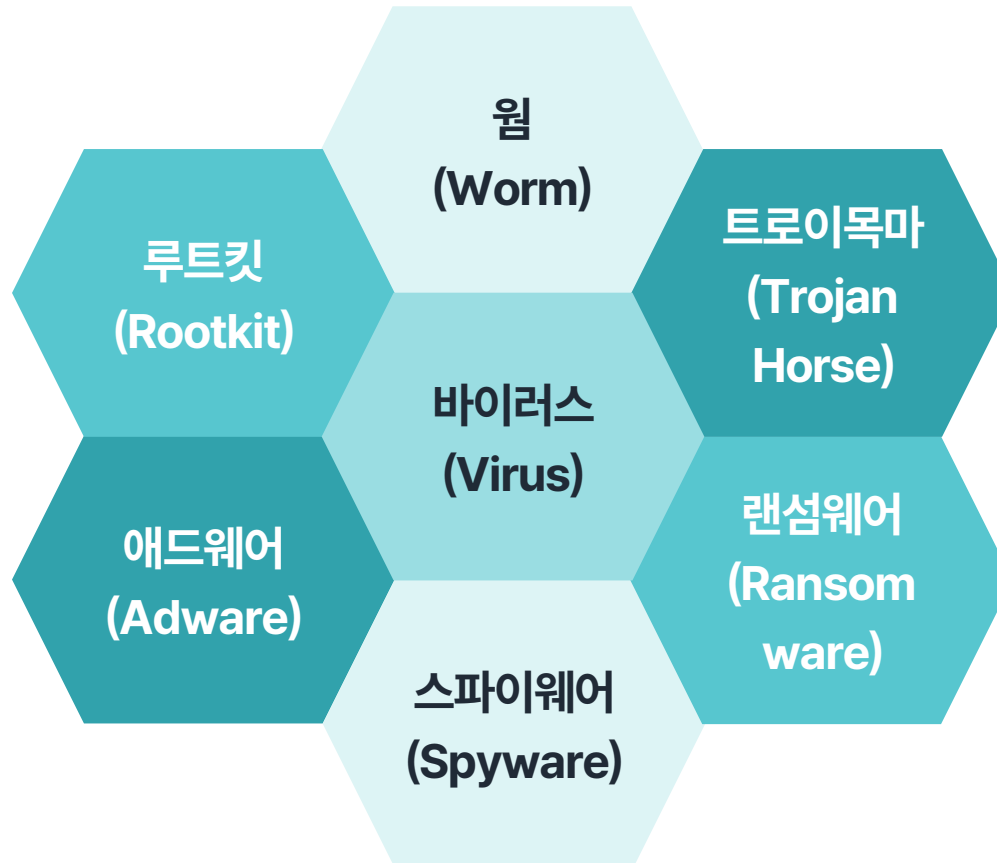
#### 제48조(정보통신망 침해행위 등의 금지)

- ② 누구든지 정당한 사유 없이 정보통신 시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니된다.



## 악성코드

### ■ 악성코드의 종류



## 악성코드

### ■ 웜 (Worm)

#### 웜 (Worm)

- **정보통신망 환경이 보편화되면서 등장한 악성코드**
- 다른 프로그램에 감염되어 전파되는 컴퓨터 바이러스와는 달리 **자체적으로 실행되면서 네트워크를 통해 다른 컴퓨터로 전파가 가능**한 악성코드
- 공유 폴더, 특정 네트워크 포트, 운영체제 취약점 등을 **악용하여 전파·확산**
- **보안 환경이 취약했던 때에는** 웜에 의해 대규모 피해가 발생하는 경우가 빈번
  - 2003년 1월, 슬래머 웜에 의한 인터넷 대란(국가적인 정보통신망 마비) 사태
  - 2003년 8월, 블래스터 웜으로 인해 전세계적으로 모든 컴퓨터가 1~2분 간격으로 강제 재부팅되는 피해 발생
- 대표적인 예
  - 모리스 웜
  - 블래스터 웜
  - 코드레드 웜
  - 슬래머 웜



## 악성코드

- 트로이목마 (Trojan Horse)

### 트로이목마 (Trojan Horse)

그리스 로마 신화에 등장하는 트로이 전쟁에 등장하는 거대한 목마처럼, 외견상 정상적인 프로그램처럼 보이지만 악성 기능을 포함하는 악성코드



### ■ 트로이목마 (Trojan Horse)

- 사용자의 실행을 유도하기 위해 **사회공학적 방법으로 유포**되는 경향이 있음
- **불법 소프트웨어나 불법 파일에 포함**되는 경우도 상당수
- 트로이목마에는 **다양한 악성 기능을 포함**시킬 수 있지만, 대부분의 트로이목마 그 자체는 **추후 공격을 위한 백도어(개구멍)을 조성**하는 목적으로 활용
  - 악성 기능을 포함시키는 만큼 악성코드 자체의 용량도 증가하므로 안티 바이러스에 의한 탐지 가능성 증가

예

2013년 2월

북한발 320사이버테러에 앞서 트로이목마 선 유포

2013년 3월

트로이목마에 의해 추가 다운로드 된 악성코드가 실행되며 320사이버테러 발생  
(주요 언론사 및 금융사 대상 다수의 자료/정보 파괴)

## 악성코드

### ■ 스파이웨어 (Spyware)

#### 스�파이웨어(Spyware)

개인이나 기업의 정보를 몰래 수집하는 **정보 절취 목적으로 사용되는 악성코드**

#### 키 로거 유형 (Key Logger)

사용자의 **키 입력이나 비밀번호 입력**을 절취

#### 원격 제어 유형 (Remote Control System, RCS)

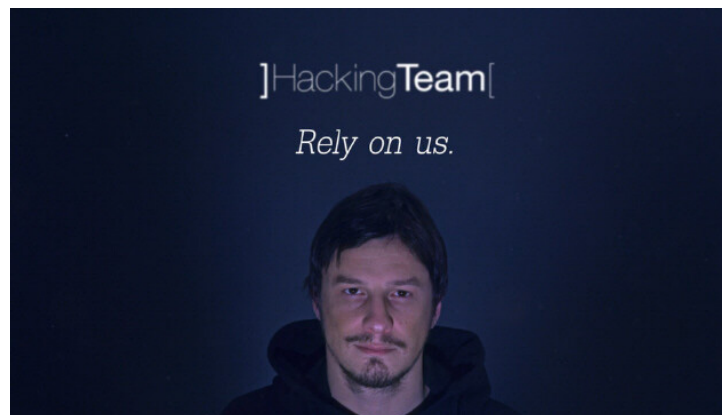
**컴퓨터 내 파일을 절취하거나 웹 카메라나 마이크를 활성화**하는 등 컴퓨터 원격 제어

- 합법적인 목적으로 사용하는 원격 제어 소프트웨어가 스파이웨어로 악용되는 경우도 존재

## 악성코드

### ■ 스파이웨어 (Spyware)

- 정보수사기관에 의해 범죄 내사/수사 목적으로 악용된 사례
  - 2015년, 국가정보원에서 이탈리아 해킹팀(社)로부터 RCS를 구입하여 블로그 게시물 열람 시 감염되도록 은닉한 사실이 적발되어 사회적인 파장 발생
    - \* 국가정보원은 동일한 스파이웨어를 국군기무사령부 소속 해군 소령이 중국 측에 군사자료를 넘긴 사실을 확인하기 위한 목적으로도 활용



## 악성코드

### ■ 애드웨어 (Adware)

#### 애드웨어(Adware)

치명적인 악영향을 끼치지 않지만 **귀찮을 정도로 광고를 보여주는 등의** 행위를 하는 악성코드

- 반복적으로 광고 팝업을 발생시키거나 웹 브라우저의 시작 페이지를 강제로 변경
- 컴퓨터 내 불필요한 파일 및 서비스가 발생되면서 컴퓨터의 성능 저하 원인으로도 작용
- 정상적인 소프트웨어, 특히 무료로 배포되는 소프트웨어를 설치할 때 설치 마법사 내 사용자의 동의를 유도하는 방식으로 같이 설치되는 경우가 빈번

## 악성코드

### ■ 랜섬웨어 (Ransomware)

#### 랜섬웨어(Ransomware)

컴퓨터 내 **파일들을 암호화**하거나 **화면을 잠그고** 이를 풀어주는 대가로 금전을 요구하는 악성코드

- 기존의 악성코드가 절도, 손괴, 폭행, 스토킨이라면 랜섬웨어는 **인질 강도**에 가까운 형태



## 악성코드

### ■ 랜섬웨어 (Ransomware)

- 비트코인 등 가상자산이 등장한 이후에 급격히 유행하게 되었으며, 많은 기업 및 개인을 대상으로 막대한 **금전적 손실**을 초래

예

2013년

러시아 국적의 해커 예브게니 미하일로비치 보가체프가 개발한 크립토락커가 유행했고, 다수의 변종 확산

2017년

워너크라이는 웜과 유사한 방식, 즉 운영체제 취약점을 통해 전 세계적으로 급격히 확산되며 대규모 피해 초래

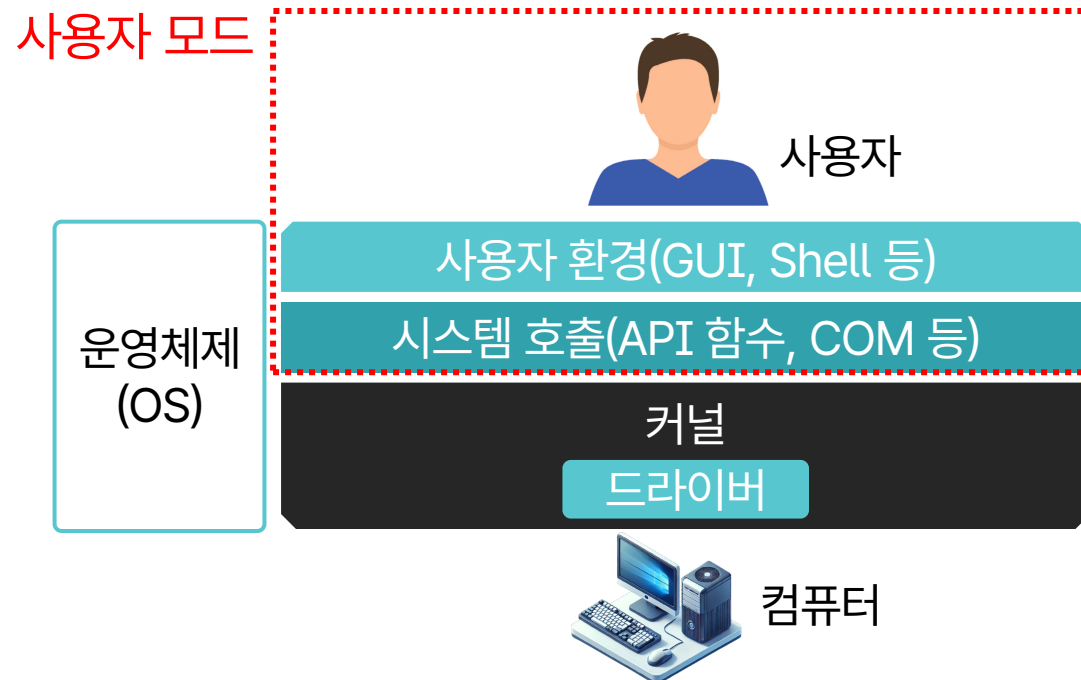
2021년

미국 동부 석유의 절반 이상을 공급하는 송유관 회사인 콜로니얼 파이프라인이 랜섬웨어에 감염되어 석유 부족, 유가 폭등 등 초래

## 악성코드

### 루트킷 (Rootkit)

- 대부분의 악성코드는 사용자 모드에서 동작하므로 **안티 바이러스에 의한 탐지가 용이**





## 악성코드

### 루트킷 (Rootkit)

- 루트킷은 커널 모드에서 동작하므로 **컴퓨터의 모든 권한을 장악**하여  
안티 바이러스에 의한 탐지를 회피하며 치명적인 영향을 초래할 가능성
  - 다만, **고도의 기술이 요구**되기 때문에 해커 입장에서 루트킷 개발은 다소 난이도가 높음



A dark blue world map is visible in the background, centered on the Atlantic Ocean. Overlaid on the map is a large cyan circle containing the Roman numeral 'II'. Below the circle, the title '안티 바이러스의 이해' is written in white Korean text. At the bottom, a thin white horizontal line with dots at each end spans the width of the slide.

II

# 안티 바이러스의 이해

## 1 안티 바이러스 (Anti-Virus, A/V)

### 안티 바이러스

컴퓨터 바이러스와 악성코드를 탐지하고 방어하는 호스트 기반 정보보호시스템

### 안티 바이러스

국가 · 공공에서 사용하는 공식 용어

### 백신(Vaccine)

우리나라에서 대중적으로 사용되는 용어

- 백신(Vaccine)이라는 용어가 널리 사용되는 이유는?

안철수에 의해 우리나라에서 최초  
개발된 안티 바이러스의 제품명

시간이 지나면서 보통명사화 됨



## 안티 바이러스 (Anti-Virus, A/V)

### 전통적인 안티 바이러스

알려진 바이러스/악성코드가 갖고 있는  
고유한 패턴(문자열, 식별자, 해시 값 등)을  
비교해가며 컴퓨터 내 **동일한 패턴의 존재 여부를  
확인**하는 방식으로 진단 및 치료

### 현대의 안티 바이러스

알려지지 않은 바이러스/악성코드에 능동적으로  
대응하기 위해 **휴리스틱 기반 탐지, 루트킷 탐지,  
실시간 감시** 등의 기능을 포함

## 1

## 안티 바이러스 (Anti-Virus, A/V)

## ■ 설치 위치

- 안티 바이러스의 핵심 기능은 커널 모드에서 동작하며, 사용자가 조작 가능한 사용자 환경(UI)은 사용자 모드에서 제공



## 1

## 안티 바이러스 (Anti-Virus, A/V)

### 설치 위치

#### 커널 모드

#### 사용자 모드

- **드라이버 설치**
- 바이러스/악성코드를 원활하게 진단 및 치료하기 위해 안티 바이러스로 하여금 **운영체제에 준하는 수준의 강력한 권한**을 부여해야 하기 때문
  - 루트킷 등 커널 모드에서 실행되는 바이러스/악성코드 탐지
- 특정 바이러스/악성코드는 안티 바이러스를 강제로 종료하고 무력화하려는 기능이 있음
  - 안티 바이러스 스스로 자가 보호를 하기 위한 우선권을 선점하기 위해 커널 모드에서 동작해야 할 필요성이 있음

1

## 안티 바이러스 (Anti-Virus, A/V)

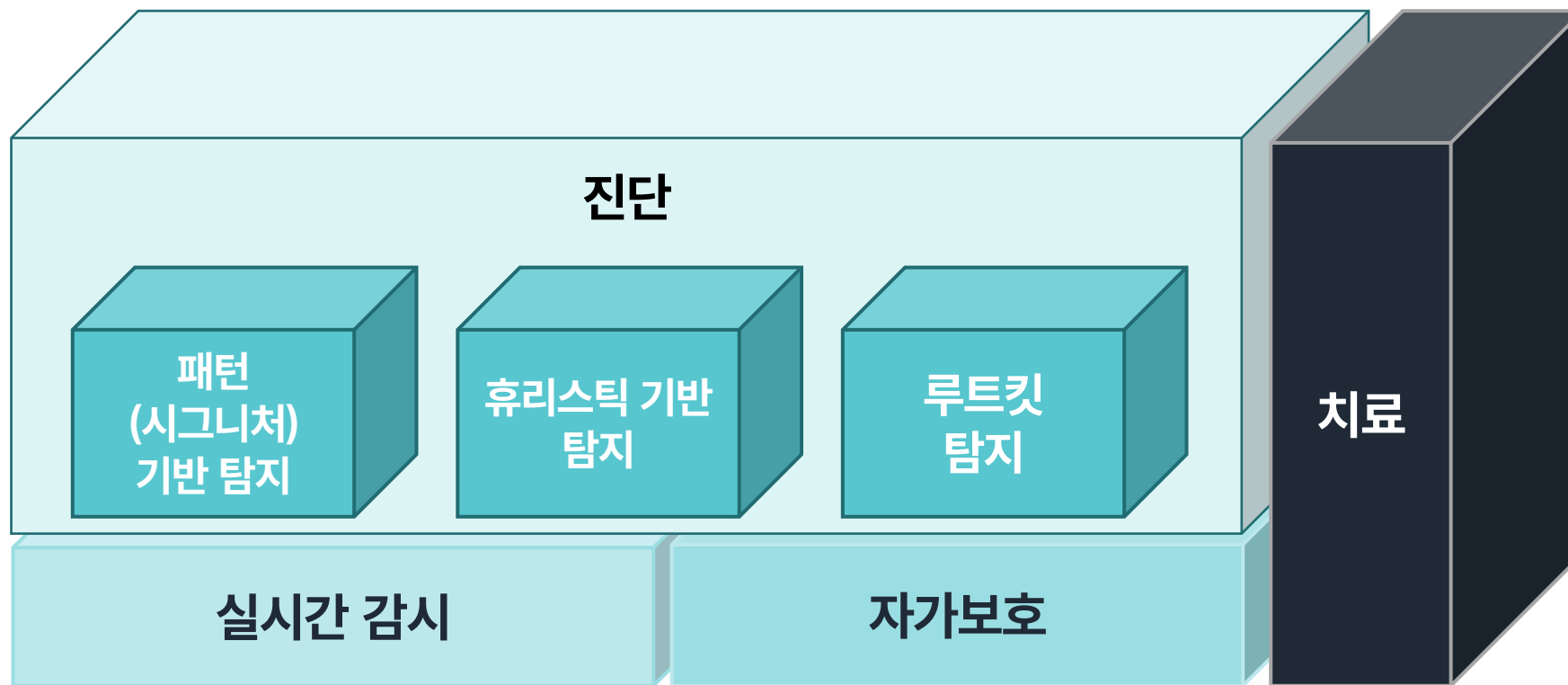
### 설치 위치

**커널 모드****사용자 모드**

- **실행 프로그램 및 서비스 설치**
- 안티 바이러스의 기능을 조작하거나 각종 환경설정을 손쉽게 변경할 수 있는 **사용자 환경(UI) 제공**
- 과거에는 실행 프로그램도 커널 모드에서 실행되도록 했으나 바이러스/악성코드가 이를 악용하는 사례가 빈번해지면서 **사용자 모드로 분리**
  - 안티 바이러스가 바이러스/악성코드의 공격 통로로 악용되는 취약성
  - 커널 모드에서 동작되어 운영체제에 중대한 영향을 미칠 수 있는 조작 또는 설정 값 변경은 권한 상승을 요구하도록 동작

## 1 안티 바이러스 (Anti-Virus, A/V)

### ■ 주요 기능





## 1

## 안티 바이러스 (Anti-Virus, A/V)

### 진단 기능

- 패턴(시그니처) 기반 탐지
  - 알려진 바이러스/악성코드가 갖고 있는 **고유한 패턴**을 시그니처 데이터베이스에 등록

#### 문자열

바이러스/악성코드로 **의심할 만한** 파일 내부의 특정 문자열

#### 식별자

바이러스/악성코드를 **특정할 수 있는** 파일 내부의 고유값 또는 문자열

#### 파일 해시 값

파일 그 자체를 일정한 길이의 **고유한 문자열로 변환한 것**

- 시그니처 데이터베이스에 등록된 패턴과 컴퓨터 내 **동일한 패턴의 존재 여부를 비교**하며 확인
  - \* **파일의 맨 앞 또는 맨 뒤의 일정 부분 만을 검사**하여 문자열 또는 식별자를 찾는 방식
  - \* **파일 내용 전체를 검사**하여 문자열 또는 식별자를 찾는 방식
  - \* **파일 자체의 해시 값을 대조**하여 일치 여부를 검사하는 방식

## 1 안티 바이러스 (Anti-Virus, A/V)

### ■ 진단 기능

- 휴리스틱 기반 탐지

패턴(시그니처) 기반  
탐지의 한계

알려진 바이러스/악성코드의 변종이나  
알려지지 않은 바이러스/악성코드를 탐지하지 못함

- 휴리스틱 기반 탐지를 위해 대부분의 바이러스/악성코드가 가질 수 있는 파일의 구조를 규칙화

예

일반적인 컴퓨터 프로그램이 실행될 때 프로그램 코드가 시작되는 진입점(Entry Point)이 위치하는  
보편적인 위치가 있지만, 바이러스/악성코드는 특이한 위치(맨 마지막)에 진입점이 존재하는 경우가 다수

- 규칙화 된 휴리스틱 데이터베이스와 검사 대상 **파일의 구조를 비교**하며 확인

\* 정교하지 못한 규칙이나 검사 방식은 오탐/오진 발생률을 높일 수 있음

도입 초기

오탐/오진율이 **높았음**

현대

머신러닝 기술의 적용으로 오탐/오진율이 **낮아짐**

## 1

## 안티 바이러스 (Anti-Virus, A/V)

### ■ 진단 기능

- 루트킷 탐지

- 대부분의 악성코드는 사용자 모드에서 동작하므로 안티 바이러스에 의한 탐지가 용이하여 공격자는 커널 모드에서 동작하는 루트킷을 제작하여 탐지 회피 시도

#### 루트킷

컴퓨터의 모든 권한을 장악하여 안티 바이러스에 의한 탐지를 회피하며 치명적인 영향을 초래할 가능성

- 안티 바이러스 또한 커널 모드에서 동작하는 만큼, 운영체제의 커널에서 불러온 드라이버 목록이나 발생한 이벤트 목록을 분석하는 방식으로 루트킷의 진단 가능

#### 예

운영체제의 커널에서 불러온 드라이버 목록을 모두 나열하고 이 중 특이한 이름을 가졌거나 비정상적인 위치에서 불러온 드라이버를 식별

## 1 안티 바이러스 (Anti-Virus, A/V)

### ■ 실시간 감시 기능

#### 전통적인 안티 바이러스

사용자가 필요할 때마다 **컴퓨터 전체 영역** 또는 **사용자가 선택한 영역**에 대해 **검사 기능을 실행**하는 방법으로 진단

- 과거 멀티 태스킹을 지원하지 않는 운영체제에서는 **실시간 감시 기능을 구현하기에 제한**
- 멀티 태스킹을 지원하는 운영체제가 보편적으로 널리 사용되면서 실시간 감시 기능이 보편적인 기능으로 자리 잡게 됨
- 실시간 감시를 통해 운영체제에서 발생하는 모든 행위를 모니터링
  - 특정 파일을 실행하려고 할 때 해당 파일만을 검사
  - 예
    - 특정 파일을 인터넷에서 다운로드했을 때 해당 파일만을 검사
- 다만, 실시간 감시 기능은 운영체제 자원을 일정 부분 사용하여 컴퓨터 성능이 저하될 가능성

## 1 안티 바이러스 (Anti-Virus, A/V)

### ■ 자가 보호 기능

- 특정 바이러스/악성코드는 안티 바이러스에 의한 탐지와 치료를 회피하기 위해 안티 바이러스를 강제로 종료하거나 삭제하는 등 **무력화하려는 기능**을 포함
- 안티 바이러스의 실시간 감시 기능에 안티 바이러스 스스로를 보호하는 자가 보호 기능을 같이 포함하는 경향

#### 강제종료 방지

실시간 감시와 치료를 수행하는 프로세스의 강제종료를 방지

#### 삭제 방지

안티 바이러스의 정상적인 동작을 위해 필요한 파일의 삭제 방지

## 안티 바이러스 (Anti-Virus, A/V)

### ■ 치료 기능

- 진단한 결과를 토대로 컴퓨터를 **감염 이전으로 복구**하는 기능
  - 바이러스/악성코드의 원인 파일을 제거
  - 바이러스에 감염되어 손상된 파일들을 원래 상태로 복구

**예** ➤ 바이러스 감염으로 인해 파일 맨 뒤에 특정 문자열이 삽입된 경우 해당 문자열만을 제거

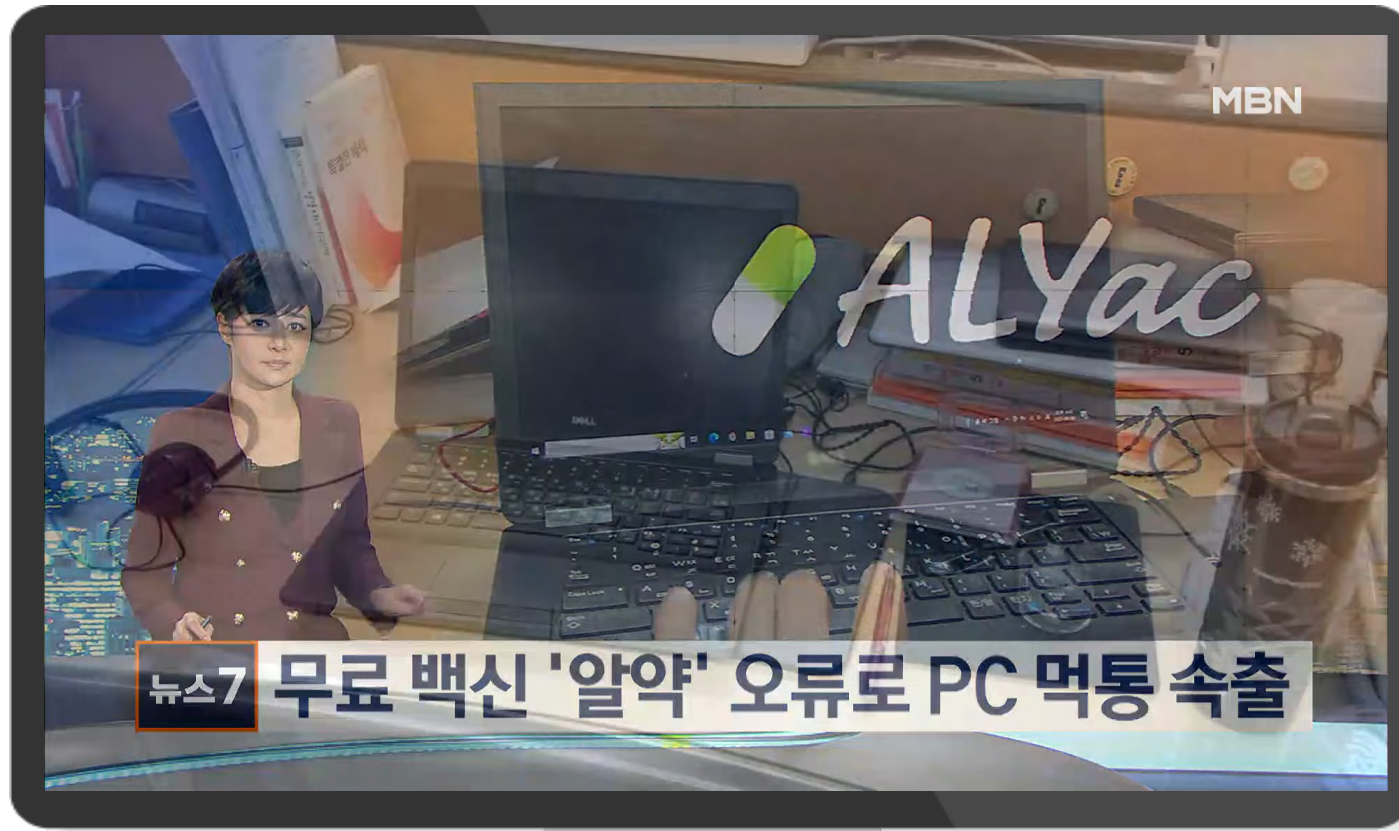
- 바이러스/악성코드로 인해 생성된 부산물을 제거

**예** ➤ 악성코드가 실행되면서 시작 프로그램에 동의 없이 등록되었던 서비스를 제거

**예** ➤ 악성코드가 실행되면서 레지스트리에 등록되었던 값을 제거

## 1 안티 바이러스 (Anti-Virus, A/V)

### ■ 치료 기능



출처 무료 백신 '알약' 오류로 PC 먹통 속출..."정상화 노력 중", MBN 뉴스(2022.08.30), <https://www.youtube.com/watch?v=KYOciflFkpY>

## 1 안티 바이러스 (Anti-Virus, A/V)

### ■ 치료 기능

#### 안티 바이러스의 치료 기능 오작동 사례

운영체제의  
정상 프로그램을  
랜섬웨어로 오탐/오진



컴퓨터가 대규모로  
먹통이 되어 버리는  
피해가 발생



## 안티 바이러스 (Anti-Virus, A/V)

### ■ 치료 기능

- 치료 기능이 잘못 동작하는 경우 컴퓨터가 망가질 수 있음
  - 제대로 치료(제거/복구)되지 **않아** 바이러스/악성코드가 잔존한 경우
  - 잘못된 치료(파일의 맨 뒤를 제거해야 하는데 맨 앞을 제거해버린 경우)로 인해 정상적인 파일이 훼손되는 경우
  - 치료 이전에 **오탐/오진**으로 인해 정상적인 파일이 훼손되거나 제거되는 경우

A dark blue world map is visible in the background, centered on the Atlantic Ocean. Overlaid on the map is a large, light blue circle containing the Roman numeral 'III'.

# III

## 바이러스/악성코드의 탐지 원리

---

## 1 바이러스/악성코드 감염 여부 확인 방법

### ■ 컴퓨터 내 파일 확인



알려진 악성코드가 갖고 있는  
**고유한 패턴(문자열, 식별자, 해시 값 등)을 비교**해가며  
컴퓨터 내 동일한 패턴을 갖는 파일의 존재 여부 확인

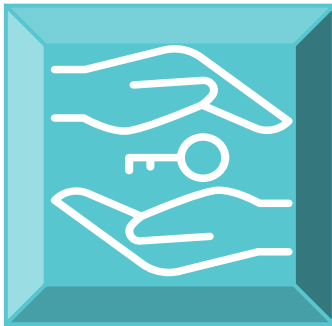


바이러스에 감염된 파일은 **원래의 파일에 변형이 발생된 것이므로**  
**이를 추적·검사하는 방식**으로 감염 사실 확인

1

## 바이러스/악성코드 감염 여부 확인 방법

- 운영체제 내 설정값 확인



운영체제의 특정 **설정 파일**이나 **설정 값**을 변형하는 경우가 있으므로 이를 확인



Windows 운영체제의 경우 **레지스트리**, **시작 프로그램**, **서비스 목록**에 특정 값을 생성하는 경우가 있으므로 이를 확인

## 1

## 바이러스/악성코드 감염 여부 확인 방법

### ■ 운영체제의 네트워크 상태 확인

- 컴퓨터는 외부와의 통신이 필요한 경우가 발생하면 **네트워크 포트를 개방**

예 ▶ 웹 서비스(80, 443), 파일 전송(20, 21), 메일 전송(25) 등

- 특정 악성코드는 알려진 포트 이외 자신을 특정할 수 있는 번호의 포트 번호를 사용하는 경향이 있어, 이러한 **포트 번호가 개방된 경우 악성코드 감염**을 의심

예 ▶ orion(1150), voodoo doll(1245), sub seven(1999), backorifice 2000(8787)

- 알려진 포트 번호라 하더라도 자의에 의해 **개방한 사실이 없는 포트 번호라면 악성코드 감염**을 의심

예 ▶ 웹 서비스(80)를 개방한 적이 없음에도 80번 포트가 개방되어 있는 경우

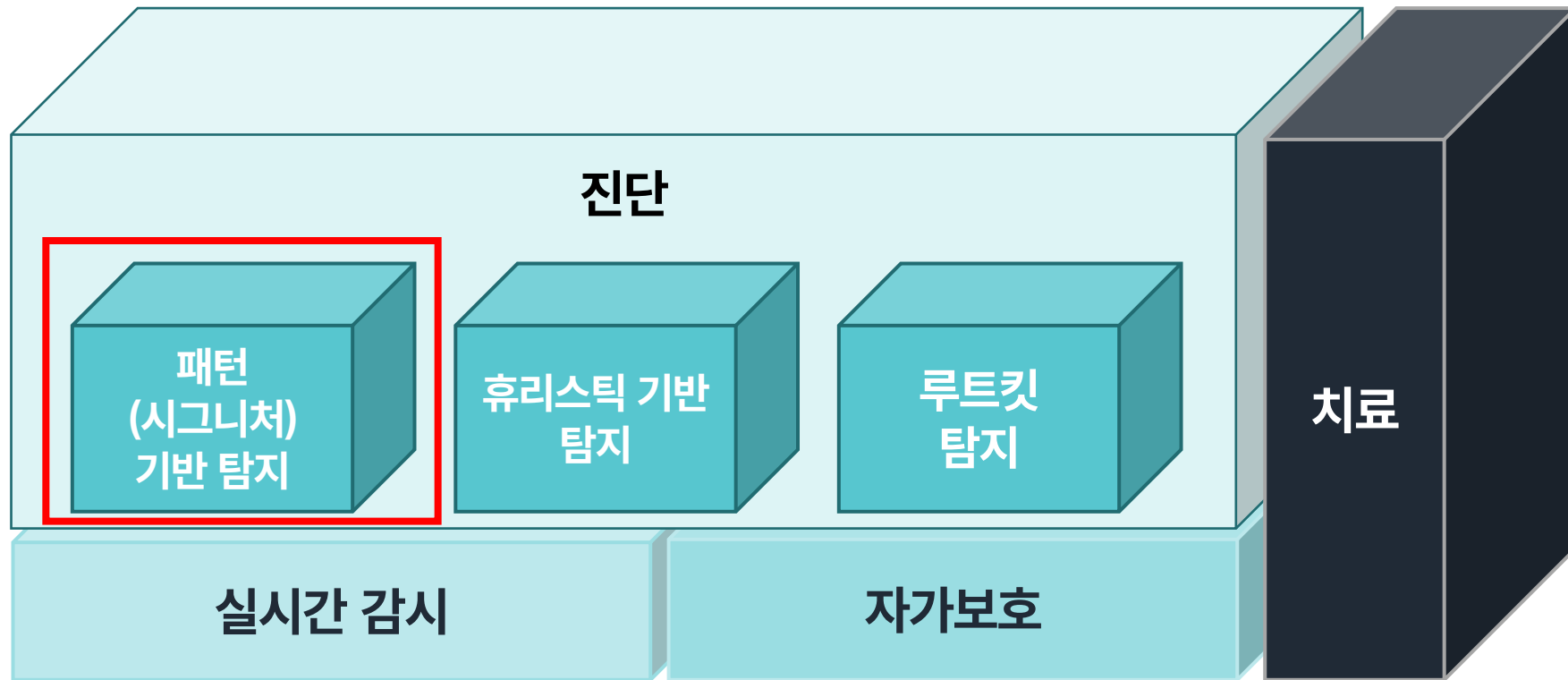
## 1

## 바이러스/악성코드 감염 여부 확인 방법

### ■ 운영체제의 실행 프로세스 확인

- 컴퓨터 프로그램이 실행되면 **운영체제에 해당 프로그램에 대한 프로세스를 생성**
  - 운영체제에서 자원 관리 등을 목적으로 생성하는 운영체제 기본 프로세스
  - 사용자가 설치·실행한 응용 소프트웨어가 생성하는 프로세스
- 악성코드도 **컴퓨터 프로그램이므로 프로세스를 생성**
  - 운영체제 기본 프로세스도 아니고 사용자가 설치·실행한 응용 소프트웨어의 프로세스가 아닌 경우 악성코드 프로세스를 의심
  - 운영체제 기본 프로세스와 혼동을 야기하기 위해 유사한 명칭의 프로세스 이름을 사용하는 경우도 존재
    - 예 csrss(정상 프로세스) – cssrs(악성코드 프로세스)
    - 예 svchost(정상 프로세스) – svhost(악성코드 프로세스)

## 패턴(시그니처) 기반 탐지 원리



## 패턴(시그니처) 기반 탐지 원리

### ■ EICAR 표준 안티 바이러스 테스트 파일

- EICAR에서 테스트 목적으로 고안한 **가짜 바이러스/악성코드**

**EICAR**(European Institute for Computer Antivirus Research)

컴퓨터 **안티 바이러스**를 연구하기 위해 유럽에서 설립된 **학술 조직**

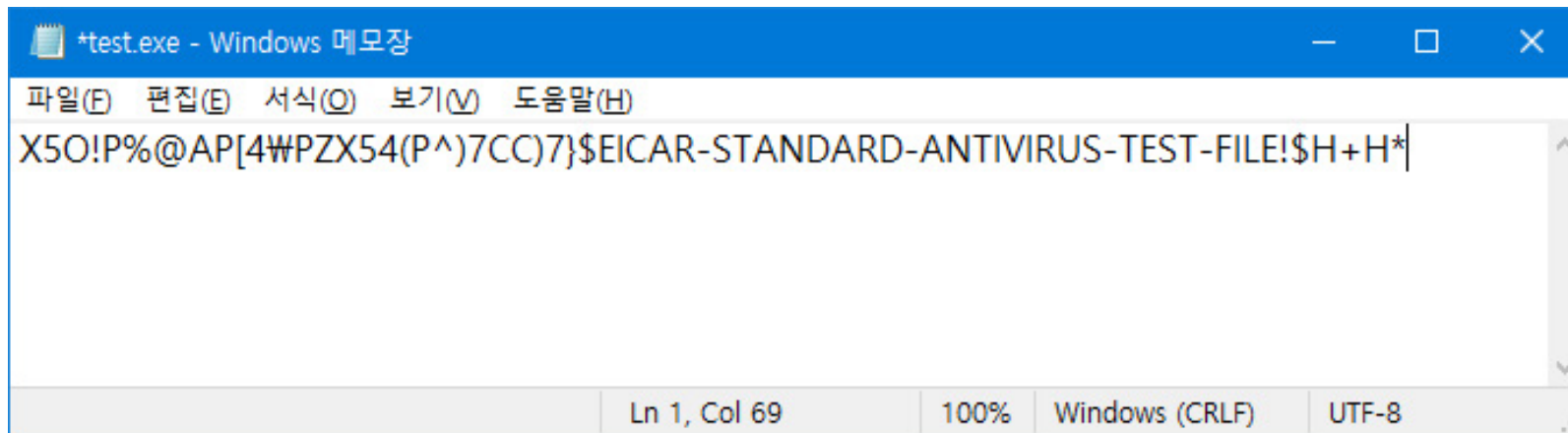
- 안티 바이러스 개발자는 EICAR 표준 안티 바이러스 테스트 파일을 활용하여, 개발하는 안티 바이러스의 효용성을 검증
  - 개발된 안티 바이러스의 효용성을 검증하기 위해 실제 바이러스/악성코드를 사용할 수도 있겠으나, 테스트 과정에서 감염될 가능성이 다분하여 위험하기 때문
- 대부분의 상용 안티 바이러스 제품은 **EICAR 표준 안티 바이러스 테스트 파일**을 바이러스/악성코드로 진단



## 2 패턴(시그니처) 기반 탐지 원리

- EICAR 표준 안티 바이러스 테스트 파일

`X5O!P%@AP[4\WZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`

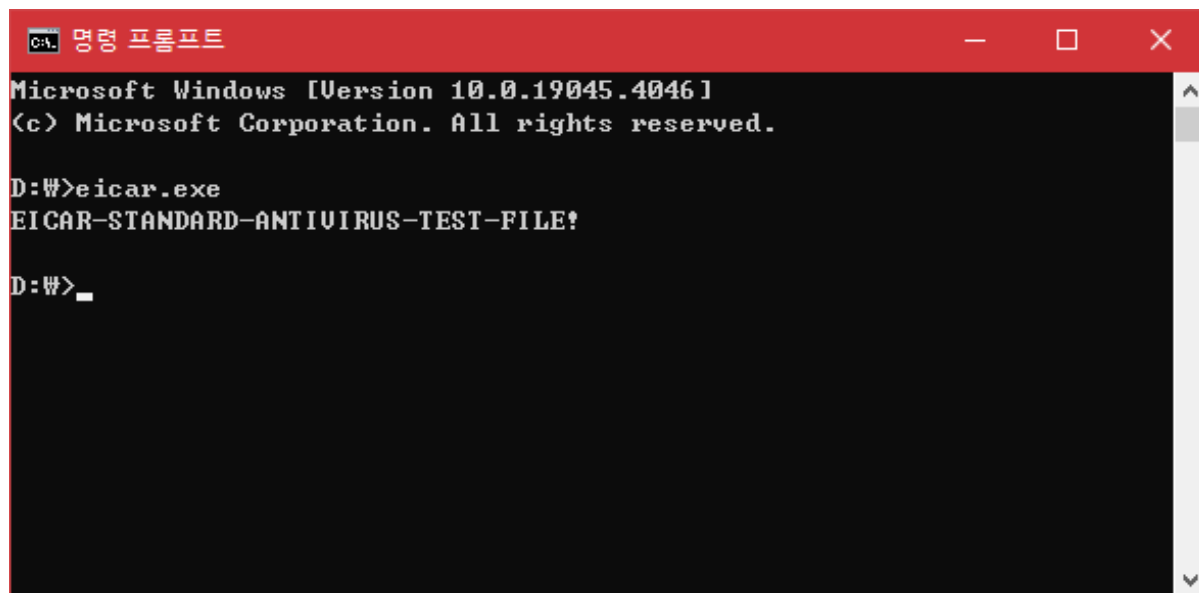


**EICAR Test File의 내용을 메모장에 붙여넣고 EXE 파일로 저장**

## 2

## 패턴(시그니처) 기반 탐지 원리

### ■ EICAR 표준 안티 바이러스 테스트 파일

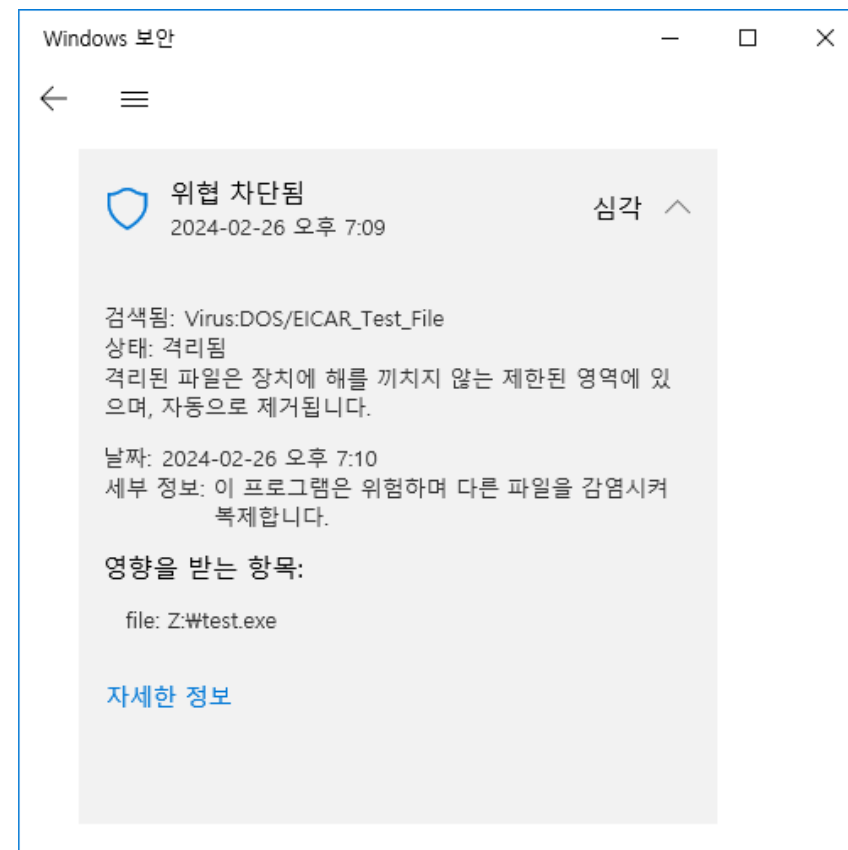


```
명령 프롬프트
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

D:\>eicar.exe
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

D:\>
```

EXE 파일로 저장한 EICAR Test File을 실행



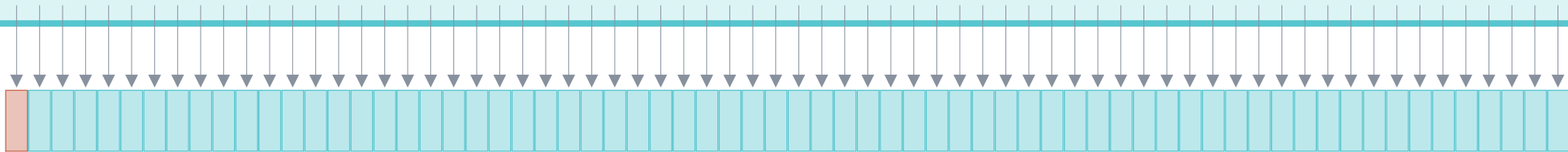
EICAR Test File의 안티 바이러스 탐지 결과

## 패턴(시그니처) 기반 탐지 원리

## ■ 고정길이 검사

- 파일의 맨 앞 또는 맨 뒤의 일정 부분 만을 검사하여 문자열 또는 식별자를 찾는 방식

x5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*



1 byte

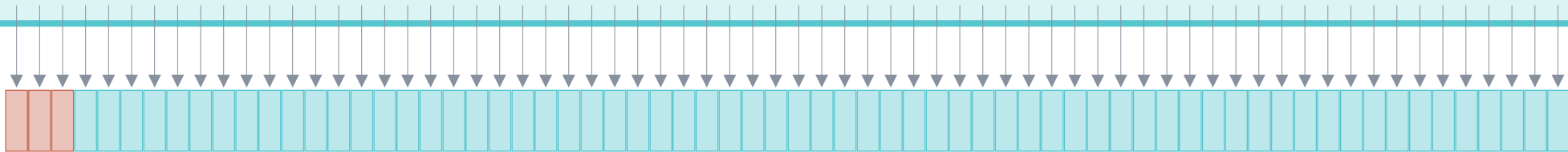
## 2

## 패턴(시그니처) 기반 탐지 원리

## ■ 고정길이 검사

- 파일의 맨 앞 또는 맨 뒤의 일정 부분 만을 검사하여 문자열 또는 식별자를 찾는 방식

**x50!** P%@AP [ 4 \ PZX54 ( P ^ ) 7CC ) 7 } \$EICAR-STANDARD-ANTIVIRUS-TEST-FILE! \$H+H\*



**3 bytes**

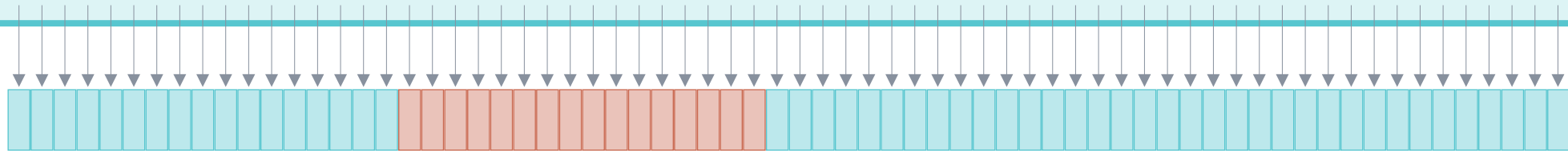
- 검사 범위가 증가할수록 오탐/오진 확률이 낮아지지만, 검사 속도 또한 저하될 수 있음  
(권장 범위 : 5~10 bytes)

## 패턴(시그니처) 기반 탐지 원리

## 가변길이 검사

- 파일 내용 전체를 검사하여 문자열 또는 식별자를 찾는 방식

X5O!P%@AP[4\ZX54 (P^ ) 7CC) 7} \$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*



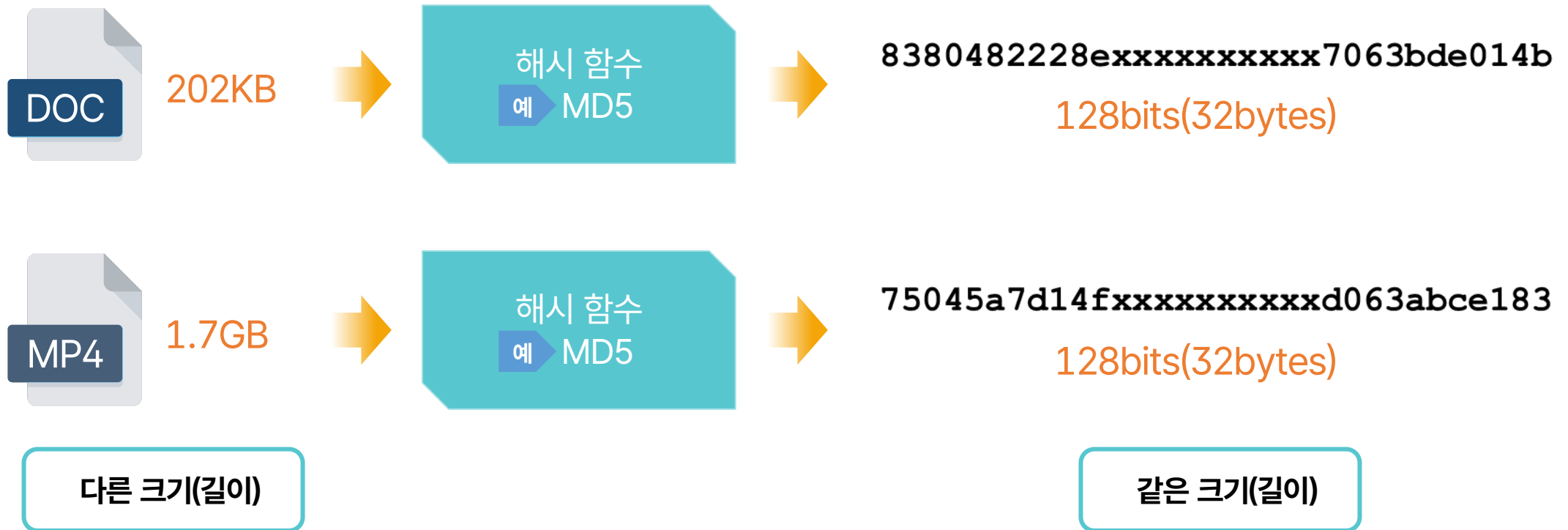
(P^ ) 7CC) 7} \$EICAR

- 파일 내용 전체를 검사하기 때문에 파일의 크기가 클수록 검사해야 할 범위가 증가하여 검사 속도가 저하될 수 있음

## 2 패턴(시그니처) 기반 탐지 원리

## ■ 해시값 검사

- 파일 자체의 해시 값을 대조하여 일치 여부를 검사하는 방식



## 2 패턴(시그니처) 기반 탐지 원리

## ■ 해시값 검사

- 파일 자체의 해시 값을 대조하여 일치 여부를 검사하는 방식



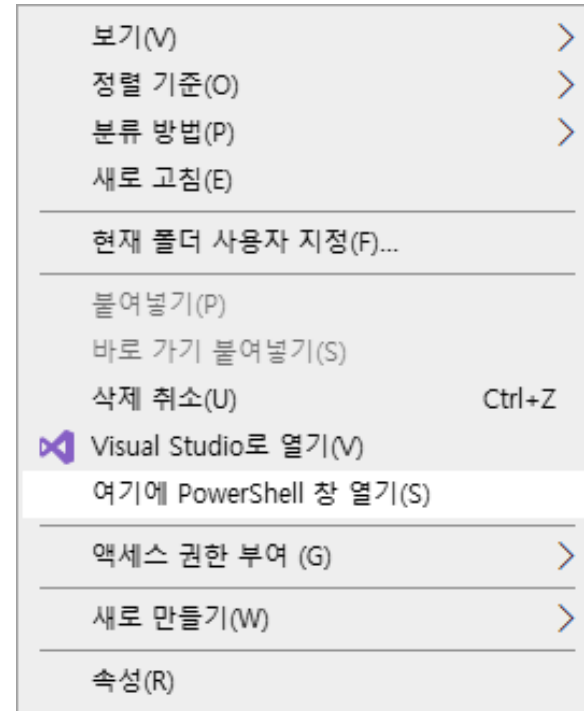
- 검사 대상 파일들의 해시 값 만을 비교하기 때문에 검사 속도가 빠름
- 컴퓨터 내 파일 해시 값들을 미리 색인하여 목록화 해두어야 효과성이 있고 파일들이 변경될 때마다 목록화해 둔 해시 값 정보도 변경 해두어야 함

## 3

## 패턴(시그니처) 기반 탐지 실습 도구 안내

## ■ antivirus.ps1

- 패턴(시그니처) 기반 탐지 원리를 실습할 수 있도록 자체 제작한 도구
- 실행 방법
  - ① [Shift] 키를 누른 상태에서 마우스 우측 버튼 클릭
  - ② 메뉴에서 [여기에 PowerShell 창 열기] 항목 선택
  - ③ 다음 명령어를 순차적으로 입력



```
$OutputEncoding = [Console]::OutputEncoding
TYPE .\antivirus.ps1 | PowerShell -noprofile -
```



4

## 패턴(시그니처) 기반 탐지 실습

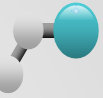
- antivirus.ps1





## 요약 정리

- 지금까지 학습한 내용을 정리해보겠습니다.



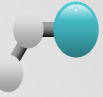
## ■ 바이러스와 악성코드

### • 컴퓨터 바이러스 (Computer Virus)

- 컴퓨터 내 다른 프로그램이나 기억장치에 자기 자신 또는 자기 자신의 변형을 복제 · 삽입해가며 감염(확산)시키는 컴퓨터 프로그램
- 바이러스의 세대 구분 : 1세대(원시형), 2세대(암호형), 3세대(은폐형), 4세대(다형성), 5세대(매크로)

### • 악성코드(Malware)

- 종래의 컴퓨터 바이러스의 개념을 포함하며, 악의적 목적을 가진 모든 종류의 실행 가능한 컴퓨터 프로그램
- 컴퓨터의 사양이 높아지고 정보통신망 환경이 보편화되면서 전통적인 바이러스의 특성을 갖지 않으면서도 악성 기능을 수행하는 컴퓨터 프로그램 등장
- 악성코드의 종류 : 바이러스(Virus), 웜(Worm), 트로이목마(Trojan Horse), 스파이웨어(Spyware), 애드웨어(Adware), 랜섬웨어(Ransomware), 루트킷(Rootkit)
  - \* 루트킷(Rootkit) : 운영체제의 커널 모드에서 동작되도록 개발 · 설계된 악성코드



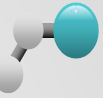
## ■ 안티 바이러스의 이해

### • 안티 바이러스 (Anti-Virus, A/V)

- 컴퓨터 바이러스와 악성코드를 탐지하고 방어하는 호스트 기반 정보보호시스템

### • 안티 바이러스의 주요 기능

- 진단 기능
  - \* **패턴(시그니처) 기반 탐지** : 알려진 바이러스/악성코드가 갖고 있는 고유한 패턴을 시그니처 데이터베이스에 등록하고, 시그니처 데이터베이스에 등록된 패턴과 컴퓨터 내 동일한 패턴의 존재 여부를 비교하며 확인
  - \* **휴리스틱 기반 탐지** : 대부분의 바이러스/악성코드가 가질 수 있는 파일의 구조를 규칙화하고, 규칙화 된 휴리스틱 데이터베이스와 검사 대상 파일의 구조를 비교하며 확인
  - \* **루트킷 탐지** : 운영체제의 커널에서 불러온 드라이버 목록이나 발생한 이벤트 목록을 분석하는 방식으로 확인
- 실시간 감시 기능 : 운영체제에서 발생하는 모든 행위를 모니터링하는 기능
- 자가 보호 기능 : 안티 바이러스의 강제종료 또는 삭제 등 무력화를 방지하는 기능
- 치료 기능 : 진단한 결과를 토대로 컴퓨터를 감염 이전으로 복구하는 기능



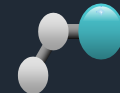
## ■ 바이러스/악성코드의 탐지 원리

### • EICAR 표준 안티 바이러스 테스트 파일

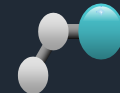
- EICAR에서 테스트 목적으로 고안한 가짜 바이러스/악성코드로, 안티 바이러스 개발자는 안티 바이러스를 개발하는 과정에서 효용성을 검증하기 위해 EICAR 표준 안티 바이러스 테스트 파일을 활용

### • 패턴(시그니처) 기반 탐지 원리

- 고정길이 검사 : 파일의 맨 앞 또는 맨 뒤의 일정 부분 만을 검사하여 문자열 또는 식별자를 찾는 방식
  - \* 검사 범위가 증가할수록 오탐/오진 확률이 낮아지지만, 검사 속도 또한 저하될 수 있음.
- 가변길이 검사 : 파일 내용 전체를 검사하여 문자열 또는 식별자를 찾는 방식
  - \* 파일 내용 전체를 검사하기 때문에 파일의 크기가 클수록 검사해야 할 범위가 증가하여 검사 속도가 저하될 수 있음.
- 해시 값 검사 : 파일 자체의 해시 값을 대조하여 일치 여부를 검사하는 방식
  - \* 검사 대상 파일들의 해시 값 만을 비교하기 때문에 검사 속도가 빠르지만 컴퓨터 내 파일 해시 값들을 미리 색인하여 목록화 해두어야 효과성이 있고 파일들이 변경될 때마다 목록화 해 둔 해시 값 정보도 변경해두어야 함.



- ☞ 정보통신기반보호법 (법률)
- ☞ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (법률)
- ☞ 사이버안보 업무규정 (대통령령)
- ☞ 국가사이버안전관리규정 (대통령훈령)
- ☞ 국가 정보보안 기본지침 (국가정보원 지침)
- ☞ 보안관제학, 2014, 안성진 등 공저, 이한미디어
- ☞ 2023 국가정보보호백서, 2023, 국가정보원 등 관계기관 합동
- ☞ 국가사이버안보센터 웹 사이트, <http://www.ncsc.go.kr>
- ☞ 한국인터넷진흥원 웹 사이트, <http://www.kisa.or.kr>
- ☞ KISA 보호나라 & KrCERT/CC 웹 사이트, <http://www.krcert.or.kr>
- ☞ Common Criteria 웹 사이트, <http://commoncriteriaportal.org>



- IT보안인증사무국 웹 사이트, <http://itscc.kr>
- 무료 백신 '알약' 오류로 PC 먹통 속출..."정상화 노력중", MBN 뉴스, 2022.08.30, <https://www.youtube.com/watch?v=KYOciflFkpY>
- EICAR – Download Anti Malware Testfile, <https://www.eicar.org/download-anti-malware-testfile/>
- Test your antivirus with the EICAR test file, <https://www.trishtech.com/2010/10/test-your-antivirus-with-the-eicar-test-file/>