

2019년도
한국정보보호학회

학술발표대회 논문집

- 일시 : 2019년 2월 14일(목)
- 주최 : 한국정보보호학회 영남지부/충청지부
- 주관 : 부산가톨릭대학교
- 후원 : (주)오픈링크시스템
(주)대신정보통신 (주)아이티센
- 장소 : 부산가톨릭대학교

행 사 일 정

■ 행 사 장 : 부산가톨릭대학교 정보공학관

□ 2월 14일(목요일)

시 간	행 사 내 용					
12:00- 13:30	등 록					
	부산가톨릭대학교 정보공학관					
	2층 202호	2층 205호	2층 206호	3층 302호	3층 305호	3층 306호
13:30- 14:30	A- 1 IoT/CPS /클라우드 보안	B- 1 IoT/CPS /클라우드 보안	C- 1 블록체인 /금융 보안	D- 1 인공지능 보안	E- 1 컴퓨터보안	F- 1 정보보호관리/정책 기타정보보호
14:30- 15:00	휴 식					
15:00- 16:00	A- 2 IoT/CPS /클라우드 보안	B- 2 모바일 보안 디지털포렌식	C- 2 블록체인 /금융 보안	D- 2 인공지능 보안	E- 2 컴퓨터보안	F- 2 컴퓨터보안
16:00- 16:30	휴 식					
16:30- 18:00	□초청강연: 2019년 보안 트렌드 (장소: 대학본부관 103호 대강의실) - 강 사: 이호웅 안랩 CTO □한국정보보호학회 영남지부 총회 및 폐회					

목 차

Session A-1 IoT/CPS/클라우드 보안 (정보공학관 202호)

13:30 ~ 14:30 좌장 : 김호원 (부산대)

- OCF 장치를 비 OCF 장치로 연결하기 위한 OCF 게이트웨이 보안
Naufal Suryanto, 김호원 (부산대) ----- 3
- IoT-DNS 네트워크 보안기법 분석
Ismail, 김현곤, 김호원 (부산대) ----- 6
- 클라우드 오토-스케일링 시스템 구축에 관한 연구
손현민, 최성철, 최현택, 이현철 (대신정보통신) ----- 9
- Wireless Sensor Network 환경에서의 윈도우 기반 에너지 소모량 예측을 통한
이상 노드 탐지 기법
신진명, 최석환, 최윤호 (부산대) ----- 12

Session A-2 IoT/CPS/클라우드 보안 (정보공학관 202호)

15:00 ~ 16:00 좌장 : 이임영 (순천향대)

- 클라우드 스토리지 환경에서 공모공격을 방지하는 ID 기반 프록시 재암호화 기술
김원빈, 이임영 (순천향대) ----- 18
- 하드웨어를 공유하는 LEA 및 HIGHT 블록 암호 저면적 구현 기법
김보훈 박종선 (고려대) ----- 21
- 최신 IoT 악성코드의 침해사례 및 특징 분석
정해선, 최슬기, 박진 (아주대) ----- 24
- 효율적인 데이터 공유를 위한 CP-ABE 접근제어 기법에 관한 연구
황용운, 이임영 (순천향대) ----- 27

Session B-1 IoT/CPS/클라우드 보안 (정보공학관 205호)

13:30 ~ 14:30 좌장 : 김정태 (목원대)

- Inversionless Berlekamp-Massey Algorithm을 이용한 BCH 부호의 하드웨어
구현
Asep Muhamad Awaludin, 윤영여, 김호원 (부산대) ----- 33
- 클라우드 보안 취약점 분석에 관한 연구

최신 IoT 악성코드의 침해사례 및 특징 분석

정해선*, 최슬기**, 곽진***

***아주대학교 사이버보안학과

**정보보호응용및보증연구실, 아주대학교 컴퓨터공학과

*haeseon@ajou.ac.kr, **skchoi.isaa@gmail.com, ***security@ajou.ac.kr

Case and Feature Analyses of The Latest IoT Malware

Hae-Seon Jeong*, Seul-Ki Choi**, Jin Kwak***

*,***Department of Cyber Security, Ajou University

**ISAA Lab., Department of Computer Engineering, Ajou University

요 약

IoT 기기의 수요는 계속해서 증가하고 있고 많은 분야에서 사용되고 있다. 하지만 IoT 기기에 대한 보안 규정 및 보안 설정 등에 대한 가이드라인이 명확하지 않아 많은 보안 문제가 존재한다. 공격자들은 이러한 IoT 기기의 취약점을 이용해 다양한 악성코드를 만들어 공격을 시도하고 있다. 더욱 정교화·고도화되고 있는 악성코드로부터 더 안전한 IoT 환경을 구축하기 위해, 본 논문에서는 최신 악성코드 사례분석을 통해 다양한 IoT 악성코드들의 공격 과정, 특징을 분석하고 대응방안 및 IoT 보안 연구의 필요성을 기술하고자 한다.

I. 서론

IoT(Internet of Things)는 전 세계적으로 보급되고 있으며, 2019년에는 142억 개의 IoT 기기가 사용될 것이라 예상된다[1]. 하지만 IoT 기기에 대한 보안 규정이나 표준이 부재하여 기본 암호 정책, 접근 제어 권한, 보안 구성과 같은 설정들이 미흡하여 다양한 보안 취약점들이 존재하고 있다[2]. 따라서, 최근에는 IoT 기기를 대상으로 하는 신·변종 악성코드들이 증가하고 있다. 카스퍼스키랩에서 2018년 09월에 발표한 자료에 의하면 2018년 상반기에 발생한 IoT 관련 악성코드의 수가 2017년에 발생한 전체 악성코드의 약 3배가량 증가한 것을 확인할 수 있다[3].

본 논문에서는 최신 IoT 악성코드

사례분석을 통해 악성코드의 동작 방식과 공격 목적 등의 특징을 분석하고, IoT 기기에 대한 보안의 필요성과 대응방안을 제시한다.

II. 최신 IoT 악성코드 사례분석

2.1 Mirai

2016년 10월 21일, IoT 기기를 대상으로 하는 Mirai 악성코드는 미국의 DNS 업체인 Dyn에 대규모 DDoS 공격을 수행하여 트위터, 넷플릭스 등 총 76개의 사이트를 마비시키거나 서비스를 지연시키는 사건을 발생시켰다[4].

이러한 Mirai 악성코드는 Mirai bot, C&C server, scan receiver, loading server로 구성되어 있다[5].

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2017R1E1A1A01075110).

2.1.1 Mirai의 동작 과정[5][6]

- ① Mirai는 원격에서 접근 가능한 서비스인 Telnet(23번 포트), SSH(22번 포트)를 스캔해서 해당 포트가 열려있는 기기를 검색
- ② 해당 서비스가 열려있는 경우, 공장 출하 시 설정되어있는 많은 초기 계정 정보들을 대입하는 사전식 전사공격 수행
- ③ 구매 후 초기 계정 정보를 변경하지 않은 IoT 기기들에 대하여 Shell에 접근
- ④ 기기 접근이 성공하고 나면 Scan receiver로 공격에 성공한 기기의 IP주소, 계정 정보를 전송하고, scan receiver는 받은 정보를 loading server로 다시 전송
- ⑤ loading server에서는 busybox의 “wget, tftp, ECCHI, echo -ne” 명령어로 Mirai 바이너리를 기기에 다운로드
- ⑥ 바이너리 실행 시 기존 telnet, SSH 서비스를 kill하고 restart하여, C&C(Command&Control) server에서 Telnet, SSH 포트를 통해 명령을 전송
- ⑦ C&C server는 또 다른 취약한 기기를 찾기 위하여 ①~⑦의 과정을 반복하거나 DDoS 공격을 수행

Mirai의 위와 같은 자기 복제 방법은 거대한 봇넷을 형성할 수 있었으며, 이를 대규모 DDoS 공격을 수행하는데 활용할 수 있었다[5].

2.1.2 Mirai 변종 악성코드

2016년 9월 20일 Mirai의 소스코드가 공개된 이후, 많은 Mirai 변종 악성코드들이 꾸준히 발견되고 있다[4]. 그중에서도 Satori는 2017년 11월에 최초 발견되었으며, 2018년에 발생한 IoT botnet 악성코드 중에서 53%를 차지하였다[6].

현재 Satori 악성코드에 대한 소스코드가 공개되어 있으며, Satori 악성코드는 사전식 전사공격이 아닌 알려진 원격 코드 실행 취약점을 이용하여 기기에 접근한다. Satori 악성코드는 스캐닝을 수행하지 않고 37215번 포트와 52869번 포트로 원격 접속을 시도한다. 따라서 웜처럼 자기 자신을 스스로, 빠르게 전파할 수 있는 특징을 가지고 있다[7].

2.2 VPNFilter

VPNFilter는 2018년 상반기에 CISCO Talos 팀에서 처음 발견한 악성코드로, 다단계 모듈형 플랫폼이다. 다양한 네트워킹 장치를 공격대상으로 삼고 있는 VPNFilter는 사용자의 중요 정보뿐만 아니라 ICS(Industrial Control System) 패킷을 수집하고, 자신의 흔적을 지우고, IoT 기기를 무력화시키는 등의 공격을 수행한다. 이러한 VPNFilter는 크게 3단계의 순서로 공격을 수행한다.

- 단계 1: linux crontab job scheduler에 자신을 기록하고, 기기의 비휘발성 메모리를 조작해서 재부팅을 해도 남아있도록 하며, 다음 단계를 위해 C&C 서버의 주소를 가져온다[8].
- 단계 2: C&C 서버 접속 시 필요한 JSON 객체를 만들고 접속한다.
- 단계 3: 공격에 필요한 많은 기능을 포함하고 있는 여러 모듈을 추가한다[7-9].

[표 19] VPNFilter에서 사용하는 공격 모듈

모듈 이름	모듈 기능
dstr	기기에 있는 VPNFilter의 흔적을 지우고 사용 불가능하게 함
ps	150bytes이상의 패킷과 ICS 트래픽 수집
ssler	80번 포트(TCP)로 가는 모든 서비스를 로컬 서비스로 리다이렉트해서 sslstrip →이를 통해 중요 계정 정보를 추출하고, 웹 트래픽에 악성코드를 삽입할 수 있어, 이는 감염된 기기에 연결되어 있는 네트워크를 감염시킬 수 있음을 의미
htpx	ssler과 비슷하게 http 통신을 검사해서 윈도우 실행 파일 존재 여부 확인, 공격자가 손상된 기기를 통과할 때 윈도우 실행 파일을 즉시 패치 할 수 있게 함
ndbr	다기능 SSH 유틸리티
nm	손상된 기기의 로컬 서브넷을 스캔하고 매핑
netfilter	서비스 거부 유틸리티
portforwarding	네트워크 트래픽을 특정 인프라에 포워딩
socks5proxy	손상된 기기에 SOCK5 프록시 생성
tcpvpn	손상된 기기에 역-TCP VPN으로 원격 공격자가 기기 내 네트워크로 접속하게 해줌

VPNFilter는 [표 1]의 모듈을 이용하여 감염된 기기에서 다른 기기에 코드 삽입을 통해 공격할 수 있고, 프록시를 사용하기 때문에 실제 공격 근원지 파악이 어렵다. 또한, C&C 서버와 데이터추출 트래픽을 난독화·암호화하여 공격에 대한 탐지를 어렵게 한다[10]. 하지만 아직도 VPNFilter가 기기에 초기 접근을 어떤 방식으로 수행하는지 명확하게 알려진 바는 없다.

III. IoT 악성코드의 특징 분석

□ IoT botnet을 활용한 DDoS 공격 수행

감염된 기기는 C&C 서버의 명령에 따라 특정 대상을 공격하는 봇넷의 일부가 되어 DDoS 공격을 수행하게 된다.

□ 감염된 IoT 기기를 숙주로 악용

IoT 기기가 악성코드에 감염되고 나면, 다른 취약한 기기를 스캔하거나 연결된 네트워크를 공격할 수 있다.

□ IoT 기기를 통한 정보 탈취

패킷을 수집하고 개인 식별 정보 등의 주요 정보를 공격자의 서버에 전송한다. 또한, 기기가 연결되어있는 네트워크의 정보 또한 수집한다.

□ IoT 기기를 통한 ICS 정보 수집

ICS 패킷을 수집하여 ICS 보안에 상당한 위협을 제공한다.

□ IoT 기기 무력화

재부팅을 수행해도 악성코드가 삭제되지 않고, 펌웨어의 값을 덮어쓰워 기기를 무력화한다.

□ 공격 트래픽 추적의 어려움

C&C 서버와 데이터추출 트래픽을 난독화·암호화하고, VPN을 사용하여 공격 근원지 파악을 어렵게 한다.

IV. 대응방안 및 결론

대부분의 IoT 악성코드들이 기기에 접근하기 위한 방식으로 사용하고 있는 사전식 전사공격은 2018년 상반기 기준으로 기기 접근방식의 약 90%를 차지하고 있다[3]. 따라서, 사용하지 않는 포트를 닫고, 공장 출하 시 설정된 초기 계정을 변경하는 것만으로도 일정 수준으로 악성코드 감염을 방지 할 수 있다.

또한, 주기적으로 기기를 재부팅·초기화함으로써 악성코드를 제거해주는 방법도 악성코드 감염을 방지할 수 있는 효과를 가져올 수 있으며[10], 이미 알려진 취약점을 이용하는 악성코드들을

방지하기 위하여 기기의 펌웨어를 최신 버전으로 업데이트하는 것이 필요하다.

하지만, 최근에 발생하고 있는 신변종 IoT 악성코드들은 재부팅에 저항성을 갖고 있으며, ICS 패킷도 수집하고 직접 감염된 IoT 기기 외에 그와 연결된 기기에도 코드를 삽입하는 등 정보 수집 및 공격 기술이 점점 더 정교화되고 있다. 또한, 감염된 기기를 무력화시킴으로써 그 피해를 증가시키며, 공격 트래픽을 난독화, 암호화하거나 프록시를 사용함으로써 공격 경로를 쉽게 추적하지 못하게 하는 등 악성 행위들이 지속적으로 고도화되고 있다.

따라서, 지속적으로 발전하고 있는 악성코드들로부터 안전한 IoT 환경을 보장하기 위하여 IoT 기기 보안에 대한 다양한 연구들이 필요하다.

[참고문헌]

- [1] Gartner, "Gartner Identifies Top 10 Strategic IoT Technologies and Trends", Nov 2019.
- [2] Infosec, "The Top Ten IoT Vulnerabilities", Feb 2018.
- [3] Kaspersky lab, "New trends in the world of IoT trends", Sep 2018.
- [4] Manos Antonakakis and others, "Understanding the Mirai botnet", 26th USENIX(Security 17), Aug 2017.
- [5] McAfee, "McAfee Labs Threats Report", Apr 2017.
- [6] SK infosec, "2019 보안 위협 전망 보고", Sep 2019.
- [7] Trend Micro, "Source Code of IoT Botnet Satori Publicly Released on Pastebin", Jan 2018.
- [8] CISCO Korea Blog, "전 세계 50만 대의 네트워크 장비를 공격한 신종 VPNFilter 악성코드", <https://ciscokrblog.com/1323>, May 2018.
- [9] CISCO Talos, "VPNFilter Update - VPNFilter exploits endpoints, targets new devices", Jun 2018
- [10] CISCO Talos, "VPNFilter III: More Tools for the Swiss Army Knife of Malware", Sep 2018.
- [11] 한국인터넷진흥원(KISA), "2019년 7대 사이버 공격 전망", Dec 2018.