OSINT 활용한 공급망 위협정보

2024. 09. 10.

ΣxWareLab

I am...

ExWareLabs

- 현 익스웨어랩스 (ExWareLabs) 운영자
- 현 ㈜한국정보보호교육센터(KISEC) 교수연구부 수석연구원
- 전 ㈜에이쓰리시큐리티 모의해킹 수행팀장

하는 또는 했던 일

- 관련분야 경력 : 23년
- 강의분야: 사이버 해킹, Penetration Test, OSINT, Cyber Threat Intelligence
- 보안교육: 경찰청 사이버수사대 대상 정보보호 강의 다수
- 보안컨설팅: 금융회사 外 기업 모의해킹 다수
- Email : coderant@fngs.kr, coderant@nate.com
- ExploitWareLabs 운영자
  https://www.facebook.com/ExWareLabs/

목차

[OSINT-Driven 공급망 위협(Supply Chain Threat)]

- **OSINT 정보 탐색**
- **OSINT를 활용한 공급망 위협정보 사례**

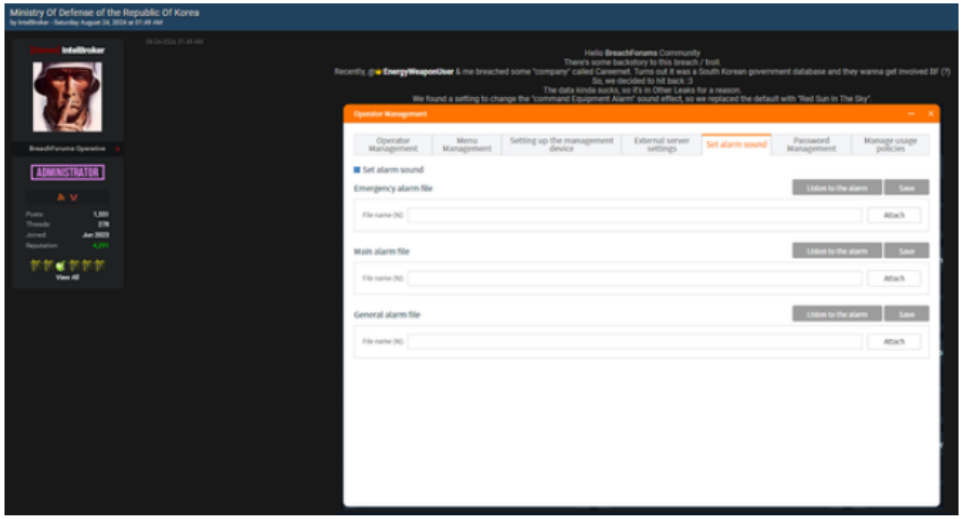
OSINT-Driven 공급망 위협(Supply Chain Threat)

최근 사이버 공급망(Cyber Supply Chain)을 통한 정보 유출이 기업의 가장 큰 보안이슈로 대두하고 있으며 근본 원인은 보안이 취약한 협력업체 시스템인 경우가 많음

사이버 공급망 생태계에서 사건사고

➢ **대표적인 사이버 공급망을 통한 해킹사고**

▶ **IntelBroker에 의한 국방부 관련 민감 정보 유출사건 - 재난안전통신망 테스트베드**



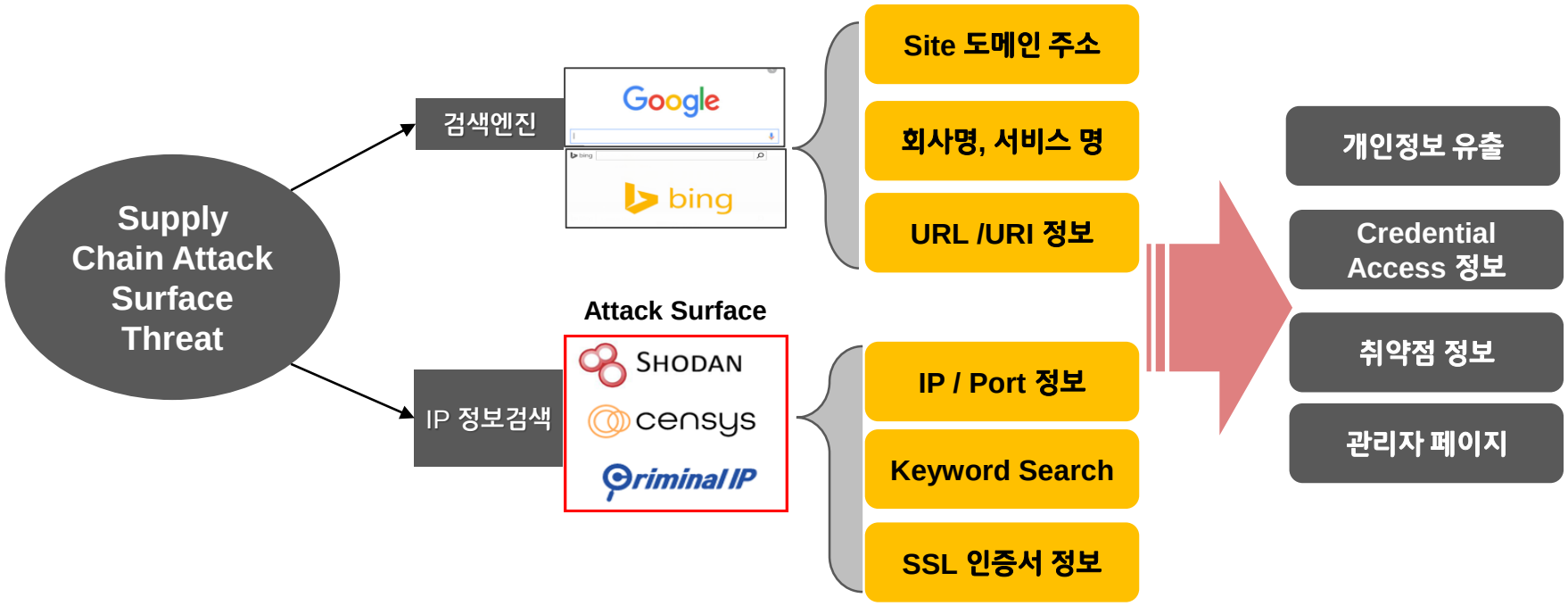
해커는 국방부와 해양경찰청 등의 내부 데이터에 접근하는 데 성공했다고 주장했다. 사진=해킹포럼

OSINT-Driven 공급망 위협(Supply Chain Threat)

기업/기관의 정보가 사이버 공급망을 통해 유출되는지 여부를 모니터링하는 방법론으로 OSINT를 주목을 받고 있음

사이버 공급망 위협정보 검색 방법

➢ **OSINT 기반의 Supply Chain Threat 정보 탐색방법론**

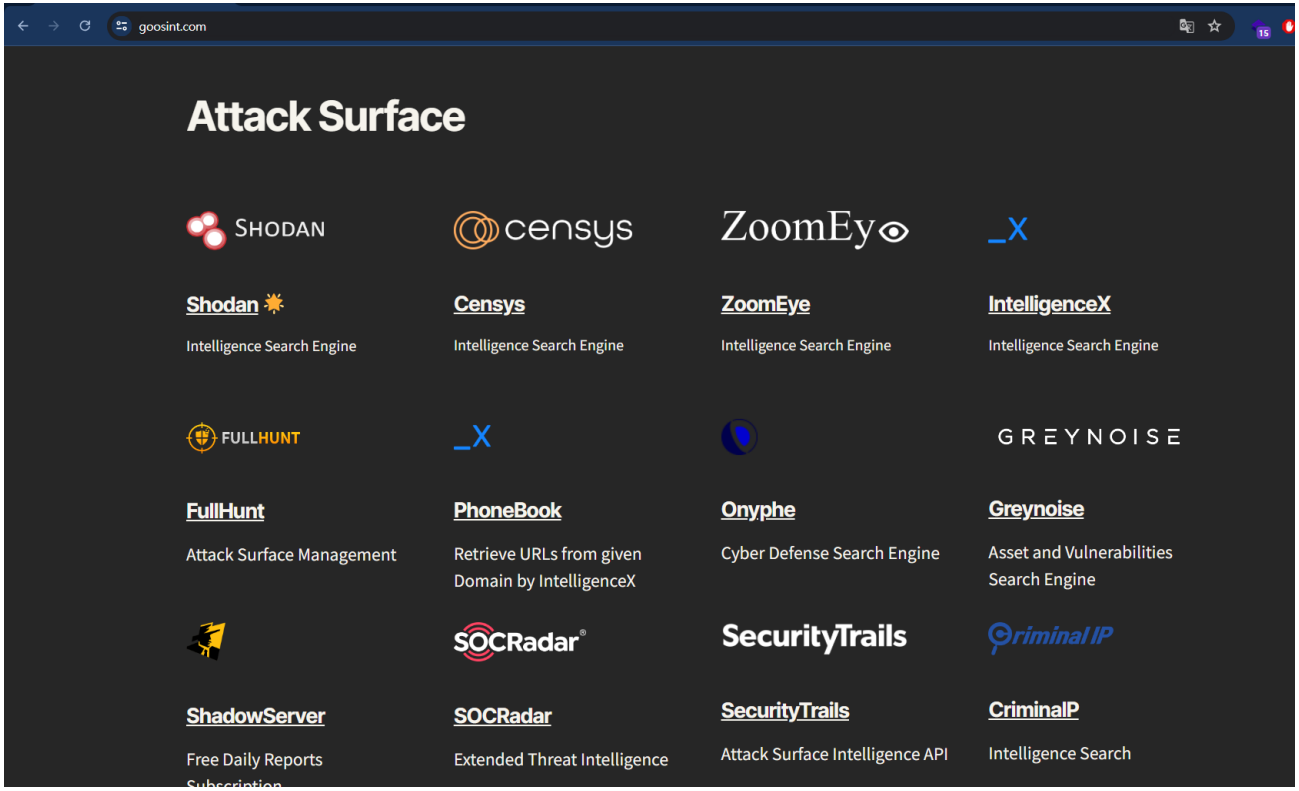


OSINT-Driven 공급망 위협(Supply Chain Threat)

사이버 범죄자들도 OSINT 방식을 활용하여 해킹 공격 Target 대상 정보를 수집합니다.

OSINT 정보 탐색을 위한 기본 지식

➢ **주요 OSINT 정보수집 도구 – Attack Surface Tools**



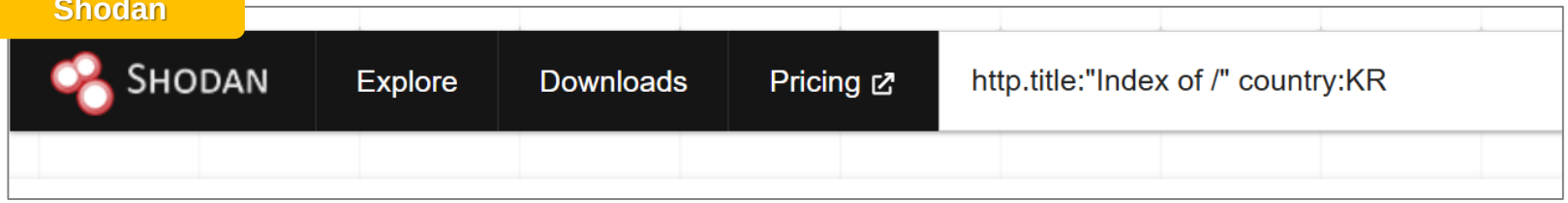
OSINT-Driven 공급망 위협(Supply Chain Threat)

대표적인 웹 취약점인 디렉터리 리스팅 사이트에서 공급망 위협 정보를 찾을 수 있음

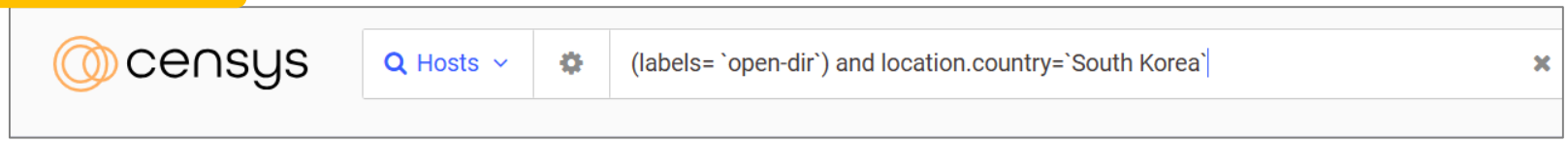
OSINT 정보 탐색을 위한 기본 지식

- **OSINT 검색도구 – IP 정보수집 검색엔진**
  - IP 정보 검색엔진에서 국내(KR) 대상으로 디렉터리 리스팅 취약점 IP 정보

Shodan



Cenasys



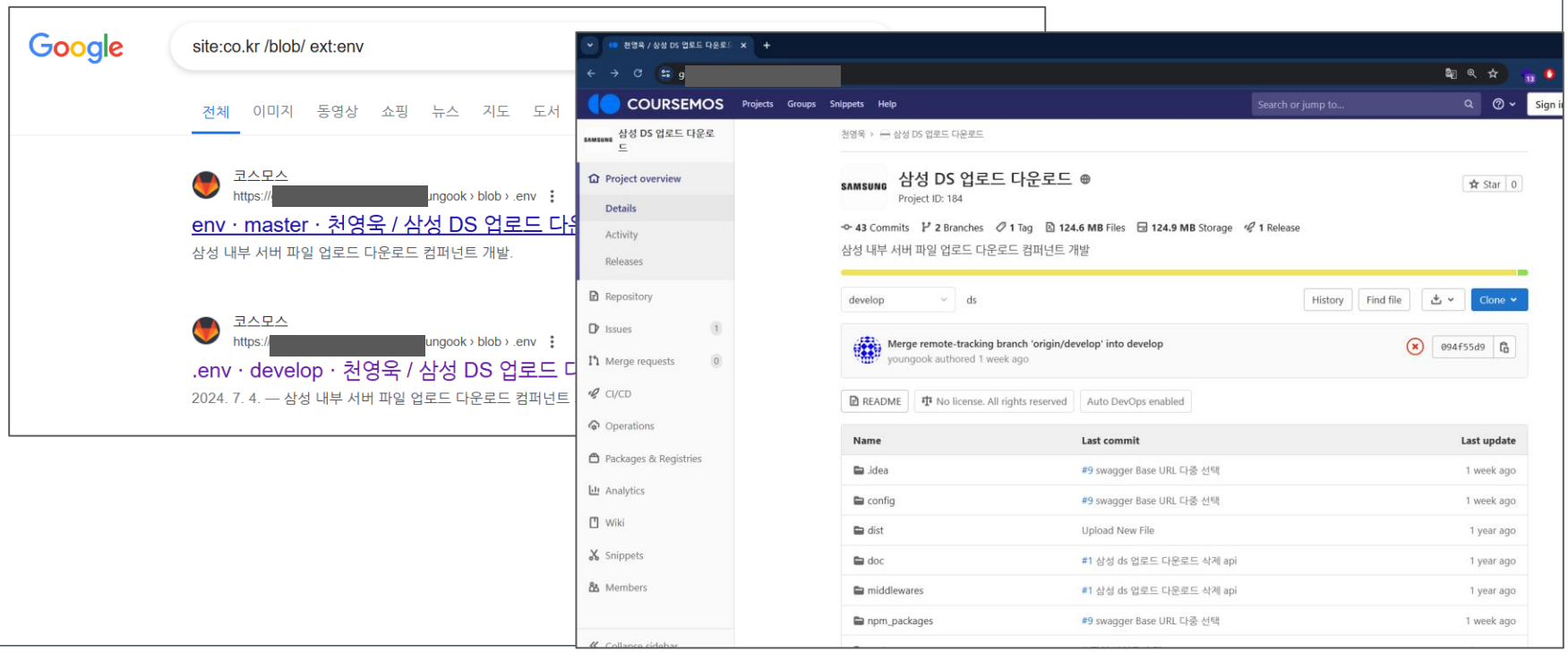
Criminal IP

OSINT-Driven 공급망 위협(Supply Chain Threat)

구글 검색에서 소스코드 저장소 대상으로 특정 정보를 검색하는 방법

OSINT 정보 탐색 - 구글 검색

- **구글 검색에서 환경변수(env) 검색**
  - **gitlab, github 등 소스코드 저장소에서 정보 검색**



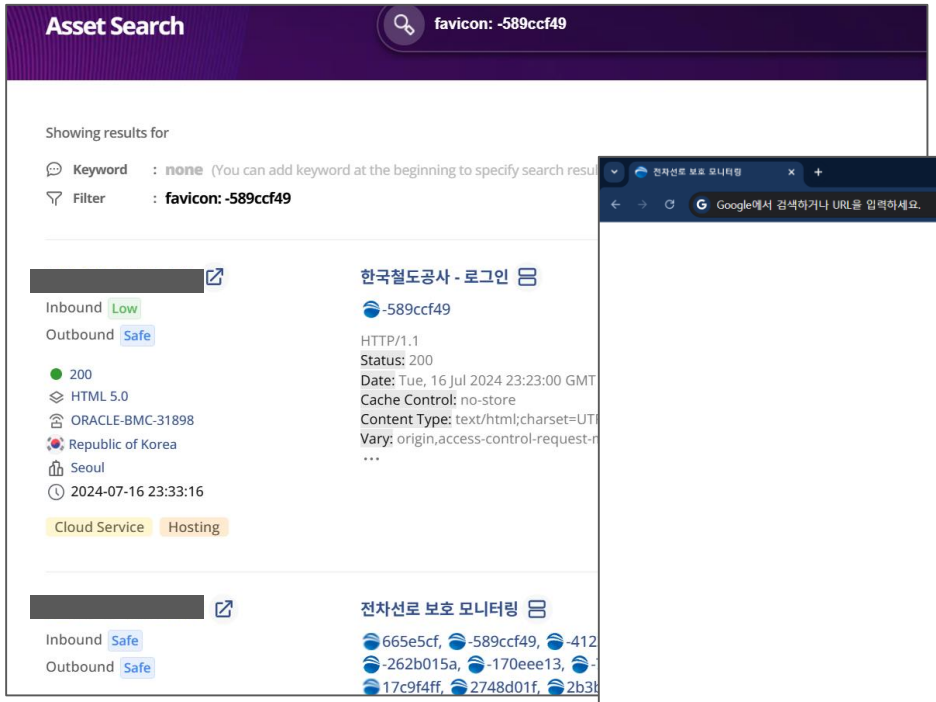
OSINT-Driven 공급망 위협(Supply Chain Threat)

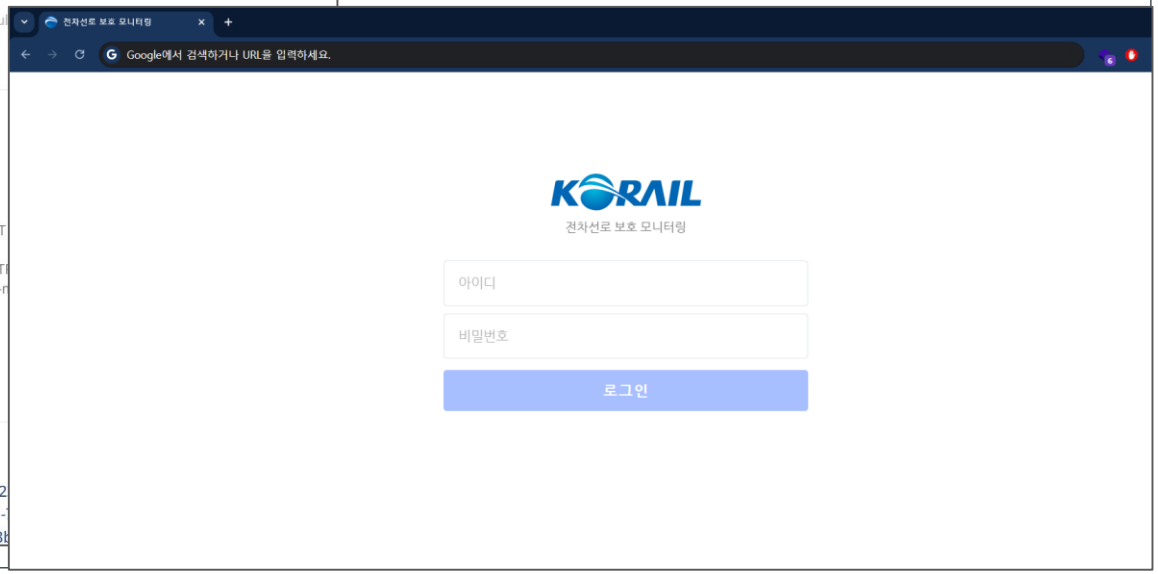
웹사이트 파비콘(favicon.ico) 이미지 해시값을 이용해서 특정 대상을 검색하는 방법

OSINT 정보 탐색 - 파비콘(Favicon)

➢ 특정 웹사이트 검색방법 – 파비콘(favicon)

▶ 파비콘(favicon) 해시값을 활용한 대상 정보자산 검색





OSINT를 활용한

공급망 위협 정보 탐지사례

공급망 위협정보 사례

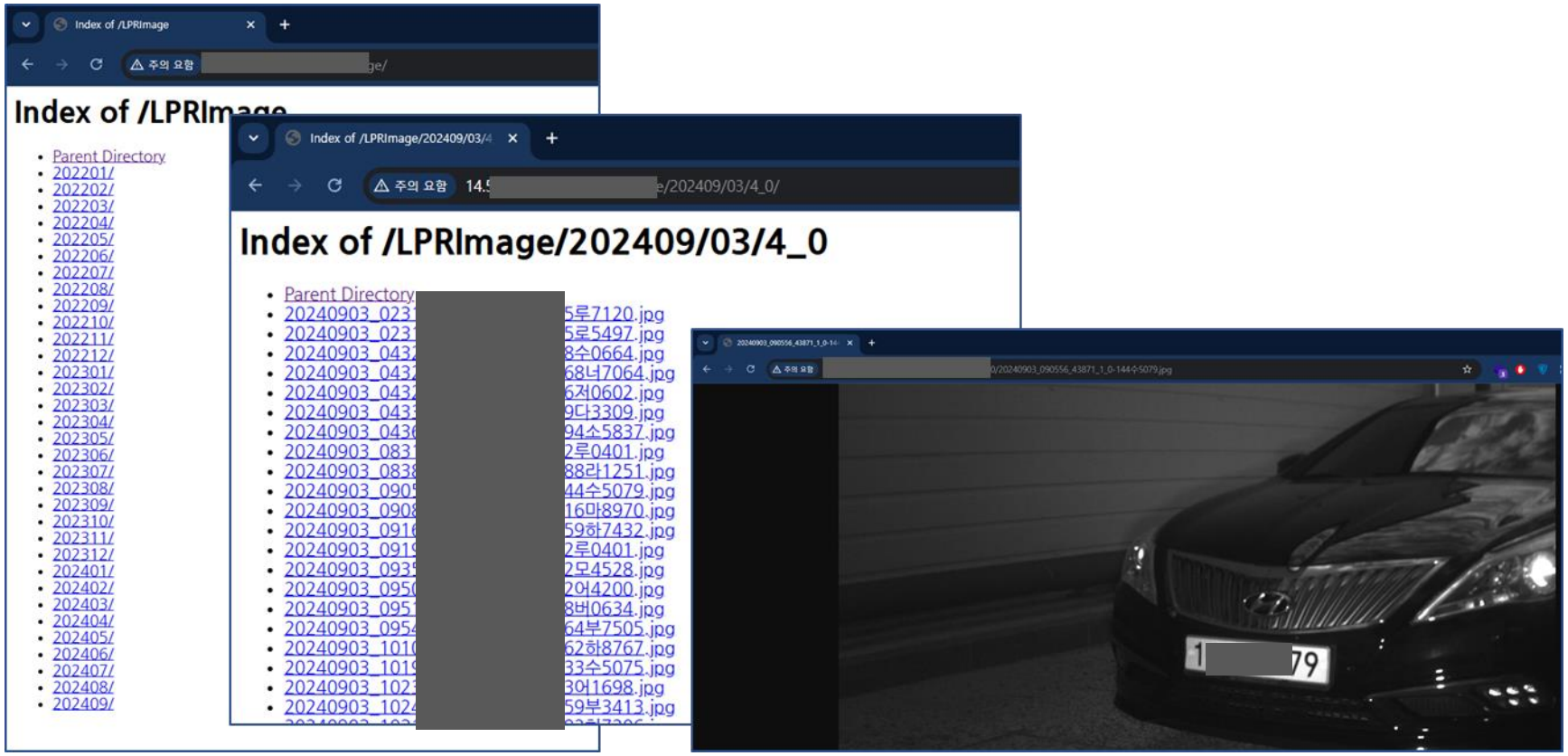
ExWareLab

OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 민감 정보 유출

➢ Directory Listing 취약 사이트 – 차량 개인정보

▶ 주차관리시스템의 차량번호 인식기 시스템(LPM) – 차량번호 등 민감정보 유출

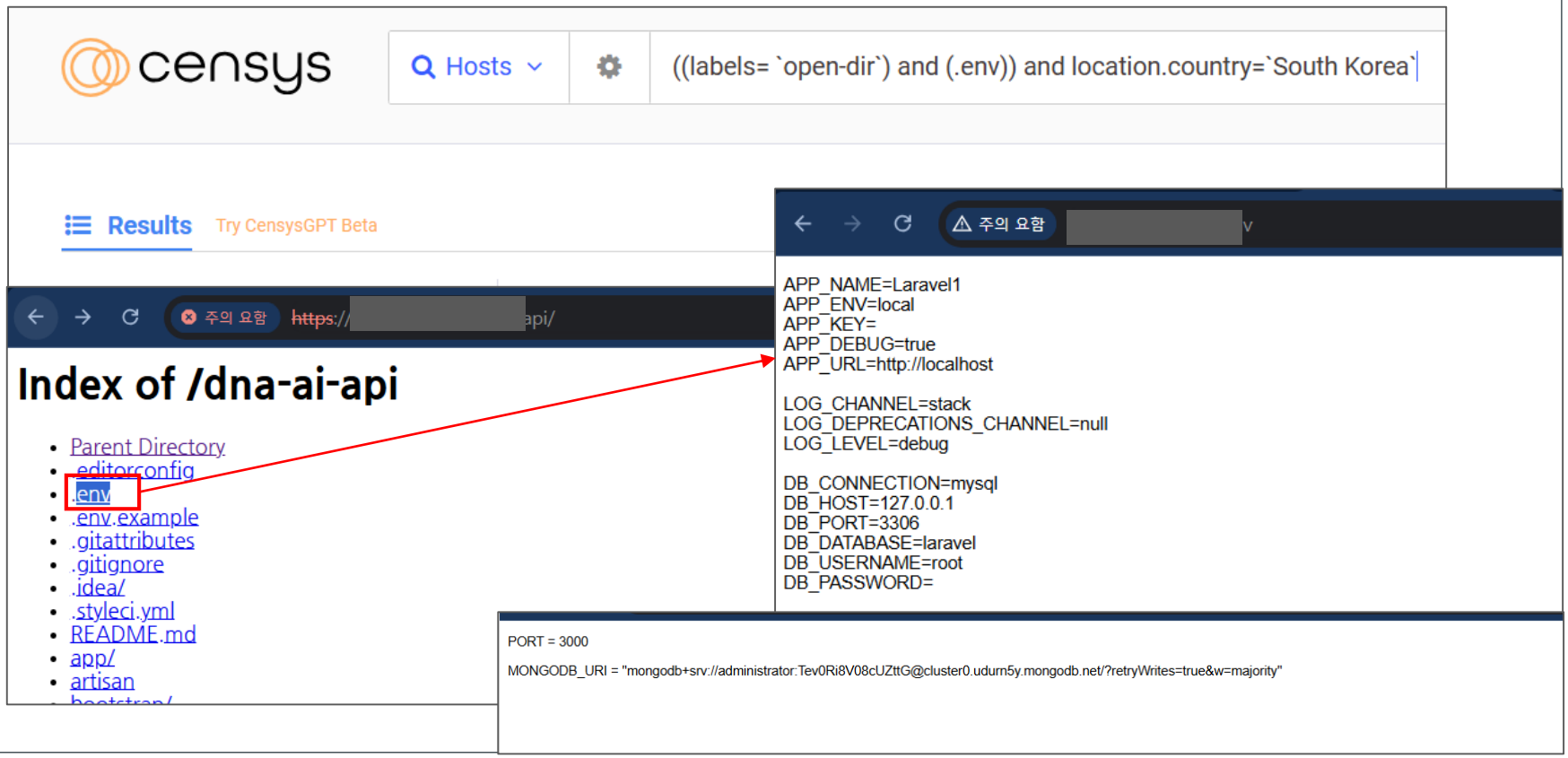


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 민감 정보 유출

➢ Directory Lising 취약 사이트 – 환경변수(.env) 찾기

▶ 환경변수 .env 파일에는 민감한 Access Key, DB 계정/패스워드 정보가 있음

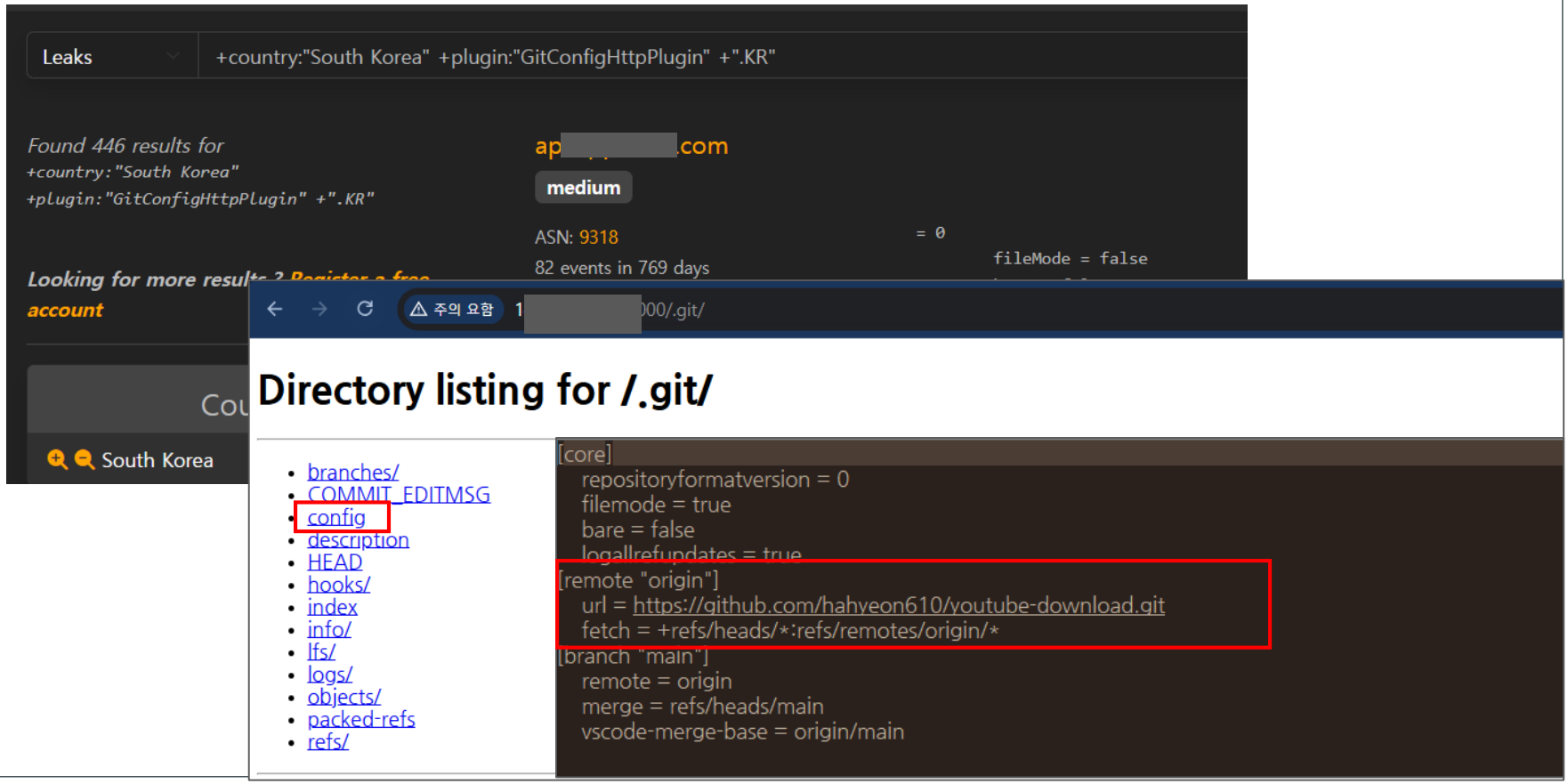


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 민감 정보 유출

➢ Directory Lising 취약 사이트 – 소스코드 저장소(.git) 찾기

▶ .git 파일에는 원격 소스코드 저장소 정보가 있음

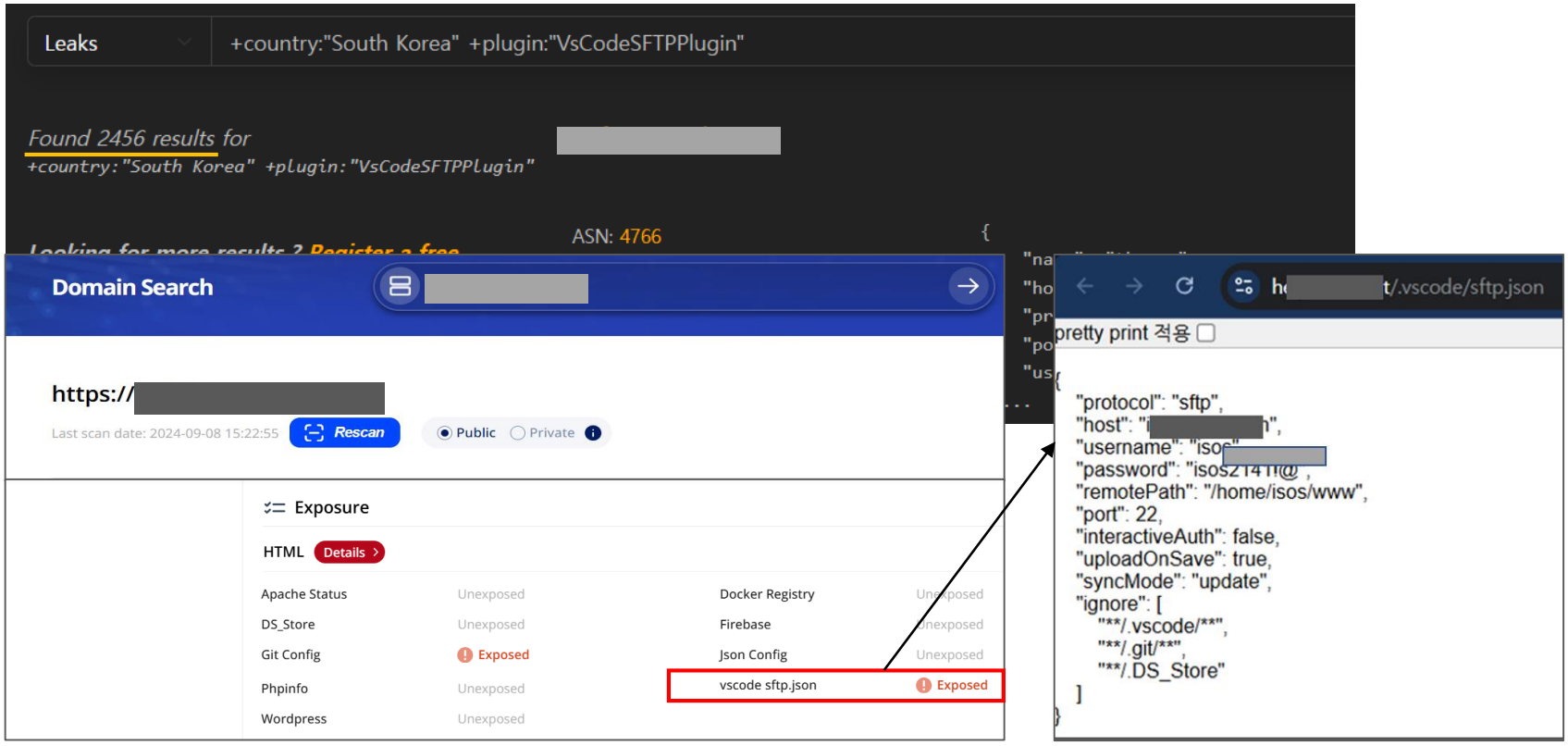


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 민감 정보 유출

➢ SSH 접속계정 정보 탈취

▶ .vscode/sftp.json 파일이 웹 경로에서 접근 가능 시 SSH 계정 정보를 담고 있었으며 공격자가 SSH 계정 정보를 탈취당할 수 있음

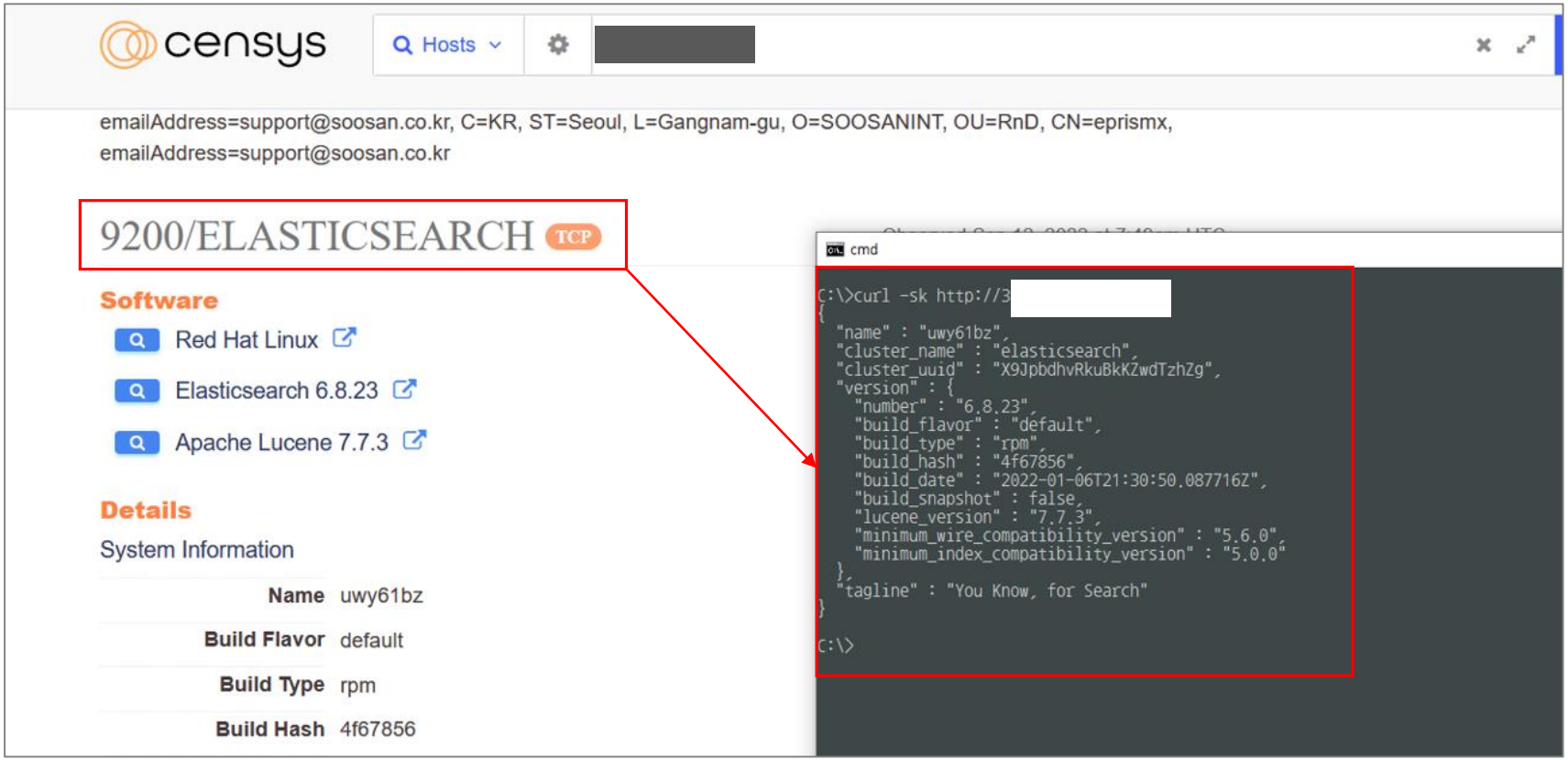


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 민감 정보 유출

➢ 국내 보안솔루션 소프트웨어 공급망 위협 정보

▶ 보안장비에서 노출된 오픈소스 DB (Elastic Search) 사례

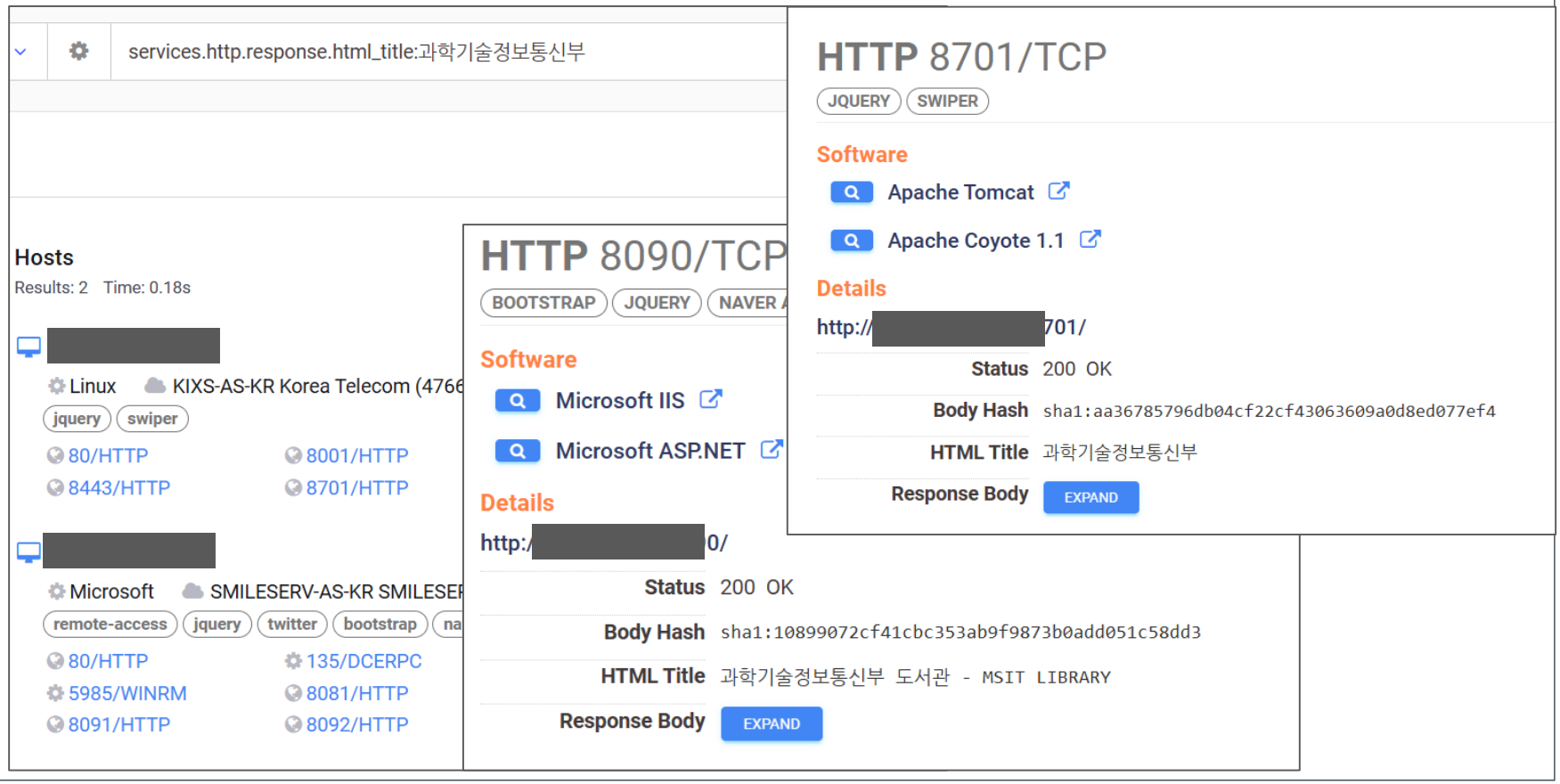


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 개발 시스템

➢ IP 정보수집 도구 OSINT 도구(Censys) – HTML 제목으로 사이트 검색

▶ 행정기관명이 포함된 HTML Title로 개발 시스템 정보검색

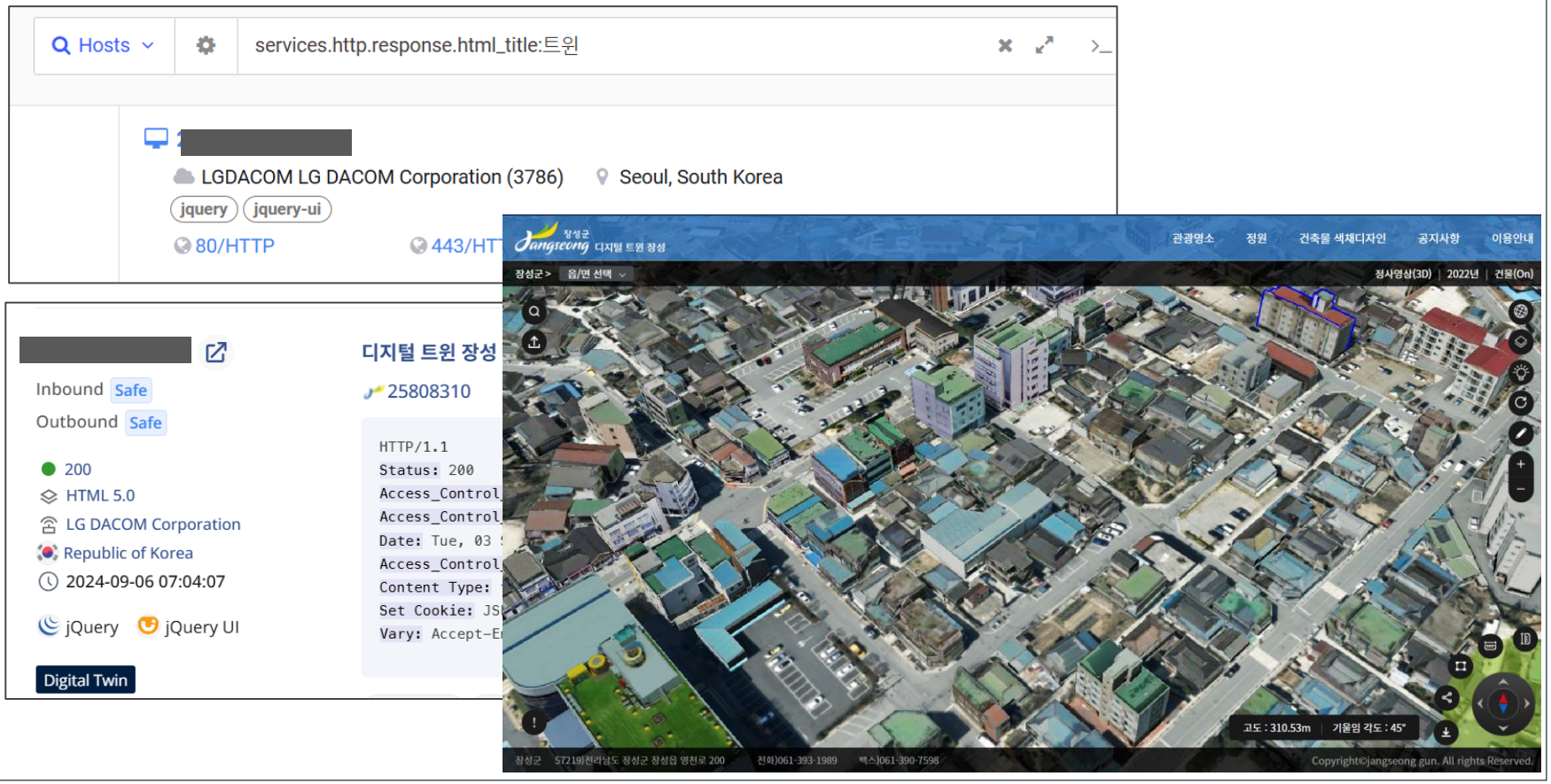


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 - 개발 시스템

➢ 공공기관의 디지털 트윈 기술을 활용한 개발 사이트

▶ 공공행정기관의 '디지털 트윈' 관련 검색

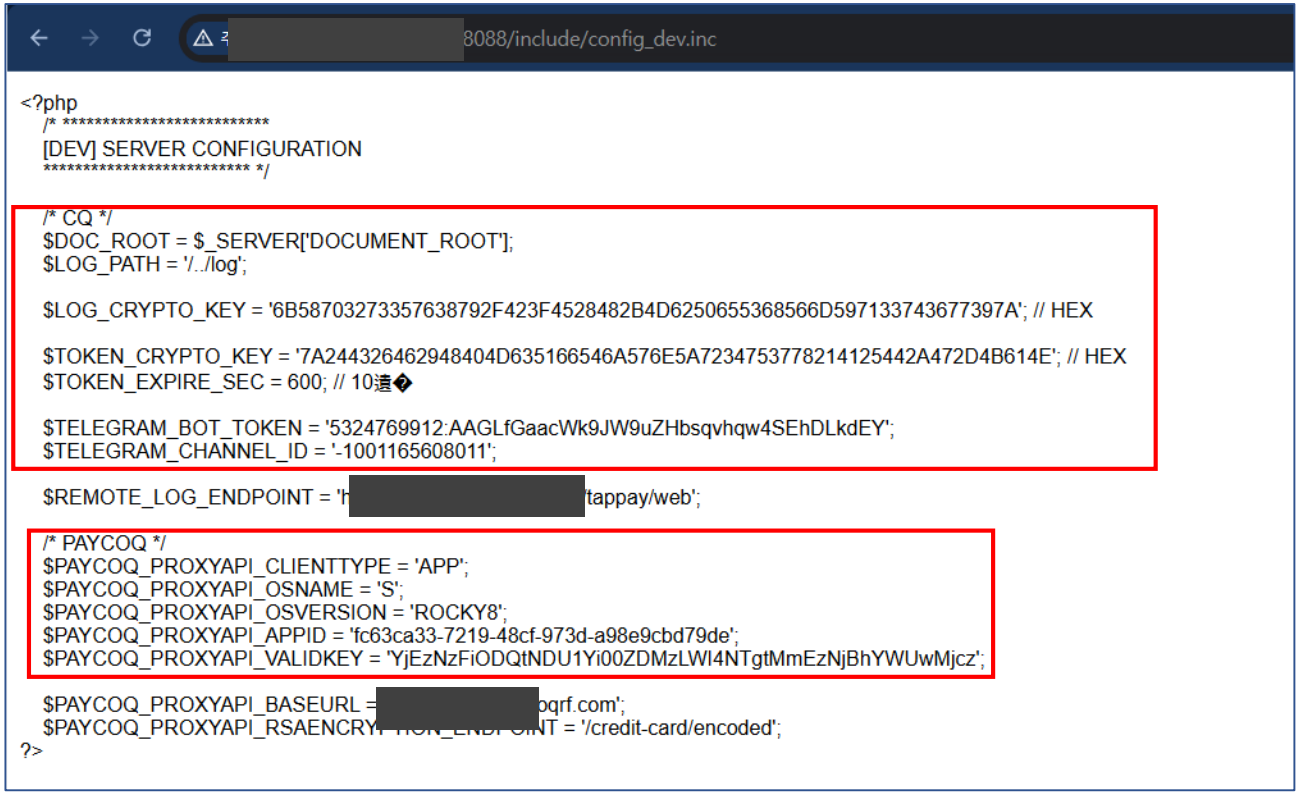


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 개발 시스템

➢ ARS 솔루션 업체의 개발서버 노출 위협

▶ 민감한 서버처리 파일이 노출되는 최악의 케이스

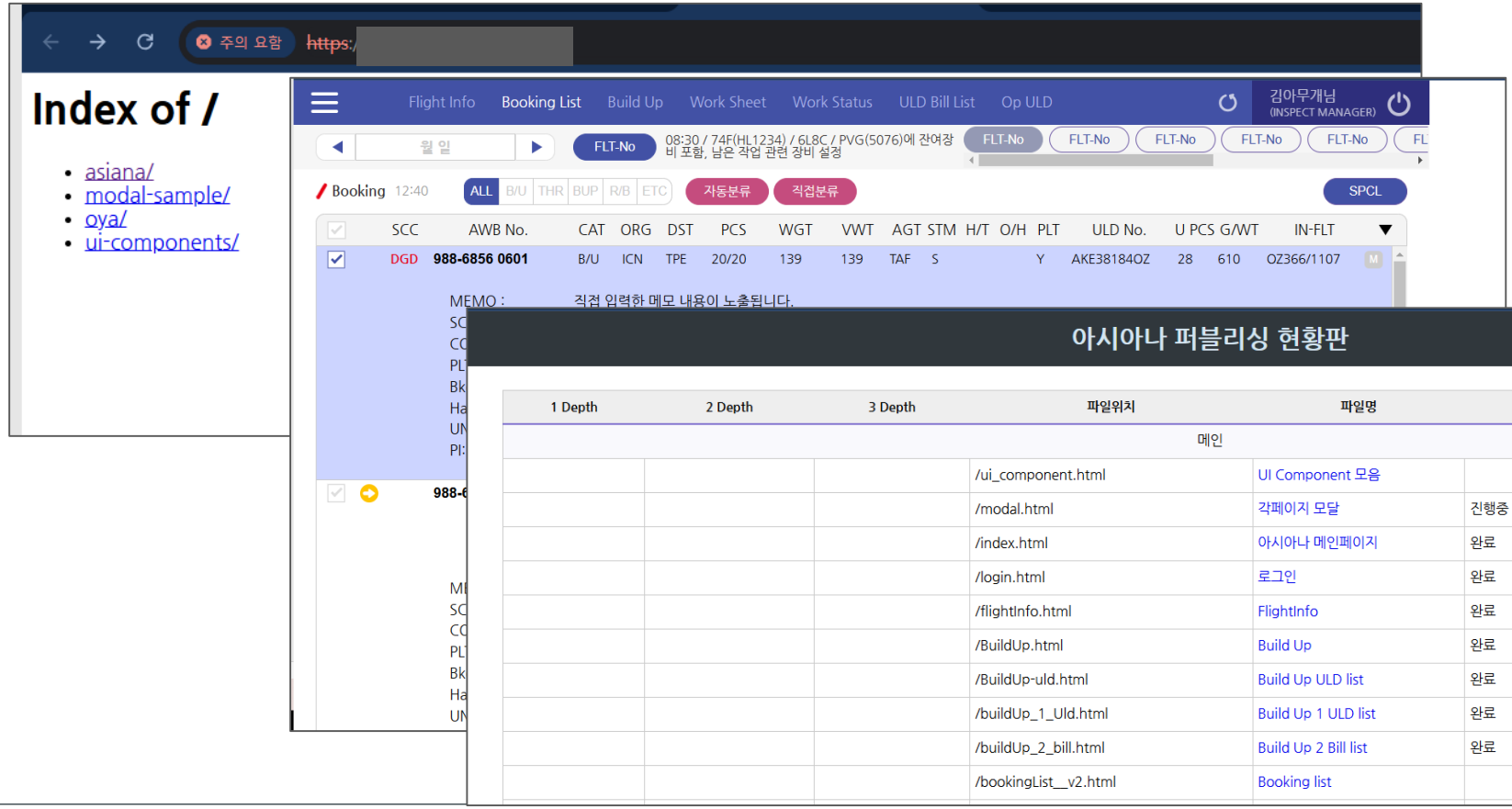


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 개발 시스템

➢ 웹 개발 퍼블리싱 사이트 정보검색

▶ 디렉터리 리스팅 + 웹퍼블리싱 사이트를 통해 기업 정보탐색



아시아나 퍼블리싱 현황판

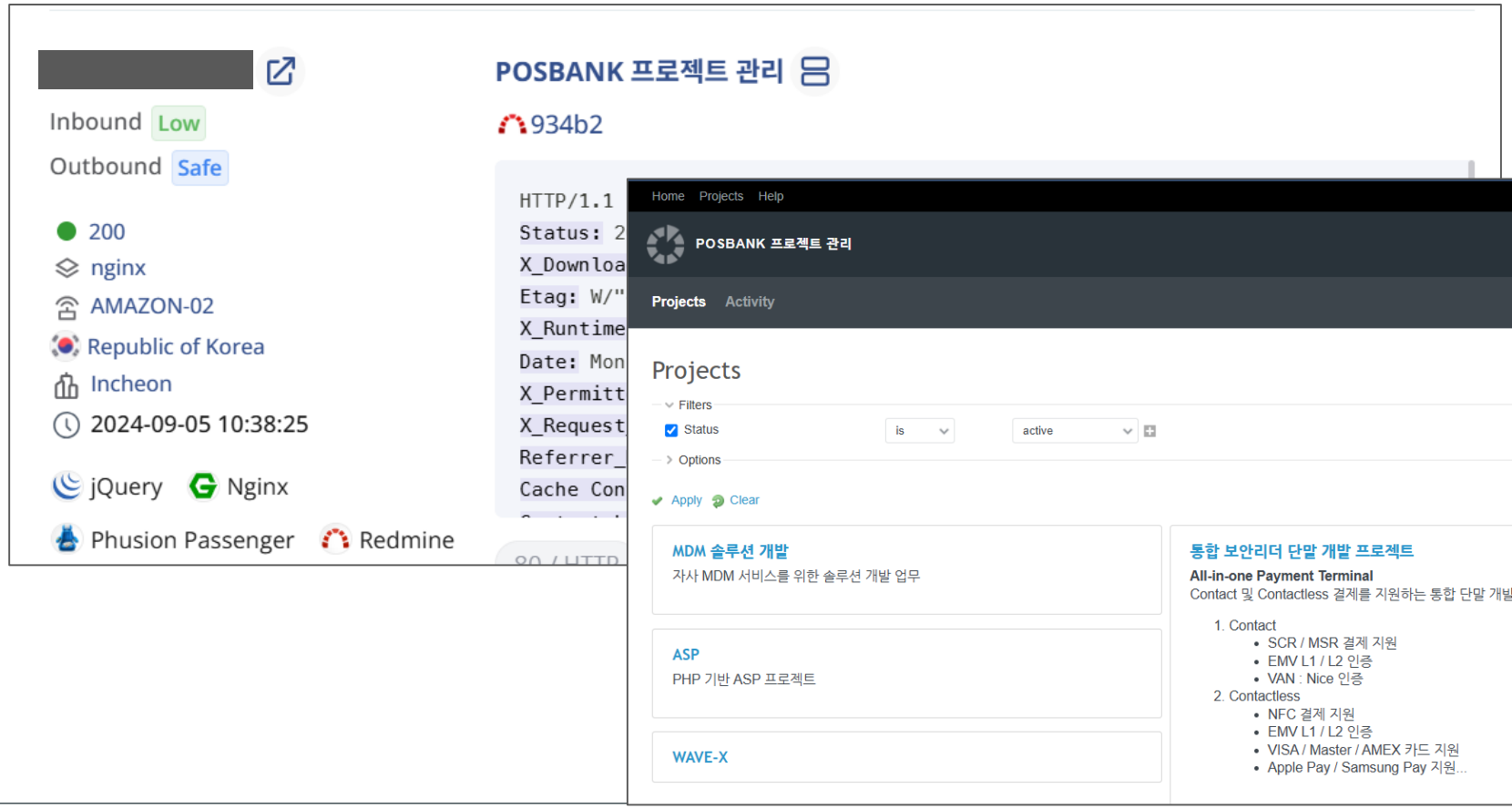
1 Depth	2 Depth	3 Depth	파일위치	파일명	상태
메인					
			/ui_component.html	UI Component 모음	
			/modal.html	각페이지 모달	진행중
			/index.html	아시아나 메인페이지	완료
			/login.html	로그인	완료
			/flightInfo.html	FlightInfo	완료
			/BuildUp.html	Build Up	완료
			/BuildUp-uld.html	Build Up ULD list	완료
			/buildUp_1_Uld.html	Build Up 1 ULD list	완료
			/buildUp_2_bill.html	Build Up 2 Bill list	완료
			/bookingList__v2.html	Booking list	

OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 개발 시스템

➢ 개발 프로젝트 관리시스템 (Project Management Sysetm)

▶ 파비콘(favicon)으로 프로젝트 관리시스템 찾기

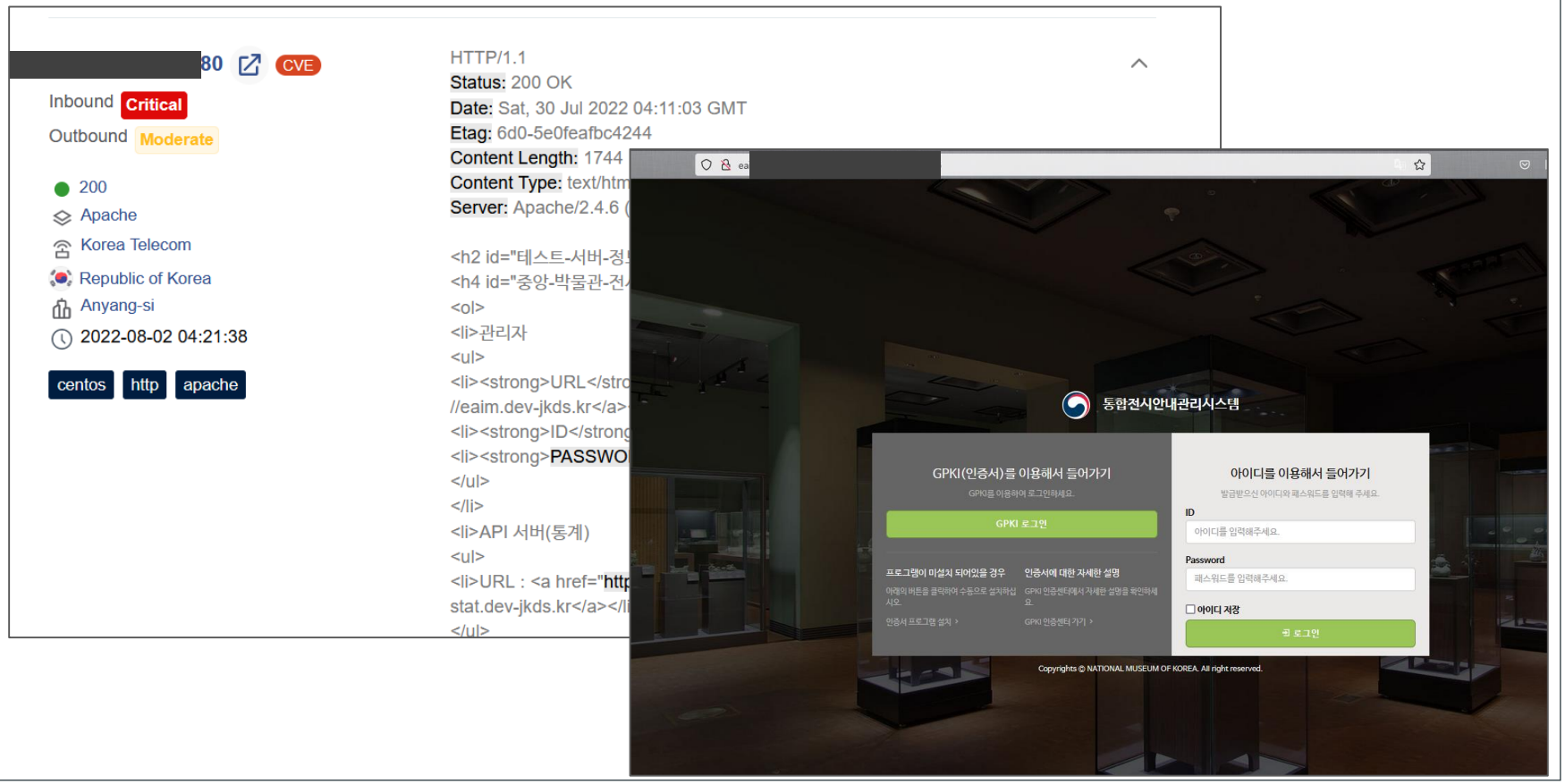


OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 유지보수 시스템

➢ 외부 유지보수 협력업체 서버을 통한 서버 민감 정보 노출

▶ 한국중앙박물관 개발시스템에서 서버 접속 계정정보 노출



OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 유지보수 시스템

➢ 외부 유지보수 협력업체 서버을 통한 서버 민감 정보 노출

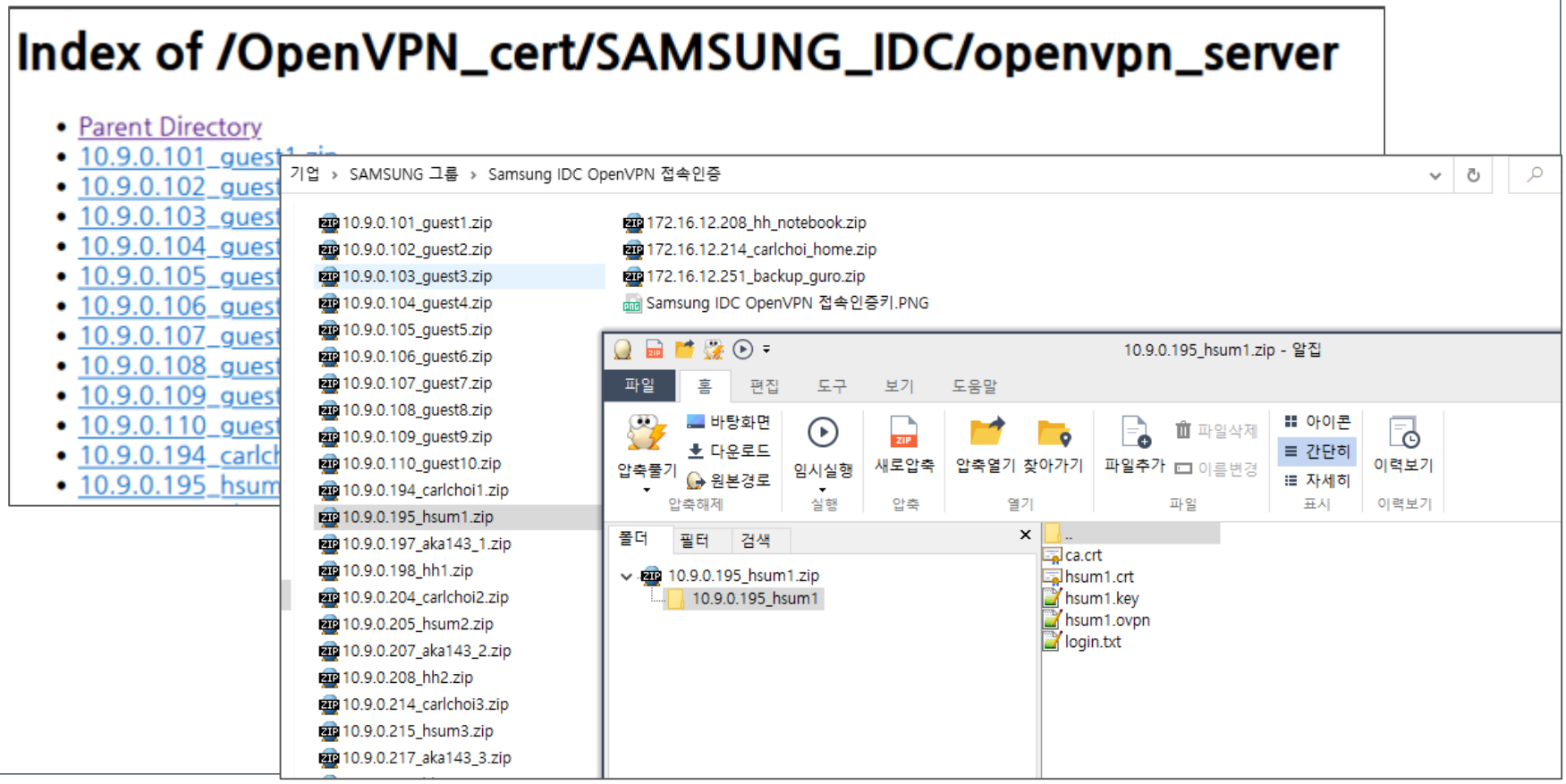
▶ 행정기관 주민센터 서버 계정 및 패스워드 정보노출 (전산시스템 운영 유지보수 업체)

OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 – 유지보수 시스템

➢ 외부 유지보수 협력업체 서버에서 VPN 계정정보 노출

▶ 유지보수 업체에서 운영하는 서버에서 IDC 접속용 OpenVPN 접속 계정 노출



- 결론 -

공급망 위협 정보 노출 기업, 기관들의 지속적인 모니터링으로 해결할 수 밖에 없다.