*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.33, NO.2, Apr. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.2.267

# 다크넷 트래픽 기반의 알려지지 않은 IoT 봇넷 선제탐지 방안*

박 건 량,[1†] 송 중 석,[2] 노 희 준[3‡]
[1,2]한국과학기술정보연구원 (연구원, 책임연구원), [3]고려대학교 (교수)

# A Preemptive Detection Method for Unknown IoT Botnet Based on Darknet Traffic*

Gunyang Park,[1†] Jungsuk Song,[2] Heejun Roh[3‡]
[1,2]Korea Institute of Science and Technology Information (Researcher, Chief Researcher),
[3]Korea University (Assistant Professor)

## 요 약

최근 컴퓨팅 및 통신 기술의 발달로 인해 IoT 디바이스가 급격히 확산·보급되고 있다. 특히 IoT 디바이스는 가정에서부터 공장에 이르기까지 그 목적에 따라 연산을 수행하거나 주변 환경을 센싱하는 등의 기능을 보유하고 있어 실생활에서의 활용이 폭넓게 증가하고 있다. 하지만, 제한된 수준의 하드웨어 자원을 보유한 IoT 디바이스는 사이버 공격에 노출되는 위험도가 높으며, 이로 인해 IoT 봇넷은 악성행위의 경유지로 악용되거나 연결된 네트워크로 감염을 빠르게 확산함으로써 단순한 정보 유출뿐만 아니라 범국가적 위기를 초래할 가능성이 존재한다. 본 논문에서는 폭넓게 활용되고 있는 IoT 네트워크에서 알려지지 않은 보안위협에 선제적으로 대응하기 위해 IoT 봇넷의 네트워크 행위특징을 활용한 선제탐지 방법을 제안한다. IoT 봇넷이 접근하는 다크넷 트래픽을 분석하여 4가지 행위특징을 정의하고 이를 통해 감염의심 IP를 빠르게 선별한다. 분류된 IP는 사이버 위협 인텔리전스(CTI)를 활용하여 알려지지 않은 의심 호스트 여부를 확인한 후, 디바이스 핑거프린팅을 통해 IoT 봇넷에의 소속 여부를 최종 결정한다. 제안된 선제탐지 방법의 유효성 검증을 위해 실제 운용 중인 보안관제 환경의 다크넷 대역에 방법론 적용 및 확인 결과, 선제탐지 한 약 1,000개의 호스트가 실제 악성 IoT 봇넷임을 10개월간 추적관찰로 검증하여 그 유효성을 확인하였다.

## ABSTRACT

With development of computing and communications technologies, IoT environments based on high-speed networks have been extending rapidly. Especially, from home to an office or a factory, applications of IoT devices with sensing environment and performing computations are increasing. Unfortunately, IoT devices which have limited hardware resources can be vulnerable to cyber attacks. Hence, there is a concern that an IoT botnet can give rise to information leakage as a national cyber security crisis arising from abuse as a malicious waypoint or propagation through connected networks. In order to response in advance from unknown cyber threats in IoT networks, in this paper, We firstly define four types of We firstly define four types of characteristics by analyzing darknet traffic accessed from an IoT botnet. Using the characteristic, a suspicious IP address is filtered quickly. Secondly, the filtered address is identified by Cyber Threat

Received(01. 19. 2023), Modified(02. 17. 2023), Accepted(02. 20. 2023)
* 본 연구는 한국과학기술정보연구원(KISTI) 지원으로 수행하였습니다.
† 주저자, gypark@kisti.re.kr
‡ 교신저자, hjroh@korea.ac.kr(Corresponding author)

Intelligence (CTI) or Open Source INTelligence (OSINT) in terms of an unknown suspicious host. The identified IP address is finally fingerprinted to determine whether the IP is a malicious host or not. To verify a validation of the proposed method, we apply to a Darknet on real-world SOC. As a result, about 1,000 hosts who are detected and blocked preemptively by the proposed method are confirmed as real IoT botnets.

**Keyworkds:** IoT, Botnet, Preemptive detection, Darknet, CTI(Cyber Threat Intelligence)

## I. 서 론

하드웨어, 소프트웨어를 비롯한 디바이스 기술이 발전함에 따라, Internet of Things(IoT) 디바이스 활용이 증가하고 있으며, 통신기술의 발전과 함께 5G, 6G 등 인터넷과 상호접속 가능한 광역통신망을 활용하는 대규모 IoT 서비스가 폭넓게 활용되고 있다[1]. IoT 디바이스는 구현 및 운용이 기존 레거시 시스템에 비하여 간단하고 저비용으로 목적 달성이 가능하기 때문에 스마트 빌딩[2], 스마트 시티[3]에서부터 가정환경[4]에 이르기까지 그 목적에 따라 다양한 활용이 이루어지고 있다. 특히 최근에는 온도, 습도 및 적외선 등을 측정하거나 폐쇄회로 텔레비전(Closed-Circuit TeleVision, CCTV) 형태로 영상을 수집하는 단일 IoT 기능에서 나아가, 여러 기능을 복합적으로 갖는 IoT 디바이스를 활용하여 군사목적[5] 또는 의료목적[6] 등으로 폭넓게 응용되고 있다.

이러한 IoT 디바이스는 직접 장치에 접근하여 제어하기보다는 주로 네트워크를 통해 관리 센터[7], 클라우드[8], 또는 에지/포그 컴퓨팅 플랫폼[9]과 같은 중앙 제어 시스템에서 통합하여 제어·운용된다. 비록 광대역 네트워크에 직접 접속하여 IoT 디바이스를 운용하는 경우도 많으나, 기존 레거시 기기(PC, 서버 등)에 비하여 훨씬 많은 수의 장치, 작은 배터리로 운용되어야 하는 전력 이슈, 제한된 서비스 범위 및 주파수 등의 현실적인 이유로 인하여 IoT 전용 통신 네트워크 기술인 LoRa·NB-IoT 등을 통해 자체 LPWA(Low Power Wide Area)기반 서브넷을 구성하여 운용하는 것이 일반적이다[10][11][12].

PC, 서버 등에 비하여 제한된 수준의 하드웨어 자원으로 구성된 IoT 디바이스는 장비 자체의 보안 수준 강화에 한계가 존재하며 많은 수의 서브넷으로 구성된 IoT 전용 네트워크에 대하여 기존 네트워크 보안장비(IDS, IPS 등)나 인공지능(AI)·기계학습(ML)등의 보안관제기술[13]을 활용하는 것은 현실적으로 매우 어렵다. IoT 디바이스 보호를 위해 장치 인증, 데이터 기밀성·무결성을 위한 보안 프로토콜 활용 등 다양한 방법이 제안되오고 있지만, 다양한 플랫폼과 프로토콜이 사용되는 복잡한 IoT 환경에서 신·변종 공격 등에 대한 네트워크 수준에서의 사전 차단은 사실상 불가능하다. 예를 들어 미라이(Mirai), 페르시라이(Persirai) 봇넷(botnet) 등에 감염된 IoT 디바이스는 악성행위의 경유지로 악용되거나 연결된 네트워크로 감염을 확산시켜 피해를 급속도로 증가시킨 사례가 있다. 따라서 태생적으로 보안상 취약한 IoT 디바이스 및 네트워크의 보호를 위해서는 주기적인 취약점 점검을 통해 알려진 공격을 사전에 차단함과 동시에 알려지지 않은 IoT 봇넷을 선제적으로 탐지하고 그 근원지를 식별·차단하는 것이 매우 중요하다.

본 연구에서는 IoT 디바이스·네트워크에 대한 알려지지 않은 공격으로부터 대응하기 위하여 IoT 봇넷의 네트워크상에 나타내는 행위특징을 활용한 선제탐지 방법을 제안한다. IoT 봇넷이 접근하는 다크넷 트래픽을 분석하여 연속성, 주기성, 빈도성, 범위성의 4가지 행위특징을 정의하고 이를 통해 감염의심 IP의 빠른 선별을 시도한다. 감염의심으로 분류된 IP를 대상으로 사이버 위협 인텔리전스(Cyber Threat Intelligence, CTI)[14]를 활용하여 알려지지 않은 악성의심 호스트 여부를 확인 한 후, 최종적으로 디바이스 핑거프린팅을 통해 IoT 봇넷 감염 여부를 결정함으로써 탐지결과의 신뢰성 향상을 추진한다.

제안된 기술의 유효성 및 실환경 운용가능성 확인을 위하여, 실제 운용중인 보안관제 환경의 다크넷 대역을 활용하여 선제탐지를 수행한 결과를 보인다. 특히 실제 선제탐지된 악성 의심 호스트에 대하여 최초 탐지 시점에서 CTI는 정상 호스트로 판별하였으나, 추적관찰 후 971개의 호스트가 악성 IoT 봇넷으로 업데이트 되었음을 확인함으로써 제안된 선제탐지 기술의 우수성 및 유효성을 검증하였다.

본 논문은 다음과 같이 구성되어 있다. 2절에서는 IoT 디바이스를 대상으로 한 사이버공격 및 탐지·대응기술 동향과 다크넷과 CTI를 활용한 사이버공격

추적기술에 대하여 살펴본다. 3절에서는 본 논문에서 제안하는 다크넷 기반의 알려지지 않은 IoT 봇넷 선제탐지 방안을 제안하고, 4절에서 제안된 방법론의 실제 구현과 더불어 실환경 IoT 디바이스 보안관제 환경에 적용한 결과를 분석함으로써 제안된 방법론의 유효성을 검증한다. 마지막으로 5절에서는 본 논문의 결론과 향후 연구에 대하여 기술한다.

## II. 관련 연구

본 절에서는 IoT 기기를 대상으로 한 사이버공격 동향에 대하여 살펴보고, 지속적인 사이버공격을 수행하는 기술·사례와 기존 대응 방법에 대하여 살펴본다. 또한 미사용 IP주소 대역에 대한 무작위 접근시도를 모니터링 가능한 다크넷 시스템 소개 및 활용사례와 더불어 CTI 기반의 사이버공격 대응 연구들에 대하여 소개한다.

### 2.1 IoT 디바이스 대상 사이버공격 및 탐지·대응기술

최근 IoT 디바이스의 보안 취약점을 악용한 악성코드이 확산되고 있다. IoT 디바이스는 대부분 stripped-down 형태의 Linux 운영체제(Operating System, OS)를 탑재하고 있기 때문에, 대역폭 제어기능이 취약하고 트래픽 및 프로세스 필터링 기능이 미비해 자체 OS에 대한 충분한 감사기능을 제공하지 않기 때문에 공격자는 개인용 컴퓨터(Personal Computer, PC), 서버 등의 디바이스에 비하여 손쉽게 인터넷에 연결된 다양한 IoT 디바이스를 대상으로 봇넷을 구축할 수 있다.

특히 IoT 디바이스를 대상으로 공격하는 악성코드의 핵심 기능 중 하나는 이미 감염된 디바이스가 보안이 취약한 새 공격대상을 찾아 악성코드를 전파시키는 감염확산으로, 대표적인 악성코드로는 미라이(Mirai)[15]가 있다. 미라이에 감염된 IoT 디바이스는 감염확산을 위해 텔넷 포트(tcp 23,2323)를 대상으로 IPv4 주소 공간을 랜덤하게 접근한 뒤 포트가 오픈되어 있는 IP를 대상으로 사전에 미리 정의된 62개의 계정 및 비밀번호로 사전 공격(Dictionary attack)을 시도한다. 로그인 성공 시 별도로 준비된 Report 서버로 새로운 공격대상 IP와 로그인이 성공한 계정정보를 유출하며, Report 서버의 Loader 프로그램이 공격대상 시스템 환경을 파악하고 악성코드를 전파시켜 새로운 봇을 확보한다. 이러한 공격으로 발행한 대표적 피해사례로서 도메인 등록 서비스를 제공하는 Dyn의 네트워크가 2016년 10월 21일 DDoS 공격을 받아 Amazon, GitHub, Netflix, Twitter 등과 같이 전 세계적으로 많이 사용되는 서비스의 도메인에 장애가 발생해 이용자들로 하여금 인터넷 자체가 마비되었다는 착각을 일으킨 바가 있다.

미라이와 같은 IoT 악성코드는 DDoS 공격을 최종목적으로 봇넷 구성을 시도한다. 이를 위해 (1)취약점을 가진 IoT 디바이스를 발견하고 (2)악성코드를 전파하여 새로운 봇(bot)을 확보하고 (3)확보된 봇을 관리하는 과정을 거치게 된다. 이러한 과정에 대한 보안 전문가들의 이해도가 높아지고 대응책이 나오면서, 악성코드의 봇넷 구성 기술은 지속적으로 발전하고 있다[16].

먼저, 봇넷 구축을 위한 IoT 악성코드 감염대상을 식별하는 방법으로 주로 네트워크 탐색을 수행하며, 초기에는 사전에 악성코드 내 하드코딩 된 IP 주소 목록을 탐색하는 방식에서 현재는 IP 주소공간 전체를 랜덤하게 탐색하는 방식으로 발전하였다.

두 번째로, 탐색된 공격대상에 악성코드 감염 전파를 하기 위해 관리자 권한 획득 목적의 사전공격(dictionary attack), 패치하지 않은 취약점을 포함한 펌웨어 대상 공격 등 크게 두 가지 방식으로 공격(exploit)을 시도하며 최근에는 두 가지 방법을 조합하여 공격하는 것이 일반적이다.

마지막으로, 확보된 봇넷을 관리하기 위해서 일반적으로 사용된 Command & Control(C&C)서버가 봇과 직접 통신하는 중앙 집중식 관리 방식에서 나아가 C&C서버를 활용하지 않는 Peer-to-Peer(P2P) 방식으로 발전하고 있다. P2P 방식으로 봇넷을 관리하는 대표적인 악성코드로서 최근 3년간 150만 대 이상의 IoT 디바이스를 감염시켜 대규모 봇넷을 구축한 Mozi가 있었으며, Mozi는 BitTorrent의 DHT(distributed sloppy hash table) 프로토콜을 활용하여 봇넷을 관리한다[17].

이와 같이 진화하고 있는 IoT 디바이스 대상 악성코드를 탐지하기 위한 접근방법으로는 크게 호스트기반 탐지와 네트워크기반 탐지가 존재한다[18]. 먼저 호스트기반 탐지방법은 임베디드 CPU를 에뮬레이트하여 IoT 디바이스 전용 허니팟을 구성한 후 허니팟에 유입되는 IoT 디바이스 대상 악성코드 및 동작을 탐지하는 구조이다[19][20]. 하지만 해당 연구들은 점차 늘어나는 IoT 디바이스의 기능을 제한적

으로 에뮬레이트할 수밖에 없기 때문에 다양한 IoT 디바이스를 대상으로 공격하는 악성코드를 탐지하기 어렵다.

네트워크기반 탐지방법으로는 IoT 디바이스의 네트워크 트래픽을 수집해 딥러닝 기법 중 하나인 오토인코더(autoencoder)를 적용하여 이상징후를 탐지하는 연구[21] 등이 있으나 IoT 디바이스 네트워크 플로우 데이터 수집이 가능한 환경에서만 제한적으로 활용이 가능하며 계산량 및 시간에 많은 소모가 필요한 단점이 존재한다.

### 2.2 다크넷 및 CTI 활용 사이버공격 탐지 기술

많은 조직에서는 글로벌 사이버 공격 동향을 파악하기 위해 다크넷(darknet)을 활용하여 네트워크에 접근하는 호스트의 모니터링을 시도한다[22]. 다크넷은 미사용 중인 IP의 집합으로써, 실제 시스템이 존재하지 않기 때문에 다크넷에 접근하는 호스트는 기본적으로 비정상 호스트로 간주할 수 있다[23][24]. IoT 디바이스 대상 악성코드가 감염확산 대상을 탐색할 때 주로 IPv4 주소공간을 랜덤하게 접근하므로 다크넷에도 유입되는 것이 일반적이기 때문에, IoT 디바이스 대상 악성코드의 접근 탐지에도 다크넷의 활용이 가능하다[25].

최근에는 다크넷을 활용해 악성코드에 감염된 IoT 디바이스의 식별을 위해 CTI를 결합하는 경우가 많아지고 있으며, IP 주소공간을 지속적으로 스캔하여 연결 디바이스 정보를 제공하는 검색엔진(Shodan, Censys 등)을 기반으로 IP 주소 정보를 상관분석하여 감염된 IoT 디바이스를 식별하고 CTI로 활용하는 방법[26]이 제안되고 있다.

또 다른 접근법 중 하나인 ex-IoT(exploited IoT)[27]는 다크넷에 유입되는 호스트를 직접 스캔하고 응답값을 기준으로 IoT 디바이스와 非 IoT 디바이스를 분류한다. 이후 IoT 디바이스로 분류된 대상을 집중 분석하여 악성코드 감염여부를 확인하고 추가적인 CTI로 활용한다.

하지만 해당 연구들은 다크넷에 접근하는 IoT 디바이스를 식별하는 방법으로 검색엔진(Shodan, Censys 등)에 크게 의존하기 때문에 해당 검색엔진에서 식별하지 못한 IoT 디바이스는 악성감염 여부 판단이 어려운 한계점과 더불어 다크넷에 유입되는 방대한 양의 IP 주소를 실시간으로 검색엔진에 조회하기 불가능한 한계점이 존재한다.

## III. 다크넷을 활용한 IoT 봇넷 선제탐지 방안

현재 실환경에서 운용되고 있는 대부분의 네트워크 보안관제 체계에서는 탐지패턴 기반의 오용탐지, 비정상 행위 탐지를 위한 이상탐지, Open Source INTelligence(OSINT) 또는 자체 구축한 사전(화이트·블랙리스트) 기반의 탐지 등 다양한 기법을 통해 사이버 위협을 탐지·대응하는 반면, IoT 환경에서는 IoT보안에 대한 예산, 장비, 노하우의 부족으로 인해 적절한 보안대책들을 수립·적용하지 못하고 있다.

또한, IoT 디바이스의 H/W 성능의 한계로 인하여 충분한 자체적 보안대책을 수립하기 어려우며, 이러한 이유로 일부 취약점 노출 시 공격 대상 및 범위가 급속도로 증가하여 빠른 속도로 피해가 확산되는 특징이 있다[28][29]. 따라서 탐지패턴을 정의하여 일반적인 보안관제가 수행되기 이전에, 선제적으로 공격시도나 의심행위를 발견하고 차단 또는 대응을 수행하는 것이 일반적인 PC, 서버 등 레거시 시스템 환경에 비하여 매우 중요하다[30].

본 논문에서 제안하는 IoT 봇넷 선제탐지 방안은 Fig. 1과 같다: (1) 다크넷 시스템과 IoT 봇넷 특징을 활용하여 대규모로 인입되는 트래픽 중 공격 의심 대상후보를 선정하고, (2) OSINT등 CTI를 활용하여 알려진 혹은 정상적인 시스템을 확인·검증 한 후, (3) 최종 추출된 공격 의심 대상을 핑거프린팅하여 IoT 봇넷 여부를 판단하고 선제적인 탐지 및 대응을 수행한다.

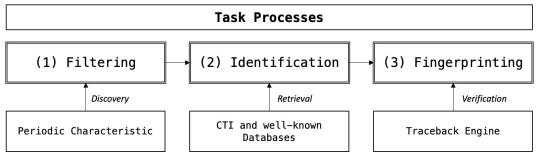


Fig. 1. Overall Task Process for Detecting IoT Botnet

### 3.1 IoT 봇넷 트래픽 행위특징 기반 필터링

2.2절에서 살펴본 바와 같이 다크넷은 미사용 IP의 집합으로, 침해위협 및 알려지지 않은 공격 탐지를 위하여 다양하게 활용되고 있다. 하지만, OSINT 제공서비스 또는 네트워크 활성 여부 확인을 위한 봇과 같이 정상적인 서비스 제공을 위해 수

행되는 스캐닝 트래픽 또한 존재하기 때문에, 다크넷 시스템을 활용하더라도 대규모의 트래픽에서 공격 의심 트래픽을 선별하는 것은 매우 중요하다.

Table 1은 정상적인 스캐닝과 IoT 봇넷 의심 트래픽의 주요 네트워크 행위 특징에 대하여 비교한 결과이다. 정상 스캐닝 행위는 일반적으로 지정된 IP 주소 대역 또는 포트 대역에 대하여 일괄적·연속적인 접근시도를 하는 것이 일반적이며, 단위시간당 많은 양의 트래픽을 발생하는 것이 특징이다. 물론 정상 스캐닝 행위와 동일하게 공격 대상을 탐색하는 악성 스캐닝의 경우도 발생하지만, 대부분의 경우 네트워크 보안장비에 설정된 단위시간당 임계치를 기반으로 차단이 수행되므로 본 연구의 고려사항에서는 제외한다. 반면에, IoT를 대상으로 하는 악성 봇은 봇넷의 규모를 늘리기 위한 감염 전파행위를 수행 할 때 정해진 대상의 IP 주소나 포트를 대역 기준으로 스캐닝을 수행하지 않고, 사전에 정의된 취약점이 존재하는 특정 서비스 포트 그룹과 IPv4 주소 공간을 랜덤하게 스캐닝하기 때문에 간헐적·비주기적으로 좁은 범위를 탐색한다.

본 연구에서는 Table 1에서와 같은 IoT 봇넷이 나타내는 트래픽상의 행위를 바탕으로 4가지 행위특징을 정의하고, 이를 통해 먼저 정상 스캐닝 행위의 필터링을 시도한다. 구체적으로, 연속성(Seriality, SR)는 일정기간 동안 출발지 IP에서 스캐닝한 대상이 연속적인 IP 대역인지의 여부를 나타낸다. 비록 알고리즘에 따라서 순차적이 아닌 랜덤 접근 형태로 스캐닝이 수행될 수는 있지만, 일반적인 스캐닝의 목적이 대상 대역의 IP를 빠짐없이 접근하는 것이기 때문에 일정 단위기간 동안 결과를 취합하면 연속적인 대상을 접근 시도한 것으로 나타난다.

$$SR_{ip_{source}} = \begin{cases} \text{if } \sum_{n=low}^{high} \nexists ip_{dst_n} < k, \ benign \\ otherwise, \ malicious \end{cases} \quad (1)$$

따라서 식(1)과 같이 다크넷에 접근한 출발지 IP($IP_{source}$)가 접근한 도착지 IP($IP_{dst}$)의 가장 낮은 수($low$)부터 가장 높은 수($high$)까지의 주소 중 접근하지 않은 IP 주소의 개수를 확인하여 연속성(SR) 필터의 결과값을 결정한다. 이때 $k$는 관제환경(관찰시간, 접근범위)에 따라 실험적으로 정해지며, 접근하지 않은 IP 주소가 $k$개 이하인 경우 정상적인 스캐닝(benign), 그렇지 않은 경우는 IoT 봇넷 의심(malicious)으로 판단한 후 주기성 검증을 시도한다.

Table 1. Characteristic Comparison between Normal Scanning and Suspicious Activities targeted on IoT devices

| Behavior Characteristics | Normal Activities | Suspicious Activities |
|---|---|---|
| Seriality (SR) | O | X |
| Periodic (PR) | O | X |
| Frequency (FQ) | High | Low |
| Range (RG) | Wide | Narrow |

주기성(Periodicity, PR)은 출발지 IP 주소가 일정한 시간 간격을 바탕으로 스캐닝을 시도했는지 여부를 나타낸다. 예를 들어 OSINT 등의 서비스들은 데이터베이스 최신성 확보를 위하여 대상 대역의 도착지 IP 주소들을 일정한 시간간격으로 스캐닝하는 것이 일반적이지만, IoT 봇의 경우 봇넷 규모를 늘리기 위한 목적으로 IPv4 주소공간 전체를 랜덤하게 스캐닝 하는 특성이 있어 비주기적으로 악성경유지 혹은 연결된 IoT 기기의 네트워크에 접속을 시도한다.

$$PR_{ip_{source}} = \begin{cases} \text{if } \sigma(TI_T) < \epsilon, \ benign \\ otherwise, \ malicious \end{cases} \quad (2)$$

식(2)에서 TI(Time Interval)는 하나의 세션에서 출발지 IP(IPsource)가 다크넷 도착지 IP 주소로 접근할 때마다의 시간간격(T)의 집합을 의미하며, σ는 각 시간간격의 표준편차를 의미한다. 즉, 동일 출발지 IP 주소로부터 다크넷에 연속적인 접근이 이루어졌을 때, 그 시간간격이 일정하다면 정상적인 스캐닝(benign)으로 분류한다. 표준편차(σ)는 0 또는 ε (〈1sec.) 이내로 설정하며, 이외의 경우는 IoT 봇넷 의심(malicious)으로 판단한 후 빈도성 검증을 이어서 수행한다.

$$FQ_{ip_{source}} = \begin{cases} \text{if } \sum_{t} ip_{dst+port} > N, \ benign \\ otherwise, \ malicious \end{cases} \quad (3)$$

빈도성(Frequency, FQ)는 출발지 IP가 단위시간(t) 동안 얼마나 자주 또는 반복적으로 스캐닝을 수행했는지 여부를 나타낸다. 예를들어 인터넷에 연결된 디바이스 정보를 제공하는 검색엔진은 스캐닝을 수행 할 때 IP스캔 및 포트스캔을 복합적으로 수행

하는 것이 일반적이지만, IoT 봇의 경우 사전에 정의된 포트 그룹만을 스캔하는 특성이 있다. 이러한 이유로 반복횟수는 동일한 도착지 IP 주소에 서로 다른 번호의 포트를 접속하는 행위도 고려하여 계산한다. 다만, 식(3)에서와 같이 임계치 N의 경우는 운용하는 다크넷 대역과 단위시간의 설정에 따라 실험적으로 설정된다.

빈도성 검증까지 거친 후 필터링된 IoT 봇넷 의심(malicious) IP 주소들은 최종적으로 출발지 IP가 얼마나 넓은 범위의 대역을 접근했는지에 대한 범위성(Range) 검증 대상이 된다. IPv4 전체 주소공간을 랜덤하게 접근하는 IoT 봇 전파 특성을 고려하여 식(4)에서와 같이 출발지 IP 주소로부터 단위시간당 전체 다크넷 운용 대역 IP($D_{ip}$) 중 접근된 비율(범위)을 검증하게 된다, 일반적으로 단위시간과 접근비율은 함께 증가하지만 정상적인(benign) 스캐닝 활동은 그 수가 선형적으로 증가하는 반면, IoT 봇넷 의심 행위의 경우는 공격 대상 대역이 크게 넓어지지 않으므로 임계치($P$)이하의 접근범위를 갖는 IP 주소를 최종 의심(malicious) IP 주소로 분류한다.

$$RG_{ip_{source}} = \begin{cases} \text{if } \dfrac{\sum_{t} ip_{dst}}{D_{ip}} > P, \ benign \\ otherwise, \ malicious \end{cases} \quad (4)$$

이와 같은 행위특징을 바탕으로 본 논문에서는 트래픽 특징 기반 IoT 공격 의심 대상 선별 방안인 Filtering task를 Def. 1과 같이 정의한다.

Definition 1 (Filtering task)

$$L_{susp} = \forall ip \in D_T, \bigcup_{i=1}^{N_{ip}} \{SR_i \wedge PR_i \wedge FQ_i \wedge RG_i\} \quad (5)$$

여기서 $L_{susp}$는 추출된 공격 의심 IP 리스트이며, $D_T$는 일정기간 동안 다크넷에 인입된 출발지 IP와 도착지 IP 집합, $SR_i$, $PR_i$, $FQ_i$, $RG_i$는 각각 연속성, 주기성, 빈도성, 범위성 특징에 해당하는 ip의 집합을 의미한다. 즉, Fig. 2에서와 같이 다크넷에 유입된 모든 출발지 IP 주소에 대하여, 연속성·주기성·빈도성·범위성 특징을 순차적으로 검증한 후 모두 만족하는 IP 주소만을 IoT 봇넷 의심 대상 목록으로 고려한다.

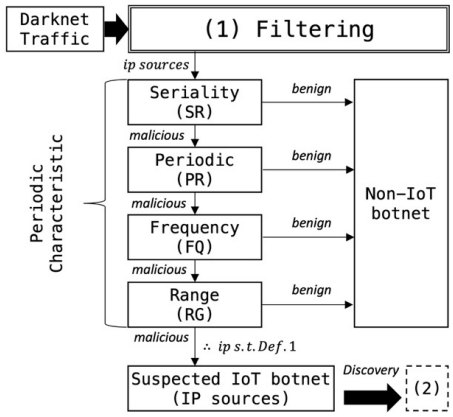


Fig. 2. Filtering Process

### 3.2 CTI(OSINT)기반 알려지지 않은 봇넷 식별

제안 선제탐지 방안의 식별단계에서는 필터링 단계를 통해 선별된 IoT 봇넷 의심 대상을 기존의 CTI와 비교·판별하여 신규 감염 또는 알려지지 않은 감염 호스트를 분류한다. 본 단계는 신규 IoT 봇넷을 탐지하는데 있어 불필요한 정보를 삭제함으로써 분석대상 축소 및 분석효율성 향상을 위해 수행한다.

2절에서 언급한 바와 같이 다크넷에는 공격자뿐만 아니라 Shodan, Censys와 같이 정상 서비스에 의해 유입되는 패킷들 또한 다량 존재하기 때문에 이를 정상으로 분류하고 분석대상에서 제외하는 것이 필요하다. 또한 알려진 공격자 역시 IP 주소 필터링을 통해 쉽게 분류가 가능하기 때문에 추가적인 분석이 불필요하다. 따라서 추가적인 분석이 불필요한 분석대상들을 IoT 봇넷 의심 대상에서 제거한다.

본 논문에서 제안하는 CTI 기반 IP 식별 방법은 Fig. 4와 같다. 분류단계로부터 수신한 감염의심 호스트 정보를 정상 서비스 IP DB에 조회하고, 존재 시 알려진 정상 IP로 간주하고 이를 IoT 봇넷 의심 대상으로부터 제외한다. 이때 오설정(misconfiguration)에 의해 다크넷에 접근한 IP들은 정상적인 행위라 가정하고 이를 IoT 봇넷 의심 대상에서 제외한다. 또한, DNS에 의한 backscatter는 출발지 IP 주소가 DNS 서버의 IP 주소이기 때문에 분석 및 공격자 특정이 매우 어렵다. 따라서 식(6)과 같이 도착지 port가 53이면서 다수의 다크넷 IP로 접근한 출발지 IP의 경우에는 DNS라 가정하고 IoT 봇넷 감염 의심 대상

**INPUT:** suspicious IP set $L_{susp}$
benign IP set $B_{ip}$
malicious IP set $M_{ip}$
**OUTPUT:** updated suspicious IP set $L_{susp}$

```
for ip in L_susp do
    if ip in B_ip then
        L_susp ← L_susp - ip
    else if IP in M_ip then
        L_susp ← L_susp - ip
    else
        pass
    end if
end for
return L_susp
```

Fig. 3. Identification Algorithm

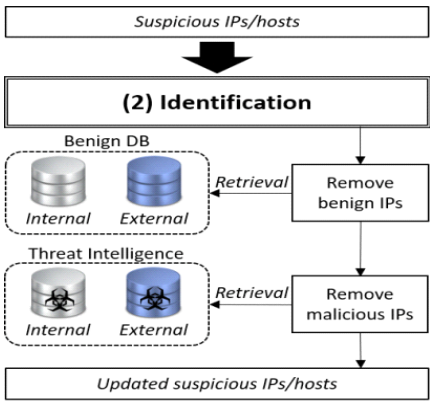


Fig. 4. Identification Process

에서 제외하였다.

$$L_{susp} = L_{susp} - B_{ip} \tag{6}$$

이후 Fig. 3의 절차에 따라 감염의심 호스트 정보를 다시 자체적으로 구축한 위협정보 데이터베이스 및 OSINT 서비스에 조회하고 악성으로 판명될 경우 이를 목록에서 제거한다(식(7)). 이를 통해 업데이트된 IoT 봇넷 의심 대상 목록은 핑거프린팅 단계로 전달된다.

$$L_{susp} = L_{susp} - M_{ip} \tag{7}$$

### 3.3 핑거프린팅을 통한 IoT 봇넷 최종 검증

디바이스의 정상 행위는 디바이스의 종류에 따라 모두 다르게 정의되기 때문에 행위정보 기반의 분석을 수행할 경우 디바이스의 종류를 파악하는 것이 중요한 과정 중 하나이다. 본 연구에서는 IoT 디바이스가 3.1절의 4단계 검증을 모두 만족시킬 경우 IoT 봇넷이라 가정하였기에 IoT 봇넷 의심 대상 목록의 IP 주소들이 IoT 기기임을 확인할 필요가 있다. 그러나 다크넷으로 유입된 모든 IP 주소의 디바이스 종류를 물리적으로 식별하는 것은 현실적으로 불가능하기 때문에 핑거프린팅을 통한 IoT 디바이스 식별 방법이 필수적으로 요구된다. 핑거프린팅은 크게 액티브 방식과 패시브 방식 두 가지로 구분할 수 있다. IoT 디바이스는 다른 디바이스에 송신하는 정보가 한정적이며 그 양이 적고 주기가 데스크톱이나 서버에 비해 길기 때문에 패시브 핑거프린팅 보다는 액티브 핑거프린팅을 활용하는 것이 더 효율적이다.

본 논문에서는 감염의심 호스트들의 선제적 탐지를 가장 부하가 적고 신속하게 활용 가능한 NMAP 기반의 OS 핑거프린팅[31]을 수행하여 디바이스의 종류를 파악하였다. 핑거프린팅을 통해 IoT 봇넷 의심 대상이 IoT기반의 OS를 사용하고 있는 것이 확인될 경우, 이를 IoT 디바이스인 동시에 IoT 봇넷으로 판정하고 이를 보안관제 센터에 전달 및 차단하였다(Fig 5).

뿐만 아니라 IoT 봇넷으로 식별된 디바이스의 정보는 Fig. 6과 같이 식별단계의 위협정보 데이터베이스 업데이트에 활용하여 시스템 성능 및 운영 효율성 향상시켰으며, 일정기간 이상 악성으로 활용되지 않은 IP 주소는 위협정보 데이터베이스에서 제거함으로써 위협정보 데이터베이스의 정확성을 향상시켰다.

**INPUT:** suspicious IP set $L_{susp}$
**OUTPUT:** malicious IP set $L_{botnet}$

```
L_botnet = ∅
for ip in L_susp do
    x ← OS fingerprinting(ip)
    if x has IoT OS then
        ip is IoT
        L_botnet ← L_botnet ∪ ip
    end if
end for
return L_botnet
```

Fig. 5. Fingerprinting Algorithm

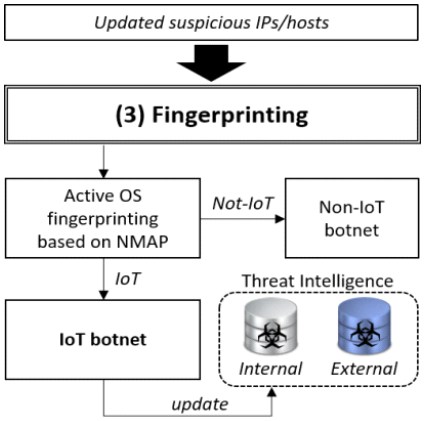


Fig. 6. Fingerprinting Process

## IV. 실환경 사례 기반 유효성 검증

### 4.1 실환경 다크넷을 활용한 데이터 수집

본 논문에서 제안된 방법의 유효성 검증을 위해 실환경에서 운용중인 다크넷 대역을 활용하여 실험을 수행하였다. 다수의 공격의심 대상 수집을 위하여 Fig. 7에서와 같이 16개의 서로 다른 지역(대전, 서울, 부산 등)에서 총 약 8,000개의 호스트가 운영중인 다크넷 대역을 사용하였으며, 추후 분류과정에서 활용을 위해 다크넷에 유입된 IP 주소 및 포트, 접근한 다크넷 IP 주소 및 포트와 프로토콜 및 시간 정보를 포함한 다양한 특징정보를 함께 수집하였다. CTI 검증을 위해서 VirusTotal[32]와 Alienvault[33] 등의 서비스 API를 활용하였으며, 핑거프린팅을 위해 공개된 라이브러리인 NMAP을 활용하였다. 전체적인 S/W는 Python 라이브러리를 통해 구현되었으며, 실험을 위해 운영된 다크넷 대역 정보와 수집

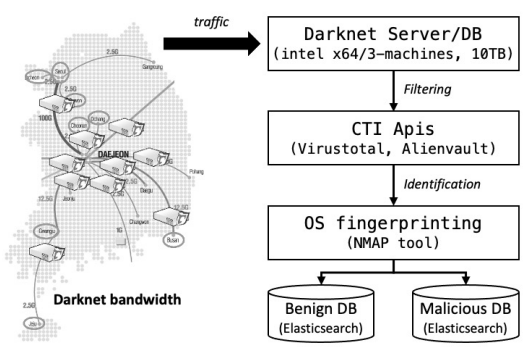


Fig. 7. System Environment for Experiment

Table 2. Darknet Environment and Dataset Statistics

| | Darknet (destination) | Dataset (source) |
|---|---|---|
| Num. of hosts(IP) | 8,192 | 133,234 |
| Num. of C-class | 32 | 532 |
| Collecting period | 7 days | |
| Total Num. of hits | 450,705,093 times | |
| Types of hosts (terminals) | PC, Server, IoT, etc | |
| Features | UID, ethernet header, IP header, Protocol header, packet data, time, location | |

된 데이터 정보는 Table 2와 같다.

실제 '22년 1월 1일부터 1월 7일까지 1주일동안 다크넷으로 유입된 총 악성의심 검증대상 IP(호스트)는 약 13만개이며, 532개의 C class에 걸쳐 분포하고 있다. 다크넷 실험환경 대역(C class 32개, 비연속적)에 대하여 수집대상 기간 동안 약 4억번 이상의 횟수로 접근이 이루어졌으며, 한 호스트로부터 가장 많이 접근된 횟수와 전체 호스트로부터 평균 접근 횟수는 각각 3,974회, 54회이다. 다만, 주로 스캐닝성의 트래픽 유입이 많은 관계로 각 패킷의 사이즈는 크지 않은 경향을 보였다. 다크넷에 접근한 호스트의 장치 유형으로는 PC, 서버 및 IoT 등 다양하게 나타났으나, 본 연구에서는 최종적으로 IoT 디바이스 만을 고려하였으며, 또한 수집된 특징정보들은 선제탐지 적용 과정에서 CTI와의 비교 혹은 핑거프린팅 단계에서 검증을 위해 활용된다.

### 4.2 제안 방법론 적용 및 유효성 검증 결과

본 논문에서 제안된 3단계 방법론의 적용을 위해 먼저 수집된 약 13만개의 호스트에 대하여 접속 범위, 기간 등 행위정보를 활용한 Filtering을 수행한다. 이때 실험적으로 결정된 연속성, 주기성, 빈도성, 및 범위성의 파라미터와 추출된 호스트의 수는 아래 Table 3과 같다.

최초 다크넷으로부터 수집된 호스트의 약 50%가 40%의 임계치($k$)로 설정된 연속성 조건으로 제외되었으며, 그 후 약 20%가 1초 이하의 주기성 조건

Table 3. Results of Filtering Process

| | SR | PR | FQ | RG |
|---|---|---|---|---|
| **Param.** | $40 < k$ | $1\ \mathrm{sec} \leq \epsilon$ | $30 < N$ (t=60s) | $5 > P$ (C-class) |
| **Hosts (133,234)** | 78,324 (-54,910) | 52,277 (-26,047) | 21,897 (-30,380) | 12,188 (-9,709) |

으로 분류되었다. 이어서 분당 30회 이하의 빈도성 조건 및 c-class 5개 대역 이상의 범위성 조건으로 최종 12,188개의 호스트가 추출되었다. 즉, 최초 수집 호스트에서 9.14%가 악성의심 호스트로 분류되었으며 분류된 모든 호스트에 대하여 두 번째 단계인 CTI 등록여부 확인을 시도한다.

기존 악성호스트 등록여부 확인의 신뢰성 확보를 위해 Virustotal, Alienvault 및 Shodan 등 API를 제공하는 다양한 CTI를 활용하였으며, 12,188개의 호스트에 대하여 악성행위여부 및 유형, 최초 등록일, 최근 등록정보 등의 세부정보를 수집하여 자체적으로 악성행위여부 재검토를 수행하였다. 최종적으로 2,649개, 21.7%의 호스트가 기존에 악성 호스트로 등록된 것을 확인하였으며, Window·Unix 서버, 유무선 공유기, IP 카메라 등 다양한 IoT 및 레거시 장비로 악용되고 있는 것을 확인하였다.

마지막 단계로 CTI에 등록되지 않은 9,539개의 호스트의 핑거프린팅을 수행하여 IoT 봇넷 의심 호스트 선별을 시도하였다. 다만 본 논문에서는 NMAP을 활용한 다수의 핑거프린팅 방법을 복합적으로 활용하였으나, 네트워크 보안장비에서의 차단 및 장비 보호를 위한 핑거프린팅 방지기술 등에 따라 1,231개(13%)의 호스트는 식별되지 않음으로 분류되었다. 식별되지 않은 호스트를 제외한 8,308개의 호스트 중에서 IoT로 식별된 호스트는 총 2,231개이며, 유무선 공유기(router), IP 카메라 및 관리장치, 임베디드 전용 OS 및 어플리케이션, Network Attached Storage(NAS)와 같은 네트워크 스토리지 등으로 구성된 것을 확인하였다. 나머지 6,076개의 호스트는 비 IoT 장비(Window, MacOS등)로 확인되어 의심 호스트로 등록한 후 유효성 검증대상에서는 제외하였다.

본 연구에서 제시된 선제탐지 방법론의 유효성 검증을 위하여 최종적으로 선별된 2,231개의 호스트에 대하여 10개월 간 OSINT에서 추적관찰을 수행하였으며, 결과는 아래 Table 4와 같이 나타났다

Table 4에서와 같이, 선제 탐지된 2,231개의 호스트 중에서 1개월 추적관찰 후 288개의 호스트가

Table 4. Results of Long-term Tracking

| Term (month) | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Malicious reg. (incr.) | 288 | 357 (+69) | 443 (+86) | 527 (+84) | 600 (+73) |
| **Term (month)** | **6** | **7** | **8** | **9** | **10** |
| Malicious reg. (incr.) | 663 (+63) | 780 (+117) | 806 (+26) | 843 (+37) | 971 (+128) |

악성으로 등록된 것을 확인 할 수 있다. 이후 매월 평균 약 80개의 호스트가 새롭게 악성으로 등록되고 있는 것을 확인하였으며, 10개월 추적관찰 후 971개(추적관찰 호스트 중 약 44%)의 호스트가 악성으로 분류된 것을 알 수 있다. 악성으로 분류된 호스트들을 실제 재확인해본 결과 보안에 취약한 IP카메라 및 유무선 공유기인 경우가 일반적이었으며, 제조사에서 기본제공한 사용자명 및 비밀번호를 사용하여 IoT 봇넷에 감염된 것으로 추정되었다(Fig. 8).

이와 같은 결과로부터 본 연구에서 제안된 방법을 통해 CTI를 통해 공유되거나 보안 장비 제조사·벤더 등에 의해서 악성 호스트 정보가 알려지기 전에 선제탐지 및 차단이 가능함을 확인하였다. 특히 선제탐지된 호스트 중 일부는 10개월 이상 발견되지 않고 악성행위를 지속한 이후에야 CTI에 등록되는 등 은밀하게 탐지회피 및 봇넷 전파를 수행하고 있는 것으로 확인되었다. 10개월간 추적관찰 과정에서 매월 약 80개의 호스트가 새롭게 검증되는 추세를 고려했을 때, 현재 2,231개의 최종 의심 호스트 중 약 44%만이 악성 호스트로 최종 확인되었으나 향후 지속적인 추적관찰을 수행한다면 추가적인 악성 호스트의 검증이 가능할 것으로 보인다[1].

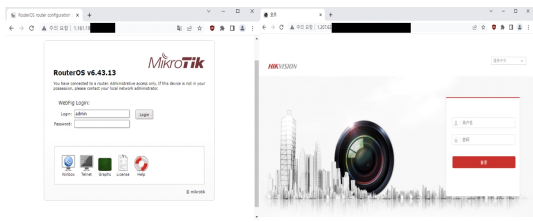


Fig. 8. Infected IoT devices from IoT Botnet

## V. 결 론

본 논문에서는 폭넓게 사용되는 IoT 네트워크·디

1) IoT 봇넷으로 검증 완료된 호스트 리스트 부록 참조(30개)

바이스에 대한 알려지지 않은 위협을 선제적으로 파악하고 대응 할 수 있는 탐지 방법론을 제안하였다. 미사용 IP 주소 대역인 다크넷을 활용한 본 연구는 정상적인 스캐닝과 악성 혹은 감염 봇넷으로부터의 트래픽을 분석한 후 연속성, 주기성, 빈도성, 범위성 4가지 특징을 정의하였다. 이를 바탕으로 CTI·OSINT를 활용하여 알려진 공격인지 여부를 확인한 후 실제 악성의심 IP 주소를 핑거프린팅함으로써 탐지 정확도 향상을 고려하였다. 특히 제안된 방법은 최근 다양한 연구가 이루어지고 있지만 대부분 시간과 비용이 크게 소모되는 인공지능 또는 기계학습 등의 학습 모델 기반이 아닌, 악성행위 특징에 기반한 경량형 필터링 방법으로서 실제 보안관제 현장에서 효율적으로 적용·활용 가능한 방법임에 그 의의가 있다. 이와 같은 효용성은 실 보안관제 환경을 활용한 실험을 통해 검증하였으며, 구체적으로 C class IP 주소 대역 32개의 다크넷 환경에서 10개월간 제안된 방법으로 선제 탐지된 악성의심 호스트 IP 주소의 44%(971개)가 추적관찰을 통하여 실제 IoT 봇넷으로 등록되었음을 CTI를 통해 검증하였다.

다만, 본 논문에서 제안한 특징분류 방법의 일부 파라미터는 관제환경에 따라 실험적·경험적으로 확정되어야 하여 정량수치로 적용하기 어려운 경우가 존재한다. 또한 핑거프린팅을 통해 최종 검증을 수행하고 있어 IoT 기기 또는 일반 컴퓨팅 자원이 공유기 하단에 위치하여 사설 IP 주소를 사용할 경우 NAT 서비스를 제공하는 공유기의 핑거프린트가 나올 수 있어 실제 다크넷에 접근한 디바이스를 구별할 수 없는 한계점이 존재하며, 일부 호스트·디바이스는 상태 확인이 불가능하였다. 따라서 실환경에서의 활용성 강화를 위하여 네트워크 환경 및 대역폭 등을 고려한 파라미터 정량화 및 호스트·디바이스 검증방법에 대한 연구를 향후 지속적으로 진행할 예정이다.

해당 연구는 실 보안관제 환경에서 실험을 통해 검증한 만큼 국내 공공 분야 사이버안전센터에 적용한다면, 다양한 보안관제 특성이 반영된 신규 블랙 IP를 선제적으로 탐지 할 수 있으며, 사이버안전센터 간 신규 블랙 IP에 대한 활발한 정보공유가 이루어진다면 알려지지 않은 사이버 보안위협에 대한 국가차원의 공동대응 체계가 마련될 수 있을 것이다.

## Appendix A. Examples of detected malicious IoT botnet hosts

| Idx. | IP address | Country code | Darknet hit date | CTI registered date | Malicious type | Access port |
|---|---|---|---|---|---|---|
| 1 | 178.49.*.94 | RU | 2022.01.01 | 2022.01.12 | Mirai | 23, 80, 8080 |
| 2 | 36.89.*.29 | ID | 2022.01.01 | 2022.01.15 | Mirai | 23, 80, 8080 |
| 3 | 203.198.*.30 | HK | 2022.01.03 | 2022.01.21 | Mirai | 23, 2323 |
| 4 | 94.181.*.117 | RU | 2022.01.04 | 2022.01.19 | Mirai | 23, 2323 |
| 5 | 103.220.*.178 | IN | 2022.01.01 | 2022.01.16 | Mirai | 23, 80, 8080 |
| 6 | 212.3.*.82 | RU | 2022.01.02 | 2022.07.26 | Mirai | 23, 80, 8080 |
| 7 | 94.240.*.34 | PL | 2022.01.01 | 2022.04.08 | Downloader | 80, 8080 |
| 8 | 1.36.*.101 | HK | 2022.01.01 | 2022.01.29 | Mirai | 23, 81 |
| 9 | 185.222.*.207 | PL | 2022.01.01 | 2022.01.29 | Mirai | 23, 81 |
| 10 | 45.224.*.26 | BR | 2022.01.01 | 2022.01.30 | Mirai | 23, 8080 |
| 11 | 116.31.*.212 | CN | 2022.01.06 | 2022.01.16 | Bruteforce | 6379 |
| 12 | 85.242.*.174 | PT | 2022.01.01 | 2022.02.12 | Mirai | 23,81 |
| 13 | 131.196.*.20 | EC | 2022.01.01 | 2022.01.16 | Bruteforce | 23, 80, 8080 |
| 14 | 138.121.*.209 | BR | 2022.01.01 | 2022.03.16 | Bruteforce | 23, 80, 8080 |

| Idx. | IP address | Country code | Darknet hit date | CTI registered date | Malicious type | Access port |
|---|---|---|---|---|---|---|
| 15 | 145.255.*.37 | RU | 2022.01.01 | 2022.01.20 | Mirai | 23, 2323 |
| 16 | 182.188.*.145 | PK | 2022.01.05 | 2022.03.16 | Bruteforce | 23, 2323 |
| 17 | 187.161.*.109 | MX | 2022.01.03 | 2022.03.16 | Bruteforce | 8000,8080,8081 |
| 18 | 85.122.*.196 | RO | 2022.01.01 | 2022.01.17 | Webattack | 23, 80, 8080 |
| 19 | 114.200.*.238 | KR | 2022.01.05 | 2022.01.18 | Bruteforce | 23 |
| 20 | 121.157.*.114 | KR | 2022.01.01 | 2022.01.19 | Webattack | 23, 81 |
| 21 | 49.158.*.66 | TW | 2022.01.04 | 2022.01.20 | Bruteforce | 23,2323,27015 |
| 22 | 218.37.*.214 | KR | 2022.01.04 | 2022.01.23 | Mirai | 23,2323 |
| 23 | 200.179.*.34 | BR | 2022.01.01 | 2022.01.25 | Bruteforce | 23, 80, 8080 |
| 24 | 119.160.*.220 | BN | 2022.01.01 | 2022.01.25 | Bruteforce | 23,2323 |
| 25 | 90.188.*.118 | RU | 2022.01.01 | 2022.01.26 | Bruteforce | 23,2323 |
| 26 | 217.79.*.142 | BG | 2022.01.01 | 2022.01.27 | Bruteforce | 23, 80, 8080 |
| 27 | 123.213.*.223 | KR | 2022.01.06 | 2022.01.29 | Mirai | 23 |
| 28 | 190.63.*.194 | EC | 2022.01.06 | 2022.01.29 | Bruteforce | 23, 80, 8080 |
| 29 | 179.208.*.204 | BR | 2022.01.03 | 2022.01.29 | Webattack | 23, 2323 |
| 30 | 185.124.*.175 | PL | 2022.01.02 | 2022.01.30 | Webattack | 23, 80, 8080 |

## References


[1] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6G Internet of Things: A Comprehensive Survey," IEEE Internet of Things Journal, vol. 9, no. 1, pp. 359-383, Aug. 2021.

[2] D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 269-283, Jan. 2017.

[3] K. Ogawa, K. Kanai, K. Nakamura, H. Kanemitsu, J. Katto, and H. Nakazato, "IoT device virtualization for efficient resource utilization in smart city IoT platform," 2019 IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 419-422, Mar. 2019.

[4] N. Y. Philip, J. J. P. C. Rodrigues, H. Wang, S. J. Fong, and J. Chen, "Internet of Things for In-Home Health Monitoring Systems: Current Advances, Challenges, and Future Directions," IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 300-310, Jan. 2021.

[5] A. H. Anwar, N. O. Leslie, and C. A. Kamhoua, "Honeypot Allocation for Cyber Deception in Internet of Battlefield Things Systems," 2021 IEEE Military Communications Conference, pp. 1005-1010 , Nov. 2021.

[6] A. Shamayleh, M. Awad, and J. Farhat, "IoT based predictive maintenance management of medical equipment," Journal of Medical Systems, vol. 44, no. 4, pp. 1-12, Feb. 2020.
[7] C. Shao, H. Roh, and W. Lee, "Next-generation RF-powered networks for Internet of Things: Architecture and research perspectives," Journal of Network and Computer Applications, vol.128, no.1 pp. 23-31, Dec. 2018.
[8] F. Chen, D. Luo, T. Xiang, P. Chen, J. Fan, and H.-L. Truong, "IoT cloud security review: A case study approach using emerging consumer-oriented applications," ACM Computing Surveys, vol. 54, no. 4, pp. 1-36, May. 2022.
[9] J. Kim and W. Lee, "Feasibility Study of 60 GHz Millimeter-Wave Technologies for Hyperconnected Fog Computing Applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1165-1173, Oct. 2017.
[10] A. Augustin, J. Yi, T. Clausen, W. M. Townsley, "A study of LoRa: Long range & low power networks for the internet of things." Sensors, vol. 16, no. 9, pp. 1-18, Sep. 2016.
[11] C. Shao, O. Muta, W. Wang, and W. Lee, "Toward Ubiquitous Connectivity via LoRaWAN: An Overview of Signal Collision Resolving Solutions," IEEE Internet of Things Magazine, vol. 4, no. 4, pp. 114-119, Dec. 2021.
[12] R. K. Jha, Puza, H. Kour, Manoj Kumar, and Shubha Jain, "Layer based security in narrow band Internet of Things (NB-IoT)," Computer Networks, vol. 185, Feb. 2021.
[13] I. Choi, J. Lee, T. Kwon, K. Kim, Y. Choi, and J. Song, "An Easy-to-use Framework to Build and Operate AI-based Intrusion Detection for In-situ Monitoring," 2021 16th Asia Joint Conference on Information Security, pp. 1-8, Aug. 2021.
[14] Y. Lee, H. Moon, G. Park, T. Kim, and J. Song, "Trends on cyber threats and their countermeasure technologies in COVID-19," Review of KIISC, 31(5), pp. 5-12 , Oct. 2021.
[15] M. Antonakakis et al., "Understanding the mirai botnet,"" 26th USENIX Security Symposium, pp. 1093-1110, Aug. 2017.
[16] B. Vignau, R. Khoury, and S. Hallé, "10 years of IoT malware: A feature-based taxonomy," 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion, pp. 458-565, Jul. 2019.
[17] J. Sahota and N. Vlajic, "Mozi IoT Malware and Its Botnets: From Theory To Real-World Observations," 2021 International Conference on Computational Science and Computational Intelligence, pp. 698-703, Dec. 2021.
[18] B. Stephens, A. Shaghaghi, R. Doss, and S. S. Kanhere, "Detecting Internet of Things Bots: A Comparative Study," IEEE Access, vol. 9, pp. 160391-160401, Nov. 2021.
[19] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: A novel honeypot for revealing current IoT threats," Journal of Information Processing, vol. 24, no. 3, pp. 522-533, May 2016.
[20] J. D. Guarnizo, A. Tambe, S. S. Bhunia, M. Ochoa, N. O. Tippenhauer, A. Shabtai, Y. Elovici, "Siphon: Towards scalable high-interaction physical honeypots," 3rd

ACM Workshop on Cyber-Physical System Security, pp. 57-68, Apr. 2017.
[21] Meidan, Yair, et al. "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12-22, Dec. 2018.
[22] Nishijima, Katsuya, et al. "Verification of the Effectiveness to Monitor Darknet across Multiple Organizations," 2021 Ninth International Symposium on Computing and Networking Workshops, pp. 346-351, Nov. 2021.
[23] J. Park, T. Kwon, Y. Lee, S. Choi, and J. Song, "A Study on Detecting Black IPs for Using Destination Ports of Darknet Traffic," Journal of the Korea Institute of Information Security and Cryptology, 27(4), pp. 821-830, Aug. 2017.
[24] K.-I. Kim, S.-S. Choi, H.-S. Park, S.-J. Ko, and J.-S. Song, "A Study on Collection and Analysis Method of Malicious URLs Based on Darknet Traffic for Advanced Security Monitoring and Response," Journal of the Korea Institute of Information Security and Cryptology, 24(6), pp. 1185-1195, Dec. 2014.
[25] S. Torabi, E. Bou-Harb, C. Assi, M. Galluscio, A. Boukhtouta, and M. Debbabi, "Inferring, characterizing, and investigating internet-scale malicious IoT device activities: A network telescope perspective," 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 562-573, Jun. 2018.
[26] F. Shaikh, E. Bou-Harb, N. Neshenko, A. P. Wright, and N. Ghani, "Internet of Malicious Things: Correlating active and passive measurements for inferring and characterizing internet-scale unsolicited IoT devices," IEEE Communications Magazine, vol. 56, no. 9, pp. 170-177, Sep. 2018.
[27] M. S. Pour, D. Watson, and E. Bou-Harb, "Sanitizing the iot cyber security posture: An operational cti feed backed up by internet measurements," 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 497-506, Jun. 2021.
[28] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019.
[29] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10102-10110, Oct. 2020.
[30] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features," Electronics, vol. 9, no. 1, pp. 1-19, Jan. 2020.
[31] L. G. Greenwald and T. J. Thomas, "Toward undetected operating system fingerprinting," 1st USENIX Workshop on Offensive Technologies, pp. 1-10, Aug. 2007.
[32] VirusTotal, "Malware and URL Scanner", https://www.virustotal.com, 8. 25. 2022.
[33] AlienVault, "Open Threat Exchange", https://otx.alienvault.com, 8. 25. 2022.

## 〈저 자 소 개〉

박 건 량 (Gunyang Park) 정회원
2013년 8월: 대전대학교 전산정보보호학과 졸업
2020년 2월~현재: 고려대학교 일반대학원 사이버보안학과 석사과정
2013년 9월~2018년 12월: 국가보안기술연구소 기술원
2019년 6월~현재: 한국과학기술정보연구원 과학기술보안연구센터 연구원
〈관심분야〉 네트워크 보안, 보안관제, 악성코드 분석, 사이버위협인텔리전스

송 중 석 (Jungsuk Song) 정회원
2003년 2월: 한국항공학교 통신정보공학 졸업
2005년 2월: 한국항공학교 정보공학 석사
2009년 3월: 교토학교(일본) 지능정보학 박사
2009년 4월~2010년 9월: 일본정보통신연구원 정보통신 보안연구소 전문연구원
2010년 10월~2011년 9월: 일본정보통신연구원 네트워크 보안연구소 선임연구원
2011년 10월~2018년 3월: 한국과학기술정보연구원 과학기술사이버안전센터 선임연구원
2018년 3월~현재: 한국과학기술정보연구원 과학기술보안연구센터 책임연구원
2012년 9월~현재: 과학기술연합학원학교 데이터 및 HPC 과학 교수
〈관심분야〉 보안관제, 침해사고대응, 악성코드 분석, 네트워크 보안

노 희 준 (Heejun Roh) 종신회원
2009년 2월: 고려대학교 컴퓨터학과 졸업
2011년 2월: 고려대학교 컴퓨터·전파통신공학과 석사
2017년 2월: 고려대학교 컴퓨터·전파통신공학과 박사
2019년 3월~현재: 고려대학교 일반대학원 사이버보안학과 조교수
〈관심분야〉 유무선 네트워크 보안, IoT 보안