지능형 지속 위협(APT) 시나리오 분석에 의한 슈퍼컴퓨터 보안 요구 사항

장 환*
*한국방송통신대학교 대학원 정보과학과
e-mail:jangh1220@knou.ac.kr

Supercomputer security requirements by Advanced Persistent Threat(APT) scenario analysis

Hwan Jang*
*Dept of Information science, Korea National Open University

요 약

매년 슈퍼컴퓨터를 표적으로 공격이 증가하고 있고, 공격의 방식은 날로 진화하고 있다. 슈퍼컴퓨터를 대상으로 하는 공격에 대응하기 위해 기존의 연구는 공격 특성을 분석하여 맞춤형 대책을 제시하거나 분석을 통해 보안 요구사항을 도출하였다. 하지만 연구과정에서 APT life cycle 관점이 반영되지 않으면, 지능형 지속 위협인 APT를 인지 및 대응하기 어려운 문제점이 있다. 이러한 문제점을 해결하기 위해, 본 논문은 APT 시나리오 기반의 위협 모델링 분석을 통해 슈퍼컴퓨터 보안 요구사항을 도출 한다.

1. 서론

TOP500 프로젝트는 고성능 컴퓨팅의 추세를 알 수 있는 신뢰할 수있는 기반을 제공하며, Top500은 오늘날 사용되고있는 가장 빠른 500 대의 컴퓨터 시스템인 High Performance Computing (HPC)를 나열한것이다[1].

미국 국립표준기술연구소 NIST(National Institutes of Standards and Technology)는 HPC를 넓은 물리적 공간을 가지고 있으며 수백만 개의 CPU 코어를 포함하고 상당한 양의 전력을 소비하는 대규모 분산 시스템으로 정의하였고, 이는 슈퍼컴퓨터로 재정의된다. 당대의 가장 빠른 계산 성능으로 정확하고 객관적인 분석 정보를 얻기 위해 슈퍼컴퓨터 도입이 증가하고 있다. 슈퍼컴퓨터의 슈퍼컴퓨팅 서비스 증가로 보안 이슈도 발생하고 있다. NIST는 2016 년 9 월 슈퍼 컴퓨터 보안 문제를 해결하기 위해 워크숍을 개최 하였고 <표 1>과 같이 슈퍼 컴퓨터 보안 과제를 제시하였다[2]. 슈퍼컴퓨터 보안 과제 목록 중에서 '부적절한 사용'과 '서비스 거부'는 슈퍼컴퓨터를 타겟으로 하는 지능형 지속 위협 APT의 목표이다.

NIST는 APT(Advanced Persistent Threat)를 정교한 수준의 전문 지식과 중요한 리소스를 보유한 적이 장기간에 걸쳐 반복적으로 사이버, 물리적, 속임수 등 여러 공격 벡터를 사용하여 거점을 설정 및 확장하고 정보 유출, 특정 임무, Target 조직의 시스템 약화 등 목표를 달성하는 위협으로 정의한다. 슈퍼컴퓨터보안 과제 목록 중 APT 목표로서 '부적절한 사용'은 허가되지 않은 목적으로 슈퍼컴퓨터를 사용하는것을 의미한다. 하지만, 최신 슈퍼컴퓨터 공격 사례를 보면 슈퍼 컴퓨터에 침입하여 암호화폐 채굴을 시도하는 부적절한 사용이 발생하고 있다.

2020년 4월 15일 미국 국무부와 재무부, 국토안보부, 연방수사국은 최근 북한의 사이버 위협에 대한 공동 보고서를 발행했다. 보고서에 따르면 북한이 피해 시스템에 암호화폐 채굴 악성코드를 설치함으로써 전력과 CPU 리소스를 가로채 암호화폐 채굴에 이용하는 크립토재킹 공격을 수행하고 채굴된 자산을 평양 김일성 대학을 포함한 북한 소재 서버에 보낸 사례를 제시하고 있다[3].

〈표 1〉 HPC Security Challenges by NIST

High-Performance Computing Security Challenges
1. Shared HPC Threat Intelligence and Best Practices
2. Wider selection Mandatory Access Control technologies that can work within parallel architectures
3. Minimally impactful HPC Anomaly Detection techniques
4. HPC Software Attestation - Application, Open Source, system
5. Ubiquitous and inexpensive multi-factor authentication
6. Inappropriate use
7. Ip theft
8. Denial of service

2020년 5월 11일 영국 애든보러 대학교의 슈퍼 컴퓨팅 센터인 ARCHER에서 Cray XC30 슈퍼 컴퓨터 로그인 노드의 보안 취약점을 악용한 슈퍼 컴퓨터 침입 시도가 발생되었고, 보안 사고를 조사하는 동안 네트워크 액세스를 차단한다고 발표했다. 동시에 독일 바덴 뷔 르템 베르크 주에있는 슈퍼 컴퓨터 연구 프로젝트를 조정하는 조직인 bwHPC도 보안 사고를 발표하고 리소스에 대한 액세스를 제한하기로 결정했다. 스위스 국립 슈퍼 컴퓨팅 센터는 코로나 바이러스 연구 프로젝트에 참여했을 때 고성능 컴퓨터 시설이 공격을 당하여 일시적으로 폐쇄했다.

2020년 5월 18일 유럽 전역의 슈퍼 컴퓨터에 대한 연구를 조정하는 범 유럽 조직인 EGI (European Grid Infrastructure)의 CSIRT (Computer Security Incident Response Team)의 보고서에 따르면, 이 사건을 "CPU mining purposes" 즉, 외부 공격자가 암호화폐 채굴 시도를 위한 목적으로 슈퍼 컴퓨터에 침입하였다고, 분석한다[4].

슈퍼컴퓨터보안 과제 목록 중 APT 목표로서 '서비스 거부'는 권한이 부여된 사용자 또는 개체가 서비스를 요청하였을 때 응답 시스템에서 서비스 요청의 처리를 거부하는 것을 의미한다. 하지만, 최신 슈퍼컴퓨터 공격 사례를 보면 슈퍼 컴퓨터의 계산 기능을 손상시키고, 시스템 중단을 유발하는 서비스 거부 공격이 발생하고 있다. 관련 사례로 수냉식 슈퍼 컴퓨터 환경에서 제어 시스템 공격을 통해 슈퍼 컴퓨팅 서비스를 중단하는 공격 시나리오가 있다[5].

이러한 보안 문제를 해결하기 위해 보안 요구사항이 필요하지만 기존의 연구는 공격 특성을 분석하여 맞춤형 대책만 제시하거나 보안 요구사항을 도출하는 과정에서 APT Life Cycle을 반영하지 않은 문제점이 있다. 이러한 문제점을 해결하기 위해, APT 시나리오 분석에 의한 슈퍼 컴퓨터 보안 요구사항 도출이 필요하다.

2. 관련 연구

2.1 슈퍼컴퓨팅 환경의 SSH 무작위 공격 분석 및 대응

Lee, Jae-Kook은 2014년 국가 슈퍼컴퓨팅연구소에서 수집한 SSH Brute Force Attack 데이터를 비정상 접속 시도, 공격 계정, 공격 지속성, 공격 국가의 기준으로 분석하고 대응 방안을 제시하였다. 하지만, 특정 공격에 대한 분석 및 대응 연구로 한정되었고, APT life Cycle이 고려되지 않았다. 이는 제시된 대응방안을 통해 APT에 대응하기 어려운 문제점이 있다. 이를 해결하기 위해, APT life Cycle을 채택 및 반영하여 위협을 분석하는 과정이 필요하다[6].

2.2 새로운 APT Life Cycle 도출

Messaoud, Brahim ID은 공격자의 목표에 따라 컴파일된 새로운 APT Life Cycle을 도출하였다. 하지만, 새로 도출된 APT Life Cycle은 실제 수행된 공격 사례를 반영하지 않았기 때문에, 연도별, 국가별 APT 특징과 공격 대상에 따른 공격 방식의 변화에 따라 매핑 되지 않고, 실제 활용하기 어려운 문제점이 있다. 문제점을 해결하기 위해 미 법무부에서 연도별 국가별로 APT 그룹을 기소할 때 미 연방법원에 제출한 공소장을 분석하고 공통의 APT Life Cycle을 도출 및 채택하는 과정이 필요하다[7].

3. APT 시나리오 분석

APT 시나리오 분석이란 소프트웨어 개발 주기 구현 전 단계에서 임의의 공격자 관점으로 분석대상의 APT 위협을 시나리오를 통해 식별하고 분석하는 방법론이다. 본 연구에서는 Microsoft threat modeling tool 2016을 사용하여 슈퍼컴퓨터에 대해 APT 시나리오 분석을 하였다. APT 시나리오 분석 순서는 APT life Cycle 채택 → 데이터 흐름 다이어 그램 도출 → APT 시나리오 분석 순서로 진행하였다.

3.1 APT life Cycle 도출

미 법무부에서 APT 그룹을 기소할 때 미 연방법원에 제출한 공소장을 분석하고 공통의 APT Life Cycle 요소를 도출하였다. 또한, <표 1>의 슈퍼컴퓨터 보안 과제 및 관련 연구에서 확인된 문제점을 반영하여 APT 시나리오 분석을 위한 APT life Cycle 을 <표 2>과 같이 설정하였다.

〈표 2〉 APT Life Cycle

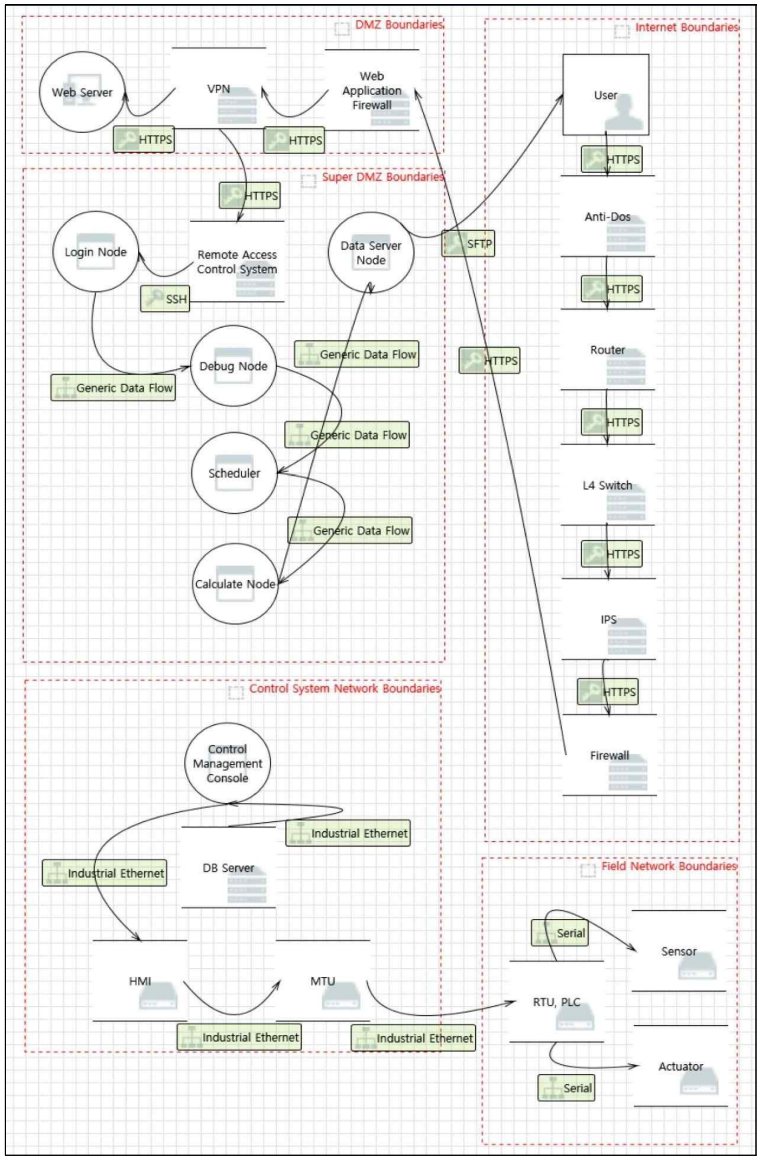
Step	Description
Initial approach	Initial approach through attack vectors such as spear phishing
Malware execution	Execution of malicious scripts
Exploit	System privilege acquisition using system vulnerability
Gathering additional information	Collect network structure, vulnerable host information and obtain additional authentication information
Base expansion	Additional intrusion and authentication of other systems
Continuous access and target control	Maintain backdoor connection and control command
Achieve the goal	Achieve APT goals such as cryptocurrency mining and system damage

3.2 데이터 흐름 다이어그램 도출

DFD(Data Flow Diagram)는 시스템 구성요소 간의 데이터 흐름을 시각화하여 나타낸 그림이다. DFD의 구성요소는 <표 3>와 같다. 이를 활용하여 슈퍼컴퓨터의 DFD를 (그림 1)과 같이 도출하였다.

〈표 3〉 Data flow diagram component

Element	Shape	Description
Entity		Generate data input/output
Device		Temporary / permanent data storage
Process		Data input/output processing
Data Flow		Data movement
Trust Boundary		Change of authority level



(그림 1) Supercomputer DFD

1) 슈퍼컴퓨터 DFD 구조 및 데이터 흐름

Supercomputer DFD는 User가 슈퍼컴퓨팅 서비스에 접근하기 위해 네트워크 장비 및 보안 장비를 거치는 구간인 Internet Boundaries, VPN을 통해 Web Server에 접근하여 슈퍼컴퓨팅 서비스 계정을 신청하고 발급받는 구간인 DMZ Boundaries, Login Node에 SSH 로그인 후 Batch Scripts를 실행하고, Scheduler를 통해 할당된 Calculate Node로 연산된 결과를 Data Server Node에서 발송하는 구간인 Super DMZ Boundaries, 원방감시제어시스템 SCADA(supervisory control and data acquisition)을 통해 냉각수를 제어하는 구간인 Control System Network Boundaries, 원방감시제어시스템에서 전달한 데이터값을 반영하여 PLC (Programmable Logic Controller) 제어로직을 통해 현장의 Sensor와 Actuator를 조종하는 구간인 Field Network Boundaries를 반영하여 작성하였다.

User가 VPN을 통해 Web Server로 계정을 신청할 때 Https 프로토콜이 사용되고, Login Node에 SSH 프로토콜을 사용하여 로그인을 하며, 연산된 결과값은 Data Server Node에서 SFTP 프로토콜을 사용하여 전송한다. 따라서, 슈퍼컴퓨팅 서비스에서 사용되는 각 각의 자산 취약점 및 프로토콜 취약점을 이용하여 공격자는 APT 공격을 수행한다. 또한, 냉각수 제어시스템은 Industrial Ethernet 취약점과 산업제어시스템의 취약점을 이용하여 공격을 수행한다.

3.3 APT 시나리오 분석

<표 2>의 APT life Cycle에 DFD 구성요소를 매핑하고 관련 연구 및 연구 배경에서 확인된 공격 시나리오 등을 반영하여 APT 시나리오 분석을 수행하였다. 슈퍼컴퓨터 보안 과제 목록 중에서 부적절한 사용에 해당 하는 APT 공격 목표인 암호화폐 채굴을 위해 <표 4>와 같이 APT 시나리오 분석을 수행하였다.

〈표 4〉 Supercomputer Cryptojacking

Step	Description
Initial approach	Initial approach through attack vectors such as spear phishing, usb attachment
Malware execution	Establish C&C connection and obtain VPN authentication information after executing malicious script on accessing user PC
Exploit	VPN authentication and authorization after exploiting VPN server vulnerability
Gathering additional information	After collecting target network configuration and system configuration information, obtain SSH authentication information that can authenticate to the login node of the super computer
Base expansion	Access to the login node of the super computer using SSH authentication information and acquire root privileges after exploiting the Linux kernel vulnerability
Continuous access and target control	Cryptocurrency mining command and infected host control through C&C server after maintaining SSH connection
Achieve the goal	Achieving the APT goal of cryptocurrency mining

슈퍼컴퓨터 보안 과제 목록 중에서 서비스 거부에 해당하는 APT 공격 목표인 슈퍼 컴퓨팅 서비스 중단을 위해 <표 5>와 같이 APT 시나리오 분석을 수행하였다.

〈표 5〉 Supercomputing service disruption

Step	Description
Initial approach	Initial approach through attack vectors such as spear phishing, watering hole
Malware execution	Infect User PC and obtain VPN authentication information by executing malicious code
Exploit	Create SCADA exploit file on USB inserted in infected user PC and access VPN after exploiting VPN server vulnerability
Gathering additional information	Control network information collection
Base expansion	Control management information is leaked through DB server after accessing the Control Managemnet Console through infected user PC or USB memory stick and executing malicious script
Continuous access and target control	Supercomputing service interruption due to actuator malfunction through PLC control logic change after maintaining access to Control Managemnet Console and exploiting SCADA and control communication protocol vulnerability
Achieve the goal	Achieve the APT goal of supercomputing service suspension

4. 슈퍼컴퓨터 보안 요구 사항 도출

APT life Cycle 도출, 데이터 흐름 다이어 그램 도출, APT 시나리오 분석에 따라 <표 6>과 같이 슈퍼컴퓨터 보안 요구 사항을 도출하였다. 목표 달성 단계를 제외한 APT life Cycle 각 단계에서 Primary Category의 보안 기능이 요구된다.

〈표 6〉 Supercomputer security requirements

Step	Primary Category
Initial approach	Simulation training and security training are required for users. In addition, threats must be detected by analyzing behaviors according to user profiles. A UBA solution is proposed.
Malware execution	Network traffic should be intercepted by mirroring, suspicious content should be analyzed in an isolated environment and malicious code execution should be blocked. Sand boxing is suggested.
Exploit	Vulnerability assessment should be performed at all times.
Gathering additional information	When a scan attempt occurs, the CERT should analyze the threat IP and block it early.
Base expansion	Honeypots should be deployed at different network locations to detect APT threats early.
Continuous access and target control	Threat traffic continuously approaching through SIEM and TMS must be analyzed and blocked early.

5. 결론

본 논문은 실제 수행된 APT 사건의 기소 사례를 통해 APT Life Cycle을 도출 및 반영하여 APT시나리오 분석을 수행하였고, 보안 요구 사항을 도출하였다. 따라서 슈퍼컴퓨터에 대한 APT를 인지 및 공격 목표 달성 저지에 도움이 된다. 또한, 도출된 슈퍼컴퓨터 보안 요구 사항은 소프트웨어 개발 주기 구현 전 단계에서 APT 위협을 식별하고, APT에 대응하는 보안 정책 수립 과정에서 활용된다.

참고문헌

[1] TOP 500, "INTRODUCTION AND OBJECTIVES" [Internet], https://www.top500.org/project/introduction/

[2] NIST. "An Action Plan for High Performance Computing Security". November 2016.

[3] CISA. "Guidance on the North Korean Cyber Threat". April 2020.

[4] Egi-Csirt. "Security incidents on multiple HPC sites". May 2020.

[5] Chung, Keywhan, et al. "Attacking supercomputers through targeted alteration of environmental control: A data driven case study." Conference on Communications and Network Security (CNS). IEEE, 2016.

[6] Lee, Jae-Kook, et al. "Analysis and Response of SSH Brute Force Attacks in Multi-User Computing Environment." KIPS Transactions on Computer and Communication Systems, 4(6), 205-212. 2015.

[7] Messaoud, Brahim ID, et al. "Advanced persistent threat: new analysis driven by life cycle phases and their challenges." International Conference on Advanced Communication Systems and Information Security (ACOSIS). IEEE, 2016.