잉카 프로젝트 보고서

악성IP 시각화

2조 : 안위재, 이유탁, 이주섭

목차

1.서론

a. 개요

- 프로젝트 배경 : 악성 IP 국가별 국내 유입 현황에 대한 통계를 내고 시각화 하여 한 눈에 파악할 수 있도록 하는 기능을 개발한다.
- 프로젝트 설명 : 악성 IP의 정보가 담긴 csv파일과 IP 주소에 해당하는 국가, 그리고 그 국가의 위도와 경도를 Python의 Pandas를 이용하여 데이터 전처리 과정을 거친 후 데이터 베이스의 사용 없이 csv파일과 json파일을 이용하여 악성 IP의 유입 현황을 세계지도, 테이블, 파이 차트, 트리 차트, 지구본 형태의 다트 차트의 형태로 한 눈에 알아볼 수 있도록 하는 프로그램을 이클립스 JSP와 Tomcat, 그리고 CSS를 사용하여 제작 제작하였다.

2.본론

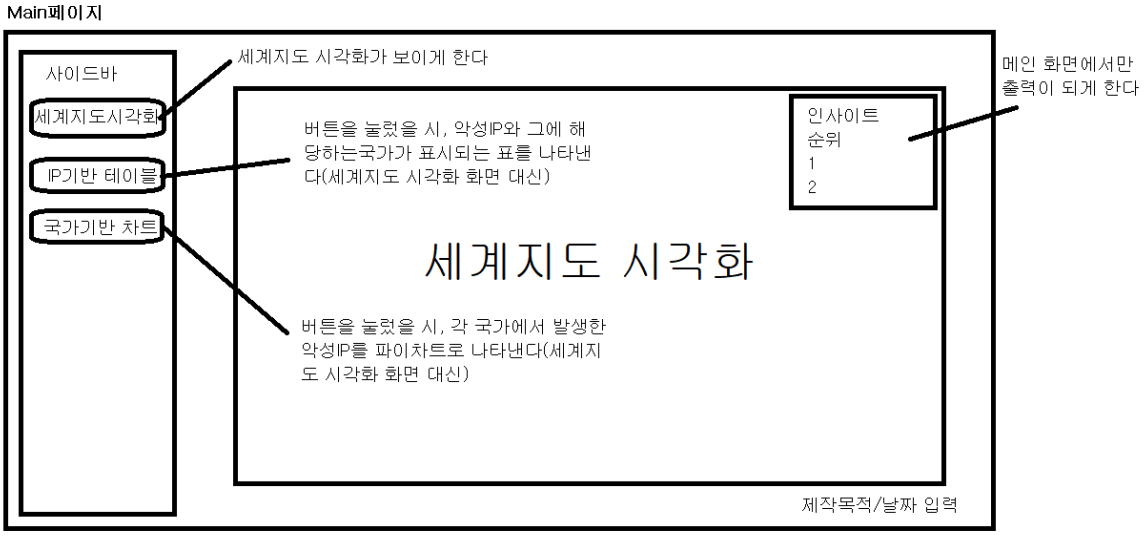
a. 프로젝트 목표

- 시각화에 필요한 csv파일 데이터를 Python으로 전처리를 하여 필요한 데이터를 가지고 악성IP 유입 현황을 시각화 하는 페이지를 구축한다.
- DB를 사용하지 않으므로 각 시각화에 필요한 데이터를 따로 전처리 한 후 사용한다.
- 사이드 바의 버튼을 클릭하여 시각화 페이지를 iframe으로 화면에 출력한다.
- 통계를 통해 알 수 있는 위험순위를 한 눈에 파악할 수 있는 인사이트를 출력한다.
- 사이드 바의 버튼에 호버 기능을 추가하여야 하며 사이드 바가 비어 보이지 않도록 해야 한다..

b. 요구 사항

- Web기반 환경 구성(Apache + Tomcat)
- 데이터 구성 방식 및 처리 기준 지침 작성(데이터 전처리 기준 작성)
- 서비스 구성 기획 문서 필수 작성
- WBS 작성 및 화면설계서 필수 작성
- 전체 통계 세계지도 기반 시각화
- 관련 통계 지표를 시각화(IP주소 기반, 국가기반 통계)
- 주요 산출물 관리 및 코드 관리(Github, Redmine등)
- 최종 결과 보고서 제출
- IP기반 표 형식으로 표현할때 나라별로 국기도 추가하면 좋을듯함
- 메인페이지 순위표(인사이트)에 차트로 표시하면 데이터 값을 레이블로 표시할 것
- R&R에서 Role별로 소항목 구성하고 페이지 구현 및 테스트 또한 각 Role별로 소항목 구성해서 관리할 것
- 사이드바에 호버기능 추가
- 기능을 더 추가하여 사이드바가 비어보이지 않게 설계
- 5시 방향에 만든 날짜 및 목적 bottom부분에 추가해줄 것(저작권 이슈 해결하기 위함)

c. 목업

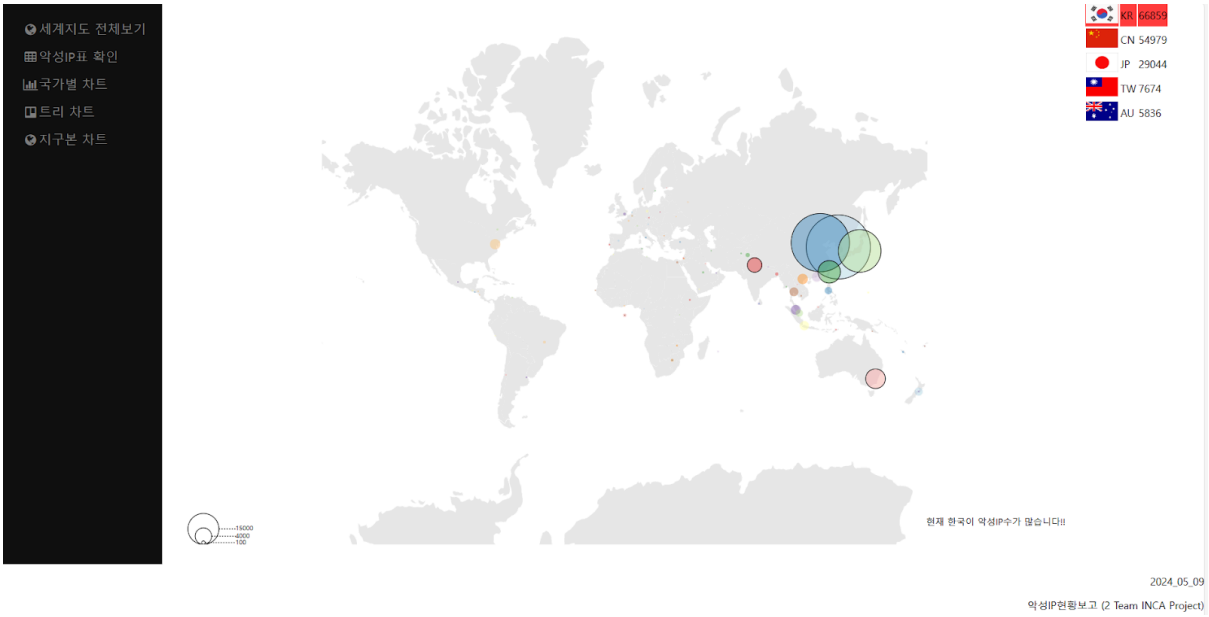


d. 프로젝트 일정

- 2024년 4월 17일 수요일 ~ 2024년 5월 16일 목요일
- 주요 일정
  - 2024년 4월 21일 : 요구사항, 서비스 기획, 기능 명세 작성 완료
  - 2024년 4월 22일 : 역할 분배(R&R) 완료
  - 2024년 4월 29일 : 데이터 전처리 작업 완료
  - 2024년 5월 2일 : 세계지도 시각화 작업 완료
  - 2024년 5월 3일 : 국가기반 파이차트 작업 완료
  - 2024년 5월 13일 : 개발 및 테스트 완료
  - 2024년 5월 9일 : 악성IP 테이블 작업 완료
  - 2024년 5월 10일 : 인사이트, 트리맵, 지구본 작업 완료
  - 2024년 5월 13일 : 메인 페이지 작업 완료 및 테스트 완료

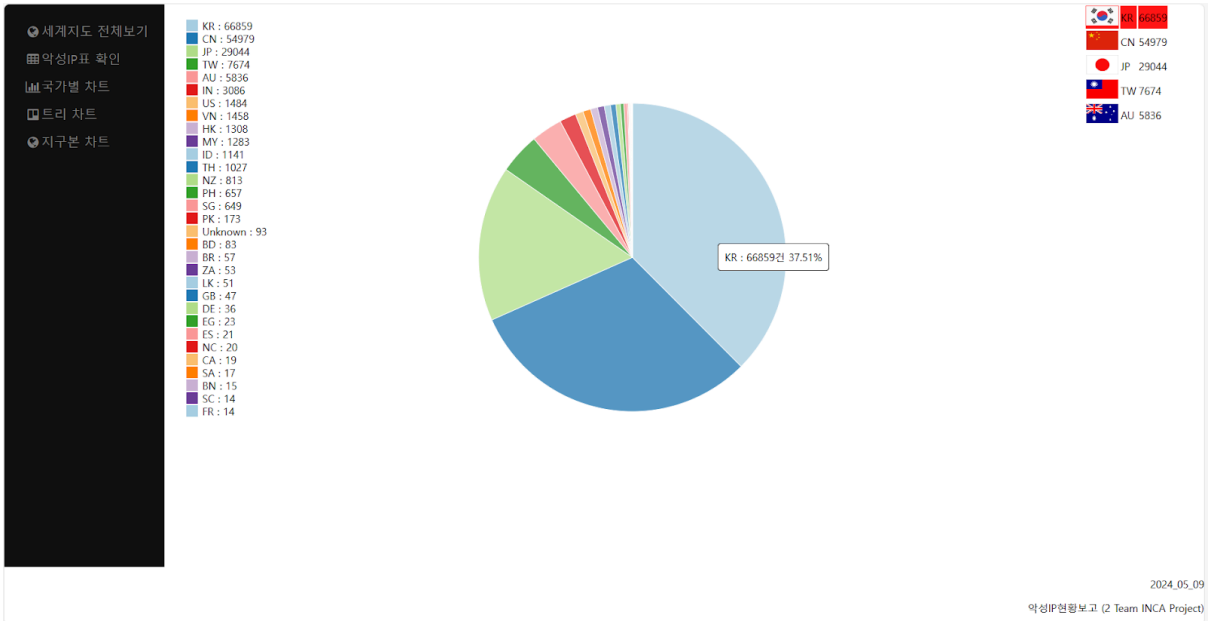
e. 프로젝트 결과

- 메인 페이지

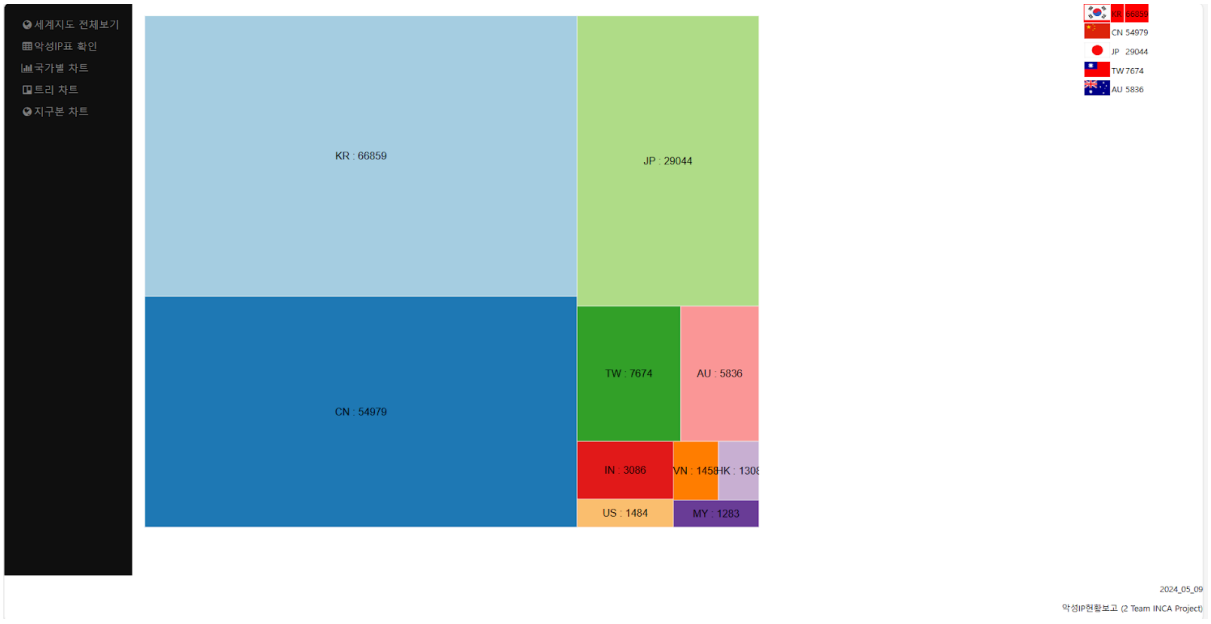


- 악성 IP 테이블

- 파이 차트


세계지도 전체보기
악성IP표 확인
국가별 차트
트리 차트
지구본 차트
KR : 66859
CN : 54979
JP : 29044
TW : 7674
AU : 5836
IN : 3086
US : 1484
VN : 1458
HK : 1308
MY : 1283
ID : 1141
TH : 1027
NZ : 813
PH : 657
SG : 649
PK : 173
Unknown : 93
BD : 83
BR : 57
ZA : 53
LK : 51
GB : 47
DE : 36
EG : 23
ES : 21
NC : 20
CA : 19
SA : 17
BN : 15
SC : 14
FR : 14
KR : 66859건 37.51%
KR 66859
CN 54979
JP 29044
TW 7674
AU 5836
2024_05_09
악성IP현황보고 (2 Team INCA Project)

- 트리 차트


세계지도 전체보기
악성IP표 확인
국가별 차트
트리 차트
지구본 차트
KR : 66859
JP : 29044
CN : 54979
TW : 7674
AU : 5836
IN : 3086
VN : 1458
US : 1484
MY : 1283
CN 54979
JP 29044
TW 7674
AU 5836
2024_05_09
악성IP현황보고 (2 Team INCA Project)

- 지구본 차트


세계지도 전체보기
악성IP표 확인
국가별 차트
트리 차트
지구본 차트
KR 66855
CN 54979
JP 29044
TW 7674
AU 5836
2024_05_09
악성IP현황보고 (2 Team INCA Project)

3. 결론

a. 결과 분석

- 악성 IP 국내 유입 현황을 국가별로 나타낸 결과 1위는 한국, 2위는 중국, 3위는 일본으로 주로 동아시아 국가에서 압도적인 발생 비율을 보입니다.
- 주된 요인으로 동아시아 국가들의 전반적인 높은 인터넷 보급률 및 속도, 동아시아 지역의 악성 커뮤니티 활성화 및 국가간 경제적 중요도, 이에 비에 상대적으로 낮은 보안 시스템의 취약성을 토대로 방대한 인프라와 그에 대비되는 보안의식 저하가 동아시아 국가들의 악성 IP 발생 빈도의 주요인으로 볼 수 있습니다.
- 따라서 국가간의 긴밀한 사이버 관계 및 시스템을 구축하고 정부와 민간 부문이 협력하여 보안의식을 제고하는 것이 문제 해결의 방안으로 보입니다.
- 프로젝트의 결과물을 통하여 다양한 시각화 차트를 통해 악성IP의 유입 현황을 파악할 수 있습니다.
- 많은 양의 데이터를 처리하는 코드를 작성하거나, DB를 사용하여 데이터를 처리하는 것이 기능성을 높일 수 있을 것이라고 생각합니다.

b. 문제점 분석

- csv파일을 그대로 불러와 시각화를 하려고 하였으나 데이터를 읽어오지 못하고 다운로드 되는 문제로 인해 json형태로 바꾸어 시각화를 하였습니다.

- 차트와 데이터 테이블을 같이 볼 수 없기 때문에 불편함이 있습니다.

- DB를 사용하지 않고 18만개의 데이터를 읽어와 테이블로 시각화 하는 과정에서 페이지에 부하가 생겨 데이터의 수를 2만개로 줄여 출력하였으나, 데이터를 국가 이름순으로 정렬하는 과정에서 부하가 한번 더 생겨 작동하지 않습니다.

- 지구본 다트 차트에서 땅에 대한 데이터에는 색 변경이 가능하지만 바다에 대한 데이터에는 색 변경이 이루어지지 않아 시인성이 저하되었습니다.

- 지구본 다트 차트에서 악성 IP의 버블 크기를 줄임과 동시에 회전하여 해당하는 국가가 보이지 않을 시 출력이 안되게 하는 범위를 수정하였으나 한 지점이 이상하게 표시되는 문제점이 있습니다.

- 트리 차트를 시각화 하는 과정에서 악성IP 유입 빈도가 적은 국가의 텍스트를 처리하지 못하여 데이터 수를 조정 하였으나 여전히

텍스트가 겹치는 문제 발생했습니다.

- 데이터가 제일 많은 2020년의 데이터만을 이용하여 구현하였으므로 월 별로 데이터를 분류하여 볼 수 없었습니다.

4. 고찰

a. 프로젝트 평가

- 프로젝트를 수행하며 전처리 과정, D3코드 수정과정, 데이터 테이블 작성 과정에서 예상하지 못한 문제가 발생하였습니다. 일부는 해결했지만 해결되지 못한 부분이 여전히 있어 수정 보완이 필요한 상태입니다. 결과물은 부족하지만 이번 프로젝트를 진행하면 다양한 방법으로, 작업을 했고 새로운 기술을 익힐수 있었습니다. 또한 실무와 동일한 프로젝트 과정을 경험하면서 실무에 대한 이해도가 향상 되었다 생각됩니다. 특히 각자 R&R을 부여하여 역할 분담에 충실 할 수 있었고, WBS를 작성함으로 스케쥴을 관리하는 방법을 알게 되었습니다.