https://doi.org/10.5392/JKCA.2021.21.02.499

신규 취약점 공격에 대한 효율적인 방어 메커니즘

Effective Defense Mechanism Against New Vulnerability Attacks

곽영옥, 조인준
배재대학교대학원 사이버보안과

Young-Ok Kwak(kwak0522@nate.com), In-June Jo(injune@pcu.ac.kr)

요약

해커들의 사이버 공격기법은 전에 볼 수 없었던 형태의 공격으로 점점 더 정교해지고 다양화 되고 있다. 정보 보안 취약점 표준 코드(CVE)측면에서 살펴보면 2015년에서 2020년에 약 9 만 건의 신규 코드가 등록되었다[1]. 이는 보안 위협이 빠르게 증가하고 있음을 나타내고 있다. 신규 보안 취약점이 발생하면 이에 대한 대응 방안 마련을 통해 피해를 최소화해야 하지만, 기업의 경우 한정된 보안 IT예산으로 보안관리 수준과 대응 체계를 감당하기에는 역 부족인 경우가 많다. 그 이유는 수동 분석을 통해 분석가가 취약점을 발견하고 보안장비를 통한 대응 방안 마련 및 보안 취약점 패치 까지 약 한 달의 시간이 소요되기 때문이다. 공공분야의 경우에는 국가사이버안전센터에서는 보안운영정책을 일괄적으로 배포하고 관리하고 있다. 하지만, 제조사의 특성에 따라 보안규칙을 수용하는 것이 쉽지 않으며, 구간 별 트래픽 검증작업까지 약 3주 이상의 시간이 소요된다. 그 외 비 정상적인 트래픽 유입이 발생하면 취약점 분석을 통한 침해행위 공격 검출 및 탐지와 같은 대응방안을 마련해야 하나, 전문적인 보안전문가 부재로 인하여 대응의 한계가 존재한다. 본 논문에서는 신규 보안 취약점 공격에 효과적인 대응 방안 마련을 위해 보안규칙정보 공유사이트 “snort.org”를 활용하는 방안을 제안하였다.

■ 중심어 : | 사이버 공격 | CVE | 취약점 분석 | 보안규칙 |

Abstract

Hackers' cyber attack techniques are becoming more sophisticated and diversified, with a form of attack that has never been seen before. In terms of information security vulnerability standard code (CVE), about 90,000 new codes were registered from 2015 to 2020. This indicates that security threats are increasing rapidly. When new security vulnerabilities occur, damage should be minimized by preparing countermeasures for them, but in many cases, companies are insufficient to cover the security management level and response system with a limited security IT budget. The reason is that it takes about a month for analysts to discover vulnerabilities through manual analysis, prepare countermeasures through security equipment, and patch security vulnerabilities. In the case of the public sector, the National Cyber Safety Center distributes and manages security operation policies in a batch. However, it is not easy to accept the security policy according to the characteristics of the manufacturer, and it takes about 3 weeks or more to verify the traffic for each section. In addition, when abnormal traffic inflow occurs, countermeasures such as detection and detection of infringement attacks through vulnerability analysis must be prepared, but there are limitations in response due to the absence of specialized security experts. In this paper, we proposed a method of using the security policy information sharing site “snort.org” to prepare effective countermeasures against new security vulnerability attacks.

■ keyword : | Cyber Attack | CVE | Vulnerability Analysis | Security Rules |

접수일자 : 2020년 11월 18일
수정일자 : 2020년 12월 11일
심사완료일 : 2020년 12월 11일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

우리 사회는 컴퓨터와 정보통신기술의 발전으로 민간·공공 전 분야에서 사이버 의존도가 높아졌다. 또한 초고속·초저지연·초연결성을 지닌 5G 이동통신이 상용화되고 이를 기반으로 한 새로운 서비스가 등장하면서 사이버보안은 더욱 중요해지고 있다[2].

이런 다양한 ICT 환경에서 이루어지는 사이버 공격에 대응하기 위해서 기업, 주요 공공단체 및 민간기관에서 많은 노력을 하고 있다. 즉 알려지지 않은 악성코드를 탐지하거나, 사전에 위협을 인지·대응하기 위해서 APT대응솔루션 도입하고, 지능형 지속 위협을 빠르게 인지하고 탐지 및 대응하기 위해 보안장비(IPS·IDS·WAF)을 도입하여 다양화되고 있는 보안위협을 관리·운영 하고 있다[3].

하지만, IT 예산·전문 인력 부족 문제 및 [그림 1]공공기관에서는 침입방지시스템을 통한 실시간 대응을 진행하고 있다[4]. 하지만 보안장비 제조사 상이, 서비스 별 트래픽이 상이하여 보안장비 검증 없이 사용하기란 쉽지가 않은 설정이다.

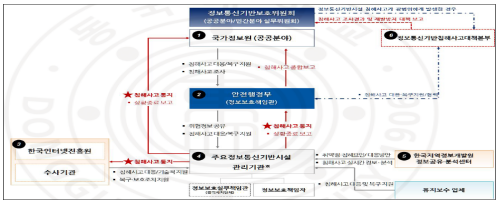


그림 1. 국가 사이버 안전관리체계

본 논문에서는 신규 취약점 공격에 대해 효과적인 대응을 위하여 보안규칙 정보 제공 사이트를 활용하는 방안을 제안하였다. 또한 보안규칙 등록 시 발생되는 문제점 개선을 통하여 신속한 대응이 가능하도록 문제점에 대한 개선안을 마련하였다.

본 논문의 구성은 제3장에서 검증시스템 구성, 제4장에서 보안장비 등록 시 발생되는 문제점 개선, 제5장에서 본 연구의 결과를 정리하고 향후 보안 분야에 추가적으로 연구가 필요한 부분을 기술하였다.

II. 관련 연구

1. 중복되거나 유사한 Snort 탐지규칙

공격이 다양해지고 복잡해짐에 따라 Snort의 탐지규칙을 생성하고 등록하는 일이 많아지고 있다. 하지만 탐지규칙이 유사하거나 중복된 사용으로 효과적인 관리가 힘들다고 연구되었다[5][6]. 다음 [표 1]는 탐지문자열은 동일하나 pcre 옵션 상이하다. 따라서 pcre 옵션 부분을 한 번에 처리하도록 수정한다면 snort 성능을 향상 시킬 수 있다.

표 1. 중복 보안규칙 최적화

구 분	보안규칙
탐지규칙 1	pcre:"/(((DestFile|encryptPass)\x3D[^\x26]{50})|((BaseDN|SearchFilter)\x3D[^\x26]{128}))/Ui"
탐지규칙 2	pcre:"/(((DestFile|encryptPass)\x3D[^\x26]{50})|((BaseDN|SearchFilter)\x3D[^\x26]{128}))/Pi"
통합규칙	pcre:"/(((DestFile|encryptPass)\x3D[^\x26]{50})|((BaseDN|SearchFilter)\x3D[^\x26]{128}))/(Ui|Pi)"

2. 국가기관 운영현황 문제점

국정원, 국자정보자원관리원, 지역정보개발원을 주축으로 사이버 침해대응에 대한 보안운영정책을 일괄적으로 배포를 진행하는 것이 가장 큰 효율적이면서 문제점이라고 볼 수 있다. 첫 번째, 상위기관에서 미 탐지시, 공공기관 이하 기관의 대응능력의 한계가 발생할 것이다. 두 번째, 정보보호대상에서 사용자군 과 정보보호시스템의 구분 없이 정책배포로 인해 보안장비의 물리적 과부하 발생과 비효율적인 운영으로 인해 문제가 발생할 수 있다[7].

III. 보안규칙 검증시스템 구성

1. Snort Rule(snort.org) 정책 현황

snort는 오픈 소스로 패킷 캡처 라이브러리인을 사용하여 패킷을 캡처하고, 수집된 패킷이 사전에 정의된 snort 공격룰과 비교하여 매칭 되었을 경우 syslog를

통해 로그를 남기거나 특정 디렉터리 특정 파일 또는 database에 남기도록 한다. 또한 최신의 공격 시도를 탐지할 수 있도록 snort 홈페이지 통해 rule을 지속적으로 지원받을 수 있다[8].

snort.org 제공 중인 규칙은 전체 51,376개이다[9]. [표 2]는 공격유형별 보안규칙을 구분하였으며, 해당 보안규칙에 대하여 보안장비를 검증하였다.

표 2. snort.org rule 사용 현황

구 분	개수	구 분	개수
attempted-user	4,991	successful-recon-limited	48
trojan-activity	4,858	denial-of-service	40
misc-activity	1,209	bad-unknown	4
attempted-admin	908	successful-user	4
web-application-attack	222	shellcode-detect	3
attempted-recon	158	default-login-attempt	2
attempted-dos	122	suspicious-filename-detect	2
misc-attack	67	network-scan	1
policy-violation	66	not-suspicious	1
protocol-command-decode	56	string-detect	1

2. 보안규칙 검증 절차

보안장비 등록 시 발생되는 문제점에 대한 원인분석 및 개선점 마련하였다. 또한 보안장비 운영자 보안규칙 등록 시 휴먼장애를 통한 장애발생을 고려하여 [표 3] 체크리스트 항목을 통해 모니터링을 진행하였다. K기관에서는 보안장비 등록 시 2인 1조 편성을 통한 크로스 체크 방식으로 운영되고 있다.

표 3. 모니터링 체크 리스트

등록 전	등록 후
보안장비 등록 개수	시스템 모니터링
보안규칙 문법 검사	대량이벤트 발생
보안규칙 정상 등록 여부	보안장비 정상 탐지 여부

3. 검증 시스템 구성

보안규칙 정보 제공 사이트 “snort.org” 통해 받은 보안규칙을 검증 없이 등록 시 장비부하 및 서비스 장애 발생 한다. 그리하여 기존 서비스 구성 환경에 신규 정책검증시스템(TAS 2000NG)을 TAB 장비를 이용하여 패킷을 전달받아 탐지하는 방식으로 진행하였다. 다수 보안장비 중 정보보호기술 선정한 이유는 첫 번째, 보안규칙 등록 시 문법 검사 가능하다. 두 번째, 보안규칙 미 등록 시 에러 메시지를 통한 미 등록 사유에 대한 정보를 제공해준다. 세 번째, 보안장비를 통한 장비 성능 모니터링이 가능한 장점이 존재하여 선정하게 되었다.

snort.org에서 사용 중인 보안규칙 12,763개에 대해 [그림 2] 정책검증시스템을 통해 발생되는 문제점을 통한 개선점을 마련하였다.

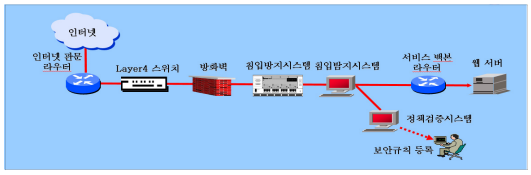


그림 2. 정책검증시스템 구성도

Ⅳ. 보안규칙 검증을 통한 규칙 개선 제안

1. 탐지문자열 길이 제한 설정

보안규칙 등록 시 에러 메시지는 발생되지 않았으나, 미 탐지되는 문제가 확인되었다. 그 이유는 탐지문자 4Byte이하 시 처리되지 않도록 설계되었기 때문이다. 이와 관련된 보안규칙은 252개이다.

앞서 확인된 문제점에 대한 개선안을 마련하였다. 첫 번째, [표 4]와 같이 탐지문자 길이 제한 설정을 변경하였다. 하지만 오탐 및 장비 부하로 인한 패킷누수현상이 발생되어 기본 값으로 변경하였다.

표 4. sig_length_min.cfg 설정파일

기존	변경
sig_length_min 4	sig_length_min 1

두 번째, [그림 3]와 같이 보안규칙 취약점 정보를 바탕으로 탐지문자 확대 하였다. 아래 [표 3] 제로엑세스 보안규칙 이며, 보안규칙 정보 제공 사이트(doc.emerg

ingthreats.net)정보를 통해 취약점 코드 정보 확인이 가능하다.

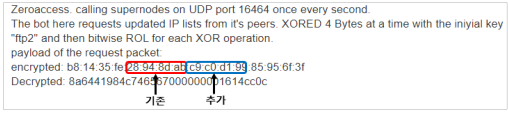


그림 3. 취약점 상세 정보

다음 [표 5]는 앞서 확인된 정보를 통해 정규화 하였으며, 보안장비에게 정상적으로 탐지되었다.

표 5. 탐지문자열 4Byte 보안규칙

보안 규칙명	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
보안 규칙 (기존)	alert udp $EXTERNAL_NET any -> $HOME_NET [16464,16465,16470,16471] (flow:to_server; dsize:16; content:"|28 94 8D AB|"; depth:4; offset:4; metadata:impact_flag red, policy balanced-ips drop, policy connectivity-ips drop, policy security-ips drop, ruleset community; reference:url,www.virustotal.com/file/50cdd9f6c5629630c8d8a3a4fe7d929d3c6463b2f9407d9a90703047e7db7ff9/analysis/;sid:31136; rev:2;)
보안 규칙 (개선)	alert udp $EXTERNAL_NET any -> $HOME_NET [16464,16465,16470,16471] (flow:to_server; dsize:16; content:"|28 94 8D AB C9 C0 D1 99|"; depth:4; offset:4; metadata:impact_flag red, policy balanced-ips drop, policy connectivity-ips drop, policy security-ips drop, ruleset community; reference:url,www.virustotal.com/file/50cdd9f6c5629630c8d8a3a4fe7d929d3c6463b2f9407d9a90703047e7db7ff9/analysis/; sid:31136; rev:2;)

[그림 4]에서 보듯이 앞선 확인된 보안규칙명 및 취약점 참고 배포 정보를 통하여 보안규칙 158개 정규화 가능하다. 하지만, 그 외 124개는 취약점에 대한 정보 미 존재하여 정규화 불가하였다.

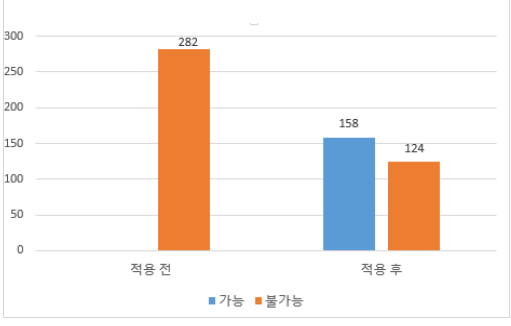


그림4. 탐지문자열 길이제한 보안규칙 검증

2. 데이터 재조합 기능 비활성화 설정

보안규칙 등록 시 에러 메시지는 미 발생되었으나 미 탐지되는 문제가 확인되었다. 그 이유는 데이터 재조합 기능 비활성화 문제가 확인되었다. 앞서 확인된 보안규칙 탐지 문자 범위는 2,070Byte(최초 탐지문자(20Byte)+탐지범위(2,050Byte))이며, 이와 관련된 보안규칙은 2개이다.

데이터 전송 시 최대 1,500Byte 이하 패킷 단위로 분할하여, 순차번호를 순서대로 조합한다. 아래[표 6] 보안규칙은 “특수하게 제작된 악성 웹페이지를 방문 시 원격 코드 실행 취약점”이다[10].

앞서 확인된 문제점 개선을 위해 첫 번째, [표 6] 보안규칙 탐지문자 검사 범위를 축소하였다.

표 6. 보안규칙 검사 범위 최적화

기존	변경
탐지문자(20Byte)+탐지범위(2,050Byte) = 2,070Byte	탐지문자(20Byte)+탐지범위(180Byte) = 200Byte

또한 중복 문자 삭제, 짧은 문자 “=” 삭제 하였다. 하지만 javascript에서 사용되는 문자로 인해 보안장비 검사하는 양이 증가하여 패킷 처리 성능 부하 문제가 확인되었다. 보안규칙 “fast_pattern” 옵션 및 페이로드 검사 범위 옵션 “dsize”을 사용하여 탐지패턴 간 매칭 감소를 통한 성능 부하를 줄였다. 보안장비시스템 모니터링 결과를 [표 7]로 정리하였다.

표 7. 보안장비 시스템 모니터링

구분	패킷 손실률	CPU	MEM	DISK
적용 전	0.00%	67%	60%	15%
검사범위축소	0.76%	78%	60%	15%
보안규칙 최적화	0.00%	67%	60%	15%

다음 [표 8]은 보안규칙 정규화를 진행된 결과이며, 공격 유입 시 정상적으로 탐지된 것을 확인하였다.

표 8. 데이터 탐지 문자 범위 축소

보안 규칙명	BROWSER-IE Microsoft Internet Explorer CStr internal string use-after-free attempt	SID	39826, 39827
보안 규칙 (기존)	alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (flow:to_server,established; file_data; content:"window.location.href"; nocase; content:"="; within:10; content:"window.location.href"; within:40; nocase; content:"<script"; distance:0; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service smtp; sid:39827; rev:4;)		
보안 규칙 (개선)	alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (content:"window.location.href"; nocase; fast_pattern:only; content:"<scriptr"; distance:0; nocase; content:"src"; within:40; nocase; content:"<script"; within:100; nocase; content:"src"; within:40; nocase;metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service smtp; sid:39827; rev:4;)		

[그림 5]는 앞에서 확인된 보안규칙 탐지 범위 축소 및 정규화를 통해 보안규칙 사용이 가능하였다.

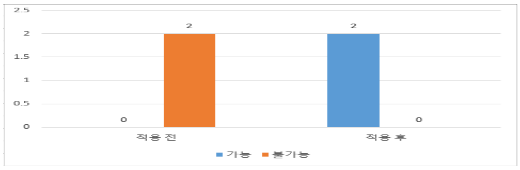


그림 5. 데이터 탐지 문자 범위 축소 검증

3. 중복 보안규칙명 사용 제한 설정

보안장비에 보안규칙명 중복 등록 시 "사용자 정의 패턴 이름이 중복 되었습니다" 에러 메시지가 발생되었다. 그 이유는 보안규칙명 중복 사용 제한 설정문제이며 이와 관련된 보안규칙은 9,432개이다.

[표 9]는 보안규칙명 중복 사용 TOP 10 이다.

표 9. 중복 보안규칙명 사용 현황 TOP 10

보안규칙명	개수
BROWSER-IE Microsoft Edge memory corruption attempt	80
FILE-FLASH Adobe Flash Player ByteArray uncompress domainMemory use after free attempt	46
MALWARE-BACKDOOR JSP webshell backdoor detected	39
BROWSER-IE Microsoft Edge scripting engine memory corruption attempt	36
MALWARE-OTHER Win.Exploit.Hacktool suspicious file download	34
FILE-IDENTIFY MOV file magic detected	28
BROWSER-IE Microsoft Internet Explorer memory corruption attempt	28
FILE-JAVA Oracle Java privileged protection domain exploitation attempt	26
BROWSER-IE Microsoft Internet Explorer use after free attempt	26
FILE-FLASH Adobe Flash copyPixelsToByteArray integer overflow attempt	26

또한 snort 일반 옵션 등록 시 "유효하지 않은 옵션 이름이거나 옵션이름 다음에 ":"이 누락되었다.(metadata)" 에러 메시지가 확인되었다. 그 이유는 보안장비 미 제공 옵션으로 확인되었다. 이와 관련된 보안규칙은 11,265개이다.

아래 [표 10]는 일반옵션 정보를 통해 20년 WebLogic 역 직렬화 취약점으로, 악의적으로 제작된 직렬화 가젯 체인을 사용하여 인증되지 않은 공격자는 원격코드 실행할 수 있는 취약점이다.

표 10. 일반 옵션(reference) 적용 보안규칙

보안 규칙명	SERVER-ORACLE Oracle Weblogic T3 remote code execution attempt	SID	54008
보안 규칙	alert tcp $EXTERNAL_NET any -> $HOME_NET 7001 (flow:to_server,established; content:"java.util.PriorityQueue.readObject"; fast_pattern:only; content:"java.util.PriorityQueue.heapify"; content:"java.util.PriorityQueue.siftDown"; distance:0; content:"java.util.PriorityQueue.siftDownUsingComparator"; distance:0; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service java_rmi; reference:cve,2020-2883; reference:url,oracle.com/security-alerts/cpuapr2020.html; classtype:attempted-user; sid:54008; rev:1;)		

아래 [표 11]는 일반옵션이 없는 보안규칙이다. 보안규칙명을 통해 POP 프로토콜 STAT 명령어 실행을 탐지하기 위한 보안규칙이다. 하지만 snort 옵션을 통해 보안규칙 생성일 확인이 불가능하였다. 이와 관련된 보안규칙은 1,498개이다.

표 11. 일반 옵션(reference) 미 사용 보안규칙

보안 규칙명	PROTOCOL-POP STAT command	SID	16594
보안 규칙	alert tcp $HOME_NET any -> $EXTERNAL_NET 110 (flow:to_server, established; content:"STAT"; nocase; flowbits:set,pop3.stat; flowbits:noalert; metadata:policy max-detect-ips alert, service pop3; classtype:protocol-command-decode; sid:16594; rev:10;)		

아래 [표 12]는 앞서 확인된 문제점 개선을 위하여, 보안규칙 명명법을 제한하였다. 일반옵션 미사용 보안규칙에 대한 보안규칙 생성일은 검토일로 지정하였다.

표 12. 보안규칙 명명법 개선안

구분	설명	데이터
기관	개발 기관	알파벳 소문자 및 숫자
유형	classtype(snort 룰 유형)	알파벳 소문자
제목	보안규칙 이름	알파벳 소문자 및 숫자
날짜	보안규칙 생성일	yyyymmdd
번호	보안규칙 일련번호	01 ~ 99

아래 [표 13]는 보안규칙 명명법 개선안을 통하여 보안규칙명을 변경 적용하였다.

표 13. 보안규칙정보 공유 사이트 명명법 개선

rule 파일	SERVER-ORACLE
기존	Oracle Weblogic T3 remote code execution attempt
개선	snort_apu_weblogic remote code_201101_01

이를 통해 관리적인 측면에서 보안규칙 목적성 및 타 업체 간 의사소통의 역할 수행이 가능해졌다. 또한 일관성이 없고 혼란이 발생될 수 있는 문제에 대한 개선이 가능하다 [11].

[그림 6]은 중복 보안규칙명 및 snort 일반 옵션 미지원 문제점 해결에 대해 보안규칙 명명법 표준안 제안을 통해 보안규칙 사용이 가능하였다.

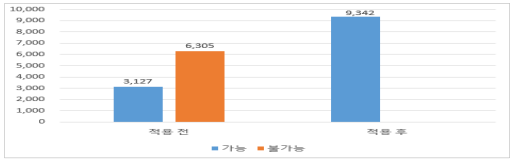


그림 6. 중복 보안규칙명 검증

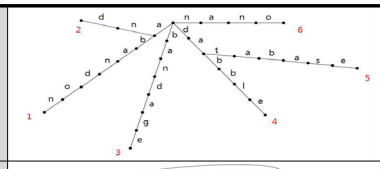
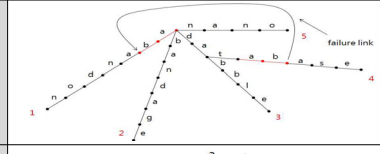
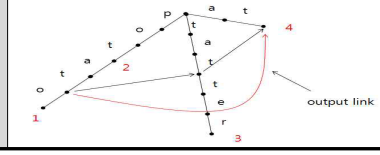
4. 유사 보안규칙 사용 제한

보안장비 유사 보안규칙 등록 시 장비 부하가 발생되었다. 그 이유는 보안장비 다중 패턴 매칭 알고리즘 "Aho-Corasick"을 통해 보안규칙 매칭 횟수가 증가하여 장비 부하가 발생되었다. 이와 관련된 보안규칙은 51개이다.

[표 14]에서 보듯이 전처리 과정을 통하여 키워드 트리를 만들고 "Failure link"와 "Output link"를 가지게 되면 글자와 Keyword Tree의 간선의 글자와 비교하면서 정점으로 내려가게 된다. 비교하면서 내려가면서 "Output link"가 존재하면 패턴이 발생했음을 알려주게 된다. 또한 틀리게 되면 "Failure link"를 따라 가서 글자를 비교해 주면서 탐색을 하게 된다.

이와 같이 텍스트에 대하여 한번 확인하였으면 다시 확인하지 않게 되고 따라서 O(m+n+k)의 시간 복잡도로 처리가 가능하게 된다[12].

표 14. Aho-Corasick 알고리즘

Pattern Set에 대한 Keyword Tree	
Keyword Tree의 한 정점에서 Failure link	
Keyword Tree의 한 정점에서의 Output link	

아래 [표 15]는 보안규칙 6개에 대해 탐지문자열이 동일하다. 하지만 서버와 클라이언트 통신 시 목적지 포트, 흐름정보를 통하여 구분하여 사용하고 있다.

또한 목적지 단일 포트 설정 시 "ANY 포트"에 포함되어진다. 다중 패턴 매칭 알고리즘(Aho-Corasick)을 통한 검사 시 보안장비 부하만 발생되어지게 된다.

표 15. 중복 보안규칙

SID	보안규칙명	보안규칙	비교
50242 50243	FILE-PDF Adobe Acrobat out-of-bounds read attempt	content:"|F6 02 00 86 E3 17 00 0D 39 EE 4B F7 8A 10 D9 91 9A 31 00 00 F0 2E 94 D3 30 A0 D4 75 78 BD 8B 0E D4 BC BF C8 50 01 00 90 35 13 C7 21 CE 19 7A C0|"; fast_pattern:only;	목적지PORT flow:to_client flow:to_server
50244 50245 50250 50251	FILE-PDF Adobe Acrobat out-of-bounds write attempt	content:"|F6 02 00 86 E3 17 00 0D 39 EE 4B F7 8A 10 D9 91 9A 31 00 00 F0 2E 94 D3 30 A0 D4 75 78 BD 8B 0E D4 BC BF C8 50 01 00 90 35 13 C7 21 CE 19 7A C0|"; fast_pattern:only;	목적지PORT flow:to_client flow:to_server

앞서 확인된 문제점 개선을 위하여 서버와 클라이언트에 대해 포트 정보를 통한 개선이 가능하다.

서버 통신 시 잘 알려진 포트(0~1023), 클라이언트 통신 시 등록된 포트(1024~49151), 동적 포트(49152~65535)로 구분한다.

[그림 7]에서 앞서 확인된 문제점 개선을 통하여 포트 제한 및 흐름정보 미 사용 등으로 인해, 전체 51개 중 유지 34개, 삭제 17개 개선이 가능하였다.

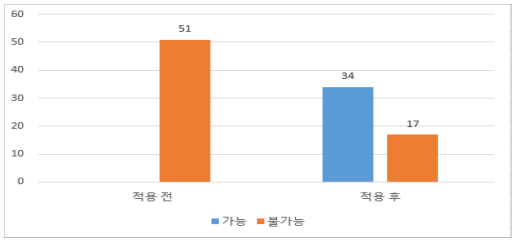


그림 7. 중복 보안규칙 검증

V. 결 론

본 논문에서는 사이버 공격 탐지를 위해 보안규칙 정보 공유 사이트 “snort.org”를 통하여 대응방안을 마련하였다. 또한 보안장비 등록 시 발생되는 문제점 개선을 통해 사이버 공격에 신속히 대응이 될 수 있도록 연구하였다.

첫 번째, 보안장비 성능 부하를 고려하여 탐지문자열 4Byte이하 시 처리되지 않도록 설계, 데이터 분할 전송 시 데이터 재조합 기능 비활성화, 보안장비 유사 보안규칙 존재 시 다중 패턴 매칭 알고리즘을 통해 보안장비 부하가 발생되는 문제점이 확인되었다. 해당 문제점 개선을 위해 보안규칙 정규화 하였다.

두 번째, 보안규칙명 개발 시 보안규칙 생명주기, 가독성과 목적성을 고려하여 개발되어야 한다. 하지만 보안규칙명 중복 사용 및 보안규칙 생성일 미 표기 문제가 확인되었다. 이로 인하여 타 기관·업체와 의사소통 시 보안규칙 관리 실태를 파악할 수 없다.

해당 문제점 개선을 위하여 보안규칙 명명법을 마련하였다.

위의 결과를 근거로 [그림 8]은 보안장비 등록 가능한 보안규칙은 12,622개, 그 외 141개는 장비부하 및 취약점 정보 부족으로 보안규칙 등록이 불가능 하였다. 이를 통하여 보안규칙 개발 시 보안규칙명, 보안규칙, 보안장비 동작방식, snort 옵션의 중요성 등에 대해 확인하였다.

또한 전문 인력 부족으로 신규 취약점 대응 불가 및 공공기관에서 보안규칙 검증 이후 보안정책 배포 지연 시 보안규칙 부재로 인한 위험성이 존재한다. 하지만 보안규칙공유 사이트 실시간 정보 획득을 통한 대응체계방안을 마련할 수 있었다.

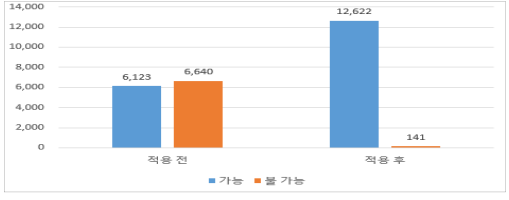


그림 8. 최종 보안장비 등록 현황

향후에는 보안규칙공유 사이트(sonrt.org)에서 제공되지 않는 신규 취약점 발견 시 오픈 소스코드 공유 사이트 깃 허브(GitHub)를 통하여 취약점 코드 분석을 통한 대응방안을 마련하기 위하여 지속적인 연구를 진행할 예정이다.

참 고 문 헌

[1] Common Vulnerabilities and Exposures, http://cve.mitre.org

[2] 한국인터넷진흥원, "2020 정보보호백서_최종"

[3] 강명훈, *빅데이터 분석으로 살펴본 IDS와 보안관제의 완성*, 와우북스, 2013(5).

[4] 안전행정부, *주요정보통신기반시설 사이버위기 대응 매뉴얼 표준안*, 2014.

[5] 박윤곤, 조호성, 박희진, "네트워크 취약점 공격의 효율적인 탐지를 위한 Snort 규칙 분석과 개선," 한국정보과학회 2012 한국컴퓨터종합학술대회, pp.304-306, 2012.

[6] 김웅휘, 권인하, 조호성, 박희진, "Snort Rule Optimizer: 최장공통부분 문자열 알고리즘을 이용하여 Snort 탐지규칙을 효율적으로 최적화하기 위한 도구 개발," 한국정보과학회, 2013 한국컴퓨터종합학술대회, pp.756-758, 2013.

[7] 이재우, 신상우, 침입방지시스템의 국가기관 보안운영 정책 표준화 연구, 동국대학교, 석사학위논문, 2016.

[8] 한국인터넷진흥원, "Snort를 이용한 IDS 구축," 2005.

[9] SNORT Network Intrusion Detection System, http://www.snort.org

[10] 한국인터넷진행원, "MS 8월 보안 위협에 따른 정기 보안 업데이트 권고," 2016.

[11] 박원형, 김양훈, 임영환, 안성진, 보안관제 위협 이벤트 탐지규칙 표준 명명법 연구," 융합보안 논문지, 제15권, 제4호, 2015.

[12] 조종길, 박희진, "네트워크 침입 탐지 시스템을 위한 Aho-Corasick 패턴 매칭 알고리즘 분석 및 멀티 쓰레딩을 활용한 성능 향상," 한국정보과학회 학술발표 논문집, Vol.38, N.2A, pp.345-348, 2011.

저 자 소 개

곽 영 옥(Young-Ok Kwak) 준회원

- 1999년 2월 : 중부대학교 정보통신 S/W과 졸업
- 2017년 11월 ~ 현재 : 이글루시큐리티
- 2019년 3월 ~ 현재 : 배재대학교 사이버보안과(공학석사)

〈관심분야〉 : 침해대응, 인공지능, 보안규칙

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 졸업
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 컴퓨터시스템응용