정 보 보 호 학 회 지
제 31 권 제6호, 2021. 12

IoT 환경에서의 취약점 악용 공격 대응을 위한 익스플로잇 수집 및 분석

오 성 택*, 고 웅**

요 약

홈, 산업 환경, 운송 네트워크 및 기타 장소의 사물 인터넷 장치가 계속 확산됨에 따라 악의적인 IoT 네트워크 공격자의 공격 표면도 증가하고 있다. 2021년 4월 IBM에 따르면 네트워크 공격 지표 중 전체 IoT 공격이 매년 500% 증가하고 있다. X-Force 연구에 따르면 이 급증은 주로 미라이 봇넷과 코드를 공유하는 비교적 새로운 봇넷인 Mozi 봇넷 활동에 의해 발생한다. 2020년에 이 악성코드는 한 해 동안 탐지된 총 IoT 공격의 89%를 차지했다. 2020년 3월 팔로알토 네트웍스의 Unit 42 IoT Threat Report에 따르면 IoT 임베디드 기기 대상 위협은 익스플로잇 감염, 멀웨어, 사용자 정보 탈취로 나뉜다. 그 중 IoT 임베디드 기기의 주요 익스플로잇은 네트워크 스캔, RCE, Command injection, Buffer Overflow 등으로 관찰된다. 본 논문에서는 이러한 IoT 환경에서의 취약점 악용 공격 대응 및 탐지 정책 생성을 위해 IoT 취약점을 악용한 익스플로잇을 분석 연구하였다.

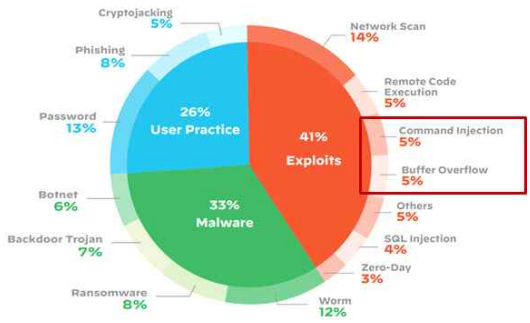
Ⅰ. 서 론

사물인터넷 기술의 발전과 더불어 전 산업영역 및 일상생활에 사물인터넷 장치의 보급이 증가하면서 관련 시장이 급격히 확대되고 있다. 시장조사업체 IHS 마킷 사물인터넷 커넥티비티 부문 선임 수석 애널리스트 줄리안 왓슨은 2017년 278억 개 디바이스에서 연평균 12% 성장하여 2030년 1,350 억 개로급사물인터넷 장치 시장의 폭발적인 성장을 예상하였다. 하지만 리소스가 제한된 사물인터넷 장치의 특성상 보안 내재화가 어려워 수많은 취약점 등을 악용한 위협이 지속적으로 증가할 것이다. KT 경제경영연구소에 따르면 2030년 국내 사물인터넷 해킹 피해액만 26조 7천억에 달한다고 분석하였다. 이러한 해킹 공격에 대응하기 위해 국내에서는 한국인터넷진흥원이 사물인터넷 제품의 보안 내재화를 위한 '사물인터넷 공통 보안원칙'을 발표하며 하드웨어 및 소프트웨어 전반에 걸친 보안 가이드라인을 제시하고 있다. 미국의 경우 사물인터넷 관련 보안 법을 통해 사물인터넷 기기에 보안 기능 탑재를 법적으로 규정하고 있다. 하지만 기존에 유통된 대다수의 기기는 보안이 취약한 상태로 사용되고 있으며, 장치를 사용하는 사용자의 기기 보안에 대한 인식 및 지식이 부족하여 자신의 기기가 감염되었는지 확인이 어려우며 대응 또한 쉽지않다. 본 논문에서는 이러한 보안 내재화 및 사용자 대응이 어려운 사물인터넷 환경의 알려진 취약점을 악용한 공격에 대응하기 위해 관련한 취약점과 익스플로잇을 분석하고 대응하기 위한 기술을 제안하였다.

Ⅱ. IoT 익스플로잇 현황

본 논문에서는 IoT 임베디드 기기 대상 익스플로잇 현황을 파악하기 위해 두 가지 조사 결과를 정리하였다. 2020년 3월 팔로알토 네트웍스의 Unit 42 IoT Threat Report[1]에 따르면 IoT 임베디드 기기 대상 위협은 익스플로잇 감염, 멀웨어, 사용자 정보 탈취로 나눌 수 있다. 그 중 IoT 임베디드 기기의 주요한 익스플로잇은 네트워크 스캔, RCE, Command injection, Buffer Overflow 등으로 관찰되었다. 기기 취약성을 통한 익스플로잇 감염의 대부분은 장치 네트워크의 다

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00232, 클라우드 기반 IoT 위협 자율 분석 및 대응 기술개발)
* 한국인터넷진흥원 침해대응기술팀 (선임연구원, angelrick@kisa.or.kr)
** 한국인터넷진흥원 침해대응기술팀 (책임연구원, wgo@kisa.or.kr)



〔그림 1〕 사물인터넷 위협 분류

른 시스템을 공격하기 위한 측면 이동(Lateral movement)의 목적으로 사용된다. 먼저 네트워크에서 많은 수의 네트워크 스캔, IP 스캔, 포트 스캔 및 취약점 스캔을 통해 다른 기기와 시스템을 식별하려고 시도하고 측면 이동의 다음 단계를 위한 대상을 찾는다. 취약한 기기를 발견 후 초기 액세스 권한을 얻기 위해 Command injection, Buffer Overflow 등과 같은 공격을 시도한다.

2008년부터 2020년까지 27개의 IoT 멀웨어를 조사한 논문[2]에 따르면 초기 IoT 멀웨어는 브루트 포스 공격을 이용하며 취약점을 거의 악용하지 않았으나, 2016년부터 감염 전략의 일환으로 취약점 사용이 보편화되었다고 한다. IoT 멀웨어 개발자가 익스플로잇에 자주 사용하는 상위 6개 CWE 유형은 CWE-20(부적절한 입력 검증), CWE-77(명령어 인젝션), CWE-78(OS 명령 주입), CWE-94(부적절한 코드 삽입), CWE-119(메모리 버퍼 오류) 및 CWE-287(부적절한 인증 오류)이다. 이는 전체 취약점의 67%를 차지하며 이러한 6가지 CWE는 모두 입력 유효성 검사 오류 또는 인증 오류이다.

〔표 1〕 CWE 익스플로잇 비율

CWE	Proportion in IoT malware	Proportion in NVD
CWE-20	9.2%	1.1%
CWE-77	14.9%	2.5%
CWE-78	23.0%	8.6%
CWE-94	5.7%	0.5%
CWE-119	6.9%	12.5%
CWE-287	6.9%	2.1%

[표 1]은 가장 많이 악용된 6가지 CWE를 보여준다. 위의 두 가지 조사 결과를 바탕으로 IoT 임베디드 기기 익스플로잇에 사용되는 위협 및 취약점 유형의 비율을 파악했다. 그 결과 <입력 유효성 검사 오류>를 이용한 익스플로잇 사례에서 Command injection이 높은 비율을 차지하는 것을 알 수 있다.

Ⅲ. IoT 익스플로잇 동향

스마트홈, 스마트공장, 산업 환경, 운송 네트워크 및 기타 여러 분야에 사물인터넷(IoT) 장치가 지속적으로 보급됨에 따라 악의적인 IoT 네트워크 공격자의 공격 표면도 증가하고 있다.2021년 4월 IBM 선임 위협 연구원 Dave McMillen[3]에 따르면 네트워크 공격 지표는 전체 IoT 공격이 매년 500% 증가하고 있다고 한다.

N	CVE	CWE	CVSS(2	CVSS(3	Exploit code	Infected device	Attack type	Malware	Descript	Payload
1	CVE-2005-0116	CWE-20	7.5		EDB-9912	AWStats(~6.3)	Command Injection - '|'	Echobot(19)	AWStats 6	https://dl.packetstormsecurity.net/0501-exploits/AWStatsV
2	CVE-2005-2773	Other	7.5		EDB-16887	HP OpenView Network No	Command Injection - '|'	Echobot(19)	HP Open\	https://www.securityfocus.com/archive/1/409179GET /OvC
3	CVE-2005-2847	Other	7.5			barracuda_spam_firewall:3.	Command Injection - Crafted GET Request	Echobot(19)	펌웨어 3.1	https://marc.info/?l=bugtraq&m=112560044813390&w=2
4	CVE-2005-2848	Other	5		EDB-1236	Barracuda Spam Firewall fi	Information Disclosure - LFI	Echobot(19)	펌웨어 3.1	https://www.exploit-db.com/exploits/1236GET $img?f=%2
5	CVE-2006-2237	Other	5.1		EDB-1755, EDB-9909	AWStats(6.4,6.5)	Command Injection - '|'	Echobot(19)	통계 업데	GET /cgi-bin/?migrate=|echo;cat /etc/hosts;echo|awstats1
6	CVE-2006-4000	Other	4		EDB-28321	Barracuda Spam Firewall v	Path Traversal - File Access	Echobot(19)	Barracuda	GET /cgi-bin/preview_email.cgi?file=/mail/mlog/lcd; /tmp
7	CVE-2007-3010	CWE-20	10		EDB-10031, EDB-168	Alcatel-Lucent OmniPCX E	Command Injection - ';'	Echobot(19)	Alcatel On	https://marc.info/?l=full-disclosure&m=119002152126755
8	CVE-2008-3922	CWE-94	9.3		EDB-6368, EDB-1732	AWStats Totals(~1.14)	Command Injection - Crafted GET Request	Echobot(19)	AWStats T	GET /awstatstotals.php?sort=%7b%24%7bpassthru%28/bi
9	CVE-2008-4873	noinfo	10		EDB-6864	Vacron NVR RCE	Command Injection - '|'	Mozi(20)	Sepal SPB	GET /cgi-bin/spboard/board.cgi?id=ors1&number=908.cg
10	CVE-2009-0545	CWE-20	10		EDB-8023	ZeroShell 'CGI-bin/kerbyn	Command Injection - ';'	Echobot(19)	ZeroShell	GET /cgi-bin/kerbynet?Section=NoAuthREQ&Action=x50
11	CVE-2009-2288	CWE-78	4.5		EDB-9861, EDB-169	nagios(~3.1.1)	Command Injection - ';'	Echobot(19)	3.1.1 이전	GET /nagios/cgi-bin/statuswml.cgi?ping=173.45.235.65%3
12	CVE-2009-2765	CWE-20	8.3		EDB-9209, EDB-100	DD-WRT 24 sp1	Command Injection - ';'	Echobot(19)	DD-WRT 2	GET /cgi-bin/;echo -ne ₩₩x00₩x00ncat -v -l -p 7777 -e /t
13	CVE-2009-5149	CWE-255	4.3			Arris DG860A, TG862A, an	Authentication Bypass - Predictable Creden	Hajime(16)	펌웨어 TS	https://github.com/borfast/arrispwgen
14	CVE-2009-5156	CWE-77	10	9.8	BID-35153	ASMAX Ar-804gu	Command Injection - Crafted GET Request	Echobot(19)	ASMAX AI	GET /cgi-bin/script?system%20whoami Host: 154.251.89.8
15	CVE-2009-5157	CWE-77	9	8.8		Linksys WAG54G2 1.00.10	Command Injection - ';'	Echobot(19)	Linksys W	https://www.securityfocus.com/archive/1/503934GET /setu
16	CVE-2010-5330	CWE-77	5	9.8	EDB-14146	Ubiquity Nanostation5 (Al	Command Injection - ';'	Echobot(19)	Ubiquity N	GET /stainfo.cgi?ifname=eth0;cat%20/tmp/system.cfg|greg
17	CVE-2011-3587	noinfo	9.3		EDB-18262	Plone 4.0 (through 4.0.9);	Command Injection - Request Parameter	Echobot(19)	Plone 4.0.	GET /p_/webdav/xmltools/minidom/xml/sax/saxutils/os/p
18	CVE-2011-4723	CWE-310	6.8			D-Link DIR-300	Information Disclosure - Credentials - Clear	VPNFilter(18)	D-Link Dil	https://www.securitylab.ru/lab/PT-2011-30
19	CVE-2011-5010	CWE-264	10		EDB-18172	CTEK SkyRouter 4200/430	Command Injection - Request Parameter	Echobot(19)	CTEK SkyF	POST / HTTP/1.1 global: true url: /apps/a3/cfg_ethping.cg
20	CVE-2012-0262	CWE-94	10		EDB-41687	op5 Monitor(5.3.5~5.5.0)	Command Injection - '"'	Echobot(19)	op5 Monit	
21	CVE-2012-1823	CWE-20	7.5		BID-53388, EDB-188	PHP 5.3.12/5.4.2	Command Injection - Crafted GET Request	Darlloz(13)	CGI 스크립	https://hackability.kr/entry/ApachePHP-5x-Remote-Code-
22	CVE-2012-2311	CWE-89	7.5		EDB-18834, EDB-188	PHP(~5.3.13, 5.4.x~5.4.3)	Command Injection - Crafted GET Request	Darlloz(13)	CGI 스크립	POST /?-dallow_url_include%%3don+-dauto_prepend_file
23	CVE-2012-2335	CWE-264	7.5			PHP 5.3.12/5.4.2	Command Injection - Crafted GET Request	Darlloz(13)	php-wrap	https://bugs.php.net/bug.php?id=61910GET /index.php?-s
24	CVE-2012-2336	CWE-20	5		EDB-18834, EDB-188	PHP(~5.3.13, 5.4.x~5.4.3)	Denial of Service - Crafted POST Request	Darlloz(13)	CGI 스크립	POST /cgi-bin/php/%63%67%69%6E/%70%68%70%2D%6
25	CVE-2012-4869	CWE-94	7.5		EDB-18649, EDB-186	FreePBX 2.9, 2.10	Command Injection - Crafted GET Request	Echobot(19)	FreePBX 2	GET /recordings/misc/callme_page.php?action=c&callmer
26	CVE-2013-5958	CWE-119	10		EDB-24455, EDB-401	UPnP Service ~1.6.18(e.g.	Buffer Overflow , Stack Overflow	VPNFilter(18)	1.6.18 이전	M-SEARCH * HTTP/1.1\r\nHOST: 239.255.255.250:1900\r\n

〔그림 2〕 IoT 위협 분류

X-Force 연구에 따르면 이 급증은 주로 미라이와 코드를 공유하는 비교적 새로운 봇넷인 Mozi 봇넷 활동에 의해 발생한다. 2020년에 이 악성코드는 한 해 동안 탐지된 총 IoT 공격의 89%를 차지했다. 현재 많은 IoT 봇넷은 공개된 미라이 코드 기반으로 수많은 변종이 발견되었다. 그 중 Mozi는 미라이 변종이지만 Gafgyt 및 IoT Reaper의 코드 스니펫과 자체 코드로 구성되었다. Mozi는 2019년 말에 라우터와 DVR을 대상으로 처음 발견되었다. 멀웨어는 분산 해시 테이블 프로토콜을 사용하여 DDoS 공격, 페이로드 실행 및 원격 명령 실행에 활용할 수 있는 봇의 P2P 네트워크를 구축한다. Mozi가 크게 확산되었던 주된 이유는 가장 일반적인 공격 벡터 중 하나인 Command injection 기술을 주로 사용하기 때문이다. IBM이 관찰한 거의 모든 IoT 타겟팅은 Command injection 공격을 사용하여 장치에 대한 초기 액세스 권한을 얻으려고 시도했다고 한다. 대상 엔드 포인트가 IoT 장치이고 이러한 공격에 취약한 경우 페이로드가 다운로드 되고 실행된다. CMDi 공격은 여러 가지 이유로 IoT 장치에서 매우 자주 사용된다. 첫째, IoT 임베디드 시스템에는 일반적으로 웹 인터페이스와 펌웨어 개발에 쓰인 디버깅 인터페이스를 통해 익스플로잇이 가능하다. 둘째, IoT 웹 인터페이스에 내장된 PHP 모듈을 악용하여 공격자에게 원격 실행 기능을 제공할 수 있다. 셋째, 관리자가 예상되는 원격 입력을 삭제하여 인터페이스를 강화하지 못하기 때문에 IoT 인터페이스는 배포 시 취약한 상태로 남아있는 경우가 많다. 이를 통해 공격자는 ‘wget’과 같은 쉘 명령을 입력할 수 있다.

Ⅳ. IoT 익스플로잇 수집

4.1. IoT 기기 및 서비스 키워드 생성

IoT 기기 및 서비스 키워드를 생성하기 위해 다양한 채널에서 IoT 키워드를 수집하였다. 해당 정보는 nmap os list, techinfodepo.shoutwiki.com, wikidevi.wi-cat.ru, zoomeye를 통해 임베디드 시스템 기기 및 서비스 키워드를 수집하고 조합하여 검색 키워드로 생성하였다. 이때 중복되거나 ‘linux’, ‘redhat’, ‘debian’과 같이 기기 성격의 범위가 큰 키워드의 경우 데이터 신뢰성을 위해 제외하였다.

4.2. IoT 취약점 수집

3.1에서 생성된 키워드를 통해 IoT 취약점(CVE ID)을 수집한다. 최초에 IP Camera용 취약점을 파싱하여 저장한다. 그리고 NVD에서 제공하는 연도별 취약점(CVE ID)을 저장한다. 우선 수집된 IoT 기기 및 서비스 키워드에서 Vendor 정보를 추출하고 연도별 취약점 파일의 CVE ID와 일치하는 취약점 정보들을 분류한다. 이 과정에서 ‘windows’, ‘microsoft’, ‘apple’ 등 기기 성격의 범위가 큰 키워드는 제외한다.

4.3. IoT 익스플로잇 코드 수집

생성된 키워드 및 nvd 연도별 취약점 정보를 통해 exploit-db.com의 IoT 익스플로잇 코드(EDB ID)를 수집한다. IoT 키워드와 일치하는 모든 데이터를 수집하고 수집된 정보의 CVE ID와 EDB ID를 확인한다. 확인된 모든 익스플로잇 정보(PoC 코드 등)를 수집 및 저장한다.

4.4. IoT 익스플로잇 공격유형 분류

모든 수집된 정보는 연구를 통해 수동으로 추출한 공격유형 별 선정된 키워드를 통해 공격유형을 분류한다. CWE 정보를 기준으로 1차 분류하였으며, 페이로드의 특징 정보를 기준으로 2차 세부 분류하였다. 추가로 1차 공격유형만 분류된 Exploit Code의 경우 수동으로 분류하였다. 21년 10월 기준 총 44,412개의 Exploit code를 수집하였으며, 이 중 IoT 관련된 12,339개의 익스플로잇을 256종으로 세부 분류하였다[그림 3].

4.5. 미라이 변종 공격유형

위 과정에서 미라이 변종을 추가 분석하였으며, 이를 통해 미라이 변종과 관련하여 107개의 EDB-ID를 수집하였다. 미라이 공격의 경우 Scanning Phase, Infection Phase, Control Phase 3개의 공격단계를 구분할 수 있다. 수집된 107개 EDB-ID는 Scanning Phase 3개, Infection Phase 86개, Control Phase 0개, 미분류 18개로 분류하였다. 이를 별도의 20종의 공격유형으로 분류하였으며 이는 [그림 4]와 같다.

Total Exploit code num : 44,412

CVE/CWE이 없는 Exploit code 대상 공격유형 추가 완료

Exploit-db.com

about IoT : 12,339

- CVE : 28,797
- CWE : 203

보안 위협 범위

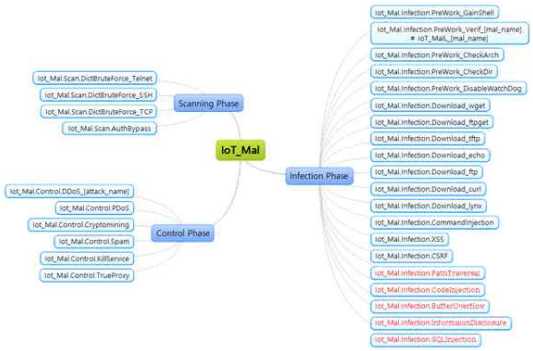
1. CWE 기반 IoT 공격유형(CWE 분류-Type A) 대분류 : 18종

SQL Injection	File Inclusion	Authentication Bypass	Cross-Site Scripting	Path Traversal	Denial of Service	Buffer Overflow	Information Leak	Cross-Site Request Forgery	Privilege Escalation	Code Injection	Security Bypass	Command Injection	URL Redirect	Wireless Attack	CRLF Injection	Sever-side request forgery	Bluetooth Attack
2227	1261	1020	1173	874	692	605	642	315	275	205	204	208	65	12	12	14	0

2. IoT 공격유형 대분류 기반 세부분류(페이로드 특징적 차이-Type B) 후 최종 공격 유형 : 256 종

〔그림 3〕 IoT 공격유형 분류

본 논문에서는 이 후 4절 IoT 익스플로잇 분석을 통해 총 90종의 IoT 익스플로잇 90종과 미라이 변종 107종의 공격유형을 탐지하기 위한 Snort Rule을 개발하였다.



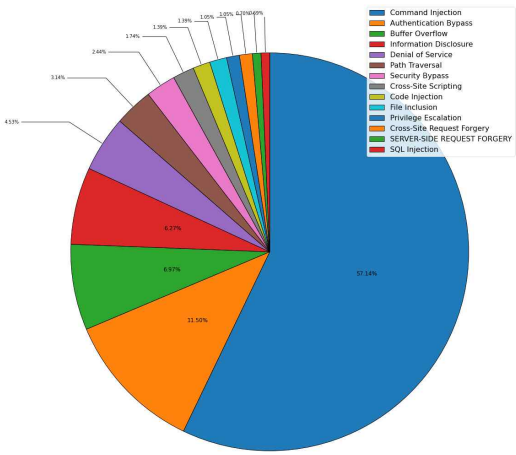
〔그림 4〕 IoT 공격유형 분류

Ⅴ. IoT 익스플로잇 분석

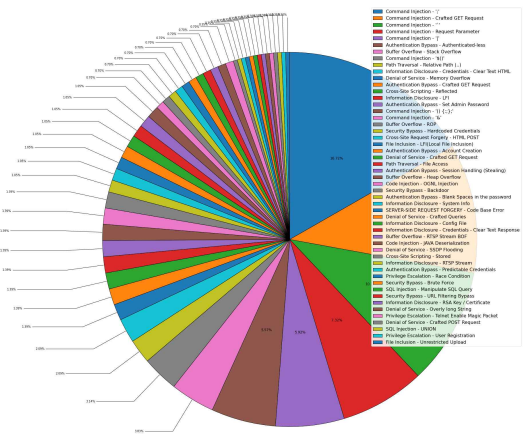
최근 IoT 익스플로잇 사례 분석을 통해 IoT 임베디드 기기 대상 익스플로잇 감염에 CMDi 공격이 주로 사용됨을 알 수 있었다. 본 절에서는 2008년부터 2021년 6월까지의 IoT 익스플로잇 감염 취약점을 조사하여 전체 취약점 중 CMDi 공격의 비율을 조사하였다. IoT 익스플로잇은 CVE취약점을 기준으로 exploit-db.com ID, 공격유형, 페이로드, 사용된 IoT 멀웨어 등을 조사했다. CVE-ID와 EDB-ID, 페이로드는 팔로알토 네트웍스 Unit42[4]와 같은 블로그, 보고서, badpackets 트위터[1], URLhaus Database[2]와 같이 매일 업데이트되는 무료 서비스를 참조하였다.

공격유형은 수집된 취약점 별 익스플로잇 코드의 페이로드를 조사한 후 기존에 분류했던 IoT 공격유형 분류 결과 [그림 2]와 익스플로잇 페이로드 특징을 비교하여 분석하였다. 기존에 조사한 IoT 공격유형 분류 결과를 바탕으로 IoT 키워드를 통해 수집된 exploit-db.com ID의 CWE 별 공격유형을 18종(Type A)으로 분류하였으며, 18종의 공격유형 분류는 페이로드의 특징적 차이를 기준으로 256종(Type B)으로 세부분류 하였다. IoT 공격유형 분류 결과는 IoT 익스플로잇 취약점으로 사용 가능한 모든 익스플로잇을 대상으로 분류한 결과이고, 이번에 조사하는 전체 IoT 익스플로잇 취약점 조사 결과는 실제 익스플로잇 공격으로 쓰인 취약점만을 대상으로 공격유형을 분류했다는 점에서 차이가 있다. 기존에 조사한 IoT 공격유형 분류 결과를 바탕으로 IoT 키워드를 통해 수집된 exploit-db.com ID의 CWE 별 공격유형을 18종(Type A)으로 분류하였으며[그림 5], 18종의 공격유형 분류는 페이로드의 특징적 차이를 기준으로 256종(Type B)으로 세부분류[그림 6] 하였다. IoT 공격유형 분류 결과는 IoT 익스플로잇 취약점으로 사용 가능한 모든 익스플로잇을 대상으로 분류한 결과이고, 이번에 조사하는 전체 IoT 익스플로잇 취약점 조사 결과는 실제 익스플로잇 공격으로 쓰인 취약점만을 대상으로 공격유형을 분류했다는 점에서 차이가 있다. 실제 IoT 익스플로잇 공격으로 쓰인 취약점의 Type B 분류 결과에

1) https://twitter.com/bad_packets
2) https://urlhaus.abuse.ch/browse/



〔그림 5〕 IoT 위협 대분류(CWE기반) - Type A



〔그림 6〕 IoT 위협 세부분류(페이로드 특징 기반) - Type B

서 전체 256 종 중 51종을 확인하였고, 이는 전체의 20%에 해당하는 비율로 공격으로 사용가능한 취약점 중 일부만 사용되고 있음을 의미한다. 그 중 5종의 CMDi 공격이 전체 50%를 넘는 것을 확인했다. IoT 익스플로잇 공격에 쓰인 취약점의 비율을 확인하기 위해 Type A 분류 결과의 전체 18종 중 14종을 확인하였다. CMDi 공격은 전체 취약점 중 57.14%를 넘는 것을 확인하였다.

Ⅵ. IoT 익스플로잇 대응

앞서 분석한 결과를 바탕으로 [그림 7]과 같이 197개의 세부공격 유형에 대한 익스플로잇 대응을 위한

Type A	Type B 개수	Type A	Type B 개수
Authentication Bypass	9	File Inclusion	4
Buffer Overflow	4	Information Disclosure	14
CRLF Injection	1	Path Traversal	8
Code Injection	3	Privilege Escalation	1
Command Injection	8	SQL Injection	8
Cross-Site Request Forgery	4	Security Bypass	7
Cross-Site Scripting	3	URL Redirect	3
Denial of Service	13	미라이 변종	107
			합 : 197

〔그림 7〕 IoT 익스플로잇 탐지 공격유형

탐지 정책을 생성하였다.

각각의 공격유형에 대해 생성된 197개의 탐지 정책 중 2개의 탐지 정책은 다음과 같다.

6.1. Crafted-GET-Request(Authentication Bypass)

Crafted Get Request 공격 패킷을 탐지하기 위해 [그림 8]과 같은 룰을 적용하였다. 탐지할 요청은 GET 요청이며 사용된 content값은 “/cgi-bin”과 “Admin.asp”, “Password”, “sessionKey”이다. 해당 익스플로잇은 [그림 9]의 CVE-2018-8898 취약점을 악용 패킷을 탐지한다.

```
alert tcp any any -> any 8000 (msg:"Authentication Bypass / D-Link DSL-3782 / A1_WI_20170303 SWVer="V100R001B012" FWVer="3.10.0.24" FirmVer="TT_77616E6771696F6E67"": content:"GET"; http_method; content : "/cgi-bin"; content: "Admin.asp";nocase; content:"Password";nocase; content:"sessionKey";nocase; classtype: Authentication-Bypass_Crafted-GET-Requests; reference : cve, CVE-2018-8898; sid:10000002;)
```

〔그림 8〕 Crafted GET Request 공격유형 탐지

```
Wireshark · Follow HTTP Stream (tcp.stream eq 2) · ens33
GET /cgi-bin/New_GUI/Set/Admin.asp?
Password=1231231231231238sessionKey=%24%28curl+-sS+http%3A%2F
%2F192.168.1.1%2Fcgi-bin%2Fget%2FNew_GUI%2Fget_sessionKey.asp%29
HTTP/1.1
Host: 192.168.42.137:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Referer: thewhiteh4t
```

〔그림 9〕 Crafted GET Request 공격 패킷 정보

6.2. DictBruteForce_Telnet(Scanning Phase)

미라이 봇넷의 Scanning Phase 단계의 공격유형 중 DictBruteForce_Telnet 공격유형을 탐지하기 위해 [그림 10]과 같은 룰을 적용하였다. 해당 정책도 GET 요

```
alert tcp any any -> any 8000 ( msg:"Wireless IP Camera (P2P) WIFICAM devices h
ave a backdoor root account that can be accessed with TELNET."; content: "GET";
http_method; content: "/set_ftp.cgi"; content: "%24%28nc";nocase; classtype: Sca
nning-Phases_DicttBruteForce-Telnet; reference: cve, CVE-2017-8224; sid:20000
001; )
```

〔그림 10〕 DictBruteForce_Telnet 공격유형 탐지

```
Wireshark · Follow HTTP Stream (tcp.stream eq 1) · ens33
GET /set_ftp.cgi?
next_url=ftp.htm&loginuse=admin&loginpas=admin&svr=192.168.1.1&port=
21&user=ftp&pwd=%24%28nc+192.168.42.137+8000+-e+%2Fbin%2Fsh&dir=
%2F&mode=PORT&upload_interval=0 HTTP/1.1
Host: 192.168.42.137:8000
User-Agent: python-requests/2.18.4
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

〔그림 11〕 DictBruteForce_Telnet 공격 패킷 정보

청을 탐지하며 content 값은 취약한 URI 경로 “/set_ftp.cgi”와 “%24%28nc”이다. 해당 익스플로잇은 [그림 11]의 CVE-2017-8224 취약점 악용 패킷을 탐지한다.

Ⅶ. 결 론

본 논문에서는 IoT 익스플로잇의 수집 및 분석을 통해 CMDi 공격이 높은 비율로 사용되고 있음을 확인하였다. 그리고 현재까지는 공격으로 사용 가능한 전체 취약점 유형 중 일부만 사용되고 있음을 확인했다. 이는 앞으로 다양한 IoT 공격에 대한 대응이 필요하다는 예상이 가능하다. 특히 전체 익스플로잇 공격 중 Command injection, Authentication Bypass, Buffer Overflow가 75.16%로 대부분을 차지하므로 무엇보다 이들 공격에 대한 확실한 대응이 필요하다고 생각한다. 또한 공격유형 분류를 통해 253종으로 공격유형을 세부 분류하였으며, 이 중 IoT 익스플로잇 공격유형 90종과 미라이 봇넷 공격유형 107종에 대한 위협 탐지 정책을 마련하였다.

참 고 문 헌

[1] Unit 42, 2020 Unit 42 IoT Threat Report, paloalto Networks Unit 42, pp. 11~12, Mar 2020.

[2] R. Khoury, B. Vignau, S.Halle and A.Hamou-Lhadj, "An Analysis of the Use of CVEs by IoT Malware," Foundations and Practice of Security: 13th International Symposium, pp. 47-62, Mar 2020.

[3] Dave McMillen, "Internet of Threats: IoT Botnets Drive Surge in Network Attacks," IBM X-Force, Apr 2021.

[4] V. Singhal, R. Nigam, Z. Zhang and A. Davila, "New Mirai Variant Targeting Network Security Devices," paloalto Networks Unit 42, Mar 2021.

〈저자소개〉

오 성 택 (Sungtaek Oh)

정회원

2013년 2월 : 아주대학교 정보컴퓨터공학부 졸업

2016년 2월 : 아주대학교 컴퓨터공학과 석사

2015년 2월~현재 : 한국인터넷진흥원 보안위협대응R&D팀 선임연구원

<관심분야> 인공지능, 사물인터넷보안, 정보보호

고 웅 (Woong Go)

정회원

2010년 2월 : 순천향대학교 정보보호학과 석사

2013년 8월 : 순천향대학교 정보보호학과 박사

2014년 1월~현재 : 한국인터넷진흥원 보안위협대응R&D팀 책임연구원

<관심분야> IoT, 기계학습, 정보보호