사물인터넷(IoT) 봇넷 악성코드 동향 분석

구준한

사물인터넷(IoT)

- 인터넷에 연결되어 있는 장치 또는 산업 장비 등 데이터를 공유할 수 있는 사물
- Gartner : 2030년 IoT 장비 500억 개로 증가할 것으로 분석

  → 의료, 스마트 홈, 스마트 공장 등 다양한 분야로 확장
- 컴퓨팅 리소스가 적어 외부 침입 방어를 위한 시스템 구축 어려움

  → 공격자들의 주요 타깃으로 사이버 위협 증가

봇넷(botnet)

- 1990년대 처음 등장한 악성코드 종류
- 하나 이상의 호스트를 감염시켜 만들어진 봇(bot)으로 구성된 네트워크
- 대표적인 공격 : DDoS

- 과거 : IRC(Internet Relay Chat) 서버를 통한 제어
- 현재 : P2P(Peer to Peer) 분산 구조

IoT 봇넷

- **환경적 요인**
  1. IoT 장치는 컴퓨팅 리소스가 적음
  2. 외부 침입을 방지하기 위한 환경 (안티바이러스) 구축이 어려움

     → 공격자가 공격하기 최적인 환경

- **사용자 요인**
  1. 초기 관리자 비밀번호 미변경
  2. 최신 펌웨어 업데이트 미수행

IoT 봇넷 구성

- **봇넷**

  감염된 좀비 IoT 장비

- **C&C (C2) 서버**

  공격 명령을 내리는 서버

  (매개변수 : 공격 유형, 공격 대상 IP 또는 URL, 공격 기간 등…)

- **로더**

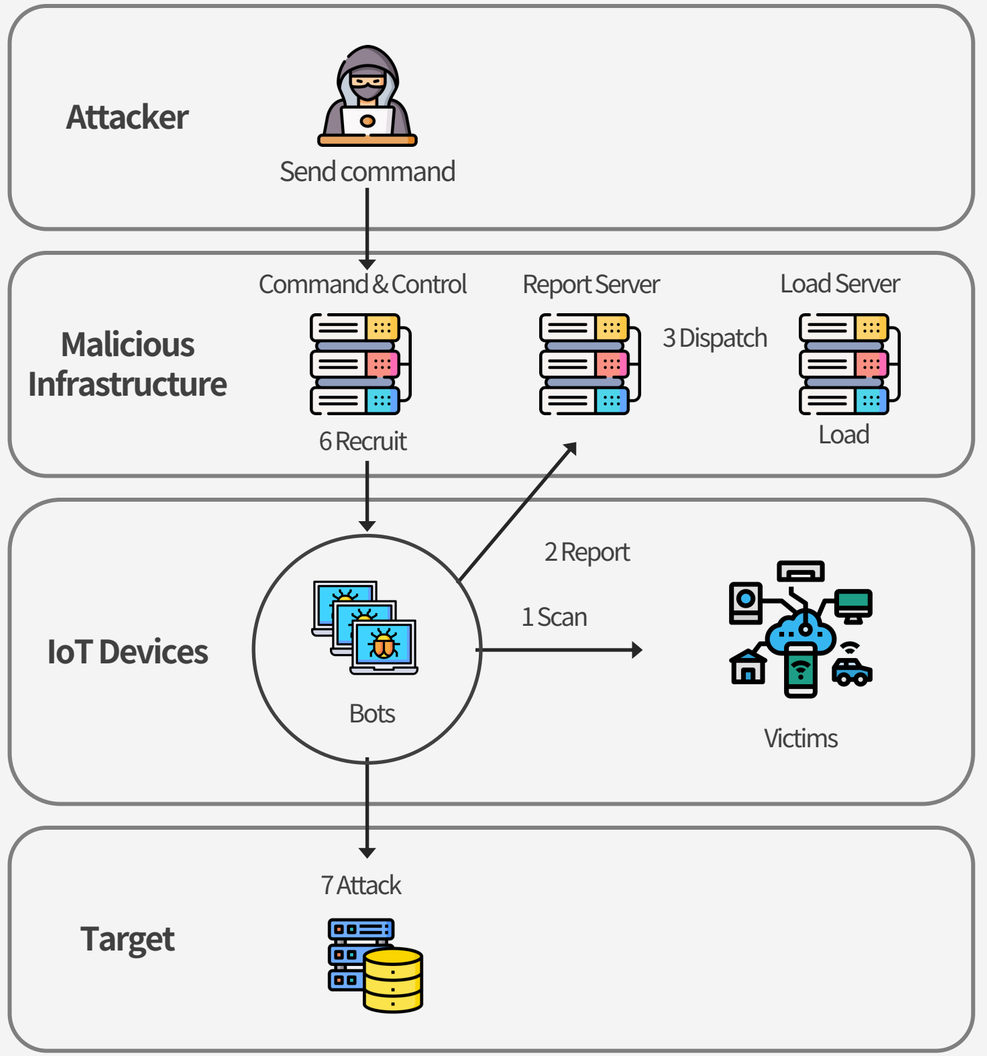
  IoT 장치 침입에 성공 시 해당 장치 아키텍처에 맞는

  악성코드 바이너리 파일 다운로드 및 실행

- **리포트 서버**

  감염된 봇넷의 정보를 보관하고 있는 서버

  (IP 주소, 포트, 하드웨어 아키텍처, 로그인 자격 증명 등…)



IoT 봇넷 공격 유형

1. DDoS 공격
2. 암호화폐 채굴
3. 익명 프록시
4. 정보 수집
5. 장치 종료

Mirai 악성코드

- 2016년 최초 발견
- 현재까지 DDoS 공격에 가장 많이 사용 된 악성코드

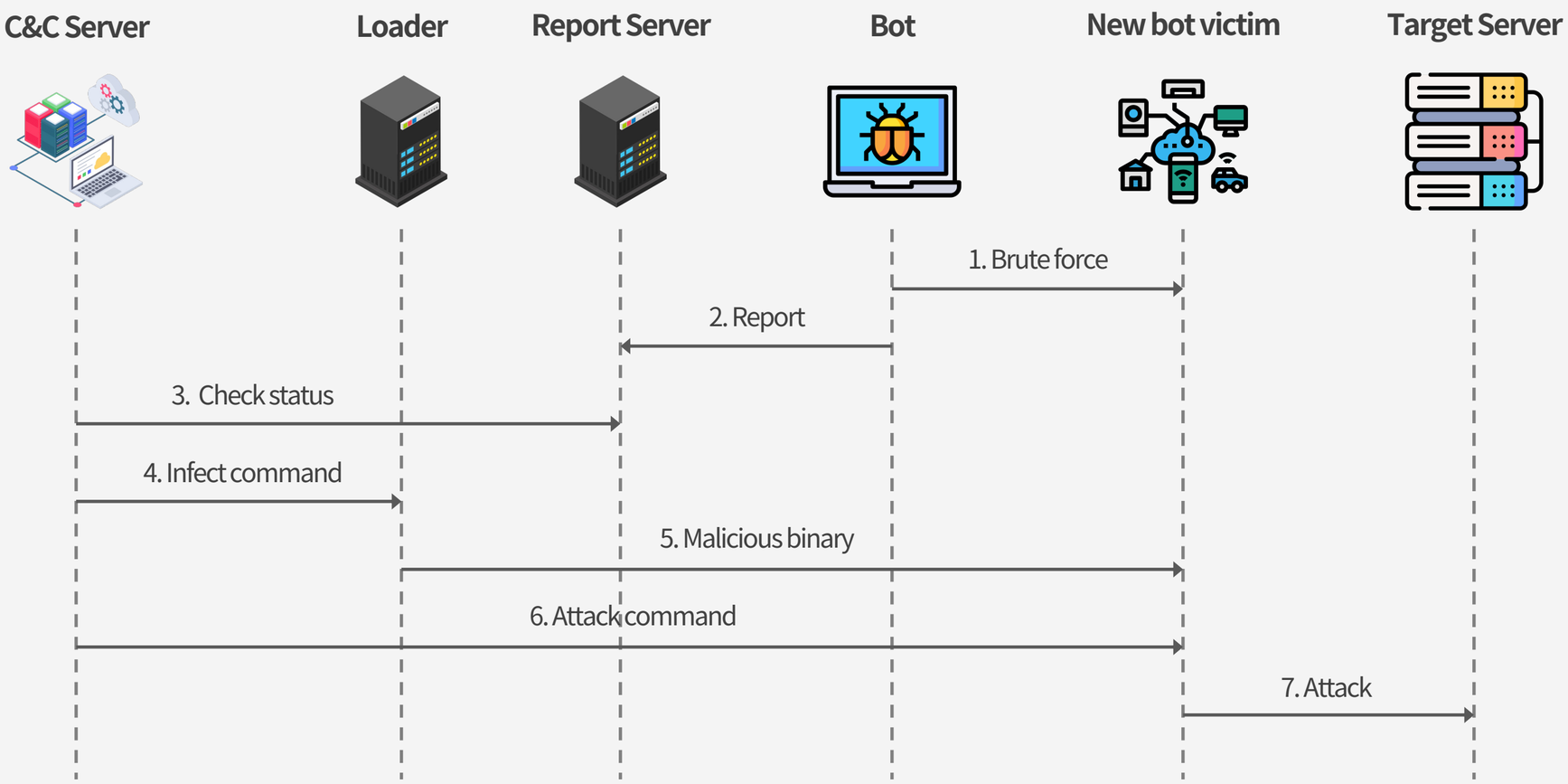
  → 2016년 Dyn, OVH Hosting 공격
- BusyBox* 기반 라우터, DVR, 웹캠 등의 장치가 타겟
- Github에 소스코드 공개

  → 공개된 소스코드를 통해 대비가 가능할 것이라 예측하였으나,

  이를 이용한 새로운 여러 변종 악성코드가 발견
- 감염된 장치를 통해 주변의 또 다른 장치를 계속 감염

*타 운영체제에서 유닉스 명령어를 사용할 수 있도록 만들어 주는 소프트웨어

Mirai 악성코드 작동 과정



Keksec 악성코드

- 2022년 3월 발견
- Gafgyt를 기반, Mirai의 모듈을 다수 채용
- 자신을 은닉하기 위해 문자열 난독화 기술 사용
- C&C 서버는 하드코딩 된 Socks 프록시 IP주소 구성
- Tor 네트워크를 통해서만 접근 가능하도록 은닉
- Log4j를 포함한 여러 취약점을 이용한 공격 코드 발견
- IoT 장치 이외 macOS, x64 기반 서버와 데스크톱 감염 가능
- Android 디버그 브리지(adb)포트 5555 노출된 Android 장치 공격 코드 발견

Mozi 악성코드

- 2019년 12월 발견
- 피어 검색 및 데이터 송수신 시 분산형 해시 프로토콜(DHT) 사용
- 117개의 ID/Password 조합 발견

- 2020년 7월 개발자 및 운영자가 체포되었으나 여전히 감염은 진행 중
- 2022년 1월 국정원 : 국내 공공기관 IoT 장비 100여대 감염으로 주의보 발령 (전 세계 1만 2천대 추정)

OMG 악성코드

- 2018년 2월 발견
- Proxy 서버로 만드는 것이 목적
- http 및 socks 통신 시 필요한 임의의 두 포트의 트래픽을 허용하는 방화벽 규칙 추가 코드 발견
- 감염된 장치의 사설 네트워크 접속 가능
- Mirai 기능은 보존되어 있음

Bashlite(Gafgyt) 악성코드

- Mirai 악성코드의 전신
- GitHub를 통한 소스코드 공개
- C&C 서버와 통신 시 평문으로 송수신

  → Mirai는 바이너리 프로토콜을 통해 통신
- TCP SYN 플러딩 공격이 대표적 (DDoS)

HnS 악성코드

- 2018년 4월 발견
- 일반적인 봇넷은 IoT 장치를 재부팅 하면 사라짐

  → 하지만 HnS는 재부팅해도 악성코드 보존
- DDoS 공격 기능은 미포함

06. 결론

HPSC LAB
High Performance & Secure Computing

- IoT 봇넷을 통한 공격은 낮은 비용으로 대규모 활동 가능
- Mirai 소스코드를 이용한 변종은 계속 등장
- 넷스카우트 : 2021년 975만회의 DDoS 공격 탐지

  랜섬 DDoS 공격을 받은 특정 VoIP 기업 약 1,200만 달러 손실 발생
- DDoS 뿐만 아니라 암호화폐 채굴 등 다양한 목적의 봇넷 등장 전망
- 제조사 차원의 취약점 업데이트 필요 및 국가적 차원의 강제성 필요
- Keksec 악성코드를 통해 IoT 포함 BusyBox 기반 장치는 모두 감염 대상

Thank You