

# S2W WEBINAR

with < ASM >



# 제2회 S2W WITH 웨비나

Session 1. Keynote

곽경주, Head of TALON (Center for Threat Research and Intelligence)

## 공격표면관리(ASM)란 무엇인가요?



# Securing Your Digital Infra:

# The **CTI-driven Attack Surface Management**

{ Cyber Threat Intelligence }

kay@s2w.inc

**Kyoung-ju Kwak**

Head of **TALON** [Center for Threat Research and Intelligence @S2W]

---

**REVEAL THE ORIGIN**

OVERWHELMING INTELLIGENCE GROUP

**TALON**

“



## 곽경주 이사

Head of Center for Threat Research & Intelligence [ **TALON** ], S2W

- 금융결제원 (~2015.04)
- 금융보안원 (~2020.07)
- S2W 위협분석센터 (탈론) 총괄이사 / Quaxar Product Owner (~현재)
- 과학기술정보통신부 사이버보안 얼라이언스 대응분과자문위원
- 개인정보보호위원회 기술포럼 탐지분과자문위원
- 한국인터넷진흥원 위협 인텔리전스 네트워크 위원
- 차세대 보안리더 양성 프로그램 디지털 포렌식 멘토
- 전, 성균관대학교 과학수사학과 겸임교수
- 사이버치안대상 행정자치부 장관상

## 주요 발표

- The Case study of incidents in Korea Financial Sector, *International Symposium on Cyber Crime Response*, 2014
- The New Wave of CyberTerror in Korea Financial Sector, *PACSEC Japan*, 2016
- Fly me to the BLACKMOON, *HITCON Taiwan*, 2016
- Silent Rifle, How to take control all of your system, *Hackon Norway*, 2016
- Campaign RIFLE : Andariel, The maiden of Anguish, Kaspersky Cyber Security Weekend (Phuket), 2017
- Underground Invasion Tunnels : State-Sponsored Cyber Miners Recent Status, Kaspersky SAS (Cancun), 2018
- Nation-State Moneymule's Hunting Season : APT Attacks Targetting Financial Institutions, *Blackhat Europe & Asia*

”

# Attack Surface



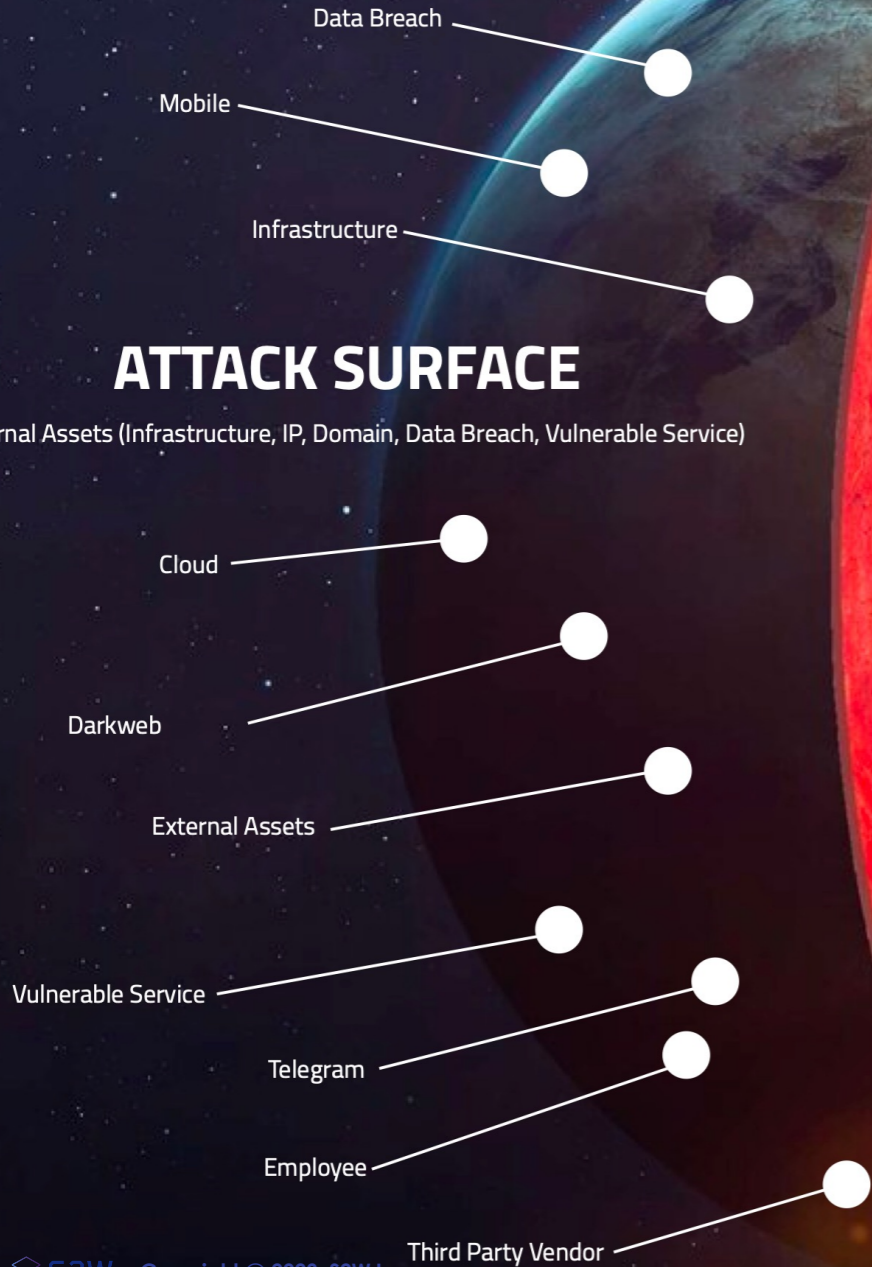
## • 공격 표면 (Attack Surface)

- 컴퓨터 시스템, 네트워크, 또는 소프트웨어에서 공격자가 악용할 수 있는 취약한 부분을 모두 합한 개념
- 공격 표면은 시스템의 여러 구성 요소와 이들 사이의 인터페이스를 포함하며, 각 구성 요소가 공격자에게 노출될 수 있는 정도를 나타냄
- 기술적인 표면 뿐만 아니라 퇴사자, 외주 업체 직원 등도 공격 표면으로 볼 수 있음
  - 딥다크웹, 텔레그램 등에 유출되는 정보를 활용한 공격이 증가하고 있음
- 공격 표면을 줄이는 것은 공격자가 시스템을 악용할 수 있는 기회를 줄이고, 보안 위협에 대한 노출을 감소시키는데 도움이 됨

# ATTACK SURFACE IS DYNAMIC & GROWING

## ATTACK SURFACE

External Assets (Infrastructure, IP, Domain, Data Breach, Vulnerable Service)



## PROTECT SURFACE

Define Your Protect Surface (DAAS, Data | Asset | Application | Service)

# DAAS: The Building Blocks of ASM

## Data

기업에서 저장, 처리하거나 내외부로 전송하는 데이터를 의미하며, 민감한 대외비 정보, 개인정보, 지적재산권과 관련된 정보가 있음

## Asset

하드웨어 또는 소프트웨어 중 기업의 데이터를 처리하고 저장하는 등의 업무를 수행하는 인프라를 의미하며, 서버, 네트워크, 데이터베이스 등이 이에 속함

## Application

기업 내 업무를 위해 작동하는 소프트웨어 프로그램 또는 스크립트 등을 의미하며, 어플리케이션은 내부에서 돌아가거나 (on-prem) 클라우드를 기반으로 작동하기도 함

## Service

외부로부터 제공받는 소프트웨어, 어플리케이션 등을 의미하며 클라우드, 호스팅, 외주업체 서비스 등을 의미함

# What to do?

- **자산 식별 (가장 중요)**

- 자산별 중요도를 기반으로 우선순위 및 대응 매뉴얼 체계화
- 각 자산의 구성요소 식별
  - 자산과 연동된 도메인, 서브도메인 식별
  - 각 웹서비스에서 사용 중인 인증서 정보 식별하고 관리
  - 운영체제, 사용 중인 오픈소스, 서비스 어플리케이션, 서비스 포트, 외부에 제공되고 있는 정보 등을 식별하고 체계적으로 관리하고 있어야 함

- 식별된 자산 정보를 기반으로 지속적으로 비식별, 비인가 자산을 모니터링해야함

- 신규 탐지된 자산은 일련의 검증 과정을 거치게 됨
- 기존 자산의 경우, 신규 서비스 포트 또는 오픈소스 버전 변경에 따른 신규 취약점 발생 여부를 면밀히 분석해야함

- 모니터링을 통해 탐지된 자산은 기존 식별 자산목록에 편입

- 일련의 과정은 자동화가 필수



# Types of Assets

## Known Assets (식별 자산)

- 내부에서 식별 되어 있는 자산
- 관리가 잘 되는 편이나 최근 클라우드로의 전환 및 서비스의 복잡도가 올라감에 따라 식별 자산의 공격 표면 역시 지속적으로 변화하고 있음

## Unknown Assets (비식별 자산)

- 내외부에서 식별되지 않은 자산이며 기존에 관리되고 있지 않던 영역에 있는 자산
- 네트워크 스캐닝, 오픈소스 인텔리전스, 딥다크웹 모니터링 등을 통해 식별 자산으로의 통합이 필요함

## Vendor Assets (위탁 자산)

- 제3의 업체에 위탁 맡긴 자산을 의미함
- SI 구축 프로젝트 업체, 클라우드 관리 업체, 복지 서비스 업체, 기타 외부 서비스 운영 업체에 위탁 맡긴 자산
- 보안에 대한 지식 또는 관리체계가 미흡한 위탁업체와 협업할 경우 민감 정보 유출 위험이 존재함

## Subsidiary Assets (계열사 자산)

- 자회사 또는 계열사의 자산
- 그룹사일 경우, 내부적으로 망이 연결되어 있을 가능성이 높음
- A 회사가 보안을 아무리 잘해도 내부적으로 연결되어 있는 B 계열사가 보안을 제대로 신경 쓰지 않을 경우, 연쇄 침해사고 발생 가능

# ATTACK SURFACE

SEVERITY

★ **Third-party Assets**

Legacy System

**Impersonating Assets**

★ **Cloud Assets**

Exposed **Credentials**

★ Exposed **Dev & QA**  
Infrastructure

Exposed **DB**  
Scheme



**Subsidiary Assets**

Public IPs

ERP Servers

Web Servers

**On-premises Assets**

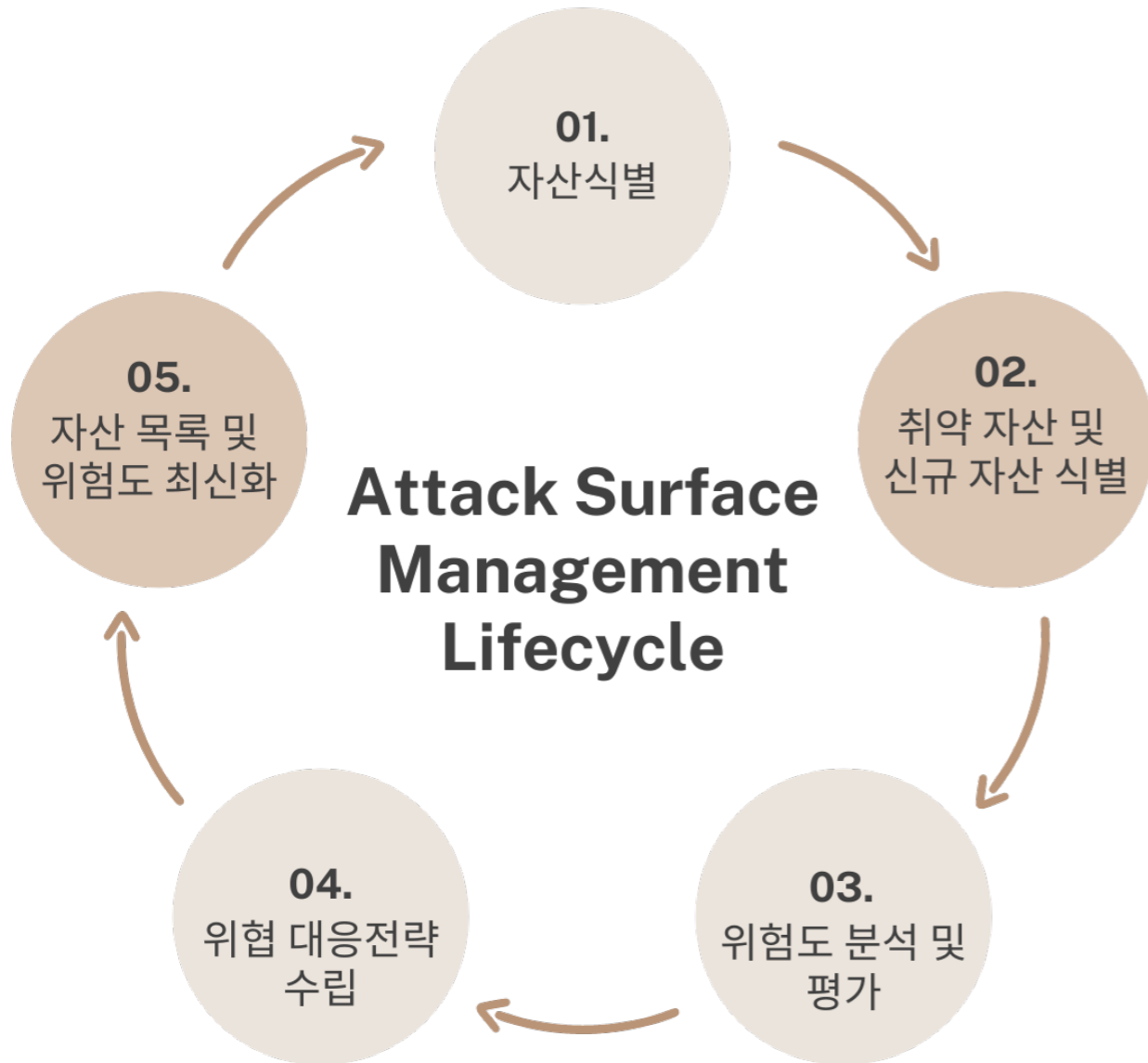
VPN Servers

Official Domains

Valid Certificates

**NO VISIBILITY OF EXPOSURE**

# Lifecycle of Attack Surface Management



## 1. 기존 자산 식별

- 내부 자산관리 시스템 활용, 네트워크 스캐닝, 딥다크웹 모니터링, 오픈소스 인텔리전스 등 다양한 방법론 활용

## 2. 취약 자산 및 신규 자산 식별

- 자산 내 운영 중인 서비스 특성 파악 후 취약점과의 연관성 식별
- 기존 식별된 자산 외 신규 자산 식별 (CTL, 신규생성도메인 등)

## 3. 위험도 분석 및 평가

- 식별된 자산 및 취약점에 대한 상세 분석 및 위험도 평가

## 4. 위협 대응전략 수립

- 분석 및 평가 결과에 따라 대응 우선순위를 정하고 조치를 위한 마스터플랜 수립

## 5. 자산 목록 및 위험도 최신화

- 신규 자산의 기존 자산으로의 편입
- 자산별 취약점과 외부로부터의 침투시 위험도에 대한 재산정

# Cyber Threat Intelligence (CTI)



- **조직이나 개인의 환경에 적합한 위협 정보와 분석을 제공함**
  - 공격그룹 (Threat Actors) 정보
  - 악성코드 (Malware) 정보
  - 취약점 (Vulnerability) 정보
  - 침해사고 (Incidents) 정보
  - 데이터 유출 (Data Breach) 정보
  - 브랜드 / 서비스 어뷰징 (Abuse) 정보
- **CTI는 단순 정보만을 제공하는 것이 아니라 정보 간의 연관성도 파악함**
- **위협 인텔리전스를 통해 현재와 미래의 대응 전략을 마련함**

# ASM + CTI = CTI-Driven ASM (CDA)

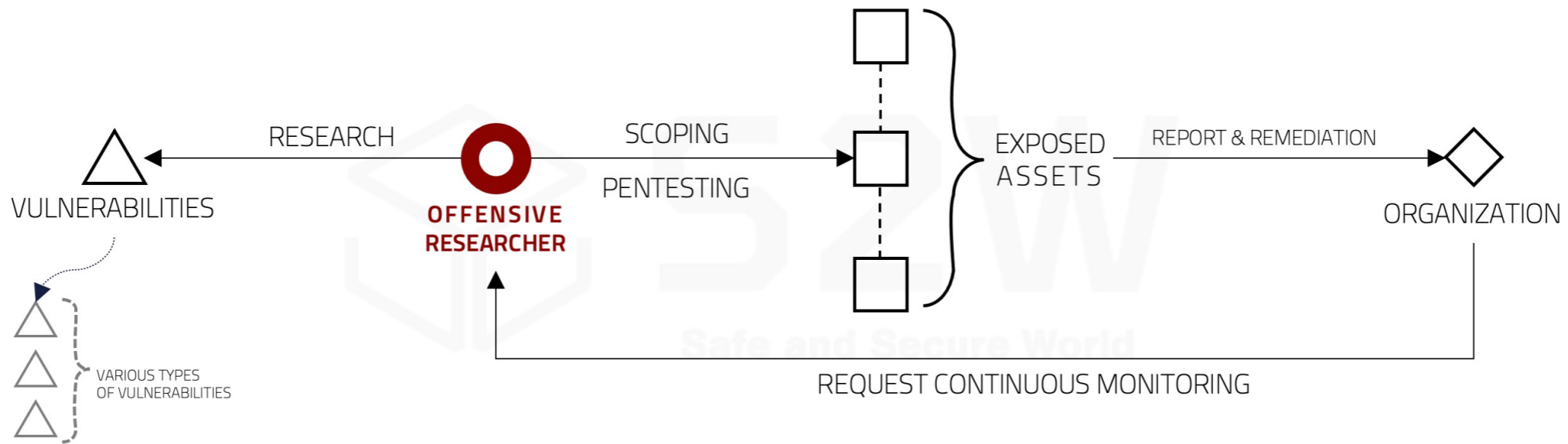
**Benefits:** Better Decision Making & Streamlined Response



Comprehensive **CTI-driven Attack Surface Management**

**enough?**

# CONTINUOUS AUTOMATED RED TEAMING



**CDA**  
CTI-DRIVEN ASM

+

CONTINUOUS AUTOMATED

**RED TEAMING**

{ CART }

- 연중 특정기간 내에 한정된 자산 대상으로 진행하는 모의해킹 뿐만 아니라 **적정한 수준의 점검을 1년 상시 진행**하는 것이 필요함
- 기업에서 사용하는 다양한 오픈소스 및 상용 소프트웨어를 식별한 후, **취약점을 포함한 기존 위협 정보 데이터베이스와 오픈시브 분석가의 지식을 활용**하여 보다 깊이 있는 공격표면관리가 진행될 필요가 있음

## Why Red Teaming Matters

기업 내 취약 자산에 대한 보다 실질적인 이해를 제공하고 위협에 대한 내부적인 준비도를 측정할 수 있음



# CONCLUSION

- **ASM은 다음과 같은 역할을 수행함**
  - **Assessing Footprint of Digital Infra**
    - 기업 자산의 외부 노출을 탐지하고 비식별 자산을 확인할 수 있음
  - **Comprehensive understanding of Vulnerability**
    - 기업에서 인식하고 있는 현재 보안 강도와 실제 외부 공격자 관점에서의 보안강도와의 갭을 인지할 수 있음
  - **Protect Privacy**
    - 기업의 개인정보 정책과 관리 수준이 규제 요구사항에 부합하는지 확인 가능

# CONCLUSION

- **성공적인 ASM 운영을 위해 기업에서는 아래와 같은 요소들을 수행해야함**
  - **Educate your Employees**
    - 기업 내 인프라 운영에 필요한 정책이 필요하고 직원들을 교육해야함
    - 신규 인프라는 보안팀 또는 인프라팀에서 정한 규정에 맞춰서 생성되고 관리되어야 함
    - 직원들의 암호 관리, 피싱 공격 식별, 의심스러운 이메일 열람시 주의사항들을 지속적으로 교육해야함
  - **Stay Current with Updates**
    - 기업에서 사용 중인 DAAS (Data, Asset, Application, Service)를 체계적으로 관리하고 관련 정보를 항상 최신으로 유지해야함
    - 오픈소스 라이브러리 사용 현황을 항상 최신 상태로 유지하고 관리해야함
  - **Perform Regular Audits (Red Teaming)**
    - 주기적인 내부 IT 감사 및 펜테스팅은 기술적인 위험 관리 뿐만 아니라 비즈니스 리스크를 관리하기 위해 필수적인 사항임

# CONCLUSION

If you can not **measure** it, you can not **manage** it.

If you can not manage it, you can not **improve** it.

측정할 수 없으면 관리할 수 없고, 관리할 수 없으면 개선할 수 없다.



If you can not **detect** it, you can not **analyze** it.

If you can not analyze it, you can not **mitigate** it.

탐지할 수 없으면 분석할 수 없고, 분석할 수 없으면 대응할 수 없다.

정보와 자산에 대한 가시성 확보는 보안의 부수적 / 수동적 활동이 아니라 필수적 / 결정적 활동



## S2W와 솔루션에 대해 더 알고 싶으신가요?

아래의 메일 주소로 문의주세요.

[info@s2w.inc](mailto:info@s2w.inc)

[www.s2w.inc](http://www.s2w.inc)

경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층 | +82 07 5066 5277

The information contained in this document is proprietary and confidential.  
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.



# Introduction

## Malware & Threat Analysis

- **TALON (Center for Threat Research & Intelligence @S2W ,2020.09 ~ )**
  - 사이버 위협 인텔리전스(**Cyber Threat Intelligence**) 연구 및 분석
    - TST (Talon Strategy Team, 2022.08 ~ )
    - BLKSMTH (Threat Analysis Team, 2020.09 ~ 2022.08)
    - Operation Newton: Hi **Kimsuky**? Did an Apple(seed) really fall on Newton's head? 주저자 @VirusBulletin (2021)
- 침해대응부 침해위협분석팀 @금융보안원 (2016 ~ 2020.09)
  - 위협 인텔리전스 분석 및 금융권 버그바운티(Bug Bounty) 운영
  - 한글문서를 이용하는 악성코드 프로파일링 'Campaign DOKKAEBI' 주저자 (2018)
  - **Kimsuky group**: tracking the king of the spear-phishing 주저자 @VirusBulletin (2019)

## Digital Forensic

- 사이버 선거 범죄 대응 센터 @중앙선거관리위원회 (2016)

## M.S. degree - Information Security

- SANE Lab, 고려대학교 정보보호대학원 (2014 ~ 2016)



- 1. Background:  
Attack Surface vs Attack Vector**
- 2. Case Study**
- 3. Conclusion**

An aerial photograph of a two-lane asphalt road winding through a dense forest of trees with vibrant autumn foliage in shades of orange, yellow, and brown. A small, light-colored car is positioned in the center of the road, facing away from the viewer. The text is overlaid on the road.

**Background:**

**Attack Surface vs Attack Vector**



# Background: Attack Surface vs Attack Vector

## Attack Surface

- 공격 가능한 표적 시스템, 서비스, 애플리케이션 및 네트워크 등의 모든 영역
- 공격자가 시스템에 침투할 수 있는 가능성이 있는 지점
- 예) 회사의 인터넷 연결된 서버, 클라우드 환경, 모바일 디바이스 등이 모두 Attack Surface의 일부

## Attack Vector

- 공격자가 Attack Surface에 침투하는 데 사용하는 구체적인 방법
- 공격자가 시스템에 악성 코드를 삽입하거나, 인증 정보를 유출하는 등의 공격을 실행하는 방법
- 예) 공격자가 시스템에 침투하는 데 사용하는 Attack Vector는 피싱 메일, 스팸 메시지, 악성 링크 등

# Where? How!

# Background: Attack Surface vs Attack Vector

**Attack Surface**

**Attack Vector**

**Attack Surface: 시스템의 공격 가능한 영역**

**Attack Vector: 공격자가 시스템에 침투하는 데 사용하는 구체적인 방법**

# Where? How!

# Background: Attack Surface vs Attack Vector

## Attack Surface

**Reconnaissance**  
(1<sup>st</sup> step of MITRE ATT&CK/Cyber Kill Chain)

# Where?

The screenshot shows the Quaxar interface for the Kimsuky Threat Actor. The MITRE ATT&CK report is displayed with columns for Reconnaissance, Resource Development, Initial Access, Execution, Persistence, and Privilege Escalation. The Reconnaissance column is highlighted with a red box, indicating it is the focus of the slide.

| Reconnaissance                              | Resource Development               | Initial Access                               | Execution   | Persistence                                | Privilege Escalation                           |
|---|------------------------------------|--|---|--|--|
| Active Scanning<br>T1595                    | Acquire Infrastructure<br>T1583    | Drive-by Compromise<br>T1189                 | Command and Scripting Interpreter<br>T1059          | Account Manipulation<br>T1098              | Abuse Elevation Control Mechanism<br>T1548     |
| Gather Victim Host Information<br>T1592     | Compromise Accounts<br>T1586       | Exploit Public-Facing Application<br>T1190   | PowerShell<br>T1059.001                             | BITS Jobs<br>T1197                         | Access Token Manipulation<br>T1134             |
| Gather Victim Identity Information<br>T1589 | Social Media Accounts<br>T1586.001 | Replication Through Removable Media<br>T1091 | AppleScript<br>T1059.002                            | Browser Extensions<br>T1176                | Boot or Logon Autostart Execution<br>T1547     |
| Gather Victim Network Information<br>T1590  | Email Accounts<br>T1586.002        | Trusted Relationship<br>T1199                | Windows Command Shell<br>T1059.003                  | Compromise Client Software Binary<br>T1554 | Boot or Logon Initialization Scripts<br>T1037  |
| Gather Victim Org Information<br>T1591      | Compromise Infrastructure<br>T1584 |  | Unix Shell<br>T1059.004                             | Create Account<br>T1136                    | Create or Modify System Process<br>T1543       |
| Phishing for Information<br>T1598           | Develop Capabilities<br>T1587      |  | Visual Basic<br>T1059.005                           | Create or Modify System Process<br>T1543   | Domain Policy Modification<br>T1484            |
| Spearphishing Service<br>T1598.001          | Establish Accounts<br>T1585        |  | Python<br>T1059.006                                 | Event Triggered Execution<br>T1546         | Escape to Host<br>T1611                        |
| Spearphishing Attachment<br>T1598.002       | Obtain Capabilities<br>T1588       |  | JavaScript<br>T1059.007                             | Hijack Execution Flow<br>T1574             | Event Triggered Execution<br>T1546             |
| Spearphishing Link<br>T1598.003             | Stage Capabilities<br>T1608        |  | Network Device CLI<br>T1059.008                     | Implant Internal Image<br>T1525            | Exploitation for Privilege Escalation<br>T1556 |
|   |                                    |  | Component Object Model and Distributed COM<br>T1175 | Modify Authentication Process<br>T1556     |  |

# Background: Attack Surface vs Attack Vector

**Attack Surface**

Attack Vector

From the defender's perspective,  
start by identifying the Attack Surface

**Where?** How!

# Case Study



## Summary

- 1) 외부에 노출된 자산(IP 주소(CIDR 포함), 도메인, 인증서 등) 식별
- 2) 내부 자산과 관련된 취약점 정보
- 3) 주요 자산에 대한 유출된 계정 정보
- 4) 외부에 노출된 클라우드 자산 식별
- 5) 개발/운영 상 잘못된 구성 및 미숙한 운영에 따른 민감정보 노출

# Case Study

## #01 Identifying External exposure of assets

- 외부에 노출된 자산: IP 주소(CIDR 포함), 도메인, 인증서 등



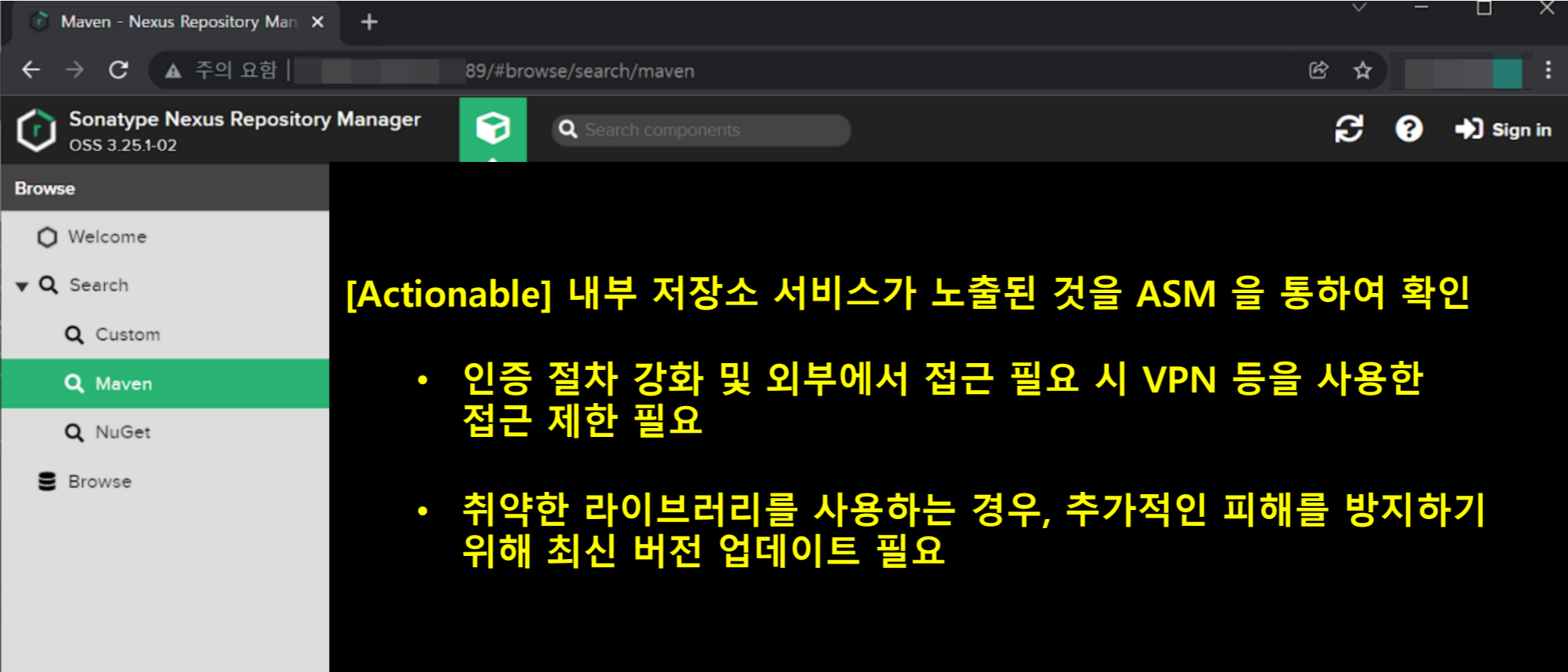
## #01 Identifying External exposure of assets

- 외부에 노출된 자산: IP 주소(CIDR 포함), 도메인, **인증서** 등
- (예) 디렉토리 리스팅이 되는 개발 서버: **A사의 SSL 인증서를 사용**하는 개발 서버를 발견



## #02 Vulnerability information of exposed assets

- 내부 저장소(repository) 서비스 외부 노출 및 미흡한 인증절차
- (예) 별도의 인증절차 없이 외부에 노출된 내부 저장소 서버: B사 소유 IP 대역에서 발견
  - 내부 저장소 내 취약한 라이브러리 사용: CVE-2021-44228에 취약한 2.16이하 버전의 log4j 사용
  - 사용중인 라이브러리의 버전 정보를 수집한 악의적인 공격자가 취약한 log4j 라이브러리를 사용하는 서비스 대상의 원격명령실행(RCE) 공격을 수행 가능



The screenshot shows the Sonatype Nexus Repository Manager (ASM) web interface. The browser address bar displays the URL `89/#browse/search/maven`. The page header includes the Sonatype logo, the text "Sonatype Nexus Repository Manager OSS 3.25.1-02", a search bar with the placeholder "Search components", and a "Sign in" button. The left sidebar contains a "Browse" menu with options: "Welcome", "Search", "Custom", "Maven" (highlighted in green), "NuGet", and "Browse".

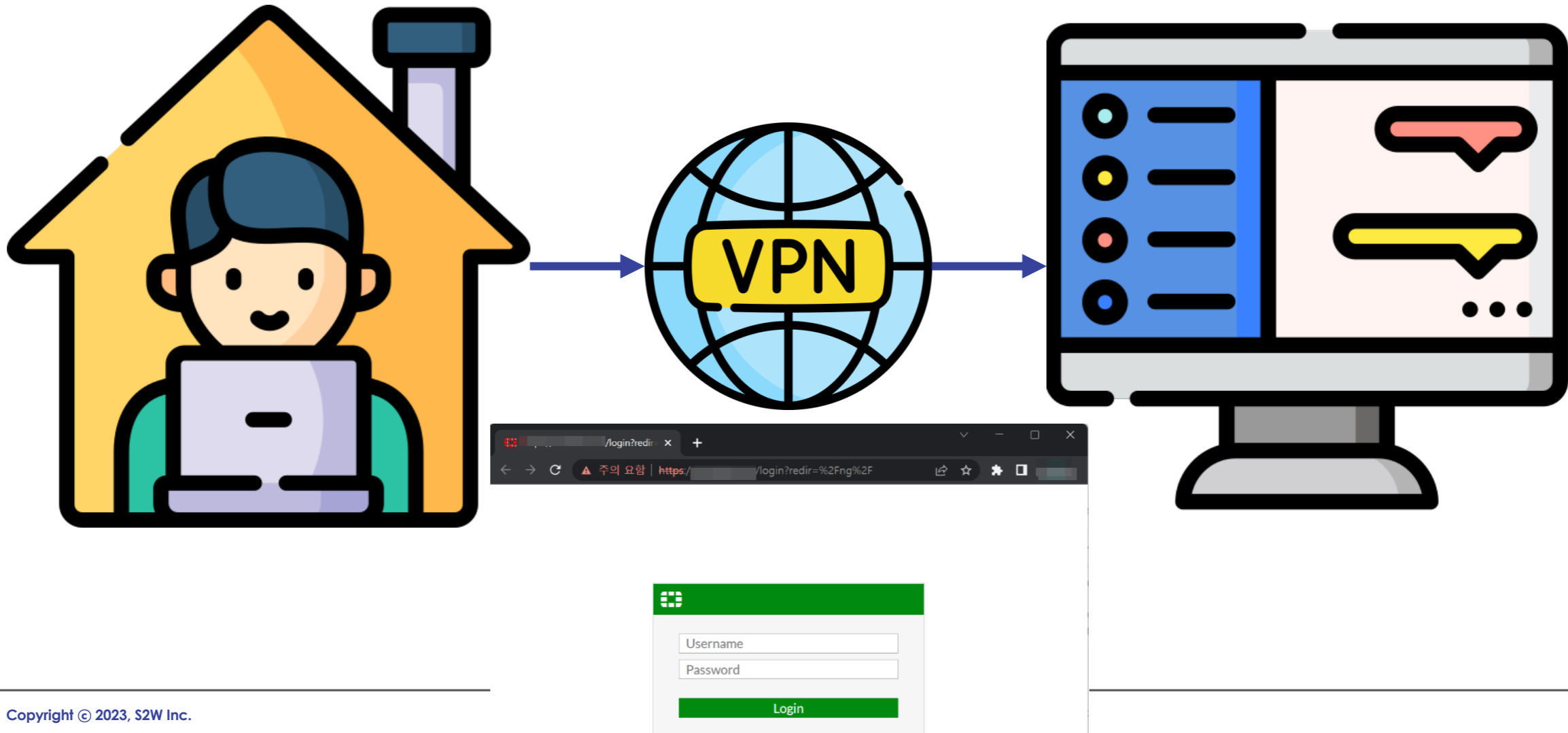
**[Actionable] 내부 저장소 서비스가 노출된 것을 ASM 을 통하여 확인**

- 인증 절차 강화 및 외부에서 접근 필요 시 VPN 등을 사용한 접근 제한 필요
- 취약한 라이브러리를 사용하는 경우, 추가적인 피해를 방지하기 위해 최신 버전 업데이트 필요

# Case Study

## #03 Credential leakage of exposed assets

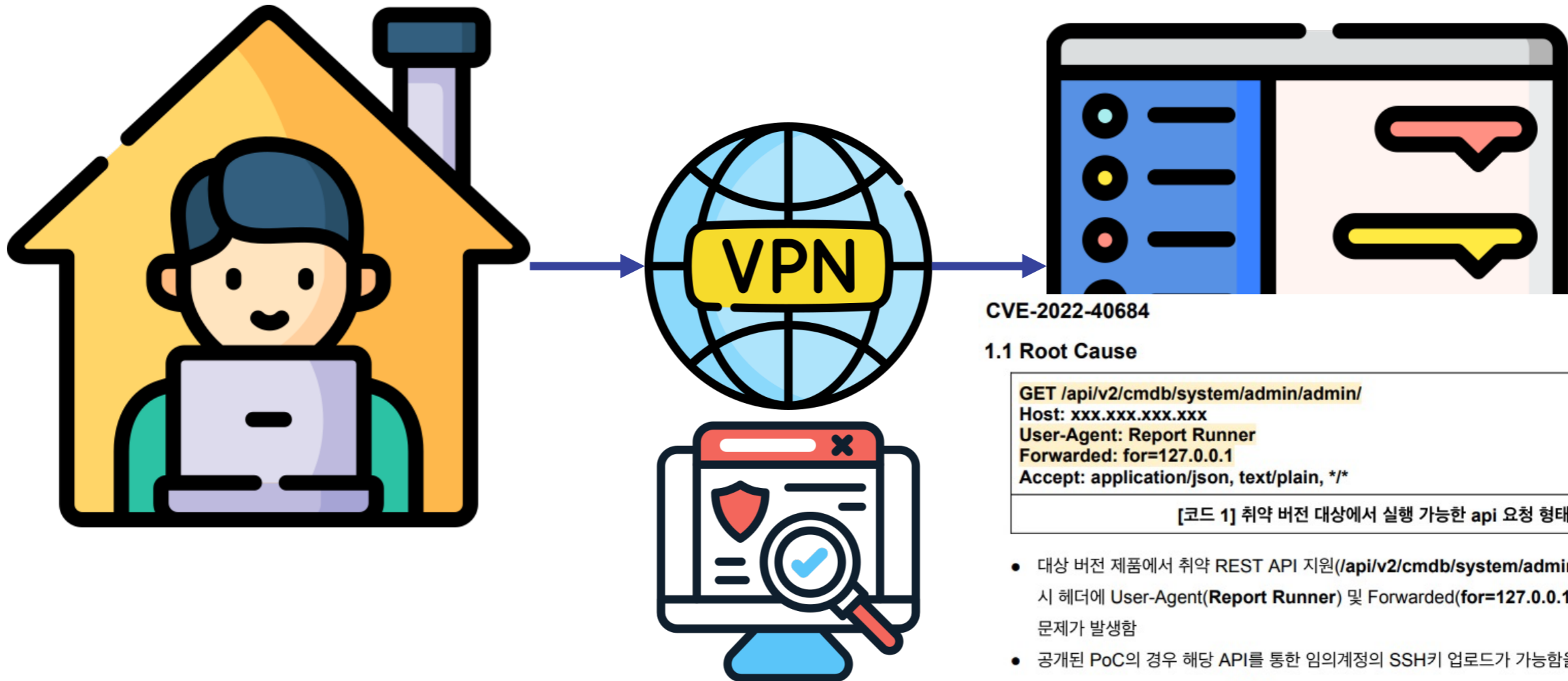
- 외부 노출된 주요 자산



# Case Study

## #03 Credential leakage of exposed assets

- 외부 노출된 주요 자산



CVE-2022-40684

### 1.1 Root Cause

```
GET /api/v2/cmdb/system/admin/admin/  
Host: xxx.xxx.xxx.xxx  
User-Agent: Report Runner  
Forwarded: for=127.0.0.1  
Accept: application/json, text/plain, */*
```

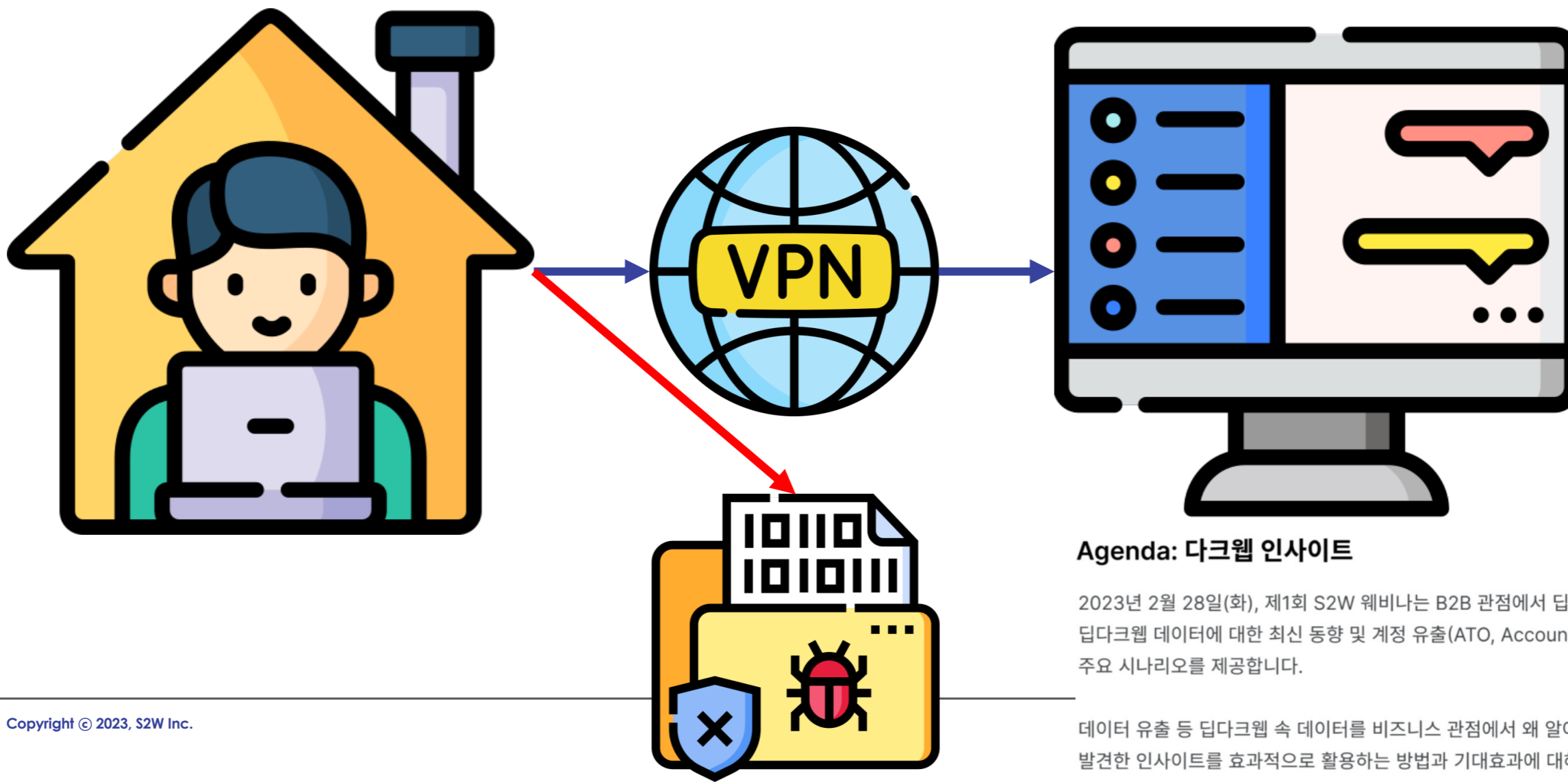
[코드 1] 취약 버전 대상에서 실행 가능한 api 요청 형태

- 대상 버전 제품에서 취약 REST API 지원(/api/v2/cmdb/system/admin/admin/)을 하며 요청 시 헤더에 User-Agent(Report Runner) 및 Forwarded(for=127.0.0.1) 필드를 충족할 경우 문제가 발생함
- 공개된 PoC의 경우 해당 API를 통한 임의계정의 SSH키 업로드가 가능함을 명시하였으며 이를 통해 공격자의 관리자 계정 SSH 접근 및 원격명령 실행, 연동된 내부 인프라 추가 접근이 가능함
- 취약 버전 대상 제품을 사용하고 있을 경우 패치 버전 혹은 최신 버전 업데이트를 권장하며 업데이트가 제한될 경우 외부에서의 HTTP/HTTPS 요청 차단을 권장함

# Case Study

## #03 Credential leakage of exposed assets

- 외부 노출된 주요 자산에 대한 계정 정보 유출



### Agenda: 다크웹 인사이트

2023년 2월 28일(화), 제1회 S2W 웨비나는 B2B 관점에서 딥다크웹 데이터 중요성과 딥다크웹 데이터에 대한 최신 동향 및 계정 유출(ATO, Account Take Over)에 대한 주요 시나리오를 제공합니다.

데이터 유출 등 딥다크웹 속 데이터를 비즈니스 관점에서 왜 알아야 하는지, 조직이 발견한 인사이트를 효과적으로 활용하는 방법과 기대효과에 대해 이야기합니다.

# Case Study

## #03 Credential leakage of exposed assets

- 외부 노출된 주요 자산에 대한 계정 정보 유출
- (예1)

### VPN 계정 정보

| <input type="checkbox"/> | Site        | Victim | Country     | Account | Date Exposed ▾ |
|--------------------------|-------------|--------|-------------|---------|----------------|
| <input type="checkbox"/> | vpn. .com   | 6 1    | South Korea |         | 2023.04.11     |
| <input type="checkbox"/> | vpn. .go.kr | 1 5    | South Korea |         | 2023.04.11     |
| <input type="checkbox"/> | .vpn. .com  | 1 .49  | -           |         | 2023.04.10     |
| <input type="checkbox"/> | vpn. .com   | 2 5    | South Korea |         | 2023.04.10     |
| <input type="checkbox"/> | vpn. .i.com | 1 9    | South Korea |         | 2023.04.10     |
| <input type="checkbox"/> | vpn. .r.com | 2 5    | South Korea |         | 2023.04.10     |
| <input type="checkbox"/> | vpn. .or.kr | 8 11   | Netherlands |         | 2023.04.10     |
| <input type="checkbox"/> | vpn. .com   | 1 1    | South Korea |         | 2023.04.10     |

# Case Study

## #03 Credential leakage of exposed assets

- 외부 노출된 주요 자산에 대한 계정 정보 유출
- (예2) Groove 유출 사이트에 공개된 전세계 Fortinet VPN 계정 정보 (중복제거 결과: 11,270개 중 한국IP 378개)

**Groove** | Утечки | Новости | О нас

### Запатченные fortinet точки входа

Опубликовано: 07 Сентября 2021 в 19:09 | Просмотров: 2093

<http://flhnknbdg7yddsu3gj5lyn2wjkb3mmuoatmi5z5qe2oddiiyizlwyad.onion/forti/>

порты 10443 и 443

Все прочекано на валид

|              |   |        |
|--------------|---|--------|
| 10443_0_1/KR | 2 | 3.txt  |
| 10443_0_1/KR | 2 | 50.txt |
| 10443_0_1/KR | 2 | 7.txt  |
| 10443_0_1/KR | 2 | 4.txt  |
| 10443_0_1/KR | 2 | 9.txt  |
| 10443_0_1/KR | 1 | 8.txt  |
| 10443_0_1/KR | 1 | 4.txt  |
| 10443_0_1/KR | 1 | 4.txt  |
| 10443_0_1/KR | 1 | 5.txt  |
| 10443_0_1/KR | 1 | 8.txt  |
| 10443_0_1/KR | 2 | 8.txt  |
| 10443_0_1/KR | 5 | 2.txt  |
| 10443_0_1/KR | 6 | 6.txt  |
| 10443_0_1/KR | 1 | 6.txt  |
| 10443_0_1/KR | 1 | 5.txt  |
| 10443_0_1/KR | 2 | 8.txt  |
| 10443_0_1/KR | 1 | 10.txt |
| 10443_0_1/KR | 5 | 9.txt  |
| 10443_0_1/KR | 5 | 5.txt  |
| 10443_0_1/KR | 1 | 52.txt |
| 10443_0_1/KR | 1 | 4.txt  |
| 10443_0_1/KR | 1 | 9.txt  |
| 10443_0_1/KR | 2 | 6.txt  |

|    |        |
|----|--------|
| 1  | 4.txt  |
| 1  | r :D   |
| 2  | r :D   |
| 3  | z :w   |
| 4  | r :De  |
| 5  | g s:Tj |
| 6  | sa :k  |
| 7  | kl :<j |
| 8  | so :k0 |
| 9  | j :j   |
| 10 | r :D   |

## #03 Credential leakage of exposed assets

- 외부 노출된 주요 자산에 대한 계정 정보 유출
- (예2) Groove 유출 사이트에 공개된 전세계 Fortinet VPN 계정 정보 (중복제거 결과: 11,270개 중 한국IP 378개)

S2W TALON <talon@s2w.inc>

안녕하세요. S2W CTI팀입니다.

보내주신 IP 관련하여, 유출 정보에 집중하여 추가 확인한 결과,

올해 9월 초 이슈가 되었던 DDW 상에서 확보 및 분석된 내용에 포함된 데이터에 해당 IP 정보를 발견 할 수 있었습니다.

### [Actionable] 주요 자산에 접근 가능한 계정 정보를 ASM 을 통하여 확인

- 내부망 또는 업무망의 접근을 위한 VPN과 같은 주요 자산의 유출된 계정정보를 공격자가 악용하는 경우, 민감 자료 열람 및 탈취와 같은 2차 피해로 이어질 수 있음
- 외부와 내부(업무)망 접점이 있는 자산과 유출된 계정정보에 대한 가시성 확보 필요

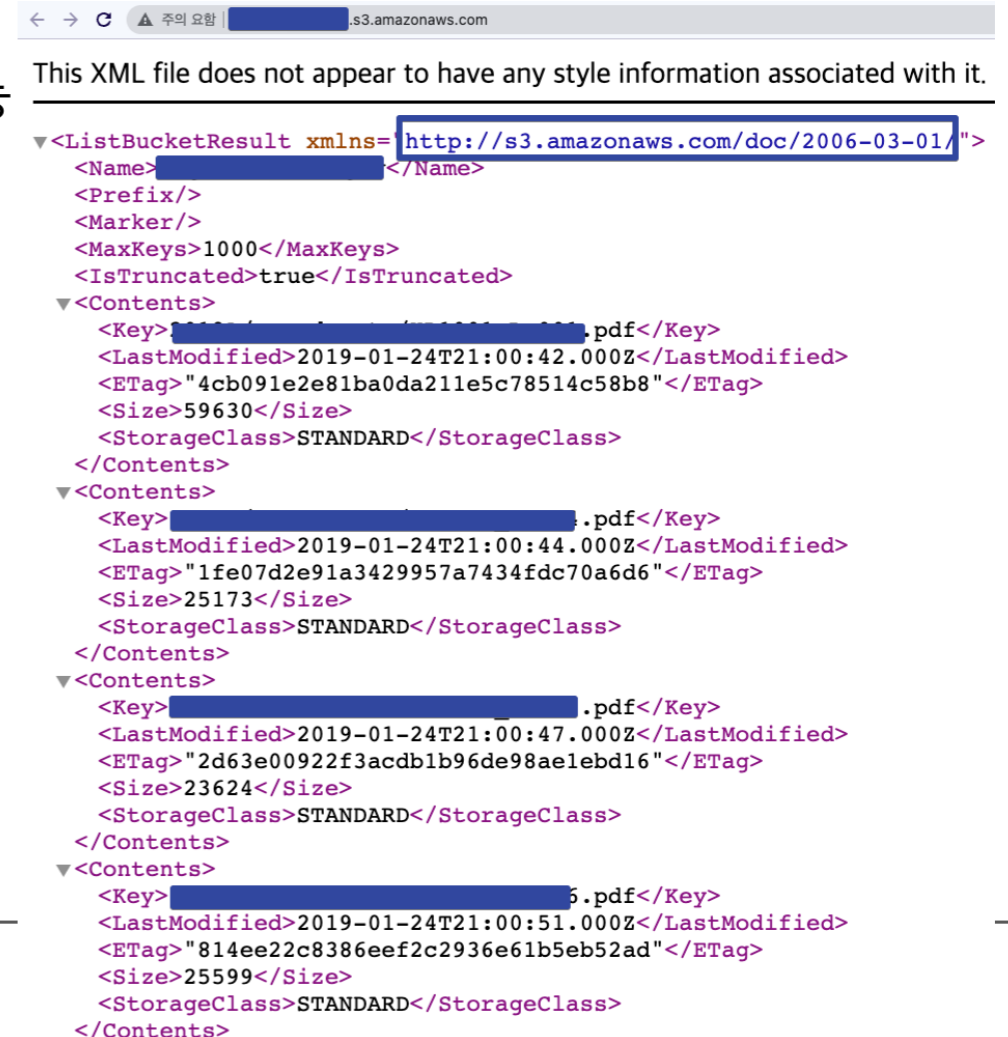


## #04 Identifying External exposure of Cloud assets

- 외부에 노출된 클라우드 자산: IP 주소(CIDR 포함), 도메인, 인증서 등
- (예) 클라우드 운영 실수에 의한 주요 자산 노출: AWS S3 Bucket 외부 노출 및 열람 가능

- 01) 별도의 인증없이 서비스 리소스에 접근 및 다운로드 가능

s3.amazonaws.com/[bucket\_name]  
[bucket\_name].s3.amazonaws.com



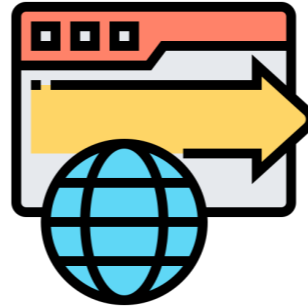
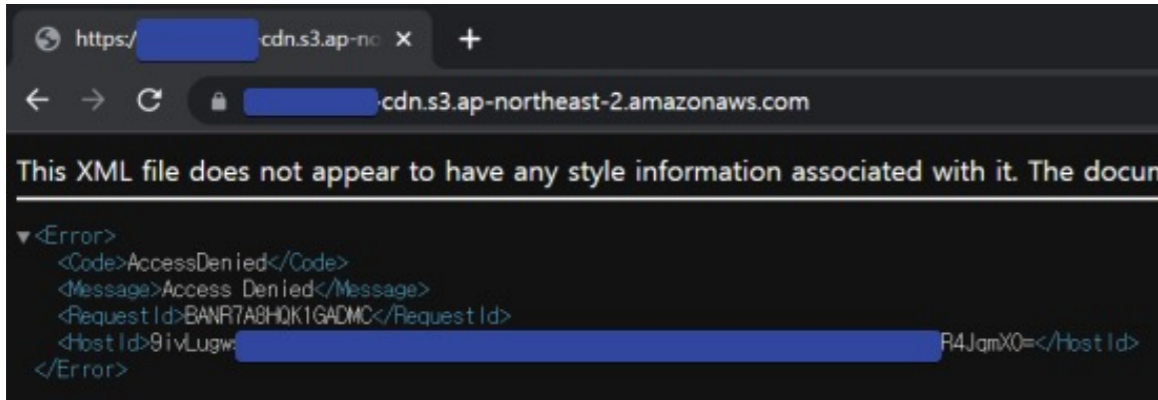
```
<?xml version="1.0" encoding="UTF-8" ?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>[redacted]</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>true</IsTruncated>
  <Contents>
    <Key>[redacted].pdf</Key>
    <LastModified>2019-01-24T21:00:42.000Z</LastModified>
    <ETag>"4cb091e2e81ba0da211e5c78514c58b8"</ETag>
    <Size>59630</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>[redacted].pdf</Key>
    <LastModified>2019-01-24T21:00:44.000Z</LastModified>
    <ETag>"1fe07d2e91a3429957a7434fdc70a6d6"</ETag>
    <Size>25173</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>[redacted].pdf</Key>
    <LastModified>2019-01-24T21:00:47.000Z</LastModified>
    <ETag>"2d63e00922f3acdb1b96de98ae1ebd16"</ETag>
    <Size>23624</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>[redacted].pdf</Key>
    <LastModified>2019-01-24T21:00:51.000Z</LastModified>
    <ETag>"814ee22c8386eef2c2936e61b5eb52ad"</ETag>
    <Size>25599</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```



# Case Study

## #04 Identifying External exposure of Cloud assets

- 외부에 노출된 클라우드 자산: IP 주소(CIDR 포함), 도메인, 인증서 등
- (예) 클라우드 운영 실수에 의한 주요 자산 노출: AWS S3 Bucket 외부 노출 및 열람 가능
  - 02) CDN 설정 오류로 인한 S3 Public Access 허용



## #04 Identifying External exposure of Cloud assets

- 외부에 노출된 클라우드 자산: IP 주소(CIDR 포함), 도메인, 인증서 등
- (예) 클라우드 운영 실수에 의한 주요 자산 노출: AWS S3 Bucket 외부 노출 및 열람 가능
  - 01) 별도의 인증없이 서비스 리소스에 접근 및 다운로드 가능
  - 02) CDN 설정 오류로 인한 S3 Public Access 허용

**[Actionable] 클라우드 저장소 서비스가 노출된 것을 ASM 을 통하여 확인**

- 클라우드 스토리지 내 디렉토리의 접근제어 및 권한 관리 적용 필요
- 클라우드 스토리지와 연결된 리다이렉트 도메인에 대한 접근제어 및 CDN 설정 오류 확인 필요

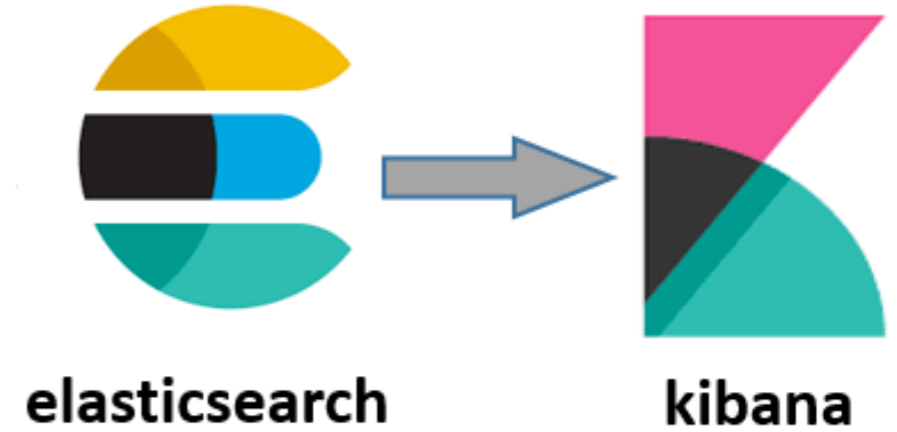
## #05 Misconfigured and inexperienced operation in the DevOps environment

- 개발/운영 상 잘못된 구성 및 미숙한 운영에 따른 민감정보 노출
- (예) 대표적인 개발/운영 환경: Database, Repository, IDE ...

# Case Study

## #05 Misconfigured and inexperienced operation in the DevOps

- 개발/운영 상 잘못된 구성 및 미숙한 운영에 따른 민감정보 노출
- (예) 대표적인 개발/운영 환경: Database, Repository, IDE ...



## 한국의 대형 뷰티 플랫폼 파우더룸, 개인정보 DB 방치해 노출됐었다

300만 넘는 회원 보유한 초대형 뷰티 플랫폼...현재는 문제 해결된 것으로 보여

요약 : 사이버뉴스 연구조사팀에 의하면 한국의 뷰티 콘텐츠 카페인 파우더룸(PowderRoom)에서 약 100만 명의 개인정보가 유출됐다고 한다. 파우더룸의 회원은 350만 명이라고 하는데, 이런 사용자들의 정보가 저장되어 있던 데이터베이스가 1년 넘게 인터넷에 노출되어 있었다고 한다. 이름, 전화번호, 이메일 주소, 인스타그램 사용자 ID, 거주지 주소 등이 아무런 보호장치 없이 공개된 상태로 유지된 것으로 조사됐다. 다행히 이러한 사실이 파우더룸과 KISA 인터넷침해대응센터에 제보돼 현재는 해당 데이터베이스가 비공개로 전환된 상황이다.

IP: [REDACTED]  
Port: 5601  
URL: http://[REDACTED]:5601 [🔗]

First seen 2021-11-19 03:54  
Last seen 2023-02-14 08:26  
Open for 452 days

Severity: **high**

```
Indices: 227, document count: 563107329, size: 151.8 GB
Through Kibana endpoint
Found index powderroom-scheduler-2023.01.27 with 12953462 documents (3.2 GB)
Found index powderroom-zuul-2023.02.01 with 1809465 documents (392.5 MB)
Found index powderroom-messaging-2023.01.25 with 12373 documents (8.3 MB)
Found index .kibana_1 with 27 documents (101.8 kB)
Found index powderroom-scheduler-2023.01.20 with 11228826 documents (2.7 GB)
Found index powderroom-zuul-2022.01.30 with 1658884 documents (667.4 MB)
Found index powderroom-zuul-2023.01.23 with 1028043 documents (223.6 MB)
Found index powderroom-oauth2-2023.01.31 with 21379 documents (60.2 MB)
Found index powderroom-server-2023.02.13 with 11571 documents (20.9 MB)
```

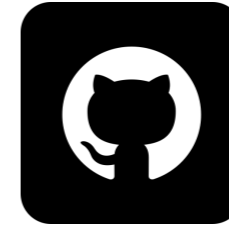
Found on 2023-02-14 08:26

151.8 GBytes 563107329 rows

# Case Study

## #05 Misconfigured and inexperienced operation in the DevOps environment

- 개발/운영 상 잘못된 구성 및 미숙한 운영에 따른 민감정보 노출
- (예) 대표적인 개발/운영 환경: Database, Repository, IDE ...



```
src/db.config.ts
14 dialect: 'mysql',
15 host: '████-mysql.████.dev.████.in',
16 port: 3306,
17 username: '████_user',
18 password: '████████████████████',
19 database: '████_log',
```

TypeScript Showing the top two matches Last indexed on 26 Mar

- C사 서비스의 데이터 베이스 접근 정보 노출:

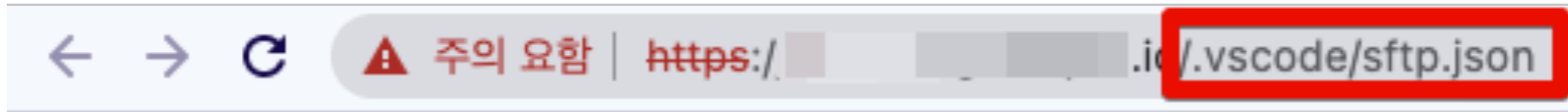
과거 C사에 재직자의 개인 코드 저장소에서 발견된 민감정보로, Github 상에서 검색 시 누구나 접근 가능

내부 도메인과 데이터베이스 서버 포트 정보, 그리고 접근 가능한 계정 정보가 노출되어 있는 상태로 유효성 판단 후 계정 초기화 작업 필요

# Case Study

## #05 Misconfigured and inexperienced operation in the DevOps environment

- 개발/운영 상 잘못된 구성 및 미숙한 운영에 따른 민감정보 노출
- (예) 대표적인 개발/운영 환경: Database, Repository, IDE ...



```
{  
  "name": ":-dev",  
  "host": "1(74",  
  "protocol": "sftp",  
  "port": 22,  
  "username": "root",  
  "password": ":",  
  "remotePath": "/var/www/html/ /",  
  "uploadOnSave": true  
}
```

- 개발환경 설정 정보 노출:

개발 환경에서 사용되는 설정 정보가 실제 운영 서비스 반영되어 노출되는 사례

예시)

- .vscode/[service].json
- .vscode/[service].config
- .ssh/config
- .gitignore
- .bashhistory
- .vim

## #05 Misconfigured and inexperienced operation in the DevOps environment

- 개발/운영 상 잘못된 구성 및 미숙한 운영에 따른 민감정보 노출
- (예) 대표적인 개발/운영 환경: Database, Repository, IDE ...

### [Actionable] DevOps 관련 민감정보가 노출된 것을 ASM 을 통하여 확인

- 데이터베이스에 대한 접근 제한 강화 및 외부노출 비활성화 또는 내부 접근으로 전환
- 저장소 상에서 노출된 민감 정보에 대한 유효성 확인 및 초기화 작업 수행, 노출된 저장소에 대한 TAKE DOWN 진행
- 실제 운영 서비스 상에 업로드 된 설정정보 삭제 및 노출된 설정 정보로 접근 하려는 시도 차단  
CI/CD 파이프라인 또는 개발자 커밋 시 보안 검사 적용

A top-down perspective of a person's feet in brown leather shoes standing on a cracked asphalt surface. A large, irregular hole in the pavement reveals a distorted, inverted reflection of a skyscraper and an airplane in flight. The word "Conclusion" is overlaid in white text on the reflection.

# Conclusion



# Background: Attack Surface vs Attack Vector

## Attack Surface

### Reconnaissance

(1<sup>st</sup> step of MITRE ATT&CK/Cyber Kill Chain)

# Where?

The screenshot shows the Quaxar interface for a threat actor named 'Kimsuky'. The 'MITRE ATT&CK' section is active, showing a grid of techniques categorized into six groups: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, and Privilege Escalation. The 'Reconnaissance' column is highlighted with a red border. The techniques listed in this column are: Active Scanning (T1595), Gather Victim Host Information (T1592), Gather Victim Identity Information (T1589), Gather Victim Network Information (T1590), Gather Victim Org Information (T1591), Phishing for Information (T1598), Spearphishing Service (T1598.001), Spearphishing Attachment (T1598.002), and Spearphishing Link (T1598.003).

| Reconnaissance                              | Resource Development               | Initial Access                               | Execution   | Persistence                                | Privilege Escalation                           |
|---|------------------------------------|--|---|--|--|
| Active Scanning<br>T1595                    | Acquire Infrastructure<br>T1583    | Drive-by Compromise<br>T1189                 | Command and Scripting Interpreter<br>T1059          | Account Manipulation<br>T1098              | Abuse Elevation Control Mechanism<br>T1548     |
| Gather Victim Host Information<br>T1592     | Compromise Accounts<br>T1586       | Exploit Public-Facing Application<br>T1190   | PowerShell<br>T1059.001                             | BITS Jobs<br>T1197                         | Access Token Manipulation<br>T1134             |
| Gather Victim Identity Information<br>T1589 | Social Media Accounts<br>T1586.001 | Replication Through Removable Media<br>T1091 | AppleScript<br>T1059.002                            | Browser Extensions<br>T1176                | Boot or Logon Autostart Execution<br>T1547     |
| Gather Victim Network Information<br>T1590  | Email Accounts<br>T1586.002        | Trusted Relationship<br>T1199                | Windows Command Shell<br>T1059.003                  | Compromise Client Software Binary<br>T1554 | Boot or Logon Initialization Scripts<br>T1037  |
| Gather Victim Org Information<br>T1591      | Compromise Infrastructure<br>T1584 |  | Unix Shell<br>T1059.004                             | Create Account<br>T1136                    | Create or Modify System Process<br>T1543       |
| Phishing for Information<br>T1598           | Develop Capabilities<br>T1587      |  | Visual Basic<br>T1059.005                           | Create or Modify System Process<br>T1543   | Domain Policy Modification<br>T1484            |
| Spearphishing Service<br>T1598.001          | Establish Accounts<br>T1585        |  | Python<br>T1059.006                                 | Event Triggered Execution<br>T1546         | Escape to Host<br>T1611                        |
| Spearphishing Attachment<br>T1598.002       | Obtain Capabilities<br>T1588       |  | JavaScript<br>T1059.007                             | Hijack Execution Flow<br>T1574             | Event Triggered Execution<br>T1546             |
| Spearphishing Link<br>T1598.003             | Stage Capabilities<br>T1608        |  | Network Device CLI<br>T1059.008                     | Implant Internal Image<br>T1525            | Exploitation for Privilege Escalation<br>T1556 |
|   |                                    |  | Component Object Model and Distributed COM<br>T1175 | Modify Authentication Process<br>T1556     |  |

## Summary

- 1) 외부에 노출된 자산(IP 주소(CIDR 포함), 도메인, 인증서 등) 식별
- 2) 내부 자산과 관련된 취약점 정보
- 3) 주요 자산에 대한 유출된 계정 정보
- 4) 외부에 노출된 클라우드 자산 식별
- 5) 개발/운영 상 잘못된 구성 및 미숙한 운영에 따른 민감정보 노출

# Conclusion

## Reality

### "한국 인터넷 침입 선포"...'샤오치잉' 정체는?

입력 2023-01-26 06:42 | 수정 2023-01-26 06:42



#### 앵커

지난 설 연휴 기간에 국내 학술기관 홈페이지 십여 곳이 해킹당했습니다.

중국 해커들로 추정되는데, 이들은 이달 초부터 해킹을 시도해서 일부 개인정보를 유출해

김윤미 기자입니다.

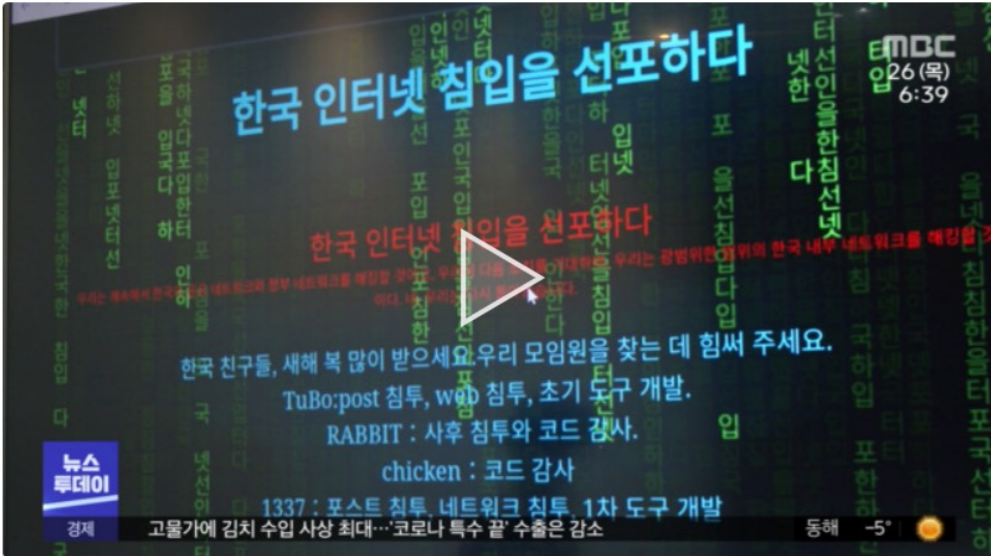
| 대상              | URL                      | IP              | 공격 유형                                   |
|-----------------|--------------------------|-----------------|---|
| 대한건설정책연구원       | ricon.re.kr              | 139.150.74.252  | 웹사이트 디펜이스<br>개인정보 유출 (ID, PW, 주소, 소속 등) |
| 한국고고학회          | kras.or.kr               | 222.239.254.105 | SQL 유출<br>웹사이트 디펜이스                     |
| 한국시각장애교육재활학회    | kaer.or.kr               | 222.239.254.105 | 일부 소스코드 샘플<br>웹사이트 디펜이스                 |
| 대한고령친화산업학회      | www.kr-kafa.org          | 222.234.3.219   | 일부 소스코드 샘플                              |
| 한국학부모학회         | aspg.or.kr               | 222.239.254.105 | SQL 유출<br>웹사이트 디펜이스                     |
| 한국교육원리학회        | edaca.kr                 | 222.239.254.105 | SQL 유출<br>웹사이트 디펜이스                     |
| 우리말학회           | woorimal.org             | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국교원대학교 유아교육연구소 | kriece.or.kr             | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국동서정신과학회       | kewms.co.kr              | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국보건기초의학회       | kmhs.newnonmun.com       | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국사회과학협회        | klsqss.or.kr             | 222.239.254.105 | 웹사이트 디펜이스                               |
| 제주대학교 교육과학연구소   | edusci.jejunu.ac.kr      | 222.239.254.105 | 웹사이트 디펜이스                               |
| 대한국순구개열학회       | cleftlp.or.kr            | 222.239.254.105 | 웹사이트 디펜이스                               |
| MeFOT창의인성학회     | mefot.kr                 | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국생리인류과학회       | www.ekspa.or.kr          | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국복지행정학회        | www.kawa.kr              | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국특수교육교과교육학회    | seci.kr                  | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국일본교육학회        | skje.co.kr               | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국연극예술치료학회      | koreadramaarttherapy.org | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국발달지원학회        | baldal.net               | 222.239.254.105 | 웹사이트 디펜이스                               |
| 영성과 보건복지학회      | kashw.net                | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국부모교육학회        | childcare.newnonmun.com  | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국기초간호학회        | www.bionursing.or.kr     | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국핵심역량교육학회      | www.kacce.kr             | 222.239.254.105 | 웹사이트 디펜이스                               |
| 페세라 학술지         | pecera.newnonmun.com     | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국관광서비스학회       | www.kotsa.kr             | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국노년학연구회        | kges.newnonmun.com       | 222.239.254.105 | 웹사이트 디펜이스                               |
| 한국보육지원학회        | www.educarechild.com     | 222.239.254.105 | 웹사이트 디펜이스                               |

- 1) 외부에 노출된 자산(IP 주소 (CIDR 포함), 도메인, 인증서 등) 식별

## Reality

### "한국 인터넷 침입 선포"...'샤오치잉' 정체는?

입력 2023-01-26 06:42 | 수정 2023-01-26 06:42



▶ 연속재생

#### 앵커

지난 설 연휴 기간에 국내 학술기관 홈페이지 십여 곳이 해킹당했습니다.

중국 해커들로 추정되는데, 이들은 이달 초부터 해킹을 시도해서 일부 개인정보를 유출해왔습니다.

김윤미 기자입니다.



JAEGI KIM 03:31

晓骑营(샤오치잉) 해킹팀 관련 현재까지 정리된 사항 공유드립니다.

(참고 : 관련 기사) [https://www.boannews.com/media/view.asp?id=113682&kind=&sub\\_kind=](https://www.boannews.com/media/view.asp?id=113682&kind=&sub_kind=)

- 최근 국내 웹사이트 디페이스 및 해킹 정보에 대하여 게시하는 해킹팀의 활동을 포착하여 관련 분석을 진행
  - [텔레그램 공지채널(메인채널)] - 晓骑营
  - [텔레그램 대화방(기술교류)] - 晓骑营技术社区
- (활동시기 : 2022.12.28 ~ 현재) 해당 해킹팀은 2022년 12월 말부터 해킹팀 소개를 하면서 2023년 1월초에는 본격적으로 팀원 모집을 진행함
  - (도구) 홍보 시 내부 라이브러리에 Yashma Ransomware builder 를 포함한 각종 도구셋을 공개
  - (데이터) 스틸러 로고를 확보한 예시 사진을 업로드 한 바 있음, 스틸러 로고를 다른 공격에 사용할 가능성 존재
    - 이외 웹 서버의 설정 오류로 config 정보가 노출된 서버를 확보하여 장악한 사례도 존재
  - (취약점) NTLM Tampering, OpenSSH 와 같은 원격 실행 취약점에 대한 언급을 하며 주로 원격에서 침투 테스트를 위한 준비를 하는 것으로 보임
- (홍보방법) 텔레그램 채널 외 별도 블로그를 개설하여 팀원 모집 게시글과 실제로 한국 대상 공격을 수행한 내용에 대하여 업로드
  - [블로그1] - [https://eisae\[.\]org/](https://eisae[.]org/)
  - [블로그2] - [https://tubosheu\[.\]github.io/](https://tubosheu[.]github.io/)
- (공격활동) 2023.01.18. 이후 본격적으로 공격 수행한 결과를 업로드 함
  - (2023.01.18.) 포천시설관리공단([pcss.kr](http://pcss.kr)) 외 국내 사이트 대상 스캐닝
  - (2023.01.20.) 대한건설정책연구원([ricon.re.kr](http://ricon.re.kr)) 웹페이지 디페이스
  - (2023.01.20.) 동아시아연구소([eai.or.kr](http://eai.or.kr)) 웹사이트 대상 SQLi Dumper V.8.5 를 구동
  - (2023.01.21.) 한국 공격 예고 선포, 필요할 때 한국의 중요한 정부 기관 및 주요 인프라의 일부 데이터를 공개할 것이라고 함
  - (2023.01.21.) Breached 포럼에 Eisea 로 가입 및 대한건설정책연구원([ricon.re.kr](http://ricon.re.kr)) 대상 공격 관련 게시글 업로드
  - (2023.01.24.) Breached 포럼에 Eisea 로 국내 학회 웹사이트 해킹 관련 게시글 업로드
    - (샘플 : [kaer.or.kr](http://kaer.or.kr) (한국시각장애교육재활학회), [www.kr-kafa.org](http://www.kr-kafa.org) (대한고령친화산업학회))
  - (2023.01.24.) Breached 포럼에 Eisea 로 국내 학회 웹사이트 해킹 관련 게시글 추가 업로드 , 디페이스 된 웹사이트 및 SQL 샘플 공개
    - [kras.or.kr](http://kras.or.kr) (한국고고학회) , [edaca.kr](http://edaca.kr) (한국교육원리학회) , [aspg.or.kr](http://aspg.or.kr) (한국학부모학회)

언론 보도가 된만큼 자사에 대한 영향도 파악 하시는데 도움이 되길 바라겠습니다.

고객사 관련 정보는 확인되는대로 별도 전달드리겠습니다. (편집됨)

• 3) 주요 자산에 대한 유출된 계정 정보

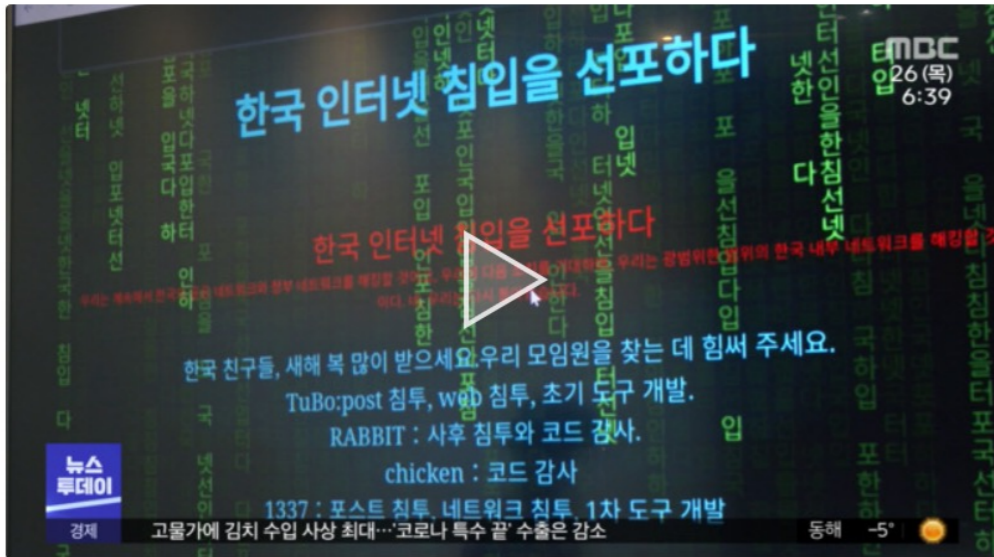
• 5) 개발/운영 상 잘못된 구성 및 미숙한 운영에 따른 민감정보 노출

# Conclusion

## Reality

### "한국 인터넷 침입 선포"...'샤오치잉' 정체는?

입력 2023-01-26 06:42 | 수정 2023-01-26 06:42



▶ 연속재생

#### 앵커

지난 설 연휴 기간에 국내 학술기관 홈페이지 십여 곳이 해킹당했습니다.

중국 해커들로 추정되는데, 이들은 이달 초부터 해킹을 시도해서 일부 개인정보를 유출해왔습니다.

김윤미 기자입니다.

2023.02.17

## Overview of vulnerabilities related to Xiaoqiying(晓骑营) Hacking Team

TALON REPORT > VULNERABILITY

↓ PDF Report

- 최근 국내 웹사이트 디페이스 및 해킹 정보에 대하여 게시하는 샤오치잉(晓骑营) 해킹팀의 활동을 추적하던 중 샤오치잉(晓骑营)이 운영하는 텔레그램 채널에 언급된 공격도구 및 취약점에 대한 분석 진행
    - (참고) [Deep & Dark web User Profiling @晓骑营\(샤오치잉\)](#) (Updated: 2023.02.16.)
  - 언급된 공격도구 관련 주요 제품 및 취약점 정보는 원격에서 임의 코드 실행이 가능한 RCE 취약점으로 확인됨
    - [Apache Log4j \(CVE-2021-44228\)](#)
    - [Spring Cloud \(CVE-2022-22947\)](#)
    - [Spring Framework \(CVE-2022-22965\)](#)
    - [F5 BIG-IP \(CVE-2022-1388\)](#)
    - [Confluence Server/Data Center \(CVE-2021-26084\)](#)
  - 총 39개 공격 도구와 관련된 취약점 영향도 식별 결과, Critical로 분류된 취약점도 20개가 포함된 상태로 취약점에 대한 영향을 받는 버전의 제품 사용 여부 확인과 최신 버전 업데이트 적용이 필요함
    - 식별된 취약점 : 총28개 (Critical 20개, High 6개, Medium 2개, CVSS 기준)
      - Action Item 의 PoC 정보 등을 대응 업무에 적용 시 참고
    - 관련 취약점 정보는 Quaxar 에서도 확인 가능
- **2) 내부 자산과 관련된 취약점 정보**

# Conclusion

Attack Surface Management is absolutely necessary

# Where?





## S2W와 솔루션에 대해 더 알고 싶으신가요?

아래의 메일 주소로 문의주세요.

[info@s2w.inc](mailto:info@s2w.inc)

[www.s2w.inc](http://www.s2w.inc)

경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층 | +82 07 5066 5277

The information contained in this document is proprietary and confidential.  
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.