ETRI

2016
Electronics and
Telecommunications
Trends

은닉형 DDoS 공격 및 대응 기술동향

Advanced DDoS Attack & Corresponding Technical Trends

김정태 (J.T. Kim) 네트워크보안연구실 선임연구원
김익균 (I.K. Kim) 네트워크보안연구실 책임연구원
강구홍 (K.H. Kang) 서원대학교 정보통신공학과 교수

* 본 연구는 미래창조과학부가 지원한 2016년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음[다중소스 데이터의 Long-term history 분석기반 사이버 표적 공격 인지 및 추적 기술].

최근 지능화된 DDoS 공격 추세를 반영하여 DRDoS 및 HTTP GET flooding 공격을 네트워크 내 탐지 포인터에서 검출할 수 있는 방법을 살펴본다. DRDoS 공격은 해커들이 스푸핑 된 IP 주소를 사용하기 때문에 기본적으로 은닉형 공격자로 판단할 수 있다. HTTP GET flooding 공격은 해커의 제어 하에 실제적으로 IP 주소를 위장하여 공격을 시도하는 좀비 PC를 검출하는 것도 중요하지만 좀비 PC를 제어하는 C&C 서버로의 통신 채널을 탐지 및 차단하는 것과 C&C 서버에 접근하는 해커를 추적하는 것이 더 원론적인 방어전략이 될 수 있으며 관련 은닉형 DDoS 공격에 대한 국내외 기술개발 동향 및 대응 기술 추세에 대해서 살펴본다.

Ⅰ. 서론

분산 서비스거부(Distributed Denial-of-Service: DDoS) 공격은 네트워크 혹은 애플리케이션이 필요로 하는 각종 컴퓨팅 자원(CPU 혹은 메모리 등)을 고갈시킴으로써 일반 사용자들이 정상적으로 접근하지 못하도록 방해하는 공격이다. 오늘날 DDoS 공격은 과거 단순한 대용량 트래픽 볼륨 형태의 공격 패턴에서 탈피하여 일련의 지능화된 공격 시리즈로 발전을 거듭하고 있다. 특히 방화벽과 침입방지시스템(Intrusion Prevention System: IPS)과 같은 보안 인프라뿐만 아니라 일반 애플리케이션을 공격 대상으로 하는 미묘하고 발견하기 어려운 공격 패턴으로 변화하고 있다.

DDoS 공격에 따른 피해 수준은 매우 심각하며 수천 가지 이상의 다양한 방법으로 공격 벡터를 진행시킬 수 있다. 그러나 공격 벡터는 다음과 같은 세 가지 카테고리 중 하나로 매핑 가능하다.

- 볼륨 공격(Volumetric Attacks): 목표 네트워크/서비스 내 혹은 목표 네트워크/서비스와 인터넷 사이 대역폭을 고갈시키도록 공격하는 형태. 이러한 공격 유형은 단순하게 혼잡(congestion)을 발생시켜 일반 사용자의 트래픽 흐름을 지연시킨다.
- TCP 상태 고갈 공격 (TCP State Exhaustion Attacks): 로드 밸런싱 (load balancers), 방화벽 그리고 애플리케이션 서버와 같은 많은 인프라 요소에는 정상적인 기능 수행을 위해 연결상태(connection 혹은 session states)를 관리하게 된다. 해커들이 다량의 연결을 시도하여 연결을 관리하는 상태표(connection state table)를 고갈시키는 공격 형태로써 심지어 수백만 연결 상태를 유지하도록 제작된 대용량 보안 장비들조차도 이러한 공격에 동작이 멈추게 된다.
- 애플리케이션 계층 공격 (Application Layer Attacks): 애플리케이션이 혹은 계층 7 서비스를 겨냥하는 공격 형태로 이러한 공격은 적은 양의 트래픽을 만들어 내는 하나의 공격 장비를 이용해 가장 효과적으로 공격을 시도할 수 있다. 따라서 이러한 공격은 예측하거나 공격을 완화시키기도 가장 어렵다. 지난 3~4년 동안 가장 흔한 공격 유형이 되었으며 간단한 애플리케이션 계층 플러딩 공격(예, HTTP Get Flooding 공격 등)들이 여기에 해당된다.

한편, 최근 분산 Reflection DoS(이하, Distributed Refection Denial of Service(DRDoS)라고 약칭한다)라고 불리는 공격은 해커들의 제어하에 있는 공격 호스트에서 victim의 주소를 발신지 주소로 위장하여 여러 개의 서버에 위장된 요청을 전송한다. 이에 서버(reflector)들은 해당 응답 메시지를 victim 호스트로 반향(reflection)시켜 victim 호스트의 각종 프로세싱 및 대역폭 자원을 고갈시키는 것이다. 만약 이들 서버로부터의 응답 메시지가 공격 호스트가 전송하는 요청 메시지보다 엄청 큰 크기의 패킷을 만들어내면 이것을 증폭 공격(amplification attack)이라고 부른다. 최근 연구결과를 보면 적어도 14개의 UDP 기반 프로토콜들이 이러한 공격에 취약한 것으로 보고되고 있다. 이러한 공격은 수백 Gbps 이상의 트래픽을 만들어 내는 것으로 보고된다. 지난 수년간 많은 연구가 DRDoS 공격을 받는 victims 자체를 방어하기 위해 많은 기법을 제안하고 있으나, 상대적으로 공격에 사용되는 실제적인 서비스(reflector)에 대한 관심은 부족하다. 그러나 증폭 네트워크(reflector가 존재하는 네트워크)의 경계에서 증폭 공격을 검출하는 것은 정상적인 요청과 악의적인 요청을 구별해 내기가 쉽지 않기 때문에 여러 가지 어려움이 있다.

2013년과 2014년 초반까지 Domain Name System (DNS) 증폭을 이용한 공격은 DDoS 공격의 최대 트래픽 양의 34.9%를 차지했고 전체 네트워크 DDoS 공격의 18.6%에 달했다[1]. 일례로 2013년 3월 중순 Spamhaus

를 대상으로 high-profile 공격을 감행한 DNS 증폭 공격은 300Gbps 이상의 트래픽 양을 발생시켰다. DNS 증폭 공격은 다음과 같은 이유로 인해 해커들에게 매우 선호되고 있다. ① 해커들은 증폭의 효과를 이용하여 victim에게 엄청난 양의 트래픽을 만들어 낼 수 있다. ② IP 주소 spoofing과 reflection을 이용하여 보안 장비로부터 자신을 숨길 수 있다. ③ victim 들은 정상적인 DNS 서비스를 방해하지 않으면서 이들 reflecting DNS 서버들의 IP 주소를 차단할 방법이 없다. DNS 서버로부터 reflected되어 돌아온 엄청난 양의 응답 메시지가 victim 컴퓨터에 수신되면 victim은 수신 패킷을 해석하여 자신이 보낸 DNS 요청 메시지에 대한 응답이 아니라는 사실을 확인 후 해당 패킷을 폐기하기 된다. 그러나 해커는 이미 victim의 네트워크와 호스트의 자원을 희생시킴으로써 공격에 성공한 것이 된다. 그뿐만 아니라, 최근 Network Time Protocol(NTP) 증폭을 이용한 공격들은 하나의 victim을 대상으로 400Gbps의 대량 트래픽을 유발하는 것으로 조사되었다. NTP 공격에서는 공격자들은 가용한 NTP 서버들을 찾아내고 victim의 IP 주소를 스푸핑하여 이들 서버들을 이용한 최근 600개 클라이언트 리스트를 요구하는 질의 패킷을 전송한다. 결과적으로 엄청난 양의 트래픽이 victim 호스트로 유입되게 된다.

본 논문에서는 이와 같은 최근 은닉형 DDoS 공격 추세를 반영하여 DRDoS 및 HTTP GET flooding 공격을 네트워크 내 탐지 포인터에서 검출할 수 있는 기술들의 동향을 살펴본다.

II. 국내외 기술동향

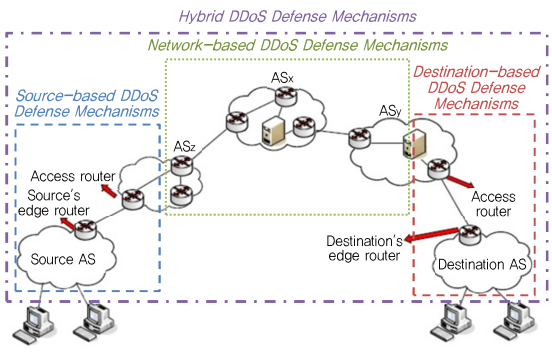
1. 국외 기술개발 현황

DDoS 방어 체계를 분류하는 방법은 크게 두 가지가 있다. 먼저, 방어 메커니즘을 설치하는 위치에 (deployment location) 초점을 맞춘다. 두 번째, DDoS 방어 체계가 언제 반응하느냐 하는 것이다. 즉 공격 전(before the attack-attack prevention), 공격 중(during the attack-attack detection), 그리고 공격 후(after the attack-attack source identification and response)로 분류된다. DNS 증폭 공격은 잘 알려진 반면 효과적인 방어 수단이 없는 것이 문제이다. 미국 컴퓨터 위기 대응팀(United States Computer Emergency Response Team: US-CERT)은 2013년 7월 게시판을 통해 다음과 같은 몇 가지 대응 매뉴얼을 제시하였다[2].

1) Open DNS resolvers 수 제한
2) Authoritative DNS 서버에 public recursion 기능 차단
3) Rate Limit 응답 구현
4) IP 스푸핑을 차단

그러나 이러한 권고를 따르는 조직들에게는 별다른 혜택이 있는 것은 아니다. 일례로, IP 스푸핑을 차단해 달라는 요구가 지난 10년 지속되어 왔지만 아직도 25% 이상의 Autonomous Systems 들이 (그림 1)과 같이 이를 따르지 않고 기관별 공격 대응에 어려움이 존재한다.

Smurf 공격과 같은 전통적인 reflection 공격들은 공격 대상 victim의 주소를 발신지 IP 주소로 위장한다. 공격자는 reflector라고 불리는 제3의 시스템으로 이처



(그림 1) DDoS 방어 시스템 구현

〈출처〉: 한국인터넷진흥원, "2012년 무선인터넷이용실태조사," 2012. 12.

럼 스푸핑된 패킷을 보내면 reflector는 해당 victim으로 정상적인 응답을 보내게 된다.

만약 대량의 공격 패킷들이 reflectors 들로 전송되거나 reflector가 브로드캐스팅 네트워크 주소가 되면 해당 victim은 트래픽 폭주로 인해 마비될 것이다. 이러한 공격의 방어 수단으로서 다음과 같은 다섯 가지를 고려해 볼 수 있다.

1) victim에서 reflected 공격 트래픽을 차단
2) 발신지 주소 스푸핑을 방지
3) reflector에서 스푸핑된 패킷을 검출하고 차단
4) reflector를 통한 발신지의 역추적
5) 감염된 시스템으로부터 공격 트래픽을 검출

이상의 다섯 가지 방어 전략 중에서 첫 번째를 제외하면 모두 제3의 기관이 공격 트래픽을 검출하고 차단하는 것을 요구하고 있다.

2. 국내 기술개발 현황

국내 기업들이 DDoS 전용 방어 장비를 잇따라 개발하는 등 내수 시장에 본격 참여하면서 상대적으로 가격 경쟁에 밀리는 외산 업체의 영향력이 점차 줄어들기 시작하고 있다. 2008년 초만 해도 DDoS 공격 위협에 대응하는 국산 장비들이 부족하여 시스코, 라드웨어, 인트루가드, 그리고 리오레이 등 외산 제품이 시장을 주도했다. 업계에 따르면 7/7 DDoS 사태 이후 공공기관에서 DDoS 장비 구축 사업이 잇따라 진행되는 가운데 국내 DDoS 장비 업체들이 선전하고 있다. 국내 기업들이 외국 업체 대비 저렴한 가격에 국산 제품을 내 놓은데다 공공기관 납품 시 필수요건이 CC 인증을 한발 앞서 획득했기 때문이다. 이에 따라 공공기관을 중심으로 한 DDoS 공격 전용 대응장비 시장은 국내 기업 위주로 시장이 재편될 것으로 전망된다. 민간 시장 역시 국내 고객에 맞춘 서비스 등을 앞세워 국내 기업들이 두각을 나타낼 전망이다.

나우콤, 컴트루테트놀러지, 시큐아이닷컴, LG CNS 등 국내 기업이 DDoS 공격 대응장비 시장에서 눈에 띄는 성적을 보이고 있다. 2009년 200억원 규모의 DDoS 방어체계를 구축한 행정안전부 프로젝트 역시 LG CNS 그리고 시큐아이닷컴 등 국내 기업이 휩쓸었다. 경찰청 수주에 라드웨어 제품이 낙점됐지만 실제 구축으로 이어지지 못하고 시큐아이닷컴 제품으로 대체하는 등 공공기관에서 국산 제품이 더 좋은 성적표를 받고 있다(DDoS 공격 대응 장비 국내 시장 현황)[3]. 이와 같은 국내 업체의 활발한 개발 현황에도 불구하고 현재 국내 DDoS 보안 시장에서 기업과 정부에서 사용하고 있는 DDoS 대응 장비의 성능이 뒷받침되지 않고 있어 공격 시 많은 양의 트래픽으로 보안 장비 자체가 다운되는 현상과 DDoS 대피소를 추가적으로 구성하는 등의 추가 자원 소모를 방지하기 위해서 DDoS 대응장비의 원천적인 구현의 변화가 필요한 실정이다.

Ⅲ. DRDoS 공격 및 대응방법

1999년 AusCERT는 스푸핑된 IP 주소로 엄청난 양의 데이터를 전송하는 DNS 서버를 이용하는 증폭공격을 경고하였다. 오늘날 DNS는 60 바이트의 요청 메시지를 이용해 쉽게 512 바이트의 응답을 만들어 낼 수 있기 때문에 증폭공격으로 늘리 사용되고 있다. 더욱이 Extension mechanisms for DNS(EDNS)을 지원하는 DNS 서버들은 요청 메시지 보다 거의 100배 큰 응답 메시지를 만들어 낼 수 있다. 자신의 도메인 외부로부터 요청에 대한 응답을 할 수 있도록 설정된 public DNS 서버를 open DNS resolvers라고 부른다. Open DNS Resolver Project에 의하면 인터넷상에 2천 5백만개 정도 존재하는 것으로 보고된다. 따라서 이들 open DNS 서버들을 해커들은 주로 사용하게 된다.

증폭공격은 DNS 서비스 이외에 과거 ICMP 요청을

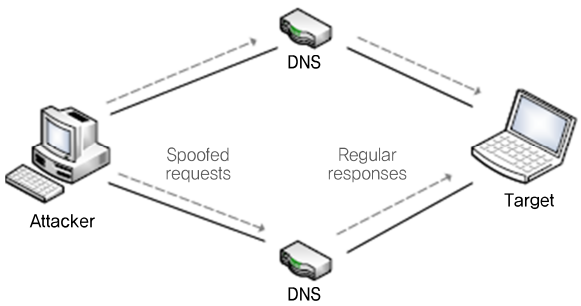
이용한 Smurf 공격[4]과 일반 호스트를 reflector로 이용하는 Fraggle 공격[5]등이 있었다. 2014년 US-CERT는 SSDP를 활용한 공격을 경고하고 있으며 하나의 공격으로 54Gbps 트래픽을 발생하는 것으로 보고되고 있다[6]. 이외에도 Simple Network Management Protocol (SNMP) 기본 공격과 NTP 서버를 이용한 증폭공격도 보고되고 있다.

1. DNS Reflection 공격 동향

Domain Name System(DNS)는 example.com과 같은 도메인 이름을 IP 주소로 변환해 주는 인터넷 서비스이다. 따라서 대부분 인터넷 사용자들은 매일 인터넷 사용을 위해 이들 서비스를 제공하는 DNS 서버에 의존한다. 오늘날 세계적으로 수백만 개 이상의 DNS 서버가 운영되고 있다고 보고된다. 그러나 이러한 정상적인 서비스를 이용하여 해커들은 타겟 네트워크 혹은 호스트들을 공격하는 양상이 해가 갈수록 증가하고 있는 추세다. 본 절에서는 이들 공격에 대해 알아보고 이러한 공격에 대처하고 있는 기존 방어 기법을 소개한다.

다음 (그림 2)는 정상적인 DNS 서비스를 이용한 reflection 공격의 예를 보여준다. 그림에서 보듯이 공격자(Attacker)는 타겟(공격지) 호스트의 IP 주소를 스푸핑하여 DNS 질의 패킷을 DNS 서버로 보내면 서버는 DNS 응답 메시지를 작성해 타겟 호스트로 보내게 된다.

(그림 2)에서 공격자는 자신의 컴퓨터를 이용해 직접 공격하기 보다는 사전에 좀비 컴퓨터들을 만들어 이를



(그림 2) DNS reflection 공격 시나리오[7]

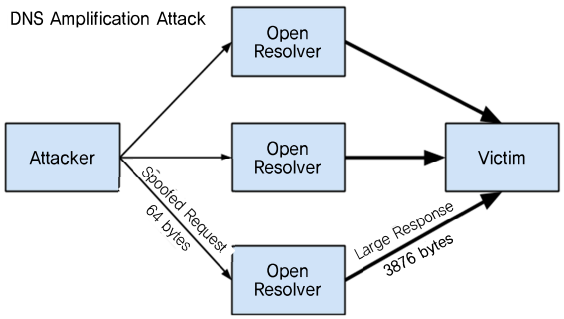
통해 공격하는 것이 일반적이다. 따라서 엄청난 수의 좀비 컴퓨터들이 DNS reflection 공격을 동시에 수행하게 되면 타겟 네트워크 혹은 호스트는 정상적인 서비스가 불가능한 상태에 이르게 되며, 이를 분산 DNS reflection (Distributed reflection Denial of Service: DRDoS) 공격이라고 말한다. 이들 좀비 컴퓨터들은 다음과 같은 특징을 갖는 트래픽을 발생시킨다.

- 무작위 발신지 포트번호를 이용해 여러 개의 DNS 서버 (목적지 포트 UDP 53번)로 DNS 요청 패킷을 발생시킨다.
- 일정하게 작은 크기의 DNS 요청 패킷은 큰 응답(MTU의 최대 크기인 1,500 바이트)을 유발하도록 한다(증폭 공격: Amplification Attack).
- 이들 DNS 서버로부터 DNS 응답 패킷들은 하나의 호스트로 향하게 한다.

한편, 이들 공격 트래픽은 다음과 같이 변형될 수 있다. 이와 같이 변형된 형태의 트래픽을 발생시키는 것은 DRDoS 검출 회피하기 위해 공격자들이 취할 수 있는 행위로 볼 수 있다.

- 작은 DNS 응답 패킷을 유발하도록 한다(증폭 공격 검출 회피용).
- 다양한 크기의 DNS 요청 패킷을 발생한다. 이러한 요청 패킷에 의해 해당 응답 패킷의 크기는 다양해질 수 있다.
- 공격에 사용될 DNS 서버 개수를 변화시킬 수 있다.

다음 (그림 3)은 DNS amplification 공격 형태를 보여준다. 위장된 IP 주소를 사용해 공격자가 보내는 ANY requests는 Open Resolver에게 현재 도메인에 대해 알고 있는 모든 정보를 요구한다. 이 정보에는 MX records



(그림 3) DNS Amplification 공격 시나리오

〈출처〉: https://blog.opendns.com/2014/03/17/dns-amplification-attacks/

(mail exchanger 메일 서버), IP 주소 등도 포함한다. 따라서 공격자들은 타겟으로 보내질 응답 패킷의 크기를 최대화시키기 위해 이런 타입의 질의를 사용하게 된다. (그림 3)에서 보는 바와 같이 64 바이트 request가 3,876 바이트 크기로 타겟 호스트로 응답된다.

이상과 같은 DRDoS 공격은 DNS 서비스뿐만 아니라 NTP(Network Time Protocol, UDP 포트번호 123)서비스와 같은 형태에서도 동일하게 발생되며 공격의 형태는 DNS 서비스를 이용하는 공격과 매우 유사한다. 즉 (그림 3)과 동일한 방법을 사용하여 공개적으로 가용한 NTP 서버들을 사용해 엄청난 양의 UDP 트래픽을 네트워크에 가할 수 있다. NTP amplification 공격은 해커들이 NTP 서버의 monlist(MON_GETLIST 명령어: 최근 해당 NTP 서버와 통신한 600개 호스트들의 IP 주소를 응답) 특징으로 알려진 방법을 사용한다. 이와 같은 증폭된 응답들은 정상적인 서버로부터 합법적인 데이터임으로 이러한 공격 유형을 막기란 쉽지 않다. US-CERT에서는 이러한 공격을 감소시키기 위해, monlist 기능을 제거하거나 NTP 버전 4.2.7(monlist 제거)로 업그레이드할 것을 권고한다.

2. DNS reflection 방어 동향

- 방화벽: 대부분 이미 방화벽을 설치하고 있으며 특정 패킷 혹은 IP 주소들을 손쉽게 차단할 수 있게 설정할 수 있다. 대부분의 환경들이 이러한 queries에 응답하지 않기 때문에 큰 피해를 발생시키지 않을 수 있다. 이러한 접근의 가장 큰 문제점은 false positives를 발생시키며 따라서 정상적인 트래픽도 차단해 버린다. 또 다른 문제점은 공격자들이 RRSIG, DNSKEY 등과 같은 큰 증폭을 야기시키는 다른 DNS queries로 쉽게 변경할 수 있다는 것이다. 만약 공격이 더 교활해지면 다른 방어 메커니즘이 필요하다.
- BCP 38: 증폭공격은 위장된 IP 주소에 의존하는 DDoS 공격의 한 형태이다. 즉 공격자가 IP 주소 위조가 없이는 DNS 서버가 victim으로 트래픽을 가할 수 없다. 한편 위장된 주소는 공격자를 역추적하는 것을 어렵게 만든다. BCP38은 라우터로 하여금 정상적인 IP 주소를 검사하도록 하는 메커니즘이다. 각 사용자들은 Internet Service Provider(ISP)로부터 IP 주소를 할당 받기 때문에 ISP는 수신된 패킷 들이 정상적인 IP 주소를 가졌는지 조사할 수 있다. 만약 IP 주소가 사용자가 가질 수 있는 범위와 매치되지 않는다면 해당 트래픽을 폐기한다. 이러한 메커니즘은 BCP38이 구현된 위치에서 사용자 혹은 ISP의 범위 밖의 위장된 IP 주소를 막게 된다. 만약 BCP38이 주요 ISP의 전반적인 인터넷에 구현되어 있다면 IP 주소가 위장되는 것을 막을 수 있을 것이다.
- DNS Dampening : BGP route flap dampening을 기초로 한다. DNS dampening의 기본 아이디어는 query 타입, 응답 크기, 그리고 다른 파라미터들을 기준으로 requester 당 penalty points를 수집한다. 만약 penalty points가 설정값을 넘어서면 dampening이 시작된다. Dampening 상태에서 서버는 위장된 IP 주소로부터 오는 모든 queries를 폐기한다. Penalty points가 시간이 지남에 따라 지수적으로 감소하게 된다. Penalty

points가 secondary limit아래로 떨어지면 dampening을 중지하고 서버는 다시 requests를 처리하게 된다. 예를 들어, ANY request는 100점을 부여한다.

이것은 이러한 query 들이 흔히 공격에 사용되며 정상적인 사용자들에 의해서는 거의 사용되지 않기 때문이다. 이러한 query가 동일한 query ID 를 가지고 반복되면 다시 100점의 penalty points를 합하게 된다. 정상적인 requests들은 무작위로 query ID를 선택하기 때문이다. 중복된 query ID는 공격 시 일반적으로 나타난다.

추가적으로, penalty points는 응답 크기에 따라 부여된다. 이러한 접근법의 문제점은 false positives를 해결할 수 있는 메커니즘을 제공하지 못하는 것이다. 즉 정상적인 사용자가 DNS를 전혀 사용할 수 없게 차단시킨다.

- RRL: Response Rate Limiting은 DNS 서버로부터 회신되는 응답(response) 양을 제한하는 메커니즘이다. 이것은 설정된 rate limit를 넘어서는 responses를 폐기시킴으로써 DNS 증폭공격의 효과를 제한하게 된다. Rate limiting은 다음과 같이 동작한다.
  - 서버가 DNS query에 대한 response를 만들 때 requesters의 IP 주소를 buckets으로 그룹화한다. 기본적으로 동일한 24 서브넷을 가진 IPv4 주소는 하나의 bucket에 저장된다. 56 IPv6 주소들은 동일하게 count 한다.
  - Wild-card, zonename 혹은 query name은 IP 주소와 Boolean error indicator (response code: REFUSED, FORMERR 혹은 SERVFAIL)와 함께 저장된다.
  - 서버는 하나의 request에 어떻게 응답하는지 결정하기 위해 〈IP, NAME, error-status〉를 사용한다.
  - Unique response의 양이 설정된 limit를 초과하면 서버는 특정 IP 혹은 network에 대한 request를 폐기한다. 서버는 requesters에게 TCP를 사용하도록 시도할 수 있다.
  - 서버는 주어진 responses를 조사하기 때문에 수신되는 requests의 양을 무시할 수 있다.

RRL을 사용하면 victim은 공격을 받고 있다는 사실을 알 수 있다. 이것은 제한된 시간 동안 request를 보내지 않는데 DNS responses를 받기 때문이다. 공격자는 DNS 서버들이 RRL limits 내에 머물러 있도록 여러 개의 서버로 공격을 분산시킴으로써 이러한 방어 메커니즘을 회피할 수 있다.

Flow FingerPrint: Huistra[7]는 NetFlow 데이터에서 reflection DDoS 공격이 어떻게 나타나는지 조사하였다. 하나의 호스트가 DNS 서버로 요청을 보낼 때 각각의 요청은 무작위 포트번호를 사용한다. 따라서 하나의 패킷으로 구성된 flow-records를 만들어 낸다. DNS reflection DDoS 공격 검출을 위해 다음과 같은 정보가 가용하다.

- DNS 요청을 보내는 호스트의 IP 주소
- DNS 서버 IP 주소
- DNS 요청 및 응답 시간
- DNS 요청 및 응답 크기 (패킷/바이트 수)
- DNS 요청 발신지/목적지 포트 번호)

증폭을 시도하는 DNS reflection DDoS 공격의 기본적인 예는 다음과 같다.

- 무작위 포트 번호를 사용하는 하나의 호스트로부터 여러 DNS 서버 53번 포트 번호로 향하는 DNS 요청 패킷을 설명하는 많은 수의 flow-records
- 큰 응답을 유발하는 작은 크기의 요청 패킷

- 53번 포트 번호를 사용하여 여러 DNS 서버로부터 하나의 호스트로 향하는 DNS 응답을 나타내는 여러 flow-records
- 이러한 응답 패킷 중 MTU 1500 바이트에 가까운 크기

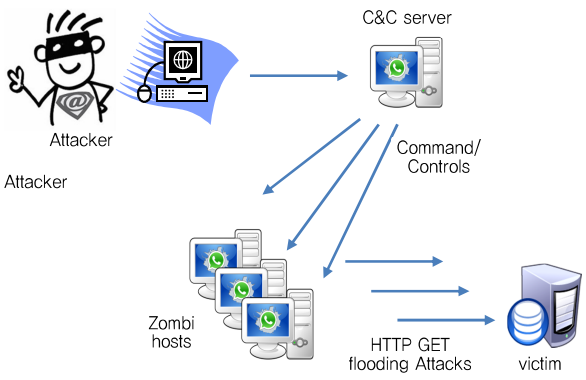
그러나 모든 reflection 공격들이 이와 비슷한 flow-records를 만드는 것은 아니다. 즉 해커들의 변형된 행위에 따라 다른 NetFlow 데이터가 수집될 것이다.

Ⅳ. HTTP Get Flooding 공격 및 대응방법

1. HTTP Get Flooding 공격 동향

HTTP Get Flooding 공격은 웹서버 응용계층을 겨냥한 서비스거부 공격 형태 중 가장 효과적인 방법으로 악용되고 있다[8][9]. 이러한 공격은 (그림 4)와 같이 컴퓨터 바이러스에 감염된 컴퓨터 혹은 C&C(Command and Control) 서버의 제어하에 있는 봇(Bot)에 의해 대량의 HTTP-GET 요청 정보를 목표 웹서버로 전송하여 해당 서버의 프로세싱 자원을 고갈시켜 더이상 정상적인 사용자의 요청을 처리하지 못하도록 서비스 불능 상태에 빠뜨린다.

이러한 공격 패킷은 정상적인 HTTP 패이로드를 유지하기 때문에 해당 서버가 정상적인 사용자들이 요청



(그림 4) HTTP GET flooding 공격의 연결도

하는 HTTP-GET 요청 메시지와 이들 악의적인 요청을 쉽게 구분할 수 없다. 응용계층을 겨냥한 이러한 공격은 다음과 같이 세 가지 클래스로 구분할 수 있다[10].

1) Request Flooding 공격: 각 공격 세션은 정상적인 세션과 비교해 대량의 request rate를 만들어 낸다.
2) Asymmetric Workload 공격: 각 공격 세션들은 서버의 자원 사용 부하를 증가시킬 수 있는 형태를 보이는 request 비율을 높인다. 예를 들어 데이터베이스 엑세스를 유발시키는 형태의 request 비율을 증가시키는 것이다. 이러한 형태는 단순한 Request Flooding 공격보다 request rate를 낮추어 공격할 수 있어 해커 입장에서는 보다 효과적이다.
3) Request One-Shot 공격: Asymmetric workload 공격의 변형된 형태로 하나의 세션을 통해 여러 개의 requests를 보내는 대신 하나의 세션에 하나의 고부하 유발 request를 보내는 것을 특징으로 한다. 따라서 이러한 공격은 threshold 기반의 DoS 방어시스템을 쉽게 회피할 수 있으며 request를 전송 후 세션을 종료하여도 해당 서버의 성능에 피해를 줄 수 있게 된다.

앞에서 설명한 바와 같이, HTTP-GET flooding 공격은 정상적인 HTTP 프로토콜을 사용하기 때문에 일반적인 공격 시그너처를 기준으로 설계된 침입탐지시스템(Intrusion Detection System: IDS)으로 검출해 내기가 쉽지 않다. 따라서 웹서버가 정상적으로 웹 서비스를 지원할 수 있는 최대 트래픽 양을 설정해 놓고 이를 초과하면 입력 요청 메시지를 차단하는 방법을 채택하고 있다. 그러나 이러한 단순한 방법은 정상적인 트래픽도 차단하는 문제점을 가지고 있다. 최근 이러한 문제점을 극복하기 위한 다양한 검출 방법들이 제안되고 있다.

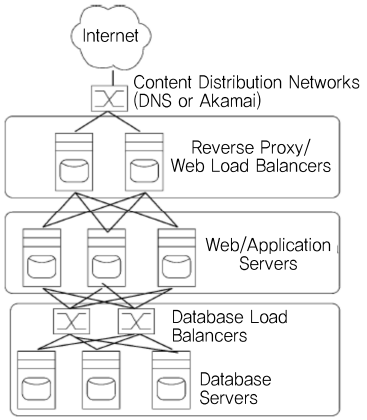
2. HTTP Get Flooding 방어 동향

HTTP/1.1 세션들은 persistent 연결을 지원한다. 따라서 하나의 클라이언트는 request 마다 새로운 TCP 연결을 열지 않고서 web-cluster로 요청을 보내고 응답을 받을 수 있다. 결과적으로 하나의 정상적인 HTTP/1.1 세션은 세션이 유지되는 동안 여러 개의 requests로 구성된다. Requests들은 클라이언트가 하나의 request를 보내고 다음 request를 전송하기 전 해당 응답을 기다리는 closed loop 형태를 갖거나 응답을 기다리지 않고 여러 request를 전송하는 pipelined 형태를 취할 수 있다. 하나의 페이지는 텍스트 콘텐츠를 위한 하나의 main request와 main 페이지에 포함된 image-files를 위한 여러 개의 embedded requests를 통해 가져온다. Main request는 일반적으로 dynamic하여 데이터베이스와 처리와 같은 프로세싱을 포함하지만, embedded requests들은 단순히 web-cluster tier 프로세싱을 처리하는 static 한 행태를 취한다.

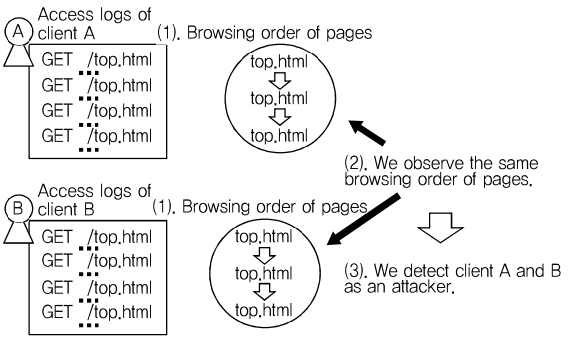
정상 사용자들의 DNS 질의 및 응답 패턴을 분석하는 것은 매우 중요한 정보이다. 이들 사용자 baseline 모델을 기반으로 공격 패턴에 대한 기준 값들을 설정할 수 있다. 따라서, 정상 사용자들의 트래픽 특징의 분석이 중요하다. 정상적인 하나의 클라이언트 요청은 다음과 같이 처리된다.

Request가 수신되면, reverse proxy server는 요청 URL을 파싱하고 로드 밸런싱 정책에 따라 하나의 웹 서버로 요청을 전달한다. 만약 request가 정적 웹 페이지 혹은 이미지 파일을 위한 것이면 해당 서버는 요청 페이지를 서비스한다. 이러한 요청들은 여러 개의 데이터베이스 query로 구성되고 이들 결과는 응답 페이지를 만들기 위해 합성된다.

(그림 5)는 Ranjan et al.[10]이 사용한 대표적인 victim 시스템 모델을 보여준다. 세션 inter-arrival time, request inter-arrival time 혹은 세션 workload-



(그림 5) Victim 모델링[10]

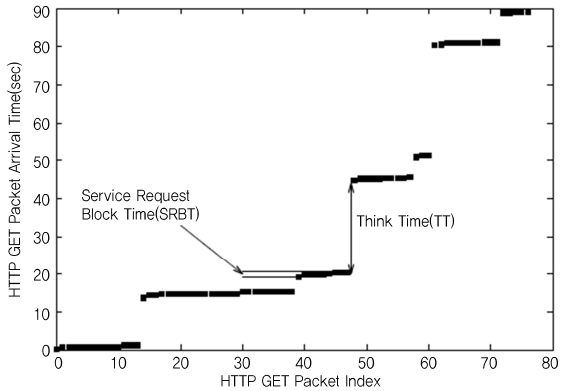


(그림 6) Yatagai et al [8] 방법

profile 등 세션 파라미터를 변화시킴으로써 공격을 시도할 수 있다. Ranjan et al.[10]은 이러한 세 가지 변화에 대한 misbehavior들을 검출하여 HTTP-GET flooding 공격을 검출하는 방법을 제안하였다.

Yatagai et al.[8]은 (그림 6)에서와 같이 각 발신지 IP 주소별 웹페이지 브라우징 순서를 기록하여 동일한 페이지의 순서를 유지하는 호스트들을 검출하는 방법을 제안하였다. 이것은 공격을 위해 감염되거나 좀비 호스트로 사용되는 클라이언트들이 동일한 순서의 웹페이지를 브라우징하는 것을 이용한 것이다. 또한, 이들은 웹페이지 사이즈와 브라우징 시간 사이의 연관성을 이용해 공격을 검출하였다. 이것은 정상적인 사용자라면 당연히 많은 정보에 접근하면 브라우징 시간이 길어지기 때문이다.

Choi et al.[9]은 main request와 sub-request 사이의



(그림 7) Main 페이지 엑세스를 위한 HTTP GET Request 패킷 도착 시각[9]

일련의 HTTP GET request 패킷을 조사하여 공격을 검출하는 방법을 제안하였다. (그림 7)은 정상적인 사용자들에 의한 main 페이지 엑세스를 위한 HTTP GET request 패킷 도착 시간을 보여준다. Choi et al.[9]은 이러한 시간 특징을 이용해 공격을 검출하는 방법을 제안하였다.

V. 결론

본 논문은 은닉형 공격자 근원지 역추적 기술, DRDoS 및 HTTP Get flooding 공격과 관련 기술적인 대응에 관하여 살펴보았다. DRDoS 공격의 경우 전체적인 네트워크 트래픽 볼륨을 타겟으로 IP를 위장하여 특정 서버를 공격하고 HTTP Get flooding의 경우 내부 네트워크 IP의 여러 Port로부터 타겟 응용 애플리케이션을 공격한다. 두 가지 공격의 경우 네트워크상에서 증폭 공격 및 정상 HTTP 요청의 정상과 악의적인 요청을 구별하기 어려우며 아울러 ISP 네트워크 구성이 이중화된 경우나 reflector가 ISP 관리 밖(해외)에 존재하는 경우에 DRDoS 탐지에 대한 어려움이 존재한다. 최근 클라우드 서비스를 활용해 저렴한 비용으로 쉽고 빠르게 가상서버를 생성하여 좀비로 활용하는 추세와 함께 모바일 환경의 DDoS 공격 증가하고 있다. 이에 따라 대역폭(bandwidth), 자원(resource) 및 응용 (application)별로 방어 전략을 수립하여야 하며 더불어 Netflow와 같은 트래픽 정보를 기반으로 정상 사용자를 흉내 내는 지능형 DDoS 공격을 탐지하기 위한 빅데이터를 활용한 네트워크 정보 기반 통계적 정책 적용 및 Anomaly 탐지 기술 등의 적용이 요구된다.

용어해설

DDoS 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 서비스 거부 공격

DRDoS IP 주소를 스푸핑한 ICMP Echo request 패킷을 브로드캐스트 주소로 보내 공격 대상에게 수많은 Echo reply 패킷을 전송함으로써 다운시키거나(Smurf 공격), TCP/IP 네트워크의 취약점을 이용하여 공격 대상에게 SYN/ACK 홍수를 일으켜 대상을 다운시키는 분산 반사 서비스 거부 공격

HTTP Get Flooding 공격 트래픽을 수신하는 서버는 정상적인 TCP 세션과 함께 정상적으로 보이는 HTTP Get 요청을 지속적으로 요청하게 되므로, 서비스를 위하여 수행하는 서버는 기본적인 TCP 세션 처리뿐만 아니라 HTTP 요청 처리까지 수행해야 함. 이 경우 HTTP 처리 모듈의 과부하까지도 야기시킬 수 있는 DDoS 공격

약어 정리

AS	Autonomous Systems
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DRDoS	Distributed Refection Denial of Service
EDNS	Extension mechanisms for DNS
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISP	Internet Service Provider
NTP	Network Time Protocol
SNMP	Simple Network Management Protocol
US-CERT	United States Computer Emergency Response Team

참고문헌

[1] D.C. MacFarland, C.A. Shue, and A.J. Kalafut. “Characterizing Optimal DNS Amplification Attacks and Effective Mitigation,” *In Passive and Active Measurement 16th Conference*, Springer, 2015.

[2] C. Rossow, “Amplification Hell: Revisiting Network Protocols for DDoS Abuse,” In Symposium on Network

and Distributed System Security (NDSS), 2014.

[3] 전자신문, "DDoS 공격 대응 장비 국내 시장 현황," 2010. 4. 27.

[4] S. Kumar, "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet," *in Proc. Second Inter. Conf. Internet Monitoring and Pretection*, 2007.

[5] A. Householder et al., "Managing the Threat of Denial-of-service Attacks," 2001, http://resources.sei.cmu.edu/library/

[6] US-CERT, "UDP-based Amplification Attack," 2014, https://www.us-cert.gov/ncas/alers/TA14-017A

[7] D. Huistra, "Detecting Reflection Attacks in DNS Flows," *19th Twente Student Conference on IT*, Feb. 2013.

[8] T. Yatagai, T. Isohara, and I. Sasase, "Detection of HTTP-GET Flood Attack Based on Analysis of Page Access Behavior," *Proc. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, 2007.

[9] Y. Choi et al., "AIGG Threshold Based HTTP GET Flooding Attack Detection," Proc. WISA, 2012.

[10] S. Ranjan et al. "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks," *IEEE/ACM Trans. On Networking*, vol. 7, no.1, 2009, pp. 26-39.