



OSINT 활용한 공급망 위협정보

2024. 09. 10.

I am...



ExWareLabs

- 현 익스웨어랩스 (ExWareLabs) 운영자
- 현 (주)한국정보보호교육센터(KISEC) 교수연구부 수석연구원
- 전 (주)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 외 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



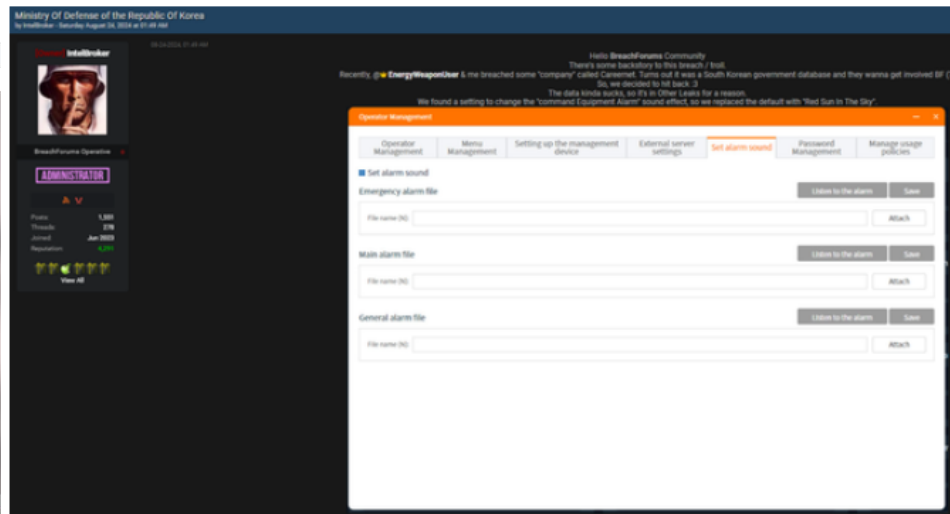
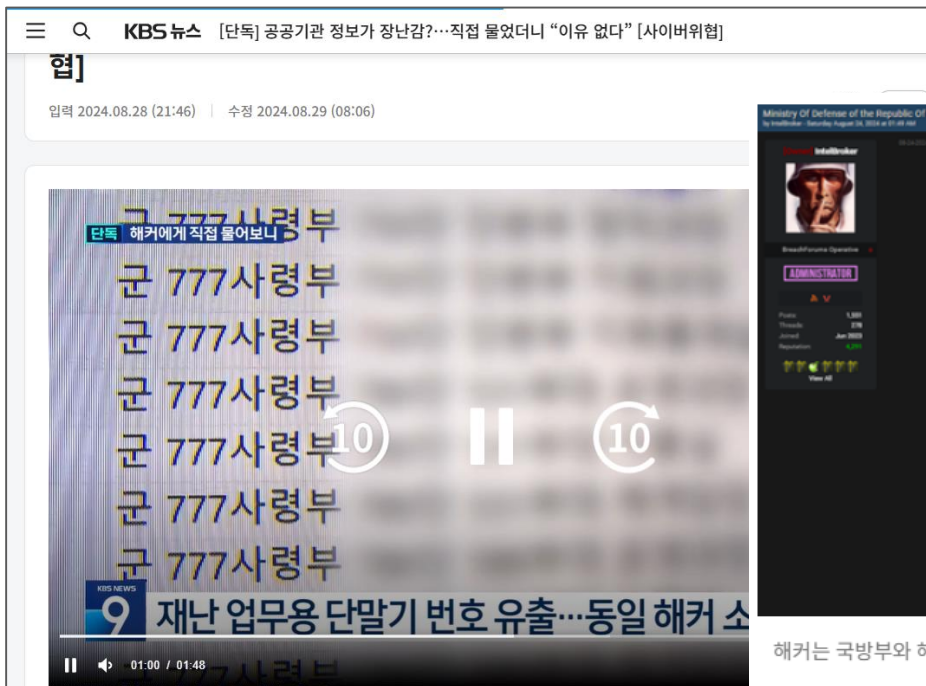
OSINT-Driven 공급망 위협(Supply Chain Threat)

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



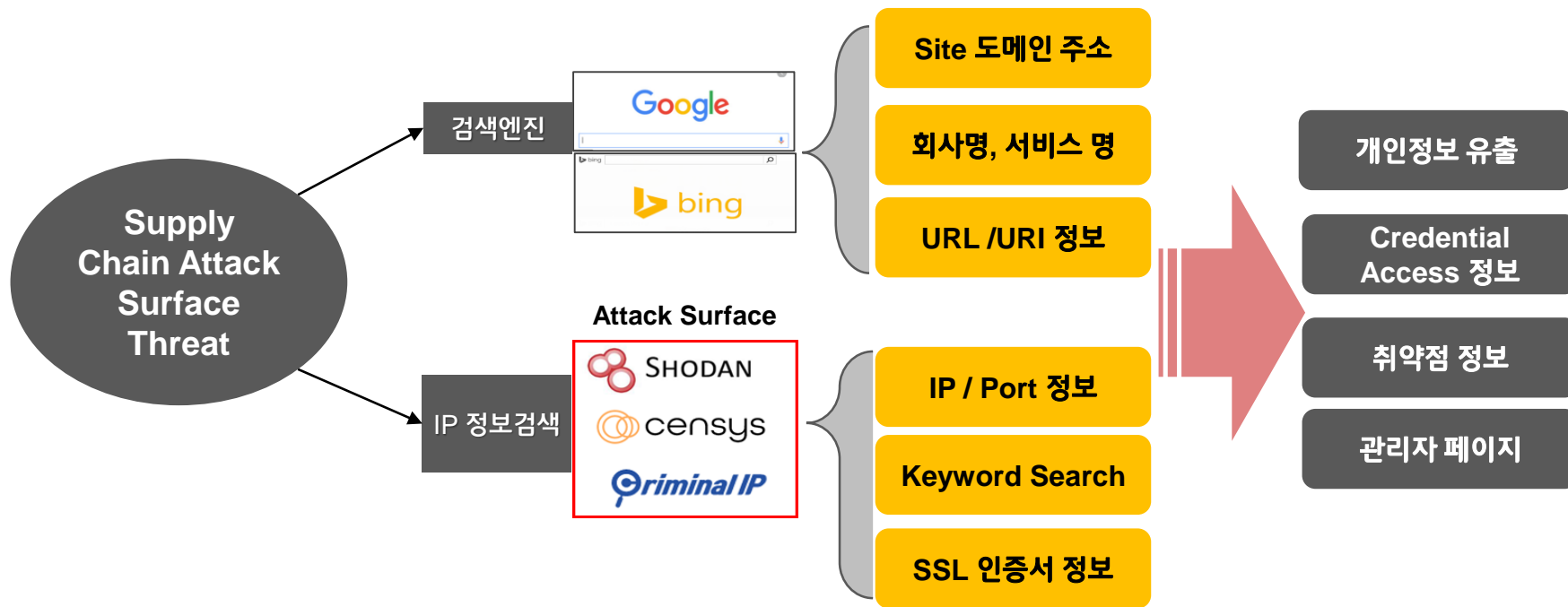
해커는 국방부와 해양경찰청 등의 내부 데이터에 접근하는 데 성공했다고 주장했다. 사진=해킹포럼

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

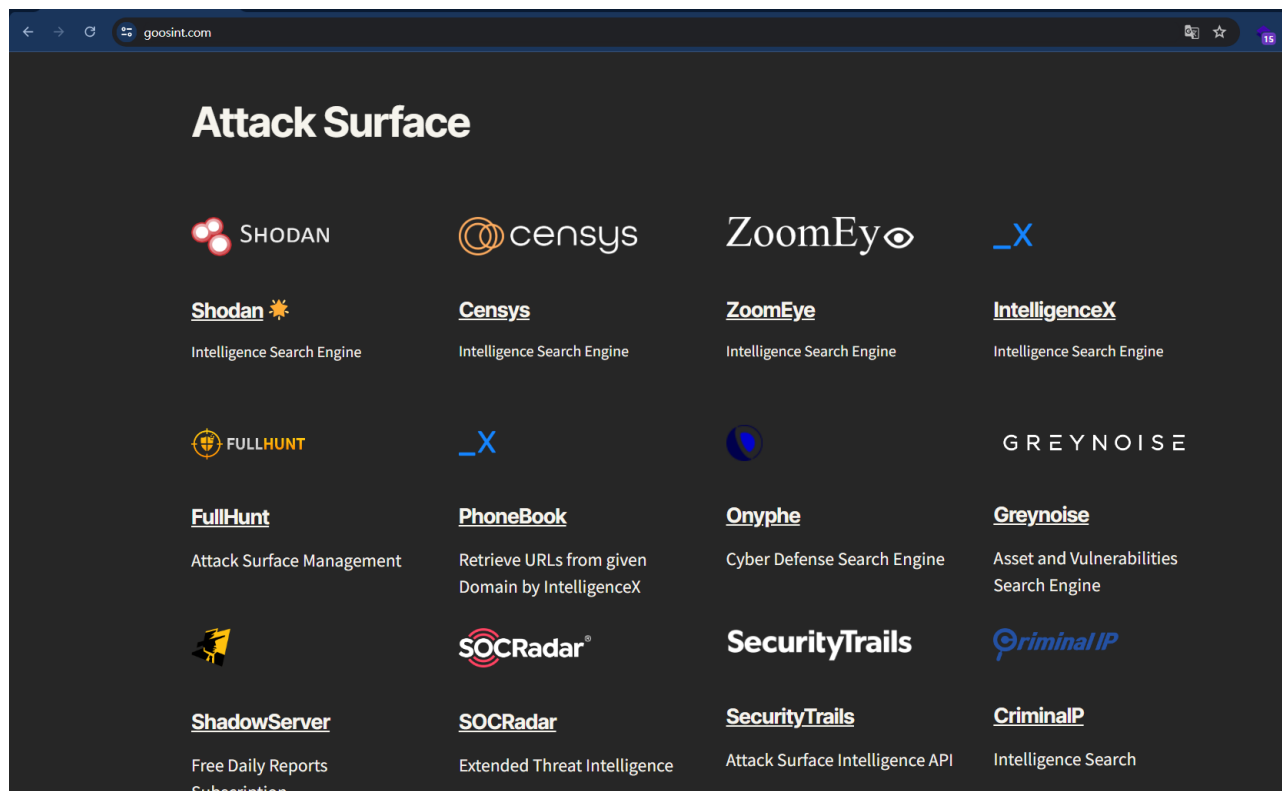


OSINT-Driven 공급망 위협(Supply Chain Threat)

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)

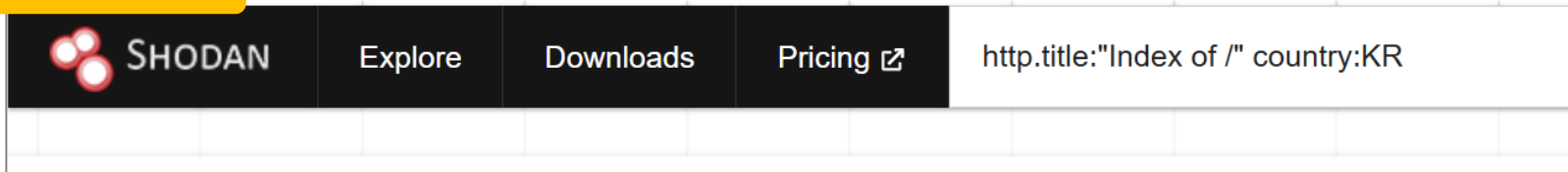
대표적인 웹 취약점인 디렉터리 리스팅 사이트에서 공급망 위협 정보를 찾을 수 있음

OSINT 정보 탐색을 위한 기본 지식

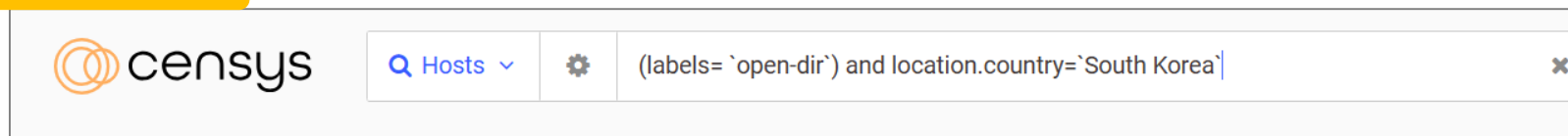
➤ OSINT 검색도구 - IP 정보수집 검색엔진

▶ IP 정보 검색엔진에서 국내(KR) 대상으로 디렉터리 리스팅 취약점 IP 정보

Shodan



Censys



Criminal IP

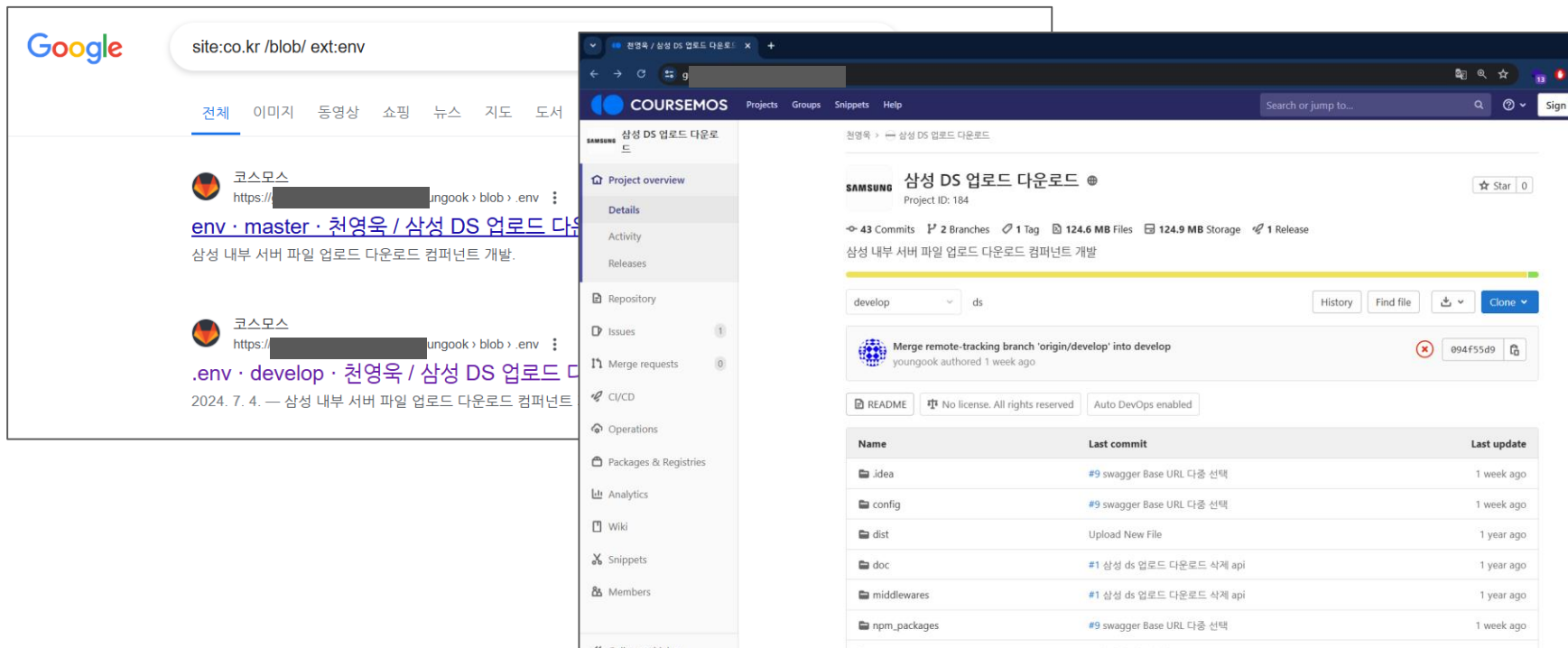


OSINT-Driven 공급망 위협(Supply Chain Threat)

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



The image shows a Google search result for the query `site:co.kr /blob/ ext:env`. The search results list two entries from '코스모스' (Cosmos) pointing to GitHub repositories. The first entry is for the `env · master · 천영욱 / 삼성 DS 업로드 다운로드` repository, and the second is for `.env · develop · 천영욱 / 삼성 DS 업로드 다운로드`. The second entry includes the date '2024. 7. 4.' and the description '삼성 내부 서버 파일 업로드 다운로드 컴퍼넌트 개발'.

The right side of the image shows the GitLab repository page for 'SAMSUNG 삼성 DS 업로드 다운로드'. The repository is located at `youngook / blob > .env`. The page displays repository statistics: 43 Commits, 2 Branches, 1 Tag, 124.6 MB Files, 124.9 MB Storage, and 1 Release. A merge request is visible, titled 'Merge remote-tracking branch 'origin/develop' into develop' by youngook, authored 1 week ago. Below the merge request is a table of files:

Name	Last commit	Last update
idea	#9 swagger Base URL 다중 선택	1 week ago
config	#9 swagger Base URL 다중 선택	1 week ago
dist	Upload New File	1 year ago
doc	#1 삼성 ds 업로드 다운로드 삭제 api	1 year ago
middlewares	#1 삼성 ds 업로드 다운로드 삭제 api	1 year ago
npm_packages	#9 swagger Base URL 다중 선택	1 week ago

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

The screenshot shows the 'Asset Search' interface with the search query 'favicon: -589ccf49'. The results list two items:

- 한국철도공사 - 로그인** (Korea Railway Corporation - Login)
 - Inbound: Low
 - Outbound: Safe
 - Score: 200
 - HTML 5.0
 - ORACLE-BMC-31898
 - Republic of Korea
 - Seoul
 - 2024-07-16 23:33:16
 - Cloud Service: Hosting
 - HTTP/1.1
 - Status: 200
 - Date: Tue, 16 Jul 2024 23:23:00 GMT
 - Cache Control: no-store
 - Content Type: text/html;charset=UTF-8
 - Vary: origin,access-control-request-headers
- 전차선로 보호 모니터링** (Overhead Line Protection Monitoring)
 - Inbound: Safe
 - Outbound: Safe
 - Hashes: 665e5cf, -589ccf49, -412262b015a, -170eee13, -17c9f4ff, 2748d01f, 2b3...

The browser view on the right shows the login page for KORAIL, titled '전차선로 보호 모니터링' (Overhead Line Protection Monitoring), with fields for '아이디' (ID) and '비밀번호' (Password), and a '로그인' (Login) button.

OSINT를 활용한 공급망 위협 정보 탐지 사례

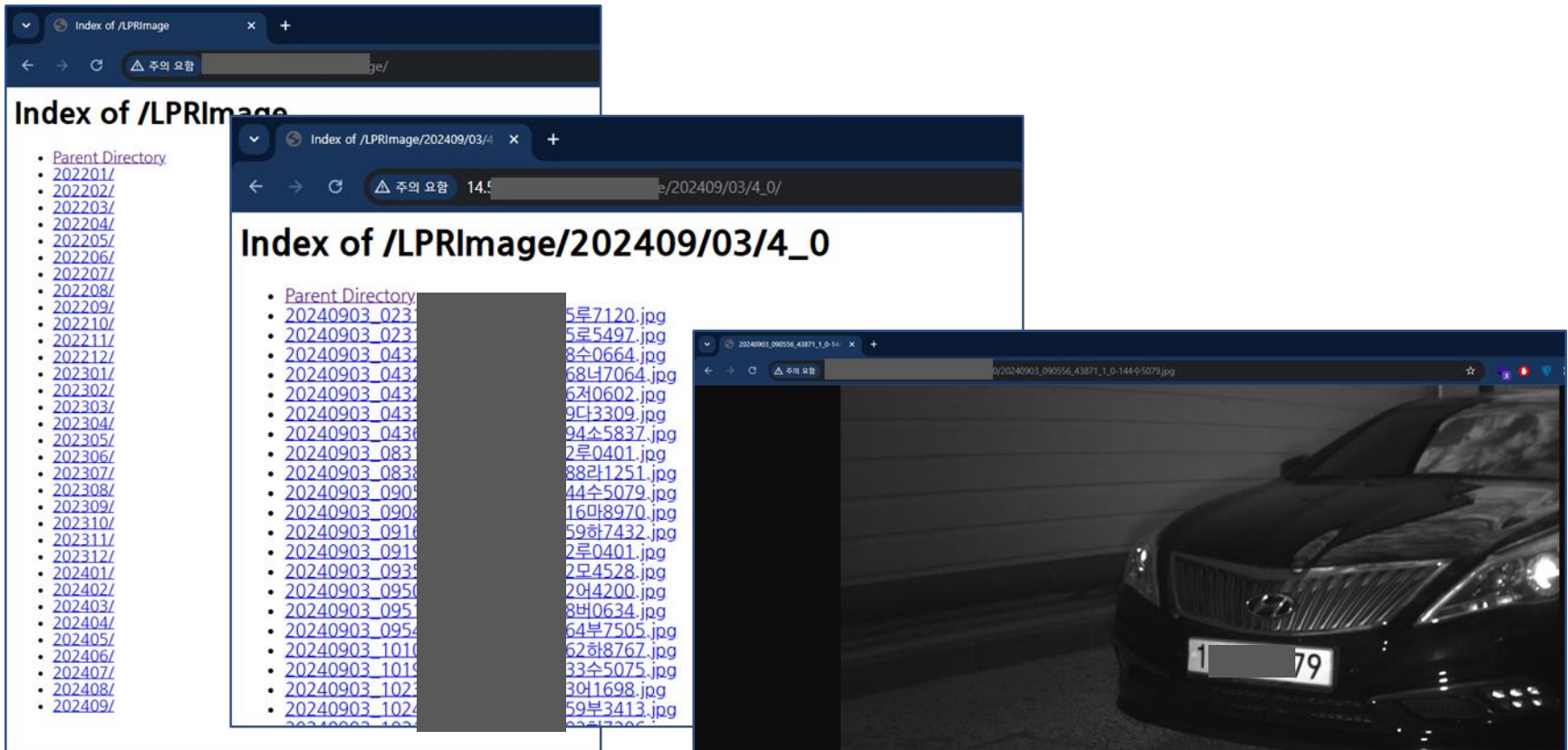
공급망 위협정보 사례

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

The screenshot shows a Censys search interface. The search query is: `(((labels= `open-dir`) and (.env)) and location.country=`South Korea`)`. The results section shows a directory listing for `/dna-ai-api`. The file `.env` is highlighted in red. A red arrow points from the `.env` file to a preview window showing the contents of the file:

```
APP_NAME=Laravel1
APP_ENV=local
APP_KEY=
APP_DEBUG=true
APP_URL=http://localhost

LOG_CHANNEL=stack
LOG_DEPRECATIONS_CHANNEL=null
LOG_LEVEL=debug

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=laravel
DB_USERNAME=root
DB_PASSWORD=
```

Below the preview window, there is a snippet of code showing database connection details:

```
PORT = 3000
MONGODB_URI = "mongodb+srv://administrator:Tev0Ri8V08cUZttG@cluster0.udurn5y.mongodb.net/?retryWrites=true&w=majority"
```

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

Leaks +country:"South Korea" +plugin:"GitConfigHttpPlugin" +".KR"

Found 446 results for +country:"South Korea" +plugin:"GitConfigHttpPlugin" +".KR"

ap[redacted].com medium

ASN: 9318 = 0

82 events in 769 days fileMode = false

Looking for more results? Register a free account

South Korea

Directory listing for /.git/

- [branches/](#)
- [COMMIT_EDITMSG](#)
- [config](#)
- [description](#)
- [HEAD](#)
- [hooks/](#)
- [index](#)
- [info/](#)
- [lfs/](#)
- [logs/](#)
- [objects/](#)
- [packed-refs](#)
- [refs/](#)

```
[core]
  repositoryformatversion = 0
  filemode = true
  bare = false
  logallrefupdates = true
[remote "origin"]
  url = https://github.com/hahveon610/youtube-download.git
  fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
  remote = origin
  merge = refs/heads/main
  vscode-merge-base = origin/main
```

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

The screenshot shows a web security tool interface with the following details:

- Search Query:** Leaks +country:"South Korea" +plugin:"VsCodeSFTPPlugin"
- Results:** Found 2456 results for +country:"South Korea" +plugin:"VsCodeSFTPPlugin"
- Domain Search:** https://[redacted] (Last scan date: 2024-09-08 15:22:55)
- Exposure Table:**

Exposure	
HTML Details >	
Apache Status	Unexposed
DS_Store	Unexposed
Git Config	Exposed
Phpinfo	Unexposed
Wordpress	Unexposed
Docker Registry	Unexposed
Firebase	Unexposed
Json Config	Unexposed
vscode sftp.json	Exposed
- File Content (vscode/sftp.json):**

```

{
  "protocol": "sftp",
  "host": "[redacted]",
  "username": "isos",
  "password": "isos21411@",
  "remotePath": "/home/isos/www",
  "port": 22,
  "interactiveAuth": false,
  "uploadOnSave": true,
  "syncMode": "update",
  "ignore": [
    "**/.vscode/**",
    "**/.git/**",
    "**/.DS_Store"
  ]
}

```

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

emailAddress=support@soosan.co.kr, C=KR, ST=Seoul, L=Gangnam-gu, O=SOOSANINT, OU=RnD, CN=eprismx,
emailAddress=support@soosan.co.kr

9200/ELASTICSEARCH TCP

Software

- Red Hat Linux
- Elasticsearch 6.8.23
- Apache Lucene 7.7.3

Details

System Information

Name	uwy61bz
Build Flavor	default
Build Type	rpm
Build Hash	4f67856

```

C:\>curl -sk http://3[redacted]
{"name": "uwy61bz",
"cluster_name": "elasticsearch",
"cluster_uuid": "X9JpbdhvRkuBkKZwdTzhZg",
"version": {
"number": "6.8.23",
"build_flavor": "default",
"build_type": "rpm",
"build_hash": "4f67856",
"build_date": "2022-01-06T21:30:50.087716Z",
"build_snapshot": false,
"lucene_version": "7.7.3",
"minimum_wire_compatibility_version": "5.6.0",
"minimum_index_compatibility_version": "5.0.0"
},
>tagline": "You Know, for Search"
}
C:\>
    
```

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

The screenshot shows search results for the query 'services.http.response.html_title:과학기술정보통신부'. It displays two host entries with their respective HTTP details.

Hosts
Results: 2 Time: 0.18s

Host 1: [Redacted IP] Linux KIXS-AS-KR Korea Telecom (4766)
 Software: jquery, swiper
 Services: 80/HTTP, 8443/HTTP, 8001/HTTP, 8701/HTTP

Host 2: [Redacted IP] Microsoft SMILESERV-AS-KR SMILESERV
 Software: remote-access, jquery, twitter, bootstrap, na
 Services: 80/HTTP, 5985/WINRM, 8091/HTTP, 135/DCERPC, 8081/HTTP, 8092/HTTP

HTTP 8701/TCP Details:
 Software: Apache Tomcat, Apache Coyote 1.1
 Details: http://[Redacted]701/
 Status: 200 OK
 Body Hash: sha1: aa36785796db04cf22cf43063609a0d8ed077ef4
 HTML Title: 과학기술정보통신부
 Response Body: [EXPAND]

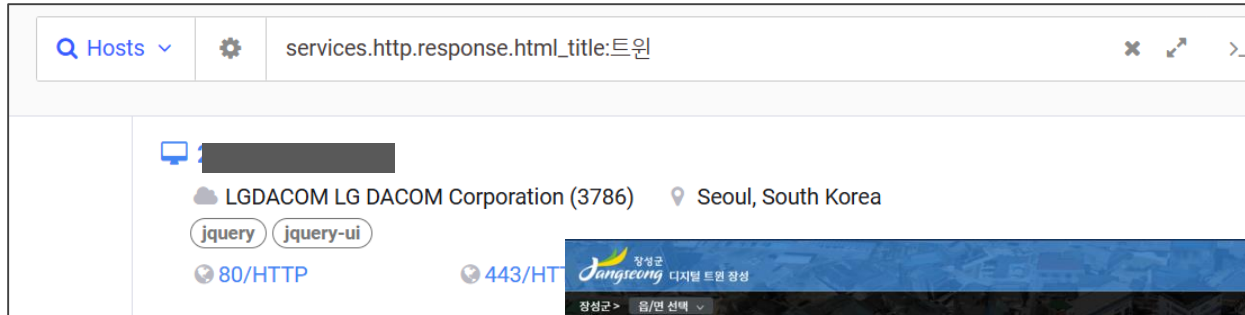
HTTP 8090/TCP Details:
 Software: BOOTSTRAP, JQUERY, NAVER A
 Details: http://[Redacted]0/
 Status: 200 OK
 Body Hash: sha1: 10899072cf41cbc353ab9f9873b0add051c58dd3
 HTML Title: 과학기술정보통신부 도서관 - MSIT LIBRARY
 Response Body: [EXPAND]

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

```

8088/include/config_dev.inc

<?php
/* *****
[DEV] SERVER CONFIGURATION
***** */

/* CQ */
$DOC_ROOT = $_SERVER['DOCUMENT_ROOT'];
$log_path = './log';

$log_crypto_key = '6B58703273357638792F423F4528482B4D6250655368566D597133743677397A'; // HEX
$token_crypto_key = '7A244326462948404D635166546A576E5A7234753778214125442A472D4B614E'; // HEX
$token_expire_sec = 600; // 10분

$telegram_bot_token = '5324769912:AAGLfGaacWk9JW9uZHbsqvhqw4SEhDLkdEY';
$telegram_channel_id = '-1001165608011';

$remote_log_endpoint = 'https://[redacted].tappay/web';

/* PAYCOQ */
$paycoq_proxyapi_clienttype = 'APP';
$paycoq_proxyapi_osname = 'S';
$paycoq_proxyapi_osversion = 'ROCKY8';
$paycoq_proxyapi_appid = 'fc63ca33-7219-48cf-973d-a98e9cbd79de';
$paycoq_proxyapi_validkey = 'YjEzNzFjODQlNDU1Yi00ZDMzLWI4NTgtMmEzNjBhYWUwMjcj';

$paycoq_proxyapi_baseurl = 'https://[redacted].bqrf.com';
$paycoq_proxyapi_rsaencry_key_endpoint = 'credit-card/encoded';
?>
    
```

OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 - 개발 시스템

➤ 웹 개발 퍼블리싱 사이트 정보검색

▶ 디렉터리 리스팅 + 웹퍼블리싱 사이트를 통해 기업 정보탐색

The screenshot shows a web browser displaying a flight booking system. The main interface includes a navigation menu with options like 'Flight Info', 'Booking List', 'Build Up', 'Work Sheet', 'Work Status', 'ULD Bill List', and 'Op ULD'. A search bar is visible with flight details: '08:30 / 74F(HL1234) / 6L8C / PVG(5076)에 잔여장비 포함, 남은 작업 관련 장비 설정'. Below the search bar, there are filters for 'ALL', 'B/U', 'THR', 'BUP', 'R/B', 'ETC', and buttons for '자동분류' and '직접분류'. A table of flight bookings is shown, with one entry selected: 'DGD 988-6856 0601'. A 'MEMO' section below the table contains the text: '직접 입력한 메모 내용이 노출됩니다.'.

Overlaid on the bottom right of the browser window is a window titled '아시아나 퍼블리싱 현황판' (Asiana Publishing Status Board). This window contains a table with columns for '1 Depth', '2 Depth', '3 Depth', '파일위치' (File Path), '파일명' (File Name), and '상태' (Status). The table lists various HTML files and their corresponding status.

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 System)

▶ 파비콘(favicon)으로 프로젝트 관리시스템 찾기

The screenshot displays a web browser window with the following elements:

- Browser Address Bar:** POS BANK 프로젝트 관리
- Page Header:** POS BANK 프로젝트 관리
- Page Content:**
 - Projects List:**
 - MDM 솔루션 개발 (자사 MDM 서비스를 위한 솔루션 개발 업무)
 - ASP (PHP 기반 ASP 프로젝트)
 - WAVE-X
 - Right Panel:** 통합 보안리더 단말 개발 프로젝트 (All-in-one Payment Terminal) - Contact 및 Contactless 결제를 지원하는 통합 단말 개발 프로젝트.
 - 1. Contact
 - SCR / MSR 결제 지원
 - EMV L1 / L2 인증
 - VAN : Nice 인증
 - 2. Contactless
 - NFC 결제 지원
 - EMV L1 / L2 인증
 - VISA / Master / AMEX 카드 지원
 - Apple Pay / Samsung Pay 지원...
- Developer Tools (Network Tab):**
 - Request: HTTP/1.1
 - Status: 200
 - Response Headers: X_Download, Etag, X_Runtime, Date, X_Permission, X_Request, Referrer, Cache-Control
- Browser Console:**
 - Inbound: Low
 - Outbound: Safe
 - 200
 - Technologies: nginx, AMAZON-02, Republic of Korea, Incheon, jQuery, Nginx, Phusion Passenger, Redmine

OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 - 유지보수 시스템

➤ 외부 유지보수 협력업체 서버를 통한 서버 민감 정보 노출

▶ 한국중앙박물관 개발시스템에서 서버 접속 계정정보 노출

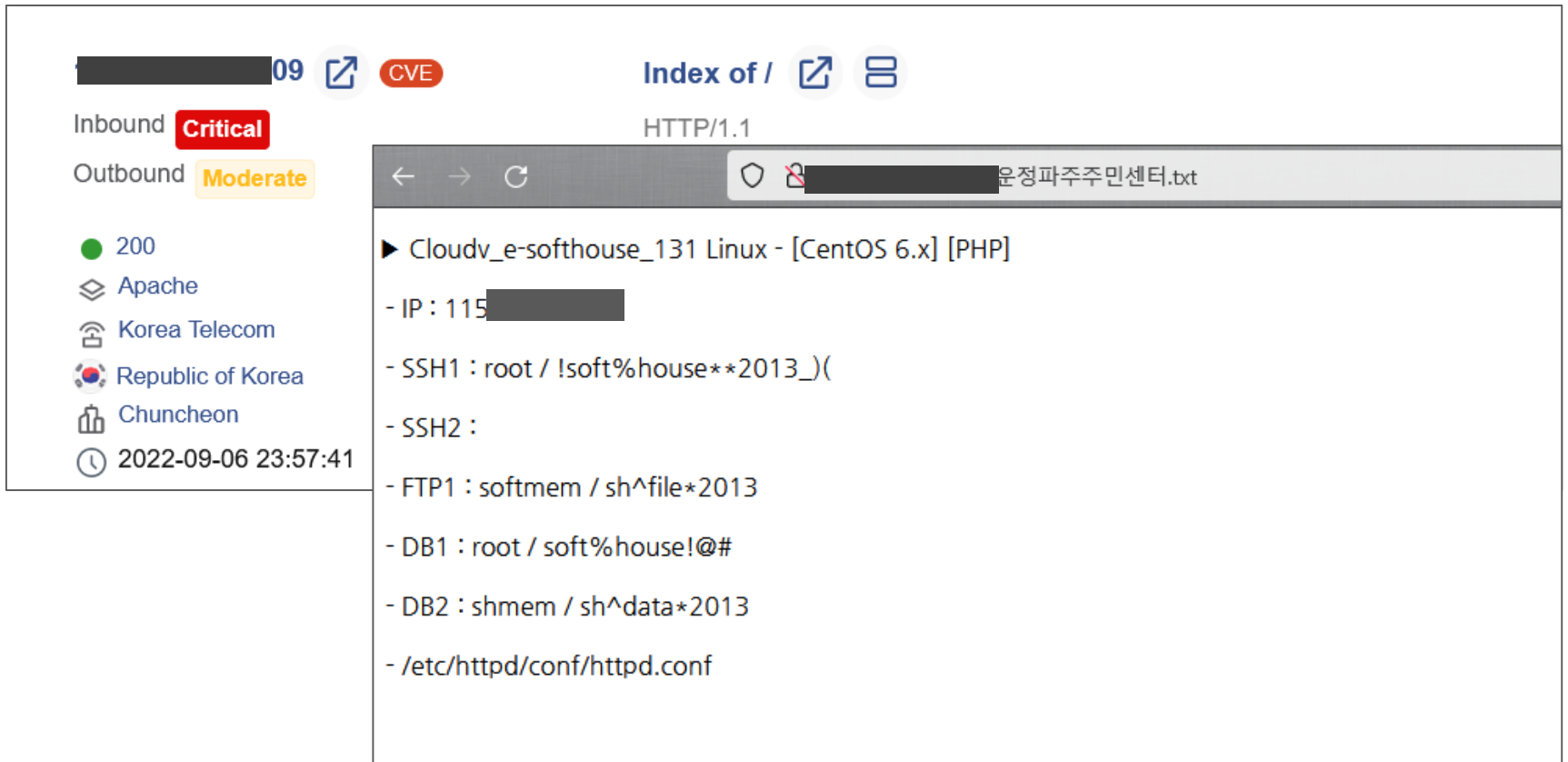
The screenshot displays a web browser window with a login form for the '동원전시안내관리시스템' (Dongwon Exhibition Guide Management System). The login form has two options: 'GPKI(인증서)를 이용해서 들어가기' (Log in using GPKI certificate) and '아이디를 이용해서 들어가기' (Log in using ID). The ID login section includes fields for 'ID' and 'Password', and a '로그인' (Login) button. A log viewer overlay is positioned on the left side of the browser window, showing an inbound request with the following details:

- Inbound:** Critical
- Outbound:** Moderate
- Score:** 200
- OS:** centos
- Protocol:** http
- Server:** apache
- HTTP Headers:**
 - HTTP/1.1
 - Status: 200 OK
 - Date: Sat, 30 Jul 2022 04:11:03 GMT
 - Etag: 6d0-5e0feafbc4244
 - Content Length: 1744
 - Content Type: text/html
 - Server: Apache/2.4.6
- HTML Content:**
 - <h2 id="테스트-서버-정보">테스트 서버 정보</h2>
 - <h4 id="중앙-박물관-전">중앙 박물관 전시 안내</h4>
 -
 - 관리자
 -
 - URL <code>/eaim.dev-jkds.kr</code>
 - ID <code>[redacted]</code>
 - PASSWO <code>[redacted]</code>
 -
 -
 - API 서버(통계)
 -
 - URL : http://stat.dev-jkds.kr
 -

OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 - 유지보수 시스템

- 외부 유지보수 협력업체 서버를 통한 서버 민감 정보 노출
 - ▶ 행정기관 주민센터 서버 계정 및 패스워드 정보노출 (전산시스템 운영 유지보수 업체)



[REDACTED]09 [CVE](#) [Index of /](#) [운정파주주민센터.txt](#) HTTP/1.1

Inbound **Critical**
 Outbound **Moderate**

● 200
 Apache
 Korea Telecom
 Republic of Korea
 Chuncheon
 2022-09-06 23:57:41

```

▶ Cloudv_e-softhouse_131 Linux - [CentOS 6.x] [PHP]
- IP : 115[REDACTED]
- SSH1 : root / !soft%house**2013_)(
- SSH2 :
- FTP1 : softmem / sh^file*2013
- DB1 : root / soft%house!@#
- DB2 : shmem / sh^data*2013
- /etc/httpd/conf/httpd.conf
    
```

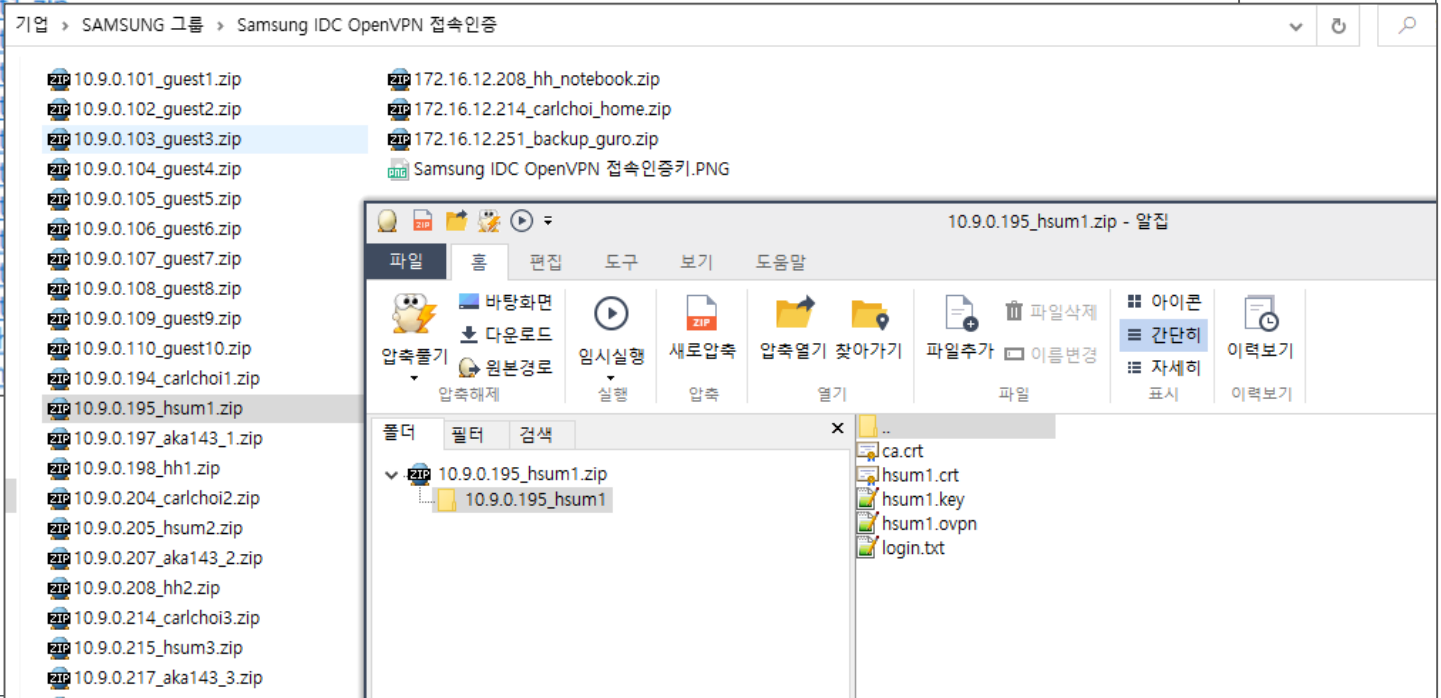
OSINT 활용한 공급망 위협정보 사례

공급망 위협 정보 사례 - 유지보수 시스템

- 외부 유지보수 협력업체 서버에서 VPN 계정정보 노출
- ▶ 유지보수 업체에서 운영하는 서버에서 IDC 접속용 OpenVPN 접속 계정 노출

Index of /OpenVPN_cert/SAMSUNG_IDC/openvpn_server

- [Parent Directory](#)
- [10.9.0.101_guest1.zip](#)
- [10.9.0.102_guest2.zip](#)
- [10.9.0.103_guest3.zip](#)
- [10.9.0.104_guest4.zip](#)
- [10.9.0.105_guest5.zip](#)
- [10.9.0.106_guest6.zip](#)
- [10.9.0.107_guest7.zip](#)
- [10.9.0.108_guest8.zip](#)
- [10.9.0.109_guest9.zip](#)
- [10.9.0.110_guest10.zip](#)
- [10.9.0.194_carlchoi1.zip](#)
- [10.9.0.195_hsum1.zip](#)



- 결론 -

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