# 변화하는 DDoS 공격을 방어하기 위한 다이내믹 리다이렉션 기법

왕정석○, 김계근▽, 최동근□, 곽후근, 정규식
롯데정보통신○▽□, 숭실대학교 정보통신 전자공학부
e-mail : {jswang○, toproach▽, dkchoi□}@lotte.net, {gobarian, kchung}@q.ssu.ac.kr,

# Using Dynamic Redirection to Protect Changing DDoS Attack.

JeongSeok Wang○, KyeGeun Kim▽, DongKeun Choi□, Hukeun Kwak, Kyusik Chung
Lotte Data Communication Company ○▽□, School of Electronics Engineering, Soongsil University,

**요 약**

악성코드의 지속적인 진화와 확대로 인해 악성코드 자체의 은닉 및 봇넷의 구성, C&C 서버의 구조뿐만 아니라 좀비 PC 를 이용한 DDoS 공격 방식에도 변화가 지속되고 있으며, 이에 대한 대응이 서비스 제공자에게 있어 가장 중요한 보호 이슈 중 하나로 대두되고 있다. 최근 이러한 DDoS 공격의 가장 일반적인 형태인 GET flooding 공격의 경우 리다이렉션 방법을 이용하여 회피하였지만, 최근들어 공격자가 일부 좀비 PC 를 이용하여 공격을 수행한 후 리다이렉션 페이지의 주소를 확보, C&C 서버를 통해 리다이렉션된 실제 응답페이지를 직접 공격하게 함으로써 이를 무력화 시키는 방법을 사용하고 있다. 본 논문은 호스트이름 변경, 페이지 주소 변경 등을 상황에 맞게 지속적으로 변경 적용하는 다이내믹 리다이렉션(Dynamic Redirection) 기법을 사용하여 효과적으로 리다이렉션 무력화 공격에 대응하는 방법을 제안한다.

## 1. 서론

악성코드로 인해 발생되는 좀비 PC 와 그를 통한 DDoS 공격은 국내외를 막론하고 최근 심각하고 파괴적인 침해사고 중 하나가 되고 있으며, 공격의 난이도가 높지 않고 쉽게 공격을 수행할 수 있음에도 불구하고 공격의 효과가 커서 다양한 상업적, 정치적 목적으로 사용되고 있다.

최근의 공격 유형을 보면 서버 자원 고갈형 DDoS 공격인 GET flooding 공격이 주류를 이루고 있는 추세이며, 이는 큰 대역폭을 필요로 하지 않으며, 접속이 많은 최초접근 페이지에 대해 GET 요청을 보내게 함으로써 공격을 구분하기 쉽지 않으면서도 서버의 세션, 디스크 I/O, 해당 페이지와 연결된 미들웨어 및 데이터베이스 등에 부하를 가중시킬 수 있는 공격이기 때문이다. 대표적인 대규모 DDoS 공격이라고 할 수 있는 2009 년 7/7 DDoS, 2011 년 3/3 DDoS 공격은 모두 이러한 형태의 공격을 통해 진행되었다.

이러한 자원 고갈형 DDoS 공격을 방어하는 가장 일반적이고 손쉬운 방법으로 악성코드의 특성을 이용한 리다이렉션 방법을 들 수 있다. 이는 일반적인 브라우저가 아닌 악성코드에서 “HTTP 302 redirection” 응답이나 HTML 태그, Javascript 기능 등으로 구현된 리다이렉션을 처리할 수 없기 때문에 초기 페이지에 대한 모든 요청을 정해진 실제 페이지로 리다이렉션 함으로써 악의적인 공격을 무력화 시키고, 브라우저를 통한 일반접속은 정상적으로 처리할 수 있기 때문이다.

하지만 최근 이러한 리다이렉션을 이용한 처리방법이 보편화 됨에 따라 이를 회피하여 공격하는 방식을 이용하여 직접적으로 실제페이지를 공격하고 있다.

본 논문에서는 실제 페이지의 주소를 확인한 후 직접적으로 실제페이지를 공격함으로써 리다이렉션 서버를 우회하는 최근의 공격에 대응하기 위해 지속적으로 리다이렉션 방식과 서버의 주소, 페이지 주소를 변경하는 다이내믹 리다이렉션(Dynamic Redirection) 기법을 통해 리다이렉션 우회 공격을 방어하는 기법을 제안한다.

## 2. 페이지 리다이렉션 종류 및 방법

### 2.1 HTTP 301, 302 Redirection Code

HTTP 응답 코드 중 하나인 “301 Move Permanently” 와 “301 Move Temporarily”를 이용한 방법으로, 웹서버의 응답 코드 중 페이지가 일시적 혹은 영구적으로 이동되었음을 의미하며, 해당 코드의 뒤에 위치하는 이동된 페이지의 주소를 브라우저가 따라서 이동하도록 하여 리다이렉션 시키는 방법이다.

웹서버가 설정된 내용대로 직접 응답을 수행하므로 디스크 I/O 등이 발생하지 않는다는 장점이 있지만, 웹서버 설정을 변경해야 하는 단점이 존재한다.

2.2 HTML 태그를 이용한 리다이렉션

그림 1 은 HTML 태그를 이용하여 리다이렉션을 구현한 예제 이다. 그림과 같은 태그를 삽입한 HTML 문서를 초기 응답 페이지로 위치시키면, 아래 그림과 같은 태그에서 이동할 페이지를 해석하여 리다이렉션 시키는 방법이다.

```
<head>
  <meta http-equiv="Refresh" content="0; url=www1.test.com/index.jsp">
</head>
```

[그림 1] HTML 리다이렉션 태그 예제

2.3 Javascript 를 이용한 리다이렉션

HTML 태그를 이용한 리다이렉션 방법과 비슷하게 초기 응답 페이지를 이용하여 이동시키는 방법으로 브라우저의 자바스크립트 해석엔진이 자바스크립트 부분의 이동명령을 해석하여 리다이렉션 시키는 방법이다.

```
<script type="text/javascript">
   document.location='www1.test.com/index.jsp';
</script>
```

[그림 2] Javascript 를 이용한 리다이렉션 예제

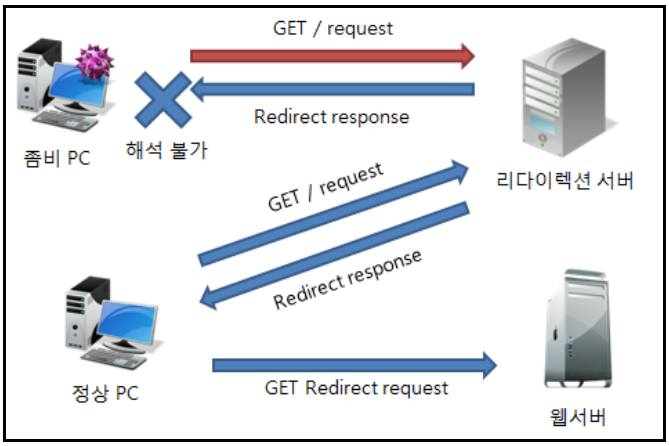
## 3. 다이내믹 리다이렉션 (Dynamic Redirection)

앞서 설명한 바와 같이 DDoS 의 GET flooding 공격의 경우 주로 해당 웹사이트의 대표 URL 로 요청을 집중시킨다. 이 때 C&C(Command and Control) 서버로부터 공격코드나 명령을 받은 좀비 PC 들은 그림과 같은 형태의 요청을 서버로 보내게 된다.

```
GET / HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml,
image/pjpeg, application/x-ms-xbap, */*
Accept-Language: ko
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Accept-Encoding: gzip, deflate
Cache-Control: no-store, must-revalidate
Proxy-Connection: Keep-Alive
Host: www.    .go.kr
```

[그림 3] GET 요청

이때 2 장에서 살펴본 각 방법에 따라 리다이렉션 응답이 클라이언트로 향하게 되고, 이를 해석한 클라이언트는 실제 응답이 존재하는 서버로 다시 요청을 보내 정상적인 서비스를 받게 된다.




[그림 4] 리다이렉션 처리

이때 클라이언트의 요청에 대한 응답으로 일정한 리다이렉션 주소를 사용하게 됨으로써 생겨나는 취약점을 막기 위해, 최초 공격 탐지 이후부터 주기적으로 리다이렉션 주소를 변경하여 실제 브라우저를 통한 일반 접속이 아닌 경우 예측이 불가능 하도록 하여 공격을 회피한다.

리다이렉션 주소를 변경하기 위해서는 DNS 서버를 이용하여 호스트네임을 변경하는 방법과 페이지주소를 변경하여 요청 URI 를 변경시키는 두 가지 방법을 사용할 수 있다.

3.1 호스트네임 변경을 통한 리다이렉션

호스트네임을 변경하여 리다이렉션을 시키는 방법은 www.test.com 으로의 접속 요청 시 www1.test.com 과 같은 다른 호스트네임을 가진 서버로 요청을 리다이렉션 시키도록 함으로써 구현된다.

이 때 리다이렉션 서버는 DNS 서버와 실제 응답 서버를 변경하여 www2, www3 등 다양한 호스트네임을 만들어 내고 해당 호스트네임이 가리키는 아이피 주소를 웹서버가 응답할 수 있게 함으로써 지속적으로 호스트 이름을 변경해 가며 리다이렉션 주소를 재지정 한다.

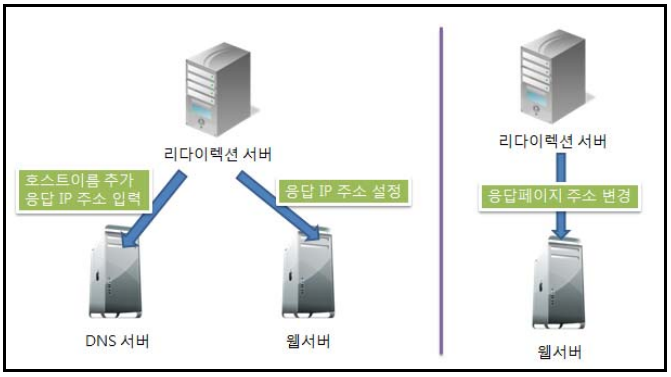
3.2 페이지주소 변경을 통한 리다이렉션

호스트네임을 변경하는 방식은 DNS 서버에 대한 변경과 응답 웹서버의 설정을 아이피 설정을 변경해야 하는 등의 적용 제약조건이 있어서 사용하기 어려울 경우가 있을 수 있다. 이 경우 서버의 설정이 아닌 응답 페이지주소를 변경함으로써 동일한 효과를 얻을 수 있다.

리다이렉션 서버는 리다이렉션 응답 페이지에 삽입된 실제 응답 페이지주소를 임의로 정한 후 (예, redirected_index.jsp 등) 응답 페이지주소를 똑같이 변경해 주는 방법을 지속적으로 사용함으로써 리다이렉션 페이지 주소를 재지정 한다.

3.3 적용 방법

앞서 설명한 두 가지 방법을 웹사이트의 운영 상황에 맞게 사용하고, 요청의 빈도에 맞게 주기적으로 변경하는 방법을 사용하면 공격자의 지속적인 리다이렉션 페이지 추적으로부터 벗어날 수 있다.




[그림 5] 다이내믹 리다이렉션의 적용 방법

이때 적용되는 주기는 서버의 상황과 DDoS 공격의 상황에 맞춰 수분~수십분의 주기를 가지고 수행되며, 공격자가 변경된 리다이렉션 주소를 파악하여 C&C 서버를 통해 재 명령을 내리는 주기보다 짧으면 된다.

또한 공격 악성코드에 간단한 리다이렉션 해석기능을 넣어 해당 웹사이트의 리다이렉션 특성에 맞게 대응을 하더라도, 앞서 언급한 세가지 리다이렉션 방법을 혼합하고, 주기적으로 다이내믹 리다이렉션 기법을 적용하면 이에 대한 대응도 쉽게 할 수 있다.

## 4. 결론

최근 다양하게 변화하고 있는 DDoS 공격 기법에서는 공격자가 일부 좀비 PC 를 이용하여 먼저 공격을 시도하고, 웹사이트에서 이를 방어하기 위해 리다이렉션을 시도할 경우 C&C 를 통해 직접 리다이렉션된 실제 응답 페이지를 공격하도록 명령함으로써 리다이렉션 방어를 무력화 시키는 공격이 사용되고 있다. 이는 리다이렉션을 해석하지 못하는 좀비 PC 의 한계를 손쉽게 극복하고 좀비 PC 를 가려내는 가장 쉬우면서도 효과적이던 방어수단을 회피하여 DDoS 공격의 방어를 더욱 어렵게 한다.

하지만 본 논문에서 제안한 다이내믹 리다이렉션 (Dynamic Redirection) 기법을 사용하면 리다이렉션 주소를 주기적으로 동적으로 생성하고, 방식에 따라 호스트네임이나 서버의 페이지 주소를 변경함으로써 리다이렉션 회피로부터 효과적으로 방어할 수 있다.

가상의 좀비 PC 를 이용한 테스트 결과 실제로 호스트이름의 변경을 통한 방법과 페이지주소 변경을 통한 방법 모두 회피를 무력화하는 효과를 보였으며, 이로 인해 좀비 PC 의 경우 웹사이트의 정상 응답페이지로 접근하지 못하게 하는데 성공하였다.

## 참고문헌

[1] Y. Chen and K. Hwang, "Collaborative Detection and Filtering of Shrew DDoS Attacks using Spectral Analysis," Journal of Parallel and Distributed Computing, Special Issue on Security in Grids and Distributed Systems, Sept. 2006, pp.1137-1151.

[2] J. Ioannidis and S. M. Bellovin, “Implementing Pushback: Router-Based Defense against DDoS Attacks,” Network and Distributed System Security Symposium. (NDSS), San Diego, CA. Feb. 6-8, 2002

[3] J. Jung, B. Krishnamurthy, and M. Rabinovich, “Flash Crowds and Denial-of-Service Attacks: Characterization and Implications for CDNs and Web Sites”, Proceedings of Int’l World Wide Web Conference, ACM Press, 2002.

[4] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-Sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds", Second Symposium on Networked Systems Design and Implementation (NSDI), Boston, MA, May 2005.

[5] J. Kong, M. Mirza, J. Shu, C. Yoedhana, M. Gerla, and S. Lu, “Random flow network modeling and simulations for DDoS attack mitigation,” Communications, vol. 1, May 2003, pp. 487–491.

[6] S. Tanachaiwiwat and K. Hwang, “Differential packet filtering against DDoS flood attacks,” in Proc. of ACM Conf. on Computer and Comm. Security (CCS), October 2003.

[7] Y. Xiang, W. Zhou, and M. Chowdhury, “A survey of active and passive defense mechanisms against DDoS attacks,” Technical Report C04/02, School of Information Technology, Deakin University, Australia, March 2004.

[8] http://www.kcert.or.kr

[9] http://www.kisa.or.kr

[10] http://www.ahnlab.co.kr