# 악성코드 탐지, 암호화 및 패키징 프로젝트

컴퓨터 바이러스 탐지 보고서



**목**

**차**

1. **바이러스 탐지 정의**
2. **바이러스 탐지 기술**
   1. 시그니처 기반 탐지
   2. 휴리스틱 기반 탐지
   3. 행위 기반 탐지
   4. 새로운 탐지 기술
3. **바이러스 토탈 API** 
   1. 소개
   2. 바이러스 토탈 작동방식
   3. 바이러스 토탈 API 기능 및 사용
   4. 장점과 한계
4. **결론**

4.1. 바이러스 탐지 기술의 중요성 요약

4.2. 통합적 바이러스 탐지 및 대응 방안 제안

1. **참고 문헌**

## 1. 바이러스 탐지 개요

컴퓨터 바이러스는 악의적인 코드가 프로그래밍된 악성 소프트웨어로, 사용자 모르게 컴퓨터 시스템에 침투하여 각종 피해를 입힙니다. 바이러스는 인터넷 및 이동식 저장장치를 통해 전파되며, 일단 시스템에 침투하면 자가 복제를 거듭하여 추가적인 악성코드를 유포하게 됩니다. 이로 인해 개인 및 기업은 데이터 손실, 시스템 다운타임 증가, 개인정보 유출 등 심각한 피해를 입을 수 있습니다. 특히 랜섬웨어와 같은 악성코드는 데이터를 인질로 삼아 금전을 요구하기도 합니다.

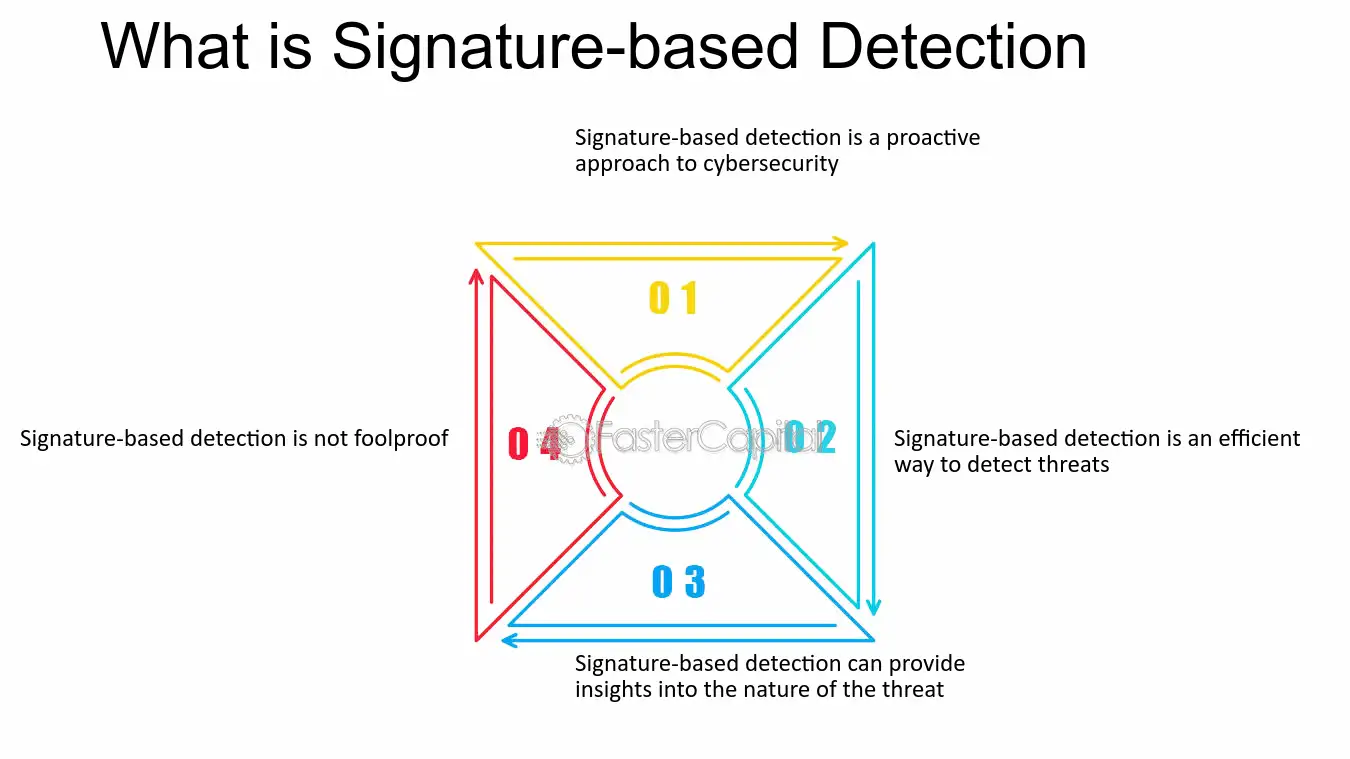
바이러스 탐지는 이러한 위험으로부터 시스템을 보호하기 위해 반드시 필요한 과정입니다. 안티바이러스 소프트웨어는 실시간으로 시스템을 모니터링하여 알려진 바이러스뿐 아니라 새로운 바이러스까지 탐지하고 차단합니다. 또한 정기적인 스캔을 통해 잠복해 있던 바이러스까지 검출하여 격리시키거나 삭제할 수 있습니다. 이렇게 바이러스 탐지 기술은 지속적으로 발전하고 있으며, 감염된 파일에서 악성코드를 제거하거나 격리시켜 시스템을 안전하게 보호하는 데 크게 기여하고 있습니다.

본 보고서에는 **VirusTotal** 도구에 대한 내용도 포함됩니다. VirusTotal은 여러 안티바이러스 엔진과 온라인 도구를 통합하여 바이러스를 빠르게 탐지하는 플랫폼입니다. 의심스러운 파일이나 URL을 분석하고, 이를 알려진 위협 데이터베이스와 비교하여 상세한 보고서를 제공합니다. 나아가 각 기술의 특징을 분석하여 바이러스 대응을 위한 통합적 접근 방안을 제시함으로써, 바이러스 탐지 기술의 현주소와 발전 방향을 가늠해볼 수 있을 것입니다.

## 2. 기존 바이러스 탐지 기술

## 2.1. 시그니처 기반 탐지

시그니처 기반 바이러스 탐지 기술은 알려진 악성코드의 고유한 특징을 나타내는 시그니처를 데이터베이스에 저장해 두고, 새로운 파일이나 프로세스와 이 시그니처를 비교하여 악성코드 여부를 판단하는 방식으로 작동합니다. 이를 위해 먼저 보안 전문가들이 악성코드 샘플을 분석하여 해당 코드에 고유한 바이너리 패턴, 코드 시퀀스, 파일 해시 등의 시그니처를 추출합니다. 추출된 시그니처는 안티바이러스 소프트웨어의 시그니처 데이터베이스에 등록되며, 사용자는 이 데이터베이스를 주기적으로 업데이트해야 합니다.



그 후 안티바이러스 소프트웨어가 사용자 시스템을 정기적으로 스캔할 때, 파일이나 실행 중인 프로세스의 내용을 데이터베이스에 저장된 시그니처와 비교합니다. 만약 일치하는 시그니처가 발견되면 해당 파일이나 프로세스를 악성코드로 탐지하고, 사용자에게 경고를 보내거나 자동으로 격리, 삭제 등의 조치를 취하게 됩니다.

이 기술의 주요 장점은 알려진 악성코드에 대해 매우 높은 정확도로 탐지할 수 있으며, 시그니처 매칭 자체가 간단한 연산이므로 실행 속도 또한 빠르다는 것입니다. 하지만 단점으로는 새로운 변종이나 아직 시그니처가 등록되지 않은 악성코드에 대해서는 탐지가 불가능하다는 점과, 정기적인 데이터베이스 업데이트가 필수적이라는 점을 들 수 있습니다. 또한 지나치게 일반적인 시그니처를 사용하면 정상 프로그램까지 악성코드로 잘못 판단할 수 있어 주의가 필요합니다.

## 2.2. 휴리스틱 기반 탐지

휴리스틱 기반 바이러스 탐지 기술은 알려진 악성코드의 시그니처가 아닌 일반적인 규칙을 사용하여 프로그램의 실행 행동과 패턴을 분석함으로써 잠재적인 악성 활동을 식별하는 원리로 작동합니다. 구체적으로는 프로그램이 시스템 자원에 접근하거나 특정 작업을 수행할 때의 행위를 모니터링하고, 이를 미리 정의된 규칙과 대조하여 악성 여부를 판단합니다. 예를 들어 레지스트리 키 변경, 원격 명령 실행 시도 등의 행위가 탐지되면 악성코드일 가능성이 있는 것으로 간주됩니다.

이러한 휴리스틱 기반 탐지 기술의 가장 큰 장점은 알려지지 않은 새로운 형태의 악성코드에 대한 대응력이 뛰어나다는 것입니다. 시그니처 기반 탐지와 달리 특정 악성코드의 패턴에 의존하지 않고 일반적인 악성 행위 규칙을 적용하므로, 새로 등장한 변종 악성코드까지도 탐지할 수 있습니다. 또한 휴리스틱 규칙을 지속적으로 업데이트하고 보완함으로써 탐지 범위를 확장할 수 있습니다.

하지만 이 기술의 단점으로는 오탐지 가능성과 리소스 소모 문제를 지적할 수 있습니다. 지나치게 포괄적인 규칙을 적용하면 정상 프로그램의 행위까지 악성으로 오인할 수 있으며, 복잡한 행동 분석 알고리즘을 실행하는 데 많은 시스템 자원이 소모될 수 있습니다. 따라서 효과적인 휴리스틱 기반 탐지를 위해서는 규칙의 정밀도를 지속적으로 높이고, 오탐지를 최소화하는 작업이 필수적입니다. 또한 리소스 소모 문제를 해결하기 위한 최적화 기술도 병행되어야 합니다.

## 2.3. 행위 기반 탐지

행위 기반 바이러스 탐지 기술은 파일이나 프로그램의 실행 행동을 지속적으로 모니터링하여 악성코드를 탐지하는 방식으로 작동합니다. 이 기술은 사전에 정의된 악성 행위의 패턴을 바탕으로 실제 프로그램의 행동을 분석하여 악성 여부를 판단합니다. 예를 들어 레지스트리 키 변경, 원격 서버와의 명령 송수신, 민감한 데이터 유출 시도 등 알려진 악성코드의 전형적인 행위가 탐지되면 이를 악성으로 간주하고 차단하게 됩니다.

행위 기반 탐지 기술의 가장 큰 장점은 알려지지 않은 새로운 형태의 악성코드에 대한 대응력이 뛰어나다는 것입니다. 시그니처 기반 탐지와 달리 특정 악성코드의 코드 패턴에 의존하지 않고, 일반적인 악성 행위 패턴을 기반으로 하므로 새로 등장한 변종 악성코드까지 탐지할 수 있습니다. 또한 행위 패턴 룰을 지속적으로 업데이트하고 보완함으로써 탐지 범위를 계속 확장할 수 있다는 장점이 있습니다.

그러나 행위 기반 탐지 기술의 단점으로는 오탐지 가능성과 시스템 자원 소모 문제를 지적할 수 있습니다. 일부 정상 프로그램의 행위가 악성 행위와 유사할 경우 이를 악성코드로 잘못 판단할 수 있으며, 실시간으로 프로그램 행동을 모니터링하고 분석하는 데 많은 CPU와 메모리 자원이 소모될 수 있습니다. 따라서 효과적인 행위 기반 탐지를 위해서는 오탐지를 최소화하고 리소스 소모를 최적화하는 기술이 함께 적용되어야 합니다.

## 2.4. 새로운 탐지 기술

**1.머신러닝 기반 탐지**

머신러닝 기반 바이러스 탐지 기술은 프로그램의 실행 행동 패턴을 분석하여 악성코드를 탐지하는 방식입니다. 방대한 양의 정상 프로그램과 악성코드 데이터를 통해 학습된 모델은 다양한 행동 패턴을 분석하여 악성 여부를 예측합니다. 이 기술은 알려지지 않은 악성코드에 대해서도 유사한 패턴을 탐지할 수 있어, 기존 시그니처 기반 탐지보다 넓은 범위의 위협에 대응할 수 있습니다.

**2. 클라우드 기반 탐지**

클라우드 기반 바이러스 탐지 기술은 사용자 단말에서 수집한 데이터를 클라우드로 전송하여 분석합니다. 강력한 컴퓨팅 파워를 활용해 대량의 데이터를 실시간 처리하며, 신속한 업데이트가 가능합니다. 이 기술은 사용자 PC에 부하를 주지 않으면서 글로벌 차원의 위협 정보를 통합 분석할 수 있어 보안 관리의 효율성을 높입니다.

**3. 인공지능 기반 탐지**

인공지능 기반 바이러스 탐지 기술은 머신러닝 모델을 사용하여 프로그램의 실행 행동 패턴을 분석합니다. 이 기술은 알려지지 않은 형태의 악성코드에도 효과적으로 대응할 수 있으며, 행동 패턴 분석을 통해 변종 악성코드를 탐지할 수 있습니다. 정교한 모델 조정을 통해 오탐지율을 최소화하여 시스템 자원 낭비를 줄이고 사용자 불편을 해소할 수 있습니다.

## 3. 바이러스 토탈 API

## 3.1. 소개

## VirusTotal은 여러 안티바이러스 엔진과 도구를 결합하여 파일, URL, IP 주소, 도메인을 분석해 악성코드를 탐지하는 온라인 서비스입니다.

## 이 서비스는 보안 전문가, 연구원, 그리고 위협을 식별하고 평가해야 하는 조직들에게 중요한 리소스입니다.

## VirusTotal API는 이 서비스를 확장하여, 사용자가 VirusTotal의 기능을 자체 소프트웨어에 통합할 수 있게 해줍니다.

## 3.2. 바이러스 토탈 작동방식

## VirusTotal은 파일이나 URL을 여러 안티바이러스 엔진에 제출하여 악성코드를 검사합니다. 이 플랫폼은 Kaspersky, McAfee, Symantec과 같은 주요 보안 업체를 포함해 70개 이상의 보안 벤더와 협력하여 제출된 콘텐츠의 안전성을 평가합니다. 그 결과는 통합되어 사용자에게 제공되며, 악성코드로 감지된 파일과 위협 유형에 대한 자세한 보고서가 포함됩니다.

## 

## 3.3. 바이러스 토탈 API 기능 및 사용 흐름(요청 예시)

VirusTotal API는 VirusTotal의 스캔 서비스를 자동으로 접근할 수 있게 해줍니다. 이를 통해 사용자는 다음과 같은 작업을 수행할 수 있습니다:

1. **파일 스캔**: 파일을 분석하기 위해 제출하고, 모든 통합된 안티바이러스 엔진의 스캔 결과를 포함한 상세 보고서를 반환받습니다.
2. **URL 스캔**: 파일 스캔과 유사하게, URL을 제출하여 악성 콘텐츠가 있는지 확인합니다.
3. **도메인 및 IP 주소 정보**: 도메인과 IP 주소를 조회해 이들이 악성 활동과 연관이 있는지 확인합니다.
4. **파일 재스캔**: 이전에 분석된 파일을 다시 스캔해, 새로운 감지가 발생했는지 확인합니다.
5. **보고서 검색**: 이전에 제출된 파일, URL, 도메인에 대한 스캔 결과를 검색합니다.

**API 사용 흐름**

VirusTotal API를 사용하는 일반적인 워크플로우는 다음 단계를 포함합니다:

1. **API 키 획득**: VirusTotal API를 사용하려면 먼저 VirusTotal 웹사이트에서 API 키를 얻어야 합니다. 이 키는 요청을 인증하는 데 필요합니다.
2. **파일 또는 URL 제출**: 파일 또는 URL을 POST 요청을 통해 VirusTotal API에 제출합니다. API 엔드포인트는 콘텐츠를 수락하고 고유 리소스 식별자(예: 파일의 경우 해시)를 반환합니다.
3. **분석 요청**: 파일이나 URL이 제출되면, 리소스 식별자를 사용해 GET 요청을 통해 분석 결과를 얻을 수 있습니다. API는 JSON 형식으로 자세한 정보를 반환합니다.
4. **보고서 해석**: JSON 응답에는 탐지된 악성코드 이름, 위협 유형, 그리고 어떤 안티바이러스 엔진이 파일을 감지했는지에 대한 세부 사항이 포함됩니다.

## 3.4. 장점과 한계

**장점**:

* **광범위한 탐지**: VirusTotal은 여러 안티바이러스 엔진의 결과를 통합하여 광범위한 탐지를 제공합니다.
* **자동화된 워크플로우**: API는 위협 탐지를 자동화할 수 있어 기존 보안 인프라에 쉽게 통합할 수 있습니다.

**한계**:

* **오탐 및 누락**: 모든 탐지 방법이 완벽하지 않으며, 서로 다른 안티바이러스 엔진 간에 차이가 있을 수 있습니다.

## 4. 결론

## 4.1. 바이러스 탐지 기술의 중요성 요약

## 컴퓨터 바이러스는 시스템 파괴, 데이터 손실, 개인정보 유출 등 심각한 피해를 초래할 수 있습니다. 따라서 바이러스 탐지 기술은 컴퓨터 시스템의 보안과 안정성을 지키는 데 필수적입니다.

## 바이러스 탐지 기술은 실시간으로 악성코드를 감지하고 차단하며, 정기적인 시스템 스캔을 통해 잠복해 있던 바이러스까지 탐지하여 제거할 수 있습니다.

## 이를 통해 바이러스로 인한 피해를 최소화하고 데이터와 개인정보를 안전하게 보호할 수 있습니다. 따라서 컴퓨터 사용자라면 반드시 바이러스 탐지 기술을 활용해야 합니다.

## 4.2. 통합적 바이러스 탐지 및 대응 방안 제안

악성코드 탐지를 위한 통합적 접근이 매우 중요합니다. 다음과 같은 다각적인 대응 방안을 제안합니다:

**1. 다중 탐지 방법 적용**

* **시그니처 기반 탐지**와 **행동 기반 탐지**를 함께 사용하여 기존 악성코드는 물론 새로운 변종까지 탐지할 수 있습니다.
  + - 예: 파일 해시 시그니처로 기존 랜섬웨어 차단, 행동 모니터링으로 새로운 위협 탐지.

**2. 클라우드 기반 통합 분석 체계 구축**

* **VirusTotal API**를 활용하여 전 세계에서 수집된 위협 정보를 클라우드에서 분석하고 빠르게 대응책을 공유할 수 있습니다.
  + - 예: VirusTotal API는 여러 바이러스 탐지 엔진을 결합하여 의심 파일에 대한 정보를 빠르게 제공.

**3. 사용자 교육**

* 안전한 파일 열람, 의심스러운 파일 실행 자제, 정기 백업 같은 보안 수칙 교육을 통해 악성코드 감염을 예방.

**4. 시스템 보안 강화**

* 운영체제 및 애플리케이션의 **정기적인 보안 패치**를 통해 시스템 취약점 최소화.

**5. 지속적 업데이트와 모니터링**

* **바이러스 정의 데이터베이스**를 지속적으로 업데이트하고, 실시간 모니터링 시스템을 통해 새로운 위협에 즉각 대응.

## 5. 참고 문헌

## “안티바이러스 소프트웨어”,

## https://namu.wiki/w/%EC%95%88%ED%8B%B0%EB%B0%94%EC%9D%B4%EB%9F%AC%EC%8A%A4%20%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC%96%B4

## “안티바이러스 소프트웨어 원리”, (2024.02.18) form

## https://dasima.co.kr/767/%EC%95%88%ED%8B%B0%EB%B0%94%EC%9D%B4%EB%9F%AC%EC%8A%A4-%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC%96%B4-%EC%9B%90%EB%A6%AC/

## “안티바이러스 기능 및 성능 분석 1부”, (2023.01.27) from

## https://csrc.kaist.ac.kr/blog/2023/01/27/%EC%95%88%ED%8B%B0%EB%B0%94%EC%9D%B4%EB%9F%AC%EC%8A%A4-%EA%B8%B0%EB%8A%A5-%EB%B0%8F-%EC%84%B1%EB%8A%A5-%EB%B6%84%EC%84%9D-1%EB%B6%80/

## “안티바이러스 기능 및 성능 분석 2부” , (2023.03.27) from

## https://csrc.kaist.ac.kr/blog/2023/03/27/%EC%95%88%ED%8B%B0%EB%B0%94%EC%9D%B4%EB%9F%AC%EC%8A%A4-%EA%B8%B0%EB%8A%A5-%EB%B0%8F-%EC%84%B1%EB%8A%A5-%EB%B6%84%EC%84%9D-2%EB%B6%80/

## **“정적 분석을 이용한 다형성 스크립트 바이러스의 탐지기법 설계”, (2003.4) form**

## https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE00622344

## **“바이러스 탐지를 위한 휴리스틱 스캐닝 기법 및 행위 제한 기법 분석”**

## **(2002.10) from**

## **https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE00616165**

## **“파일 바이러스 복제 특성을 이용한 바이러스 탐지 및 복구”, (2001.10) from**

## **https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE00615587**