악성 IP 기반 국가별 국내 유입 현황 데이터 시각화 웹 페이지

3조

팀원 : 이종운, 권성직, 김혜진, 신선호

제출일 : 2024. 5. 16

목차

1. 서론

1.1. 보고서 목적 : 본 보고서는 2018년부터 2020년까지 수집된 악성 IP 데이터를 기반으로, 국가별 국내 유입 현황을 분석하고 시각화한 웹페이지의 개발 과정을 설명하는 것을 목적으로 한다. 이를 통해 악성 IP의 분포와 주요 유입 국가를 파악하고, 향후 보안 강화 방안을 제안하고자 한다.

1.2. 프로젝트 개요 : 본 프로젝트는 악성 IP 데이터를 수집하고, 이를 국가별로 분류하여 시각화하는 웹페이지를 개발하는 것이다. 주요 기능으로는 3개년 데이터를 보여주는 가로막대 그래프, 연도별 데이터를 보여주는 트리맵, 표, 세계지도 위의 원형 시각화 등이 포함된다.

2. 프로젝트 배경 및 필요성

2.1. 악성 IP의 정의 및 중요성 : 악성 IP란 악성 행위를 하는 IP 주소를 의미한다. 이는 해킹, 스팸, 피싱 등의 보안 위협을 유발할 수 있다. 악성 IP의 식별과 차단은 네트워크 보안에 있어 매우 중요하다.

2.2. 국내 유입 현황 분석의 필요성 : 국내로 유입되는 악성 IP의 현황을 파악함으로써 주요 공격 원천 국가를 식별하고, 효과적인 방어 전략을 수립할 수 있다.

3. 데이터 수집 및 처리

3.1. 데이터 소스 : 본 프로젝트에서는 2018년부터 2020년까지 공적으로 제공하는 국가별 IP 데이터와 위치 정보, 보안 기관에서 제공하는 악성 IP 데이터를 사용하였다.

3.2. 데이터 정제 및 저장 : 수집된 데이터는 국가별 IP 데이터와 대조를 통해 악성 IP의 국가 정보를 라벨링하는 등의 정제 과정을 거쳐 데이터베이스에 저장하였다.

4. 시스템 설계 및 개발

4.1. 아키텍처 설계 : 전체 시스템은 JSP, MySQL, 아파치 톰캣으로 구성되어있다.

4.2. 웹페이지 개발

프론트 엔드 (D3.js 사용) : Dynamic Web Project 기반의 JSP 프로젝트에 시각화 라이브러리인 D3.js를 사용하여 데이터를 시각화하였다.

데이터베이스 : MySQL을 사용하여 데이터를 저장하고, 효율적으로 데이터를 관리할 수 있도록 설계하였다.

서버 : 아파치 톰캣 9.0.85 버전을 사용하였다.

5. 시각화 방법 및 구현

5.1. 시각화 자료 설명

가로막대 그래프 (2018~2020년 전체 데이터) : 3개년 데이터를 한눈에 비교할 수 있도록 가로막대 그래프로 시각화하였다.
트리맵 (연도별 데이터) : 각 연도의 데이터를 트리맵으로 시각화하여, 국가별 악성 IP의 분포를 직관적으로 보여준다.
표 (연도별 데이터): 연도별 데이터를 표 형태로 제공하여, 세부적인 데이터를 쉽게 확인할 수 있다.
세계지도 위의 원형 시각화 (연도별 데이터): 연도별 데이터를 세계지도 위에 원형으로 시각화하여, 각 국가별 악성 IP의 수를 시각적으로 표현 하였다.

5.2. 사용자 인터페이스와 전환 기능

버튼을 통한 연도 선택 및 시각화 전환 : 사용자 인터페이스에 버튼을 배치하여, 클릭 시 연도별 데이터를 선택하고 시각화를 전환할 수 있다.

6. 기능 및 특징

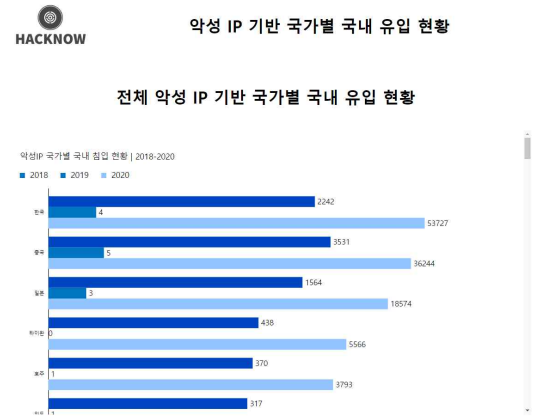
6.1. 주요 기능 설명

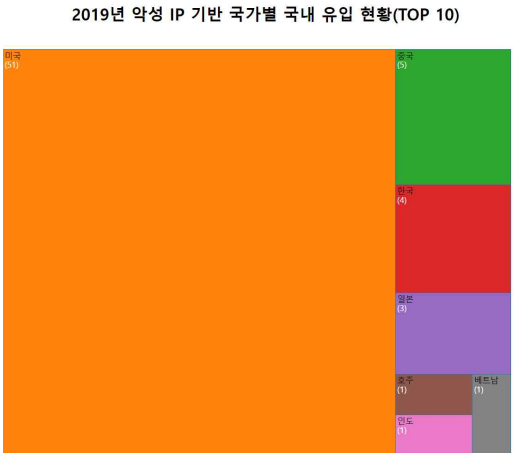
실시간 데이터 시각화 : 수집된 데이터를 데이터베이스에 업데이트하면 실시간으로 시각화하여 사용자에게 제공한다.

사용자 인터페이스 디자인 : 직관적이고 사용하기 쉬운 인터페이스를 설계하여, 사용자가 쉽게 데이터를 탐색할 수 있도록 하였다.

7. 결과 및 분석

7.1. 웹페이지 시연





7.2. 국내 유입 현황 데이터 분석

한국, 중국, 일본 : 세 국가에서 유입되는 악성 IP의 수가 가장 많았다. 이는 이 지역의 인터넷 사용자 수와 네트워크 활동이 많기 때문으로 추정된다.
호주 : 예상과는 달리 호주에서도 상당한 양의 악성 IP가 유입되고 있음을 발견했다. 이는 호주 내의 특정 네트워크 또는 서버가 악성 활동에 연루되었을 가능성을 시사한다.
다른 국가들 : 그 외에도 다양한 국가에서 악성 IP가 유입되었으나, 상대적으로 적은 수치를 보였다.

이러한 분석 결과를 통해, 특정 국가에서 발생하는 보안 위협에 대해 보다 집중적인 대응이 필요함을 알 수 있다. 특히, 호주의 경우 추가적인 조사가 필요할 것으로 보인다.

8. 문제점 및 개선사항

8.1. 현재 시스템의 한계

기간 제한 : 2018년부터 2020년까지의 데이터만 처리할 수 있다.

데이터 추가의 불편함 : 데이터를 추가하거나 업데이트하는 작업이 자동화되어 있지 않고, 수작업으로 데이터베이스를 수정해야 하는 불편함이 있다.

확장성 부족: 시스템이 고정된 데이터 구조에 의존하고 있어, 향후 데이터 양이 증가하거나 새로운 분석 요구사항이 생길 경우 대응하기 어렵다.

8.2. 향후 개선 방안

데이터 기간 확장 : 시스템을 업데이트하여 2018년부터 2020년까지의 데이터뿐만 아니라, 추가적인 기간의 데이터를 처리할 수 있도록 한다. 이를 위해 데이터베이스 스키마를 유연하게 설계하고, 데이터 처리 로직을 확장한다.

UI를 통한 데이터 추가 : 데이터를 웹 인터페이스를 통해 추가할 수 있는 기능을 개발한다. 사용자가 데이터를 손쉽게 업로드하고 관리할 수 있도록, 파일 업로드 및 데이터 검증 기능을 갖춘 UI를 제공한다.

자동화된 데이터 업데이트 : 외부 데이터 소스로부터 자동으로 데이터를 수집하고, 정제된 데이터를 데이터베이스에 업데이트하는 파이프라인을 구축한다. 이를 통해 데이터 업데이트 작업을 자동화한다.

확장성 고려 : 시스템 아키텍처를 재설계하여, 데이터 양이 증가하더라도 성능 저하 없이 데이터를 처리하고 시각화할 수 있도록 한다. 필요시 분산 데이터베이스 또는 클라우드 기반 솔루션을 도입할 수 있다.

9. 결론

9.1. 프로젝트 요약

본 프로젝트는 2018년부터 2020년까지의 악성 IP 데이터를 수집하여 국가별 국내 유입 현황을 분석하고, 이를 시각화한 웹페이지를 개발하는 것을 목표로 했다. D3.js를 사용하여 다양한 시각화 방법을 구현하였으며, 사용자가 직관적으로 데이터를 탐색할 수 있는 인터페이스를 제공하였다. 이를 통해 주요 국가별 악성 IP 유입 현황을 파악하고, 보안 위협에 대한 대응 방안을 모색할 수 있었다.