JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 31 No. 7, pp. 127-140, July 2026
https://doi.org/10.9708/jksci.2026.31.07.127

A Study on the Empirical Analysis of South Korea's Cyber Threat Landscape and Internet-Exposed Asset Vulnerabilities through the Integration of Shodan EASM and Threat Intelligence

Seung Han Yoon*, Ah Reum Kang**

*Student, Dept. of CyberSecurity, Pai Chai University, Daejeon, Korea
**Professor, Dept. of CyberSecurity, Pai Chai University, Daejeon, Korea

[Abstract]

This paper presents a comprehensive analysis of South Korea's cyber threat landscape and internet-exposed asset vulnerabilities by integrating Shodan EASM scan data (April 11, 2026) with CYFIRMA threat intelligence. The scan identified over 37.17 million exposed ports, with 538,230 hosts vulnerable under CISA KEV and 1,820,536 under VulnCheck KEV. Critical findings include 4,321 ICS/OT devices directly exposed to the internet, 25,742 unauthenticated databases, 1,171 BlueKeep-unpatched systems, and 50 hosts with confirmed remote code execution vectors. North Korea-linked APT groups including Lazarus Group, Kimsuky, and APT37, alongside ransomware operators Qilin and LockBit, are actively exploiting these vulnerabilities. This paper proposes a tiered security roadmap with immediate (0-30 days), short-term (1-6 months), and long-term (6+ months) countermeasures, along with sector-specific priority action matrices.

▸ **Key words**: EASM, Cyber Threat Intelligence, KEV, ICS/OT Security, APT Group, Ransomware

[요 약]

본 논문은 2026년 4월 11일 Shodan EASM 스캔 데이터와 CYFIRMA 위협 인텔리전스를 통합 분석하여 대한민국의 사이버 위협 환경 및 인터넷 노출 자산 취약점 현황을 종합 진단한다. 스캔 결과 3,717만 개 이상의 인터넷 노출 포트가 확인되었으며, CISA KEV 기준 538,230개, VulnCheck KEV 기준 1,820,536개의 호스트가 실제 악용이 확인된 취약점에 노출되어 있다. ICS/OT 장비 4,321개의 인터넷상 노출, 인증 없이 접근 가능한 데이터베이스 25,742개, BlueKeep 미패치 1,171개, RCE 가능 호스트 50개가 식별되어 즉각적 대응이 요구된다. 위협 행위자 분석에서 라자루스 그룹, 김수키, APT37 등 북한 연계 APT 그룹과 Qilin, LockBit 랜섬웨어 집단이 해당 취약점을 실제 공격에 활용하는 것으로 분석되었다. 본 논문에서는 즉시·단기·중기·장기 단계별 보안 강화 방안 및 부문별 우선순위 조치 매트릭스를 제시하였다.

▸ **주제어**: 외부 공격표면 관리, 사이버 위협 인텔리전스, 알려진 악용 취약점, ICS/OT 보안, APT 그룹, 랜섬웨어

• First Author: Seung Han Yoon, Corresponding Author: Ah Reum Kang
*Seung Han Yoon (nuricaps@naver.com), Dept. of Information Security, Pai Chai University
**Ah Reum Kang (armk@pcu.ac.kr), Dept. of Information Security, Pai Chai University
• Received: 2026. 05. 13, Revised: 2026. 06. 15, Accepted: 2026. 06. 17.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

1.1 Background and Purpose of Analysis

대한민국은 세계 최고 수준의 인터넷 인프라와 반도체, 조선, 방위산업 등 전략적 첨단 산업을 보유한 디지털 강국이다. 그러나 이러한 디지털 발전의 이면에는 인터넷에 무방비 상태로 노출된 수천만 개의 서비스 포트, 수십만 개의 취약한 호스트, 그리고 이를 집요하게 노리는 국가 지원 해킹 집단과 사이버 범죄 조직이라는 심각한 위협이 도사리고 있다[1]. 2026년 4월 11일 Shodan 기반 외부공격 표면관리(EASM : External Attack Surface Management) 스캔으로 수집된 데이터는[2] 이러한 현실을 구체적으로 보여준다.

본 연구는 두 가지 핵심 데이터 소스를 통합 분석하였다. 첫째, 2026년 4월 11일 실시한 Shodan EASM 스캔 대시보드에서 수집된 13개 모듈의 정량적 취약점 데이터로, 전국적으로 공개된 포트, ICS/OT 시스템, 침해 데이터베이스, CISA/VulnCheck KEV(Known Exploited Vulnerabilities) 취약 호스트, 취약 ISP 및 취약 IP 정보를 망라한다.

Table 1. Shodan EASM scan data (13 modules) as of April 11, 2026

Analysis Item	Description
MODULE 1	Internet-Exposed Open Ports
MODULE 2	Port Usage TOP 10
MODULE 3	Industrial Control Systems
MODULE 4	BlueKeep Unpatched
MODULE 5	Compromised Databases
MODULE 6	Ivanti Pulse Secure
MODULE 7	SMB Authentication
MODULE 8	Top Vulnerability
MODULE 9	RCE to Shell
MODULE 10	CISA KEV (2021.1.1~2026.4.11.)
MODULE 11	VulnCheck KEV (2021.1.1~2026.4.11.)
MODULE 12	Top Vulnerable ISPs
MODULE 13	Top Vulnerable IPs

둘째, 사이버 위협 인텔리전스 전문기관 CYFIRMA의 대한민국 위협 환경 보고서(South Korea Threat Landscape Report, 2026.04.28)로, 북한 및 중국 연계 국가 지원 APT 그룹의 동향, 랜섬웨어 그룹의 공격 추이, 다크웹 지하경제 활동을 분석한다.

본 연구의 목적은 기술적 취약점 데이터와 위협 행위자 분석을 결합하여, 대한민국의 사이버 공격표면(Attack Surface)에 대한 종합적인 현황을 진단하고, 이를 바탕으로 조직이 즉시 실행에 옮길 수 있는 구체적이고 우선순위화된 대응 방안을 제시하는 것이다. 특히 단순한 취약점 목록 나열을 넘어, 실제 위협 행위자가 어떤 경로로 어떤 취약점을 공략하는지를 연계 분석함으로써 리스크 기반 우선순위 결정을 지원한다.

1.2 Overview of South Korea's Cyber Threat Environment

대한민국은 아시아-태평양 지역에서 가장 전략적으로 표적화되는 사이버 환경 중 하나에 속한다[1][3]. 세계 최고 수준의 반도체 생산국이자 글로벌 기술 강국으로서, 정부, 국방, 제조, 금융 부문에 걸쳐 고부가가치 표적을 제공한다. 고도로 통합된 공급망, 성숙한 금융 인프라, 확대되는 전자정부 서비스는 재정적으로 동기화된 사이버 범죄와 국가 주도 정보 수집 작전 모두에 대한 노출을 증가시킨다.

동북아시아의 지정학적 특수성은 국내 디지털 자산에 대한 정찰 활동을 가속화하며, 이는 본 스캔에서 확인된 수천만 개의 포트 노출이라는 결과로 직결된다. 특히 북한 연계 위협 행위자들은 금융 절도, 방산 기밀 탈취, 암호화폐 세탁이라는 다층적 목표하에 대한민국을 집중 공략하고 있다[3]. CYFIRMA 보고서에 따르면, 최근 활동은 이중적 양상을 보인다. 국가 연계 행위자들은 방위 조달, 군사 준비 태세, 경제 협상, 외국인 투자 전략을 표적으로 한 장기 정보 수집을 추구하는 한편, 재정적 동기를 가진 그룹들은 랜섬웨어, 데이터 절도, 탈취한 자격 증명 수익화를 통해 대한민국의 대규모 기업 생태계와 디지털 결제 인프라를 악용하고 있다.

이러한 위협 환경에서 EASM 스캔 결과는 심각한 현실을 보여준다. Shodan 스캔을 통해 파악된 대한민국의 인터넷 연결 자산 규모는 전 세계적으로도 손꼽히는 수준이며, 이 중 미국 CISA가 실제 악용을 공식 확인한 취약점 목록(KEV) 기준으로 절반을 훌쩍 넘는 호스트가 위험에 노출되어 있는 것으로 나타났다. 상용 위협 데이터베이스 기준으로 범위를 넓히면 취약 호스트의 수는 CISA 기준 대비 약 3.4배 이상으로 급증하여, 공식 통계가 실제 위협의 일부만을 반영하고 있음을 시사한다.

이 수치들은 단순한 통계가 아니라, 현재 이 순간 실제 사이버 공격자들이 악용할 수 있는 실제 공격 표면의 크기를 의미한다.

1.3 Methodology and Data Sources

본 논문의 분석 방법론은 세 가지 핵심 요소로 구성된다. 첫 번째는 외부 공격표면 관리(EASM: External

Attack Surface Management) 방법론으로, Shodan API를 통해 대한민국(KR) 국가 코드에 귀속된 모든 인터넷 연결 자산을 수동적으로 스캔하여 노출 현황을 파악한다. 이 방법은 실제 공격자의 시각에서 외부에서 볼 수 있는 공격 표면을 그대로 반영한다는 점에서 전통적인 내부 취약점 스캔과 차별화된다.

구체적 수집 절차로는 기본 쿼리에 country:KR 필터를 적용하였으며, ICS/OT 프로토콜 탐지를 위해 port:502 (Modbus), port:20000(DNP3), port:1883(MQTT) 등 프로토콜별 전용 필터를 추가 적용하였다.

스캔 시점은 2026년 4월 11일 17:56:52(KST) 단일 스냅샷이며, 중복 호스트 제거를 위해 동일 IP의 다중 포트 노출은 호스트 단위로 집계하였다. host는 단일 공인 IP 주소를, port는 해당 IP에서 응답한 TCP/UDP 서비스 포트를 의미한다. CVE 매칭은 Shodan이 배너 및 버전 정보를 기반으로 NVD 및 KEV 데이터베이스와 교차 분석하는 방식으로 수행되었다.

두 번째는 알려진 악용 취약점(KEV: Known Exploited Vulnerabilities) 데이터베이스와의 교차 분석이다. CISA KEV는 미국 사이버보안 및 인프라 보안국(CISA)이 실제 악용이 확인된 취약점을 등재하는 권위 있는 데이터베이스로, 논문 작성 시점 기준 1,559개 CVE가 등재되어 있다[4]. VulnCheck KEV는 CISA KEV를 확장하여 보다 광범위한 위협 인텔리전스를 통합한 상용 데이터베이스로 CISA KEV 보다 3.4배 더 많은 3,623개 CVE를 포함한다[5].

세 번째는 CYFIRMA의 위협 행위자 인텔리전스로, 다크웹 모니터링, 행위자 프로파일링, 섹터별 피해 분석을 통해 정성적 위협 정보를 EASM과 KEV 등 정량적 취약점 데이터와 연계한다.

1.4 Report Structure

제2장은 EASM 스캔의 13개 모듈 데이터를 체계적으로 분석하여 포트 노출, ICS/OT 취약점, 침해 데이터베이스, VPN 취약점, SMB 인증 현황, 주요 CVE, KEV 취약 호스트, 취약 ISP/IP 현황을 기술적으로 심층 분석한다.

제3장은 CYFIRMA 위협 인텔리전스를 바탕으로 북한 및 중국 연계 APT 그룹, 랜섬웨어 집단, 다크웹 지하경제 생태계를 분석한다. 제4장은 앞선 분석의 결론으로서, 조직이 즉시·단기·중기·장기적으로 실행에 옮겨야 할 구체적인 보안 강화 조치와 우선순위 매트릭스를 제시한다.

연구의 흐름은 다음 Table 2.와 같다. 본 연구는 2026년 2월부터 3월까지의 선행 연구 검토 및 ICS/OT 보안 분석을 시작으로, 4월에 Shodan을 통한 대한민국(KR) 대상 EASM 데이터 수집을 실시하였다. 이후 5월에 수집된 취약점 데이터를 북한 및 중국 연계 위협 행위자의 TTP와 매핑하는 분석 단계를 거쳐, 동월 보안 강화 방안 및 우선순위 매트릭스를 도출하는 평가 및 권고 단계로 완료되었다.

이러한 연구 흐름은 기술적 취약점 데이터와 위협 인텔리전스를 체계적으로 통합하여 실무적 대응 방안을 도출하기 위한 순차적 접근법을 따른다.

Table 2. Research Flow

Research	Month	Contents
Research	Feb ~ Mar	• Previous Studies • ICT/OT Analysis
Data Collection	Apr	• Shodan Data Collection (KR)
Analysis	May	• Mapping Vulnerabilities to DPRK Actors
Evaluation & Recommendations	May	• Security Measures & Priority Matrix

II. Related Research

2.1 Research on EASM and Vulnerability Management

기존 사이버보안 연구의 패러다임은 조직 경계 내부에서의 취약점 식별과 관리에 집중해 왔으나, 클라우드 전환과 원격 근무 확산으로 인해 조직의 디지털 경계가 모호해지면서 외부 공격자 시각에서의 노출 분석, 즉 EASM 접근법의 중요성이 부각되고 있다.

인터넷 전체를 대상으로 한 스캐닝 기법의 기술적 실현 가능성이 학술적으로 검증된 이후[6], Shodan·Censys 등의 플랫폼을 활용한 외부 공격표면 분석 연구가 해외를 중심으로 꾸준히 축적되고 있으나[7], 국내에서는 연구 범위가 특정 공개 홈페이지 서비스나[8] 단일 프로토콜에 한정된 부분적 분석에 머물러 있으며, 국가 전체의 인터넷 노출 자산을 망라하면서 동시에 실제 위협 행위자의 공격 전술과 연계한 종합적 분석은 아직 이루어지지 않고 있다. 나아가 기존 연구 대부분은 이미 구축된 공격자 인프라를 사후적으로 추적하는 데 초점을 맞추고 있어[9], 취약한 노출 자산이 어떤 위협 행위자의 표적이 될 수 있는지를 사전에 예측하고 매핑하는 연구는 여전히 미개척 영역으로 남아 있다. 본 연구는 이러한 연구 공백을 메우고자 국가 단위 EASM 정량 데이터와 위협 인텔리전스를 결합한 통합 분석 프레임워크를 제안한다.

2.2 Security Analysis of ICS/OT Environments

산업제어시스템(ICS)의 인터넷 노출은 국가 핵심 인프라 보호 측면에서 중요한 연구 주제다. Liao[10]는 Shodan을 통해 전 세계 ICS 장비 노출 현황을 분석하고 SCADA 시스템의 인터넷 노출 위험을 제시하였다.

산업제어시스템의 사이버 보안은 IT 보안과 근본적으로 다른 특성을 지닌다. 가용성과 실시간성을 최우선으로 설계된 OT 환경은 패치 적용이나 시스템 재시작이 구조적으로 어렵고, 설계 당시 네트워크 보안을 고려하지 않은 레거시 프로토콜이 여전히 광범위하게 사용된다. Modbus, DNP3 등 산업용 프로토콜의 인터넷 노출은 원격 제어 및 데이터 조작 공격으로 직결될 수 있어[12] 즉각적인 격리 조치가 필요하다. 선행 연구들은 이러한 ICS 환경의 인터넷 노출이 단순한 정보 유출을 넘어 물리적 시설 파괴나 생산 중단과 같은 물리적 피해로 직결될 수 있음을 반복적으로 경고해 왔다[12].

그러나 기존 연구의 대부분은 글로벌 또는 특정 산업군 단위의 거시적 분석에 집중하여, 대한민국이라는 특정 국가의 ICS 노출 현황을 실제 위협 행위자의 공격 패턴과 연계하여 분석한 사례는 찾아보기 어렵다. 특히 북한 연계 APT 그룹이 한국의 에너지·제조 인프라를 전략적 표적으로 삼고 있는 현실을 감안할 때, ICS 노출 현황과 국가 지원 위협 행위자를 연계한 리스크 평가는 실질적인 정책적 함의를 가진다.

2.3 North Korea-Linked Cyber Threat Landscape

라자루스, 김수키, APT37 등 북한 연계 APT 그룹에 대한 연구는 국내외에서 활발히 진행되고 있다. 이들은 스피어피싱, 공급망 침해, 취약한 인터넷 노출 서비스 악용을 주요 초기 침투 경로로 활용한다[13]. 특히 랜섬웨어와 암호화폐 탈취를 병행하는 이중 전략은 제재 회피와 전략적 정보 수집을 동시에 달성하는 수단으로 분석된다[14].

북한 연계 사이버 위협은 단순한 해킹 집단의 활동이 아니라 국가 전략과 긴밀하게 연동된 복합적 작전으로 이해되어야 한다. 학계와 보안 업계의 연구들은 이들 그룹이 정보 수집, 외화 획득, 심리전이라는 세 가지 목표를 동시에 추구하며, 목표에 따라 전술과 표적을 정교하게 분화시키는 고도의 운영 체계를 갖추고 있음을 공통적으로 지적한다. 그러나 기존 연구의 한계는 위협 행위자의 전술·기법·절차(TTP) 분석이 주로 사후적 침해 사고 분석에 의존한다는 점이다. 즉, 실제 공격이 발생한 이후에야 해당 그룹의 공격 벡터가 밝혀지는 구조로, 선제적 방어를 위한 취약 자산 식별과의 연계가 부족하다. 본 연구는 이 간극을 해소하기 위해, 현재 인터넷에 노출된 취약 자산 데이터를 북한 연계 APT 그룹의 알려진 공격 선호 벡터와 사전에 매핑함으로써, 어떤 취약점이 어떤 위협 행위자에 의해 먼저 악용될 가능성이 높은지를 예측하는 새로운 분석 관점을 제시한다.

III. Internet-Exposed Vulnerabilities & Nation-State Threat Profiles

3.1 Global/Current Status of Internet-Facing Assets (Module 1~2)

2026년 4월 11일 기준, Shodan 스캔을 통해 탐지된 대한민국의 인터넷 노출 포트 총수는 37,171,622개에 달한다. 이는 전 세계에서도 손꼽히는 규모의 인터넷 연결 자산 노출 수치로, 대한민국이 글로벌 수준에서 광범위한 사이버 공격 표면을 보유하고 있음을 의미한다. 이 광범위한 공격 표면은 단순한 기업 및 기관 서버만이 아니라 IoT 기기, 가정용 라우터, 산업 제어 장비, 클라우드 인프라 등 다양한 유형의 자산을 포함한다. 포트별 사용 현황 분석에서 가장 주목해야 할 사실은 포트 7547의 압도적인 노출 규모다. 포트 7547은 총 11,617,415개가 노출되어 전체 노출 포트의 약 31.3%를 차지하며 1위를 기록하였다. 이 포트는 통신사업자가 가정용 및 소규모 사무용 라우터를 원격 관리하기 위해 사용하는 TR-069(CWMP: CPE WAN Management Protocol) 서비스 포트다. 과거 Mirai 봇넷이 이 포트를 통해 수백만 대의 라우터를 감염시켜 대규모 DDoS 공격에 활용한 전례가 있다. 1,160만 개 이상의 디바이스에서 이 포트가 노출되어 있다는 사실은 ISP가 관리하는 가입자 장비 전반에 걸쳐 심각한 보안 위험이 내재되어 있음을 보여준다.

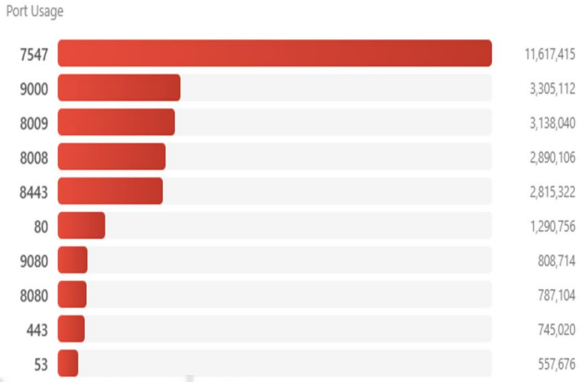

Fig. 1. Port Usage TOP 10

2위부터 4위는 각각 포트 9000(3,305,112개), 8009(3,138,040개), 8008(2,890,106개)으로, 이 포트들은 주로 웹 애플리케이션 서버 및 미디어 서비스 관련 포트다. 5위는 포트 8443(2,815,322개)으로 HTTPS 대체 포트이며, 6위는 포트 80(1,290,756개)으로 표준 HTTP 서비스다. 포트 9080(808,714개), 8080(787,104개), 443(745,020개), 53(557,676개)이 그 뒤를 잇는다. 주목할 점은 표준 HTTPS 포트인 443보다 비표준 포트들의 노출이 훨씬 많다는 사실로, 이는 관리 통제를 벗어난 다수의 서비스가 운영되고 있음을 시사한다.

3.2 Analysis of Internet-Exposed ICS/OT Systems (Module 3)

Module 3은 대한민국 사이버보안 현황에서 가장 심각한 우려 사항 중 하나를 드러낸다. 산업제어시스템(ICS: Industrial Control Systems) 및 운영기술(OT: Operational Technology) 장비가 총 4,321개 인터넷에 직접 노출되어 있는 것으로 확인되었다. 이 4,321개는 Shodan이 ICS/OT 전용 지문(fingerprint)으로 분류한 장비 수이며, 이후 제시되는 MQTT 263,832개, DNP3 10,371개, Modbus 4,703개 등의 수치는 해당 산업용 프로토콜 포트가 개방된 호스트 수를 나타낸다. MQTT와 같은 경량 메시징 프로토콜은 IoT 센서 및 산업 시스템에서 광범위하게 사용되므로 포트 개방 수가 ICS 장비 식별 수보다 현저히 클 수 있으며, 두 수치는 상이한 분류 기준에 의한 것으로 직접 비교는 적절하지 않다.

ICS/OT 장비는 전력, 수도, 가스 등 국가 핵심 인프라와 제조 공장, 교통 시스템 등을 직접 제어하는 장비들로, 이들이 인터넷에 노출된다는 것은 국가 안보와 공중 안전에 대한 직접적인 위협을 의미한다. 프로토콜별 분석에서 MQTT가 263,832개로 압도적 1위를 차지하였다. MQTT는 IoT 기기와 산업 센서 간 경량 메시지 전송을 위한 프로토콜이나, 인증 없이 노출된 MQTT 브로커는 공격자가 산업 시스템의 센서 데이터를 감청하거나 오염된 명령을 주입하는 데 악용될 수 있다. DNP3 프로토콜이 10,371개 노출되었는데, DNP3는 전력 및 수자원 관리 시스템에서 사용되는 핵심 제어 프로토콜로 이 수치는 매우 위험하다.

Modbus(4,703개)는 산업 자동화의 표준 프로토콜이며, Fox/Niagara(1,128개)는 빌딩 자동화 시스템(BAS)에서 널리 사용된다. EtherNet/IP(949개), S7 Siemens(881개), OPC UA(806개), BACnet(86개)도 각각 상당한 수준으로 노출되어 있다. ICS 노출 기관별 분석에서 Korea Telecom(KT)이 3,762개로 1위를 차지하여, 국내 최대 통신사업자 네트워크에서 가장 많은 ICS 자산이 인터넷에 노출되어 있음을 보여준다. 서울대학교(105개), SK Broadband(91개), SK Telecom(40개), LG U+(34개) 등 교육기관과 통신사들도 상당수 ICS 자산이 노출된 것으로 나타났다. 지역별로는 서울(740개)이 단연 1위이며, 광주(163개), 대구(162개), 전주(155개), 군산(129개), 익산(125개), 부산(123개) 순이다. 제품별로는 LS ELECTRIC(88개), Lantronix X90(63개), Moxa Nport(40개), Rockwell Automation(15개) 등이 주요 노출 제품으로 파악되었다. 이 중 Moxa Nport는 산업 시리얼 포트를 이더넷으로 변환하는 기기로, 과거 다수의 취약점이 발견된 바 있어 즉각적인 조치가 요구된다.

3.3 Analysis of Unpatched BlueKeep Vulnerabilities (Module 4~5)

Module 4에서 확인된 BlueKeep(CVE-2019-0708) 미패치 시스템 수는 1,171개다. BlueKeep은 2019년 마이크로소프트가 공개한 Windows Remote Desktop Services(RDS)의 원격 코드 실행(RCE) 취약점으로, 인증 없이 악용 가능한 워너블(Wormable) 취약점이다. 즉, 감염된 시스템이 네트워크를 통해 자동으로 다른 취약한 시스템을 감염시킬 수 있어 WannaCry급 대규모 사이버 재난을 유발할 잠재성을 가진다.

공개된 지 6년이 지난 BlueKeep 취약점이 여전히 천여 곳 이상의 시스템에서 탐지된다는 점은, 국내 보안 패치 거버넌스의 고질적인 지체 현상을 방증한다. 미패치 시스템들은 현재 CISA KEV에도 등재되어 있으며 실제 랜섬웨어 공격에 악용되고 있다.

Module 5의 데이터베이스 노출 현황은 총 25,742개의 데이터베이스 서비스가 인터넷에 노출되어 있음을 보여준다. 유형별로는 MySQL 관련 포트 노출이 23,784개로 가장 많아 전체의 92.4%를 차지한다. Redis 인증 없음(No Auth) 상태가 1,845개, Memcached 개방이 111개, MongoDB Meow 감염이 2개로 나타났다. MySQL 포트(3306 등) 노출은 곧 무인증 접근을 의미하지 않으며, 실제 인증 없는 접근 가능 여부는 추가 검증이 필요하다. 다만 포트 노출 자체로도 잠재적 공격 표면을 형성하므로 접근 통제 강화가 요구된다. Redis 1,845개는 인증 설정이 없는(No Auth) 상태가 Shodan 배너에서 직접 확인된 경우이며, MongoDB Meow 감염 2개는 기존에 무인증으로 노출된 후 실제 데이터 삭제 공격을 받은 사례로 구분하여 이해해야 한다.

Redis 무인증 노출의 경우 단순 데이터 탈취를 넘어 서버 내 파일 시스템 접근 및 원격 코드 실행으로 이어질 수

있어 위험성이 더욱 높다.

3.4 Vulnerabilities in VPN and Remote Access: Ivanti Pulse Secure (Module 6)

Module 6은 Ivanti(구 Pulse Secure) VPN 제품군의 인터넷 노출 현황을 분석한다. 탐지된 총 노출 수는 7,080개이며, 세부적으로는 Ivanti Connect Secure가 6,952개, Pulse Secure VPN이 91개, Pulse Connect Secure가 37개로 구분된다. Ivanti VPN 제품은 2024년에 CVE-2024-21887, CVE-2023-46805, CVE-2024-21893 등 다수의 고위험도 제로데이 취약점이 연이어 발견되어 전 세계적으로 광범위한 침해 사고를 야기하였다.

특히 미국 CISA는 2024년 1월 Ivanti VPN 취약점과 관련하여 긴급 지시(Emergency Directive)를 발령하고 모든 연방 기관에 즉각적인 패치 또는 제품 오프라인 조치를 명령하였다. 엔터프라이즈 인프라의 출입구인 VPN 자산의 결함은 단순한 침해를 넘어 공격자에게 내부망 전반에 대한 무제한적 통제권을 허용하는 결과로 귀결된다.

CYFIRMA 보고서에 따르면, Kimsuky와 Lazarus 그룹이 한국 기업을 대상으로 VPN 취약점을 초기 침투 경로로 적극 활용하고 있어 이 위협의 현실성은 더욱 높다.

3.5 Current Status of SMB Authentication Vulnerabilities (Module 7)

Module 7은 SMB(Server Message Block) 프로토콜의 인증 현황을 분석한다. SMB 인증이 활성화된 시스템은 5,143개이며, 비활성화된 시스템은 429개로 전체의 7.7%를 차지한다. SMB는 파일 및 프린터 공유, 네트워크 통신에 사용되는 윈도우 핵심 프로토콜로, SMB 인증이 비활성화된 시스템은 인증 없이 파일 및 데이터에 접근할 수 있는 상태다. 2017년 WannaCry 랜섬웨어는 SMBv1 취약점(EternalBlue)을 악용하여 전 세계 150개국 30만 대 이상의 컴퓨터를 감염시켰다. 현재도 SMB 인증 취약 시스템은 랜섬웨어의 네트워크 내 전파(Lateral Movement)를 위한 핵심 경로로 활용되고 있다. 429개의 무인증 SMB 시스템은 각각 내부 네트워크 전체의 침해를 야기할 수 있는 심각한 보안 위협 요소다.

3.6 Analysis of Top-Exposed Vulnerabilities and RCE Attack Vectors (Module 8~9)

Module 8에서 가장 많은 호스트에 영향을 미치는 취약점 Top 5는 다음과 같다.

CVE-2011-1176과 CVE-2012-4360이 각각 179,644개 호스트에 영향을 미쳐 공동 1위를 차지하였고, CVE-2007-4723과 CVE-2011-2688이 각각 179,639개로 3위, CVE-2012-3526이 179,638개로 5위에 올랐다. 이 취약점들은 대부분 Apache HTTP Server의 mod_authnz_external 모듈 관련 취약점으로, 10년 이상 된 구 버전 취약점들이 여전히 약 18만 개에 달하는 호스트에서 해결되지 않고 있다는 사실은 국내 웹 서버 관리의 심각한 문제를 보여준다. Module 9의 원격 코드 실행(RCE to Shell) 분석은 특히 주목할 필요가 있다. 16개의 고위험 RCE 벡터를 점검한 결과, 50개의 호스트에서 실제 원격 쉘 실행이 가능한 것으로 확인되었다.

유형별로는 Cisco IOS XE Implant(CVE-2023-20198)가 18개로 가장 많았고, PaperCut RCE(CVE-2023-27350) 16개, ProxyShell(CVE-2021-34473) 8개, Spring4Shell(CVE-2022-22965)6개, ProxyLogon(CVE-2021-26855) 2개 순이다. Cisco IOS XE 취약점(CVE-2023-20198)[15]은 2023년 CVSS 10.0 만점의 초임계(Critical) 취약점으로, 인증 없이 관리자 권한의 계정을 생성하고 완전한 시스템 제어권을 획득할 수 있다.

이 취약점이 활성화된 임플란트(Implant) 형태로 18개 호스트에 존재한다는 것은 해당 시스템들이 이미 침해되었거나 침해 직전의 상태임을 시사한다. ProxyShell과 ProxyLogon은 Microsoft Exchange Server의 치명적 취약점으로, 각각 기업 이메일 시스템 전체를 장악하는 데 활용된다.

3.7 Analysis of Known Exploited Vulnerabilities Based on CISA KEV (Module 10)

Module 10은 CISA KEV 데이터베이스와의 교차 분석 결과를 보여준다. CISA KEV 전체 1,559개 CVE 중 183개가 대한민국 네트워크에서 탐지되었으며, 총 538,230개 호스트가 CISA KEV 취약점에 노출된 것으로 확인되었다.

이는 실제 사이버 공격에서 악용되고 있음이 증명된 취약점들이 53만 개 이상의 한국 호스트에 존재한다는 의미로, 매우 심각한 수준의 위협이다.

Table 3. CISA KEV Top 10 (2021 ~ 2026. 4.11)

CVE	Contents	Count
2023-44487	IETF - HTTP/2	144,112
2024-38475	Apache - HTTP Server	141,672
2021-40438	Apache - Apache	127,984
2020-11023	JQuery - JQuery	33,833
2019-0211	Apache - HTTP Server	23,164
2012-1823	PHP - PHP	14,141
2019-11043	PHP - FastCGI P.M	9,645
2014-0160	OpenSSL - OpenSSL	5,349
2020-0796	Microsoft - SMBv3	2,906
2024-4577	PHP Group - PHP	2,793

상위 CISA KEV 취약점 현황을 분석하면 다음과 같다. 1위는 CVE-2023-44487(HTTP/2 Rapid Reset Attack, 144,112 호스트)로 IETF HTTP/2 프로토콜의 DDoS 증폭 취약점, 2위는 CVE-2024-38475(141,672 호스트)로 Apache HTTP Server의 취약점, 3위는 CVE-2021-40438 (127,984 호스트)으로 Apache HTTP Server SSRF 취약점이다.

4위는 CVE-2020-11023(33,833 호스트)으로 jQuery XSS 취약점, 5위는 CVE-2019-0211(23,164 호스트)로 Apache HTTP Server의 권한 상승 취약점, 6위는 CVE-2012-1823(14,141 호스트)은 PHP CGI 원격 코드 실행 취약점으로 2012년에 공개된 취약점이다.

랜섬웨어 연계 취약점으로는 CVE-2019-11043(PHP FPM RCE, 9,645 호스트), CVE-2020-0796(SMBv3 EternalDarkness, 2,906 호스트), CVE-2024-4577(PHP 원격 코드 실행, 2,793 호스트), CVE-2019-0708(BlueKeep, 1,171 호스트)이 확인되어 랜섬웨어 공격 위험이 특히 높다.

Microsoft SharePoint 관련 취약점인 CVE-2026-20963, CVE-2025-49704, CVE-2025-53770, CVE-2024-38094도 각각 1,148 호스트에서 탐지되었는데, 이 중 세 개는 랜섬웨어 연계 취약점으로 표시되어 있어 기업 협업 플랫폼에 대한 공격 위험이 높다.

3.8 Extended Vulnerability Analysis Based on VulnCheck KEV (Module 11)

Module 11에서 VulnCheck KEV와의 교차 분석 결과, 총 3,623개 CVE 중 220개가 탐지되었으며 노출 호스트 수는 1,820,536개에 달한다. CISA KEV 기준 53만 8천 개보다 VulnCheck KEV 기준으로는 182만 개로 약 3.4배 많은 호스트가 취약한 것으로 나타났다. 이는 CISA KEV에는 아직 등재되지 않았으나 실제 악용이 관찰된 추가 취약점들이 대한민국 네트워크에 광범위하게 존재함을 보여준다.

Table 4. VulnCheck KEV Top 10 (2021 ~ 2026. 4.11)

CVE	Contents	Count
2011-2688	mod_authnz_external_project - mod_authnz_external	179,947
2023-44487	IETF - HTTP/2	144,112
2024-38475	Apache - HTTP Server	141,672
2021-40438	Apache - Apache	127,984
2023-25690	Apache - HTTP Server	126,862
2018-1303	Apache - HTTP Server	107,457
2017-9798	Apache - HTTP Server	103,879
2017-9788	Apache - HTTP Server	102,427
2019-10098	Apache - HTTP Server	95,372
2017-15715	Apache - HTTP Server	86,569

VulnCheck KEV 상위 취약점의 특징적 패턴은 Apache HTTP Server 관련 취약점의 광범위한 노출이다.

CVE-2023-25690(Apache HTTP Server 요청 스머글링), CVE-2018-1303, CVE-2017-9798, CVE-2017-9788. CVE-2019-10098, CVE-2017-15715, CVE-2016-0736 등 Apache 계열 취약점이 상위를 대거 점령하고 있다. 이는 대한민국 웹 서버 인프라의 Apache 의존도가 매우 높으며, 오래된 버전의 Apache가 광범위하게 운용되고 있음을 보여준다.

OpenSSH 관련 취약점인 CVE-2023-48795(Terrapin Attack, 81,832 호스트)와 CVE-2023-38408(79,580 호스트)도 주목할 만하다.

jQuery 관련 취약점군인 CVE-2020-11022, CVE-2020-11023, CVE-2019-11358, CVE-2015-9251이 각각 3만 개 내외의 호스트에서 탐지되어 웹 프론트엔드의 라이브러리 취약점도 심각함을 보여준다.

3.9 Status of Vulnerabilities by ISP and IP Address (Module 12~13)

Module 12는 취약한 호스트를 가장 많이 보유한 ISP(Internet Service Provider) 현황을 분석한다.

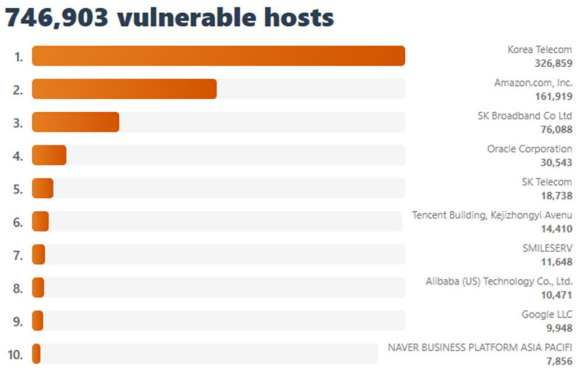

Fig. 2. Top Vulnerable ISPs by Host Count

전체 취약 호스트 746,903개 중 Korea Telecom(KT)이 326,859개(43.8%)로 압도적 1위를 기록하였다. 이는 KT 네트워크 내 가입자 및 기업 고객의 취약 시스템이 가장 많음을 의미한다. 2위 Amazon.com(161,919개, 21.7%)는 AWS 클라우드 인프라에서 운영 중인 취약 인스턴스를 반영한다. 3위 SK Broadband(76,088개), 5위 SK Telecom(18,738개)을 합산하면 SK 그룹 계열 통신사의 취약 호스트가 94,826개로 국내 2위 규모다. 4위 Oracle Corporation(30,543개)은 Oracle Cloud Infrastructure(OCI) 기반 서비스의 취약점을 반영한다. 6위 Tencent(14,410개)와 8위 Alibaba(10,471개)

등 중국계 클라우드 사업자 네트워크에서의 취약 호스트도 주목할 필요가 있다.

Module 13은 단일 호스트 기준으로 가장 많은 취약점을 보유한 IP 주소 Top 10이다.

1위는 43.201.35.16(Amazon.com)으로 498개의 취약점이 탐지되었다. CVE-2018-10549, CVE-2018-10548 등 PHP 관련 다수 취약점이 핵심이다. 2위는 222.113.18.218(Korea Telecom)으로 389개, 3위는 43.202.64.180(Amazon.com) 343개 취약점, 4위는 211.37.174.80(Korea Telecom) 331개이며 CVE-2024-38474 등 최신 취약점도 포함되어 있다.

5위 115.68.102.85(SMILESERV)는 174개 취약점을 보유하는데 CVE-2014-0117, CVE-2017-7679 등 고령 취약점이 다수 포함되어 있다. 이 Top 10 IP 목록은 즉각적인 점검 및 조치가 요구되는 최우선 대응 대상이다.

3.10 Analysis of North Korea-Linked APT Groups: Lazarus, Kimsuky, and APT37

3.10.1 Lazarus Group

대한민국에 대한 사이버 위협의 핵심 주체는 북한 연계 APT 그룹들로, 이들은 라자루스 그룹(Lazarus Group), 김수키(Kimsuky), APT37(Reaper)이라는 세 개의 주요 행위자를 중심으로 활동한다.

CYFIRMA 위협 인텔리전스 보고서는 이들의 활동이 단순한 사이버 범죄를 넘어 북한 정권의 전략적 목표와 긴밀하게 연계된 국가 주도 사이버 작전임을 명확히 한다.

라자루스 그룹은 북한 정찰총국(RGB) 소속으로 추정되며, 한국 정부, 국방, 암호화폐, 금융기관을 지속적으로 표적으로 삼는다.

주요 전술로는 한미 관계를 주제로 한 무기화된 문서를 활용한 스피어피싱, 지속성 확보와 데이터 탈취를 위한 맞춤형 악성코드 프레임워크 배포, 디지털 자산 절도 및 공급망 침해 활동이 포함된다.

라자루스의 하위 클러스터인 안다리엘(Andariel)은 한국 방위 계약업체와 군사 관련 인프라에 대한 침입에 더욱 집중적인 역량을 발휘하며, 공개 취약점 악용과 맞춤형 악성코드를 통해 군사 정보 수집을 지원하고 있다.

EASM 데이터와의 연계 분석에서 주목되는 점은 라자루스 그룹이 VPN 취약점, 인터넷 노출 서비스, 그리고 미패치 웹 애플리케이션을 초기 침투 경로로 활용한다는 것이다. Module 6에서 확인된 7,080개의 Ivanti VPN 노출과 Module 9의 50개 RCE 가능 시스템은 라자루스 그룹의 공격 표면이 될 가능성이 있는 것으로 분석된다. 특히 ProxyShell (CVE-2021-34473, 8개 호스트)과 ProxyLogon(CVE-2021-26855, 2개 호스트)은 라자루스 그룹이 과거 실제 공격에서 활용한 것으로 보고된 취약점 유형과 유사하며, 해당 그룹의 관심 대상이 될 가능성이 있는 것으로 분석된다.

3.10.2 Kimsuky Group

Module 5에서 탐지된 23,784개의 무방비 MySQL 데이터베이스는 정치 정보 수집을 주 목적으로 하는 김수키(Kimsuky) 그룹에게 최적의 공격 표면을 제공할 수 있다.

사회공학(Social Engineering), 자격 증명 피싱 포털, 악성 첨부파일을 통해 로그인 데이터를 수집하고 외교 및 국방 관련 담론을 모니터링한다.

김수키의 작전은 주로 한국의 외교 정책 입장, 남북 협상, 동맹 조율에 대한 정보 획득을 목표로 한다.

김수키의 활동과 EASM 데이터를 연계하면, Module 5에서 확인된 25,742개의 무방비 데이터베이스(특히 MySQL 23,784개)가 핵심 관심 대상이 된다. 정부기관, 연구소, 언론사가 사용하는 데이터베이스가 인증 없이 노출되어 있다면, 김수키는 스피어피싱을 통한 자격 증명 획득 후 추가 래터럴 무브먼트 없이 직접 데이터베이스에 접근하여 외교 및 정책 자료를 탈취할 수 있다.

3.10.3 APT37 Group

APT37은 북한 연계 스파이 행위자로 한국 정부기관, 방위 계약업체, 언론 기관, 정책 기관을 표적으로 한다. 스피어피싱 캠페인, 제로데이 익스플로잇, 맞춤형 악성코드를 사용하여 초기 접근을 획득한 후 자격 증명 수집과 데이터 탈취를 수행한다.

APT37의 작전은 주로 정치, 군사, 전략 정보 수집에 집중되어 한국의 국가 안보와 국방 생태계에 지속적인 위협이 된다.

Module 9에서 확인된 Spring4Shell(CVE-2022-22965, 6개 호스트)은 APT37이 과거 활용한 것으로 보고된 공격 벡터와 유사한 취약점 유형에 해당한다.

다만, EASM 노출 자산과 실제 공격 행위자 간의 직접적 인과관계를 의미하는 것이 아니라, 해당 취약점이 위협 행위자의 관심 대상이 될 가능성을 시사하는 것이다.

3.11 Analysis of China-Linked APT Groups: APT41 and Mustang Panda

3.11.1 APT41 Group

APT41은 스파이 활동과 재정적 동기의 캠페인을 결합한 이중 용도 작전으로 알려진 중국 연계 그룹이다. 아시아 전역에서 역사적으로 표적으로 삼은 한국의 반도체, 전

자 제조, 게임 산업이 주요 공격 대상이다. APT41은 인터넷에 노출된 애플리케이션의 미패치 취약점을 악용하여 초기 접근을 획득한 후 자격 증명 수확, 권한 상승, 지적 재산 탈취를 수행한다. EASM 데이터에서 확인된 대규모 Apache 서버 취약점(Module 8~11)과 VPN 취약점은 APT41의 전형적인 초기 침투 벡터와 유사한 특성을 보이는 것으로 분석된다. 특히 반도체 제조사와 전자 기업들이 사용하는 ERP, SCM 시스템이 VulnCheck KEV 취약 호스트에 포함될 가능성이 높다.

3.11.2 Mustang Panda Group

머스탱 판다는 동아시아 전역의 정부 및 정책 관련 기관을 표적으로 하는 중국 연계 스파이 행위자다. DLL 사이드로딩 기법과 맞춤형 백도어를 활용하여 탐지를 회피하면서 지속적인 접근 권한을 유지한다.

한국에서의 표적은 주로 정치 정보 수집, 해양 정책 모니터링, 지역 안보 분석 등 베이징의 전략적 우선순위와 일치한다. Module 3에서 확인된 ICS 프로토콜 노출, 특히 서울 소재 정부기관 네트워크에서의 ICS 노출은 머스탱 판다의 인프라 정찰 활동 경로가 될 수 있다.

3.12 Trends in Ransomware Groups: Qilin, LockBit, and Play

3.12.1 Qilin Group

CYFIRMA 보고서에 따르면, 2025년 12월부터 2026년 2월까지의 모니터링 기간 동안 대한민국을 표적으로 한 랜섬웨어 활동이 지속적으로 관찰되었다.

2026년 1월이 피해자 목록 등재 건수가 가장 많았고, 이후 소폭 감소하였으나 지속적인 위협 상태가 유지되고 있다.

Qilin은 이 기간 가장 활발하게 한국 피해자를 등재한 랜섬웨어 그룹으로, RaaS(Ransomware-as-a-Service) 모델로 운영된다. 핵심 운영자들이 암호화 페이로드, 유출 인프라, 협상 포털을 관리하며 제휴 파트너들이 침입을 실행한다.

주요 공격 기법으로는 VPN 및 웹 애플리케이션의 공개 취약점 악용, 인포스틸러 로그와 지하 마켓플레이스에서 획득한 유효 자격 증명 사용, 커스텀 로더를 통한 랜섬웨어 페이로드 스테이징, 공개 데이터 유출 사이트를 통한 이중 갈취 전술이 포함된다.

EASM Module 10에서 확인된 CVE-2024-4577(PHP 원격 코드 실행, 2,793 호스트)과 CVE-2019-11043(PHP FPM RCE, 9,645 호스트)은 Qilin이 활용하는 것으로 보고된 초기 침투 벡터와 유사한 것으로 분석된다.

3.12.2 Technical Analysis of LockBit 5.0 and the Play Group

LockBit은 국제 사법당국의 지속적인 압박에도 불구하고 제휴 파트너들이 잔존 인프라를 통해 LockBit 5.0 등의 변종으로 활동을 계속하고 있다.

한국에서의 활동은 기회주의적 성격을 띠며, 인터넷 노출 취약점을 통한 초기 접근과 구조화된 협상 포털 및 시한부 데이터 유출 위협을 통한 강제 결제 전술을 구사한다.

Play 랜섬웨어 역시 기업 환경을 표적으로 한 이중 갈취 전술로 활동하며, 인터넷 노출 서비스와 원격 접속 인프라 취약점을 통한 진입, 암호화 이전 신속한 데이터 탈취를 특징으로 한다.

피해 업종 분석에서는 제조업이 가장 높은 랜섬웨어 피해 집중도를 보였으며, 금융, 정부, IT, 교육, 통신 및 미디어, 부동산 순으로 피해가 확인되었다.

3.13 The Dark Web Underground Economy and Data Breach Ecosystem

CYFIRMA의 다크웹 모니터링 데이터는 한국 관련 사이버 범죄 생태계의 심각성을 보여준다.

3개월(2025.12~2026.02) 모니터링 기간 동안 대규모 침해 사고 공개와 대량 데이터 유통에 의해 주도된 12월의 활동 급증이 특히 주목된다. 다크웹 경제 생태계 내에서 데이터 침해 담론이 주를 이루는 현상은, 외부 노출 자산에서 유출된 정보가 지하 시장의 주요 상품으로 유통되고 있음을 시사한다.

데이터 유출(Data Leak) 논의도 두드러지며, 크레딧 카드 사기와 자격 증명 기반 공격이 꾸준히 관찰되고 있다.

EASM Module 5의 25,742개 무방비 데이터베이스는 다크웹의 데이터 침해 생태계와 직접 연결된다. 인증 없이 노출된 MySQL 데이터베이스는 공격자가 자격 증명 획득 과정 없이 직접 접근하여 수백만 건의 개인정보와 기업 데이터를 탈취할 수 있는 상태다.

이렇게 탈취된 데이터는 다크웹 마켓플레이스에서 신속하게 유통되며, 이후 자격 증명 스터핑(Credential Stuffing), 계정 탈취(Account Takeover), 결제 사기(Payment Fraud) 등 2차 공격에 활용된다. 업종별 표적 분석에서는 전문 서비스 및 정부 분야가 가장 높은 주목도를 보였으며, 이어 의료, 금융, 소비재 서비스 순이었다. 전문 서비스 분야의 높은 관심은 공급망 침입 기회를 나타내며, 정부 관련 논의는 공공 데이터와 인프라에 대한 관심을 반영한다.

IV. Immediate Action Strategies and Recommended Measures

4.1 Synthesis of Key Findings and Implications

EASM 스캔과 CYFIRMA 위협 인텔리전스의 통합 분석에서 도출된 핵심 시사점은 네 가지로 요약된다. 첫째, 대한민국의 사이버 공격 표면은 수천만 개의 노출 포트와 수백만 개의 취약 호스트를 포함하며, 이는 공격자에게 광대하고 다양한 진입 경로를 제공한다. 둘째, 알려진 악용 취약점(KEV)에 노출된 53만 8천 호스트(CISA KEV)와 182만 호스트(VulnCheck KEV)는 이미 실제 사이버 공격에서 활용 중인 취약점들로 즉각적인 패치가 요구된다. 셋째, 국가 핵심 인프라를 직접 제어하는 산업제어시스템 다수가 방화벽 보호 없이 외부에 노출되어 있으며, 인증 체계를 갖추지 못한 채 개방된 데이터베이스 역시 수만 건에 달해 기업 및 개인 데이터의 직접 탈취 위험이 현실화되어 있다. 특히 원격 코드 실행이 실제로 가능한 것으로 검증된 일부 호스트들은 이미 침해 상태이거나 공격자가 언제든 악용 가능한 임계 상태에 있어, 즉각적 격리와 포렌식 조사가 불가결하다. 넷째, 라자루스, 김수키, APT37, APT41 등 국가 지원 APT 그룹들이 EASM에서 확인된 취약점들을 실제 공격에 활용하고 있어 위협의 현실성이 매우 높다.

4.2 Immediate Action Items (0-30 Days)

4.2.1 Critical Immediate Actions: Priority 1

① **RCE 가능 시스템 50개 즉각 격리 및 포렌식 조사**: Module 9에서 확인된 Cisco IOS XE Implant(18개), PaperCut RCE(16개), ProxyShell(8개), Spring4Shell(6개), ProxyLogon(2개) 시스템들을 네트워크에서 즉시 격리하고 침해 여부를 조사한다. 이미 임플란트가 설치된 시스템은 완전 포맷 후 재설치를 고려한다.

② **무방비 데이터베이스 25,742개 즉각 접근 차단**: MySQL 23,784개, Redis 1,845개, Memcached 111개 등 인증 없이 노출된 데이터베이스에 대해 방화벽 규칙으로 외부 접근을 차단하고 강력한 인증을 즉시 적용한다. 특히 Redis는 설정 파일에 requirepass 지시문을 추가하여 인증을 활성화한다.

③ **BlueKeep(CVE-2019-0708) 미패치 1,171개 시스템 긴급 패치**: 2019년에 공개된 BlueKeep 취약점이 아직도 1,171개 시스템에 존재한다는 사실을 조직 책임자에게 즉시 보고하고 긴급 패치를 집행한다. 패치 적용이 즉각 불가한 경우 RDP 서비스 비활성화 또는 네트워크 레벨 인증(NLA) 강제 적용을 시행한다.

④ **SMB 무인증 429개 시스템 즉각 조치**: SMB 인증이 비활성화된 429개 시스템에 대해 SMB 서명(SMB Signing) 강제화 및 외부 노출 차단을 즉시 적용하고, SMBv1 프로토콜 비활성화를 실시한다.

⑤ **Ivanti VPN 7,080개 즉각 패치 점검**: CVE-2024-21887, CVE-2023-46805, CVE-2024-21893 등 2024년 공개된 Ivanti VPN 취약점에 대한 패치 적용 현황을 긴급 점검하고 미패치 시스템을 즉시 업데이트한다.

4.2.2 Prioritized KEV Patching: Within 30 Days

⑥ **HTTP/2 Rapid Reset(CVE-2023-44487, 144,112 호스트) 패치**: 웹 서버 및 리버스 프록시의 HTTP/2 설정을 점검하고, 해당 취약점에 대한 패치 또는 완화 조치를 적용한다. Nginx, Apache, IIS 등 웹 서버별 패치 절차를 즉시 수행한다.

⑦ **Apache HTTP Server 취약점 군 패치**: CVE-2024-38475, CVE-2021-40438, CVE-2019-0211, CVE-2023-25690 등 Apache 취약점이 전체 노출의 대부분을 차지하므로 조직 내 모든 Apache 서버를 최신 버전으로 즉시 업그레이드한다.

⑧ **Microsoft SharePoint 취약점 패치**: CVE-2025-49704, CVE-2025-53770, CVE-2024-38094 등 랜섬웨어 연계 SharePoint 취약점에 대한 긴급 패치를 실시한다.

4.3 Mid-Term Structural Response Strategies (1-6 Months)

4.3.1 Strengthening ICS/OT Security Posture

① **ICS/OT 인터넷 노출 4,321개 전수 조사 및 격리**: MQTT, DNP3, Modbus, Siemens S7 등 ICS 프로토콜을 사용하는 장비들이 인터넷에 직접 노출되지 않도록 방화벽 규칙을 수정하고, 필요시 산업용 DMZ(비무장지대) 구조를 도입하여 IT-OT 네트워크 분리를 강화한다.

② **Moxa Nport, Lantronix X90 등 취약 ICS 장비 교체 또는 패치**: 탐지된 취약 ICS 제품들에 대해 제조사 보안 권고를 즉시 확인하고 취약점 패치를 적용한다. 패치가 불가한 경우 장비 교체를 계획한다.

③ **ICS/OT 이상 탐지 시스템(OT-IDS) 도입**: 인터넷 노출 ICS 장비에 대한 실시간 트래픽 모니터링과 이상 행위 탐지 기능을 갖춘 OT 전용 침입 탐지 시스템을 도입한다.

4.3.2 Attack Surface Reduction and Visibility Enhancement

④ **포트 7547(TR-069) 관리 체계 강화**: 1,160만 개 이상 노출된 TR-069 포트는 ISP와의 협력을 통해 인터넷 방향 접근을 차단하고 관리망 전용 인터페이스로 이전한다. ISP 가입자 장비 보안 가이드라인을 강화한다.

⑤ **정기적 EASM 스캔 체계 구축**: Shodan, Censys, FOFA 등 EASM 도구를 활용하여 월별 또는 분기별 정기 스캔을 수행하고, 새로운 취약 자산 발견 시 자동 알림 체계를 구축한다.

⑥ **비필수 포트 및 서비스 폐쇄**: 포트 9000, 8009, 8008 등 비표준 포트에서 운영 중인 서비스들의 필요성을 재검토하고, 업무상 불필요한 서비스는 즉시 중단하거나 내부망으로 이전한다.

4.3.3 Strengthening Response Frameworks against Threat Actors

⑦ **APT 스피어피싱 대응 강화**: 김수키, APT37의 주요 공격 벡터인 스피어피싱에 대응하여 이메일 보안 게이트웨이 강화, DMARC/DKIM/SPF 정책 적용, 첨부파일 샌드박스 분석 자동화를 구현한다.

⑧ **랜섬웨어 대응 백업 전략 강화**: 3-2-1 백업 원칙(3개 복사본, 2가지 매체, 1개 오프사이트)을 적용하고, 정기적인 백업 복구 훈련을 실시하여 랜섬웨어 피해 시 신속한 복구 능력을 확보한다.

⑨ **다크웹 모니터링 체계 구축**: 기업 및 기관의 자격 증명, 데이터, 내부 정보가 다크웹에서 유통되는지 지속적으로 모니터링하는 위협 인텔리전스 서비스를 도입하고, 유출 발견 시 즉각 대응 프로세스를 확립한다.

4.4 Long-Term Strategic Security Enhancement Directions (6+ Months)

① **제로 트러스트 아키텍처(ZTA) 전면 도입**: 모든 사용자, 기기, 서비스에 대해 '절대 신뢰하지 않고, 항상 검증한다'는 원칙을 적용하는 ZTA를 단계적으로 구현한다[16]. 다중 인증(MFA) 전면 적용, 마이크로 세그멘테이션을 통한 내부망 분리, 최소 권한 원칙(PoLP) 기반 접근 제어를 순차적으로 도입한다.

② **취약점 관리 프로그램(VMP) 성숙도 향상**: CVSS 점수만이 아닌 SSVC(Stakeholder-Specific Vulnerability Categorization)와 KEV 데이터를 결합한 리스크 기반 취약점 우선순위 체계를 도입하여[17], 실제 위협 행위자가 악용하는 취약점을 먼저 패치하는 체계를 구축한다.

③ **AI/ML 기반 위협 탐지 및 대응(TDIR) 플랫폼 도입**: 라자루스, APT41 등이 구사하는 정교한 회피 기법에 대응하기 위해 행위 기반 분석과 AI를 결합한 TDIR 플랫폼을 도입하여, 알려지지 않은 위협에 대한 탐지 능력을 강화한다.

④ **사이버 공급망 보안 프로그램 강화**: 방위산업체, 반도체 기업, 제조업체의 N차 하도급 업체까지 포함한 공급망 전반의 보안 수준을 점검하는 SCDR(Supply Chain Detection and Response) 체계를 구축하고 공급업체 보안 평가 기준을 강화한다.

⑤ **위협 기반 사이버보안 훈련 정례화**: MITRE ATT&CK 프레임워크[18] 기반의 레드팀/블루팀 연습, 사이버 위기 대응 훈련, 랜섬웨어 시나리오 모의 훈련을 연 2회 이상 실시하여 실전 대응 역량을 강화한다.

4.5 Priority Action Matrix by Sector

4.5.1 Government and Public Sector Organizations

김수키, APT37의 주요 표적인 정부기관은 스피어피싱 방어, 이메일 보안 강화, MFA 전면 적용을 최우선 과제로 삼아야 한다. 서울 소재 740개 ICS 노출 장비에 대한 긴급 점검과 격리 조치를 즉각 시행하고, CISA KEV 기반 패치 관리 체계를 국가 차원의 의무 사항으로 강화해야 한다. 무방비 데이터베이스에 대한 전수 조사를 실시하고 공공 데이터 유출 방지 체계를 강화한다.

4.5.2 Defense Industry and Military-Related Institutions

라자루스 그룹 안다리엘 클러스터의 집중 표적인 방산기업들은 모든 VPN 및 원격 접속 솔루션에 대한 즉각적인 취약점 점검과 패치를 실시해야 한다. 네트워크 세그멘테이션을 강화하고 내부망 접근에 대한 행위 기반 모니터링을 도입한다. 공급망 보안을 강화하여 협력업체를 통한 침투 경로를 차단하고, 비밀 데이터가 포함된 시스템에 대한 MFA 및 권한 최소화를 즉시 적용한다.

4.5.3 Manufacturing and Semiconductor Industries

랜섬웨어 피해 1위 업종인 제조업과 APT41의 주요 표적인 반도체 기업은 ICS/OT 보안을 최우선 과제로 삼아야 한다. 생산 라인과 연결된 ICS 장비의 인터넷 노출을 즉각 차단하고 IT-OT 네트워크 분리를 철저히 유지한다. 랜섬웨어에 의한 생산 중단에 대비한 업무 연속성 계획(BCP)을 수립하고 정기적으로 훈련한다. Apache 서버 취약점 패치를 전사적으로 즉시 실시한다.

4.5.4 Financial and Cryptocurrency Sectors

라자루스 그룹의 금융 탈취 활동의 핵심 표적인 금융 및 암호화폐 기업은 거래 시스템과 고객 데이터베이스에 대한 접근 통제를 최강화해야 한다. 자격 증명 탈취 탐지를 위한 이상 로그인 감지 시스템을 구축하고, 다크웹 모니터링을 통해 자사 자격 증명 유출 여부를 지속 모니터링한다. SWIFT 거래 모니터링 및 이상 거래 탐지 체계를 강화한다.

4.5.5 ISPs and Telecommunications Providers

취약 호스트 1위(326,859개)인 Korea Telecom과 SK 계열 통신사는 가입자 네트워크의 보안 강화를 위해 TR-069 포트(7547) 접근 통제 강화, 가입자 장비 자동 보안 패치 체계 구축, 취약한 가입자 IP에 대한 적극적 고지 및 지원 서비스를 제공해야 한다. 중국계 클라우드 사업자(Tencent 14,410개, Alibaba 10,471개) 네트워크에서의 취약 호스트 문제는 해당 클라우드 플랫폼과의 협력을 통해 해결 방안을 모색한다.

V. Conclusions

디지털 전환이 가속화되는 현대 사회에서 인터넷 연결 자산의 폭발적 증가는 필연적으로 공격 표면의 확장을 동반한다. 본 연구는 이러한 현실을 대한민국의 사이버 환경에 적용하여, 외부 공격자의 시각에서 실제로 관찰 가능한 취약점 지형을 정량적으로 측정하고, 이를 위협 행위자의 전술·기법·절차(TTP)와 연계함으로써 리스크 기반의 대응 우선순위를 도출하고자 하였다.

분석 결과는 대한민국의 사이버 공격 표면이 단순한 관리 부재의 문제를 넘어, 국가 안보 차원에서 다루어야 할 구조적 취약성을 내포하고 있음을 보여준다. 특히 주목해야 할 점은 취약점의 '규모'가 아니라 '성격'이다. 확인된 취약 호스트 중 상당수는 이미 실제 사이버 공격에서 악용이 검증된 취약점을 보유하고 있으며, ICS/OT 장비의 직접 노출과 무인증 데이터베이스 문제는 단일 조직의 피해를 넘어 국가 핵심 인프라와 국민 개인정보 전반에 영향을 미칠 수 있는 파급력을 지닌다.

위협 행위자 분석에서도 중요한 시사점이 도출되었다. 북한 연계 APT 그룹들의 공격 전술은 단순한 기술적 침투를 넘어, 외교·안보·경제 정보 수집이라는 전략적 목표와 정밀하게 연계되어 있다. 이는 사이버 위협이 더 이상 IT 보안의 영역에 국한되지 않으며, 국가 차원의 정보 전략과 맞닿아 있음을 의미한다. 랜섬웨어 집단의 공격 역시 기회주의적 침투에서 벗어나 특정 산업군을 겨냥한 표적형 공격으로 진화하고 있어, 제조·금융·공공 부문의 선제적 대응이 더욱 중요해졌다.

기존 연구와의 비교 관점에서 본 연구의 차별성을 살펴보면 다음과 같다. Liao et al.[10]은 글로벌 ICS 장비 노출 현황을 Shodan을 통해 분석하였으나, 특정 국가의 위협 행위자 TTP와의 연계 분석은 수행하지 않았다. Bou-Harb et al.[7]은 사이버 스캐닝 방법론을 체계적으로 제시하였으나 KEV 교차 분석 및 랜섬웨어 그룹과의 매핑은 포함되지 않았다. Choi & Lee[8]는 국내 공공 홈페이지를 대상으로 ASM 솔루션을 활용한 취약점 분석을 수행하였으나, 분석 범위가 특정 서비스에 국한되었다. Kim et al.[17]과 Shin et al.[18]은 Shodan·Censys 기반 공격자 인프라 추적 및 ICS 취약점 분석을 각각 수행하였으나, 국가 단위 전수 조사와 위협 인텔리전스 통합이라는 측면에서 본 연구와 차이가 있다. 이에 비해 본 연구는 국가 전체(KR)를 대상으로 한 EASM 정량 데이터(37,171,622개 노출 포트, 13개 분석 모듈)와 CYFIRMA 위협 인텔리전스를 통합하여, 노출 취약점과 실제 위협 행위자(Lazarus, Kimsuky, APT37, APT41, Qilin 등)의 TTP를 연계 분석한 종합적 프레임워크를 제시하였다는 점에서 기존 연구 대비 분석 범위와 실용성을 확장하였다. 특히 KEV(CISA·VulnCheck) 교차 분석과 RCE 가능 호스트 식별을 통해 우선순위 기반의 대응 방안을 제시하였다는 점은 선행 연구에서 찾아보기 어려운 기여점이다.

본 연구는 몇 가지 한계를 지닌다. 분석에 활용된 Shodan EASM 스캔은 2026년 4월 11일 단일 시점의 스냅샷[19]으로, 사이버 위협 환경의 동적 변화를 시계열적으로 추적하지 못한다는 제약이 있다. 또한 CYFIRMA 위협 인텔리전스는 공개 및 상용 데이터에 기반하므로, 비공개 채널을 통한 위협 활동은 분석 범위에 포함되지 않을 수 있다.

향후 연구에서는 월별·분기별 EASM 스캔 데이터를 축적하여 취약점 노출 추이를 시계열로 분석하고, 이를 실제 침해 사고 데이터와 연계함으로써 공격 표면 변화와 피해 발생 간의 상관관계를 규명할 필요가 있다.

나아가 산업 부문별 취약점 위험 지수를 정량화하는 모델을 개발한다면, 제한된 보안 자원을 가진 중소기업과 공공기관이 보다 효율적으로 우선순위를 설정하는 데 실질적인 기여를 할 수 있을 것이다. 사이버 위협의 선제적 억제는 기술적 대응을 넘어, 지속적인 공격 표면 가시성 확보와 위협 정보 기반의 의사결정 체계 구축에서 시작된다.

ACKNOWLEDGEMENT

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government(MSIT)(IITP-2026-RS-2022-00156334).

REFERENCES

[1] CYFIRMA, “South Korea Threat Landscape Report,” Apr. 2026., *https://www.cyfirma.com/research/south-korea-threat-landscape-report/*

[2] Shodan, "EASM Dashboard - South Korea Internet Exposure Dashboard," easm_KR_20260411_175652, 2026-04-11T17:56:52.

[3] KISA, "2025 Cyber Threat Trend Report," Korea Internet & Security Agency, 2025.

[4] CISA, "Known Exploited Vulnerabilities Catalog," U.S. CISA, 2026. *https://www.cisa.gov/known-exploited-vulnerabilities-catalog*

[5] VulnCheck, "VulnCheck Known Exploited Vulnerabilities," 2026. *https://vulncheck.com/kev*

[6] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-Wide Scanning and Its Security Applications," Proc. USENIX Security Symp., pp. 605-620, 2013. *https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_durumeric.pdf*

[7] E. Bou-Harb, M. Debbabi, and C. Assi, "Cyber Scanning: A Comprehensive Survey," IEEE Communications Surveys and Tutorials, vol. 16, no. 3, pp. 1496-1519, 2014. https://doi.org/10.1109/SURV.2013.102913.00020

[8] Kangsock Choi, Soojin Lee, "A Study on the Analysis of Vulnerabilities in Public Homepage using ASM Solution and Efficient Countermeasures," Journal of Korean Institute of Information Technology (JKIIT), Vol. 23, No. 1, pp. 201-212, 2025. DOI : 10.14801/jkiit.2025.23.1.201

[9] Jae-Pil Yun, Kuk-Jin Kim, Young-Jun Park, Hyeok-Jun Kim, and Dong-Gyu Shin, “Development of AI-based Cyber Attack Group Infrastructure Tracking System,” Defense and Security, Vol. 6, No. 1, pp. 11-38, 2024. https://doi.org/10.23027/ds.2024.6.1.11

[10] K. Liao et al., "Industrial Control System Security: Current Status and Future Prospects," IEEE Access, vol. 7, pp. 64514-64530, 2019. https://doi.org/10.1109/ACCESS.2019.2916086

[11] R. Langner, "Stuxnet: Dissecting a Cyberweapon," IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, 2011. https://doi.org/10.1109/MSP.2011.67

[12] Dragos, "Year in Review: OT Cybersecurity 2024," Dragos Inc., 2025. *https://www.dragos.com/year-in-review/*

[13] Mandiant, "APT41: A Dual Espionage and Cyber Crime Operation," Mandiant Intelligence, 2019. *https://www.mandiant.com/resources/apt41-dual-espionage-and-cyber-crime-operation*

[14] IBM Security, "X-Force Threat Intelligence Index 2025," IBM Corp., 2025. *https://www.ibm.com/reports/threat-intelligence*

[15] Cisco Talos, "CVE-2023-20198: Cisco IOS XE Web UI Privilege Escalation Vulnerability," Cisco Talos Intelligence Group, 2023. *https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/*

[16] NIST, "Special Publication 800-207: Zero Trust Architecture," NIST, 2020. https://doi.org/10.6028/NIST.SP.800-207

[17] Min Cheol Kim, Sejoon Oh, Hyunjae Kang, Jinsoo Kim, and Huy Kang Kim, “Analysis of Attackers' Infrastructure through Data Correlation: Focused on Shodan and Censys,” Journal of the Korea Institute of Information Security & Cryptology (JKIISC), Vol. 28, No. 6, pp. 1449-1461, 2018. DOI: 10.13089/JKIISC.2018.28.6.1449

[18] Wook Shin, Hyunggwan Kim, Hyunggyu Lee, and Jungmin Kang, “Analysis of Vulnerabilities in Industrial Control Systems using Shodan and MITRE ATT&CK,” Journal of the Korea Institute of Information Security & Cryptology (JKIISC), Vol. 35, No. 5, pp. 1185-1194, 2025. DOI: 10.13089/JKIISC.2025.35.5.1185

[19] Seung Han Yoon and Ah Reum Kang, "Shodan EASM and Threat Intelligence Dataset: South Korea Internet-Exposed Asset Vulnerability Analysis (KR_20260411)," GitHub Repository, 2026. *https://github.com/newlife-wq/shodan-easm*

Authors

Seung Han Yoon obtained a bachelor's degree in Information Security through the Korean Academic Credit Bank System in 2022. His major experiences include serving as the head of the integrated security control team at the Gyeongsangnam-do Office of Education (from 2012 to 2016), Director of the Cyber Safety Center at Korea Midland Power and Korea Land & Housing Corporation (from 2016 to 2019), Information Security Team Leader at the Korea Forest Welfare Agency (from 2019 to 2020), and Director of the Cyber Security Talent Center at the Korea Internet & Security Agency (from 2021 to 2022). Currently, he works as the head of the technology infringement analysis team at the Defense Agency for Technology and Quality.

Ah Reum Kang received the M.S. and Ph.D. degrees in information security from Korea University, South Korea, in 2012 and 2016. She is a professor in the Department of Information Security at Pai Chai University in Daejeon, South Korea. Her current research interests include security, artificial intelligence, malware, medical data analysis, and online game security.