봇넷

https://youtu.be/wZ4FwW515Tg

봇넷?

- **봇넷(botnet) = 로봇(Robot) + 네트워크(Network)**
- 인터넷에 연결되어 있으면서 위해를 입은 여러 컴퓨터들의 집합
- 다수의 좀비 컴퓨터로 구성되어 있는 네트워크
- 봇마스터에 의해 원격 조정
- DDoS공격, 개인정보 수집, 스팸 메일 전송 등에 이용

봇넷의 역사?

- 1998년 **최초로 웜 개발** 성공 (로버트 모리스 주니어)
- 1999년 **IRC**통신을 통해 감염된 PC로 명령 받는 최초의 악성코드 개발
- 2004년 **P2P** 사용한 최초의 봇넷 개발
- 2013년 **안드로이드** 봇넷 발견
- 2016년 최초로 **사물인터넷**을 이용한 봇넷 등장

봇넷 프로토콜

- **IRC**
- **HTTP**
- **P2P**
- **TOR**

봇넷 프로토콜

- **IRC**

✓ 중앙 집중형 구조, 보안성 ↓

✓ 가장 보편적으로 사용되는 방식

✓ IRC를 통해 비밀 채널을 생성하여 사용

✓ 디도스 공격용 봇넷의 경우, IRC 채널 방식을 가장 선호

https://namu.wiki/w/IRC

봇넷 프로토콜

- **HTTP**

  ✓ 정상적인 HTTP 웹 트래픽 속에 섞여 발각되지 않도록 하는 방식

  ✓ 도메인 생성 알고리즘 사용하여, 도메인 주소로 C&C서버 노출 방지

  ✓ FAST-FLUX DNS 기법 사용

봇넷 프로토콜

✓ **Fast-Flux DNS**

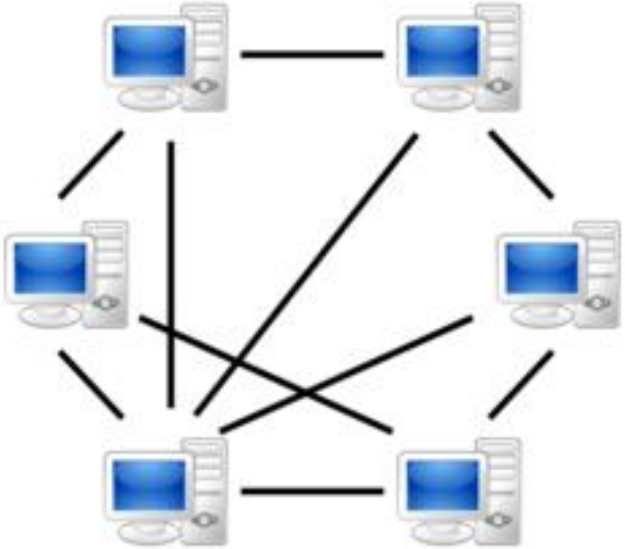
- 한 개의 도메인 주소에 다수의 IP 주소를 매핑시켜 놓는것
- 대응된 IP 주가 짧은 시간 간격으로 변경되는 것
- TTL(Time-To-Live) 시간도 짧게 대략 5분 이내로 지정

봇넷 프로토콜

- **P2P**

  ✓ 각 노드 C&C 서버 기능 수행

  ✓ 분산형 구조

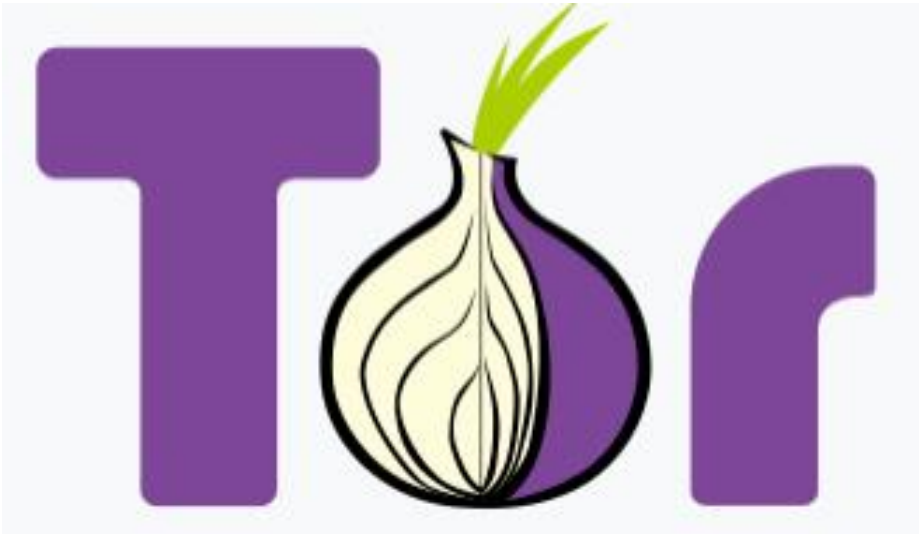


봇넷 프로토콜

- **Tor**

  ✓ Tor 네트워크에서 제공하는 서비스를 이용하여 C&C 서버 운영

  ✓ 제우스 트로잔 봇넷이 토르 방식 사용

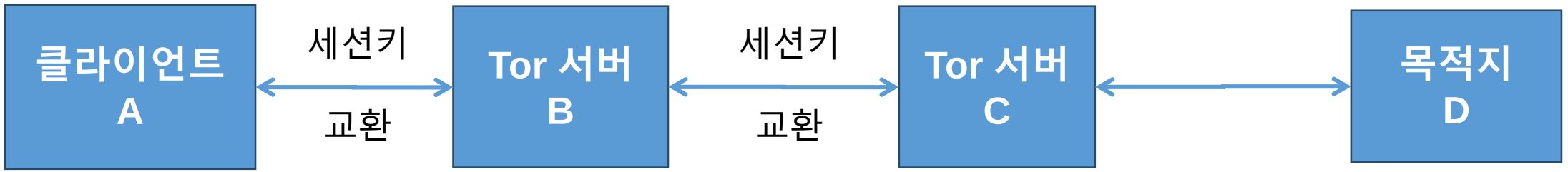


봇넷 프로토콜

✓ **Tor 네트워크**

세션키 교환: Diffie - Hellman 키 교환 방식

통신의 암호화 : AES



봇넷의 구성

- **봇넷 컨트롤러**

  ✓ 봇넷을 컨트롤 하는 공격자는 원격에서 C&C 서버 or 특정한 좀비 디바이스에 명령 전달

- **C&C 서버**

  ✓ 좀비 디바이스에 명령을 전달
  ✓ 좀비디바이스로부터 정보를 수신

- **P2P 봇넷**

  ✓ 봇넷을 보호하고 네트워크가 끊기는 것을 방지

- **좀비 디바이스**

  ✓ 봇넷 중 인터넷을 통해 연결되어 있는 각각의 디바이스
  ✓ PC 스마트폰 태블릿 iot등으로 확대

미라이 봇넷

- 2016년 9월 처음 공격 시작
- 미라이 봇넷 코드는 배포되어 누구든지 불법행위 가능
- 보안 카메라 등 보안이 허술한 사물인터넷 기기에 악성코드를 설치하여 인터넷 트래픽을 라우팅하는 DYN 서버를 공격하는 방식

미라이 봇넷

- 스캔 기능

  ✓ 최초 실행 시 네트워크 스캔 기능을 수행하여 사전식 전시공격 시도

- 전파 기능

  ✓ IoT 기기에 접속 성공 후 악성코드 주입하여 실행하는 과정 반복
  ✓ 악성코드 다운로드 실패시, Busybox를 주입하여 전파

- 재부팅 방지 기능

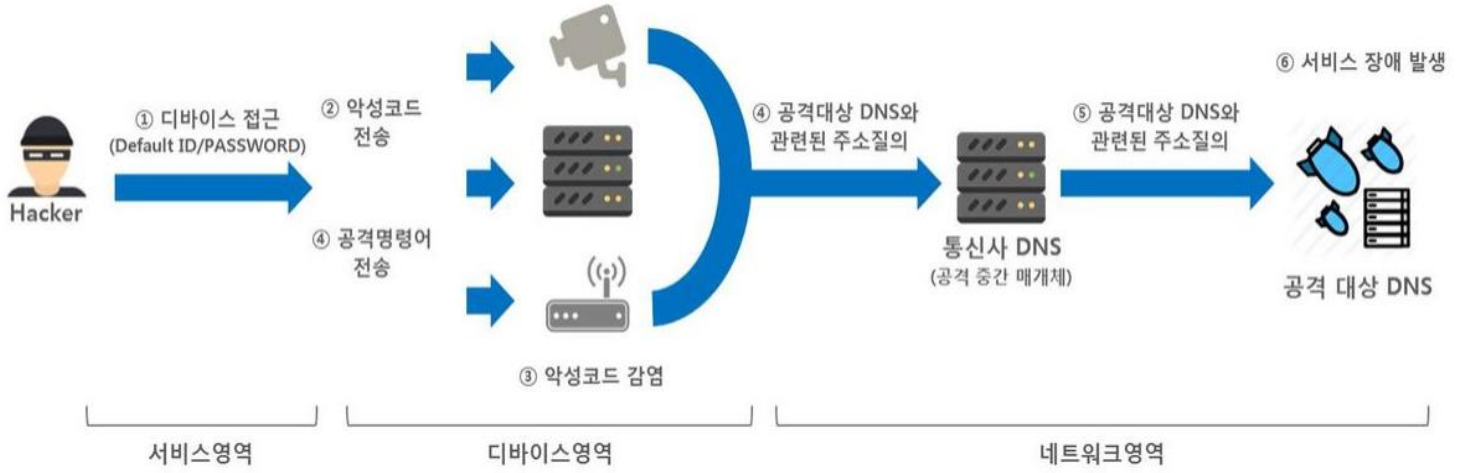
- 디도스 공격

미라이 봇넷

- 동작원리

임베디드 기기 스캐닝 접속 → 악성코드 전파 및 감염 → 취약한 기기 감염

으로 좀비PC 확보 → 봇넷 구성 → 봇넷을 이용한 디도스 공격



Q & A