금보원 2010-015

DDoS 공격 대응 절차서

2010. 12

금융보안연구원

본 절차서의 내용 중 오류가 발견되었거나, 내용에 대한 의견이 있을 경우 금융보안연구원 해킹대응팀(fsah@fsa.or.kr)으로 해당 내용을 보내주시기 바랍니다.

차례

DDoS 공격 대응 절차서

그림 · 표

DDoS 공격 대응 절차서

제1장 개 요

제 1 절 배 경

DDoS 공격은 지난 2003년 MS-SQL의 취약점을 이용한 웜(Worm)의 유포로 세계적인 인터넷 불통을 발생시킨 1.25 인터넷 대란으로 유명해졌고, 최근에는 특정 기업의 인터넷 서비스를 마비시키고 이를 빌미로 금전을 요구하는 일명 '사이버 조폭' 형태로 사회적 이슈가 되고 있다.

더욱이 작년 7.7 DDoS 대란(일부 은행의 인터넷 뱅킹, 조선일보 및 청와대, 국방부 등의 홈페이지 서비스 장애가 발생한 사건) 이후, 언론 매체나 커뮤니티 등을 통해 해당 사고와 관련 정보에 대해 많이 접하였을 것이다. 이러한 사고로 더 이상 특정 산업군, 특정 직군에 속하는 사람들만의 이슈가 아닌 우리 사회 전반적인 '범사회적인 이슈'가 되었음을 증명하게 되었다. 더욱 우려되는 것은 비밀스런 공격방식에서 공개적인 공격방식으로 그 수법이 날로 대담해지고 있다는 것이다.

이에 인터넷을 통한 비즈니스 모델을 가지고 있는 기업이라면 누구나 피해자가 될 수 있는 공격임을 알고, 최신 동향과 사고 사례를 알아보고 그에 따른 공격 유형을 분석하여 체계적인 예방활동과 대응방안, 업무 계획을 수립하는 것이 DDoS 공격에 대비하는 최선의 방책이 될 것이다.

제 2 절 목 적

본 절차서의 목적은 금융권에서 제공하고 있는 전자금융 서비스의 안정성 및 가용성을 위협할 수 있는 최근의 DoS/DDoS 공격에 대한 예방 및 대응 방안을 마련하여 DoS/DDoS 공격에 효과적으로 대응하고 공격에 대한 피해를 최소화하는데 그 목적이 있다.

제 3 절 범 위

DoS/DDoS 공격의 유형 및 증상, 대응 방안을 네트워크 장비, 운영체제 등의 보안 설정 기능을 이용한 측면에서 살펴본다.

제2장 DDoS 정의 및 유형

제 1 절 DDoS 정의 및 유형

1. DDoS 정의

□ DDos(Denial of Service attack)

○ 많은 수의 호스트들에 DoS 공격용 프로그램들이 분산 설치되어 이들이 서로 통합된 형태로 어느 목표 시스템을 공격해 해당 시스템의 리소스를 독점하거나, 파괴함으로써 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격 방법으로,

○ 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.

2. DDoS 공격 방식

□ DDoS 공격 순서

○ 공격자는 악성코드를 개발 후 악성 이메일, 웜・바이러스, 게시판 등 다양한 방법을 동원하여 불특정 다수의 시스템에 감염시킴으로써

원하는 때에 원하는 대상을 공격하기 위한 봇넷을 구성한다.

○ 명령 제어 서버(Command & Control Server)를 통해 공격 대상, 공격시간, 공격 방식 등을 감염 시스템에 전달하여 일시에 특정 사이트 및 시스템을 무력화 시킨다. 그러나 7.7 DDoS 대란과 같이 명령 제어 서버를 이용하지 않고 DDoS 공격을 수행하는 등 공격 형태가 더욱 더 다양화 되고 있다.

○ 이후 공격에 사용된 PC의 파일 및 디스크 삭제하여 증거를 인멸한다.

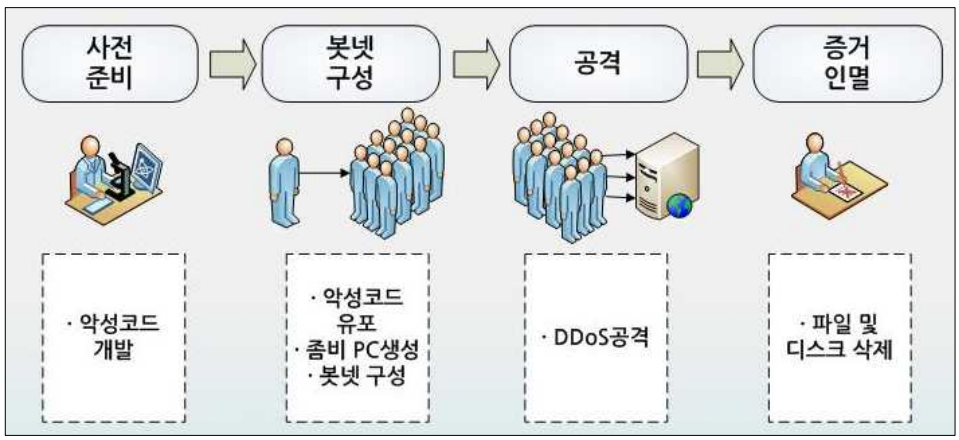


그림 1 DDoS 공격 순서

□ DDoS Agent 유포방법

○ DDoS 공격을 하기 위해 좀비 PC를 이용하여 봇넷을 구성해야 하며, 일반 PC를 좀비 PC화 하기위해 악성코드에 DDoS Agent를 포함하여 아래와 같은 방법으로 감염시킨다.

- P2P : 정상 S/W에 삽입하여 전파
- 웜/바이러스 : 웜/바이러스에 삽입하여 전파
- 사회공학 : 이메일, 게시판 첨부파일 등을 통한 전파
- 홈페이지 : 취약한 사이트 해킹을 통한 전파

3. DDoS 공격 유형

□ DDoS 공격은 크게 대역폭 공격, PPS공격, 어플리케이션 공격으로 나뉘며 최근에는 이를 혼합하는 혼합형 공격이 많이 이뤄지고 있다.

	대역폭 공격	PPS 공격	어플리케이션 공격
사용 프로토콜	주로 UDP/ICMP	TCP	HTTP
공격 PC 위치	국내	국내/국외	국내/국외
IP변조여부	변조/실제IP	변조/실제IP	실제IP
공격 유형	1000~1500byte 1Gbyte 수십만 PPS	64byte 이하 100Mbyte 수십만~수백만 PPS	동일 URL 접속 시도 CC Attack 등
공격 효과	회선 대역폭 초과	네트워크 장비, 보안장비, 서버 등의 부하 발생	웹/DB 서버 부하 발생
피해 시스템	동일 네트워크에서 사용 중인 모든 시스템	공격 대상 시스템 및 동일 네트워크의 모든 시스템	공격 대상 시스템

표 1 DDoS 공격 유형

제3장

세부 DDoS 공격 유형 및 증상, 대응방안

제 1 절 대역폭 공격

대역폭 공격은 다수의 PC를 이용하여 다량의 패킷을 전송함으로써 네트워크 대역폭의 처리 한계를 초과시키는 공격 유형이다. UDP Flooding, ICMP Flooding 등이 대표적이며 동일 네트워크 내 모든 서버의 접속 장애를 유발하는 특징을 가진다.

1. 공격 개요

□ UDP Flooding

○ UDP(User Datagram Protocol)는 비연결형(Connectionless) 서비스로서 포트 대 포트로 패킷 전송

○ 대표적인 응용 서비스로는 TFTP, SNMP, 실시간 인터넷 방송 등이 있으며, 출발지 IP 주소 및 포트를 스푸핑 하기 쉬움

○ 1000~1500 바이트 정도의 큰 패킷을 대량으로 공격 대상 서버로 전송하여 네트워크 회선의 대역폭을 고갈시킴

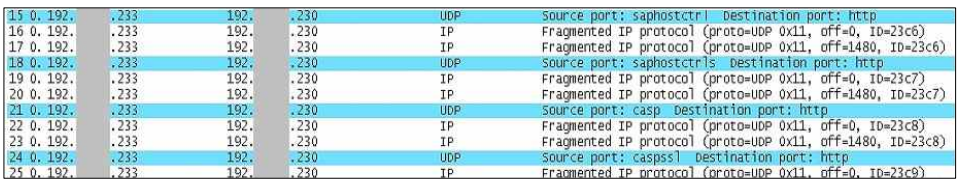
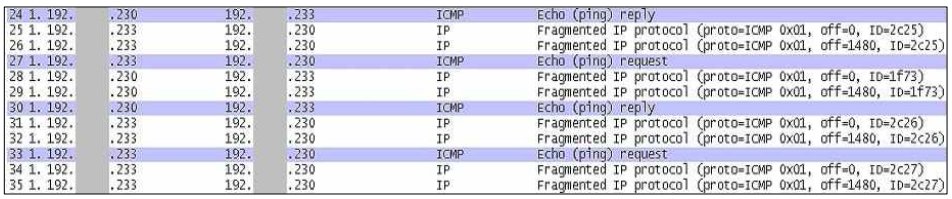


그림 2 UDP Flooding 공격 예시

□ ICMP Flooding

○ ICMP(Internet Control Message Protocol)는 호스트간의 혹은 호스트와 라우터간의 에러와 상태변화를 알려주고 요청에 응답하는 기능을 하는 네트워크 제어프로토콜로써 활성화된 서비스나 포트가 필요 없는 프로토콜

○ 사용 대역폭 용량이 초과할 정도의 많은 ICMP 패킷을 서버에 전송함으로써 네트워크 회선의 대역폭을 고갈시키는 공격



24 1. 192.	.230	192.	.233	ICMP	Echo (ping) reply
25 1. 192.	.233	192.	.230	IP	Fragmented IP protocol (proto=ICMP 0x01, off=0, ID=2c25)
26 1. 192.	.233	192.	.230	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1480, ID=2c25)
27 1. 192.	.233	192.	.230	ICMP	Echo (ping) request
28 1. 192.	.230	192.	.233	IP	Fragmented IP protocol (proto=ICMP 0x01, off=0, ID=1f73)
29 1. 192.	.230	192.	.233	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1480, ID=1f73)
30 1. 192.	.230	192.	.233	ICMP	Echo (ping) reply
31 1. 192.	.233	192.	.230	IP	Fragmented IP protocol (proto=ICMP 0x01, off=0, ID=2c26)
32 1. 192.	.233	192.	.230	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1480, ID=2c26)
33 1. 192.	.233	192.	.230	ICMP	Echo (ping) request
34 1. 192.	.233	192.	.230	IP	Fragmented IP protocol (proto=ICMP 0x01, off=0, ID=2c27)
35 1. 192.	.233	192.	.230	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1480, ID=2c27)

그림 3 ICMP Flooding 공격 예시

2. 탐지 및 대응 방안

□ 탐 지

○ 네트워크 모니터링 시스템을 통한 트래픽 변화주시

○ 네트워크 속도 저하, 라우터 과부하

○ 방화벽, IDS/IPS 트래픽 처리량 증가

○ UDP Flooding의 경우, 잘못된 서비스 포트로 UDP 패킷이 전달되었을 때 발생하는 ICMP Destination Port Unreachable 메시지가 비정상적으로 다수 발생

□ 대응 방안

○ 불필요한 UDP/ICMP 서비스 차단

- 가능한 최상위 구간(국제 GW, IDC 라우터 등)에서 차단

○ 공격 대상 서버에 대한 NULL 라우팅 적용(임시방안)

- 공격 대상 서버에 대한 NULL 라우팅을 적용하여 점진적으로 공격 트래픽 감소
- 동일네트워크에서 운영중인 다른 서버/서비스 보호

○ DNS 서버의 다중화
- 다중 DNS 서버를 운영
- 제3의 등록회사에 DNS를 등록

○ DNS 전용 회선 준비
- 서비스 네트워크 회선과 별도로 우회할 수 있는 DNS 전용 회선 마련

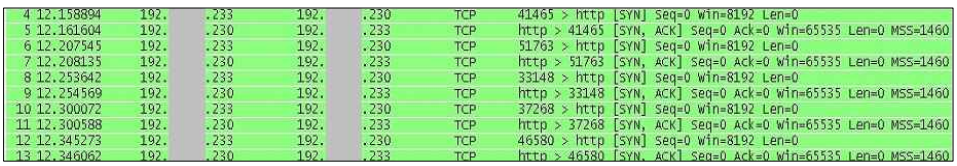
제 2 절 PPS 공격

PPS공격은 Three-way Handshaking을 하는 TCP 프로토콜의 특성을 악용하여 다수의 SYN 패킷을 보내 서버의 연결대기 큐를 고갈시키는 SYN Flooding 공격과 다수의 정상적인 TCP 세션을 생성하여 서버의 CPU 및 메모리 자원을 고갈시키는 TCP Connection Flooding 공격이 있다.

1. 공격 개요

□ SYN Flooding

○ IP가 변조된 다량의 SYN 패킷을 공격 대상 서버로 전송하고, 공격 받은 서버는 다수의 SYN_RECEIVED 세션 상태가 발생하여 서버의 CPU 및 Connection 자원의 고갈을 유발시키는 공격



4	12.158894	192. .233	192. .230	TCP	41465 > http [SYN] Seq=0 Win=8192 Len=0	
5	12.161604	192. .230	192. .233	TCP	http > 41465 [SYN, ACK] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460	
6	12.207545	192. .233	192. .230	TCP	51763 > http [SYN] Seq=0 Win=8192 Len=0	
7	12.208135	192. .230	192. .233	TCP	http > 51763 [SYN, ACK] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460	
8	12.253642	192. .233	192. .230	TCP	33148 > http [SYN] Seq=0 Win=8192 Len=0	
9	12.254569	192. .230	192. .233	TCP	http > 33148 [SYN, ACK] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460	
10	12.300072	192. .233	192. .230	TCP	37268 > http [SYN] Seq=0 Win=8192 Len=0	
11	12.300588	192. .230	192. .233	TCP	http > 37268 [SYN, ACK] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460	
12	12.345273	192. .233	192. .230	TCP	46580 > http [SYN] Seq=0 Win=8192 Len=0	
13	12.346062	192. .230	192. .233	TCP	http > 46580 [SYN, ACK] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460	

그림 4 SYN Flooding 공격 예시

□ TCP Connection Flooding

○ 다량의 SYN 패킷을 공격 대상 서버로 전송하고 3way handshaking이 정상적으로 완료되어, 서버에 다수의 ESTABLISHED 세션 상태가 발생해 서버의 CPU 및 Connection 자원의 고갈을 유발시키는 공격

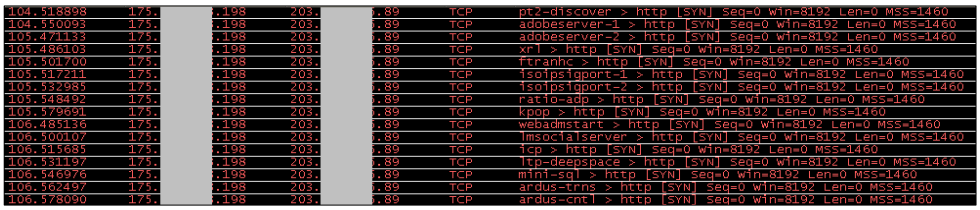


그림 5 TCP Connection Flooding 공격 예시

2. 탐지 및 대응 방안

□ 탐 지

○ 피해 서버 부하 발생, 보안장비 트래픽 처리량 증가

○ 서버 CPU 확인, netstat 명령으로 TCP 세션 상태 확인

○ 평소보다 established 세션이 급격하게 증가

□ 대응 방안

○ 비정상 IP에 대한 ACL 적용

- RFC1918에서 지정한 비공인 IP
- 특정 목적을 가진 IP 및 IANA에서 reserved한 IP

○ Syn Proxy또는 Cookie 기능 사용

- Syn Proxy/Cookie 기능을 제공하는 보안 장비 및 네트워크 장비이용

○ 공격의 진원지가 국외일 경우

- ISP/IDC 등과 협조하여 국제 GW에서 해외 트래픽 차단(NULL 라우팅)
- 라우터간의 Dynamic Routing을 통한 점진적인 트래픽 감소 유도

○ 공격의 진원지가 국내일 경우

- C&C 서버의 조정을 받고 있는 봇넷 PC에 의한 경우가 대부분
- 대외회사에서 공격 IP를 제공하여 봇넷 샘플 확보

- 샘플 분석을 통하여 C&C 서버와 봇넷 PC와의 통신 차단(대외 회사 등 협조)
- 긴급한 보안 프로그램 업데이트 수행(보안업체 협조)
- 공격 소스 IP가 소수일 경우, ACL을 이용하여 차단

제 3 절 어플리케이션 공격

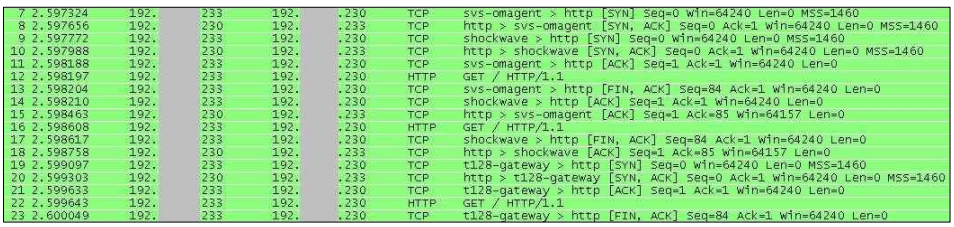
어플리케이션 공격은 Three-way Handshaking을 수행하여 정상적인 TCP connection을 맺은 후, 짧은 시간동안 웹페이지를 반복적으로 요청하여 웹서버의 과부하를 유발시킴으로써 원활한 서비스를 불가능하게 하는 공격 기술로 일반적으로 GET Flooding 공격이라 부르며 변형된 공격기법으로는 NoCache Get, Circle CC Attack, Slowloris Attack 등이 있다.

1. 공격 개요

□ NoCache Get

○ HTTP Request 헤더 User-agent 필드의 Cache-Control 옵션에 'no-cache, must-revalidate' 설정 후 특정 웹 페이지를 요청함으로써 웹서버 및 DB서버의 CPU 및 Connection 자원의 고갈을 유발하는 공격

○ 공격자가 대상 서버에 페이지를 요청할 때 캐싱을 요청하지 않아 웹서버와 DB서버에 부하가 가중되어 서비스 불능 상태 발생가능



7	2.597324	192.	233	192.	.230	TCP	svs-omagent > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
8	2.597656	192.	230	192.	.233	TCP	http > svs-omagent [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9	2.597772	192.	233	192.	.230	TCP	shockwave > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
10	2.597988	192.	230	192.	.233	TCP	http > shockwave [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
11	2.598188	192.	233	192.	.230	TCP	svs-omagent > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
12	2.598197	192.	233	192.	.230	HTTP	GET / HTTP/1.1
13	2.598204	192.	233	192.	.230	TCP	svs-omagent > http [FIN, ACK] Seq=84 Ack=1 Win=64240 Len=0
14	2.598210	192.	233	192.	.230	TCP	shockwave > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
15	2.598463	192.	230	192.	.233	TCP	http > svs-omagent [ACK] Seq=1 Ack=85 Win=64157 Len=0
16	2.598608	192.	233	192.	.230	HTTP	GET / HTTP/1.1
17	2.598617	192.	233	192.	.230	TCP	shockwave > http [FIN, ACK] Seq=84 Ack=1 Win=64240 Len=0
18	2.598758	192.	230	192.	.233	TCP	http > shockwave [ACK] Seq=1 Ack=85 Win=64157 Len=0
19	2.599097	192.	233	192.	.230	TCP	t128-gateway > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
20	2.599303	192.	230	192.	.233	TCP	http > t128-gateway [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
21	2.599633	192.	233	192.	.230	TCP	t128-gateway > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
22	2.599643	192.	233	192.	.230	HTTP	GET / HTTP/1.1
23	2.600049	192.	233	192.	.230	TCP	t128-gateway > http [FIN, ACK] Seq=84 Ack=1 Win=64240 Len=0

그림 6 NoCache Get 공격 예시

□ Circle CC Attack

○ 특정 웹 페이지만을 요청하는 것이 아닌, 웹 페이지 내의 변경된 파라미터 값을 변경하며 페이지를 대량으로 요청함으로써 DB서버에 부하를 일으키는 공격. 마찬가지로 HTTP 헤더에 Cache-Control(CC) flag 'no-store, must-revalidate'가 설정됨

○ 공격 예시 URL : /board/board_view.asp?num=%d(%d가 변경됨)

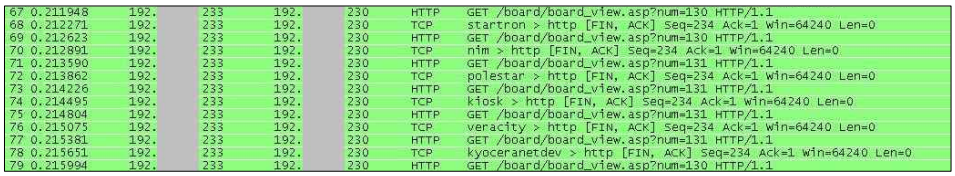


그림 7 Circle CC 공격 예시

□ Slowloris Attack

○ 아파치(Apache) 웹서버를 대상으로 하는 공격기법으로 정상적인 연결을 공격 대상 서버와 맺은 뒤 미완성된 HTTP 헤더를 서버로 전송하면 해당 서버가 완성된 HTTP 헤더를 위해 대기 상태로 머물게 됨

○ 이로 인해 서버에 해제되지 않은 다수의 연결이 존재하여 추가적인 접속 요청을 받아들일 수 없게 됨

○ 비교적 소량의 패킷 전송으로도 공격이 가능하며, Apache 1.x, Apache 2.x, dhpptd, GoAhead Webserver, Squid 등의 웹서버가 취약함

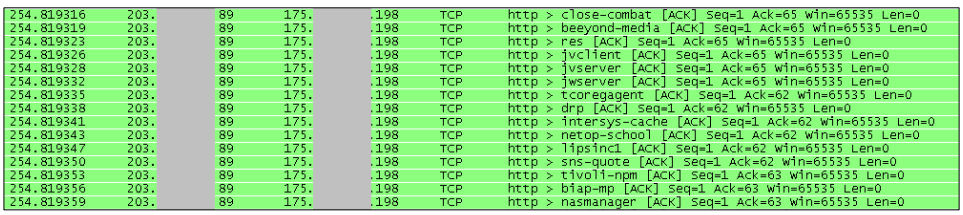


그림 8 Slowloris 공격 예시

□ HTTP Get Flooding

○ 웹페이지(URL)나 php, asp 등과 같은 웹사이트 내의 다이나믹 컨텐츠(Dynamic Contents)에 대한 요청을 집중적으로 수행함으로써 공격 대상 웹서버와 DB서버의 처리용량을 고갈시키는 공격

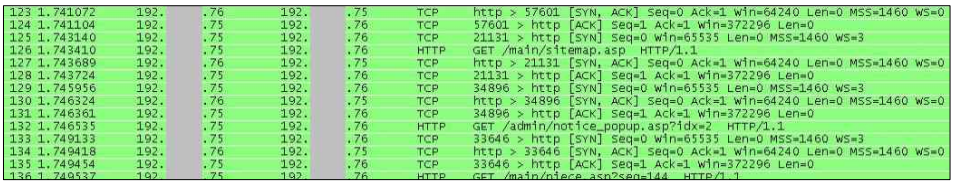


그림 9 HTTP Get Flooding 공격 예시

□ HTTP Transaction Flooding

○ 정상적인 세션을 맺은 뒤 랜덤한 HTTP 요청을 지속적으로 서버로 보냄으로써 서버의 처리용량을 고갈시키는 공격

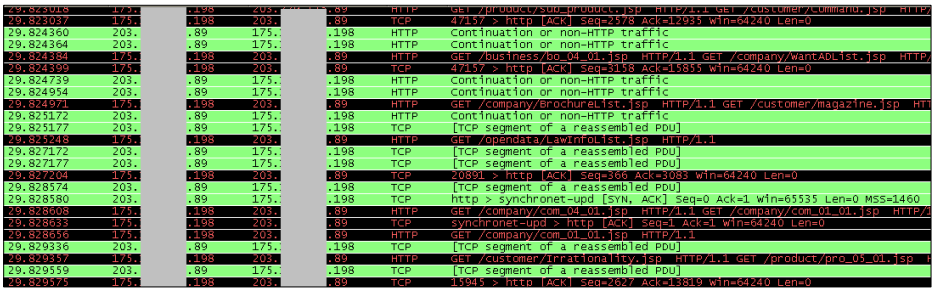


그림 10 HTTP Transaction Flooding 공격 예시

2. 탐지 및 대응 방안

□ 탐 지

○ 피해 서버의 CPU 과부하 상태를 확인하고 netstat 명령으로 TCP 세션 상태 확인(다수의 established 세션 존재)

○ 피해 서버 로그에 비정상적(존재하지 않는) URL로의 접근기록이 다수의 IP 주소로부터 다량 존재

○ 상태코드 414(Request-URL too long)로그가 다량 존재

○ 단시간에 동일한 IP 주소로부터 여러 건의 로그가 존재

○ CC Attack의 경우, 피해 서버의 로그에 'Cache Control : no-cache, no-store, must-revalidate, max-age=0' 값이 다수 존재하며, 패킷을 캡쳐해 봐도 동일 문구가 있음을 확인할수 있음

○ Slowloris Attack의 경우, 패킷을 캡쳐해 보면 HTTP 헤더의 끝이 /0d0a0d0a/로 끝나지 않음

□ 대응 방안

○ 서비스별 트래픽 대역폭을 제한하고, 사용하지 않는 서비스를 사전에 차단

○ 존재하지 않는 페이지나 상대적으로 많은 페이지 요청 등 IPS/IDS에서 비정상 행위 연결 차단

○ 공격의 진원지가 국외일 경우

- ISP/IDC 등과 협조하여 국제 GW에서 해외 트래픽 차단(NULL 라우팅)
- 라우터간의 Dynamic Routing을 통한 점진적인 트래픽 감소 유도

○ 공격의 진원지가 국내일 경우

- C&C 서버의 조정을 받고 있는 봇넷 PC에 의한 경우가 대부분
- 대외회사에서 공격 IP를 제공하여 봇넷 샘플 확보
- 샘플 분석을 통하여 C&C 서버와 봇넷 PC와의 통신 차단(대외회사 등 협조)
- 긴급한 보안 프로그램 업데이트 수행(보안업체 협조)
- 공격 소스 IP가 소수일 경우, ACL을 이용하여 차단

○ 서버 설정 변경(임시방안)

- KeepAlive를 off로 변경
- MaxClient를 최대수치로 조정

○ 패턴 차단 적용

- “cache-Control: no-store must-revalidate” 문자열 차단

○ Timeout 설정 변경

- httpd.conf 에서 Timeout 300을 5 이하로 변경

○ iptables의 connlimit(커넥션 제한) 설정

- *#iptables -A INPUT -p tcp --dport 80 -m connlimit --connlimit-above 30 -j DROP*

제4장 DDoS 예방 및 대응

최근 DDoS 공격은 봇넷을 이용해 다수의 좀비 PC에서 대량의 트래픽을 발생시켜 특정 사이트를 마비시키는 형태를 보인다. 어떤 기업이 도입한 DDoS 공격 대응 시스템의 처리 대역폭이 수Gbps 급이라 하더라도 대규모 봇넷을 이용하여 그 대역폭을 뛰어넘는 공격을 한다면 DDoS 공격 피해를 입을 수밖에 없다.

또한 DDoS 공격이 점점 정교화 되어 대응 시스템의 탐지 및 차단 방식을 우회하는 형태로 진화하고 있다. 그 예로 동일 IP에서 같은 웹 페이지에 대한 요청이 초당 5번 이상일 경우 탐지하는 룰이 있다고 가정했을 때, 동일 IP에서 5개의 다른 웹페이지에 대한 요청을 동시에 하게 만든다면 해당 공격을 탐지 못하고 웹서버가 다운 될 것이다.

이와 같이 보안장비를 통한 DDoS 공격 대응에는 분명히 한계점이 존재한다. 효과적인 대응과 신속한 복구를 위해서는 공격을 받은 회사, 관제 회사(업체), 망 제공 회사(업체)의 유기적인 협력이 필요하다. 이를 위해 비상시 연락체계, 역할 분담, 상황별 행동 양식이 수립되어 있어야 하며, 평상시 DDoS 공격을 대비한 준비에서부터 DDoS 공격 발생 시 대응 및 복구 방법 등이 포함 된 자체 DDoS 대응 매뉴얼이 필요하다. 또한 DDoS 공격 대응 훈련을 주기적으로 실시하여 취약 요소 파악 후 조치하여 사전에 대비 해두어야 한다.

본 장에서는 DDoS 공격을 예방 및 대응하기 위한 기술을 설명한다. 각 회사마다 네트워크 구성도, 보유 네트워크 및 보안장비, 서버 성능, 제공해야 하는 서비스 종류, 품질 등이 다르기 때문에 회사의 설정에 맞는 설정 값과 정책 등을 스스로 결정해야 한다.

제 1 절 예방 활동

1. 관리적 예방

□ ISP 협조

○ KT, LG U+, SK Broadband 등의 ISP 업체와 DDoS 대응 방안에 대한 협의

○ UDP/ICMP Flooding 공격과 해외에서의 공격 시 해당 IP차단 적용 요청(업체들의 특징에 맞게 긴밀한 협약이 필요함)

□ 내부 조직간의 협조

○ DDoS 대응을 위한 TFT(Task Force Team) 구성

○ 실제 상황 발생 전에 비상설 조직으로 TFT조직을 구성

○ TFT조직 구성원의 R&R을 명확히 하여 DDoS 공격 발생 시 신속히 대응 가능

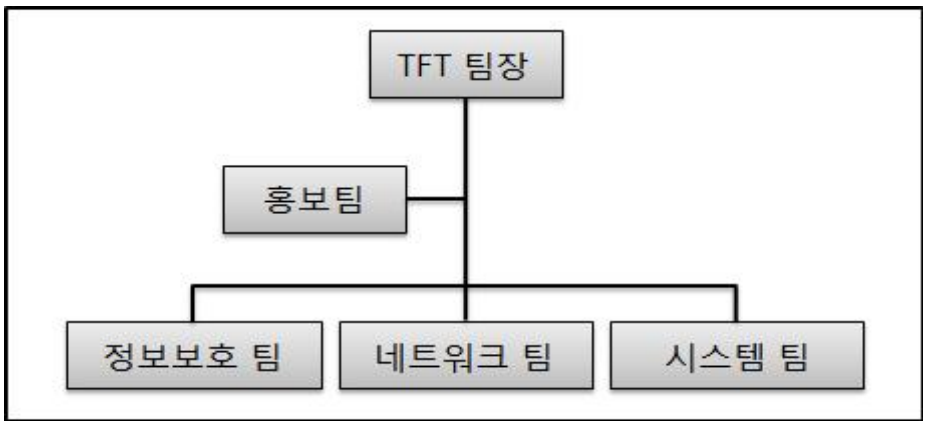


그림 11 DDoS 대응 TFT 예시

□ 업무 R&R 정의

구분	담당
TFT팀장	- DDoS 공격 발생시 운영반 총괄 - 피해범위 및 상황보고서 작성 - DDoS 공격 발생시 부문별 관제센터에 상황통보 및 상부 보고 - 평시 네트워크 및 서버 운영상황 파악 - DDoS 모의훈련 주관 및 예방정책 수립 - DDoS 공격 후 복구방안 수립 및 복구수행 책임
홍보팀	- 대외홍보 방안 마련 및 홍보 수행 - DDoS 공격 대응 TFT 운영 지원
정보보호팀	- 평시 네트워크 및 서버 운영상황 점검 - 정보자산에 대한 주기적 보안점검 및 보안강화 방안 수립·시행 - 이상 징후 발생여부 모니터링을 통한 공격여부 인지 - 네트워크/보안장비/서버담당과의 협조하에 긴급조치 수행 - 공격내용 분석 및 피해범위 파악을 통한 현황 보고 - 대응조치 수행 총괄 및 ISP 협조 - DDoS 공격 후 복구방안 수립 및 복구수행 실무 총괄
네트워크팀	- 평시 네트워크 트래픽 통계 및 예방책 마련 - 이상 징후 발생시 정보보호 실무책임자에 통보 - 보안장비/서버 담당 및 유지보수업체와 협력 - 네트워크 장비 상태 확인 후 긴급조치 수행 - DDoS 대응 절차에 따라 피해 최소화를 위한 대응 수행 - DDoS 공격 후 복구방안 수립 협조 및 복구수행
시스템팀	- 평시 서버 로그분석을 통한 설정 최적화 수행 - 이상 징후 발생시 정보보호 실무책임자에 통보 - 네트워크/보안장비 담당 및 유지보수업체와 협력 - 보안장비 상태 확인 후 긴급조치 수행 - DDoS 대응 절차에 따라 피해 최소화를 위한 대응 수행 - DDoS 공격 후 복구방안 수립 협조 및 복구수행

표 2 업무 R&R 정의

□ 비상연락망 유지

○ 신속한 대응조치 수행을 위해 비상연락망 구성 및 유지 필요

○ 분야별 담당자, 관련 회사, 유지보수 업체등 상시 운영반 및 비상시 운영반의 모든 담당자와 회사에 대한 연락망 구성

□ 유관기관 협조

○ 평시에 유관기관과 최신 동향 및 기술 관련 정보 공유

□ DDoS 공격 대응 모의훈련

○ DDoS 공격 대응 모의훈련의 정기적인 실시

○ 모의훈련을 통하여 DDoS 대응 절차와 업무협조체계, 비상연락망 등 점검

2. 기술적 예방

□ 네트워크 장비 설정

○ 네트워크 구성 점검

- DDoS 공격 발생을 가정하여 취약요소 판별 목적
- DDoS 공격 발생시, 취약요소 및 원인 파악을 위해 네트워크 구성 정보 필요
- 어떤 장비의 과부하로 인한 서비스 장애 발생인지 파악에 활용
- 장비에 유입되는 최대 트래픽은 장비에서 처리 할 수 있는 최대 처리량을 고려하였는지 확인에 활용
- 웹서비스 사용량이 많을 경우 웹 가속기 사용 검토

□ 라우터 및 스위치 설정

○ 라우터 혹은 스위치에서 제공하는 ACL을 이용하여 DDoS 공격 트래픽일 가능성이 큰 패킷 차단

○ ACL 변경 방법

- access-list list {PERMIT|DENY} protocol source source-mask destination destination-mask [operator operand] [ESTABLISHED]

- list : 패킷의 출발지 주소만을 보는 것이 아닌 ACL이므로 100-199까지의 정수 사용
- protoco l: ip, tcp, udp, icmp
- source, source-mask : 제한(혹은 허용)할 출발지 IP주소 네트워크 대역
- destination, destination-mask : 제한(혹은 허용)할 도착지 IP 주소 네트워크 대역
- operator : It(less than), gt(greater than), eq(equal), neq(not equal)
- operand : 목적지 포트 번호(10진수)

표 3 IP Spoofing 공격 차단을 위한 ACL 설정

○ 패킷 출발지 IP 주소 확인

- 출발지 주소가 라우팅이 불가능하거나 차단해도 서비스에 지장이 없는 IP 주소 대역인 경우 해당
- 출발지 주소가 사설 IP 주소인 경우 대부분이 spoofing 패킷이므로 전부 차단(RFC 191811), 사설 IP 주소에 대한 라우팅이 필요한 경우 사용하는 IP 주소만 허용하고 이외의 IP 주소에 대해서는 차단)

- Loopback 주소 영역, Broadcast 목적지 주소 영역, Test를 위해 할당된 영역 차단(RFC 333012)

○ IP 주소 Spoofing 공격 트래픽 차단 ACL 설정

- URPF(Unicast Reverse Path Forwarding) 기능을 사용함으로써 변조된 Source IP 주소를 가지고 접근하는 것을 차단
- Cisco의 경우 CEF(Cisco Express Forwarding)의 FIB tables(Forwarding Information Base)을 이용해서 Table에 없는 Source IP 주소가 유입 시 차단
- ACL(Access Control List)을 사용해서도 사설 네트워크 대역이나 Broadcast 주소를 차단함으로써 IP 주소 Spoofing 방지

- RFC 1918에 정의된 모든 사설 IP 주소 영역 차단
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any

- RFC 3330에 정의된 영역 중 일부
- LoopBack, Test-Net, Multicast 대역
access-list 102 deny ip 127.0.0.0 0.255.255.255 any
access-list 102 deny ip 192.0.2.0 0.0.0.255 any
access-list 102 deny ip 224.0.0.0 31.255.255.255 any

- RFC 2267 (edge 라우터에만 설정)
access-list 103 deny ip [회사 CIDR_BLOCKs] any
access-list 103 permit ip any any

표 3 IP Spoofing 공격 차단을 위한 ACL 설정

○ UDP, ICMP Flooding 트래픽 차단을 위한 ACL 설정

- UDP 패킷의 크기가 2M 이상이면 drop

access-list 104 remark CAR-UDP ACL

access-list 104 permit udp any any

- 해당 인터페이스 설정모드로 이동

rate-limit input access-group 104 2000000 25000 25000 confrom-action

transmit exceed-action drop

- ICMP 패킷의 크기가 256K 이상이면 drop

access-list 106 remark CAR-ICMP ACL

access-list 106 permit icmp any any echo

access-list 106 permit icmp any any echo-reply

- 해당 인터페이스 설정모드로 이동

rate-limit input access-group 106 256000 8000 8000 conform-action

transmit exceed-action drop

표 4 UDP, ICMP Flooding 공격 차단을 위한 ACL 설정

○ CAR(committed Access Rate) 설정

- 단위 시간 동안 일정량 이상의 패킷이 라우터로 들어올 경우, 일정량 이상의 패킷은 초과시키지 않도록 설정

○ 라우터에서 TCP SYN Attack 방지 설정

- Cisco 라우터는 DDoS 공격 중 SYN flooding 공격 또는 half-open 공격에 대한 방어 방법으로 TCP Intercept 기능 제공
- SYN flooding 공격 시 정당한 호스트와 공격 호스트를 구분하는

기술로서 클라이언트의 접속 요청인 SYN을 가로채어 라우터 운영 체제인 IOS가 프락시로서 응답을 하며 이에 상응하는 응답(ACK)으로 호스트의 정당성을 확인하는 기술

- 운영 모드는 Intercept와 Drop 두 종류가 있으며, Intercept는 다시 Intercept 모드와 Watch 모드로 나뉨

- Intercept/Intercept 모드는 디폴트 모드로서 클라이언트의 SYN 요청에 대해 IOS는 서버 대신 SYN/ACK을 보내고 ACK를 기다리다가 클라이언트로부터의 ACK 수신 시 IOS는 서버와 three way-hand shake를 진행하고 establish 완료 시 서버와 클라이언트를 연결

- Intercept/Watch 모드는 클라이언트의 SYN 요청을 가로채지 않고 establish 와료 시 까지 모니터링하다가 만약 클라이언트와 서버 간 establish 연결이 30초안에 설립되지 않으면 IOS는 서버쪽으로 RST을 보내고 state table에서 해당 연결 요청 제거

- Drop 모드는 DoS 공격을 받고 있는 상태에서 얼마간의 불완전 연결을 유지할 것인지를 정의하며, 디폴트로는 불완전 연결 수가 1100을 초과할 시 가장 먼저 시도된 연결을 state table에서 삭제

```
- 서비스 대역 지정
 access-list 107 permit tcp any services network or host
- Intercept Enable 설정
 ip tcp intercept list 107
- Intercept mode config [DoS half-open 방지설정]
 ip tcp intercept mode watch
 ip tcp intercept watch-timeout 5
- Intercept mode config [DDoS 공격 발생시]
 ip tcp intercept mode drop
```

표 5 라우터 TCP SYN Attack 방지 설정

□ 보안장비 설정

○ DDos 공격 대응 시스템 혹은 IPS

- 주기적인 패턴 업데이트

· 알려진 패턴추가 (Slowloris, CC-attack 등)

- 인계치 값 설정을 위한 서버 및 네트워크 성능 테스트 필요

- 상시 모니터링을 통한 통계 데이터를 축적하고, 이를 이용해서 서비스 품질 저하를 일으키지 않는 수준에서 임계치 설정

- 임계치 설정 시 고려사항

· 대역폭 관련 임계치는 Next Hop에 위치한 장비에서 처리할 수 있는 트래픽만을 전달 할 수 있도록 임계치를 설정해야 함

· 동시 세션 개수에 대한 임계치는 서비스별(서버별)로 설정 할 수 있어야 하고, 서버에서 처리할 수 있는 양을 기준으로 함

- 장비 최대 처리량 확인

· 보안장비의 최대 처리량은 대다수의 업체에서 정상 트래픽을 기준으로 이야기 함

· 보안장비의 경우, 서비스의 연속성을 보장하기 위해 유입 트래픽이 정책적용 가능한 트래픽을 초과하는 경우, 초과 트래픽에 대해 정책 적용하지 않고 다음 목적지로 포워딩하는 경우가 있음

· DDoS 공격 발생 시, 서버로 유입되는 공격 트래픽을 최소화 하기 위해 모든 유입 트래픽에 대해 정책 적용을 해야 함

· 회사 내 사용 보안장비마다 정책을 적용 할 수 있는 최대 처리량을 사전에 알고 있어야 함 (장비 업체, 유지보수 업체에 문의 필요)

- SYN Proxy 기능이 탑재되어 있는 경우 해당 기능 사용

· 사용자가 세션을 맺기 위해 SYN을 보내면 보안장비에서 SYN ACK로 응답하고 사용자는 ACK를 다시 보내 정상적인 세션을 이룰 때, 보안장비는 사용자를 SYN Proxy 테이블에

등록하여, 이후 해당 사용자의 통신이 확인 되는 방식 이용
· 접속처리 한계 초과 공격에 대한 대응 가능(사용자별 세션 관리)
- ISP와 DDoS 대응 전용장비는 모니터링이나 차단 등의 기능이 비슷하고 임계 설정 및 공격차단 패턴 등이 유사하나, DDoS 대응 전용장비의 경우 DDoS 공격 탐지만을 위한 다양한 패턴을 이용할 수 있으며 대용량 트래픽을 실시간으로 분석 가능
- 또한 많은 접속 사용자 및 대량의 트래픽이 발생하는 회사의 경우, ISP 만을 이용하는 것보다 DDoS 대응 전용장비를 도입함으로써 DDoS 공격 탐지 및 차단에 소요되는 부하를 분산 시킬 수 있음

○ 방화벽
- 서비스 연결에 필요한 포트를 제외한 모든 Inbound 트래픽 차단
- DMZ 운영 시 , 네트워크 대역이 아닌 서버별 허용 트래픽 설정
- 모니터링을 위해 서버별 통계자료를 확보할 수 있는 형태로 설정
- 장비 부하 및 서비스 품질을 고려하여 로그 정책 설정
- 스푸핑된 IP로 부터의 트래픽 유입을 차단하기 위해 방화벽에 '192.168.X,X, 10.10.X,X, 172.16.X.X'로 부터의 트래픽 차단 정책 적용 필요
- 대역폭 공격을 차단하기 위해 불필요한 UDP, ICMP 패킷 차단 정책 적용 필요

□ 서버 보안 설정

○ Windows 2000, 2003 서버 : 레지스트리 편집을 통한 설정

변수이름	설명	설정 값
SynAttack Protect	- SYN Flooding 공격에 대한 탐지 설정 - 0 : 탐지안함 1 : 탐지	1
TcpMaxConnect ResponseRetrans missions	- 클라이언트가 요청한 데이터를 재전송 하는 횟수를 제한하는 값	3
TcpMaXHalfOpen	- 허용할 Half Open 상태의 세션 수 - AFD에서 허용한 Backlog 보다 작은 값이어야 함	100
TcpMaXHalfOpen Retried	- 현재 Half Open 상태의 세션 수 (SYN 요청이 재전송된 세션 유지 개수) - TcpMaxHalfOpen 값보다 작아야 함	80
KeepAlive Time	- 연결 유지(Keep-alive) 패킷을 보내어 유휴 연결이 열려 있는지 확인하는 시간	300,000ms
EnableICMPRedirect	- ICMP Redirect 설정 가능 여부	0
PerformRouter Discovery	- RFC 1256 기반 router discovery 사용 여부	0
EnableSecurityFilters	- 1일 경우 IP 보안 필터가 활성화 됨	1
DisableIPSource Routing	- IP 원본 라우팅 가능 여부	1
MaxUserPort	- 사용 가능 최대 포트 수(세션 수)	65,534

표 6 윈도우즈 2000, 2003 서버 설정

○ Solaris : ndd 명령을 이용하여 설정

ex) /usr/sbin/ndd -set /dev/tcp_conn_req_max_q0 8192

변수이름	설명	설정 값
tcp_time_wait_interval	– 커넥션이 종료됐을 때 TIME_WAIT 상태로 머물게 되는 시간을 설정 (default: 240,000ms)	60,000
tcp_conn_req_max_q	– Complete Queue 개수(deafult: 128) tcp_conn_req_max_q()보다 작거나 같은 값	8,192
tcp_conn_req_max_q	– Incomplete Queue 개수(default: 1024)	8,192
tcp_ip_abort_cinterval	– Incomplete 상태의 TCP 연결 유지 시간, 시간 경과 후 큐에서 삭제 (default:180,000ms)	30,000ms
tcp_ip_abort_interval	– 데이터 송, 수신이 없는 상태에서 연결을 유지하는 시간(default: 480,000ms) ※ 메일 서비스 운영 시, 5분 이하로 값을 설정하면 오류 발생	60,000ms
tcp_keepalive_interval	– 서버 애플리케이션에서 KEEPALIVES가 설정되어 있고 응답하지 않은 연결이 계속 활성화된 경우 검사하는 간격	응용에 맞춰 설정
tcp-rexmit_interval_max	– 재전송을 위한 최대 시간 간격 (default:60,000ms)	10,000
tcp_rexmit_interval_min	– 재전송을 위한 최소 시간 간격 (default : 200ms)	200

표 7 Solaris 서버 설정

○ IBM AIX

/usr/sbin/no -o clean_partial_conns=1

○ HP-UX

 # ndd -set /dev/tcp tcp_ip_abort_cinterval 600000

 # ndd -set /dev/tcp tcp_conn_req_max_q0 2048

□ 웹서버 보안 설정

○ mod_dosevasive

- HTTP DoS 공격, DDoS 공격, brute-force 공격 등으로부터 아파치 웹서버를 보호하기 위한 도구
- 탐지는 IP 주소와 URL를 이용해 동적 해쉬 테이블을 생성하여 수행하고 다음과 같은 경우에 아이피별로 차단함
  · 초당 몇 번 이상의 같은 페이지를 요청하는 경우
  · 초당 같은 자식노드를 동시에 50번 이상 생성하는 경우
  · 일시적으로 차단되는 동안 요청을 생성하는 경우
- 설정값 (httpd.conf에 설정)

변수이름	설명	설정값
DOSHashTableSize	–각 자식 해쉬테이블 마다 탑레벨 노드의 수를 지정 –수치가 높으면 높을수록 좋은 성능이 나타나지만 테이블을 위한 메모리가 소모되며, 접속량이 많으면 이 수치를 높여야 함	3097
DOSPageCount	–같은 페이지(또는 URL)에 대한 요청 횟수 /page interval –지정된 값이 초과되면 클라이언트에 대한 IP 정보를 차단 리스트에 추가	2
DOSSiteCount	–동일 클라이언트로부터의 요청 횟수 / site interval –지정된 수 보다 초과될 경우 IP 정보를 차단 리스트에 추가	50
DOSPageInterval	–페이지 카운트 간격, 디폴트 1초	1
DOSSiteInterval	–사이트 카운트 간격, 디폴트 1초	1
DOSBlockingPeriod	–클라이언트가 차단 리스트에 추가되어 차단되는 시간	10

	–클라이언트는 403 (Forbidden) 에러를 출력하게 됨	
DOSEmailNotify	–IP가 차단될 때마다 지정된 이메일로 해당정보 발송	–
DDOSSystemCommand	–시스템은 IP가 차단될 때마다 해당 명령행 실행 *–예) "su –root –c '/sbin/iptables –A INPUT –s %s –j DROP"*	–
DOSWhitelist	–차단에서 제외할 호스트 IP 설정 *–예) DOSWhitelist 127.0.0.1, DOSWhitelist 127.0.0.****	–

표 8 mod_dosevasive 설정

○ mod_security

- mod_security는 아파치 웹서버 기반의 오픈소스 웹 방화벽으로 다음과 같은 특징을 가지고 있음
  · request 필터링
  · 우회 방지 기술
  · HTTP 프로토콜 인식
  · HTTP 필터링
  · POST 페이로드(payload) 분석
  · 감사로깅
- mod_security와 iptables를 이용하여 HTTP flooding 공격 완화 가능하며 룰에 다음의 내용 추가

```
- SecAction initcol:ip=%{REMOTE_ADDR}, nolog
  · 연결 정보의 초기화를 위해 initcol 변수를 사용하고, 같은 IP에서의 요청 횟수를 측적
```

- SecRule REQUEST_LINE"^GET(?:/|.+\.html|.+\.php|.+\.cgi|.+\.pl) HTTP"\"nolog,setvar:ip.ddos=+1,deprecatevar:ip.ddos=100/10" · HTTP 요청 중 'GET'요청에 대한 필터링을 적용하고, 루트 디렉터리("/")의 html,php,cg,pl파일만 필터링에 포함시킴
- "SecRule IP:DDOS "@gt 50" "log,exec:/path_to/modsec2ipt.pl" "SecRule IP:DDOS "@gt 25" "nolog,drop" · DDOS변수가 25보다 크면 drop(tcp reset)시키고 50이 넘으면 'modsec2ipt.pl'을 이용해 iptable의 #drop chain(packet drop)으로 해당 IP를 넘겨줌 · 'modsec2ipt.pl'은 modsecurity가 넘겨주는 "REMOTE_ADDR"을 iptables로 넘겨주는 동작을 하며, perl script로 되어 있음

표 9 mod_security 설정

□ 기타 DDoS 관련도구

○ SecRule mod_limitipconn

- 하나의 IP에서 동시에 접속하는 요청 수를 아파치 서버의 설정을 통해 제한하는 기능을 함으로써 DDoS 공격으로부터 피해를 완화할 수 있음
- 'MaxConnPerIP' 변수를 설정하여 접속 제한 가능

○ mod_antiloris

- 아파치 웹서버를 대상으로 하는 Slowloris 공격에 대한 방어를 목적으로 개발된 도구

□ Apatche 설정(httpd.conf)을 이용한 DDoS 대응

변수이름	설명
MaxKeepAlive Requests	- 클라이언트가 한번 요청으로 접속을 끊지 않고 연속으로 요청을 할 수 있도록 연결을 허용해주는 'KeepAlive' 요청 허용 횟수 - DDoS 징후가 발생하면 허용 횟수를 낮추는 것이 효과적
KeepAliveTimeout	- 클라이언트의 요청을 유지해야 하는 시간으로 Timeout 이내에 다음 요청이 없으면 연결을 끊어 버림 - DDoS 징후가 발생하면 Timeout 값을 낮추는 것이 효과적
MinSpareServers	- 아파치 서버가 안정적인 서비스를 위해 유지하려고 하는 최소 유휴 서버 개수 - DDoS 징후가 발생하면 해당 값을 높이는 것이 효과적(단, 서버의 성능을 고려하여 설정 필요)
MaxSpareServers	- 아파치 서버가 안정적인 서비스를 위해 유지하려고 하는 최대 유휴 서버 개수(즉, 너무 많을 경우 유휴 서버의 수를 죽임) - DDoS 징후가 발생하면 해당 값을 높이는 것이 효과적(단, 서버의 성능을 고려하여 설정 필요)
StartServers	- 아파치 웹서버를 처음 시작할 때 생성하는 서버 개수 - DDoS 징후가 발생하면 서버의 수를 높이는 것이 효과적
ThreadsPerChild	- 서버 하나가 만들어낼 수 있는 최대 쓰레드 개수(최대 64)
MaxClients	- 허용하는 최대 클라이언트 수 - MaxClients = StartServer * ThreadsPerchild - DDoS 징후가 발생하면 MaxClients 수를 높이는 것이 효과적
MaxRequestsPer Childs	- MaxRequestsPerChilds이 0으로 세팅되어 있다면 child process는 종료없이 계속 실행 - MaxRequestsPerChilds 값을 높이면 메모리 고갈로 인한 성능 저하를 막을 수 있고, 무한루프 등에 의한 서버 부하를 감소시킬 수 있음 - DDoS 징후가 발생하면 MaxRequestsPerChilds 값을 높이는 것이 효과적

표 10 httpd.conf 설정

□ ISP 협조

○ 네트워크 장비 보안설정

- 관문라우터는 평시 트래픽(시간별, 요일별 등)을 체크
- Fragment 패킷을 차단하도록 설정

○ 관문라우터, 백본스위치용 SYSLOG서버 구축

- 외부 SYSLOG 서버 지정하여 각종 시스템로그는 별도 서버에 저장
- DDoS 공격 발생 시 분석할 수 있는 raw 데이터 확보

□ 최신 공격 동향 분석

○ 공격패턴에 대한 최신 동향을 항시 분석

○ 위험도가 높은 공격의 경우 내·외부로 전파

○ 각종 교육 및 세미나 참석을 통한 사이버 공격 동향 파악

제 2 절 대응 업무

본 절에서는 DDoS 공격에 적절히 대응하기 위해서 DDoS 대응 매뉴얼 작성 시 필요한 대응 절차 및 요령에 대한 작성기준을 제시한다. 세부 수행 내용은 회사의 전산환경에 맞게 작성해야 한다.

1. DDoS 공격 대응 절차

□ 아래의 대응 절차를 따라 웹 서버 및 DDoS, IPS 장비 등을 통하여 공격유형을 분석한 후 서비스 영향 여부를 확인하여 상황에 맞는 대응을 하여야 한다.

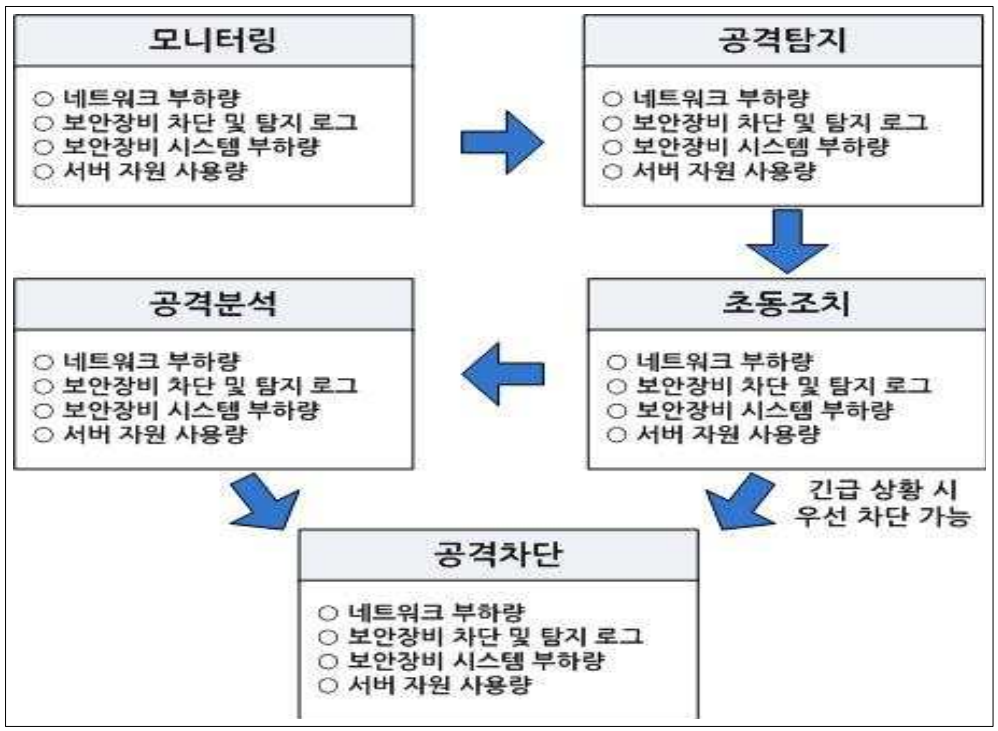


그림 12 DDoS 공격 대응 절차

○ 1단계(모니터링)

- 네트워크, 보안장비, 서버 담당자는 각각의 장비 부하량, 차단 및 탐지 로그, 사용량 등을 지속적으로 모니터링하고 장비 상태 점검을 수시로 수행
- 모든 장비는 가능한 최신 버전의 운영체제와 보안패치를 적용해야 하며, 최신 공격기법에 대한 차단 정책을 적용해야 함

○ 2단계(공격탐지)

- 장비별 모니터링 결과가 자체적으로 선정한 공격탐지 기준 초과 여부를 판단하고 담당자는 정보보호 실무책임자에게 통보
- 정보보호 실무책임자는 네트워크, 보안장비, 서버 담당자들과의 협의를 통해 공격 탐지 여부를 결정하고 정보보호책임자에게 통보

○ 3단계(초동조치)

- 상세분석을 수행하기 전에 간단한 대응조치 수행
- ISP, 유지보수 업체에 통보하고 협조 요청
- 부문별 관제센터, 상급회사 등 유관회사에 통보
- 네트워크 담당자는 해외 IP 및 스푸핑 된 IP 주소는 Null 라우팅 처리
- 보안장비 담당자는 트래픽 차단 임계치를 낮추고 상태 모니터링
- 서버 담당자는 자원 사용 임계치를 높이고 상태 모니터링

○ 4단계(공격분석)

- 장비의 상태를 확인하고 공격과 관련된 정보를 수집하여 공격기법, 사고원인 등을 분석
- 피해범위를 분석하고, 공격현황 보고서 작성
- 장비 설정 변경, 별도 대응 조치 등 차단조치 방안 수립

○ 5단계(공격차단)

- URL Redirection 등 별도 대응 조치 수행
- 분석 결과를 이용해 각 장비별 설정 변경 수행

2. DDoS 탐지기준

□ 아래와 같은 3가지 정도의 모니터링 방식을 통해 징후를 사전에 파악하고 빠른 분석을 통한 대응으로 큰 피해를 예방할 수 있다. 각 모니터링 방법에 따른 탐지기준을 각각 회사의 특징과 보유 장비의 특성에 따라 달리하여 효과적이고 효율적인 기준안을 만들어 사전 모니터링을 실시해야 할 것이다.

○ PPS(Packet per Second) 모니터링
- 트래픽 분석 시스템을 통해 PPS 모니터링을 실시하여 공격 징후 및 그에 따른 유형을 파악
- 모니터링 시, 평소 Baseline 대비 2배 이상의 많은 PPS가 10분 이상 지속될 경우를 공격징후로 파악하고 분석 시작

○ BPS(Bit per Second) 모니터링
- 트래픽 분석 시스템을 이용하여 bps 모니터링을 하는 것을 말하며 이 또한 공격 증후 및 유형을 파악하기 위해서 진행
- 만약 평소보다 트래픽 양이 증가하여 사용하고 있는 회선 대역폭의 2배 이상 사용될 경우 이상 징후로 파악하고 분석 시작

○ 서비스별 사용량
- 트래픽 분석 시스템을 이용하여 서비스별 bps, pps 등을 모니터링
- 특정 서비스의 사용량이 평소 사용량의 임계치 이상으로 10분 이상 지속될 경우 공격 징후로 파악하고 분석 시작

3. DDoS 공격 유형별 대응 절차

□ 아래 그림은 공격유형 별로 대응 절차를 도식화 한 것으로 공격 분석 후 해당 유형에 따라 그림과 같은 대응 절차를 수행 할 수 있다.

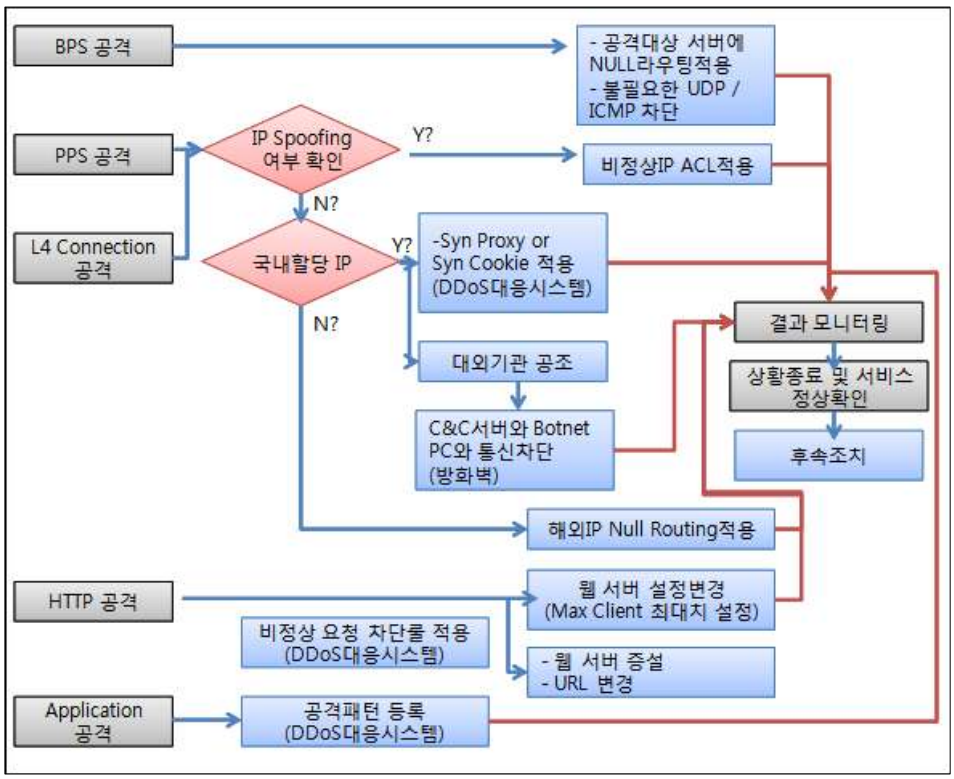


그림 13 공격 유형별 대응 절차

○ 정보 수집을 통한 세부분석

- 장비별 공격탐지 지표에 해당하는 정보를 수집하여 장비 간 상호연관성 및 피해내용 등을 고려하여 공격유형 식별
- 복수개의 공격유형이 동시에 발생할 수도 있으며, 기존에 알려지지 않은 DDoS 공격 기술 및 취약점을 이용한 공격이 발생할

수 있으므로 반드시 세부분석 수행 후 정확한 유형 파악 필요
- 장비 상태 확인 및 서버 운영 상태 점검을 통해 피해범위를 분석하여 차단조치 방안 수립에 활용

○ 공격유형별 차단조치 수행
- 공격유형이 식별되고 피해범위가 확인되면 효과적이고 신속한 대응을 위한 방안을 수립하여 차단조치 수행
- 공격 차단조치 수행 후, 모니터링을 통해 공격차단 성공여부를 확인하여 공격의 강도가 완화되고 소강상태에 접어들면 유관기관 통보 후 복구절차 수행
- 공격 차단조치 수행 후에도 피해가 지속될 경우 유관기관 협조 요청 후, 공격 탐지지표에 대한 세부분석을 반복적으로 수행하여 공격유형 식별 및 차단조치 방안 수립 필요

제 3 절 복구 업무

1. 복구 절차

□ DDoS 사고 발생 후 복구 과정은 아래와 같이 정해진 순서와 절차로 진행하는 것이 좋다. 먼저 피해복구 범위를 결정하고, 자산의 중요도에 따라 복구 우선순위를 결정해야 한다.

순서	절차	세부내용	
1	피해복구 범위결정	단순 데이터 복구	-시스템의 데이터에만 손상이 발생
		소프트웨어 복구	-시스템 내 프로그램 및 운영체제에 단순 오류 발생
		시스템 재설치	-시스템 운영체제 복구 불가능
2	복구우선 순위결정	-피해복구 대상시스템이 2개 이상인 경우, 이들 대상에 대한 복구 우선순위를 정함 -즉시 조치해야 할 복구 내용과 중장기적인 계획에 의해서 수행해야 할 복구 내용을 정함	
3	피해복구	단순 데이터 복구	-백업 데이터로 복구
		S/W 복구	-백신프로그램을 이용하여 치료 -공격에 이용된 취약점 제거 -응용프로그램 재 설치 -OS CD를 이용한 OS 복구
		시스템 재설치	-운영체제/응용프로그램 재 설치 -백업 자료를 이용한 데이터 복원 정상상태 복귀 확인
4	사후관리	-시스템 재개 후 일정기간 동안 모니터링 재개 -보완 보고서 작성 및 일정기간 동안 시스템 및 네트워크 주기적 재점검	

표 11 복구 절차

○ 피해복구 범위 및 우선순위 결정

- 피해현황 분석을 통해 피해 수준을 산정하여 피해복구 범위를 결정해야하며, 대부분의 장비와 서버가 항상 동작해야 되는 경우가 많으므로 복구범위와 우선순위 결정시 이를 고려해야 함
- 피해복구 범위는 위 복구절차 예시에서와 같이 복구 형태에 따라 단순데이터 복구, 소프트웨어 복구, 시스템 재설치등으로 구분하여 결정

○ 피해 복구 및 사후관리

- DDoS 공격으로 인해 데이터의 손실은 발생하지 않은 경우가 많으나 DB 서버 등 데이터 처리가 주된 장비에서는 데이터의 손실 및 훼손이 발생할 수 있으므로 평상시 주기적인 백업을 통해 공격 발생 이전의 상태로 데이터 복구 수행
- 웹서버 등에서 동작하는 응용프로그램의 경우 DDoS 공격으로 인해 정상적으로 동작하지 않으면 프로그램을 재설치 후 최신 보안패치와 서비스 팩을 적용하고, 복구 프로그램을 통해 공격 이전의 상태로 복원 수행
- DDoS 공격으로 인해 시스템에 심각한 오류가 발생하여 정상적으로 동작하지 않을 경우 운영체제 재설치, 응용프로그램 재설치, 데이터 복원 등 전반적인 시스템 재설치가 필요하며, 시스템 재설치가 완료된 후 정상 동작 여부를 확인해야 함
- 피해복구 수행 후 일정기간 동안 네트워크 장비, 보안장비, 서버 등에 대한 정상동작 여부 모니터링 수행
- 피해복구 내용 및 보안 강화 방안 등에 대한 보고서를 작성하고, 시스템 및 네트워크에 대한 주기적 재점검 필요

참고 문헌

[1] 금융보안연구원, DOS/DDOS 공격 대응 가이드, 2007

[2] 금융보안연구원, DDoS 공격 및 대응 실무, 2010

[3] 정부통합전산센터, DDoS 공격유형 및 보안장비별 대응방법, 2010

[4] 김인석, 김태호, 강형우, 이정호, 홍기석 공저, 전자금융 이러면 안전할까?, 2010

[5] Apache mod_evasive, http://www.zdziarski.com/blog/?page_id=442

이 절차서 작성을 위해 다음 분들께서 수고하셨습니다.

2010년 12월

총괄 책임자	금융보안연구원		
	사이버대응센터	센 터 장	성 재 모
참여 연구원	해킹대응팀	팀 장	이 성 욱
		주임연구원	박 찬 홍
		연 구 원	오 인 환
		연 구 원	홍 영 우
		연 구 원	사 준 호
외부 전문가	KT	과 장	장 현 철

DDoS 공격 대응 절차서

2010년 12월 발행

발행인 : 곽 창 규

발행처 : 금융보안연구원

서울시 영등포구 여의도동 36-1

키움파이낸스 스퀘어 빌딩 15층

Tel: (02) 6919-9136

<비 매 품 >