P2P BOT을 이용한 집중 서비스 거부 공격

권 오 현, 김 진 욱, 박 지 영, 심 홍 철, 정 찬 영
단국대학교 레드빈즈

Concensrational Denial Of Service in P2P Bot

Kwon Ohhyun, Kim Jinwook, Park Jiyoung, Sim Hongcheol, Jung Chanyoung
DANKOOK University Security Club, RED BeanZ

< 목차 >

0. 요약

최근 사회적으로 심각한 타격을 줬던 7.7DDOS공격은 기존 DDOS공격의 변종 방법으로서 시시각각 변하고 있는 해킹 공격에 대한 사례라 할 수 있겠다.
이에 우리는 새로운 유형의 DDOS공격을 개발하고자 하여 CDOS를 개발하였다.
CDOS공격은 기존의 다수의 좀비pc로부터 victim서버로의 공격이 아닌 소수의 좀비pc가 victim서버에게 다수의 트래픽을 유발이 가능한 방법이다.

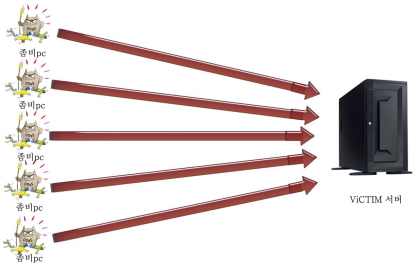


그림 1 기존 DDOS 공격방법

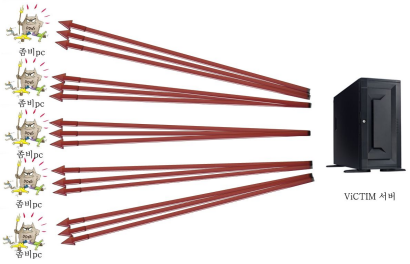
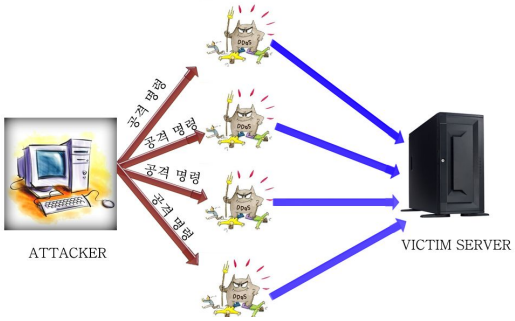
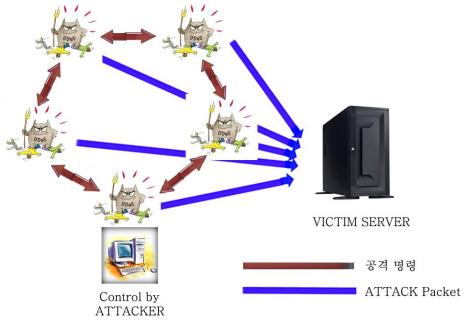


그림 2 새로이 구상한 CDOS공격 방법

DOS공격시 필요한 좀비PC의 수는 기존 DDOS에 비해 30%수준까지 낮출 수 있다.
다음으로는 공격명령 전달 체계의 변화이다.





위의 그림과 같이 기존 DDOS공격은 공격명령의 전달이 직접 전달 또는 미리 프로그래밍 된 스케쥴러를 이용한다면 CDOS공격은 좀비PC간의 통신을 통해 스케쥴링 프로그램을 전파하여 공격을 지시하게 된다. 이때에 중요한점은 공격자 역시 좀비pc가 되어 다른 좀비pc와 통신을 하게 된다. 좀비pc는 정상적인 공격명령 이외에 수시로 가짜 공격명령(쓰레기값)을 통신하여 방어에 어려움을 주는 한편 분석하여햐 할 패킷의 양이 늘어 공격자의 신원보장 및 공격코드의 보호에 용이한 이점을 주게 된다.
공격명령 예시)
0kf1x11wefj(해쉬값) destinaton url:http://www.naver.com/1111.zip date:2009/11/30
앞의 해시값은 공격자가 사전에 미리 해시키값을 정해 공격자에 의해 생성된 해시코드만을 정상으로 인식하여 쓰레기값 및 타인의 공격통제를 예방한다.
victim 서버에 대한 공격은 victim서버에 존재하는 다운로딩 URL을 통해서 무조건/반복적인 연결을 형성하여 해당서버를 마비시키는 방법을 택하였다. 은행/증권/정부기관에는 일반 사용자들이 항상 연결이 가능한 다운로드 URL을 포함하고 있어 대부분의 웹상에서 시도가 가능하다.
구체적인 공격툴 프로그램과 좀비pc툴킷은 본문에서 자세히 기술하였다.

1. 기존 DoS, DDoS 공격 분석

1-1. < DoS 란 >

● 서비스 거부 공격(영어: Denial of Service attack, DoS)은 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다. 특정 서버에게 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나, 서버의 TCP 연결을 바닥내는 등의 공격이 이 범위에 포함된다. 수단, 동기, 표적은 다양할 수 있지만, 보통 인터넷 사이트 또는 서비스의 기능을 일시적 또는 무기한으로 방해 또는 중단을 초래한다. 통상적으로 DoS는 유명한 사이트, 즉 은행, 신용카드 지불 게이트웨이, 또는 심지어 루트 네임 서버를 상대로 이루어진다.

1-1-① < DoS의 형태 >

◈공격자가 목표 TARGET
에게 트래픽 초과 유도

1-1-② < DoS의 기법 >

(1) SYN Flood 공격

기본적으로 서버와 클라이언트 사이에 통신은 3단계 구조로 이루어져 있다.

① 클라이언트는 일련번호와 패킷크기를 포함한 정보를 서버에 전송하여 연결을 시작한다.

② 서버는 클라이언트가 보낸 세션 정보로 응답한다.

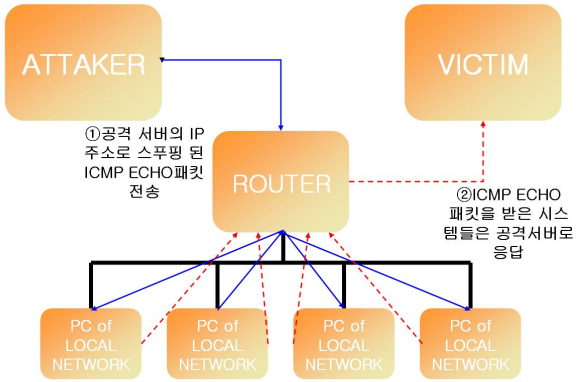
③ 클라이언트는 서버로부터 수신한 정보에 동의하고 승인한다.

일단 서버에 수천 개의 TCP 접속(SYN) 요청 메시지를 보낸다. 이 때 이 패킷내부의 소스 IP 주소를 속이거나, 인터넷 상에서 사용하지 않는 IP 주소값으로 변형한다. 그러면 서버는 새로운 접속을 맺기 위해 실제로는 존재하지 않거나 동작하지 않는 IP 주소값으로 SYN/ACK로 응답을 한다.

이 때, 서버는 SYN/ACK 응답을 보낸 클라이언트로부터 ACK가 올 때까지 기다리게 되는데, 서버는 ACK 메시지를 받지 못하게 된다. 이렇게 되면 서버는 ACK 받을 때까지 버퍼와 같은 자원을 계속 종료하지 않고 열어두게 되는데, 계속 누적될 경우 결국은 시스템이 다운되거나 서비스를 중단하는 사태가 발생한다.

(2) Smurfing 공격

Smurfing 공격은 그 광범위한 효과로 인하여 가장 무서운 DoS 방법 중에 하나이며, IP와 ICMP의 특징을 이용한다. 브로드캐스트 핑 요구는 네트워크 주소나 네트워크 브로드캐스트 주소에 직접 보내질 수 있다. 만약 192.168.0.0/24 범위를 가진 네트워크가 있다면, 네트워크 ID는 192.168.0.0될 것이고 브로드캐스트용 주소는 192.168.0.255가 될 것이다. 브로드캐스트는 전형적으로 지정된 범위 내에서 조정된 각각의 주소 없이 무엇이 활동하는지 진단할 목적으로 사용된다.



● Smurfing의 구조도

Smurfing 공격은 직접적인 브로드캐스트와 세 가지 구성요소인 공격자, 증폭 네트워크와 표적을 최대한 이용한다. 공격자는 증폭 네트워크의 브로드캐스트 주소로 공격 서버가 요구하는 것처럼 패킷들의 원본 주소를 위조하여 ICMP ECHO 패킷을 전송하고, ICMP ECHO 패킷을 수신한 증폭 네트워크 내의 모든 시스템은 공격 서버에 응답을 하게 된다. 만일 공격자가 브로드캐스트 핑에 응답할 100개의 시스템을 가진 증폭 네트워크에 하나의 ICMP 패킷을 보내게 되면, 공격자는 100만큼의 효과로 DoS 공격을 할 수 있다.

Smurfing 공격을 방어하기 위해서는 직접적인 브로드캐스트를 경계 라우터에서 사용할 수 없게 만들어야 한다.

1-1-③ < DoS와 기존 해킹방법과의 차이점 >

지금까지의 해킹은 정보 시스템의 "기밀성", "무결성", "가용성" 중에서 '기밀성'과 '무결성'을 깨는 비밀번호 및 개인정보 도용, 정보의 변화로 인한 이익 창출 같은 방법이었다. 반면에 '가용성'영역은 사람들의 인식이 적었던 만큼 해킹 기법도 발달하지 못한 영역이었다. 그래서 수많은 인터넷 사이트들이 동시 접속자수가 늘어나면 가용성 문제를 일으켰음에도 불구하고 서비스 제공 업체들은 이 같은 문제를 해킹이나 바이러스처럼 심각하게 생각하지 않는 경우가 많았다. 그러나 요즘의 '가용성' 손실은 곧바로 생산성 손실로 연결된다. 특히 유료 서비스를 제공하는 상황에서 가용성에 문제가 발생했다면 수익성이 직접적인 영향을 받게 된다. 즉, 예정되지 않은 정지 시간은 생산성 손실을 의미하고, 사용자들은 해당 인터넷 사이트에 대해 다시 생각하게 될 것이다. 결국 이렇게 요즘 가용성에 대한 인식이 높아지면서, 기존의 방식과는 다른 가용성을 이용한 DoS 공격이 등장하게 된다. 또한 원리도 단순히 해당서버에 접속하는 방법으로 시스템 최대 사용 능력을 초과하는 트래픽을 발생시켜 문제를 일으키는 간단한 방식이기 때문에, '가용성' 해킹의 KEY가 되었다.

1-1-④ < DoS의 한계점 >

일반적으로 DoS 공격은 목표를 가지고 공격할 때, 1:1로 하게 된다. 그래서 이에 따른 한계가 있다. 목표서버를 공격하지만 개인PC로는 한계가 있기 마련이다. 또한 중간계층이 존재하지 않음으로 공격자가 비교적 쉽게 추적당할 염려가 있다.

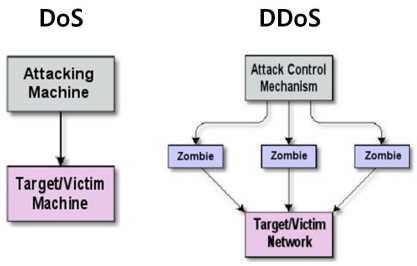
1-2 < DDoS 란? >

'분산 서비스 거부' 또는 '분산 서비스 거부 공격'이라고도 한다. 여러 대의 공격자를 분산 배치하여 동시에 동작하게 함으로써 특정 사이트를 공격하는 해킹 방식의 하나이다. 서비스 공격을 위한 도구들을 여러 대의 컴퓨터에 심어놓고 공격 목표인 사이트의 컴퓨터시스템이 처리할 수 없을 정도로 엄청난 분량의 패킷을 동시에 범람시킴으로써 네트워크의 성능을 저하시키거나 시스템을 마비시키는 방식이다.

공격은 일반적으로 악성코드나 이메일 등을 통하여 일반 사용사의 PC를 감염시켜 이른바 '좀비PC'로 만든 다음 C&C(명령제어) 서버의 제어를 통하여 특정한 시간대에 수행된다.

1-2-① < DoS와의 차이점 >

Dos와 DDoS 공격은 해당 서버의 트래픽을 초과시켜 네트워크 시스템을 마비시키는 점에서는 공통적이나 중간 계층을 두고 명령을 내려서 공격을 실행한다는 점에서 차이를 보인다. 또한 ZOMBIE를 만들기 위한 악성코드나 스크립트의 배포작업이 추가적으로 필요하다. 그러나 DDoS는 DoS보다 추적하기 어려우며, BOT의 사용으로 인하여 해당 서버의 트래픽 초과를 보다 쉽게 유발할 수 있고, 감염된 PC는 공격자의 마음대로 원격조종이 가능하다.



● DoS와 DDoS의 차이

1-2-② < BOT NETWORK >

'봇'은 원격 제어 프로그램을 의미한다. 해커들은 원격으로 특정 시스템을 목적으로 '봇'을 제작한다. 보안 패치가 안된 시스템의 경우 감염될 가능성은 매우 높다. 일단 유입된 '봇'은 시스템에 몰래 상주하며, 해커의 명령에 따라 움직이게 된다. 또한 정보를 빼내갈 수도 있다. 요즘 일부 '봇'은 자신을 숨기는 은닉 기능과 백신 프로그램을 종료시키고 업데이트도 차단하는 기능을 가지고 있다. 이 때문에 감시가 실시간으로 적절하게 이루어져야 한다. 2005년 상반기 동안, 하루 평균 10,352개의 봇이 발견됐다. 이러한 봇 네트워크의 급격한 증가가 최근 DoS 공격 사례 증가의 주된 요인으로 작용한 것으로 추정된다. 공격의 동기는 금전적일 가능성이 높다. 또한 감염된 봇을 묶어 네트워크화 하여 유료로 서비스하는 사례를 발견하기도 했다.

1-2-③ < DDoS의 사례 >

● 7.7사태

2009년 7월 한국과 미국의 주요 정부기관과 포털사이트, 은행사이트 등에 가해진 공격을 7.7대란 또는 사태라고 표현하고 있다. 7월 4일 미국 사이트들에 대하여 1차 공격이 수행되었고, 한국에서는 7월 7일부터 3차례 공격이 수행되었다. 공격 대상에는 미국의 백악관과 한국의 청와대를 비롯하여 한국 주요 언론사와 주요 정당, 주요 포털사이트가 포함되었는

데, C&C서버로부터 공격명령을 하달받는 것이 아니라 감염시 생성되는 공격목표 설정파일을 기반으로 자동공격을 수행하는 방식이었다. 감염된 수만 대의 컴퓨터가 좀비PC로 활동하면서 국내 주요 기관과 포털 사이트에 장애를 일으켰다.

● 아이템거래 사이트 피해

2007년 10월부터 12월까지 수차례에 걸쳐 국내 최대 온라인 게임 아이템 거래 사이트가 DDoS공격으로 인하여 마비되는 사태가 벌어졌었다. 전형적으로 좀비PC를 이용하여 트래픽 초과를 유발하는 가용성 위반 공격이었다. 첫 공격은 지난 10월 초에 일어났다. 이 공격으로 인해 근 2주간 사이트 접속이 원활히 되지 않아 어려움을 겪었다. 이 후로도 수차례 공격이 있었고, 그 때마다 사이트는 마비되는 현상이 발생하였다. 이번 서비스장애로 이 회사의 손해는 1400억원 정도로 추정되고 있다.

1-2-④ < DDoS의 한계점 >

DDoS는 명령이 여러 단계를 거쳐서 가기 때문에, 몇 대의 마스터 좀비 PC만 복구하면, 공격을 더 이상 수행할 수 없게 된다. 또한 공격자는 추적을 피하기 위하여 명령을 보통 한 번 하달한다. 공격을 수행하려면 봇 네트워크를 형성하는 시간도 고려해야 한다. 또한 스케줄러를 이용하는 방식에 있어서는 악성코드의 전파 후에는 ZOMBIE를 제어할 수 없다. 최근에는 '봇'을 개인PC에서 치료하는 방법도 많이 나오고 있고, 방화벽이나 백신을 이용하여 애초에 예방하는 경우가 많기 때문에, BOT NETWORK관리의 어려움이 있다.

2. CDoS 기법

2-1. <CDoS란?>

CDOS공격은 기존의 다수의 좀비pc로부터 victim서버로의 공격이 아닌 소수의 좀비pc가 victim서버에게 다수의 트래픽을 유발이 가능한 방법이다.

DOS공격시 필요한 좀비PC의 수는 기존 DDOS에 비해 30%수준까지 낮출 수 있다.

CDOS공격은 좀비PC간의 통신을 통해 스케쥴링 프로그램을 전파하여 공격을 지시하게 된다. victim 서버에 대한 공격은 victim서버에 존재하는 다운로딩 URL을 통해서 무조건/반복적인 연결을 형성하여 해당서버를 마비시키는 방법을 택하였다. 은행/증권/정부기관에는 일반 사용자들이 항상 연결이 가능한 다운로드 URL을 포함하고 있어 대부분의 웹상에서 시도가 가능하다.

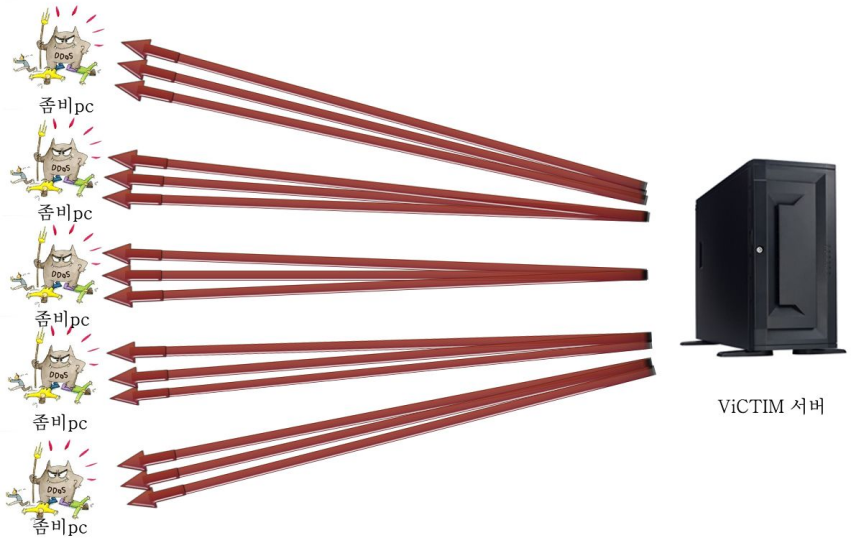
2-2. < CDoS 개발배경 >

최근 사회적으로 심각한 타격을 줬던 7.7 DDOS공격은 위와 같은 비교적 간단한 원리에 심각한 타격을 줄 수 있는 공격으로 추후에도 충분히 발전 가능성이 있는 공격 방법이다.
이에 DDOS에 대한 방어도 점차 발전하고 있는 상황이지만 다양해지는 공격패턴에 대한 방어에는 한계가 있다고 생각한다.
우리가 미리 다양해지는 패턴에 대해 예상해보고 그 방법을 연구해 보기로 하였다.

- 기존 DDOS 공격의 맹점 -

● 기존 DDOS는 좀비PC가 victim에게 정상적인 트래픽을 유도하여 공격하는 방식으로서 다수의 좀비PC로 행해지는 공격기법이다.

그러나 이번에 구상한 CDOS공격은



● **새로이 구상한 CDOS공격 방법**

위의 그림과 같이 한 대의 Victim서버에서 여러개의 syn/ack를 한 대의 좀비PC로 인하여 유발시키는 공격방법을 택하였다.

또한 기존의 여러 대의 좀비pc에서 한 대의 VICTIM서버로 패킷을 보내는 대신 한 대의 VICTIM서버에서 한 대의 좀비PC로 여러개의 패킷을 보내는 방식이다.

물론 어느 정도는 DOS공격과 비슷한 양상을 보이기도 하지만 아래에서 설명할 내용을 보게 되면 확연한 차이점을 느낄 수 있을 것이다.

한마디로 DDOS공격에 비해 30~50배정도 적은 수의 좀비PC를 이용하여 똑같은 효과를 낼 수 있는 공격방법이라고 하겠다.

	기존 DDOS공격	새로운 CDOS공격
공격패킷 방향	좀비PC→VICTIM서버	VICTIM서버→좀비PC
공격패킷의 양 (좀비PC 1 : VICTIM 서버 1)	1 connection(공격패킷양 상대비 1)	30~50 connection(공격패킷양 상대비 30~50)
필요한 좀비pc 상대대수	100%	30%

표 2 기존 DDOS공격과 새로운 CDOS공격의 공격방법의 성능비교

공격루트 또한 일반적으로 누구에게나 자유로이 공개된 지점을 이용하여 공격하고 일정치 않은 source ip로 인해 사실상의 방어는 불가능 할 것으로 보고 있다.

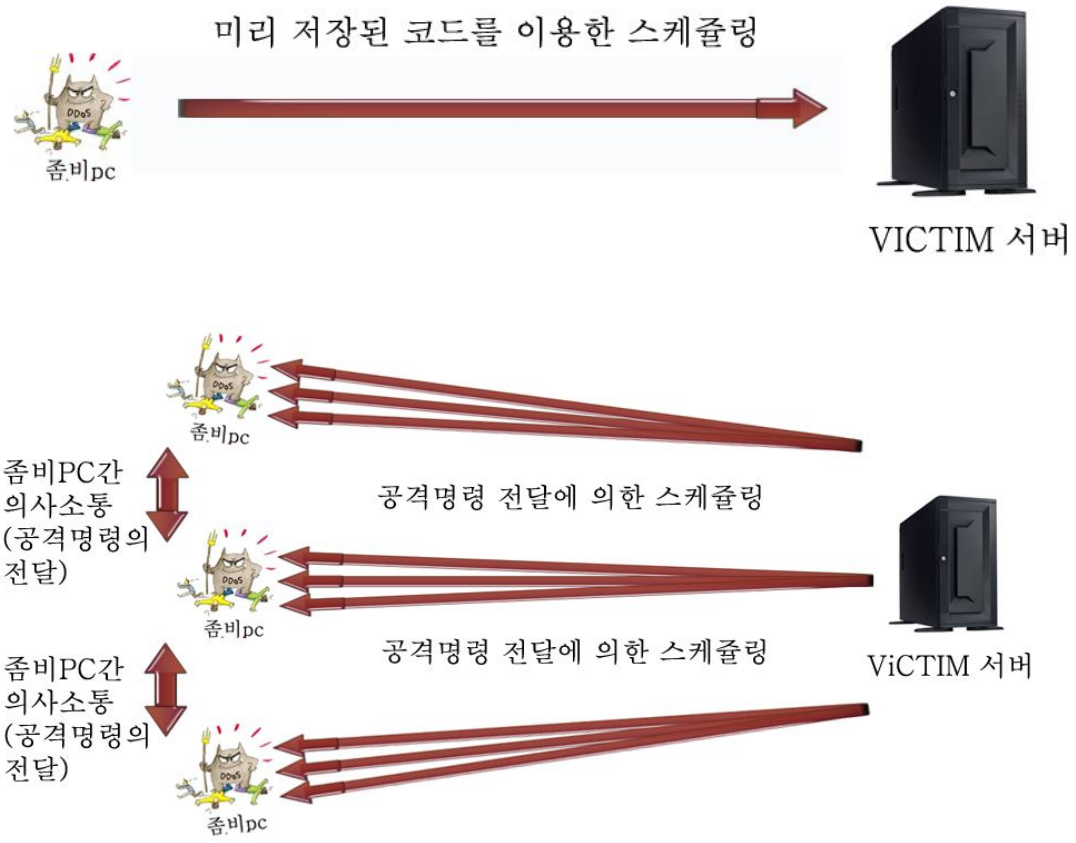
● 두 번째로 공격통제권이다.

7.7대란에 사용되었던 변종DDOS 공격은 스케쥴링을 이용하여 미리 삽입된 공격지/시간에만 공격이 가능하도록 프로그래밍 되어 있어 공격자의 통제가 불가능 하였다.

물론 그로 인해 공격자의 신변보호가 되었지만 목적을 가지고 있는 공격 방법으로는 매우 부적합한 것이 사실이다. 이에 우리는 공격통제권을 공격자가 소유함은 물론 공격자의 신변보호까지 가능한 방법을 생각해 보았다.

여기서의 핵심은 좀비PC끼리의 의사소통이다. 좀비PC끼리 주기적 의사소통을 통하여 공격지를 결정하고 시간을 결정하며 유효치 않을 시에는 변경 및 변종 비활성 등의 동작이 가능케 한다.

여기서 중요한 사실은 좀비PC끼리의 의사소통으로 인하여 공격의 진앙지는 사실상 찾기가 불가능하며 공격자 또한 좀비PC를 사용하게 되어 공격에 대한 통제권을 획득 할 수 있게 된다.



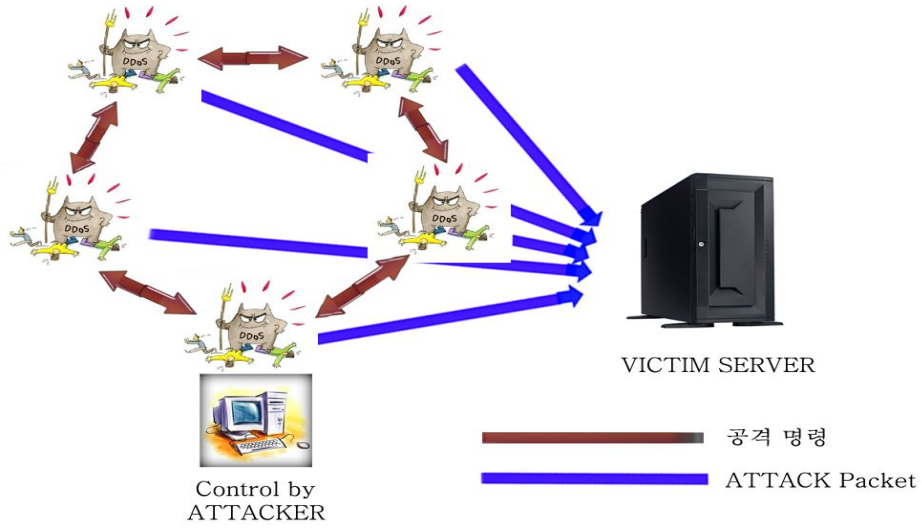
● DDOS 스케쥴링 기법과 CDOS 스케쥴링 기법 비교

기존의 DDOS 공격은 attacker->zombi pc->victim 이었다면 CDOS공격은 (zombi pc(공격자가 보유한 좀비 PC)->zombi pc->zombi pc->...->zombi pc->zombi pc(공격자가 보유한 좀비PC)...->zombi pc-> victim)으로 순환된다.

CDOS공격에서는 ATTACKER 자신도 좀비PC가 되어서 다른 좀비PC와 똑같이 동작하게 된다.

CDOS공격은 공격자가 보유한 좀비PC의 신변보호를 좀비PC간의 지속되는 데이터전송에

의해 유지하게 된다. 또한 zombiPC끼리 쓰레기값의 지속적 통신을 통해 실제 암호의 공격 코드를 찾기란 거의 불가능에 가깝다.



.

● CDOS 공격명령 전달 체계

위 그림에서 볼수 있듯이 이러한 방법으로 공격자는 안전하게 공격통제권을 가지게 된다.

	DDOS	7.7 DDOS	CDOS
공격명령 전달체계	직접 전달방식	사전 코딩된 스케쥴링 삽입	좀비PC간의 공격명령 전달
공격명령 전달 시기	공격시에 전달	사전에 스케쥴링	공격시에 스케쥴링 전달
ATTACKR/공격 명령 노출 위험	좀비PC에게 직접 공격명령 전달로 인해 역추적이 용이	스케쥴링을 이용하여 공격과 ATTACKER와 연관성 희미	ATTACKER가 직접 공격 스케쥴링을 전달하지만 ATTACKER 역시 좀비PC를 통한 전달로 구별이 어려움 또한 공격명령외에도 지속적인 쓰레기값 통신을 통해 정상적인 공격명령을 찾기가 힘듬

● 각 DOS 공격간 공격명령 전달에 대한 비교

2-3. <전개 과정에서의 시행 착오>

victim url 다운로드 공격시 좀비PC의 동시접속을 유지하려면 VIctim과 좀비PC간의 연결 시간이 충분히 길어져야한다. 그러기 위해서 첫 번째 방법으로 우리는 웹상에서의 다운로드 시 윈도우의 임시템퍼러리 파일에 저장된다는 점에 주목하였다. 임시 템퍼러리 파일의 해당

파일을 지속적으로 지워주는 방법을 생각해보았다. 그렇게 함으로써 다운로드율을 계속적으로 낮춰서 지속적인 연결이 가능하도록 하려고 하였다.

다음 두 번째 방법으로는 해당 다운로드 프로세스의 suspend 모드로의 전환이다. 해당 다운로딩 프로세스를 지속적으로 suspend모드로 전화시켜 주면 그만큼 victim서버와의 연결시간을 늘릴 수 있어 동시접속 프로세스 개수를 늘릴 수 있을거라 생각했다. 그러나 우리의 최종안은 자연적인 다운로딩 속도의 감소였다. 프로그래밍화된 다운로드툴을 이용하여 해당 다운로드 url을 자동적/지속적으로 실행시키게 되면 좀비PC의 리소스를 소모하여 자동적으로 다운로딩속도가 낮아져 동시접속task를 유지시킬수 있다.

다음으로 공격 전달 방법을 생각해보았다. 공격 전달 방법은 기존의 마스터PC나 공격자pc에서 상하방식으로 내려지는 공격명령에서는 공격자의 신분노출이 우려되는 상황이었다.

그래서 첫 번째로 우리는 좀비PC끼리의 전방위적인 공격명령 전달 체계를 구축하고자 생각하였다. 좀비 PC에 감염되게 되면 해당pc는 즉시 주변 좀비pc에게 무작위로 의미없는 패킷의 전송을 시작한다. 이런식으로 좀비pc는 주변 좀비pc와 지속적인 패킷 전송을 함으로써 공격명령 전달 준비를 마친다. 여기서의 핵심은 공격자 역시 일반 좀비pc를 보유한다는 생각이다. 그렇게 되면 공격자의 좀비pc 역시 다른 좀비pc와 마찬가지로 지속적인 좀비pc간 통신이 이루어지게 된다. 이때에 공격목표가 지정이 되면 공격자가 해당 공격목표에 대한 destination url 및 스케쥴링 시간을 미리 정해놓은 패킷으로 전송하게 된다. 좀비pc는 좀비툴속에 포함된 프로그래밍된 url연속공격프로그램으로 해당 패킷을 수신하게 되면 해당패킷이 미리 공격자가 정해놓은 형식의 패킷이라는 것을 해쉬값을 통해서 확인한후에 해당 목표ip와 스케쥴링 데이터를 입력받게 된다. 그러나 여기서 문제점은 좀비pc간의 인식의 문제였다. 좀비pc간의 인식을 위해서는 좀비pc의 ip주소나 mac address에 대한 리스트나 특정 대역대의 ip만을 좀비pc만으로 규정화 해야하는데 이렇게 되면 방어측면에서 해당 좀비pc의 색출이 손쉽게 되어 공격의 강도가 약해질 수 밖에 없다. 그럼으로써 생각한 방법이 고전적인 방법인 IRC채팅서버를 이용한 방법이다. 일단 좀비pc는 감염 즉시 IRC채팅채널을 랜덤값(1~1000범위내/서버는 10개내외)을 이용하여 생성하게 된다. 그 후 채팅채널을 만듬과 동시에 감염즉시 IRC채팅채널랜덤값(1~1000범위내/서버는 10개내외)에 대한 탐색을 시작한다. 이렇게 하여 좀비pc끼리의 연결을 형성해준다. 특정 좀비pc가 생성한 irc채팅채널에 다른 좀비pc가 접속하게 되면 둘간의 통신이 이루어지게 된다. 이런식으로 irc채팅채널에는 수개의 좀비pc가 연결되어 해당 좀비pc들끼리는 채널을 생성한 좀비pc로부터 해쉬값과 공격지 ip/url 과 date 스케쥴링을 전송받게 된다.

(ex. 0kf1x11wefj(해쉬값)

destinaton url:http://www.naver.com/1111.zip date:2009/11/30(공격지 url및 스케쥴링 데이트))

그러나 여기서 또 한가지 중요한 점은 해쉬값이다. 위의 ex 메시지를 받은 좀비 pc는 우선 해쉬값을 분석하여 정확한 킷값에 의한 해쉬값인지를 분석한다. 그래서 정확한 hash키에 의해 decrtptinon된 값이면 뒤의 url 및 스캐쥴링 date를 입력받게 되고 그렇지 않을 시에는 해당 url 및 스케쥴링을 버리게 된다. 공격자의 좀비pc만이 정확한 해쉬키값을 이용한 encrytion을 하게 되고 나머지 일반 좀비pc들은 엉뚱한 킷값을 이용하여 encrytion을 하게 된다. 그렇게 되면 공격자의 좀비pc만이 공격통제권을 가지게 된다. 또한 공격자에 대한 역추척에 대해서도 위에서 말한 방법으로 방어가 가능하게 된다. 공격자의 공격명령이 내려지

기 전에 이미 좀비pc들은 IRC채팅채널을 이용하여 지속적으로 쓰레기값들을 교환하게 된다. 그러던 중에 공격자가 공격 명령을 내리게 되면 진짜 공격명령 값을 찾는것은 불가능하다. 또한 모든 좀비pc가 irc채팅채널을 개설하여 서로간의 유기적인 통신이 가능하게 되어 공격명령은 상하 방식이 아니 루프 방식으로 좀비pc간의 통신으로 이뤄지게 되면 특정 시간후에는 몇회의 반복적인 공격명령을 하달받게 되면 공격자를 찾는 것은 더욱 어렵게 된다.

	대안	최종대안
동시접속프로세스 유지의 문제	1.윈도우 임시 템퍼러리 파일의 지속적 삭제 2.해당 다운로드 프로세스의 suspend mode로의 수시전환	자연스러운 다운로딩 속도의 감소(연속적으로 추가되는 다운로딩 프로세스의 중첩으로 좀비PC 리소스 감소로 인해 다운로딩 프로세스의 속도가 저하된다.
공격전달 방법의 문제	1.좀비PC IP를 목록화 하여 좀비PC간 통신 유지 2.좀비PC MAC ADDRESS를 목록화 하여 좀비 PC간 통신 유지	IRC채널을 이용한 통신 (좀비PC가 IRC채널 개설/참여를 통해 좀비PC간 공격명령 전달)
공격통제권의 문제	누구나 공격통제권 획득 가능	공격명령 구성에 해시값을 넣어 ATTACKER에 의한 공격명령인지 판단

● 시행착오의 도식화

마지막으로의 문제점은 다운로딩 URL공격으로서 해당 통신이 성립이 되야만 공격이 이루어지게 되는데 그럴러면 ip spoofing이 불가능하게 된다. 그렇게 되면 좀비pc가 노출이 되게 된다. 또 한가지는 다운로드 프로세스 multitaksing의 이유로 ip address의 변경이 불가능하게 되어 방어하는 입장에서는 중복 ip에서 반복된 작업의 요청을 deny하게 되면 방어가 쉬워진다.

2-4. < 최종 전개 >

좀비pc는 victim url에 대한 다운로딩 multi tasking 공격을 감행하게 된다. 한 개의 좀비pc당 30~50회정도의 multi tasking을 통해 victim 서버를 busy하게 만들게 된다. 이렇게 함으로써 공격자는 안전하게 공격통제권을 가지게 된다.

3. CDoS공격 분석

< 공격방법 단계적 기술 >

● 공격방법 순서도

(참조)

1)공격프로그램/IRC채널관리/공격명령 프로그램 공격싸이트 다운로드url접속 루프 스크립트 IRC채팅 채널 생성 PERL언어로 작성(채널랜덤생성)

IRC채팅채널PEAL언어로 작성(채널랜덤접속)

2)공격단계 1,2,3

①victim의 공개된 다운로드 URL로 미리 구현해 놓은 다운로드 루프 프로그램을 이용하여 해당 URL에 반복적인 다운로드를 시도한다. 이때에 다운로드 프로세스가 중첩될 수 있게끔 빠르게 연결을 형성하여 중첩된 프로세스가 30~50개를 유지한다.좀비PC성능상 30~50개의다운로드 프로세스가 걸리게 되면 자연스레 다운로딩 속도가 느려져 동시접속 프로세스 개수의 유지가 용이해진다.

②일정횟수 이상의 좀비PC와 VICtim간의 연결이 성립되면 좀비PC의 과부하를 막기 위해 VICTim과의 접속을 제한한다.

③해당 VICTIM서버는 과도한 연결로 인해 정상적인 동작이 어렵게 된다.

3-1. <CDoS공격 가능 범위, 대상>

● 모든 관공서.은행.기업,학교 등 일반인이 사용하는 서버를 보유한 VICTIM

● 다운로드 URL을 보유한 모든 서버

(예 입사시즌에 많은 기업들은 입사 관련 자료를 다운로드 링크한다.

● 게임사이트의 게임 다운로드

● MS의 다운로드센터 등

기관명	다운로드 URL	CDOS 공격 적합성
삼성 다운로드 센터	http://www.samsung.com/sec/support/download/supportDownMain.do	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
LG 다운로드 센터	http://www.lgservice.co.kr/SearchSddr.laf	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
MS 다운로드 센터	http://www.microsoft.com/downloads/search.aspx?displaylang=ko	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
토마토 저축은행	http://www.tomatobank.co.kr/04_customer/data/09.pdf	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
신한은행	http://img.shinhan.com/hpe/data/upload/comadm/bizbbs/03/091111_230011502_seol.pdf	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
단국대학교 서식파일/공지	http://www.dankook.ac.kr/web/kor/d1_2?p_p_id=BBS_1_INSTANCE_Um1p&p_p_lifecycle=1&p_p_state=exclusive&p_p_mode=view&p_p_col_id=column-1&p_p_col_pos=1&p_p_col_count=2&_BBS_1_INSTANCE_Um1p_struts_action=%2Fext%2Fnotice%2Fgeta&_BBS_1_INSTANCE_Um1p_messageId=893238&_BBS_1_INSTANCE_Um1p_attachment=%EC%A1%B0%EC%A7%81%EC%9E%AC%EC%83%9D%EA%B3%B5%ED%95%99%EC%97%B0%EA%B5%AC%EC%86%8C+%ED%95%99%ED%9A%8C.jpg	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
시청 행정서식파일	http://spp.seoul.go.kr/cms/board/Download.jsp?fileId=IUAjJDI0MDA0LS0kJA http://spp.seoul.go.kr/cms/board/Download.jsp?fileId=IUAjJDEzNzk2LS0kJA	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음

	http://spp.seoul.go.kr/cms/board/Download.jsp?fileId=IUAjJDExMzUwLS0kJA	
우리은행 공지사항 게시물	http://pot.wooribank.com/pot/comm/bbs/NewsBBS_Qry.jsp?q=C0A8582B189E02D2E8CBAF1B1720C416D16BC557C325D4&Seq=3274&NowPage=2&BbsCode=45&RowCnt=10&SearchGubun=01&SearchValue=&BbsInfo=Y|N|N|N&GRP=3274	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
한국은행 공지사항 게시물	http://www.bok.or.kr/down.search?file_path=/attach/kor/561/2009/11/1257227713294.hwp&file_name=1118 공고.hwp	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
국방부 홈페이지 게시물	http://www.mnd.go.kr/mndMedia/inform/notice/index.jsp?topMenuNo=1&leftNum=1/홍보자료.hwp	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
청화대 홈페이지	http://www.president.go.kr/kr/_lib/bbs/remote_view.php?data_path=bWFpbnRodW1icy8xMjU4MTc4NzQzLmpwZw	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
국세청 공지사항 게시물	http://www.nts.go.kr/news/news_06.asp?minfoKey=MINF5320080211205338&top_code=&sub_code=&sleft_code=&ciphertext=&type=V#	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음
서울 지방 경찰청 공지사항	https://www.smpa.go.kr/smpa2007/bbs/board/down.asp?anum=42779	중복 다운로딩/특정 작업에 대한 중복 IP 가능/전체 다운로딩 트래픽 제한 없음

3-2. < 공격방법 상세 분석 >

1) victim 다운로드 url 공격

(1)

victim의 웹을 scan하여 공격이 유효한 다운로드 URL을 찾아낸다.
조건 ① 일반인 누구에게나 공개된 웹다운로드 URL ② 정책테스트 : 특정 ip의 반복된 작업 시도에 대한 차단의 enable/disable에 대한 설정 테스트 ③ 임계치를 설정하여 총 다운로드 연결 개수의 제한이 없는지 테스트 ex)입사시즌 회사의 이력서 다운로드 URL, 게임싸이트의 게임 s/w 다운로드 URL, 업데

이트(각종제품에 대한 펌웨어) URL

(2)

victim destination url과 스캐쥴링 데이트의 업데이트
①시작프로그램에 등록된 좀비PC툴에는 프로그램을 통하여 IRC채팅채널을 생성하게끔 포함된다. 채팅채널의 주소값은(0~10000)까지의 값을 랜덤으로 취하여 채널값을 생성해낸다. 또한 위와 같은 방법으로 채팅채널 주소값을 생성하여 채팅채널로의 접근을 시도한다. 채팅채널의 접근은 루프로 계속 반복하여 access시에는 해당 루프를 멈추게 된다. 그런후에는 채팅채널을 개설한 컴퓨터와 채팅채털에 접속한 pc들간의 접속을 시스템의 종료시까지 유지한다. 시스템 재시작시에는 위의 방법을 되풀이하여 다시 채널을 통한 좀비pc간의 통신을 유지한다. ②공격자 좀비pc는 접속된 채팅채널을 통해 다른 좀비pc에게 공격지 url과 스케쥴링을 전송한다. 전송 방식 : fghjshksd11x1(해쉬값) dst:http://www.naver.com/1111.zip date:09/11/30 해쉬 : sha-256 이용 위와 같은 공격명령을 다른 좀비pc에게 IRC 스크립크를 통해서 전송하게 된다. 앞의 해쉬값은 공격자가 좀비pc툴에 미리 심어놓은 공격툴을 통해 해쉬값을 분석한다. 공격자는 뒤의 공격지 ip와 스케쥴링 데이트를 미리 공격툴끼리 정해놓은 해시키값을 이용하여 해싱처리 한뒤 공격메시지 앞에 첨부한다. 그렇게 되면 공격명령을 전송받은 좀비 pc는 우선 공격지url과 date를 미리 사전에 정해진 해시키값을 이용하여 encryption한후에 전송되어진 해시값과 비교하여 본다. 비교 되어진 해시값이 일치 하게 되면 공격자가 사전에 정해놓은 해시키값을 이용한 공격명령이라는 것이 확인이 된다. 그렇게 되면 좀비pc는 해당 명령을 다운로드URl 멀티테스킹 공격툴에 입력하여 destinaton url과 date 스케쥴링을 완성한다.

(3)

victim에 대한 공격을 시행한다.
① 좀비pc들은 충분한 시간동안 IRC채팅채널을 통해 destination url과 데이트 스캐쥴링을 전부 전송받은후에 해당 시간이 되면 일제히 공격을 시작한다. ② 좀비pc툴에는 다음과 같은 프로그래밍이 포함되어있다. ► 동시 다운로드 수 제한 해제 레지스트리(windows 기준) 기본적인 동시 다운로드 가능개수는 2~3개로 되어 있지만 해당 레지스트리 값을 늘려주어 동시 다운로드수의 제한을 풀어준다. ► auto loop downloading 프로그램 전송받은 공격 url을 입력하여 해당 url을 연속적으로 50~80회이상의 다운로드가 이루어

지도록 프로그램밍 되어있다.(multi tasking을 이용하여 순차적인 접속이 아니라 격자형으로 동시접속이 이루어지게 해준다.)
③다운로드 URl 멀티테스킹 공격을 감행한다.
②번의 프로그램을 이용하여 자동적으로 해당 다운로드 URL로의 연결을 형성한다.
이때에 사람에 의한 작업이 아닌 자동화된 프로그래밍을 이용하게 되므로 훨씬 빠르게 다수의 연결을 형성하여 50개정도의 다운로드 프로세스를 가동시키게 된다.
④victim으로의 공격을 일정시간 유지시킨다.
일반 좀비pc에서의 50개정도의 다운로딩 프로세스의 생성은 좀비pc의 리소스를 많이 차지하게 되어 많은 속도 저하를 가져오게 하여 일정시간이상의 다운로딩 프로세스 유지를 가능하게 해준다.
⑤좀비pc에서 모든 다운로딩 프로세스가 종료된후에는 다시 일상적인 pc로 복귀하여 다시 ①~⑤과정을 반복하게 된다.

2) 공격명령전달 체계의 확립

IRC채팅을 이용한다.
①activex , p2p를 통해 다운로드 된 좀비pc툴에는 공격명령 체계의 확립과 관련하여 아래의 프로그래밍이 존재한다(공격명령 전달에 관한 프로그램은 시작프로그램에 등록되어 항시 메모리상에 올려놓는다.).
► IRC 채팅채널 개설 : 자바스크립트를 이용하여 채팅채널을 개설하게 된다. 채팅채널명 값은 랜덤(범위:1~1000,a~f, 10개서버)하게 생성된다.
시스템의 종료시까지 채팅 채널은 유지가 되고 시스템의 재시작 시에는 다시 랜덤값을 이용하여 채팅채널을 개설한다.
►IRC채팅채널로의 접속 : 자바스크립트를 이용하여 채팅 채널로의 접속을 시도한다.
채팅채널명값은 랜덤(범위:1~1000,a~f, 10개서버)하게 생성된다.
생성된 채팅 채널명값으로 지속적으로 접속을 시도하고 IRC서버로부터의 접속이 되었다는 response 값을 받게 되면 접속을 중지하고 해당 채팅채널에 머무르게 된다.
►공격명령 전달 스크립트 : 채팅채널을 개설한 좀비pc는 공격명령을 스크립트를 통해 전달한다.
예) fkjaasx01x00 (해쉬값) dst url:http://www.naver.com/1111.avi (공격지 url)
date: 09/11/30 (공격 시간 스케쥴)
공격 명령은 위와 같이 구성되고 해시값은 뒤의 dst url과 date를 해시처리 하여 생성한다.
해시키값은 사전에 공격자가 정의해놓은 킷값을 사용한다.
또한 쓰레기값 생성기에서 생성된 공격명령을 수령하여 스크립트를 통해 다른 좀비 pc로 전달한다.
►공격명령 수령 스크립트 : 채팅채널에 참가한 좀비pc는 공격명령을 스크립트를 통해 전달 받게 된다.
예) fkjaasx01x00 (해쉬값) dst url:http://www.naver.com/1111.avi (공격지 url)
date: 09/11/30 (공격 시간 스케쥴)
공격명령은 위와 같이 구성되고 명령을 받게 되면 우선 해시값을 분석한다.

사전에 정의해놓은 킷값을 이용하여 dst url과 date를 해쉬처리하여 전송받은 해시값과 비교하여 같으면 정상적인 공격명령으로 인지하고 그렇지 않으면 비정상적인 공격명령으로 간주하여 명령을 drop하게 된다.
►IRC 공격명령 스크립트와 다운로드URL multitasking 공격프로그램간의 연결 자바스크립트
공격명령을 전달받게 되면 해당 dst url과 스케쥴링 데이트를 multitasking 공격프로그램과 연결해줄 수 있는 스크립트가 필요하다.
스크립트는 해시테스트를 통과한 dst url과 스케쥴링 데이트를 multi tasking 공격 프로그램에 삽입한다.
그 후에 삽입된 dst url과 스케쥴링 데이트를 IRC 채팅채널에 스크립트로 뿌리게 된다.
위의 두가지 작업을 실행하게 된다.
►쓰레기 값 생성기
정상적인 공격명령을 숨기기 위하여 사전에 정의해놓은 해시키값과 다른 값을 이용하여 해싱한 데이터를 생성한다.
예) 0x0xfffgak (해쉬값) dst url:http://www.naver.com/1111.avi (공격지 url)
date: 09/11/30 (공격 시간 스케쥴)
위에서 해시값은 사전에 정의해놓은 정상적인 킷값을 이용하지 않고 쓰레기값생성기에서 임의로 생성한 킷값을 이용하여 해싱처리 하였다.
생성된 해시값은 공격명령 전달 스크립트를 통해서 다른 좀비pc로 전송되게 되고 전송 받은 좀비pc는 해시를 통하여 값의 진위여부를 판단하여 명령을 drop시키게 된다.

②좀비pc의 채팅채널의 개설과 채팅채널의 참여가 이루어진다.
좀비 pc는 감염과 동시에 ①에 설명한 프로그램을 통하여 채팅 채널을 랜덤값으로 개설하게 된다.
한번 개설이 되게 되면 시스템의 종료 이전까지 지속적으로 유지되고 다른 좀비pc가 채팅채널을 접속할 수 있게 채널을 유지시킨다.
채팅채널을 개설함과 동시에 ①의 프로그램을 이용하여 랜덤한값의 채팅채널명으로의 접속도 지속적으로 시도하게 된다.
접속이 이루어져 서버로부터 정상적인 response를 받게 되면 다른 채널로의 접속 시도를 중지하고 해당 채널에서 공격명령을 대기하게 된다.
시스템이 재시작 된 후에는 다시 위의 작업을 반복하여 IRC채널에 접속하게 된다.

③지속적인 좀비pc간의 통신
IRC채널로 개설과 접속이 이루어지게 되면 IRC를 개설한 좀비 pc는 쓰레기 값 생성기를 통해 생성된 쓰레기 값을 IRC스크립트로 지속적으로 채널참가좀비pc들에게 전파한다.
그렇게 하여 지속적으로 허위공격신호를 주고 받음으로써 로그를 통한 역추적을 방해하게 한다.
쓰레기값을 받은 좀비pc는 공격명령 수령 스크립트를 통해 해시값이 적당한 킷값에 의한 것인지 아닌지를 판단하여 명령을 drop시킨다.

④공격명령의 전달
공격자 역시 한 대의 좀비 pc를 보유하여 다른 좀비 pc와 마찬가지로 irc채널의 수립 및 참여를 반복한다.
공격자좀비pc 역시 좀비pc간의 연결이 이루어지면 쓰레기값을 생성하여 지속적으로 통신을 시도한다.
그러다가 공격 목표가 정해지면 공격자는 정상적인 해시키값을 이용하여 해싱처리한 값을 포함한 정상 공격명령을 자신의 IRC채널에 참여한 좀비pc에게 전달하게 된다.

⑤공격명령의 전파
공격자로부터 정상적 공격명령을 받은 A좀비pc는 공격명령 수령 스크립트,공격명령 전달 스크립트,IRC 공격명령 스크립트와 다운로드URL multitasking 공격프로그램간의 연결 자바스크립트 를 이용하여 자신의 IRC채널에 참가한 B,C,D,E,F좀비pc들에게 전달한다.
이 공격명령을 받은 B,C,D,E,F좀비pc들은 자신의 IRC채널에 접속한 G.....X.....a....x까지의 컴퓨터들에게 명령을 전달하게 된다.
물론 랜덤한 값으로 IRC채널이 개설되고 참여를 하게 되지만 범위를 정해두었고 IRC채널에 대한 참여가 범위내에서 정상적인 참여를 하였다는 response를 받기 전까지 지속되기 때문에 시기의 문제일뿐 결국에는 모든 좀비pc는 공격명령을 전달받게 된다.

⑥공격자의 신변 보호
공격 당일 해당 시간까지 위의 프로세스는 지속적으로 이루어진다.
충분한 시간을 두게 되면 공격명령은 대부분의 좀비pc에서 1~2회이상을 거쳐가게 되고 결국은 로그분석을 통한 진원지를 찾기란 사실상 불가능 하다. 또한 지속적인 쓰레기값의 통신으로 인해 분석해야 로그의 양은 기하급수적으로 늘어 공격진원지의 판단은 불가능하고 가능하여도 매우 오랜 workfactor가 소요된다.

3-3. < 좀비PC툴킷 상세내용 >

● CDOS 툴킷 상세내용

1) 레지스트리 변경/등록 관련

① 동시 다운로드 수 제한 해제

```
;MaxConnectionsPerServer number
[HKEY_CURRENT_USER₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings]
"MaxConnectionsPerServer"=dword:00000028

;MaxConnectionsPer1_0Server number
[HKEY_CURRENT_USER₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings]
"MaxConnectionsPer1_0Server"=dword:00000028
```

MaxConnectionPerServer 레지스트리 DWORD값을 늘려 줌으로써 기본 2~3개로 되어있는 웹 다운로딩 멀티테스킹의 제한이 풀리게 된다.

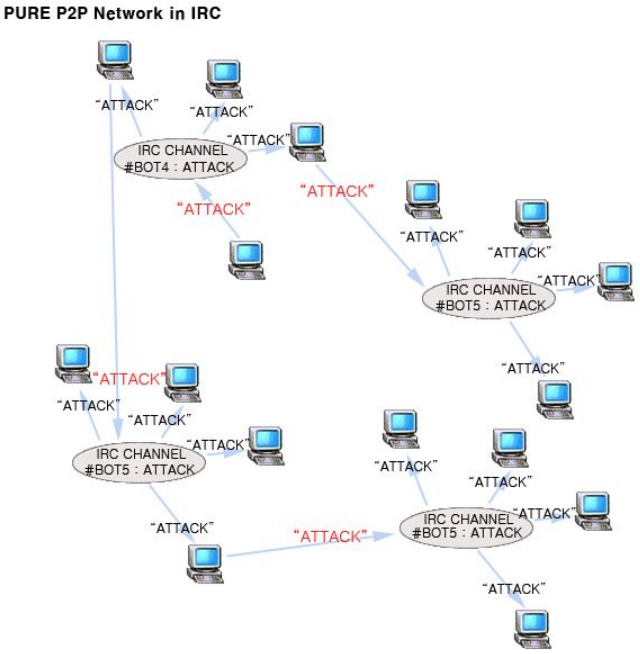
② CDOS툴킷(공격명령 체계 구성 프로그램) 시작프로그램 등록

```
[HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RUN]
[HKEY_CURRENT_USER_₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RUN]
```

③ 인터넷 보안 해제

```
[HKEY_CURRENT_USER_₩SOFTWARE₩MicrosoftWindows₩CurrentVersion₩Internet Settings₩Zones₩0]
```

인터넷 보안 관련 activex차단해제,
다운로드 프로세스 작동시 차단 해제



2) 공격명령 체계 구성 프로그램

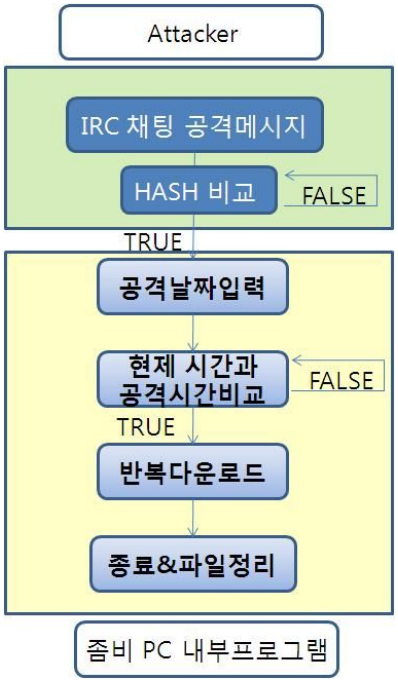
IRC채널을 이용한 좀비PC간의 통신을 관장하는 프로그램 좀비PC는 IRC채널을 생성하고 다른 좀비PC의 IRC채널에 접근한다. 해당 프로그램은 위의 레지스트리를 통해 윈도우의 시작프로그램에 등록되어 시스템 시작시마다 작동을 하게 된다. PERL을 이용하여 프로그래밍 하였다.
아래에 자세한 소스코드가 등록되어 있다.

```
//IRC 컴포넌트 사용
use POE qw(Component::IRC);

//랜덤으로 채널 5개 생성 (접속할 채널)
for(my $i=1;$i<6;$i++)
{
my $tempch[0] = '#'
my $tempch[1] = 'rand(10000)'
@joinchannel = join('',@tempch)
}

//랜덤으로 채널 5개 생성 (생성할 채널)
for(my $i=1;$i<6;$i++)
{
my $tempch[0] = '#'
my $tempch[1] = 'rand(10000)'
```

```
@createchannel = join('',@tempch)
}
      print "Connected to ", $irc->server_name(), "₩n";
//랜덤으로 생성된 5개 채널 생성
      $irc->yield( creat => $_) for @channel;
//랜덤으로 생성된 5개 채널에 접속       $irc->yield( join => $_ ) for @joinchannel;
```

3) CDOS 공격 프로그램

IRC채널을 통해 공격명령을 수령하게 되면 공격 프로그램이 공격메세지를 분석하여 우선 HASH코드를 분석한다. 공격자가 사전에 정의해놓은 킷값이 정확하면 해당 공격명령을 입력받게 되고 정확하지 않다면, 해당 명령은 DROP 된다. 이 프로그램에서는 공격명령을 받아 공격날짜와 공격지 URL을 입력하고 스케쥴링 하게 된다. 이렇게 하여 공격 시간이 되면 공격을 시작하여 공격 URL로의 무제한 접근이 시작되게 된다.




```
/*스케쥴러 & 반복 다운로드*/
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#define MAXREPET 10  //반복다운로드수
#define MAXSTR 3

int main()
{
        int j=0,i=0;
        char* str[MAXSTR];
        FILE* fd;
//------------------------------스케쥴러----------------------//
        time_t curr_time,att_time;
        struct tm curr_ts,att_ts;
```

```
        time(&curr_time);
        curr_ts=*localtime(&curr_time);

    att_ts.tm_year=109; //1900+
    att_ts.tm_mon=11-1; //0이 1월
    att_ts.tm_mday=15;
    att_ts.tm_hour=17;  //0~23
    att_ts.tm_min=23;
        att_ts.tm_sec=0;
        att_time=mktime(&att_ts) ;
        while(1){
                if(curr_time==att_time){break;}
                if(curr_time>att_time){exit(1);}
                time(&curr_time); }
//--------------------자동 다운로드 ----------------------------//
        fd=fopen("c:₩₩temp₩₩down.html","w+t");
    str[0]="<HTML><HEAD><TITLE>Down</TITLE>";
        str[1]="<META  HTTP-EQUIV=₩"REFRESH₩"  CONTENT=₩"0;URL=다운로드URL경
로₩">";
        str[2]="</HEAD><BODY></BODY></HTML>";

        for(i=0;i<MAXSTR;i++){fputs(str[i],fd);}
        fclose(fd);
//-------------------다운로드 반복 ----------------------------//
        while(j<MAXREPET){system("c:₩₩temp₩₩down.html");j++;}
//---------------------종료&파일정리--------------------------//
        system("del c:₩₩temp₩₩down.html");
        exit(1);

        return 0;}
```

4. 사회에 미치는 파급

● 4-1. CDoS의 파급

CDOS는 서버에 지속적인 다운로드 요청을 보내 과부하를 일으키는 방식이기 때문에 다운로드 가능한 파일이 존재하는 서버는 모두 공격이 가능하다는 가정이 성립한다.

이를 서버입장에서 살펴보면 다운로드 가능한 파일을 제공하는 것 만으로 CDOS에 취약점을 노출하는 것이 된다. 반대로 말하면 파일 다운로드를 제공하지 않는 서버는 CDOS공격에 취약점을 노출하지 않는 것으로 볼 수 있으나, 이러한 웹서버는 현실적으로 존재하기 어렵다. 이는 웹사이트에 있어 파일 다운로드 기능이 필수적인 기능임을 반증하는 것으로 절대다수의 웹사이트가 CDOS공격에 취약점을 노출하고 있는 것으로 결론지을 수 있다.

따라서 파일 다운로드가 가능한 서버들은 제공하고 있는 파일에 대해 총체적인 점검이 이루어져야 하며 이로 인해 소모되는 사회적인 비용은 상당할 것으로 생각된다. 위에서 소모

되는 작업들은 결과적으로 서버 관리에 있어 다운로드 제공 파일의 인덱스화, 접근 가능/제공 가능 임계치 설정을 의무화시키므로 역설적으로 웹서버의 보안향상에 기여하는 상황이 발생하게 된다.

● 4-2. P2P BOT이 사회에 미치는 파장

기존 master -> slave 방식의 irc bot nertwork는 공격을 내리는 마스터pc의 ip 또는 마스터 irc 채널을 차단하면 감염된 bot을 모두 치료하지 않아도 임시적으로 공격을 중단시키는 것이 가능하였다. 그러나 pure p2p방식의 irc bot network는 공격자도 하나의 bot이 되므로 마스터ip를 차단하는 것이 원천적으로 불가능하다. 다시 말해 bot 스스로 공격명령을 송/수신하므로 이들의 공격을 중지시키기 위해서는 감염된 모든 bot을 치료해야만 한다.

DoS공격은 bot의 확보 측면에서 바라보았을 때 개개인의 부주의로 인해 감염이 이루어지므로, 개개인이 보안관리에 관심을 기울인다면 bot의 다수 확보가 불가능하게 된다.

따라서 대다수의 개개인이 pc의 관리에 관심을 기울이기 전까지 dDoS공격은 계속 될 수밖에 없다. 또한 P2P Bot 방식은 감염된 pc의 치료 전까지 공격을 중단할 수 없으므로 1. 공격이 이루어지는 회선의 접속 차단 2. bot pc의 강제 회수 3. 전화/문자등을 통한 bot pc유저와의 직접 통보 등을 통해서만 공격을 중지시킬 수 있다.

DDoS 공격은 일정 수 이상의 bot이 확보되었을 때 영향력이 있으므로, 위의 1/2/3과 같은 대처방안이 수행되고 있을 때는 이미 수만 대 이상의 P2P Bot이 감염된 것으로 바라볼 수 있다. 따라서 감염 pc의 치료를 위한 Anti-Virus(백신)의 폭발적인 수요 증가가 예상된다. 또한 이를 악용해 결제를 유도하는 악성 유사 Anti-Virus 프로그램이 대량 생산/유포될 수 있으므로 Anti-Virus의 제작/유포와 관련된 관계 법령을 정비해야 할 것으로 생각된다.

5. 참고 자료

1) 정보 보안 개론 : 큰 그림을 그려주는 정보 보안 입문서
[IT COOKBOOK 시리즈 (한빛미디어) 84]
양대일 저한빛미디어2008.06.28
2)바이러스디도스 Virus DDOS : 그 해 짧았던 휴가와 컴퓨터 & 바이러스
배상일 저샤프론2009.10.01
3)애플리케이션 해킹 Application Hacking (양장) : 대한민국 최고의 보안 연구원들이 공개하는 애플리케이션 해킹의 비밀
정상민, 남성일, 김태훈 저이호웅 감수북앤라이프2009.06.25
4)정보보호 대학동아리 웹사이트 KUCIS http://kucis.org/
5)네이버 카페 - 정보보호커뮤니티 http://cafe.naver.com/korsec
6)안철수 연구소 http://home.ahnlab.com
7)웹, 해킹과 방어 : 사용자 정보 보호를 위한 웹 개발 가이드
최경철 저프리렉(이한디지털리)2008.12.01
8)웹 해킹 & 보안 완벽 가이드 : 웹 애플리케이션 보안 취약점을 겨냥한 공격과 방어
[에이콘 해킹 보안 시리즈]
대피드 스투타드, 마커스 핀토 저조도근,김경곤,장은경,이현정 역에이콘출판사2008.11.21
9)서비스 거부 공격에 대비한 TCP/IP 스택 강화 블로그
http://www.wssplex.net/TipnTech.aspx?Seq=127