Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.2, Apr. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.2.401

전력분야 사이버 위협 분석 및 기반시설 보안 강화를 위한 해외 IP 대역 차단 방안 연구

한 충 희,[1†] 박 순 태,[2] 이 상 준[3‡]
[1]한국전력거래소, [2]한국인터넷진흥원, [3]전남대학교

Oversea IP Ranges Blocking for Security Enhancement of Critical Infrastructures with Cyber Threats Analysis in Electric Industry

Choong-Hee Han,[1†] Soon-Tai Park,[2] Sang-Joon Lee[3‡]
[1]Korea Power Exchange
[2]Korea Internet & Security Agency, [3]Chonnam National Univ

요 약

최근 기반시설에 대한 사이버 공격의 증가에 따라 기반시설의 안전성 강화를 위한 연구와 노력이 계속되어 왔다. 본 논문에서는 다양한 사이버 위협의 정의와 유형에 대해 살펴보고 사이버 위협의 정의를 명확히 하였다. 중국으로부터의 심각한 사이버 위협에 대해 살펴본 후, 사이버 위협의 실체, 즉, 사이버 위협의 출발지, 위협의 유형, 빈도 등을 분석하여 사이버 위협의 명확한 모습을 규명하였다. 이를 통해 사이버 위협 차단을 위한 불필요한 해외 IP 대역 차단 기준을 확립하였다. 불필요한 해외 IP 대역 차단을 위한 방법으로 정보시스템 단위별 차단 방법과 네트워크 단위별 차단방법을 제안하였다. 또한 보안장비별 차단 특성과 보안관제 개선 효과, 악성 해외 IP 대역 차단시의 영향, 해외 정상 사용자들에 대한 서비스 방안 등을 제시하였다.

ABSTRACT

Recently, there has been a lot of studies and efforts to strengthen the stability of critical infrastructures against increasing cyber attacks to critical infrastructures. In this thesis, I defined what cyber threats are, after showing you various definitions about what cyber threats are and what the types are. After studying about significant cyber threats from China, I showed you the realities of cyber threats with the analysis about starting points, types of cyber threats, ratios of attacks and so on. At last, I defined guidelines about unnecessary oversea IP range blocking. Also, I proposed unnecessary oversea IP range blocking methodologies with per information system and per network system. Furthermore, I proposed blocking characteristics per security equipment and security operation improvement and blocking effects and service process to normal oversea users.
Keywords: cyber threats, critical infrastructures, cyber security, cyber threats, IP blocking

I. 서 론

정보기술의 비약적인 발전으로 사이버공간은 급속히 확대되어 의존성이 심화되고 있다. 사이버 공간의 위협은 다양하게 확대되어 완벽한 차단 및 대응을 하기 매우 어려운 상황이다[1]. 전 세계적으로 사이버 공간의 위협을 방어하기 위한 노력을 계속하고 있지만 웜이나 바이러스는 인터넷 환경을 이용하여 우리가 탐지하고 방어하기 어렵게 형태를 변형하여 유입될 수 있는 상황인 것이다[2].

Received(12. 10. 2018), Modified(02. 01. 2019), Accepted(02. 21. 2019)
† 주저자, justicehan@kpx.or.kr
‡ 교신저자, s-lee@chonnam.ac.kr(Corresponding author)

2003년 1월 25일 인터넷 대란을 계기로 국가 위기관리 노력이 강화되고 있다. 다형성 악성코드의 증가, 봇넷 기반의 공격들이 많아짐에 따라 봇넷을 네트워크 위협 전조 증상으로 정의하고 NCSC, KrCERT 등의 경보 등급 산정체계를 기반으로 예·경보 발령 및 공격량 예측 시스템에 대한 연구를 진행하였다. 그러나 취약성을 공격하는 exploit코드 발생 시간에 비해 해당 취약점 탐지 시그니쳐 생성과 배포에 소요되는 시간이 길어 제로 데이 공격에 대응하기 어려운 실정이다. 즉, 사이버 위협 대응 기술 개발을 위해 많은 노력이 계속되고 있지만 위협 대응에는 한계가 존재한다는 것이다[3].

공격자들은 경유지와 유포지를 변경하여 노출을 최소화하고 악성코드의 탐지를 회피한다. 또한 웹사이트 악성코드 은닉기술 이용하여 탐지를 회피한다. 지속적으로 변화하는 악성코드들을 탐지하기 위해 Whitelist기반의 악성코드 탐지기술과 가상환경을 활용하여 분석하는 정상행위 모델링 기법이 제안되고 있다. 그러나 근본적으로 웹브라우저가 웹서버 애플리케이션의 통제범위에 없다는 웹의 근본적인 취약점으로 인해 공격자의 임의조작, 훼손이 얼마든지 가능하다. OWASP Top10에 나온 취약점들을 보면 웹의 근본적인 취약점을 이용하는 공격이 다수를 이루고 있다[4].

II. 선행 연구

2.1 주요정보통신기반시설의 정의

본 논문에서 사용하는 '기반시설'은 '주요정보통신기반시설'을 의미한다. 정보통신기반보호법 제2조에 따르면 '정보통신 기반시설'이란 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 규정에 의한 정보통신망을 말한다. 동법에서는 정보통신 기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 '주요정보통신 기반시설'로 지정할 수 있도록 하였다.

이용우[5]는 '주요정보통신 기반시설'이란, 국가나 공공기관 뿐 아니라 민간이 운영・관리하는 정보통신시설을 포함한다고 설명한다. 사이버 침해행위 발생 시 국가안보, 국민의 기본생활 경제적 안정에 중대한 영향을 미치게 되는 정보통신 기반시설을 의미한다고 설명하였다.

2.2 사이버 위협의 정의, 유형

사이버 위협에 대한 정의와 유형은 연구자에 따라 다양하게 나타나고 있다. 송동훈[6]은 사이버 위협을 '새로운 유형의 테러리즘으로서 사이버공간을 통해 공격을 감행하는 것'이라고 설명한다. 경찰학 사전은 '컴퓨터해킹, 바이러스, 메일폭탄, 사이버 스토킹 등'으로 기술한다. 경찰청 사이버 안전국에서는 '해킹, 서비스 거부공격, 악성프로그램 및 기타 정보통신망 침해형 범죄'를 사이버 위협의 유형으로 기술한다. 한국인터넷진흥원의 침해사고대응안내서에 따르면 '바이러스, 트로이목마, 악성코드 등의 공격, 네트워크 및 시스템의 정상적인 서비스를 마비 파괴시키는 서비스 방해, 네트워크 서비스의 취약점을 이용하여 서비스를 무단 이용하는 비 인가된 서비스 이용, 비인가 접근 등'을 사이버 위협의 유형으로 설명하고 있다.

이임섭[7]은 사이버 위협을 '감청, 통신 데이터 분석, 무선데이터 패킷 가로채기, 사람의 실수로 인한 정보유출, 정보매체 조사를 통한 해킹 정보 수집, 트로이 목마, 백도어, 서비스 스푸핑, 위장, 우회조작, 허가 침해, 물리적 침해, 재생 공격, 불법적 도용, 서비스 지연공격'의 15가지로 나누었다. 그러나 사이버 위협에 '물리적 침해'를 포함하는 것은 너무 포괄적인 적용이다.

이상에서 살펴본 것과 같이 사이버 위협에 대한 기존의 정의들은 사이버 위협을 너무 광범위하게 포괄적으로 제시하고 있다. 이에 3.2.1절에 사이버 위협의 정의와 유형을 명확히 정리하였다.

주차원[8]은 2010~2012년 사이의 몇몇 공공기관들 중 3개 기관을 대상으로 사이버 공격에 대한 위협들을 수집 조사하였다. 중복을 제거하여 173개의 사이버 공격 위협을 분류하고 위험 등급을 상중하로 구분하였다. 위험도 상(High) 23종, 중(Medium) 60종, 하(Low) 90종으로 제시하였다. 주차원의 연구의 한계점은 우선 173개의 위협은 'malware-downloader(dogrobot), txt?? (PHP URL mainpulate Remote File injection-1, mass sql injection-1' 등과 같이 정보보안 설비들에 등록해 놓은 탐지정책 명칭들로서 비전문가들은 그 탐지정책명만으로는 위협 내용이 무엇인지를 파악하기 어렵다는 한계가 존재한다. 또한 위협의 위험도를 상중하의 3단계로 구분하는 것은 가운데 위협단계에 대한

모호함이 존재한다는 점에서 위험도를 고위험과 저위험의 2단계로 구분하는 것보다 명시성이 떨어지는 한계점이 존재한다.

2.3 중국의 사이버 위협 현황

이후기[9]는 2014년 12월 15일부터 2015년 3월 12일까지 총 6회에 걸쳐 한국수력원자력 사이버테러 사건의 IP를 분석하였다. 북한의 해커조직의 IP 대역과 중국 IP 대역들이 12자리 중 9자리까지 일치하였고, 북한 IP 주소 25개, 북한 체신성 산하 통신회사인 KPTC에 할당된 IP주소 5개가 접속한 흔적이 발견되었다고 설명하고 있다. 악성 IP들이 재사용되는 사례가 대부분이며 기존의 유해 IP들에 대한 보관 기준을 연구하였다. 공공기관들을 대상으로 악성 유해 IP의 탐지, 경과일, 유해 IP 발생 비율, 재사용 비율 등에 관한 연구를 통해 국내외 구분 없이 1년간 보관하는 것이 바람직하다고 주장하였다.

신경수[10]는 중국의 사이버전 인력이 약 10만명에 이르며 북한의 사이버전 인력을 약 7,700여명으로 추정한다. 북한의 IP 주소는 총 1,024개로 추정하며 이러한 사실은 북한의 체신성과 태국의 '록슬리(Loxley)그룹'이 합자해서 만든 '스타조인트벤처'라는 회사의 이름으로 지난 2009년에 ANPIC(Asia Pacific Network Information Centre)에 등록하면서 밝혀졌다. 실제로 북한의 공식 포털 사이트 '내나라'와 '조선중앙통신', '노동신문' 등이 이 대역의 IP 주소를 쓰고 있으며 북한의 대남 선전용 홈페이지 '우리민족끼리'는 중국 선양의 IP 주소를 사용하고 있다. 북한은 남한정부를 상대로 미처 방어하지 못하는 신기술을 이용해 해킹공격과 사이버 테러작전을 지속적으로 구가하고 있다고 설명한다.

최해권[11]은 시만텍사의 자료를 이용하여 2007년의 국가별 보안위협 발원지 현황을 제시하였는데 전 세계를 대상으로 한 보안 위협의 발원지 1위 국가는 미국 중국의 순이었다. 중국 발 악성코드의 특징으로 PC를 다운시키거나 다른 파일을 감염시키지는 않으면서 개인정보나 파일들을 빼내는 유해 프로그램들이 많다고 설명한다.

2.4 미국의 익명 사용자 IP 차단 연구

Patrick[12]은 익명의 라우팅 네트워크 뒤에 숨어 있는 익명 사용자의 IP주소 차단에 대해 연구하였다. 웹사이트에 연결하기 전에 웹사이트의 '블랙리스트'에 있는지 여부를 확인하여 블랙리스트에 있을 경우 연결을 제한하는 것이다. 사전에 선정해 놓은 신뢰할 수 있는 노드들은 웹 사이트의 블랙리스트를 최신 버전을 유지 관리하게 함으로써 안전한 네트워크 환경을 제공하는 방법을 연구하였다. 신뢰할 수 있는 노드들과 블랙리스트의 관리를 통해 네트워크 보안을 향상시키는 방법을 제안하였다.

Chris[13]는 전자 메일 트래픽의 90%를 넘어서는 스팸 전자메일의 보안 문제를 연구하였다. 기존의 방법은 내용과 헤더의 내용을 분석하여 탐지 필터링하고 스팸 호스트 IP 주소 목록을 유지 관리하는 방법이다. 그러나 많은 IP 주소가 동적으로 할당되므로 시간이 지남에 따라 다른 주소로 변경될 수 있는 한계가 있다. 이를 해결하기 위해 IP 주소간의 상관관계를 측정하는 방법을 도입하여 스팸 호스트 IP에 대한 효율적인 차단 방법을 제안하였다.

Ferry[14]는 TOR(The Onion Router) 환경에서 패킷 분석과정을 거쳐 토르 트래픽을 차단하는 방법을 제안하였다. 포트 미러링을 통해 패킷을 수집하여 패킷 정보를 추출한다. 유효한 토르 패킷 정보를 추출하여 로그파일에 목적지 IP주소를 기록하고 해당 IP정보를 토르 연결 차단시 참고자료로 활용하는 방법을 제안하였다.

Ferguson[15]은 BCP 38이라는 모델을 통해 IP 변조와 위장을 통한 익명성의 위협을 차단하고자 하였다. 패킷의 유입을 필터링하여 불법적인 IP주소를 가진 패킷들을 라우터에서 차단하였다. 그러나 BCP 38은 패킷 필터링을 위해 많은 자원과 노력을 요구한다는 점이 문제였다. 또한 라우터 경계구간에서는 동작이 잘 되지만 다른 구간에서는 탐색시간이 상당히 소요되는 단점이 있는 것으로 나타났다.

Vijayalakshmi[16]는 단일-패킷 IP 추적 방법을 제안하여 익명의 사이버 공격자를 추적하고자 하였다. 기존의 SPIE(Single-Packet trace-back scheme)은 많은 양의 저장 공간과 과부하를 유발하였다. 이를 개선하기 위해 HPSIPT (High-precision single-packet IP traceback scheme)을 제안하여 저장 공간과 과부하 발생을 유발하지 않도록 개선하였다.

2.5 미국의 해외 IP 차단 현황

미국의 경우 2001년 9.11 테러 이후 국가 위기관

리의 핵심적 요인으로 인식하고 2007년 12월 조지부시 대통령의 행정명령 'Implementation of Trusted Internet Connection'에 의해 미국 연방정부시설의 웹사이트 접속에 대한 외부로부터의 접점을 최소화 또는 Blocking과 같은 강화된 안전성 확보조치들을 진행하였다[17][18]. 아래의 그림 1, 2에서 미국 텍사스의 전력시장 계통운영기관 ERCOT의 해외 IP 차단 사례를 확인할 수 있다.

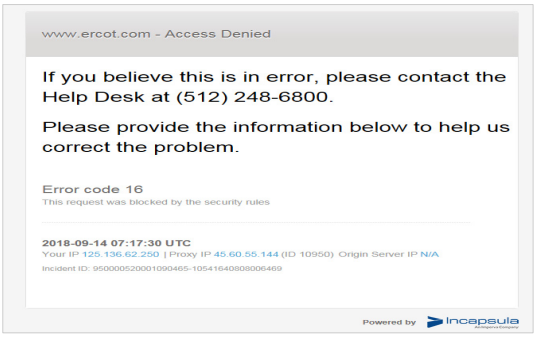

Fig. 1. Blocking case of ERCOT

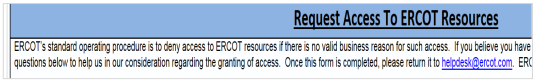

Fig. 2. Blocking policy of ERCOT

2.6 국내 민간 사이트의 중국 IP 차단 현황

국내의 경우 2006년을 전후로 중국의 해킹 위협으로 인한 피해가 늘어나자 IP 차단 방법들을 공유하기 시작하였다. 주로 웹호스팅, 게임, 실시간 방송 업체 등이 중국 IP 차단을 하고 있는 것으로 조사되었다. 아래의 표 1은 Naver.com에서 '중국 IP 차단'이라는 검색어로 검색할 경우 나타나는 중국 IP 차단 결과들 중 일부를 표로 정리한 것이다.

Table 1. Blocking cases for China IP

	Name of website	Day of blocking
1	internet fishing community	2012.4.27
2	geochat	2013.3.21
3	JNS	2017.3.28
4	F-coin	2018.8.28

※ 'blocking China IP' Search result with Naver.com

III. 전력 분야 사이버 위협 분석

3.1 분석 목적, 대상 및 방법

전력분야 사이버 위협 분석의 목적은 국가 중요 서비스인 전력분야에 대한 구체적인 사이버 위협의 실체, 종류와 내용들을 명확하게 규명하는 것이다. 이를 통해 국가 중요시설을 보유한 기관들의 사이버 위협 대응 활동에 새로운 방법론을 제시 한다.

사이버 위협 분석의 대상은 전력분야 공공기관의 2015년부터 2018년 12월까지의 IPS에 의한 사이버 위협 차단 로그 데이터를 기반으로 한다. 차단 로그들은 대상 공공기관의 대외 인터넷 서비스망에 설치된 IPS 장비들로부터 수집되었다.

분석 방법은 4개년, 약 40,000여개의 사이버 위협 차단 로그들을 엑셀의 피벗 기능을 이용하여 분석하였다. 다양한 각도에서 데이터들을 살펴보는 과정 속에서 사이버 위협의 실체, 즉, 어디로부터 어떤 방법으로 나타나고 있는지를 분석하였다.

분석의 제한사항은 1개의 전력분야 공공기관의 2015년부터 2018년 12월까지의 IPS 차단 로그들을 대상으로 한다는 것이다. 전력분야 공공기관 전체의 IPS 차단로그들을 협조 받아 분석하는데 제한이 존재하여 1개 기관의 데이터를 면밀히 분석한다. 그러나 사이버 위협은 불특정, 무작위적인 성격이 강하므로 우리나라 기반시설 전체와 외국과의 업무적 연관성이 없는 일반적인 IT기업들의 사이버 위협 연구에 적용 가능할 것이다.

3.2 사이버 위협 분석

3.2.1 사이버 위협 정의와 종류

사이버 위협의 분류와 정의는 선행 연구에서 살펴보았듯이 다양하다. 본 논문에서는 사이버 위협을 '정보화 자산이 인터넷 네트워크를 통해 악의적인 행위들에 노출되는 위협'으로 정의하며, 보안관제 침해대응활동을 통해 24시간 365일 끊임없이 분석 및 차단되고 있는 '악성 IP'를 이용하여 사이버 위협의 실체를 분석한다.

이하의 분석과정에서 사용되는 사이버 공격 명칭들은 IPS장비의 복잡한 탐지 명칭들을 쉽게 이해할 수 있도록 풀어서 표현하였다. 사이버 공격 명칭들 중 정보 수집성 공격을 제외한 고위험도 사이버 공격들

은 High라는 (H)를 표시하였다. (H)가 붙은 사이버 공격 탐지 비율들의 연도별 합계 비율을 활용하여 고위험도 공격의 증가 현상을 분석하였다.

3.2.2 사이버 위협의 출발지

사이버 공격을 시도하는 사이버 위협, 즉 악성 IP의 출발지를 국내와 국외로 나누어 볼 때 전력분야의 사이버 위협은 4개년 평균으로 국외로부터의 사이버 위협이 전체 사이버 위협의 약 96%를 차지하는 것으로 분석되었다. 사이버 위협을 발생시키는 국가별로 살펴보면 중국으로부터의 사이버 위협이 4년 연속 최다국으로 분석되었다. 2015년, 2016년에는 중국이 전체 사이버 위협 발생국 중 44~55%를 점유하였으나 2017년, 2018년도에는 다른 국가들의 점유율 증가로 25~36.9% 수준으로 다소 낮아졌다.

2017년과 2018년 2개년의 통계자료를 기준으로 사이버 위협 2위국은 미국으로 22~24%, 3위는 브라질로 10~22% 사이를 점유하는 것으로 표 3과 같이 분석되었다.

2015년부터 2018년 12월까지의 각각의 연도별 상위 10개국의 사이버 위협 발생 현황은 최소 69.9%에서 최대 79.7%이며 평균 74.5%의 점유율을 나타낸다. 아래의 표 2와 3으로 정리하였다.

Table 2. Yearly Top10 Nations share of Bad IPs

category	Year			
	2015	2016	2017	2018
10 nations total	4,479	3,666	6,662	10,700
year total	5,961	4,598	9,159	15,313
share of 10 nations	75.8%	79.7%	72.7%	69.9%

Table 3. Top10 Nations of Bad IPs

[Year 2015]

	Nation	Count	Ratio
1	China	1,982	44.25%
2	USA	1,012	22.59%
3	Korea	285	6.36%
4	Netherland	243	5.43%
5	Germany	205	4.58%
6	France	175	3.91%
7	Taiwan	173	3.86%
8	Russia	167	3.73%
9	Thailand	126	2.81%
10	Japan	111	2.48%
	Total	**4,479**	

[Year 2016]

	Nation	Count	Ratio
1	China	2,035	54.78%
2	USA	657	17.69%
3	Netherland	205	5.52%
4	Germany	146	3.93%
5	Russia	126	3.39%
6	Canada	125	3.36%
7	France	103	2.77%
8	HongKong	102	2.75%
9	Taiwan	95	2.56%
10	Brazil	72	1.94%
	Total	**3,666**	

[Year 2017]

	Nation	Count	Ratio
1	China	1,674	25.13%
2	Brazil	1,495	22.44%
3	USA	1,467	22.02%
4	Germany	351	5.27%
5	Korea	350	5.25%
6	Netherland	286	4.29%
7	England	283	4.25%
8	Russia	282	4.23%
9	France	241	3.62%
10	Canada	233	3.50%
	Total	**6,662**	

[Year 2018]

	Nation	Count	Ratio
1	China	3,948	36.9%
2	USA	25,84	24.1%
3	Brazil	1,088	10.2%
4	Egypt	591	5.5%
5	Korea	496	4.6%
6	Russia	418	3.9%
7	England	403	3.8%
8	Canada	401	3.7%
9	HongKong	391	3.7%
10	France	380	3.6%
	Total	**10,700**	

3.2.3 사이버 위협의 연도별 변화

전체 사이버 공격 탐지 건을 살펴볼 때, 2017년보다 2018년에는 직접적인 공격 목적을 가진 고위험도 공격이 더 높아지는 것으로 분석된다. 관리자 페이지 접근, 임의코드 실행, 원격명령 실행, DOS공격 등의 고위험도 공격이 2017년에는 80.79%, 2018년에는 86.82%로 점차 높아지는 것으로 표 4와 같이 조사되었다. 이를 통해, 사이버 공격의 형태와 위험도는 연도별로 일정하지 않으며 매년 끊임없이 변화되고 있다는 것을 확인할 수 있다.

Table 4. Cyber Attacks Top 10

	Cyber Attacks Top 10 in 2017	Count	Ratio
1	Wordpress management page connection(H)	1,073	21.39%
2	file excution by wireless router remote excution vulnerability(H)	848	16.91%
3	Remote Command excution vulnerability attack with Apache struts 2(H)	728	14.51%
4	PBX system scan with SIPVicious	643	12.82%
5	Scanning for inner server status	320	6.38%
6	Management page connectin & webserver vulnerability checking by Muieblackcat(H)	317	6.32%
7	phpmyadmin basic page connection(H)	299	5.96%
8	DOS attack by abnormal TCP Flag mix(H)	285	5.68%
9	FCK Editor management page connection(H)	252	5.02%
10	D-Link ID, PW disclosure attack(H)	251	5.00%
	Total	5,016	

	Cyber Attacks Top 10 in 2018	Count	Ratio
1	OS command injection attack by URL vulnerability(H)	1,373	18.10%
2	Wordpress management page connection(H)	1,366	18.01%
3	Oracle web logic vulnerability attack(H)	1,300	17.14%
4	BOF Attacks by Webdav propfind(H)	753	9.93%
5	remote excution vulnerability of Dasan router attack(H)	564	7.43%
6	zgrab Scanner Scan	507	6.68%
7	Scanning for inner server status	494	6.51%
8	wget file download to server(H)	420	5.54%
9	D-Link ID, PW disclosure attacks(H)	408	5.38%
10	file excution by wireless router remote excution vulnerability(H)	401	5.29%
	Total	7,586	

3.2.4 주요 3개국의 사이버 위협 현황

2018년 기준 주요 사이버 위협국 Top 3 국가(중국, 미국, 브라질)의 2015년부터 2018년까지의 악성 IP 차단 건수의 변화 추이와 전체 악성 IP 건수 대비 점유율을 표 5와 그림 3으로 표현하였다. 주요 사이버 위협 3개국의 악성 IP 점유율은 최소 50%에서 최대 60% 수준이며 평균 53% 수준이다.

Table 5. Counts & share of bad IPs of 3 nations

category	Year			
nation	2015	2016	2017	2018
China	1,982	2,035	1,674	3,948
USA	1,012	657	1,467	2,584
Brazil	39	72	1,495	1,088
3 nations total	3,033	2,764	4,636	7,620
all nations total	5,961	4,598	9,159	15,313
share of 3 nations	51%	60%	51%	50%

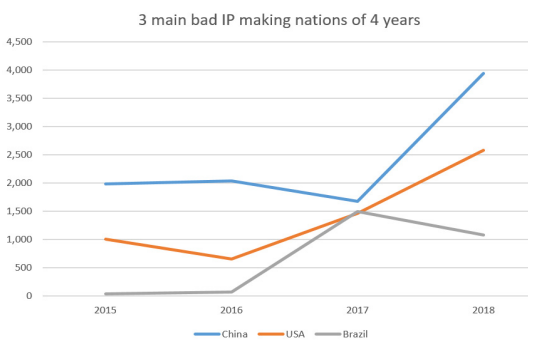

Fig. 3. 3 main cyber threat nations

3.2.4.1 중국의 사이버 위협

그림 3에서 보는 바와 같이 중국의 사이버 위협은 전체적인 점유율은 다소 낮아졌으나 고위험도가 대체적으로 증가하고 있는 것으로 분석된다. 2017년에 비해 2018년에는 고위험도가 높아져서 웹로직 취약점을 이용하는 공격 시도가 40.51%, 버퍼 오버플로우 유도 공격이 27.76% 등 10위권 내의 공격 시도 중 89.26%가 고위험도 공격인 것으로 표 6과 같이 분석되었다. 2017년에는 64.65% 정도가 고위험도 공격이었다.

Table 6. Cyber Attacks Top 10 from China

	Cyber Attacks Top 10 in 2017	Count	Ratio
1	Remote Command excution vulnerability attack with Apache struts 2(H)	263	26.95%
2	DOS attack by abnormal TCP Flag mix(H)	161	16.50%
3	Sharing folder scanning	88	9.02%
4	FCK Editor management page connection(H)	75	7.68%
5	Scanning for inner server status	74	7.58%
6	Wordpress management page connection(H)	74	7.58%
7	Possible Methods scanning in webserver	64	6.56%
8	135/TCP RPC Port Scanning	63	6.45%
9	phpmyadmin basic page connection(H)	58	5.94%
10	vulnerability scanning for network infra	56	5.74%
	Total	976	

	Cyber Attacks Top 10 in 2018	Count	Ratio
1	Oracle web logic vulnerability attack(H)	683	40.51%
2	BOF Attack by Webdav propfind(H)	468	27.76%
3	apache tomcat directory login trials	134	7.95%
4	Remote Command excution vulnerability attack with Apache struts 2(H)	128	7.59%
5	Webshell file upload(H)	65	3.86%
6	wget file download to server(H)	50	2.97%
7	vulnerability scanning for network infra	47	2.79%
8	Wordpress management page connection(H)	39	2.31%
9	FCK Editor management page connection(H)	37	2.19%
10	DDos by changing Http Header(H)	35	2.08%
	Total	1,686	

3.2.4.2 미국의 사이버 위협

그림 3에서 보는 바와 같이 미국의 사이버 위협은 고위험도가 동일하거나 다소 낮아진 것으로 분석된

다. 2017년에 비해 2018년에는 고위험도가 다소 높아져서 웹로직 취약점 공격 시도가 13.34%, SQL Injection 공격 6.63% 등 10위권 내의 공격 시도 중 37.25%가 고위험도 공격인 것으로 표 7과 같이 분석되었다. 2017년에는 42.11% 정도가 고위험도 공격이었다.

Table 7. Cyber Attacks Top 10 from USA

	Cyber Attacks Top 10 in 2017	Count	Ratio
1	PBX system scan with SIPVicious	189	25.68%
2	Remote Command excution vulnerability attack with Apache struts 2(H)	103	13.99%
3	Scanning for inner server status	78	10.60%
4	vulnerability scanning for network infra	61	8.29%
5	Wordpress management page connection(H)	61	8.29%
6	Simple Scanning	56	7.61%
7	Management page connectin & webserver vulnerability checking by Muieblackcat(H)	53	7.20%
8	Webshell file upload(H)	48	6.52%
9	phpmyadmin basic page connection(H)	45	6.11%
10	Sharing folder scanning	42	5.71%
	Total	736	

	Cyber Attacks Top 10 in 2018	Count	Ratio
1	zgrab Scanner Scan	452	37.92%
2	Scanning for inner server status	161	13.51%
3	Oracle web logic vulnerability attack(H)	159	13.34%
4	PBX system scan with SIPVicious	89	7.47%
5	SQL INJECTION(H)	79	6.63%
6	Wordpress management page connection(H)	60	5.03%
7	Webshell file upload(H)	51	4.28%
8	BOF Attacks by Webdav propfind(H)	49	4.11%
9	MSSQL Scan	46	3.86%
10	wget file download to server(H)	46	3.86%
	Total	1,192	

3.2.4.3 브라질의 사이버 위협

그림 3에서 보는 바와 같이 브라질의 사이버 위협은 고위험도가 대체적으로 동일하거나 다소 증가하고 있는 것으로 분석된다. 2017년에 비해 2018년에는 고위험도가 높아졌다. 2018년에는 D-Link 관련 중요정보 노출 공격 40%, 무선 공유기 임의코드 원격 실행 39%, URL 취약점을 이용한 OS명령어 삽입공격 7.9%, 관리자 페이지 접근시도 5.5%, 웹쉘 파일 업로드 시도 2.5% 등 10위권 내의 공격 시도 중 96.68%가 고위험도 공격인 것으로 표 8과 같이 분석되었다. 2017년에는 93.6% 정도가 고위험도 공격이었다.

Table 8. Cyber Attacks Top 10 from Brasil

	Cyber Attacks Top 10 in 2017	Count	Ratio
1	file excution by wireless router remote excution vulnerability(H)	848	62.40%
2	D-Link ID, PW disclosure attack(H)	251	18.47%
3	OS command injection attack by URL vulnerability(H)	84	6.18%
4	Wordpress management page connection(H)	41	3.02%
5	Host information collection by packet	39	2.87%
6	Slider Revolution of WordPress plug-in file download vulnerability attacks(H)	33	2.43%
7	vulnerability scanning for network infra	25	1.84%
8	Remote Command excution vulnerability attack with Apache struts 2(H)	15	1.10%
9	Network sharing netbios port scanning	12	0.88%
10	PBX system scan with SIPVicious	11	0.81%
	Total	1,359	

	Cyber Attacks Top 10 in 2018	Count	Ratio
1	D-Link ID, PW disclosure attack(H)	408	39.80%
2	file excution by wireless router remote excution vulnerability(H)	400	39.02%
3	OS command injection attack by URL vulnerability(H)	81	7.90%
4	Wordpress management page connection(H)	56	5.46%
5	wget file download to server(H)	26	2.54%
6	vulnerability scanning for network infra	22	2.15%
7	Oracle web logic vulnerability attacks(H)	10	0.98%
8	SQL INJECTION(H)	10	0.98%
9	Network sharing netbios port scanning	6	0.59%
10	Scanning for inner server status	6	0.59%
	Total	1,025	

3.2.5 주요 20개국의 사이버 위협 현황

2018년 1월부터 12월까지의 악성 IP 발생 주요 사이버 위협국 상위 20개국의 전체 국가 대비 비율은 약 84.1%를 점유하는 것으로 나타난다. 이를 통해, 파레토의 법칙(Pareto's Law)에서 말하는 통계학의 현상이 동일하게 적용되고 있음을 알 수 있다. 아래의 표 9는 악성 IP 발생 상위 20개국 현황과 점유율이다.

주요 사이버 위협 20개국의 악성 IP 점유율은 최소 80%에서 최대 89% 수준이며 평균 84.3% 수준이다. 아래의 표 10에 2015년부터 2018년 4개년 동

안의 상위 20개국의 점유율 현황을 정리하였다.

Table 9. Top 20 Nations of Cyber Threats in 2018

[Year 2018.1 ~ 12]

	Nation	Count		Nation	Count
1	China	3,948	11	Netherlands	331
2	USA	2,584	12	Mexico	300
3	Brazil	1,088	13	Italy	274
4	Egypt	591	14	Japan	228
5	Korea	496	15	Germany	200
6	Russia	418	16	India	190
7	England	403	17	Mauritius	178
8	Canada	401	18	Thailand	176
9	HongKong	391	19	Indonesia	153
10	France	380	20	Vietnam	150
20 nations total		12,880(84.1%)	all nations Total		15,313

Table 10. Yearly Top20 Nations share of Bad IPs

category	Year			
	2015	2016	2017	2018
20 nations total	4,984	4,097	7,394	12,880
year total	5,961	4,598	9,159	15,313
share of 20 nations	83.6%	89.1%	80.7%	84.1%

3.2.6 보유 IP 대역 대비 국가별 악성 IP 비율

한국인터넷진흥원(KISA) 인터넷정보센터의 전세계 국가별 보유 IP대역은 총 190,350개이다. 2018년 한국을 제외한 5대 주요 악성 IP 발생 국가들의 보유 IP대역 현황을 살펴보면 미국이 가장 많은 IP대역을 보유하여 약 28%(53,522개)으로 나타난다. 브라질은 약 4.8%(9,091개), 러시아는 약 4.6%(8,823개), 중국은 약 4.3%(8,251개), 이집트는 약 0.1%(164개)를 보유하고 있는 중이다.

국가별 악성 IP 비율은 2018년 5대 주요 악성 IP 발생 국가들의 악성 IP 발생 건수와 국가별 보유 IP대역 수량의 비율로 계산한다. 최대 악성 IP 비율 국가는 이집트로 244.5%, 그 다음은 중국으로 47.85%를 나타내는 것을 확인할 수 있다. 이러한 악성 IP 발생 비율을 근거로 살펴본다면 이집트와 중국의 사이버 위협이 가장 심각한 것을 알 수 있다. 중국의 악성 IP 발생비율을 1로 볼 경우 이집트는 5.11배로 높고, 미국과 러시아는 0.1배 수준이며 브라질이 0.25배 수준을 나타낸다. 이를 표로 나타내면 표 11과 같다.

Table 11. Bad IP Ratio per countries' IP Ranges in 2018

category	USA	Brazil	Russia	China	Egypt
retention IP Ranges (A)	53,522	9,091	8,823	8,251	164
retention IP ranges ratio in 2018	28.1%	4.8%	4.6%	4.3%	0.1%
Bad IPs in 2018 (B)	2,584	1,088	418	3,948	401
Bad IP making Ratio(B/A)	4.83%	11.97%	4.74%	47.85%	244.51%
Bad IP Ratio Magnification with China	0.10	0.25	0.10	1.00	5.11

※ Total IP ranges are 190,350 in the world(2018.12.31)

IV. 해외 사이버 위협 차단 방안

4.1 해외 IP대역 차단 및 허용 기준 확립

기반시설을 보유한 기관들의 외부 인터넷 정보시스템들에 대한 차단 및 허용 기준을 범국가적인 사이버 안보 강화라는 관점에서 재검토하여야 한다. 국민을 위한 기본적인 인프라 서비스 제공을 목적으로 하는 기반시설들에 대해 해외로부터의 접근 허용이 과연 필요한 것인지에 대한 심도 있는 고찰이 필요하다. 이를 통해 해외 IP대역으로부터의 접근에 대한 차단 및 허용 기준을 수립해야 한다. 만약 기반시설의 업무와 직접적인 연관이 없다면 해외 IP대역으로부터의 외부 인터넷 정보시스템들에 대한 접근을 원칙적으로 차단하고 필요한 경우 접속 목적과 IP와 연락처 정보를 이메일로 신청 받아 검토한 후 제한적으로 허용하는 것이 필요하다.

4.2 해외 IP 대역 차단 방안

4.2.1 정보시스템 단위별 해외 IP 대역 차단

해외로부터의 접속이 불필요한 정보시스템들에 대

해 한국 IP대역만 접속을 허용하는 정책을 적용하여 악성 해외 IP대역을 차단할 수 있다. 정보시스템별로 해외 접속을 차단하는 방안은 개별 정보시스템별 특성에 따라 차단 정책을 적용할 수 있는 것이 장점이다. 보안관제 부서의 입장에서는 더 많은 차단정책 등록 과정이 필요하지만 꼭 필요한 정보시스템별로 신속하게 차단할 수 있어서 우수하다.

정보시스템별로 차단할 경우에는 해외와의 연관성과 차단의 복잡도를 종합적으로 고려하여야 한다. 이를 통해 해외 차단 긴급도를 1순위와 2순위로 도출해 낸다. 해외 차단 긴급도 1순위는 우선적으로 차단할 수 있는 정보시스템들이며 2순위는 추가적인 영향 검토를 필요로 하는 정보시스템들에 해당한다. 2순위 정보시스템들에는 돈과 연관이 있는 시스템들이거나 기관의 대표 홈페이지이거나, 메일시스템이거나 통계시스템을 포함할 수 있다. 1순위와 2순위 판단은 철저하게 정성적인 판단으로 기관 자체의 개별적인 특성에 따라 다르게 적용 가능할 것이다.

정보시스템 구축시 국내와 국외 구분 없이 열어둔 웹서비스(HTTP, HTTPS)에 대해서 해외로부터의 접속이 필요 없다면 국내 IP대역과 각 회사내 인터넷 IP대역만 접속을 허용하여야 한다. 국내 IP대역은 한국인터넷진흥원 인터넷정보센터의 IP대역자료 중 한국 IP대역 자료를 참고한다. 그림 4는 국가별 IP 대역 조회화면이다.

Fig. 4. Nations' IP ranges pages of KISA

4.2.2 네트워크 단위별 해외 IP 대역 차단

해외 IP 대역 차단을 네트워크 단위별로 적용할 수도 있을 것이다. 이 경우에는 각 네트워크 단위 내의 모든 정보시스템들이 차단의 영향을 받게 될 것이다. 우선, 전 세계 IP 대역을 모두 막은 후 국내 IP 대역을 허용하는 방법을 사용할 수 있을 것이다. 이 방법은 보안관제부서의 차단정책 적용 과정이 가장 간편하고 적용하기 쉬울 것으로 판단된다. 기반시설을 보유한 기관의 경우 이 방식이 가장 효과적이다. 그 이유는 기반시설의 서비스 목적이 국내에 있기 때문이다. 기반시설을 운영하는 목적이 해외의 전세계 사람들을 대상으로 하는 것이 아니기 때문에 특별한 경우가 아니라면 네트워크 단위별로 해외 IP대역을 차단하고 국내만 허용하는 정책의 적용이 반드시 필요할 것으로 판단된다.

Table 12. Oversea IP range Blocking methods

Category	Per Information System	Per Network System	
		All Nation	some Nation
① Convenience	○	○	
② Repulsion		○	
③ accuracy	○		
④ effectiveness		○	
⑤ availability	○		○

전체 해외 국가를 차단하는 것이 어렵다면 최대 사이버 위협국 몇 개만 막는 것도 가능할 것이다. 이 경우에는 Blacklist 방식으로 최대 사이버 위협국의 IP 대역을 방화벽에 등록해서 차단 효과를 낼 수 있다. Blacklist방식으로 사이버 위협국의 IP 대역을 무한정 차단하는 것은 어려울 것으로 판단된다. 보안장비의 특성상 차단 IP 대역을 무한정 등록시킬 수 없기 때문이다. 중국으로부터의 IP 유입만 차단시켜도 악성 IP 감소율은 전체를 막아서 얻을 수 있는 효과의 약 50% 정도의 악성 IP 발생 감소효과를 볼 수 있을 것이다. 아래의 표 12로 해외 IP 차단 방법별 특징들을 정리하였다.

4.3 웹서비스 방식별 접근 가능 현황

현재 인터넷으로 웹서비스(HTTP, HTTPS)를 제공하는 정보시스템들은 국내와 국외를 구분하지 않고 모두 웹서비스에 대한 접근이 허용되어 있는 상황이다. 특히 인가된 사용자를 기반으로 웹서비스를 하는 정보시스템에서도 국내와 국외로부터 접근이 가능한 상황이다. 아래의 표 13에서 웹서비스 인증 형태에 따른 접근 가능 현황을 정리하였다.

Table 13. Access permission cases per web authentication types

Category	Non-Authenticated members		authenticated members
	Abroad	domestic	
① IP Authentication by Firewall	×	×	○
② URL Authentication (www.url.co.kr /admin)	○	○	○
③ ID/PWD Authentication	○	○	○

4.4 차단 가능 보안장비 특성 검토

해외 IP 대역 차단은 4가지 장비에서 실현이 가능하다. 라우터 장비에서는 싱크홀 라우팅을 이용하여 차단이 가능하며, DDoS, 방화벽, IPS에서는 차단 및 허용 정책을 통해 차단이 가능할 것이다. 그러나 각 장비들의 고유한 기능을 고려할 때 DDoS와 방화벽을 이용하는 것이 가장 타당할 것이며 단기적인 관점에서는 DDoS가 유리하며 장기적인 관점에서는 방화벽을 이용하는 것이 가장 이상적인 차단방법이 될 것으로 판단된다. 아래의 표 14와 같이 장비별 차단 특성 및 가능 여부를 정리하였다.

Table 14. Access permission cases per web authentication types

Category	Per Information System	Per Network System	
		All Nation	some Nation
① Router	×	△	△
② DDoS	○	○	○
③ FireWall	○	○	○
④ IPS	△	△	△

※ Possible but not recommendable is '△'
Possible and recommendable is '○'
Impossible is '×'

4.5 해외 IP 대역 차단시 보안관제 업무 개선

보안관제 업무 중 해외의 악성 IP 차단을 위해 여러 가지 활동들을 수행하고 있다. 추가공격 여부 확인, 악성 IP의 WHOIS 검색, 네트워크별 보안장비에 악성 IP 차단 등록, 실무부서에 취약점을 보유한 SW 설치 및 변조 여부 확인 요청 등의 활동들이 수행된다.

4.5.1 추가 공격 여부 확인

악성 IP가 확인되었을 때 가장 먼저 해야 할 일은 해당 악성 IP가 추가적인 공격을 시도했는지 여부이다. 이러한 과정을 통해 악성 IP의 배후가 어느 정도 악성 의지를 가지고 있는지를 판단할 수 있다. 추가 공격 여부를 확인하는데 소요되는 시간은 악성 IP 1개 당 약 3분 정도로 나타났다.

4.5.2 악성 IP 조회

악성 IP가 확인되는 경우 한국인터넷진흥원의 WHOIS 검색을 통해 악성 IP의 발생 국가와 IP 대역을 확인할 수 있다. 악성 IP의 WHOIS 검색 활동에 소요되는 시간은 악성 IP 1개 당 약 3분정도 소요되는 것으로 나타났다.

아래의 그림 5은 WHOIS검색을 통해 악성 IP 175.45.177.145의 관련 정보를 조회하는 그림이다. 조회를 통해 위 악성 IP는 북한의 IP이며, 해당 대역은 175.45.176.0~179.255임을 확인할 수 있다. 상세지역은 'Ryugyong-dong, Potong-gang District'임을 알 수 있다.

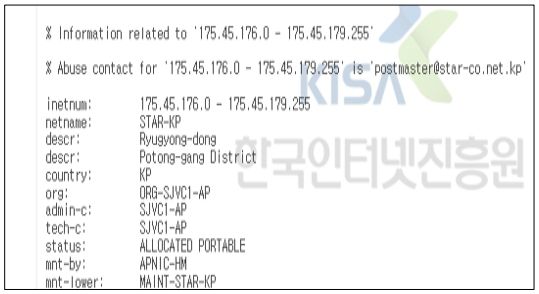

Fig. 5. WHOIS search page for IP ranges

4.5.3 보안장비 차단 등록 사례

4.5.3.1 방화벽을 이용한 차단 등록 사례

방화벽을 이용한 차단은 2가지 방법으로 구현할 수 있을 것이다. 차단 IP 또는 IP 대역을 수동을 등록하는 방법과 한국인터넷진흥원의 인터넷정보센터의

국가별 IP 대역을 CSV 파일로 다운로드 받아서 방화벽 장비에 일괄적으로 등록하는 방법이다. 방화벽과 같은 보안장비에 악성 IP를 등록하는 활동은 악성 IP 1개당 약 3분 정도의 시간이 소요되는 것으로 나타났다. 안랩 방화벽 장비의 차단 사례를 이용하여 수동 등록방법과 일괄 등록방법을 아래와 같이 설명하고자 한다.

4.5.3.1.1 차단 IP 수동 등록 사례

첫째, '추가' 표시를 눌러서 '방화벽 정책 그룹명'을 생성한다.

둘째, 생성된 그룹명에 차단할 국가의 IP 또는 IP 대역을 그림 6과 같이 입력하여 등록한다.

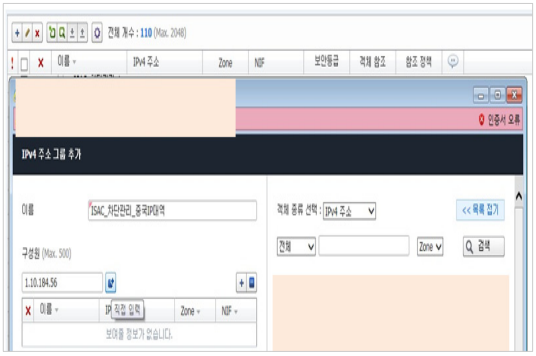

Fig. 6. Bad IP enrollment

셋째, 입력을 완료한 후 해당 그룹명을 선택하여 정책을 적용하고 그림 7과 같이 동기화를 실행한다.

Fig. 7. Enrollment synchronization

넷째, 적용이 완료된 경우 아래의 그림 8과 같이 악성 IP 대역이 차단 정책으로 등록된다.

4.5.3.1.2 차단 IP 일괄 등록 사례

첫째, 그림 9와 같이 '파일 가져오기'를 눌러서 '국가별 IP 대역 CSV파일'을 선택하여 불러온다.

둘째, '저장'버튼을 눌러서 CSV 파일을 방화벽 차단 정책으로 저장한다.

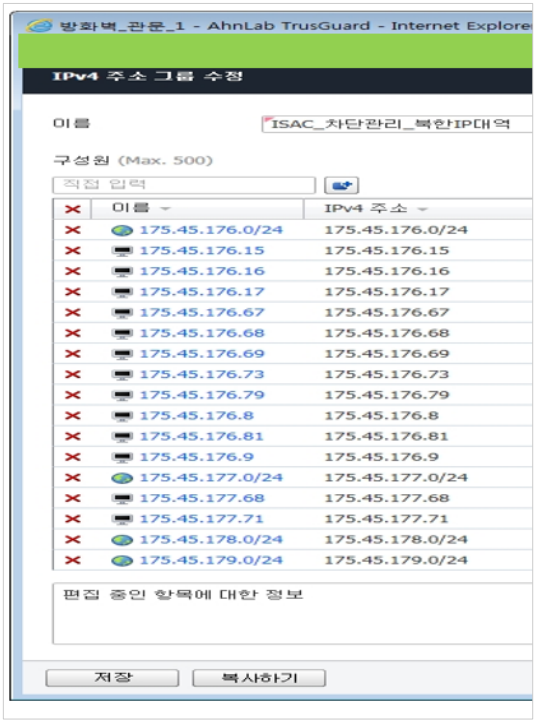

Fig. 8. Enrollment completion page

이때, CSV파일의 형식을 방화벽에서 인식할 수 있도록 맞추어 주는 것이 필요하다. 표 15의 Group Name, Group DESC, Inclusion, Name, Type, ADDR, NIF, Security, DESC 항목들을 맞춰 주어야 일괄 등록이 가능하다.

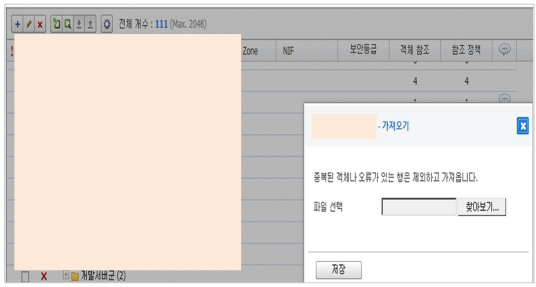

Fig. 9. CSV file upload example

4.5.4 실무부서 확인 활동

사이버 위협 차단 대응활동 과정 중에는 실무부서에 확인하는 활동들이 포함된다. 예를 들어 취약점을 내포한 SW가 설치되었는지, 사이버 공격으로 인해

Table 15. CSV file format descriptions

	Item	Description
1	Group Name	Name of Group
2	Group DESC	Description of Group
3	Inclusion	Direction of Inclusion
4	Name	Name of IP
5	Type	Range or Host
6	ADDR	Real IP Address or Range
7	NIF	Abbreviation of Network Interface

SW설정 상태가 변조되었는지 여부 등을 확인하는 활동들이 이루어진다. 실무부서 확인 활동은 악성 IP 1개당으로 이루어지지 않는 활동으로 업무량으로 측정하기 어렵다.

4.5.5 해외 IP 대역 차단시 보안관제 개선 효과

위에서 살펴본 악성 IP 차단 활동들에 소요되는 업무량들을 계산해 볼 수 있다. 차단할 네트워크가 1개일 경우 악성 IP 1개를 차단하기 위해 소요되는 시간들은 총 9분이다. 차단할 네트워크가 2개일 경우에는 보안장비가 추가되므로 12분, 3개일 경우 15분이 소요된다. 조사기관의 경우 차단해야 할 네트워크는 2개이며 1일당 평균 20개 내외의 해외 악성 IP를 차단하고 있으므로 240분, 4시간의 업무량이 발생하는 것을 알 수 있다. 분석 대상기관의 경우 해외 악성 IP 전체를 차단할 경우 약 4시간의 업무량 감소 효과를 볼 수 있을 것으로 판단된다. 만약 중국 IP만 차단할 경우 약 50% 내외의 업무량 감소를 볼 것으로 추정할 경우 약 2시간의 업무량 감소를 예상할 수 있다. 정보시스템별로 차단할 경우에도 5% 내외정도의 업무량 감소 효과가 나타날 것으로 예상된다.

```
V1= additional attacks checking=3 Min
V2= WhOIS IP checking = 3 Min
V3= enrollment per 1 network = 3 Min
if network=1 & IP = 1,
N(1,1)= activities time for IP blocking
   = V1 + V2 + V3 = 9Min
if network=2 & IP = 1,
N(2,1)=activities time for IP blocking
   = V1 + V2 + V3×2 = 12Min
if network=n & IP = 1,
N(n,1)=activities time for IP blocking
   = V1 + V2 + V3×n
if network=n & IP = m,
N(n,m)=activities time for IP blocking
   = (V1 + V2 + V3×n)×m
```

4.6 해외 IP 대역 차단시 영향

국내에 기반을 둔 기반시설의 특성상 해외 IP 차단으로 관련 고객들의 업무불편이나 영향은 없을 것으로 예상된다. 국외로 출장을 가는 경우와 해외의 정상적인 접속 희망자들의 경우 부득이하게 인터넷 접속에 제한을 받게 될 것으로 예상되나 사전에 접속 희망자 정보, IP 정보, 목적, 기간 등을 사전에 제출받아 허용한다면 크게 문제될 부분은 없을 것으로 판단된다. 또한, 국가 중요시설에 대한 해외 IP 대역으로부터의 접속 차단은 해외 공격자들로부터 국가 중요시설이 탐지되지 않도록 하는 효과가 있어 공격자들의 공격 시도를 감소시키는데 중요한 역할을 할 것으로 보인다.

4.7 해외 정상 사용자 서비스 방안

해외 정상 사용자가 기반시설의 웹페이지에 접근하고자 할 때 미국 ERCOT의 사례와 같이 안내 전화번호를 별도 페이지에 띄워주는 방안을 강구할 수 있다. 안내 페이지의 역할은 정상 사용을 희망하는 사용자에게 추가적인 연락을 취할 수 있게 하는 목적과 악의적인 공격자에게는 공격의지를 철회하도록 만드는 것이다.

안내페이지에 소개된 전화번호로 전화 연락하여 자신의 이메일 주소를 안내센터에 알려준다. 안내센터에서는 정상사용자의 이메일 주소로 접속 허용 신청을 위한 신청서를 보내주고 정상사용자는 신청서의 내용에 따라 회신 한다.

이메일 신청서에는 기반시설의 웹페이지에 대한 ① 접속 목적, ② 고정 IP, ③ 연락처 3가지를 회신하도록 한다. 이메일 회신 내용은 보안부서의 관리하에 검토되고 접속을 허용하게 된다. 이러한 최소한의 사전확인 과정을 통해 기반시설에 대한 악의적인 공격의지를 감소시킬 수 있을 것으로 판단된다.

이메일 신청 접수시 사이버 공격 위협을 차단하기 위해 고성능 악성 이메일 탐지솔루션을 함께 활용하는 것이 필요할 것으로 보인다. 또한 이메일 신청시 첨부파일을 첨부해서 신청하는 것은 차단되도록 구현

Table 16. Example of ERCOT's process

	ERCOT's blocking process
blocking reason	ERCOT's standard operating procedure is to deny access to ERCOT resources if there is no valid business reason for such access.
how to un-block	If you believe you have a valid reason for accessing ERCOT reasources, please answer the questions below to help us in our consideration reguarding the granting of access. Once this form is completed, please return it to helpdesk@ercot.com. ERCOT will contact you when a final determination is made. 〔5 questions〕 1. What is your reason for accessing ERCOT resources? 2. Is your company/organization a current ERCOT Market Pacticipant? Is your company/organization affiliated with a current ERCOT Market Participant? 3. What is your physical address? 4. What is your IP from where you will access ERCOT resources? 5. What is your contact information?

하는 방법도 검토할 수 있을 것이다. 아래의 표 16에서는 미국 텍사스주의 전력시장 및 계통운영기관인 ERCOT의 이메일 접속신청 절차를 정리하였다.

4.8 정보시스템 단위 해외 IP 대역 차단 사례

분석 대상기관의 A정보시스템에 대해 '18.12월 해외 IP대역의 접근을 방화벽에서 차단하였다. 차단 이전까지 1일 최소 700~ 최대 2300여개의 사이버 공격시도가 발생하여 이중 1일 평균 2건 이상의 악성 IP를 차단하였다. 그러나, '18.12월 해외 IP대역차단 이후 사이버 위협 탐지 및 차단 건수가 Zero가 되었다.

V. 결 론

인터넷 네트워크를 통해 외부에 서비스 되고 있는 우리나라 기반시설에 대한 해외로부터의 사이버 위협은 말 그대로 사이버 전쟁이라고 할 만큼 24시간 365일 지속되고 증가하고 있다. 2018년 기준 전체 사이버 위협의 96%가 해외로부터 유입되고 있는 상황에서 해외 IP 대역의 접속 허용에 대한 근본적인 재검토가 반드시 필요한 시점이다. 기존에 각 기관에서 수행하고 있는 일반적인 악성 IP 차단방식은 개별적인 IP단위의 차단인 반면, 본 논문에서 제안하는 방식은 국내와 국외를 구분하여 국외 전체 IP대역 또는 주요국가의 IP대역을 차단한다는 점이 다르다. 현재 인터넷으로 웹서비스(HTTP, HTTPS)를 제공하는 정보시스템들은 국내와 국외를 구분하지 않고 모두 웹서비스에 대한 접근이 허용되어 있는 상황이다. 표 13에서와 같이 인가된 사용자를 기반으로 한 웹서비스 정보시스템에서도 국내와 국외로부터 접근이 가능한 상황이다.

본 논문에서 제안하는 기반시설의 외부 인터넷 연계 정보시스템들에 대한 해외 IP 대역 차단은 네트워크 단위와 정보시스템 단위로 설정할 수 있다. 기반시설의 운용목적이 국가와 국민이므로 네트워크 단위별로 차단하는 것이 좋을 것이다. 다만, 네트워크 단위별 해외 IP 대역 차단시의 영향도에 대한 판단이 어렵다면 정보시스템 단위별로 해외와의 연관성과 차단의 복잡도를 정성적으로 판단하여 단계별로 차단하는 것이 필요할 것이다.

해외의 주요 위협국 또는 전체 해외 IP 대역에 대한 차단을 통해 기반시설 정보시스템의 IP가 해외에서 안보이게 됨으로써 악의적인 사이버 위협을 근본적으로 감소시킬 수 있을 것이다. 더불어 악성 해외 IP를 정보보안 설비에 지속적으로 등록하는 과정에서의 불필요한 자원 낭비를 줄일 수 있을 것이다.

기반시설의 외부 인터넷 연계 정보시스템들에 대한 해외 IP 대역 차단을 통해 불필요한 보안관제 업무부담을 줄여 주어야 한다. 악성 IP 차단을 하는 과정에서 Whois 검색과정, 보안장비 등록 과정 등을 줄이게 될 것이다. 또한 정보시스템에 악영향을 주었는지 여부를 확인하기 위해 실무부서에 확인하는 보안관제 업무활동들도 대폭 줄어들 것으로 생각된다. 만약 중국 IP 대역만을 차단할 경우에는 보안관제 악성 IP 차단 관련 업무량의 50% 정도가 감소하고, 해외 IP 대역 전체를 차단할 경우에는 95% 내외가 감소할 것으로 추정된다.

References

〔1〕 Dennis H. McCallam and Preston D. Frazier, "Ubiquitous Connectivity and Threats: Architecting The Next Generation Cyber Security Operation," The 7th Annual IEEE International Conference, pp. 1506~ 1509, Aug. 2017.

〔2〕 Geet Parekh, David DeLatte, Geoffrey L. Herman, "Identifying Core Concepts

of Cybersecurity: Results of Two Delphi Processes," IEEE Transactions on Education, vol. 61, no. 1, pp. 11~20, Feb. 2018.
〔3〕 Giyoung Kim, "Threats quantification technics for pre-detection about cyber threats," Journal of The Korea Institute of Information Security & Cryptology, 22(8), pp. 15~20, Dec. 2012.
〔4〕 SeolHwa Lim, "APT present condition and malignant code countermeasures," Journal of The Korea Institute of Information Security & Cryptology, 24(2), pp. 63~70, April. 2014.
〔5〕 YongWoo Lee, "A Study on the Critical Information Security Threat and Measures to Protect," Master's Thesis, Department of Management & Industry Graduate School of Hannam University, pp. 51~59, Aug. 2011.
〔6〕 DongHoon Song, "Cyber security threats assessment with atomic power infrastructures' cyber invasion cases studies," Journal of The Korea Institute of Information Security & Cryptology, 28(2), pp. 51~59, Apr. 2018.
〔7〕 Imsup Lee, "A study for Electric IT's Security Improvement measures," Master's Thesis, Department of Information Security Engineering Graduate School of Goryo University, pp. 50~75, Jun. 2012.
〔8〕 ChaWon Joo, "A study about Risk analysis and countermeasures with Public Agencies' cyber invasion types," Master's Thesis, Department of Information Security Engineering Graduate School of Goryo University, pp. 38~60, Jun. 2013.
〔9〕 Hoogy Lee, "A Study on Estimation of Malicious IP Storage Cycle in Security Monitoring Base," Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology Vol.7, No.7, pp. 953-962, July. 2017.
〔10〕 GyoungSoo Shin, "A Study on Cyber Threats from North Korea and Countermeasures," Doctor's Thesis, Department of Political Science and Diplomacy Graduate School of ChungNam University, pp. 103-239, Feb. 2018.
〔11〕 HaeGwon Choi, "Study on trend of DDoS threats and prevention for the network service security risk," Master's Thesis, Department of Technology & Industry Graduate School of Jeonbuk University, pp. 3-10, Feb. 2008.
〔12〕 Patrick P. Tsang, "Anonymous IP-address Blocking in Tor with Trusted Computing," Dartmouth College of USA, pp. 1-7, 2006.
〔13〕 Chris Wilcox, "Correlating Spam Activity with IP Address Characteristics," Colorado State University of USA, pp. 1-6, 2010
〔14〕 Ferry Astika Saputra, "Detecting and Blocking Onion Router Traffic Using Deep Packet Inspection," International Electronics Symposium(IES), pp. 283-288, June. 2016.
〔15〕 P. Ferguson, D. Senie, "Network ingress filtering: defeating denial of service attacks which employ ip source address spoofing(BCP 38)," May. 2000. http://tools.ietf.org/html/rfc2827
〔16〕 Vijayalakshmi Murugesan, "HPSIPT: A high-precision single-packet IP traceback scheme," Elsevier journal of Computer Networks, 143, pp. 275-288, July. 2018.
〔17〕 Clay Johnson III, "Executive Office of the President _ implementation of Trusted Internet Connections_ m08-05," Executive office of the President, pp. 1, Nov. 2007.

[18] Federal Network Resilience, "Trusted Internet Connections reference Architecture Document version 2.0_ TIC_Ref_Arch_v2.2_2017," Homeland Security, pp. 1-75, June. 2017.

〈저자소개〉

한 충 희 (Choong-Hee Han) 정회원
1996년: 동국대학교 컴퓨터공학(학사)
2002년: 동국대학교 정보보호학과(이학석사)
2002년 3월~현재: 한국전력거래소 정보보안팀 차장
2017년 3월~현재: 전남대학교 대학원 정보보안협동과정 박사과정
〈관심분야〉 보안관제, 침해대응, 주요정보통신기반시설 보호대책, 개인정보보호 등

박 순 태 (Soon-Tai Park) 정회원
1992년: 단국대학교 전자계산학과 학사
1998년 8월: 국민대학교 정보과학대학원 정보통신학과 석사
2010년 8월: 전남대학교 대학원 정보보안협동과정 박사
1994년 7월~1999년 9월: 육군 전산장교
2000년 4월~현재: 한국인터넷진흥원 보안위협대응R&D팀장
〈관심분야〉 정보보호, 보증, IT보안성 평가, 정보보호 인력 양성, 정보통신 기반보호, 정보보호 R&D

이 상 준 (Sang-Joon Lee) 정회원
1991년: 전남대학교 전산통계학과(이학사)
1993년: 전남대학교 전산통계학과(이학석사)
1999년: 전남대학교 전산통계학과(이학박사)
2007년~현재: 전남대학교 경영학부 교수
〈관심분야〉 경영정보시스템, 전자상거래, 정보보호 등