9차시. 4차 산업혁명과 사이버 전쟁

01. 사이버 전쟁의 이해

- 2013년 6월 25일 국제 해커집단인 어나니머스가 북한을 대상으로 대대적인 사이버공격을 감행 하였고 우리나라도 북한의 정찰총국 소속 해커부대 소행으로 추정되는 사이버공격을 받았다. 청와대를 비롯한 주요 정부기관 등이 홈페이지 변조, 전산망 마비, 개인 신상정보 유출 등의 피해를 입었다. 6.25 사이버공격의 특징은 디버깅을 회피할 수 있는 프로그램을 사용하여 분석과 탐지를 어렵게 하였고 역추적을 하지 못하도록 하는 프로그램을 사용하였으며, 현재 지능형 공격(APT: Advanced Persistent Threat)으로 분류되는 공격을 탐지할 수 있는 솔루션을 회피할 수 있는 기능도 있었다. 아울러 공격 이후에는 컴퓨터 내에 저장된 파일 삭제, 사용자의 컴퓨터를 재부팅할 때 하드디스크 파괴 등의 피해를 입혔다.
- 2013년 3월 20일에는 KBS, MBC, YTN 방송사와 신한은행, 농협, 제주은행 등 방송·금융기관 6곳이 사 이버 공격으로 전산망이 마비됐으며 일부 방송사의 홈페이지는 접속불능 사태가 발생하였다. 4.10일 미래창조과학부는 3.20 사이버테러 주체자로 북한 정찰총국을 지명하였다. 민·관·군 합동대응팀은 접속경로를 추적결과 지난 2월말 북한 측이 내부 PC로 해외 IP를 이용, 우회경로를 통해 피해업체에 악성코드를 감염시킨 사실을 확인했다.
- 이러한 사이버공격에 대비하여 선진국들은 사이버전력을 강화하거나 새로운 개념의 국가 사이버 안보 전략을 수립하고 있다. 우리나라도 사이버사령부 창설, 사이버안보 컨트롤타워 설립 추진, 한·미 사이버안보 협정 체결 등 사이버전력 강화에 노력을 기울이고 있다.

사이버 전쟁의 이해

- 사이버 공격이란 국가의 주도적인 계획과 의도가 반영된 사이버 공격을 의미한다. 사이버 테러, 사이버 첩보 및 사이버 전쟁이 포함된다. 사이버 테러는 인터넷 기반의 테러 활동으로 사이버 무장 단체 조직인 핵티비스트, 어노니머스, 위키리크스(어산지)가 대표적이다. 사이버 첩보는 트로이목마, 스파이웨어와 같은 해킹기술을 이용하여 개인, 경쟁자, 정부 등이 보유한 정보를 허락 없이 획득하는 행위를 의미한다. 사이버 전쟁은 전자적 수단을 동원하여 적의 IT 자원이나 네트워크를 공격하는 것으로 자국의 정보를 보호하기 위한 다양한 방어적인 전략들도 포함된다.
- 구체적으로 사이버 전쟁은 특정 국가 또는 이에 준하는 집단이, 다른 국가의 컴퓨터 시스템이나 네트워크 등에 대하여 무력사용이나 전투에 이를 정도로 심각한 사이버 공격을 감행하여, 생명, 신체, 재산에 대한 실질적인 피해를 야기함으로써, 국가 차원의 대응 활동이 요구되는 안보 위협 상황이라고 정의할 수 있다.

- 하지만 어떠한 사이버 공격이 사이버 전쟁에 해당하며, 해당 사이버 공격에 대하여 사이버 전쟁이나 재래식 공격을 감행할 수 있는지에 대하여 검토해 보아야 한다.
- **사이버 전쟁의 특징**

  - 물리적인 충돌 없이 승리할 수 있는 최신 비대칭전의 한 영역

  . 적은 비용으로 최대 효과와 함께 공격자의 익명성 유지 가능

  . 공격자가 노출돼도 보복이 어려운 공격자에게만 유리한 전쟁 형태

  - 사이버전은 비국가행위자(Non-State Actors)인 개인에 의해서도 수행 가능

  . 국제법은 국가 간 무력 사용만을 규제

  . 사이버공격은 누구나 S/W 개발 능력만 있으면 제작, 구매, 대여해 공격을 진행할 수 있는 점에서 위험성이 존재

  - 사이버전은 대부분 물리적 피해와는 관련이 없어 UN헌장에서 금지하는 무력사용이라 보기 어려움

  - 피해대상 구분의 어려움

  . 목표를 지정(민군 구분)하여 공격이 어려워 윤리성 논란이 존재

  - 공격자 식별 및 사실관계 확인의 어려움

  . 좀비PC의 이용, 타국 서버 경유 등을 통해 공격이 진행되어 공격자를 식별하고 확인이 어렸기 때문에 정당한 보복과 처벌을 통한 전쟁 억제가 곤란

  . 방어자에게 과도한 부담을 지우는 비대칭성

  - 공격자에게도 피해 전파 가능성

  . 인터넷 속성상 사이버 공격이 공격자에게도 전파될 가능성 존재

  . 예를 들어 미국은 이라크 공격 시 이라크 금융시스템 공격을 고려했으나, 여파가 자국에도 미침에 따라 포기

사이버 전쟁의 역사

- 정치적 목적으로 국가 전체를 공격한 최초의 사이버 전으로 2007년 러시아의 에스토니아 사이버 공격을 꼽는다. 에스토니아 정부의 소비에트전 기념 동상 철거 계획으로 러시아와 마찰을 빚으면서 발생하였다. 에스토니아는 러시아의 DDoS(Distributed Denial of Service: 분산 서비스 거부) 공격으로 3주간(4.27~5.18) 국가 시스템 전체가 마비되었다. 봇넷을 이용한 전형적인 사이버 공격이었다. 대통령궁, 의회, 정부기관, 은행, 이동통신 네트워크 등이 공격을 당했다. 에스토니아는 인터넷 무선 접속이 비교적 자유롭고 인구 절반이 인터넷 뱅킹을 사용하고 있어서 그 피해가 심각하였다.


BBC NEWS

Watch One-Minute World News

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news
Video and Audio
Programmes
Have Your Say
In Pictures
Country Profiles
Special Reports

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

E-mail this to a friend Printable version

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says many state websites have been affected

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia technical help.

"In the 21st century it's not just about tanks and artillery," Nato spokesman James Appathurai told BBC News.

"We have sent one of our experts at the request of the Estonian authorities to help them in their defence."

[〈당시 BBC 뉴스기사〉 '모스크바 발 사이버전쟁']

- 러시아의 에스토니아를 대상으로 한 사이버 공격이 시사하는 바는
  - 사이버 공격으로 가상 공간의 피해는 물론 사회적, 물리적 피해를 동반한 군사적 행동
  - 공격주체 추적 곤란
  - 사이버전에 대한 국제적 논의가 필요하다는 인식이 확산되면서 2013년 사이버전 국제법으로 알려진 탈린 매뉴얼이 발표되는 계기가 됨
- 2008년에도 러시아는 그루지아를 사이버 공격을 감행하였다. 그 배경으로는 남오셰티아 자치주의 독립문제로 그루지아가 남오셰티아를 공격하자 러시아가 참전하면서 전면전으로 발발하였다. 사이버 공격은 6월 28일부터 3일간 그루지아 정부의 홈페이지, 언론사, 포털 사이트 등이 대규모 DDoS 공격을 받았다. 평균 2시간 15분, 최장 6시간의 DDoS 공격가운데 평균 211Mbps, 최대 814Mbps의 트래픽 공격으로 사회적 혼란이 야기되었다. 이 공격은 사이버 공격으로 사회를 혼란에 빠뜨린 이후 물리적 공격을 감행한 대표적 사례로 기록되었다. 아래 사진은 당시 그루지아 대통령 및 외교부 홈페이지를 변조하는 공격으로 그루지아 대통령사진이 히틀러 사진과 함께 편집되었다.

북한의 사이버 공격

- **7·7 DDoS 공격**

  2009년 7월 7일부터 3일간 총 61개국 435대 서버를 활용하여 한국과 미국의 주요 기관 등 35개 사이트를 DDoS 공격하여 피해를 입힌 대표적 사이버 테러 사건이다.
  국가정보원은 2009. 10. 29. 열린 국회 정보위원회의 국정감사에서 같은 해 7월 발생한 '디도스공격'에 동원된 IP주소가 북한 체신청이 사용해 온 IP라고 확인하였다.

  DDoS 공격에 이어 디스크 파괴가 발생한 7.7 DDoS 사이버 공격 시나리오는

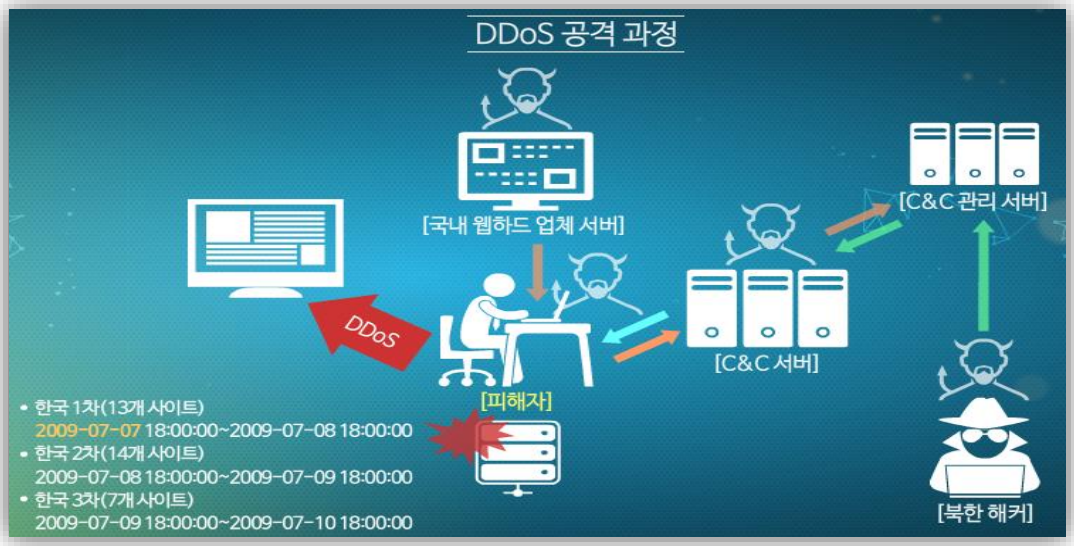
  ① 웹하드 이용자는 감염된 국내 웹하드 업체 서버에 접속하여 업데이트를 위장한 악성코드를 다운로드 받아 감염

  ② 감염된 피해자의 PC는 C&C 서버에 연결

  ③ 북한 해커가 C&C 관리 서버를 통하여 C&C 서버로 공격명령을 전달: C&C서버에 연결된 피해자 PC는 DDoS 공격수행

- **7·7 DDoS 공격**

  ④ DDoS 공격 후 감염된 피해자 PC 하드디스크를 파괴하는 명령을 수행



- **3·4 DDoS 공격**

  2011년 3월 3일부터 3일간 총 70개국 746대 서버를 활용, 국내 주요 40개 사이트를 DDoS 공격하였던 사건으로써, 디도스 공격체계 및 악성코드의 설계방식, 통신방식, 해외 공격명령서버 일부 등이 기존 7·7 DDoS 사건과 동일한 점 등에 비추어, 7·7 디도스 공격자와 동일하다고 확인되었다.

- **2011. 4. 12. 농협 해킹사건**

  2011. 4. 12. 국내 농협전산망 전체가 이용 불가상황에 빠진 초유의 사건으로써, 해당 공격은 농협 유지보수업체 직원의 노트북을 좀비PC로 감염시켜 총 7개월 이상 노트북을 집중 관리, 원격조종하는 지능형 공격(APT: Advance Persistent Threat)에 의한 신종 공격 방식이다.

- **2013. 3. 20. 사이버 테러 사건**

  국내 주요 방송사(KBS · MBC · YTN)와 금융회사(신한은행 · NH농협은행 · 제주은행) 전산망이 2013년 3월 20일 오후 2시경 악성코드에 감염, 총 3만 2000여 대에 달하는 컴퓨터가 일제히 마비되는 사상 초유의 정보보안 사고가 발생했다. 특히, 분석 결과에서 2012년 6월 28일부터 북한 내부 PC 최소한 6대가 1,590회 접속해 금융사에 악성코드를 유포하고 PC저장자료를 탈취한 사실이 확인되었으며, 북한 해커가 사용하고 있는 PC의 고유번호가 붙어있는 악성코드도 18종이나 발견됐다.

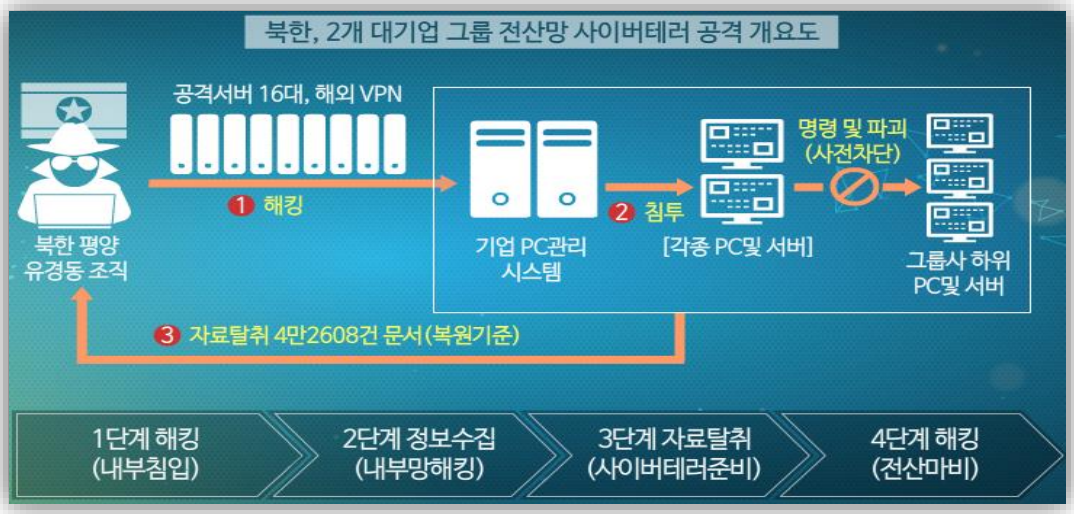
- **2013. 6. 25. 사이버테러 사건**

  청와대, 국무조정실, 새누리당, 연합뉴스, 조선일보, 대구일보, 매일신문 등의 홈페이지가 해킹되고, 주요 정부기관의 서버가 DDoS 공격으로 인하여 마비되는 사태가 발생하였으며, 이 역시 북한의 소행으로 확인되었다.

- **또 다른 공격: 대한항공·SK 해킹**

  2014.7~2016.2 기간 동안 대한항공 등 한진그룹 10개 계열사와 SK 네트웍스 등 SK 17개 계열사가 북한으로부터 공격을 받아 42,608건의 군통신망, F-15 전투기 날개도면, 중고도 무인정찰기 부품 사진 등이 유출된 사건이다. '유령쥐(Ghost Rat)'라는 악성코드로 해당 사의 PC 통합관리망을 공격한 것이다.

  사용된 악성코드는 원격제어, 정찰 및 해킹 등 다용도 기능을 수행하였다. 해킹근원지는 3.20 해킹사건과 같은 IP(평양 유경동 소재) 사용하였다. 아래 그림은 관련 사이버 공격 개용도이다. 공격 시나리오는 해킹, 정보수집, 자료탈취 및 파괴의 과정을 거치도록 설계되었다. 다행히도 마지막 단계인 파괴 행위는 사전에 차단되어 최악의 상황은 면하였다.



사이버 전쟁 무기 '분산 서비스 거부 공격'

- 미국의 국가안보회국(NSA)은 이란의 핵 프로그램, 북한의 미사일 프로그램, 이슬람국가(IS) 등에 대한 공격용으로 수십억 달러를 들여 사이버 무기들을 개발했으나 이제 이것들이 미국의 동맹국들은 물론 미국의 핵심 사회 기반시설을 파괴하는 공격용으로 쓰일 수 있다는 '디지털 악몽'에 시달리고 있다고 뉴욕타임스가 진단한 바 있다. 미국이 7년 전 이란 핵 프로그램 공격에 사용했던 해킹 프로그램 '스턱스넷'의 일부 요소가 최근 일부 해킹 공격에 활용되기도 했고, 북한 해커들이 인터넷으로 돈을 훔친 해킹 도구도 미국의 국가안보국(NSA)이 만든 것을 개량한 것이다.
- 이번 절에서는 사이버전에서 가장 일반적으로 사용되고 있는 분산서비스 공격에 대해 학습하고 다음 절에서는 지금까지 가장 위력적인 파괴력을 보인 스턱스 넷에 대해서 학습한다.
- **서비스 거부 공격(DoS: Denial of Service)**

  분산서비스 거부 공격에 대한 학습을 하기 전에 이해를 돕기위하여 먼저 서비스 거부 공격에 대해서 학습하기로 한다. 서비스 거부공격은 호스트의 하드웨어나 소프트웨어 등의 자원을 무력화하여 호스트에서 적법한 사용자의 서비스 요구를 거부하도록 만드는 일련의 행위를 말한다

- **서비스 거부 공격(DoS: Denial of Service)**

  즉, 대역폭, 프로세스 처리 능력 및 시스템의 자원을 고갈시키는 공격을 수행하는 것이다. 이 공격의 특징으로는

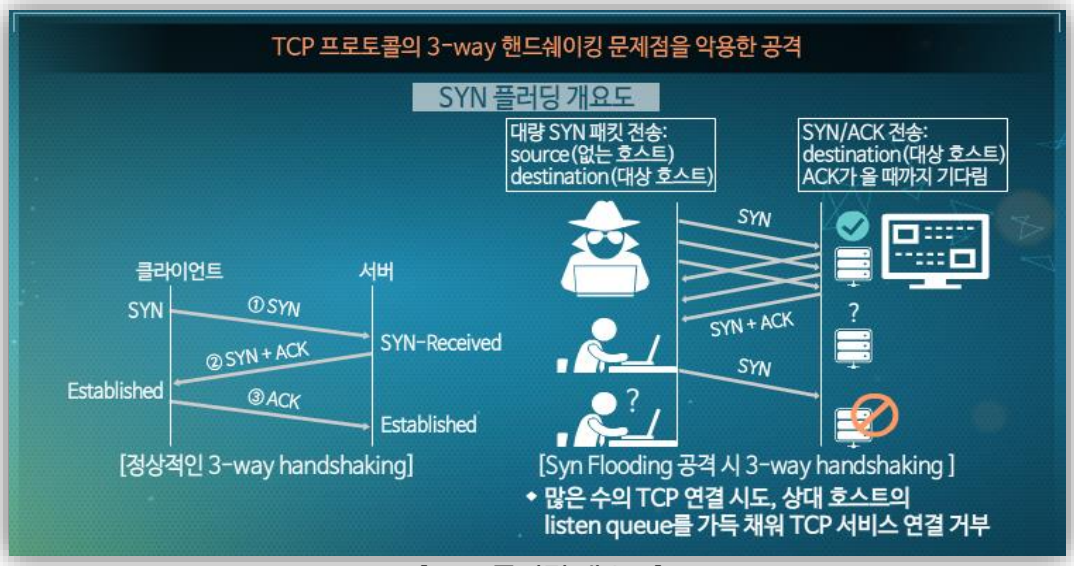
  - 공격의 원인 및 원천지를 찾기 힘듬
  - 공격 방법이 매우 다양
  - 단순한 공격 방법이 많아 누구나 쉽게 이용 가능
  - 뚜렷한 방지 대책 부재
  - 최근 네트워크를 이용한 분산 서비스 거부 공격(Distributed DoS(DDoS) 공격)이 급증

  이 공격의 유형으로는 아래와 같이 매우 다양하다.

  - Boink, Bonk, TearDrop공격: error control 취약점 악용
  - Land 공격: 출발지와 목적지 IP를 동일하게 하여 CPU 부하 소진
  - Ping of Death 공격: 윈도우 95, 98, 리눅스 6.0 버전 이하에서 유효
  - SYN Flooding 공격: 3-way handshaking 취약점 악용
  - Smurf 공격: direct broadcast 기능을 악용한 공격
  - Mail Bomb: 스팸 메일과 같은 종류

- **Syn 플러딩(Flooding)**

  SYN 플러딩 서비스거부(DoS)는 TCP 프로토콜의 3-way 핸드쉐이킹 문제점을 악용한 공격이다. 아래의 그림에서 보는 바와 같이 정상적인 3-way 핸드쉐이킹과 달리 많은 수의 TCP연결을 시도하여 상대 호스트의 listen queue를 가득 채워 TCP 서비스의 연결을 거부하게 하는 방식이다. 이 공격의 대응방안으로 서버에서의 SYN received 대기시간을 줄여서 SYN 패킷이 큐에 쌓이지 않도록 하기도 한다.

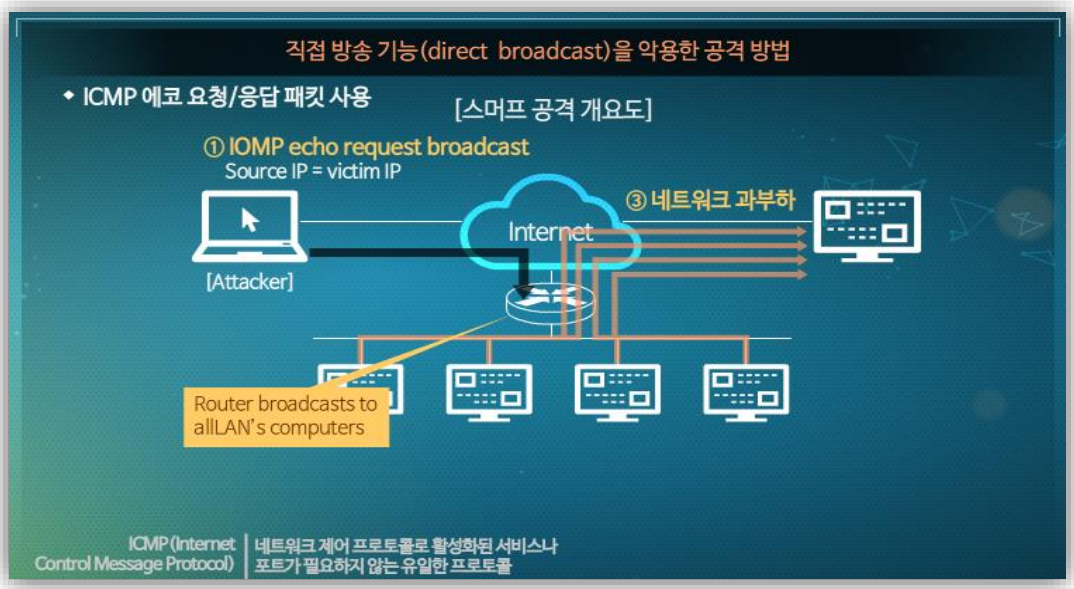


[SYN 플러딩 개요도]

- **스머프 공격(Smurf Attack)**

  스머프 공격은 직접 방송 기능(direct broadcast)을 악용한 공격 방법이다. 이때 ICMP 에코 요청/응답 패킷을 사용한다. 아래의 그림에서 공격자가 발송지(source) IP 주소를 공격대상(victim)의 IP 주소로 설정한 후, 방송주소(broadcast address)로 ICMP 에코 요청 패킷을 전송하면 그 하위 모든 시스템은 ICMP 에코 응답 패킷을 공격대상(victim)으로 전송하게 되어 자원을 고갈시킨다. 이 공격에 대하여는 라우터에서 직접 방송(direct broadcast)의 지원을 차단하여 대응한다.

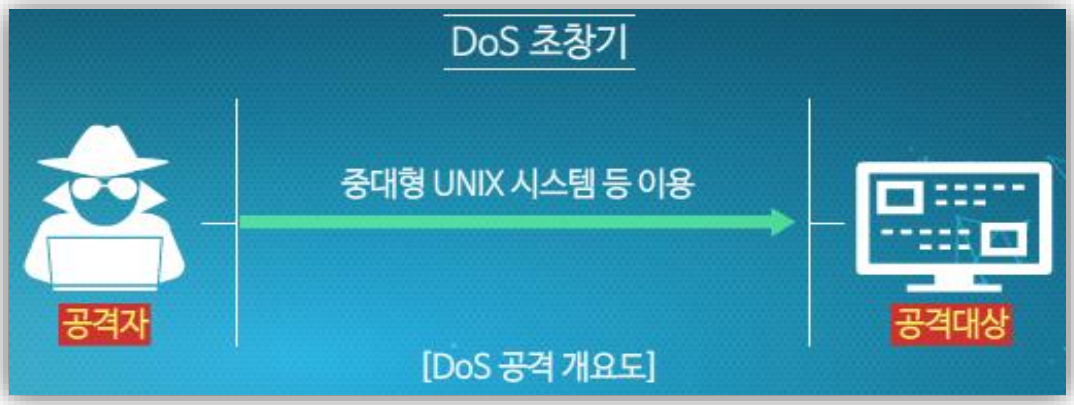
  * ICMP(Internet Control Message Protocol) : 네트워크 제어 프로토콜로 활성화된 서비스나 포트가 필요하지 않는 유일한 프로토콜



[스머프 공격 개요도]

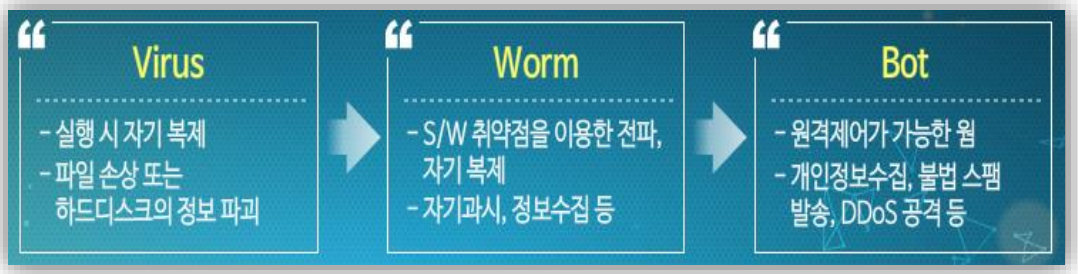
- **분산서비스거부 공격(Distributed DoS: DDoS)**
- **DDoS 공격의 등장**

  DoS 초창기에는 중대형 UNIX 시스템 등을 이용하여 공격자와 공격대상 간의 일대일 형태의 공격이 주를 이루었다(그림 참조). 서비스 거부(DoS) 공격 준비에 오랜 기간과 노력과 함께 전문적인 실력이 필요한 고비용과 저효율의 비지니스였다.



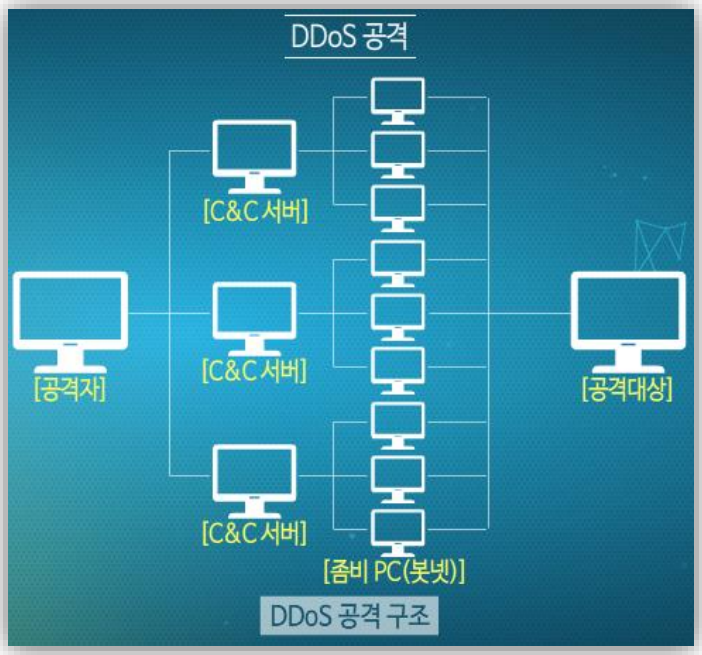
DDoS 공격의 등장

하지만 상대적으로 보안 취약한 PC의 성능과 보급이 크게 확대되면서 공격을 위해 활용할 PC의 확보가 용이해 졌고, 인터넷의 확산과 대역폭이 크게 증가하면서 대량의 트래픽을 발생시키기 좋게 인터넷 환경이 변화하였다. 한편 원격제어가 가능한 웜 유형인 봇(bot)이 출현(아래 그림 참조)하면서 공격시스템을 제어하기가 더욱 용이해졌다. 즉 봇 집단으로 구성된 봇넷을 활용한 공격인 분산 서비스 거부 공격이 등장하게 된다.



분산서비스거부 공격(DDoS: Distributed Denial of Service)

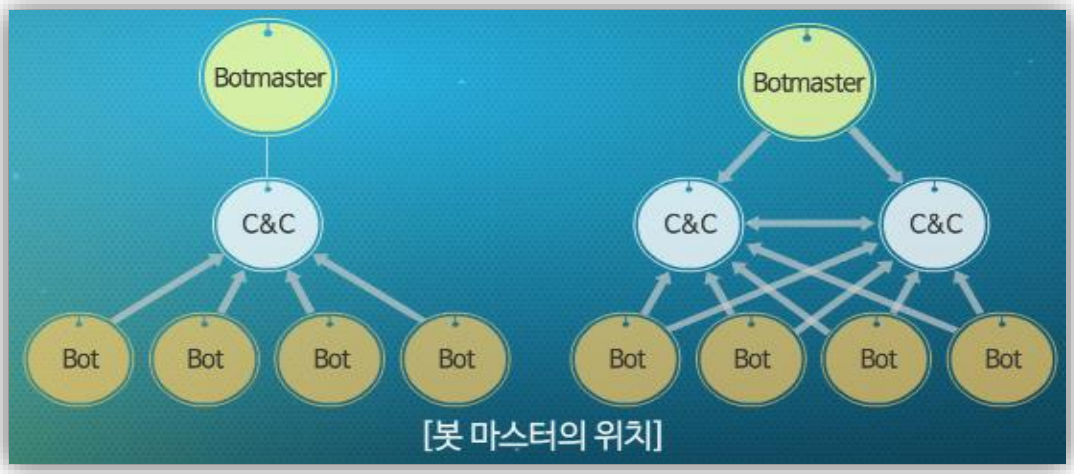
봇에 감염된 여러 대의 클라이언트(좀비PC)를 이용하여 공격대상 시스템에 DOS 공격을 가하여 공격대상의 자원을 고갈시킨다. 즉, DDoS 공격은 공격자 - 명령제어 서비(C&C 서버) - 좀비PC(봇넷)로 구성되는 3-tier 구조의 DoS 공격이다.



여기서 봇(bot)은 robot의 줄임말로 봇에 감염된 PC는 해커가 마음대로 조정할 수 있기 때문에 좀비 PC라고도 불린다. 봇넷(botnet)은 좀비 PC들로 구성된 네트워크를 의미하며 봇 마스터는 악성 행위를 수행하도록 봇넷에게 명령을 내린다(그림 참조). 명령제어(C&C: Command and Control) 서버는 해커에 의해서 봇넷에 스팸메일 전송이나 DDoS 공격 등을 수행하도록 명령과 통제를 내리는 서버를 말한다.

특히 봇넷(Botnet)은 아래의 특성을 지닌다.

- 웜/바이러스, 백도어, 스파이웨어, 루트킷 등 다양한 악성코드 특성을 지님
- 많은 종류의 변종이 등장하여 안티바이러스 솔루션으로 대응이 어려움

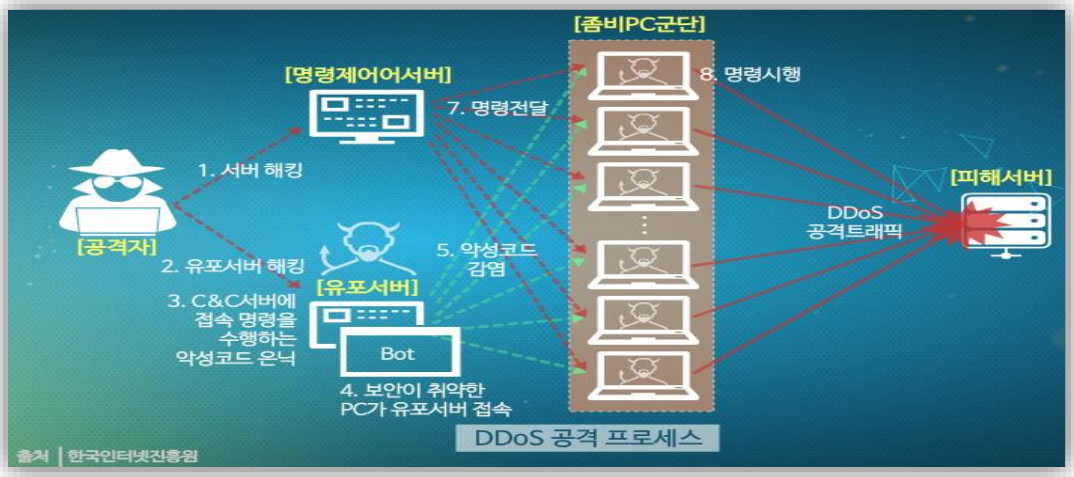


[봇 마스터의 위치]

- DDoS, Ad-ware, Spyware, 스팸발송, 정보불법 수집 등의 공격에 활용
- 공격자에 의해 봇넷을 마음대로 제어가 가능하며, 그 수법이 지능화 됨

봇넷을 이용한 DDoS 공격 프로세스를 도시한 것이다.

- 1. 서버를 해킹하여 명령제어 서비를 확보
- 2. 봇을 감염시킬 유포서버를 해킹하여 확보
- 3. 명령제어서버로부터의 명령을 수행할 악성코드 은닉
- 4. 보안 취약한 PC가 유포서버에 접속
- 5. 다수 PC가 감염되어 봇넷을 형성
- 6. 공격자는 명령제어 서버에 명령 하달
- 7. 명령제어서버에서 봇넷으로 명령전달
- 8. 봇넷은 공격대상 서버를 DDoS 공격

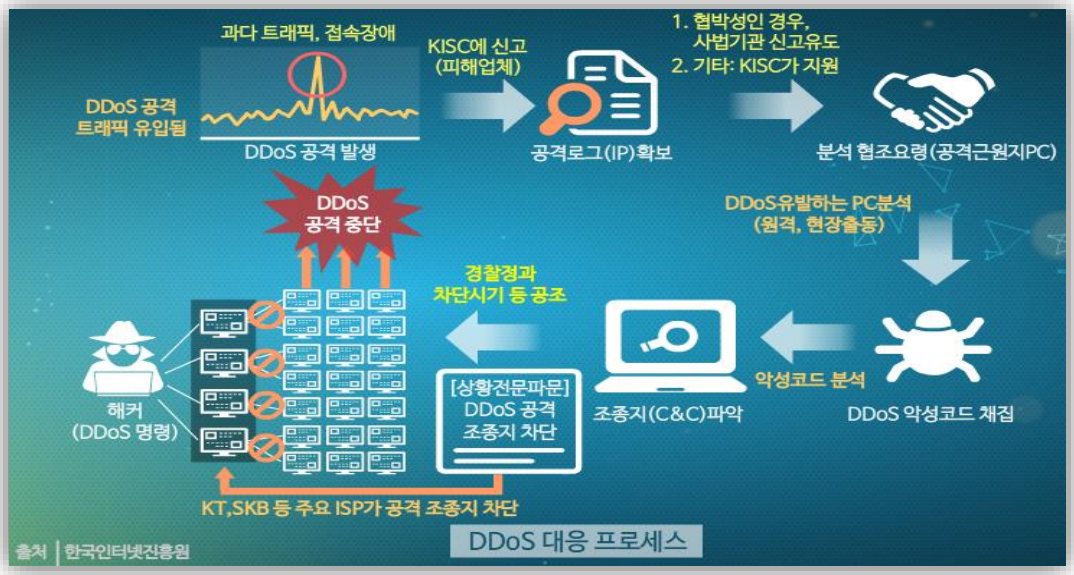


- **DDoS 대응 절차**

  - DDoS 공격으로 접속장애가 발생하면 한국인터넷진흥원의 KISC(Korea Internet Security Center)로 신고(전화 국번 없이 118)

  - DDoS 공격 대응의 핵심은 공격 IP를 확보하여 빠르게 DDoS 악성코드를 채집하고 분석하여 공격명령을 하달하는 명령제어 서버를 찾는 일

  - 명령제어 서버의 IP주소를 찾게 되면 상황전파문을 통신 사업자에게 보내 해당 IP 주소를 차단하여 해커로부터의 DDoS 공격 명령을 차단하여 DDoS 공격을 중단



02. 스턱스 넷을 통해 본 실전 사이버 전쟁

- 스턱스넷(Stuxnet)은 보안 위협의 패러다임을 바꾸는 차원이 다른 악성코드이다. 지금까지 등장한 악성코드가 자기 과시나 금전적인 이득을 목적으로 한 것과 달리 스턱스넷은 단지 핵심 시설의 파괴만을 목표로 하고 있다. 이로 인해 스턱스넷은 악성코드가 사이버 무기화된 첫 번째 사례로 주목 받고 있는 것이다. 또한 현존하는 악성코드 가운데 가장 정교한 것으로도 평가 받고 있다.

- 스턱스넷(Stuxnet)은 폐쇄망으로 운용되는 대규모 산업 시설을 겨냥해 제작된 악성코드로서, 특정 산업 자동화시스템만을 공격 목표로 제작된 프로그램이다. 이 악성코드는 원자력, 전기, 철강, 반도체, 화학 등 주요 산업 기반 시설의 제어 시스템에 오작동을 유발함으로써 시스템 마비 및 파괴 등의 치명적인 손상을 입힐 수 있다. 실제로 이란 부셰르 원자력핵발전소와 중국 1천여 개 주요 산업 시설을 비롯해 전세계 여러 국가에 감염이 확산된 것으로 알려지고 있다. 스턱스 넷은 진화하여 4차 산업혁명 시대의 사회 인프라를 위협하는 보다 강력한 사이버 무기로 등장할 전망이다.

미국과 이스라엘의 '올림픽 게임' 작전

- 2006년 미국과 이스라엘의 소위 '올림픽 게임' 작전의 배경은 이란의 핵개발 계획을 막으려는 수단으로 사이버 공격을 선택하면서 시작된다. 당시 이란의 나탄즈에는 대규모 우라늄을재처리할 수 있는 부셰르 원전시설이 건설되었다.

[나즈탐 부쉐르 원전]

[원심분리기]

- 8m 깊이에 22m 흙을 덮어 폭격에 대비한 시설로 수천 개의 원심분리기가 가동되고 있다. 이것을 무력화하기 위하여 선택된 무기가 사이버 무기인 '스턱스넷(Stuxnet)'인 것이다. 미국과 이스라엘의 주도로 최고의 군관민 전문가를 동원하여 제작한 것으로 알려졌다. 공격 시나리오는 우라늄 농축 원심분리관을 통제하는 컴퓨터에 악성코드를 감염시켜 원심분리관의 회전속도를 변화시켜 원심분리관을 무용지물화 하는 계획인 것이다.

- **스턱스 넷의 침투**

  - 당시 니즈탄 핵시설 통제망은 외부 전산망과 철저히 분리되어 있었기 때문에 다른 파일에 감염시켜 전파하는 방식을 선택

  - 이란 정부의 컴퓨터 관련 공급업자(알리 아쉬타리) 포섭하여 USB를 통해 전파하는 계획

  - 알리 아쉬타리를 적발 후에도 이란 핵시설 통제망의 감염사실을 알지 못함

- **스턱스 넷 감염사실 발견**

  - 당초 계획에는 stuxnet이 이란의 핵시설만 공격하도록 설계

  . 스턱스넷은 윈도우환경을 사용하는 발전소, 철도와 같이 국가 기관 시설을 공격

  . 특히 지멘스사에서 만든 국가 기관 시설에서 사용하는 PLC 프로그램을 대상으로 공격

  * PLC(Programmable Logic Controllers) : 산업 자동제어 시스템에서 실제 장비들을 제어하기 위한 장치

  - 2010. 6월 민간보안업체에 의해 발견

  . 인터넷으로 유출되면서 수많은 다른 컴퓨터가 감염되면서 스턱스넷이라는 악성코드 포착됨

- **스턱스 넷 감염사실 발견**

  - 상대방과 함께 아군 시설에도 타격을 주면서 국제적으로 잠재적 통제 불가능성과 피해 광범위성 이슈가 제기되어 핵무기와 같은 양상으로 국가 간 사이버 전쟁에 대한 억지력 발생

- **스턱스 피해**

  - 원심분리기 1,000~5000개 사이의 피해 발생
  - 이란 핵개발이 상당히 지연
  - 이란에서는 2010년 여름까지 스턱스넷(stuxnet) 존재를 파악하지 못함
  - 2011년 이란은 사이버 전쟁 전개를 선언하는 계기가 됨

- **이란의 사이버 보복 공격**

  - 2012.8 사우디 국영 석유회사 사우디 아람코 컴퓨터 3만대에 악성코드 감염 소장 데이터 ¾ 삭제되고 컴퓨터 화면에는 불에 탄 미국 성조기 이미지가 뜸
  - 카타르 천연가스 회사인 라스가스(RasGas)에 대규모 사이버 공격 발생
  - 미국의 대형 금융사도 DDoS 공격 피해를 당함

- **스턱스넷 사건의 이슈**

  - 폐쇄망에 대한 보안의식 재조명이 필요
  - 안전하다고 인식한 SCADA(원격자동제어 시스템)에 대한 보안 강화 필요
  - 사이버 무기의 등장과 함께 사이버전 개념의 확산 계기
  - 초연결 특성의 4차 산업혁명 시대는 사회적 인프라가 ICT를 기반으로 구축되기 때문에 스턱스 넷은 그 근간을 위협하는 강력한 무기가 될 수 있음을 시사

스턱스넷와 같은 감염 예방을 위한 일반적인 조치 사항

- 스턱스넷은 기존 악성코드와는 다른 패턴을 보여주고 있다. 하지만 감염과 유포 방식에 있어서는 USB라는 이동형 저장장치와 윈도우 OS의 취약점을 이용하고 있다. 이 부분에 초점을 맞춰 기업 보안 담당자가 취할 수 있는 예방 방법은 다음과 같다.
- 최신 버전으로 업데이트된 백신 소프트웨어 사용
  - 최신 버전의 백신 프로그램을 사용해서 감염을 예방해야 한다.
- **USB 자동 실행 방지**
  - 대부분의 SCADA 시스템은 폐쇄망에서 운영되므로 실제 감염이 발생하는 경로로 이용될 수 있는 것은 USB일 가능성이 높다.

  * SCADA(Supervisory Control and Data Acquisition) : 산업 기반 시설의 감시와 제어를 담당하는 감시 제어 데이터 수집 시스템

  - 폐쇄망에서 사용되는 시스템의 경우 백신 소프트웨어의 CD/USB 자동실행 방지 옵션을 활성화하여 감염을 예방한다.

- **최신 보안 패치 적용**

  사내 시스템이 윈도우 OS의 취약점을 이용한 공격에 의해 감염되는 것을 예방하기 위해 최신 보안 패치를 업데이트하는 것이 중요하다.

- **공유폴더 사용 주의**

  불필요한 공유 폴더 생성은 금지하고 생성한 공유 폴더에는 접근이 필요한 사용자 계정에게만 읽기 권한 주도록 하고 함부로 쓰기 권한은 주지 않도록 한다.