# 악성코드 탐지, 암호화 및 패키징 프로젝트

컴퓨터 바이러스에 대한 보고서



**목**

**차**

1. **컴퓨터 바이러스의 정의**
2. **바이러스 유형**

**2.1 파일 바이러스**

**2.2 부트 바이러스**

**2.3 매크로 바이러스**

**2.4 스크립트 바이러스**

**2.5 암호화 바이러스**

1. **바이러스 전파 방식**

**3.1 이메일 및 메신저 전파**

**3.2 웹사이트 방문으로 인한 감염**

**3.3 이동식 저장 매체를 통한 전파**

**3.4 네트워크 취약점 이용**

1. **바이러스 피해 사례**
2. **바이러스 예방 및 대응**
3. **참고문헌**

## Ⅰ. 바이러스의 정의

컴퓨터 바이러스는 다른 정상 프로그램 코드에 자신을 삽입하여 그 프로그램이 실행될 때 함께 실행되면서 스스로를 복제하고 확산하는 악성코드입니다. 웜과 달리 바이러스는 자체적으로 실행되지 않고 숙주 프로그램에 기생하는 형태로 존재합니다. 트로이 목마 역시 독립적인 프로그램이지만 자기 복제 기능이 없어 사용자의 행동에 의해 실행되는 점이 바이러스와 다릅니다.

컴퓨터 바이러스의 역사는 1971년 개발된 크리퍼 바이러스로부터 시작됩니다. 크리퍼는 실험적인 자기 복제 프로그램으로 아파넷을 통해 전파되며 메시지를 출력했습니다. 이후 1986년 파키스탄에서 유행한 브레인 바이러스가 최초의 본격적인 바이러스로 알려졌습니다. 이들 초기 바이러스는 단순한 시스템 파괴 행위에 그쳤지만, 점차 PC를 인질로 잡고 금전적 이득을 노리는 랜섬웨어 등 교활한 형태로 진화했습니다.

1980년대 이후 파일 바이러스, 부트 바이러스, 매크로 바이러스, 스크립트 바이러스, 암호화 바이러스 등 다양한 유형의 바이러스가 지속적으로 등장했습니다. 이들 바이러스는 코드 암호화, 자기 복제 등의 기술을 활용해 점점 더 교활해졌습니다. 2000년에는 러브레터 바이러스가 전 세계적으로 수십억 달러의 경제적 손실을 야기하는 등 바이러스의 위협은 고조되었습니다. 컴퓨터와 네트워크의 보편화에 따라 바이러스는 개인과 기업, 나아가 국가 기반 시설과 산업 전반에 심각한 피해를 입히는 주요 위험 요인이 되었습니다.

## Ⅱ. 바이러스의 유형

## 2.1 파일 바이러스

파일 바이러스는 실행 파일이나 문서 파일과 같은 정상 프로그램에 자신의 코드를 삽입하여 감염시키는 바이러스 유형입니다. 따라서 파일 바이러스는 숙주 프로그램에 기생하는 특성을 가지며, 이는 부트 바이러스와는 구분되는 주요 차이점입니다. 파일 바이러스는 감염된 파일이 실행되면 함께 실행되어 자신을 복제하고 다른 파일로 전파되는 방식으로 작동합니다.

파일 바이러스는 주로 실행 가능한 파일(.exe, .com 등)에 감염하지만, 매크로 바이러스처럼 문서 파일(.doc, .xls 등)에도 침투할 수 있습니다. 감염 과정에서 바이러스 코드는 파일 본문의 여유 공간에 삽입되거나 파일 헤더를 변조하는 등의 방식으로 숙주 프로그램을 변형시킵니다. 이후 사용자가 해당 파일을 열거나 실행할 때 바이러스 코드도 함께 실행되면서 다른 파일을 감염시키게 됩니다. 일부 파일 바이러스는 파일 시스템이나 운영 체제에 심각한 손상을 입히기도 합니다.

파일 바이러스는 주로 이동식 저장 매체, 네트워크 공유 폴더, 전자 메일 등을 통해 확산됩니다. 특히 USB 메모리나 외장 하드디스크와 같은 이동식 저장 매체는 바이러스 전파에 취약한 경로로 알려져 있습니다. 2008년 발견된 제나 바이러스는 USB를 통해 전파되어 전 세계 수십만 대의 컴퓨터를 감염시킨 바 있습니다.

파일 바이러스에 효과적으로 대응하기 위해서는 정기적인 백신 업데이트와 보안 패치 설치가 중요합니다. 또한 출처가 불분명한 파일은 실행하지 않는 주의가 필요하며, 중요 데이터의 백업을 주기적으로 수행해야 합니다. 이동식 저장 매체 사용 시에도 주의를 기울여야 하며, 가급적 바이러스 백신을 통해 검사를 하는 것이 안전합니다.

**2.2 부트 바이러스**

부트 바이러스는 컴퓨터의 부팅 과정을 감염시켜 시스템을 손상시키는 바이러스 유형입니다. 이 바이러스는 부트 섹터나 마스터 부트 레코드(MBR) 등 컴퓨터 부팅에 핵심적인 영역에 자신의 코드를 삽입합니다. 그 결과, 컴퓨터가 시동될 때마다 바이러스 코드가 메모리에 로드되어 실행되게 됩니다.

부트 바이러스는 숙주 프로그램에 감염되는 파일 바이러스와는 달리 시스템 자체를 직접 공격합니다. 이들 바이러스는 부팅 과정을 방해하거나 파일 시스템을 손상시켜 컴퓨터를 사용할 수 없게 만들 수 있습니다. 또한 부트 레코드 영역 감염으로 인해 운영 체제 및 주요 프로그램이 제대로 작동하지 않을 수 있습니다.

최초의 본격적인 부트 바이러스로 알려진 브레인은 1986년 파키스탄의 파루크 알비 형제에 의해 개발되었습니다. 이 바이러스는 플로피 디스크의 부트 섹터를 감염시켜 전파되었으며, 일정 횟수 부팅 시 시스템을 멈추게 하는 기능이 있었습니다. 당시 신기술이었던 플로피 디스크의 광범위한 사용으로 인해 브레인 바이러스는 전 세계로 빠르게 확산되었습니다.

부트 바이러스는 주로 USB 드라이브, 외장 하드디스크, CD/DVD와 같은 이동식 저장 매체를 통해 전파됩니다. 감염된 매체를 사용하여 부팅하면 바이러스가 시스템에 침투할 수 있습니다. 또한 네트워크 공유 폴더에 있는 부팅 가능한 파일이나 이미지를 통해서도 바이러스가 전파될 수 있습니다.

부트 바이러스에 대한 대응 방안으로는 출처가 불분명한 이동식 저장 매체의 사용을 자제하고, 정기적인 바이러스 백신 업데이트를 통해 최신 바이러스 정보를 유지하는 것이 중요합니다. 또한 부팅 디스크를 이용하여 시스템을 안전하게 부팅한 후 바이러스 검사 및 치료를 수행해야 합니다.

**2.3 매크로 바이러스**

매크로 바이러스는 워드프로세서나 스프레드시트 프로그램에 내장된 매크로 기능을 악용하는 바이러스 유형입니다. 매크로는 반복적인 작업을 자동화하기 위한 프로그래밍 언어로, 문서 파일이나 스프레드시트에 기록되어 있습니다. 매크로 바이러스는 이 매크로 코드에 자신을 삽입하여 문서나 스프레드시트 파일에 숨어 있다가 파일이 열리면 실행되는 방식으로 작동합니다.

일단 매크로 바이러스가 실행되면 자신의 복제본을 다른 파일에 삽입하여 전파됩니다. 이 과정에서 매크로 바이러스는 시스템 파일이나 부트 섹터 등 다른 영역을 감염시키기도 합니다. 감염된 문서나 스프레드시트 파일이 다른 사용자에게 전달되면 바이러스도 함께 확산되는 것입니다. 매크로 바이러스는 주로 이메일 첨부 파일, 공유 폴더, 이동식 저장 매체 등을 통해 전파됩니다. 과거 문서 공유가 활발했던 회사 내부 네트워크에서 대규모 확산 사례가 많았습니다.

1999년 발견된 멜리사 바이러스는 당시 마이크로소프트 워드 문서를 통해 급속히 퍼져 나가 전 세계적으로 80억 달러 이상의 피해를 입혔습니다. 이 바이러스는 워드 문서에 숨어 있다가 문서를 열면 실행되어 자신의 복제본을 다른 문서에 퍼뜨리고, 아웃룩 주소록에서 수집한 이메일 주소로 자신을 전송하는 방식으로 작동했습니다. 이처럼 매크로 바이러스는 네트워크와 이메일을 활용하여 기하급수적으로 확산될 수 있습니다.

매크로 바이러스에 대응하기 위해서는 신뢰할 수 없는 문서나 스프레드시트 파일은 열지 않는 것이 중요합니다. 또한 정기적으로 바이러스 백신을 업데이트하고 매크로 기능의 차단을 고려해야 합니다. 마이크로소프트는 2003년 이후 매크로 바이러스 확산을 막기 위해 문서 파일에서 매크로 실행을 기본적으로 차단하는 등 대책을 마련했습니다. 사용자 역시 매크로 기능을 불필요한 경우 비활성화하고, 안전한 매크로만 신중히 실행하는 주의가 필요합니다.

**2.4 스크립트 바이러스**

스크립트 바이러스는 웹 페이지나 응용 프로그램에 사용되는 스크립트 언어를 악용하는 바이러스 유형입니다. 이들 바이러스는 자바스크립트, VBScript, PHP 등 다양한 스크립트 언어에 자신의 코드를 삽입하여 해당 스크립트가 실행될 때 함께 실행되는 방식으로 작동합니다.

스크립트 바이러스는 웹 브라우저나 프로그램이 스크립트를 실행할 때 침투할 수 있습니다. 예를 들어 악성 코드가 삽입된 자바스크립트가 웹 페이지에 포함되어 있다면, 사용자가 해당 페이지를 방문할 때 바이러스가 실행되어 시스템에 침투할 수 있습니다. 이처럼 스크립트 바이러스는 웹과 응용 프로그램 환경에서 빠르게 확산될 수 있는 특징이 있습니다.

대표적인 스크립트 바이러스 사례로 2000년에 발견된 루팅 바이러스가 있습니다. 이 바이러스는 VBScript 코드에 자신을 삽입하여 윈도우 운영 체제의 취약점을 공략했습니다. 감염된 시스템에서 열린 파일은 바이러스에 의해 암호화되었고, 복구를 위해서는 해커에게 금전을 지불해야 했습니다. 루팅 바이러스는 이메일과 네트워크 공유 폴더를 통해 빠르게 확산되어 전 세계적으로 피해를 입혔습니다.

또한 2008년에 발견된 굼벙크 바이러스는 자바스크립트에 자신을 심어 웹 페이지를 통해 전파되었습니다. 사용자가 감염된 웹 페이지를 열면 바이러스가 활성화되어 시스템 취약점을 공격하고 다른 웹 페이지로 전파되었습니다. 굼벙크 바이러스는 전 세계 수백만 대의 컴퓨터를 감염시켰으며, 특히 아시아 지역에서 큰 피해를 입혔습니다.

이처럼 스크립트 바이러스는 스크립트 언어의 취약점을 노리며, 웹과 응용 프로그램 환경에서 급속히 확산될 수 있습니다. 따라서 스크립트 언어 취약점에 대한 지속적인 보안 업데이트와 함께 출처가 불분명한 웹 페이지나 프로그램 실행에 주의를 기울여야 합니다. 또한 스크립트 바이러스 감염 시 백신 프로그램을 통한 제거와 시스템 복구 작업이 필요합니다.

**2.5 암호화 바이러스**

암호화 바이러스는 자신의 코드를 암호화하여 안티바이러스 프로그램의 탐지를 피하는 교활한 유형의 바이러스입니다. 이들은 암호화된 형태로 존재하기 때문에 기존 바이러스 패턴과 다르며, 계속해서 변형되어 새로운 형태로 나타납니다. 이처럼 암호화 바이러스는 '폴리모픽(polymorphic)' 또는 '메타모픽(metamorphic)' 기능을 갖추고 있어 탐지와 제거가 매우 어렵습니다.

암호화 바이러스의 작동 원리는 다음과 같습니다. 바이러스 코드는 암호화된 형태로 실행 파일에 포함되어 있습니다. 사용자가 해당 파일을 실행하면 암호화된 코드가 메모리에 로드되고, 바이러스 본체 코드를 복호화하는 루틴이 실행됩니다. 이 과정에서 복호화된 바이러스 코드가 메모리상에 로드되며, 이후 자기 복제와 전파, 데이터 파괴 등의 악성 행위를 수행하게 됩니다.

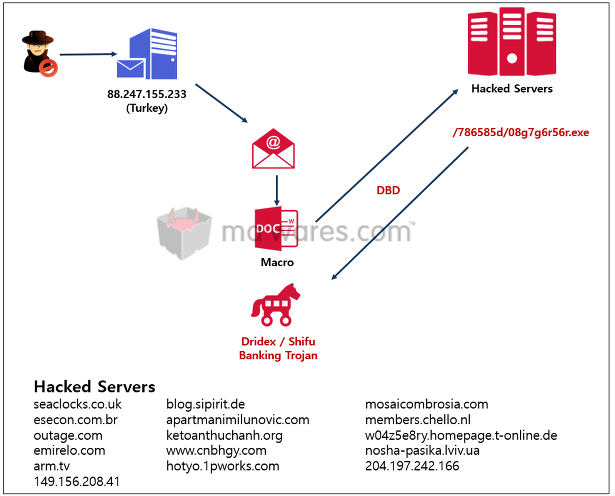
암호화 바이러스는 계속해서 변형되는 특성 때문에 탐지와 제거가 매우 어렵습니다. 백신 프로그램이 특정 암호화 바이러스를 식별하더라도, 바이러스 코드가 변형되면 기존 패턴과 다르기 때문에 더 이상 탐지할 수 없게 됩니다. 또한 바이러스 본체가 메모리에 로드된 이후에야 비로소 복호화되므로, 디스크상의 암호화된 코드만으로는 바이러스 여부를 판단하기 어렵습니다.

이러한 암호화 바이러스에 대응하기 위해서는 고도의 분석 기술과 최신 백신 정보가 필요합니다. 행위 기반 탐지, 휴리스틱 분석, 클라우드 기반 분석 등 다양한 기법이 동원되어야 합니다. 또한 사용자는 출처가 불분명한 프로그램 실행을 자제하고, 정기적으로 백신을 업데이트하는 등 주의가 필요합니다. 암호화 바이러스는 지속적으로 진화하고 있어 최신 보안 대책이 필수적입니다.

## Ⅲ. 바이러스 전파 방식

**3.1 이메일 및 메신저 전파**

바이러스는 이메일과 메신저 플랫폼을 통해 효과적으로 전파될 수 있습니다. 이메일과 메신저는 파일 첨부 및 링크 공유가 가능하기 때문에 바이러스가 숙주에 쉽게 침투할 수 있는 경로가 됩니다.

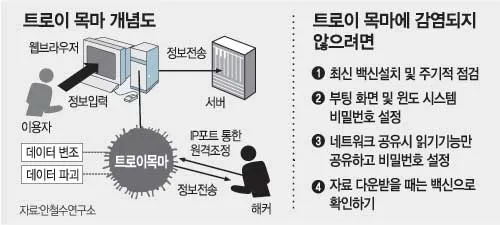


바이러스는 메일이나 메신저에서 실행 파일, 문서 파일 등의 형태로 첨부되어 전파됩니다. 또한 악성 링크를 메시지에 포함시켜 사용자를 가짜 사이트로 유인하고 시스템을 감염시키기도 합니다. 바이러스 메일은 제목이나 본문 내용이 의심스럽거나 발신자가 불분명한 경우가 많습니다. 피싱 메일처럼 긴급하거나 당혹스러운 내용으로 사용자를 기만하는 수법을 사용하기도 합니다.

**3.2 이동식 저장 매체를 통한 전파**

웹사이트 방문은 바이러스 감염의 주요 경로 중 하나입니다. 웹 페이지에 악성 코드가 숨겨져 있다면 사용자가 해당 페이지를 열람할 때 바이러스가 실행되어 시스템에 침투할 수 있습니다. 대표적인 기법으로 크로스 사이트 스크립팅(XSS) 공격이 있습니다. 공격자가 웹 페이지의 스크립트 코드에 악성 스크립트를 삽입하면, 사용자가 이 페이지에 접속할 때마다 바이러스 코드가 실행되는 원리입니다.

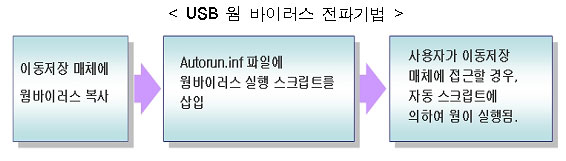
또한 웹 브라우저와 플러그인의 취약점을 노리는 공격도 발생합니다. 이를 '드라이브-바이 다운로드' 공격이라고 하며, 웹 페이지에 악성 코드가 숨겨져 있지 않더라도 브라우저나 플러그인의 보안 취약점을 이용하여 바이러스가 시스템에 침투할 수 있습니다. 최근에는 취약점 공격 코드가 포함된 '익스플로잇 킷'을 웹사이트에 삽입하는 사례도 있습니다. 2016년에는 구글 광고 네트워크를 통해 '말버타이징'이 유포되어 수많은 웹사이트 방문자가 감염된 바 있습니다.



**3.3 웹사이트 방문으로 인한 감염**

이동식 저장 매체는 바이러스 전파의 주요 경로입니다. USB 드라이브, 외장 하드디스크, CD/DVD 등의 이동식 저장 매체는 쉽게 다른 컴퓨터와 연결되어 데이터를 주고받을 수 있습니다. 그러나 이 과정에서 바이러스에 감염된 매체가 다른 시스템과 연결되면 바이러스도 함께 전파될 수 있습니다.

이동식 저장 매체는 주로 세 가지 방식으로 바이러스에 감염됩니다. 첫째, 바이러스에 감염된 컴퓨터에 연결된 이동식 매체 자체가 바이러스에 감염될 수 있습니다. 둘째, 바이러스가 포함된 파일을 매체에 복사하거나 이동하면 매체가 감염됩니다. 셋째, 매체 자체의 보안 취약점을 이용하여 바이러스가 직접 매체에 침투할 수 있습니다.



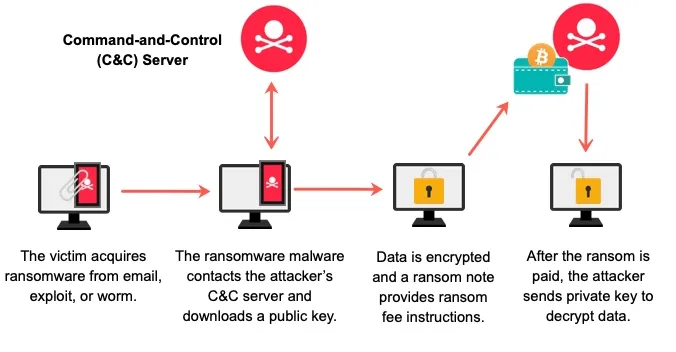
감염된 이동식 저장 매체를 다른 컴퓨터에 연결하면 바이러스가 시스템에 침투할 수 있습니다. 대부분의 바이러스는 사용자가 매체의 파일을 실행하거나 복사할 때 함께 실행되어 시스템을 감염시킵니다. 또한 자동 실행 기능을 악용하여 매체가 연결되자마자 바이러스가 실행되는 경우도 있습니다.

USB 드라이브와 같은 이동식 저장 매체는 바이러스 확산에 취약한 경로로 알려져 있습니다. 예컨대 2008년에 발견된 제나 바이러스는 USB를 통해 전파되어 전 세계 수백만 대의 컴퓨터를 감염시켰습니다.

**3.4 네트워크 취약점 이용**

바이러스는 네트워크 취약점을 악용하여 전파되기도 합니다. 네트워크 상에서 작동하는 프로그램이나 프로토콜의 보안 허점이 존재하면, 바이러스가 이를 공격 경로로 활용할 수 있습니다. 네트워크 서비스와 운영체제의 취약점을 노리는 공격 기법이 주로 사용됩니다.

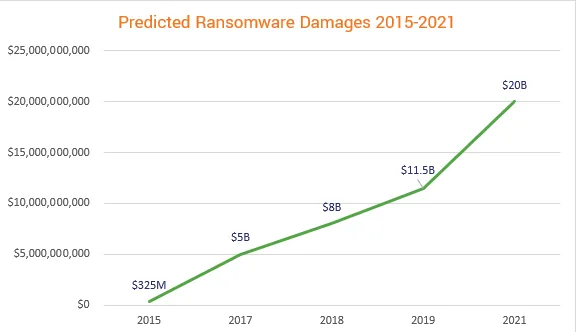
대표적인 사례로 2017년 전 세계적으로 큰 피해를 입힌 워너크라이(WannaCry) 랜섬웨어가 있습니다. 이 랜섬웨어는 윈도우 운영체제의 SMB(Server Message Block) 프로토콜 취약점을 공격해 전파되었습니다. 한번 감염되면 랜섬웨어가 내부 네트워크를 따라 자동으로 확산되어 다른 시스템을 연쇄 감염시켰습니다. 워너크라이는 러시아, 우크라이나, 인도, 대만 등 전 세계 150여 개국에서 피해를 입혔으며, 특히 영국 NHS 병원 네트워크가 마비되는 등 심각한 타격을 가했습니다.



## Ⅳ. 바이러스 피해사례

과거 주요 바이러스 사건 중 2000년 ILOVEYOU 바이러스는 이메일 첨부 파일의 형태로 전 세계로 급속히 확산되었습니다. 이 바이러스는 메일 주소록을 탈취하여 자신을 재전송함으로써 수억 달러의 경제적 손실을 입혔습니다. 2004년 마이둠 웜 역시 이메일과 네트워크 공유 폴더를 통해 전파되어 당시 최악의 사건으로 기록되며 수백만 대 이상의 시스템을 감염시켰습니다. 2017년 워너크라이 랜섬웨어는 운영체제 취약점을 노려 150개국 이상에서 피해를 입혔고, 영국 NHS 병원망 마비 등 주요 인프라에 심각한 타격을 주었습니다.

개인 차원에서는 바이러스 감염으로 인한 데이터 손실과 시스템 복구 비용 발생, 개인정보 유출과 이로 인한 신원 도용 위험, 정신적 스트레스 등의 피해가 있습니다. 기업은 시스템 다운타임으로 인한 업무 마비와 생산성 저하, 데이터 유출에 따른 법적 분쟁 비용, 고객 이탈과 브랜드 이미지 실추, 바이러스 제거와 예방을 위한 보안 투자 비용 증가 등의 타격을 받습니다.



사회적으로는 주요 기반시설과 공공 서비스 마비로 인한 혼란과 경제적 손실, 국가 안보 위협 증가, 디지털 시스템에 대한 대중의 불신 확산 등의 문제가 발생할 수 있습니다. 2017년 워너크라이 사태에서 볼 수 있듯이 병원 의료 서비스 지연으로 인한 생명 위험도 발생할 수 있습니다. 이처럼 대규모 바이러스 확산은 개인과 기업, 나아가 국가 전반에 심각한 피해를 줄 수 있는 주요 위험 요인입니다.

## Ⅳ. 바이러스 예방 및 대응

컴퓨터 바이러스 위협에 효과적으로 대응하기 위해서는 예방, 탐지, 대응의 체계적인 접근이 필요합니다. 우선 예방 차원에서 바이러스 백신 프로그램을 최신 버전으로 유지하고 정기적인 업데이트를 수행해야 합니다. 새로운 바이러스 유형과 변종이 지속적으로 등장하므로 바이러스 정의 파일을 주기적으로 갱신하는 것이 중요합니다. 또한 운영체제와 애플리케이션의 보안 취약점을 해결하기 위해 공식 패치를 적시에 설치해야 합니다. 이와 함께 출처가 불분명한 파일, 웹사이트, 링크 등에 대한 실행과 방문을 자제하는 주의가 필요합니다. 개인과 기업 차원에서 바이러스 예방 교육을 통해 보안 인식을 높이는 것도 중요한 예방책입니다.

바이러스 탐지 측면에서는 실시간 검사 기능을 활성화하여 이메일, 메신저, 웹 브라우징 등에서 바이러스를 실시간으로 모니터링해야 합니다. 또한 행위 기반 탐지와 휴리스틱 분석을 통해 새로운 유형의 바이러스도 탐지할 수 있어야 합니다. 네트워크 트래픽과 시스템 로그를 모니터링하여 이상 징후를 포착하는 보안 관제도 중요한 역할을 합니다. 기업에서는 전문 보안 관제 센터를 운영하거나 외부 서비스를 활용하는 방안을 고려해볼 수 있습니다.

바이러스에 감염되었을 경우에는 신속한 대응이 필수적입니다. 먼저 정기 백업을 통해 깨끗한 상태로 시스템을 복원할 수 있어야 합니다. 감염된 파일과 프로세스는 격리 및 치료를 수행해야 하며, 상황에 따라 운영체제 전체를 재설치하는 것도 고려해볼 수 있습니다. 바이러스 확산 경로를 분석하고 취약점을 점검하여 재발 방지 대책을 마련하는 것 또한 중요합니다. 기업에서는 바이러스 대응 매뉴얼을 수립하고 전담 보안 조직을 운영하며, 직원 대상 정기 교육을 실시하는 등 체계적인 관리 체계를 갖추는 것이 바람직합니다.

바이러스 위협은 지속적으로 진화하고 있으므로 예방, 탐지, 대응의 다각적인 노력이 필수적입니다. 정기적인 보안 업데이트와 예방 조치, 다중 계층의 모니터링, 신속하고 체계적인 대응을 통해 개인과 기업은 안전한 디지털 환경을 구축할 수 있습니다.

## Ⅵ. 참고 문헌

## “컴퓨터 바이러스 정의”,

## https://www.fortinet.com/kr/resources/cyberglossary/computer-virus

## “멀웨어(Malware)란 무엇인가요?

## https://www.ibm.com/kr-ko/topics/malware

## “컴퓨터 바이러스란 무엇인가?”, (2012.04.20) from

## https://blog.naver.com/hdj20/40157301683

## “컴퓨터 바이러스”

## https://ko.wikipedia.org/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0\_%EB%B0%94%EC%9D%B4%EB%9F%AC%EC%8A%A4

## “악성코드란 무엇인가, 바이러스, 웜, 트로이목마, 그 이상의 것 이해하기”, (2018.08.14) from

## https://www.itworld.co.kr/news/110408

## “컴퓨터 바이러스 유형에 따른 백신 프로그램의 성능분석 = The Performance Analysis of Vaccine Programs According to Computer Virus Classes”, (2011.02)

## https://www.riss.kr/search/detail/DetailView.do?p\_mat\_type=be54d9b8bc7cdb09&control\_no=8c96bb342aac3677ffe0bdc3ef48d419&outLink=K

## “컴퓨터 바이러스와 소프트웨어 에러의 비교연구”, (1990.4)

## https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE00620426