BT 대응을 위한 IoBE Kill Chain 프레임워크

송유래[1], 김득훈[2], 곽진[3]
[1]아주대학교 사이버보안학과, 정보보호응용및보증연구실
[2]아주대학교 정보통신연구소
[3]아주대학교 사이버보안학과
clara701@ajou.ac.kr, kimdh1206@ajou.ac.kr, security@ajou.ac.kr

IoBE Kill Chain Framework against Blended Threat

Yu-Rae Song[1], Deuk-Hun Kim[2], Jin Kwak[3]
[1]ISAA Lab., Dept. of Cyber Security, Ajou University
[2]Institute for Information and Communication, Ajou University
[3]Dept. of Cyber Security, Ajou University

요 약

IoT(Internet of Things) 디바이스가 상호연결됨에 따라 융합환경인 IoBE(Internet of Things Blended Environment)가 발전하고 있다. 그러나 IoBE 내 IoT 디바이스가 상호연결되고, 네트워크가 복잡해짐에 따라 공격 표면도 증가하고 있다. 이를 통해 증가한 공격 표면에서 서로 다른 취약점들이 복합된 보안위협인 BT(Blended Threat)가 나타날 수 있다. 기존에 보안위협 대응을 위한 프레임워크 중 하나로 Cyber Kill Chain이 활용되고 있지만, 이는 공격자가 한 번의 공격을 수행하는 과정을 분석하므로 IoBE에서 발생 가능한 BT에 적용하기 어렵다. 따라서, 본 논문에서는 IoBE 내 BT 기반 공격에 대한 분석이 가능한 IoBE Kill Chain을 제안한다.

1. 서론

IoT 디바이스 및 5G 통신기술의 발달로 공장, 발전소, 의료 등 다양한 분야에서 IoT 디바이스를 활용하고 있다. 각 분야에서 활용되는 IoT 디바이스는 상호연결되어 스마트팩토리, 스마트그리드 등의 환경을 이루고, 이러한 환경들이 서로 영향을 주고받는 융합환경인 IoBE(Internet of Things Blended Environment) 형태로 발전하고 있다. 그러나 IoBE 내 디바이스가 서로 연결되고 네트워크가 복잡해짐에 따라 공격 표면이 증가하며, 증가한 공격 표면의 취약점으로 인해 BT(Blended Threat)가 새롭게 발생할 수 있다.

보안위협에 대응하기 위해 연구된 대응체계 중 Cyber Kill Chain은 일련의 공격 과정을 단계별로 분석하고, 이를 통해 단계별 대응방안을 도출하는 사이버 공격 대응체계이다. 또한, Cyber Kill Chain을 응용하여 IoT 디바이스를 대상으로 하는 공격에 초점을 맞춘 IoT Kill Chain도 존재한다[1]. 그러나 Cyber Kill Chain과 IoT Kill Chain은 한 번의 공격 수행 이후 연쇄적으로 발생 가능한 공격을 분석하기 어렵다는 한계점이 존재한다. 따라서, 본 논문에서는 기존에 연구된 Kill Chain의 한계점을 개선하여 BT 기반 공격에 대응할 수 있는 IoBE Kill Chain을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 IoBE와 BT의 정의를 설명하고, Cyber Kill Chain과 IoT Kill Chain의 과정에 대하여 설명한다. 다음으로 3장에서는 본 논문에서 제안하는 IoBE Kill Chain의 단계를 설명한 뒤, 4장에서 결론을 맺는다.

2. 관련연구

2.1 IoBE

IoBE는 스마트팩토리, 스마트그리드 등의 융합환경이 상호연결된 환경이다. 융합환경은 센싱, 네트워킹, 빅데이터, 인공지능, 클라우드 등 다양한 IT 기술이 융합된 환경으로, IoT 디바이스들이 복잡하게 연결되어있다. IoBE는 다양한 융합환경이 연결됨에 따라 스마트시티, 스마트 사회, 스마트 국가로 발전할 수 있다.

IoBE 내에 포함된 IoT 디바이스가 상호연결되어 데이터 수집, 가공, 저장 등의 데이터 통신이 복잡해짐에 따라 보안위협이 발생 가능한 공격 표면이 증가하고 있으며, 이에 대응하기 위한 연구가 진행되고 있다[2].

2.2 BT

BT는 IoBE 내 각 융합환경을 구성하는 디바이스 아키텍처, 네트워크 프로토콜, 플랫폼 등의 취약점을 통해 발생 가능한 복합적인 보안위협을 의미한다. IoBE 내에 새로운 환경이 유입될수록 구성 요소가 많아지므로 발생 가능한 보안위협의 복잡성이 증가할 것이다. 이에 대응하기 위해, 보안 취약점이 융·복합되어 발생할 수 있는 BT 대응 관련 연구가 수행되고 있다[2, 3].

2.3 Cyber Kill Chain

Cyber Kill Chain은 공격자가 목적을 달성하기 위해 수행하는 준비부터 실행까지의 일련의 과정을 단계별로 정의한 프레임워크이다. 공격자의 단계별 사이버 침입 활동을 분석하여 각 단계에서 수행 가능한 대응방안을 도출하는 것을 목적으로 한다. 총 7단계로 구성되어 있으며, 각 단계에 대한 설명은 <표 1>과 같다[4].

<표 1> Cyber Kill Chain[4]

단계	설명
정찰	이메일 주소, 직원 정보, 서버 정보 등 필요한 모든 정보 수집
무기화	정찰 단계에서 얻은 정보를 기반으로 공격대상에 사용할 멀웨어, 익스플로잇 등이 포함된 페이로드 준비
전달	이메일, USB 등을 통해 악성코드를 공격대상에 전달
익스플로잇	사용자가 페이로드를 실행하도록 유도하여 공격대상에 대한 접근 권한 획득
설치	접근을 유지하기 위한 백도어 설치
C&C (Command & Control)	명령 및 제어(C&C) 단계에서는 대상 시스템과 공격자의 C&C 서버를 연결하여 원격조작 준비
행동 개시	데이터 수집, 수정, 시스템 파괴 등 공격자의 목표를 달성하기 위한 활동 수행

2.4 IoT Kill Chain

Junaid H. 등이 제안한 IoT Kill Chain은 IoT 디바이스에 초점을 맞춰 공격의 세부 단계를 조사한 Kill Chain이다. 총 9단계로 구성되어 있으며, 각 단계에 대한 설명은 <표 2>와 같다[1].

<표 2> IoT Kill Chain

단계	설명
디바이스 발견	공격 수행할 디바이스 탐색
디바이스 침입	전수조사 공격, 사전 공격 등을 통해 디바이스에 대한 접근 시도
디바이스 정보 수집	쉘 활성화, 사용자 정보 수집, 파일 또는 디렉토리 탐색 수행
디바이스 준비	디바이스 비밀번호 변경, 파일이나 디렉토리에 특정 동작 수행 등 디바이스를 사용할 준비 수행
패키지 다운로드	CURL, WGET, TFTP 등의 명령어를 통해 다운로드, 복사 및 이동
패키지 준비	CHMOD 명령어로 권한 설정
패키지 설치	쉘 스크립트나 바이너리 파일 작동
흔적 삭제	다운로드한 바이너리나 스크립트 등 디바이스 활용 흔적 제거
행동 개시	다른 공격대상에 TCP/IP Request 전송

3. IoBE Kill Chain

기존 보안위협 대응체계인 Cyber Kill Chain과 IoT Kill Chain은 공격자가 한 번의 공격을 수행하는 일련의 과정을 일반화한 프레임워크이므로, IoBE 내 구성 요소의 취약점들이 융·복합된 BT 기반 공격을 설명하기 어렵다. 따라서, 본 장에서는 BT 기반 공격 과정을 분석 및 일반화한 IoBE Kill Chain을 제안한다.

Step 1. 정찰 및 스캔
공격자가 공격대상으로 선정할 IoT 디바이스나 시스템 A를 정찰하는 단계로, 공격자는 사용자 및 서버 정보 수집, 제로데이 취약점 등을 통해 보안이 취약한 IoT 디바이스 및 시스템을 스캐닝한다.

Step 2. 무기화
공격자가 스캐닝한 공격대상 A에 사용할 멀웨어, 익스플로잇 등이 포함된 악성 프로그램을 생성한다.

Step 3. 접근
공격자는 A에 접근하여 패킷 스니핑, 스피어피싱, Drive By Download 등의 공격방법을 통해 A와 공격자의 디바이스를 연결한다.

(그림 1) Proposed IoBE Kill Chain Framework

Step 4. 권한 획득

공격자의 디바이스가 A와 연결되면 A의 패스워드를 탈취하거나, OS 또는 앱의 권한 상승 취약점 등을 활용하여 데이터를 악용할 수 있는 권한을 획득한다.

Step 5. 악성 프로그램 설치

공격자는 A의 사용자 및 관리자가 악성 페이로드를 실행시키도록 한다. A의 사용자 및 관리자에 의해 실행된 악성 페이로드는 악성 프로그램 및 원격 백도어를 설치하여 원격으로 A에 접근할 수 있다.

Step 6. 명령 및 제어

공격자는 원격 백도어로 A에 접근하고, 공격자와 C&C 서버 간의 연결 설정을 통해 시스템 권한을 원격으로 획득한다. 이를 통해 명령어 전달 및 대기, 원격제어 등의 활동을 수행한다.

Step 7. 공격 실행

공격자가 A에 대한 공격을 실행하는 단계로, 데이터 유출, 데이터 위변조, DDoS 공격, 시스템 오작동 및 중단 등의 공격을 수행한다.

Step 8. 탐색

공격자는 현재 침투한 A에서 접근할 IoBE 내 다른 IoT 디바이스 및 융합환경(스마트팩토리, 디지털 헬스케어 등)을 추가적으로 탐색한다. 지능형 악성코드를 활용하여 접속 가능한 네트워크나 취약점을 탐색하거나, 이미 수집한 정보를 활용하여 공격대상 B를 찾는다.

Step 9. 전파

공격자가 B를 찾았다면 네트워크, USB 등을 통해 새로운 공격대상이 된 B에 연결 및 이동한다. 공격자는 초기에 무기화하였던 악성 페이로드를 활용하거나 필요한 무기를 추가적으로 만들어 공격을 수행한다.

Step 10. 흔적 삭제

공격자는 페이로드를 전파한 뒤, 공격을 위해 A에 악용되었던 악성코드 또는 이벤트 로그를 삭제한다. 이를 통해 공격자의 침입 흔적을 지워 공격자에 대한 추적의 난이도를 높인다.

4. 결론

본 논문에서는 IoBE에서의 BT 기반 공격에 대하여 단계별 분석이 가능한 IoBE Kill Chain을 제안한다. IoBE Kill Chain은 IoBE의 융복합성을 고려한 탐색, 전파 단계를 포함하여 BT를 기반으로 하는 공격의 단계별 악성 행위를 분석할 수 있다. 추후 IoBE Kill Chain을 기반으로 BT에 대한 단계별 대응방안을 분석할 계획이다.

사사문구

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1A2C2011391).

참고문헌

[1] J. Haseeb, M. Mansoori., and I. Welch, “A measurement Study of IoT-Based Attacks Using IoT Kill Chain”, 2020 IEEE 19th International Conference on TrustCom, Guangzhou, China, 2020, pp.557-567.

[2] M. K. Lee, J. Jang-Jaccard, and J. Kwak, “Novel Architecture of Security Orchestration, Automation and Response in Internet of Blended Environment”, CMC-COMPUTERS MATERIALS & CONTINUA, vol.73, no.1, 2022, pp.199-223.

[3] M. K. Lee., I. S. Jeong., D. H. Kim, J. Jang-Jaccard, and J. Kwak, “Applicability Analysis of Knowledge Graph Embedding on Blended Threat”, 2022 International Conference on Platform Technology and Service(PlatCon), Jeju, Korea, 2022, pp.48-52.

[4] L. Martin, “Gaining the Advantage”, Lockheed Martin Corporation, 2015.