NISN HPC 서비스 환경에서 2016년 사이버 공격 탐지 데이터 분석

이재국*°, 김성준*, 홍태영*
*한국과학기술정보연구원 슈퍼컴퓨팅인프라실
e-mail:{jklee°, sjkim, tyhong}@kisti.re.kr

An Analysis of the 2016 Cyber Attack Detection Data in NISN HPC Service Environment

Jae-Kook Lee*, Sung-Jun Kim*, Teayoung Hong*
*Dept. of Supercomputing Infrastructure, KISTI

요 약

정보통신기술(ICT)의 발전으로 원격지에서 고속으로 HPC(High Performance Computing) 서비스를 이용할 수 있게 되었지만, HPC 서비스 환경을 대상으로 하는 사이버 공격도 끊이지 않고 발생하고 있다. 본 논문에서는 슈퍼컴퓨터 4호기 서비스 환경에서 탐지/차단된 사이버 공격 증가 추이를 살펴보고, 2016년 사이버 공격 탐지 데이터와 슈퍼컴퓨팅서비스 네트워크 내부로 유입된 트래픽 데이터를 분석하여 급격히 증가한 공격지 IP 주소의 분포 및 특징을 확인한다.

1. 서론

한국과학기술정보연구원 국가슈퍼컴퓨팅연구소(이하 NISN: National Institute of Supercomputing and Networking)에서는 과학기술 분야의 핵심 R&D 인프라인 공공 서비스용 국가슈퍼컴퓨터를 구축하여 서비스하고 있다. 현재 200여개 국내외 연구소, 정부 산하 기관, 대학 및 기업 등에 서비스 중인 슈퍼컴퓨터 4호기는 클러스터형의 TACHYON 2와 대용량메모리형의 신바람 등으로 구성되어 있으며 360TFLOPS의 처리성능을 갖고 있다[1]. NISN은 안전한 슈퍼컴퓨팅 인프라 및 서비스를 제공하기 위하여 시스템 레벨에서의 접근로그와 네트워크 레벨에서의 보안 장비 이벤트를 수집·분석하여 사이버 공격 징후를 탐지하고 차단한다.

본 논문에서는 2016년 NISN의 슈퍼컴퓨터 4호기 HPC 서비스 환경에서 수집한 사이버 공격 데이터와 원격지에서 HPC 서비스 네트워크 내부로 유입된 트래픽 데이터를 분석하여 사이버 공격지 IP 주소 분포를 분석하고 특징을 살펴본다. 슈퍼컴퓨터 4호기 서비스 환경은 HPC 인프라 접속 및 데이터 전송을 위한 로그인 노드(login-nodes)와 DM 노드(datamover-nodes), 사용자의 계정 신청 및 서비스 지원을 위한 웹서버, 계정관리 및 인증서버 등으로 구성되어 있다. 우리는 사이버 공격 탐지 데이터 분석을 통하여 공격의 특징을 이해하고 향후 발생할 수 있는 공격을 대응할 수 있도록 활용하고자 한다.

본 논문의 구성은 다음과 같다. 2절에서는 관련연구로 NISN에서 사이버 공격 이상 징후를 탐지하기 위해 적용한 탐지기법을 서술한다. 그리고 3절에서 NISN에서 수집한 사이버 공격 데이터를 이용하여 공격지 IP 주소의 분포를 살펴보고, 전체 유입 트래픽을 함께 분석하여 특징 및 원인을 확인한다. 끝으로 4절에서는 제언을 하고 결론을 맺는다.

2. 관련연구

NISN은 서버에서 발생한 접근 로그 중 인증 실패 로그를 출발지 IP 주소나 사용자 계정 등 특정 구분자로 군집화(clustering)하여 임계값(Threshold) 이상 실패 로그가 발생하면 공격 이상 징후로 탐지하는 기법[2]을 적용하여 운영 중이다. 또한, 방화벽에 의해 차단된 이벤트를 출발지 IP와 목적지 IP, 포트 정보만을 추출하고 하여 특정 출발지 IP에서 임의시간 내(타임윈도우, Δt_0)에 임계값 이상 차단 이벤트가 발생하는지 확인하여 공격을 탐지하는 기법[3]도 적용하여 사이버 공격을 탐지하고 차단하고 있다. 더불어 안전한 HPC 인프라 및 서비스를 제공하기 위해 보안을 강화하고 있다.

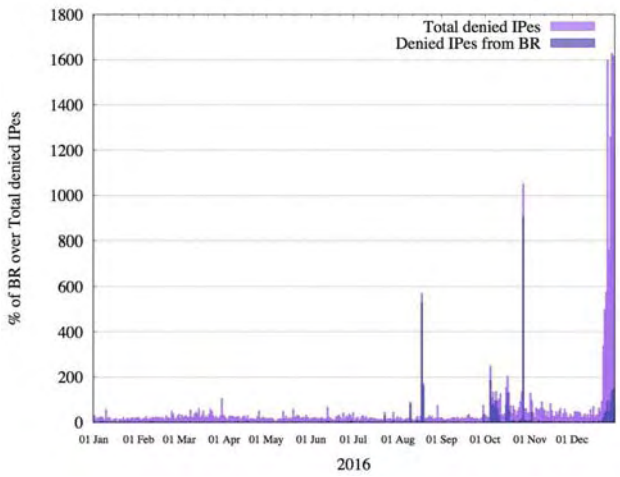
3. 사이버 공격 데이터 분석

본 절에서는 NISN에서 수집한 사이버 공격 탐지/차단 IP 주소 데이터(22,084개)와 HPC 인프라 및 서비스 네트워크로 유입된 전체 패킷 데이터(약 18.25억 개)를 이용하여 2016년도 NISN에서 탐지/차단한 사이버 공격을 분석하고 특징을 살펴본다.

2013년에 NISN에서 탐지/차단한 공격지 IP 주소는 중복을 제거하고 7,618개였다. 그러나 2014년 8,233개, 2015

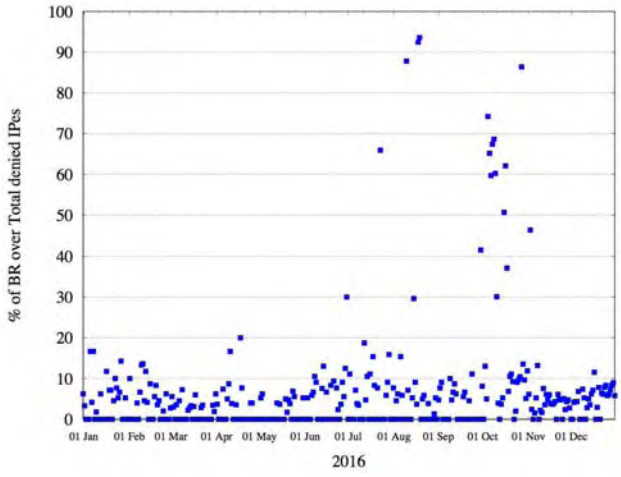
년 10,574개로 증가하더니 2016년에는 22,084개로 2015년도에 비해 2배 이상 큰 폭으로 증가하였다.

(그림 1)은 2016년도에 NISN에서 탐지하고 차단한 공격 IP 주소의 개수를 일별로 나타낸 것이다. 100건 이상인 날이 간헐적으로 나타나지만 8월에 500건 이상 10월, 12월에 1000건 이상 사이버 공격을 탐지/차단한 것은 이례적인 일인 것을 확인할 수 있다. 특히나 10월 이후 연말에 공격이 다른 월에 비해서 많이 공격이 집중된 것을 확인할 수 있다. 8월과 10월 차단한 공격 IP가 급증한 날은 브라질 IP 주소가 많이 나타났다.



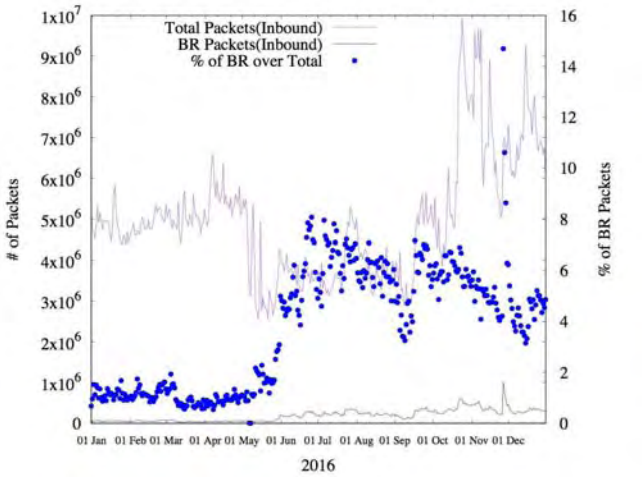
(그림 1) 2016년도 일자별 차단 IP 주소 통계 분포

(그림 2)는 탐지하고 차단한 전체 공격 IP 주소 중에서 브라질을 국가코드로 갖고 있는 IP 주소의 비율을 나타낸 것이다. 8월과 10월에 브라질에서 유입된 공격 IP 주소 비율이 50% 이상 높게 나타난 날이 있는 것을 확인할 수 있다.



(그림 2) 2016년도 일자별 브라질에서 유입된 공격지 IP 주소의 비율

브라질에서 유입되는 공격의 증가를 알아보기 위하여 HPC 서비스 네트워크로 유입되는 전체 트래픽과 브라질 트래픽의 분포를 나타내면 (그림 3)과 같다. 6월 이전에는 전체 트래픽의 2% 미만으로 브라질 트래픽이 유입되었으나 6월부터는 2배 이상 증가하여 전체 트래픽의 4% 이상 브라질에서 트래픽이 유입되는 것을 확인할 수 있다. 이렇게 브라질에서 유입되는 트래픽이 많아지면서 HPC 인프라 및 서비스를 대상으로 하는 공격도 증가한 것으로 유추해 볼 수 있다. 한 가지 특이사항은 2016년 8월 브라질에서는 리우올림픽이 개최되었는데. 6월부터 브라질 발 유입 트래픽이 증가한 원인과의 연관성을 배제할 수 없을 것으로 보인다.



(그림 3) 2016년도 일자별 유입 트래픽 통계 및 브라질 유입 트래픽 비율

4. 결론

본 논문에서는 NISN에서 수집한 사이버 공격 탐지/차단 데이터 및 HPC 서비스 네트워크로 유입되는 네트워크 트래픽 데이터를 분석하여 HPC 서비스를 대상으로 하는 공격이 전체적으로 증가한 것을 확인할 수 있었다. 특히 8월과 10월에 브라질에서 유입되는 공격과 트래픽이 다른 월에 비해 증가폭이 큰 것도 확인할 수 있었다. 향후 이러한 분석한 결과를 활용하여 평소보다 특정 국가에서 트래픽이나 공격이 증가하면 선제적으로 대응할 수 있는 방법 등을 HPC 서비스 환경에 적용하여 보다 안전하게 서비스할 수 있도록 사이버 공격 예측 기술 등에 활용할 수 있는 방안에 대한 연구가 필요할 것으로 보인다.

참고문헌

[1] 이재국, 김성준, 박찬열, 홍태영, “슈퍼컴퓨터 4호기에서 다중 임계값을 이용한 저속 공격 탐지 기법,” 한국정보과학회 2016년 한국컴퓨터종합학술대회 논문집, June 2016.

[2] 이재국, 김성준, 우준, 박찬열, “다중 사용자 컴퓨팅 환경에서 SSH 무작위 공격 분석 및 대응,” 정보처리학회논문지, 컴퓨터 및 통신시스템, No. 4, Vol. 6, April 2015

[3] Jae-Kook Lee, Sung-Jun Kim, Taeyoung Hong, “Brute-force Attacks Analysis against SSH in HPC Multi-user Service Environment,” Indian Journal of Science and Technology, Vol. 9(24), June 2016