IoT 봇넷 악성코드 기반 침해사고 흔적 수집 방법

이형우*
한신대학교 컴퓨터공학부 교수

Intrusion Artifact Acquisition Method based on IoT Botnet Malware

Hyung-Woo Lee*
Professor, Div. of Computer Engineering, Hanshin University

요 약 IoT와 모바일 기기 사용이 급격히 증가하면서 IoT 기기를 대상으로 한 사이버 범죄 역시 늘어나고 있다. IoT 기기 중 Wireless AP(Access Point)를 사용할 경우 자체 보안 취약성으로 인해 패킷이 외부로 노출되거나 Bot과 같은 악성코드에 손쉽게 감염되어 DDoS 공격 트래픽을 유발하는 등의 문제점이 발견되고 있다. 이에 본 연구에서는 최근 급증하는 IoT 기기 대상 사이버 공격에 능동적으로 대응하기 위해 공공분야 시장 점유율이 높은 IoT 기기를 대상으로 침해사고 흔적을 수집하고, 침해사고 분석 데이터의 유효성을 향상시키기 위한 방법을 제시하였다. 구체적으로, 샘플 IoT 악성코드를 대상으로 동작 재현을 통해 취약점 발생 요인을 파악한 후 침해 시스템 내 주요 침해사고 흔적 데이터를 획득하고 분석하는 방법을 제시하였다. 이에 따라 대단위 IoT 기기를 대상으로 한 침해사고 발생시 이에 효율적으로 대응할 수 있는 체계를 구축할 수 있을 것으로 기대된다.

주제어 : IoT 기기, 봇넷, 악성코드, 침해사고, 디지털 아티팩트 및 흔적 수집

Abstract With the rapid increase in the use of IoT and mobile devices, cyber criminals targeting IoT devices are also on the rise. Among IoT devices, when using a wireless access point (AP), problems such as packets being exposed to the outside due to their own security vulnerabilities or easily infected with malicious codes such as bots, causing DDoS attack traffic, are being discovered. Therefore, in this study, in order to actively respond to cyber attacks targeting IoT devices that are rapidly increasing in recent years, we proposed a method to collect traces of intrusion incidents artifacts from IoT devices, and to improve the validity of intrusion analysis data. Specifically, we presented a method to acquire and analyze digital forensics artifacts in the compromised system after identifying the causes of vulnerabilities by reproducing the behavior of the sample IoT malware. Accordingly, it is expected that it will be possible to establish a system that can efficiently detect intrusion incidents on targeting large-scale IoT devices.

Key Words : IoT devices, botnets, malware, intrusion, digital evidence and artifacts collection.

이 성과의 일부는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No 2021R1F1A1046954).
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2021년 6월 24일 수정일 2021년 8월 17일 심사완료일 2021년 8월 24일

1. 서론

최근 IoT(Internet of Things)와 모바일 기기 사용이 급격히 증가하면서 사이버 범죄 위험이 더욱 증가하고 있다. 특히 일상생활에서 사용하는 각종 서비스들이 대부분 보안에 취약한 IoT·경량형 통신 기기 등과 연동되면서 사이버 보안 위협에 노출되고 있다. 특히 무선랜 공유기인 Wireless AP(Access Point)를 사용할 경우 패킷이 외부로 노출되거나, 보안 취약성을 악용하여 자동 전파되는 악성코드인 Bot에 의해 손쉽게 감염되어 사용자도 모르게 DDoS 공격 트래픽을 발생하는 등의 문제점이 발견되고 있다[1].

이는 대부분의 IoT 기기가 stripped-down 형태의 Linux OS를 탑재하고 있어 악성코드에 손쉽게 감염되는 특성을 보이고 있기 때문이다. 대부분의 경량형 IoT 기기인 경우 대역폭 제어, 필터링 기능 없이 인터넷 연결 기능을 제공하고 있으며, 경량화된 OS가 탑재되어 있어 감사(auditing) 기능 없이 최소화된 보안 기능만을 제공하고 있다. 또한, IoT 기기 개발시 기개발된 모듈을 단순 수정하여 탑재하므로 결국에는 다양한 보안 취약성을 내포하고 있다. 따라서 이와 같은 IoT 기기의 보안 취약점을 악용하여 악의적인 공격자는 손쉽게 IoT 기기에 악성코드를 감염시키고 네트워크 내 다른 IoT 기기로 자동 전파하여 궁극적으로는 IoT 봇넷(IoT Botnet)을 구축할 수 있다[2,3].

IoT Botnet의 핵심 모듈인 악성코드(Malware)는 Linux 기반 OS에서 구동 가능하도록 제작되었으며, IoT 기기 내 RAM에 일시적으로 상주하여, 호스트에 대한 성능 저하 등 Side-effect 없이 해당 기기를 감염시킨다. 또한 대부분의 IoT Botnet Malware는 reflection 이나 amplification 방법 등을 사용하지 않고도 공격을 수행하므로, 기존의 일반적인 Malware 보다 탐지되지 않는 특성이 있다. 게다가 IoT Malware에 의해 생성되는 DDoS 트래픽은 기존의 PC 기반 Botnet 보다도 강력하여 대량의 트래픽을 손쉽게 생성할 수 있으며, 광범위한 지역에 대량으로 Bot을 전파시킬 수 있다[4]. 따라서 IoT 기기가 Botnet에 감염되어 DDoS 트래픽을 발생하는 등의 침해사고가 발생할 경우 침해사고 흔적을 수집하고, 획득된 데이터를 분석할 수 있는 방법이 제시되어야 한다.

이에 본 연구에서는 최근 급증하는 IoT 기기를 대상으로 한 Botnet 기반 사이버 공격에 능동적으로 대응하기 위해 시장 점유율이 높은 IoT 기기를 대상으로 침해사고와 관련된 침해사고 흔적(intrusion artifacts)를 수집하고, 유효한 침해사고 분석 데이터를 도출하기 위한 방법론을 제시하고자 한다. 구체적으로, 샘플 IoT Botnet 악성코드를 선별한 후 이를 직접 동작 재현한 후 침해사고가 발생한 IoT 기기 내 주요 침해사고 흔적 데이터를 식별하고 이를 효율적으로 분석하는 방법을 제시하고자 한다.

2. IoT Botnet Malware

2.1 IoT 기기 대상 Botnet Malware 침해사고

최근 IoT 기기의 보안 취약점을 악용한 IoT Botnet Malware가 급속히 확산되고 있다. IoT 기기 내부 보안 취약성으로 인해 공격자는 손쉽게 인터넷에 연결된 다양한 형태의 IoT 기기를 대상으로 Botnet을 구축할 수 있다. 이는 대부분의 IoT 기기가 stripped-down 형태의 Linux OS를 탑재하고 있으며, 대역폭 제어 기능이 취약하고, 필터링 기능을 제공하지 않은 채로 자체 OS에 대한 충분한 형태의 감사 기능을 제공하지 않기 때문이다[5].

IoT Botnet의 진화 과정을 살펴보면 다음과 같다. 2008년 처음 발견된 Linux/Hydra 이후 지속적으로 진화하고 있으며, DNS 서버 설정 변경을 통해 구동되는 IRC bot(Tsunami), empty 또는 default credential 취약점을 대상으로 한 Bot(Carna) 등이 발견되었다. 특히 Linksys 라우터 등을 대상으로 한 IoT worm(TheMoon), CCTV/DVR/홈 라우터 등을 대상으로 한 DDoS IoT Botnet Malware(Mirai) 등이 발견되었고, 하드웨어 독립적이며 IRC 없이 TCP 기반 C&C 서버를 사용하는 Bot(Qbot) 등으로 진화하였다[4-6].

심지어는 IoT 기기를 대상으로 DDoS 공격을 수행할 수 있는 샘플 IoT 악성코드가 인터넷에 배포되고 있는 실정이다. 단돈 $19.99로 20분 동안 35Gbps TCP/UDP 트래픽을 발생시키는 Shenron Attack Tool 및 Mirai, Kaiten, Qbot Botnet 기반 DDoS 공격 도구 등이 오픈소스 형태로 인터넷에서 무료로 다운로드가 가능한 실정이다.

2.2 IoT 기기 대상 Botnet Malware 대응 필요성

IoT Botnet Malware를 통한 DDoS 공격 피해가 지속적으로 발생하고 있다. 구체적으로 살펴보면 KrebsOnSecurity.com (2016.9.30. vDOS 도구 기반 DDoS 공격 피해), OVH (2016.9.22. Mirai/BASHLITE

malware 기반 CCTV/DVR 장비에 대한 DDoS 공격 피해), Dyn(2016.10.21. 프린터, IP 카메라, 게이트웨이 등 Mirai Malware 기반 tcp/udp DDoS 공격 피해), Deutsche Telecom(2016.11.27. 홈라우터 접속 장애) 등 해킹공격이 지속적으로 발생하고 있다[5]. 국내인 경우 2018년 2월 국내 D사 가정용 공유기 취약점을 이용해 4만여 대를 해킹, 최소 24만여 대를 감염시키고 CCTV내 사생활 침해 문제를 야기하는 등의 문제가 보고되고 있다. 따라서, 최근 급증하는 IoT 기기를 타켓으로하는 Botnet 기반 사이버 공격에 능동적으로 대응하기 위해서는 침해사고 원인 분석을 위한 증거자료를 수집하고, 수집된 데이터를 분석하여 유효한 결과를 도출하기 위한 방법론이 필요하다.

3. IoT Botnet Malware 동향 분석

3.1 IoT Botnet 기반 DDoS 공격 상세 현황

IoT Botnet Malware 기반 공격 현황을 구체적으로 살펴보면 다음과 같다. 우선, NAS IoT 장비를 대상으로 2014년에 TheMoon Botnet이 개발되었다. CVE-2014-9583에 근거하여 ASUS 라우터에 대한 공격이 발견되었으며, NAS(Network Attached Storage)에 대한 보안 취약성을 악용한 악성코드가 최초로 개발되었다. 이후에는 일반 IoT 장비를 대상으로 2016년에 Mirai IoT Botnet이 발견되었다. 이는 IoT 장비를 좀비화 하여 네트워크 상에서 해커가 마음대로 제어할 수 있는 Botnet으로, 2016년 10월, DNS 제공업체인 Dyn이 대규모 DDoS 공격을 받으면서 알려지게 되었다. 보안 카메라 등 보안이 허술한 IoT 장비에 악성코드를 설치한 후 인터넷 트래픽을 라우팅하는 Dyn 서버를 공격하는 방식으로 동작한다. 이후에도 아래와 같이 IoT Botnet 기반 공격 사례가 지속적으로 발생하고 있다.

- 2016년 09월 13일 : 컴퓨터 보안기자 Brian Krebs의 웹사이트(krebsonsecurity.com)에 대한 665Gbps DDoS 공격 진행
- 2016년 09월 18일 : 프랑스 웹 호스트 OVH에 최초 1.1 Tbps 공격시작, 최종 1.5 Tbps 공격으로 세계에서 가장 큰 규모의 DDoS 공격으로 기록
- 2016년 09월 30일 : 해커 포럼(Hacker Forum)에 미라이 제작자 소스코드와 상세한 내용 공개
- 2016년 10월 21일 : 2016 Dyn cyberattack 1.2 Tbps 크기 공격(미국의 주요 도메인 서비스 마비된 사건 발생, 장기간 서비스 중단)

3.2 IoT Botnet Malware 진화 상세 분석

2017년 이후 IoTroop Botnet 등 Mirai Botnet[4]의 변종이 발견되었다. DNS 증복 기술을 활용하여 금융권을 대상으로 DDoS 트래픽 양을 늘리도록 수정되었으며, Mirai Okiru 라는 변종 Bot도 개발되어 각종 CCTV나 DVR, 웹 카메라, 라우터 및 기타 사물인터넷 기기의 보안 취약점을 악용해 해당 기기와 연결된 네트워크를 장악해 수십만 대 가량의 디지털 기기를 제어할 수 있는 악성 프로그램을 유포시키는 방식으로 DDoS 공격을 수행한다. 또한, NAS 스토리지 관련 취약점(CVE-2019-7192, CVE-2019-7195) 등이 지속적으로 발견되었다. 주로 기업에서 데이터 저장이나 클라우드 시스템 운영을 위해 사용하고 있는 W사의 대부분의 NAS 장비에 존재하는 보안 취약점을 이용해 악의적인 해커는 루트권한으로 원격 명령을 실행할 수 있고, 해외 해커는 이미 이 취약점을 이용해 원격으로 설치할 수 있는 랜섬웨어를 만들어둔 상태이다. Black Hat Security Conference에서 독립 보안 평가 기관의 보안 연구원인 Jacob Holcomb에 의하면 10개 제조사의 NAS를 분석한 결과 "해킹에 안전한 제품은 단 하나도 없었으며, 최소한 절반의 NAS에 인증 절차 없이 접근이 가능하다고 밝혔다. 이와 같이 최근 IoT 장비를 대상으로 한 공격이 지속적으로 발생하고 있으며, IoT Botnet Malware의 진화 과정을 살펴보면 다음과 같다.

- Linux/Hydra : 2008년 처음 발견된 Open source botnet framework
- Psyb0t : 2009년 DSL 모뎀을 대상으로 IRC(Internet Relay Chat) 기반 C&C 서버 구동
- Chuck Noris : 2010년 DSL 모뎀 기반 IRC Bot, DNS 모뎀과 감염된 라우터에서 발견된 IRC bot
- Tsunami : 2001년 발견, Kaiten으로 불림. DNS 서버 설정 변경을 통해 구동되는 IRC bot
- LightAidra/Aidra : IRC 기반 대량 스캔 및 exploit 도구
- Carna : empty 또는 default credential을 기반으로 라우터, IoT 장비를 대상으로 하는 공격
- Linux.Darlloz : 2014년 발견, IoT Worm 이라고 할 수 있음, PHP 취약점을 이용
- Linux.Wifatch : weak 또는 default credential을

공격하는 open-source malware

- TheMoon : 2014년 Johannes Ullrich에 의해 개발된 IoT worm. Linksys 라우터 대상 공격
- Spike / Dofloo : 2014년 backdoor/DDoS malware. MIPS/ARM 아키텍쳐 기반 리눅스 PC 공격. Syn Flooding/UDP flooding/DNS query flood, GET flooding 공격을 수행함
- BASHLITE / Lizkebab / Torlus / gafgyt :2015년 IoT 장비에 대한 DDoS 공격을 수행. Default credential을 기반으로 brute-force 공격을 수행
- KTN-RM / Remaiten : Tsunami와 BASHLITE를 결합한 공격. 자체 리스트 내 사용자 id/pw 조합을 통해 로그인 과정을 수행하고 IoT 장비에 대한 brute-force 공격을 수행
- Mirai : DDoS IoT botnet malware. 시간당 4천여대의 IoT 장비를 감염. 1.1Tbps DDoS 공격 수행. CCTV, DVR, 홈 라우터를 대상으로 함. GRE IP, GRE ETH, SYN, ACK, STOMP, DNS, UDP, HTTP 트래픽 발생. MySQL/MS SQL 구동되는 서버에도 작동
- Linux/IRCTelnet : IPv6 호환 IoT 장비에서도 구동됨. IRC botnet ELF malware. 기존 malware들(Tsunami, BASHLITE, Mirai, LightAidra/Aidra) 조합 방식으로 구동되며, IPv4/IPv6 프로토콜 기반 UDP, TCP flooding 공격 수행
- Qbot : Bashlite, Gafgyt, Lizkebab, Torlus 등으로 알려짐. 다수의 하드웨어에서 구동되며, IRC 없이 TCP 기반 C&C 서버를 사용하여 최근의 변종인 경우 타 Botnet을 제거하는 기능도 포함함

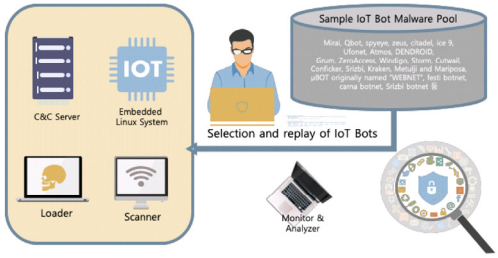
이를 통해 다음과 같이 요약 정리할 수 있다. 2008년 이후 최근까지 지속적으로 IoT 기기를 대상으로 한 공격이 계속되고 있다. 따라서 샘플 코드를 통한 IoT Botnet 재현 과정이 필요하고, 이를 통해서 IoT 해킹 공격에 대한 세부 동작 방식에 대한 분석이 필요하다. 그리고 이를 통해서 각각의 IoT 기기 내에서 획득 가능한 침해사고 흔적에 대한 수집 및 분석 방법 등에 대해 체계화할 필요가 있다.

4. IoT 기기 Botnet Malware 동작 분석

4.1 IoT 기기 Botnet Malware 동작 재현

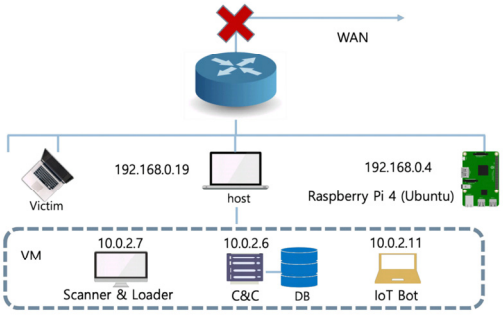
본 연구에서는 IoT 기기를 대상으로 한 Botnet Malware에 대한 침해사고 분석 방법을 수행하였다. 우선 인터넷에 공개된 샘플 형태의 IoT Botnet Malware 실행코드를 수집한 다음 IoT 기기를 대상으로 한 Botnet Malware 동작을 재현하였다.

아래 그림 1과 같이 샘플 IoT Botnet Malware Pool 내에서 Mirai Botnet[4]을 대상으로 IoT 기기에 대한 Botnet을 구성한 후에 해당 IoT 기기 내에서 생성되는 침해사고 흔적을 수집/분석하는 방법을 사용하였다.



[Fig. 1] Select IoT Botnet to be analyzed and replay its behavior

IoT 기기를 대상으로한 Botnet 재현을 위해 아래 그림2와 같이 실험 환경을 구축하였다. 외부 네트워크로의 피해를 차단하기 위해 폐쇄망을 구축한 후 Mirai Botnet Malware 동작 재현을 위한 C&C 서버, Scanner 및 Loader를 구현한 다음 Victim으로의 DDoS 공격이 수행하는 방식이다.



[Fig. 2] Network diagram to replay IoT Botnet

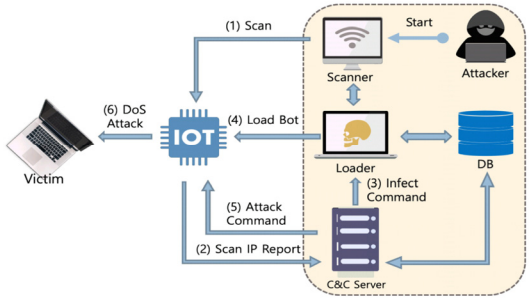
4.2 Mirai Botnet Malware 동작 메커니즘 분석

Mirai Botnet Malware에 대한 전체적인 동작 메커니즘을 도식화하면 공격자는 Scanner를 통해 네트워크 내 구동 중인 IoT 기기를 스캔한 후 기기에 대한 상세 정

보를 C&C 서버로 전송한 후, 해당 서버 내에 이미 저장된 ID/PW DB 정보를 사용하여 해당 기기에 대한 무작위 로그인 과정을 수행하게 된다. 만일 로그인이 성공하게 되면, 네트워크 접속을 통해 Mirai Bot Malware 코드를 해당 기기 내에 전송하여 감염시키는 과정을 진행하게 된다.

감염시키는 과정은 해당 장비에 대한 스캔 결과를 CNC 서버에 전송한 후에 CNC 서버는 해당 정보를 토대로 악성 바이러리를 전송하게 된다. 해당 IoT 장비 내에 Bot이 설치, 실행된 후에는 해당 바이너리를 삭제하고 바인딩된 프로세스를 종료하게 된다.

아래 그림 3과 같이 Scanner를 설치 및 구동하였을 경우 정상 작동하는 것을 확인할 수 있었다. 대상 타켓을 찾게되면 스캐너 모듈은 바로 다음 목표 호스트를 스캔하게 되며, 이후 scanListen 프로그램이 실행중인 C&C 서버로 스캔 내용을 전송하게 된다.

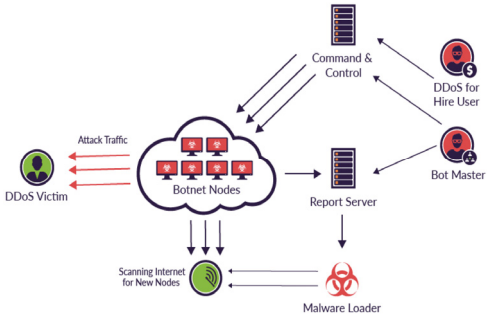


[Fig. 3] IoT Bot infection procedure diagram

따라서, Mirai Botnet 작동 메커니즘을 상세 분석하면 다음과 같다. Mirai Bot은 Self-propagating worm으로 자기 복제 과정을 반복하면서 IoT 장비를 감염시키는 악성코드로 감염된 IoT 기기는 C&C 서버에 의해 제어되는 특성을 보인다. 또한, Mirai IoT Bot은 Replication Module과 Attack Module의 두 개의 모듈로 구성되어 있다. 동작 과정을 살펴보면, (1단계) 관리자 계정설정이 취약한 임베디드 OS 기반 IoT 기기(공유기, CCTV, NAS 등)를 대상으로 스캐닝(Scanning) · 접속 과정을 수행한 후, (2단계) 악성코드 전파 및 감염, 취약한 기기 감염을 진행하고, (3단계) IoT 기기에 대한 감염을 점진적으로 확대하여 IoT 봇넷(Botnet)을 구성한 후 DDoS 공격을 수행한다. Mirai IoT Botnet 기반 해킹공격 전체 흐름도 및 DDoS 공격 동작 방식을 정리하면 다음과 같다.

- (1단계) Mirai Botnet 스캔 기능
  - Mirai Bot은 최초 실행시 네트워크 스캔 기능을 수행하는데, 랜덤 IT 주소를 생성하여 23번 포트(Telnet)으로 해당 IoT 기기에 대한 ID/PW 로그인에 사전식 전사공격(Brute Force Attack)을 시도함
- (2단계) Mirai Botnet 전파 기능
  - IoT 기기에 접속을 성공하면 미라이 악성코드를 주입하고, 실행하는 과정을 반복해 감염 장비를 확보한 후 거대한 Botnet을 형성함. 악성코드 주입시 Busybox(리눅스 기반 명령어 모음도구)를 주입하고 **wget 명령어를 이용하여 Mirai 악성코드를 다운받아 실행하여 전파 기능을 수행함
- (3단계) Mirai Botnet 기반 DDoS 공격 수행 기능
  - Botnet은 C&C(Command and Conquer) 서버에 접속하여 명령을 기다리고 있다가 공격 명령이 떨어지면 DDoS 공격을 수행함

IoT 기기를 대상으로 한 Botnet Malware 기반 전체 동작을 구도조로 표현하면 다음 그림 4와 같다.

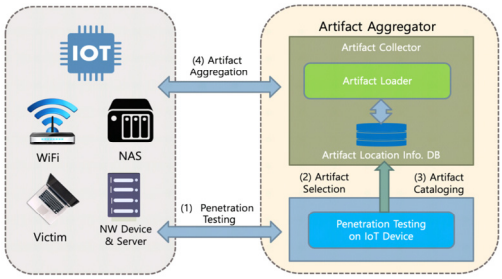


[Fig. 4] IoT Botnet Malware Flow diagram

5. IoT 기기 Botnet Malware 침해사고 흔적 수집 방법

5.1 IoT 기기 침해사고 흔적 수집기 개발

IoT 기기를 대상으로 한 Botnet Malware에 의해 침해사고가 발생하였을 경우 이에 대한 증거자료, 흔적을 수집 및 분석할 수 있어야 한다. 이에 본 논문에서는 아래 그림 5와 같은 방식으로 IoT 기기를 대상으로 한 Botnet Malware 침해사고 흔적을 수집하는 방법을 개발하였다.



[Fig. 5] Structure diagram of an intrusion artifact collector for IoT devices

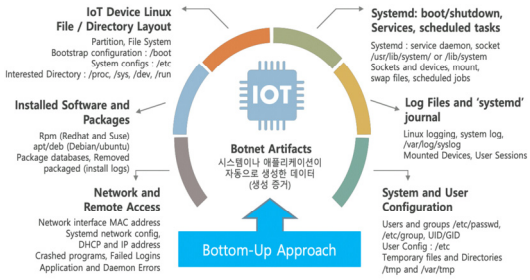
샘플 IoT Bot Malware를 선별하여 동작을 재현하는 등의 이른바 (1단계) IoT 기기에 대한 모의해킹 과정을 수행하여, (2단계) 해당 기기별 침해사고 흔적 대상을 선별하고, (3단계) 침해사고 흔적에 대한 발생 여부, 위치 및 침해사고 흔적을 목록화하여 이를 DB 형태로 저장한 후 이를 다양한 IoT 기기를 대상으로 확대한다. 이제 축적된 침해사고 흔적 위치 정보 DB를 토대로 만일 침해사고가 발생하게 되면 (4단계) IoT 기기별로 침해사고 흔적을 수집하고 이를 토대로 최종적인 분석 및 판별 과정을 진행하게 된다.

5.2 IoT 기기 침해사고 흔적 수집 절차

일반적인 공유기를 대상으로 한 침해사고 분석과 유사하게 IoT 기기에 대한 침해사고 흔적 분석을 위해서는 분석 대상이 되는 기기의 종류와 내부 정보를 식별하고, Live 데이터를 획득하여야 한다. 그런 다음에 내부 데이터 접근을 위한 관리자 권한을 획득한 후에 시스템 및 로그 정보를 수집하고, 네트워크 이벤트 분석을 통해 외부 접속 흔적이 있는 경우 Botnet 감염 여부를 판별하고 만일 감염되었을 경우 파일 및 폴더 등 내부 변경 정보를 수집한 후 부가적인 아티팩트 정보 등을 획득하여 최종적으로 해당 기기에 대한 침해사고 흔적을 수집하여야 한다[7,8].

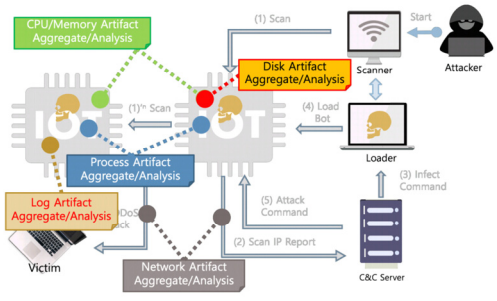
5.3 IoT 기기 침해사고 흔적 수집 결과

IoT 기기를 대상으로한 침해사고 흔적을 수집하기 위해서는 우선 기기 내부 프로세스 정보를 수집하고, 악성코드에 의해 활성화된 네트워크 트래픽 정보 등을 획득할 필요가 있다. 또한, IoT 기기 내부 시스템 정보와 각종 로그 정보 등을 획득할 필요가 있다. 이를 토대로 Mirai Bot에 의해 내부에 설치된 악성코드 등에 대한 흔적을 조사하고, 피해 시스템 내 생성된 로그 정보 등을 획득 및 분석하여 악성 Botnet Malware에 의한 감염 여부와 DDoS 공격 수행 등과 관련된 증거자료를 획득할 수 있게 된다. 따라서 아래 그림 6과 같은 Bottom-up 접근 방법을 사용해서 해당 IoT 기기 내 침해사고 흔적을 수집하는 방법을 사용하였다.



[Fig. 6] Target for collecting artifacts on IoT devices

대부분의 IoT 기기가 임베디드 리눅스 OS를 기반으로 구동[10]되기 때문에 내부 시스템 정보 등을 획득하여야 하고, 시스템 내부 구동되는 소프트웨어에 대한 정보와 해당 이벤트/시스템 로그 정보 등을 수집하여야 한다[11]. 또한 IoT 기기에 대한 설정 정보 및 네트워크 접속 등에 대한 정보를 수집해야 한다. 따라서 아래 그림 7과 같이 시스템 구성도 전체를 대상으로 각 부분별로 침해사고 흔적을 수집할 필요가 있다.

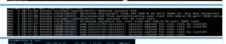
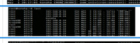
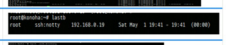


[Fig. 7] Structure diagram of collecting artifacts on IoT devices

Mirai Botnet Malware에 대한 동작 재현 결과 감염된 공유기로부터 수집된 주요 침해사고 흔적은 다음과 같다. syslog 내에 Mirai Botnet Malware에 의해 생성된 접속을 확인할 수 있었으며, auth.log인 경우 Bot에 의한 악의적인 로그인 접속 기록, 그리고 Malware 실행 및 감염을 위해 수행되었던 명령어 등에 대한 정보가

.ash_history 내에 기록되어 있음을 확인할 수 있었다. 이밖에도 다양한 형태의 침해사고 흔적 데이터가 생성됨을 확인할 수 있었다.

〈Table 1〉 Result of collecting traces of intrusion accidents from routers

Artifacts	Description	Note
Var/log/syslog	Record the entire system log (general Linux equipment)	
.bash_history	Check for system boot messages. Log kernel output messages to a certain level	
/var/log/auth.log	User login authentication record for Telnet/ssh connection	
last	record for latest connection	
lastlog	user's recent login IP record and access date by account	
lastb	failed login history	
.ash_history	Record the commands executed for infection	

5.4 기존 연구와의 비교 분석 및 평가

IoT 보안 우려가 급증하고 있는 반면에 침해사고 해킹 범죄 사범에 대한 검거율은 감소하고 있다. 경찰청이 발표한 해킹 발생 및 검거 현황에 따르면 2019년 해킹 범죄 발생 건수가 전년 대비 22.3% 늘어난 2664건으로 증가했다. 하지만 검거율은 2017년 40.7%에서 2020년 상반기에 17.6%로 감소하고 있다. 이는 IoT 관련 해킹 공격이 날로 지능화, 고도화 되고 있음을 의미하므로 IoT 기기를 대상으로 한 침해사고 대응 기술에 대한 연구가 시급한 실정이다. 따라서 IoT 기기에 대한 Botnet Malware 기반 침해사고가 발생하였을 경우 본 연구에서 제시한 기법을 이용할 경우 해당 기기내 침해사고에 대한 흔적을 수집 및 분석하는 과정에 매우 유용하게 사용될 것으로 예상된다.

본 연구에서 제시한 기법과 기존 연구를 비교하면 다음 표 2와 같이 차이점을 확인할 수 있다. 기존 연구[3,8]와 달리 본 연구에서 제시한 기법은 수집하는 침해사고 흔적과 IoT Botnet 자동 검출 기법에서 기존 기법과 차이점이 있음을 확인할 수 있었다.

또한 다양한 형태의 IoT 기기로부터 수집된 대단위 침해사고 흔적 데이터는 Botnet 공격 검출 성능을 향상키시고 침해사고 판별 과정에서의 수집된 데이터에 대한 유효성을 향상시키기 위해 규격화 및 정규화 과정을 수행할 필요가 있다[12,13]. 따라서, 본 연구에서는 해당 IoT 기기로부터 수집된 침해사고 흔적 데이터의 포맷에 따라 파서(Parser)를 적용한 후 JSON 파일 형태로 규격화하여 저장하는 방법을 적용하였다. 이를 통해서 향후 IoT 기기에 대한 침해사고 판별 과정에서 매우 유용하게 사용될 수 있을 것으로 기대된다.

〈Table 2〉 Comparative analysis results with existing studies

		IoT Botnet Detection [8]	IoT Botnet Forensics [3]	Proposed System
Used IoT Bot		Not Specified	Mirai Bot	Mirai Bot
Target IoT Device		Not Specified	Not Specified	Wireless AP
Artifacts	Scanner & Loader	×	○	○
	C&C Server	×	○	○
	MySQL DB Server	×	○	○
	Infected IoT Device	○	○	○
	Vulnerable IoT Device	○	○	○
	Network Packet	○	×	○
	Victim	○	×	○
IoT Botnet Auto-Detection		○	×	△
Artifact Management		×	Not Specified	JSON Format

6. 결론

최근 IoT와 모바일 통신 기기의 사용이 지속적으로 증가하면서 이를 악용한 사이버 범죄 위험이 점차 증가하고 있다. 이에 본 연구에서는 IoT 기기 대상 사이버 공격에 능동적으로 대응하기 위해 공공분야 시장 점유율이 높은 주요 IoT 기기를 대상으로 IoT 기기 관련 침해사고에 해당하는 디지털 포렌식 관련 침해사고 흔적을 수집하고, 이를 토대로 유효한 침해사고 분석 데이터셋을 구축하기 위한 방법론을 제시하였다. 구체적으로 Mirai Botnet과 같은 샘플 IoT 악성코드 동작 재현을 통해 취약점 발생 요인 파악 및 침해 시스템 내 주요 데이터 식별, 획득/분석 방법을 제시하였으며, 향후 샘플 악성코드를 중심으로 획득한 침해사고 흔적 데이터에 대한 유효성을 검증할 수 있는 기초 분석 데이터 셋을 구축할 수 있었다.

연구 결과를 토대로 앞으로 다기종 대량 IoT 장비 기반 대단위 네트워크에서 발생하는 다양한 형태의 이기종 다형상 침해사고 흔적 데이터를 규격화하여 저장하여 침해사고 분석 과정에 정확도를 향상시킬 수 있는 방법에 대한 연구를 수행하고자 한다. 그리고 IoT 기기로부터 획득된 침해사고 흔적 데이터에 대해 각각의 파일 포맷에 적합한 파서(Parser)를 적용하여 정규화된 형태로 통합 저장하고 이를 DB화 하여 침해사고 분석 및 판별 과정에서의 정확도를 더욱 더 향상시킬 수 있는 방법에 대한 연구를 수행하고자 한다.

REFERENCES

[1] I. Ali et al., "Systematic Literature Review on IoT-Based Botnet Attack," in IEEE Access, Vol. 8, pp. 212220-212232, 2020,

[2] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Vol. 22, No. 2, pp.1191-1221, SECOND QUARTER 2020.

[3] Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo. "IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers," Digital Investigation, Elsevier, Vol.32, pp.S1-S10, 2020.

[4] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, ''An in-depth analysis of the mirai botnet,'' in Proc. Int. Conf. Softw. Secur. Assurance (ICSSA), pp. 6-12, Jul. 2017.

[5] Anchit Bijalwan, Vijender Kumar Solanki, Emmanuel Shubhakar Pilli, "Botnet Forensic: Issues, Challenges and Good Practices," Network Protocols and Algorithms, Vol.10, No. 2, pp.28-51, 2018.

[6] Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Arif Ahmed, S. M. Ahsan Kazmia, Choong Seon Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," Future Generation Computer Systems · September 2018.

[7] Dongkwan Kim, Daeyong Jeong, Cheolsoo Lee, "A Study on Digital Forensic Process Model of Wireless Router," Journal of Digital Forensics, Vol.11, No.1, pp.17-35, 2017.

[8] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, L. Cheng, "Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research," Applied Science Vol.11, 5713, 2021.

[9] A. Alenezi, H. Atlam, R. Alsagri, M. Alassafi, and G. Wills, "IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions," Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2019), pages 106-115.

[10] Bruce Nikkel, "Forensic Artifacts in Modern Linux Systems," Bern University of Applied Sciences, https://digitalforensics.ch/nikkel18.pdf

[11] Weam Saadi Hamza, Hassan Muayad Ibrahim, Methaq Abdullah Shyaa, Jane J. Stephan, "IoT Botnet Detection: Challenges and Issues," Test Engineering & Management, Vol. 83, pp.15092-15097, 2020.

[12] X. Zhang, K. R. Choo and N. L. Beebe, "How Do I Share My IoT Forensic Experience With the Broader Community? An Automated Knowledge Sharing IoT Forensic Platform," IEEE Internet of Things Journal, Vol. 6, No. 4, pp. 6850-6861, Aug. 2019.

[13] Harichandran, Vikram & Walnycky, Daniel & Baggili, Ibrahim & Breitinger, Frank, "CuFA: A more formal definition for digital forensic artifacts," Digital Investigation. Vol.18, pp.S125-S137, 2016.

[14] Sun-Jib Kim, "A IoT Security Service based on Authentication and Lightweight Cryptography Algorithm," Journal of KIoTS. Vol.7, No.1, pp.1-7, 2021.

[15] Ho-Seung Kim, Chang-Won Choi, "A Degisn on Error Tracking System for Enhanced-Reliable IoT Service," Journal of KIoTS. Vol.6, No.3, pp.15-20, 2020.

이 형 우(Hyung-Woo Lee) [종신회원]

- 1994년 2월 : 고려대학교 컴퓨터학과 (학사)
- 1996년 2월 : 고려대학교 컴퓨터학과 (석사)
- 1999년 2월 : 고려대학교 컴퓨터학과 (박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

〈관심분야〉
사물인터넷, 정보보호, 모바일 보안 및 디지털 포렌식