7.7 DDoS 공격 사고 분석

202219934
it지능정보공학과
정보경

목 차

7.7 DDoS
공격 사고 분석

DDoS 공격이란?

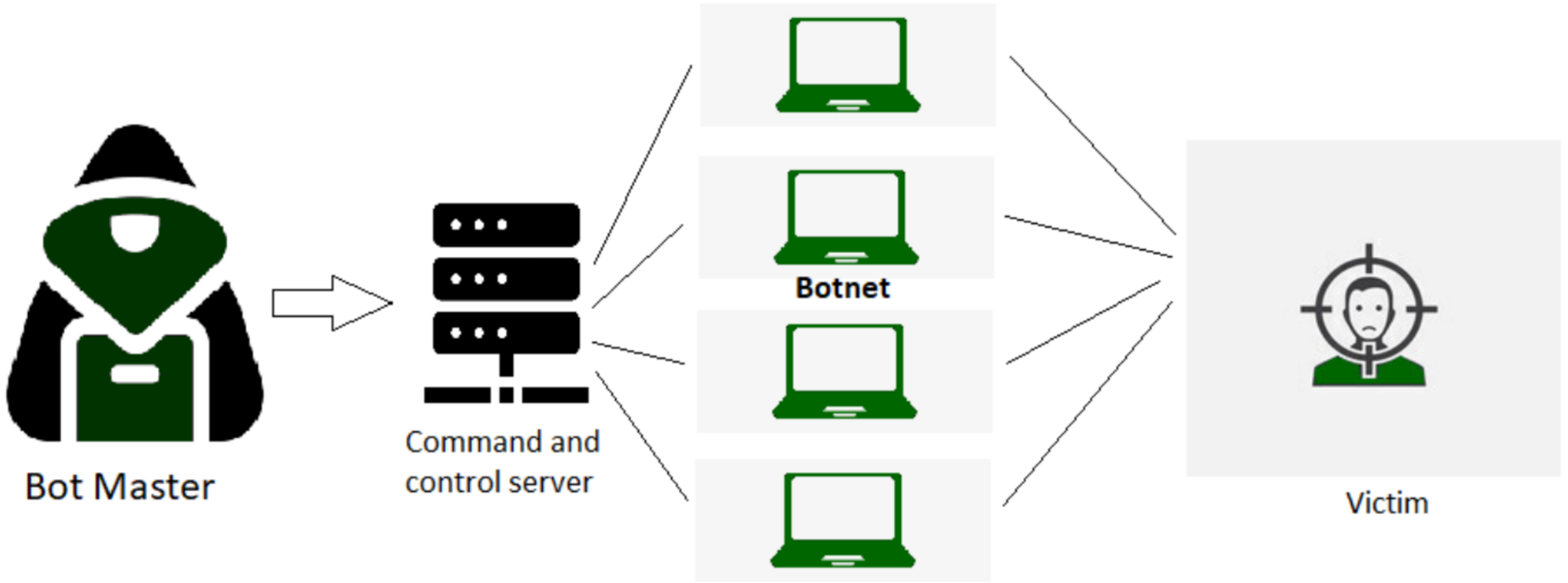
Distributed Denial of Service

- 공격하는 컴퓨터를 분산배치해 '서비스 거부 공격'을 하는 것
- 해커가 감염시킨 개인용 컴퓨터(PC) 또는 서버로 공격을 하여 특정 시스템 자원을 고갈시킴으로서 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격 방법
- 최초의 디도스 공격 중 하나는 1999년 미국 미네소타 대학의 홈페이지를 공격한 기록 (114대의 컴퓨터를 사용했음)

DDoS 공격 종류

- 증폭 : 피해 대상 리소스 대역폭을 포화 상태로 만들어 대량의 트래픽으로 네트워크를 압도함
  - UDP Flood, ICMP Flood 공격
- 프로토콜 : 프로토콜 통신을 악용하는 악의적인 연결 요청을 통해 서버나 방화벽과 같은 다양한 네트워크 인프라 리소스의 컴퓨팅 용량을 소비하고 고갈시키려고 시도
  - SYN Flood, Smurf 공격
- 어플리케이션 레이어
  - HTTP Flood 공격: HTTP 요청으로 대상 서버를 압도하도록 설계

DDoS 공격이란?



7.7 DDoS 공격 사건

- 2009년 7월7일부터 만 3일동안 좀비PC 11만 5천여대가 청와대 홈페이지를 포함, 국내.외 주요 홈페이지를 공격하여 접속 장애를 발생시킴

- 금품요구를 목적으로 이루어진 대부분의 해킹과는 다르게 사회적 공공재를 겨냥한 테러의 성격을 띰

- 공격 자체를 널리 알리려는 목적이 강한 것으로 판단됨

<표 1> 국내 피해사이트 현황

구분	일자	피해사이트				소계
1차	7. 7 18:00 ~ 7. 8. 18:00	청와대 국방부	옥션 조선일보 네이버 (메일)		외교통상부, 국회 한나라당, 농협 신한은행 외환은행 네이버(블로그)	12
2차	7. 8 18:00 ~ 7. 9. 18:00	청와대 국방부	옥션 조선일보 네이버 (메일)	전자민원G4C 다음(메일) 파란(메일) 국민은행	기업은행 하나은행 우리은행 국가사이버안전센터 알툴즈 안철수연구소	15
3차	7. 9 18:00 ~ 7. 10. 18:00		옥션 조선일보 네이버 (메일)	전자민원G4C 다음(메일) 파란(메일) 국민은행		7

자료출처 : 방송통신위원회, 국회 국정감사 제출자료, 2009.10

7.7 DDoS 공격 분석

- 공격을 위한 치밀한 사전계획

  - 시차를 두고 순차적으로 1차, 2차, 3차 공격을 하였음

  - 다른 DDoS 공격에서는 실시간으로 이용됐던 C&C서버가 실시간이 아니라 pc에 감염되는 악성코드에 사전에 공격 대상과 시간을 담은 스케줄이 있어 C&C서버와 통신 없이도 계획된 시각에 지정된 목표를 공격한 것

  - 마지막 공격에서는 치료등으로 좀비PC의 수가 줄어들 것을 예상하고 공격 도중 컴퓨터 기억저장장치 파괴하라는 자폭명령이 내려짐

구 분	기존 DDoS	7.7 DDoS
명령 · 제어 서버 존재여부	해커로부터 명령을 받는 명령 · 제어 서버 존재	악성코드를 업데이트하는 서버 존재
공격 방법	명령 · 제어 서버의 네트워크를 통한 실시간 공격 제어	일정 주기로 악성코드를 업데이트 받아 스케줄링을 통한 공격
감염경로	윈도우즈 또는 브라우저 취약점을 악용한 홈페이지 악성코드로 인한 감염	공격자가 정상적인 프로그램에 숨겨둔 악성코드가 동작
방어 방법	명령 · 제어 서버 차단	공격PC의 악성코드 제거
공격 대상	홈페이지 1~2개	다수 홈페이지에 동시 다발 공격
악성코드 갯수	DDoS 공격을 수행하는 악성코드 1개 다운로드	압축파일 형태의 악성코드를 다운로드, DDoS 공격 외에도 다양한 악성행위 수행
네트워크 연결정보	평문 채널을 통한 통신으로 공격명령내용 모니터링 가능	암호화된 채널을 사용하여 통신하므로 통신내용 확인 불가
악성 행위	해커의 명령을 지속적 수행	단기공격 수행후, 하드디스크 삭제
공격 목적	금전적 이득	사회혼란 유발(추정)
공격 주체	주로 중국 등에 위치한 해커 조직	미확인

7.7 DDoS 공격 분석

- **감염경로 불특정**

  - 좀비PC 악성코드는 감염 경로를 추적할 만한 정보를 모두 제거함

- **최종적으로 좀비PC를 파괴하는 특징**

  -일반적으로 좀비PC는 또 다른 추후 공격에 사용할 목적으로 유지하는데 반해, 7.7 DDoS의 경우 목적달성 후 좀비PC 자신의 하드디스크를 손상시키는 행위를 수행함

구 분	기존 DDoS	7.7 DDoS
명령 · 제어 서버 존재여부	해커로부터 명령을 받는 명령 · 제어 서버 존재	악성코드를 업데이트하는 서버 존재
공격 방법	명령 · 제어 서버의 네트워크를 통한 실시간 공격 제어	일정 주기로 악성코드를 업데이트 받아 스케줄링을 통한 공격
감염경로	윈도우즈 또는 브라우저 취약점을 악용한 홈페이지 악성코드로 인한 감염	공격자가 정상적인 프로그램에 숨겨둔 악성코드가 동작
방어 방법	명령 · 제어 서버 차단	공격PC의 악성코드 제거
공격 대상	홈페이지 1~2개	다수 홈페이지에 동시 다발 공격
악성코드 갯수	DDoS 공격을 수행하는 악성코드 1개 다운로드	압축파일 형태의 악성코드를 다운로드, DDoS 공격 외에도 다양한 악성행위 수행
네트워크 연결정보	평문 채널을 통한 통신으로 공격명령내용 모니터링 가능	암호화된 채널을 사용하여 통신하므로 통신내용 확인 불가
악성 행위	해커의 명령을 지속적 수행	단기공격 수행후, 하드디스크 삭제
공격 목적	금전적 이득	사회혼란 유발(추정)
공격 주체	주로 중국 등에 위치한 해커 조직	미확인

7.7 DDoS 공격 사건 분석

- 최초 감염은 msiexec.exe라는 파일이 DDoS 공격을 수행하는 악성코드에 감염되면서 시작

- 공격자는 웹하드 서비스 업체의 서비스 서버에 침입하여 웹하드 프로그램 업데이트 파일에 악성코드를 심어 놓고 웹하드 서비스를 이용하는 사용자의 PC는 수행 시 자동으로 업데이트되면서 msiexec.exe 파일을 감염시킨 것