악성코드 분석, 암호화 및 패키징 프로젝트

컴퓨터 바이러스 탐지 보고서

문서 번호 : SRP-001

목 차

I. 바이러스 탐지 개요

컴퓨터 바이러스는 악의적인 의도로 만들어진 프로그램으로, 사용자도 모르는 사이에 컴퓨터에 침투해 여러 가지 피해를 줍니다. 이런 바이러스는 주로 인터넷이나 USB 같은 저장 장치를 통해 퍼지며, 한번 컴퓨터에 들어가면 자기 복제를 통해 더 많은 악성 프로그램을 퍼뜨립니다. 이로 인해 개인이나 회사는 중요한 정보를 잃거나, 시스템이 멈추거나, 개인 정보가 유출되는 등 심각한 문제를 겪을 수 있습니다. 특히 랜섬웨어 같은 경우는 데이터를 인질로 잡고 돈을 요구하기도 합니다.

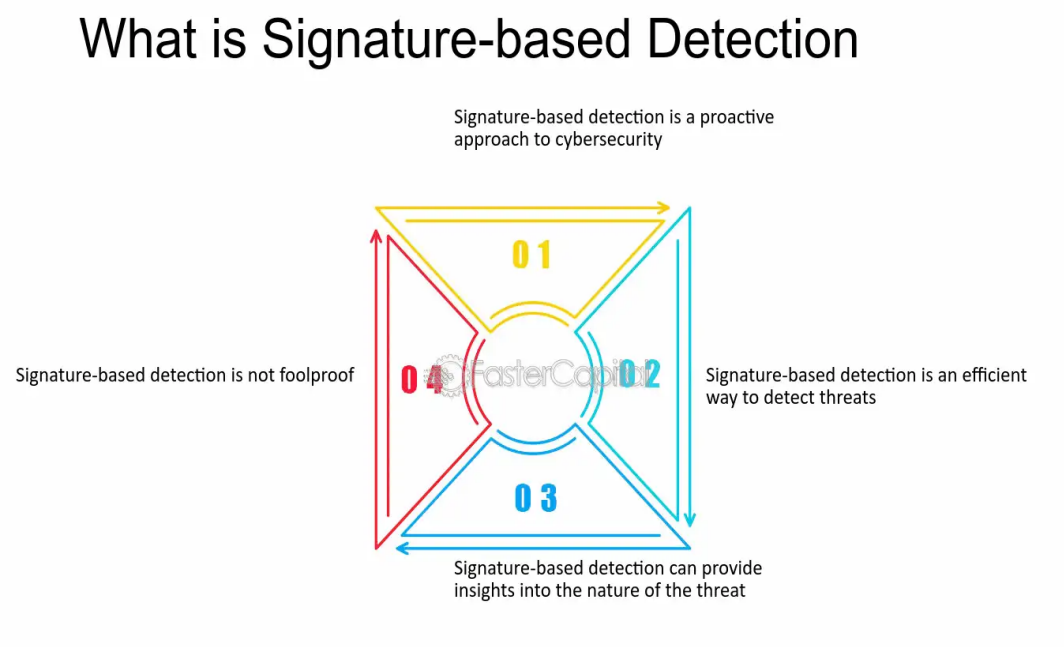
이런 위험으로부터 컴퓨터를 지키기 위해서는 바이러스를 찾아내는 것이 매우 중요합니다. 안티바이러스 프로그램은 컴퓨터를 계속 지켜보면서 알려진 바이러스뿐만 아니라 새로운 바이러스도 찾아내고 막아냅니다. 또한 주기적으로 컴퓨터를 검사해서 숨어있던 바이러스도 찾아내 격리하거나 삭제할 수 있습니다. 이렇게 바이러스를 찾아내는 기술은 계속 발전하고 있어서, 바이러스에 감염된 파일을 치료하거나 격리해서 컴퓨터를 안전하게 지키는 데 큰 도움을 주고 있습니다.

이 보고서에서는 VirusTotal 이라는 도구에 대해서도 다룹니다. VirusTotal 은 여러 안티바이러스 프로그램과 온라인 도구를 한데 모아 바이러스를 빠르게 찾아내는 플랫폼입니다. 의심스러운 파일이나 웹사이트 주소를 분석하고, 이를 알려진 위험 목록과 비교해서 자세한 보고서를 만들어 줍니다. 더 나아가 각 기술의 특징을 살펴보고 바이러스에 대응하는 종합적인 방법을 제안함으로써, 현재 바이러스 탐지 기술의 수준과 앞으로의 발전 방향을 가늠해볼 수 있을 것입니다.

II. 바이러스 탐지 기술

1. 시그니처 기반 탐지

시그니처 기반 탐지 기술은 이미 알려진 악성코드의 고유한 특성을 데이터베이스에 저장해 두고, 새로운 파일이나 프로세스와 비교하여 악성코드인지 판단하는 방식입니다. 보안 전문가들이 악성코드를 분석해 해당 코드의 고유한 패턴, 코드 시퀀스, 파일 해시 등의 시그니처를 추출하여 데이터베이스에 등록해 두면, 사용자는 이를 주기적으로 업데이트해야 합니다.



안티바이러스 프로그램이 시스템을 정기적으로 스캔할 때, 파일이나 실행 중인 프로세스를 데이터베이스와 대조하여 일치하는 시그니처가 있으면 악성코드로 탐지합니다. 이 경우 사용자에게 경고가 뜨거나 파일이 자동으로 격리 또는 삭제됩니다.

이 방법의 장점은 이미 알려진 악성코드를 정확하게 탐지할 수 있다는 점이며, 비교적 간단한 연산으로 빠르게 처리된다는 것입니다. 하지만 새로운 변종이나 데이터베이스에 없는 악성코드는 탐지할 수 없다는 한계가 있습니다. 또한 너무 일반적인 시그니처를 사용하면 정상적인 파일을 잘못 탐지할 가능성도 있습니다.

2. 휴리스틱 기반 탐지

휴리스틱 기반 탐지 기술은 악성코드의 특정 패턴이 아닌, 프로그램의 실행 행동과 패턴을 분석하여 잠재적인 악성 활동을 찾아내는 방식입니다. 예를 들어, 프로그램이 시스템 자원에 접근하거나 레지스트리 키를 변경하는 등의 행동을 모니터링하여 미리 정의된 규칙에 맞는지 비교하는 방식입니다.

이 방식은 시그니처 기반 탐지와 달리 새롭게 등장한 악성코드도 탐지할 수 있다는 장점이 있습니다. 규칙을 계속 업데이트함으로써 탐지 범위도 넓힐 수 있죠. 하지만 규칙이 너무 넓으면 정상적인 프로그램까지 악성코드로 잘못 판단할 수 있고, 복잡한 분석이 필요하기 때문에 시스템 자원을 많이 사용할 수 있습니다.

3. 행위 기반 탐지

행위 기반 탐지 기술은 프로그램이 실행되는 동안 지속적으로 행동을 모니터링하여 악성코드를 찾아내는 방식입니다. 예를 들어, 레지스트리 키 변경, 민감한 데이터 유출 시도 등의 행위가 발생하면 악성코드로 의심하여 차단하는 식이죠.

이 방법의 장점은 새로운 변종 악성코드까지 탐지할 수 있다는 점입니다. 하지만 정상 프로그램이 악성 행위와 비슷한 행동을 할 경우, 잘못 탐지할 가능성이 있습니다. 또한 프로그램의 행동을 실시간으로 모니터링하기 때문에 시스템 자원을 많이 소모할 수 있습니다.

4. 새로운 탐지 기술

① 머신러닝 기반 탐지

머신러닝을 활용한 탐지 기술은 방대한 양의 데이터를 학습한 모델을 통해 프로그램의 행동 패턴을 분석해 악성코드를 예측하는 방식입니다. 덕분에 기존 시그니처 기반 탐지보다 더 넓은 범위의 위협을 탐지할 수 있습니다.

② 클라우드 기반 탐지

클라우드 기반 탐지 기술은 사용자의 시스템에서 수집한 데이터를 클라우드 서버로 전송해 분석하는 방식입니다. 강력한 컴퓨팅 자원을 활용하여 대규모 데이터를 실시간으로 처리하며, 신속한 업데이트가 가능하다는 장점이 있습니다.

③ 인공지능 기반 탐지

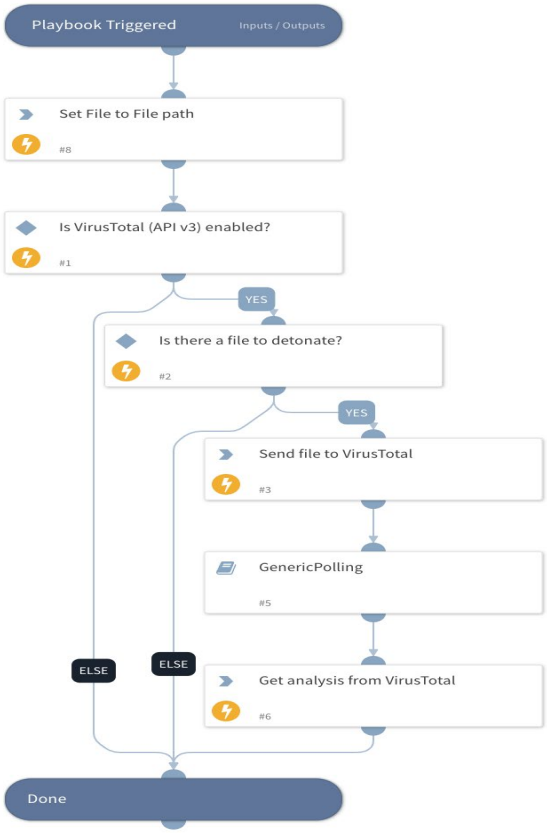
인공지능을 이용한 탐지 기술은 머신러닝 모델을 통해 프로그램의 실행 행동 패턴을 분석합니다. 변종 악성코드까지 효과적으로 대응할 수 있으며, 오탐지율을 줄여 시스템 자원 낭비를 최소화할 수 있습니다.

III. 바이러스 토탈 API

1. 소개

VirusTotal 은 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 리소스 입니다.
VirusTotal API 는 이 서비스를 확장하여, 사용자가 VirusTotal 의 기능을 자체 소프트웨어에 통합할 수 있게 해줍니다.

2. 바이러스 토탈 작동방식



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

3. 바이러스 토탈 API 쿼리문

바이러스 토탈 API 에는 endpoint 를 통한 웹 액션을 쿼리문으로 사용합니다. 주요 쿼리문은 아래와 같습니다.

① 파일 업로드 및 분석 요청

Endpoint: /file
기능: 사용자가 파일을 업로드하여 멀티 엔진 분석을 요청합니다.
쿼리 예시: POST https://www.virustotal.com/api/v3/files

② 해시 또는 파일에 대한 분석 결과 조회

Endpoint: /file/id
리소스 ID 를 사용하여 파일의 분석 결과를 조회합니다.
쿼리 예시: GET https://www.virustotal.com/api/v3/files/id

③ URL 스캔 및 분석 요청

Endpoint: /url
기능: 특정 URL 에 대한 멀티 엔진 분석을 요청합니다.
쿼리 예시: POST https://www.virustotal.com/api/v3/urls

④ URL 분석 결과 조회

Endpoint: /urls/id
기능: URL 에 대한 분석 결과를 확인합니다.
쿼리 예시: GET https://www.virustotal.com/api/v3/urls/id

⑤ IP 주소 정보 조회
Endpoint: /ip_addresses/ip
기능: 특정 IP 주소와 관련된 보안 정보를 조회합니다.
쿼리 예시: GET https://www.virustotal.com/api/v3/ip_addresses/ip

⑥ 도메인 정보 조회
Endpoint: domains/domain
기능: 특정 도메인과 관련된 보안 정보를 조회합니다.
쿼리 예시: GET https://www.virustotal.com/api/v3/domains/domain

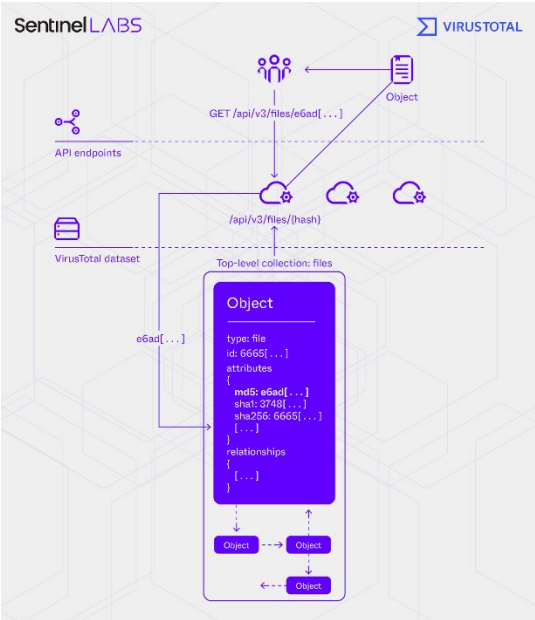
⑦ 파일 재분석 요청
Endpoint: /files/id/analyse
기능: 이전에 분석된 파일을 다시 분석합니다.
쿼리 예시: POST https://www.virustotal.com/api/v3/files/id/analyse

⑧ 댓글 추가
Endpoint: / files/id/comments
기능: 특정 파일에 대해 의견을 추가합니다.
쿼리 예시: POST https://www.virustotal.com/api/v3/files/id/comments

⑨ 대용량 파일에 대한 upload 주소 얻기
Endpoint: /files/upload_url
기능: 크기가 큰 파일을 업로드 하기 위한 url 주소를 얻습니다.
쿼리 예시 : GET https://www.virustotal.com/api/v3/files/upload_url

아래 이미지는 API 를 통해 파일을 스캔하는 과정과 보고서로 나오는 구조 입니다.

Pre-Vision



IV. 결론

컴퓨터 바이러스 및 악성코드의 위협은 날로 증가하고 있으며, 이에 대응하기 위한 탐지 기술의 발전이 필수적입니다. 시그니처 기반 탐지, 휴리스틱 탐지, 행위 기반 탐지와 같은 전통적인 방법은 여전히 유용하지만, 악성코드의 고도화에 따라 새로운 기술의 도입이 요구되고 있습니다. 특히 머신러닝과 클라우드 기반 탐지 기술은 다양한 변종 악성코드를 더 효과적으로 탐지하고 분석하는 데 중요한 역할을 하고 있습니다.

이 보고서에서 다룬 VirusTotal API 는 다수의 보안 엔진을 통합하여 파일, URL, IP 주소 및 도메인에 대한 멀티 엔진 분석을 제공하는 강력한 도구입니다. 이를 통해 보안 위협에 대한 신속하고 포괄적인 평가가 가능해지며, API 를 통해 자동화된 위협 탐지 및 대응 시스템을 구축할 수 있습니다.

V. 참고문헌

"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 1 부", (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 2 부" , (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
바이러스 토탈 API 쿼리
https://blog.virustotal.com/2024/08/VT-S1-EffectiveResearch.html