Reverse Proxy Group과 PMS를 이용한 멀티벡터(Multi-Vector) DDoS 공격 방어시스템 구축 방안

김민수* · 신상일* · 김종민* · 최경호** · 이대성*** · 이동휘**** · 김귀남*****

요 약

본 연구는 최근 들어 DDoS 공격이 단순히 서비스를 방해하는 것에서 벗어나, 다양한 공격 기법을 혼합한 멀티벡터(Multi-Vector) 공격으로 발전하고 있다.

이러한 멀티벡터 공격은 DDoS 공격과 더불어 악성코드를 감염시켜, 내부 정보 유출 및 좀비PC를 만들어 DDoS 공격용에 활용될 경우에는 기존의 DDoS 공격 및 악성코드 감염에 대한 방어 전략으로는 한계점이 있다.

따라서 본 논문에서는 다양한 방법을 이용한 멀티벡터 공격을 효과적으로 방어하기 위한 Reverse Proxy Group과 PMS(Patch Management Server)를 제시하고자 한다.

Multi-Vector Defense System using Reverse Proxy Group and PMS(Patch Management System) Construction

Min-Su Kim* · Sang-Il Shin* · JongMin Kim* · KyongHo Choi** · Daesung Lee***
DongHwi Lee**** · Kuinam J. Kim*****

ABSTRACT

The objective of DDoS Attacks is to simply disturb the services. In recent years, the DDoS attacks have been evolved into Multi-Vector Attacks which use diversified and mixed attacking techniques.

Multi-Vector Attacks start from DDoS Attack and Malware Infection, obtain inside information, and make zombie PC to reuse for the next DDoS attacks. These forms of Multi-Vector Attacks are unable to be prevented by the existing security strategies for DDoS Attacks and Malware Infection.

This paper presents an approach to effectively defend against diversified Multi-Vector attacks by using Reverse Proxy Group and PMS(Patch Management Server).

Key words : 악성코드, DDoS, 멀티벡터(Multi-Vector), 좀비PC, PMS

접수일(2013년 3월 5일), 수정일(1차: 2013년 3월 14일),
게재확정일(2013년 3월 22일)

* 경기대학교 산업보안학과
** 경기대학교 산업기술보호특화센터
*** 부산카톨릭대학교 컴퓨터공학과
**** 경기대학교 산업보안학과(교신저자)
***** 경기대학교 융합보안학과

1. 서 론

인터넷을 통하여 거대한 위협을 제공하는 대표적인 공격으로 분산 서비스 거부(DDoS : Distributed Denial of Service) 공격이 있다.

DDoS 공격은 보안의 3대 요소인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availavility) 중 가용성을 저해하는 공격으로 공격자가 다수의 PC에 악성코드를 감염시켜, 공격자의 지시에 따라 대량의 유해 트래픽을 특정 사이트나 시스템에 전송하여, 정상적인 서비스를 방해하는 좀비PC활용 공격기법이다.

DDoS 공격의 방어방법으로는 방어자가 공격자의 공격량 만큼의 가용성을 확보해야만 방어를 할 수 있다.

하지만, 가용성을 확보한다는 것은 많은 비용과 시간 그리고 공격자의 공격량을 예측하기 어렵기 때문에 방어하기 어렵다.

최근 들어 이러한 DDoS의 공격이 단순히 서비스를 방해하는 것에서 벗어나, 방어자로부터 큰 혼란을 야기 시킬 수 있는 수단으로 다양한 공격 방법을 혼합한 멀티벡터(Multi-Vector) 공격이 증가하고 있다.

멀티벡터 공격은 악성코드를 감염시켜 PC 및 내부 네트워크의 정보를 수집·유출시키고, 좀비PC를 만들어 DDoS 공격용으로 활용하게 된다.

이러한 멀티벡터 공격은 기존의 방어 전략으로는 한계점이 있다.

따라서 본 논문에서는 다양한 방법을 이용한 멀티벡터 공격을 효과적으로 방어하기 위한 Reverse Proxy Group과 PMS(Patch Management Server)를 이용한 방어시스템을 제시하고자 한다.

2. 관련연구

본 장에서는 멀티벡터 공격을 방어하기 위해 기존의 악성코드 탐지 및 DDoS 공격의 방어기법에 대하여 살펴보고자 한다.

2.1 악성코드 탐지

악성코드는 공격자의 의도에 따라 공격대상 시스템에 영향을 미치는 명령어들의 집합으로, 최근 확산력과 파괴력이 강한 변종 악성코드가 급속하게 생성되고 있다. 우리 생활에 밀접한 컴퓨팅 환경에서 피해가 늘어나고 있어, 이에 대한 대책이 시급히 요구되고 있다[1][2][3][4].

이러한 악성코드의 탐지방법으로는 패턴매칭에 의한 방식으로, 악성코드가 확산되면 이들에 대한 정보를 수집 및 분석하여 시그니처(signature)를 생성한 뒤, 탐지하는 방식이다[5][6].

2.2 DDoS 공격 및 방어

2.2.1 DDoS 공격 기술

DDoS 공격의 유형을 살펴보면 Flooding 공격, Connection 기반 공격, Application 기반 공격 유형으로 구분할 수 있다.

기존의 공격유형이 동일한 공격기법을 지속적으로 발생하는 것과 달리 발전된 공격유형은 Syn, UDP, ICMP, HTTP Flooding 공격과 웹 어플리케이션의 과부하를 동시에 공격하는 등의 다양한 공격이 발생하는 사례가 늘고 있다[7][8][9][10].

2.2.2 DDoS 공격 탐지 및 차단

DDoS 공격을 탐지할 수 있는 방법은 기존의 IDS/IPS, 방화벽 등을 활용하는 방법이나 DDoS 전용 대응시스템이나 망 차원의 Netflow, MRTG(Multi Router Traffic Grapher) 등을 이용하는 방법이 있다[11]. 또한, 웹 서비스 사용자 page 이동경로에 따른 분류, 허용된 사용자에 한해 웹 서비스 접속을 허용하는 Admission Control을 통한 대응 방안 등이 제안되고 있다[12][13].

2.3 Proxy 서버

Proxy 서버는 자신을 통해 컴퓨터나 네트워크가 다른 네트워크나 컴퓨터에 간접적으로 접속할 수 있게 함으로써, 접속을 시도한 클라이언트와 최종 접속된 서버 사이에 중계역할을 수행하는 기능을 갖는다[14]. 즉, 사용자의 접속정보를 프록시 캐시(Proxy Cache)에 일시 보관하고 여러 사용자가 이를 공유하여 망의 부하와 웹서버의 부하를 감소시키는 역할을 하며, 동시에 사용자에 대한 서비스 속도를 개선하는 기능을 제공할 뿐만 아니라, 제한적인 대역폭을 갖는 구간에서 인증서버 역할을 대신하여 인증을 해주는 역

할을 하고 있다[15].

2.4 PMS(Patch Management System) 서버

패치관리시스템은 논리적 또는 물리적인 특정 그룹으로 나눈 호스트들의 모든 소프트웨어 버그를 자동으로 검색하고 패치해 주는 시스템을 말한다.

관리하는 시스템들의 모든 소프트웨어를 검색하고 패치하다는 점에서 단일 소프트웨어 벤더에서 제공하는 자동패치시스템하고는 개념적으로 다르다.

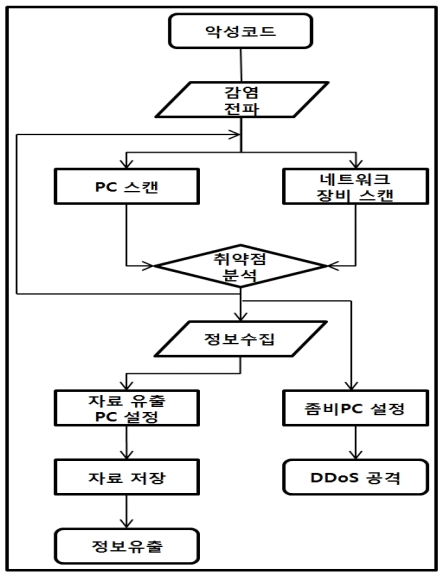
패치관리시스템은 패치대상시스템들의 다양한 운영체제와 소프트웨어 패치들을 관리한다[16][17][18][19][20][21][22].

3. 제안하는 방법

멀티벡터 공격의 형태를 알아보고 악성코드와 DDoS 공격의 방어를 위한 Reverse Proxy Group과 PMS의 시스템의 구성을 제안한다.

3.1 멀티벡터공격의 형태

(그림 1)은 멀티벡터공격의 Flowchart를 나타낸 것이다.



(그림 1) 멀티벡터공격 Flowchart

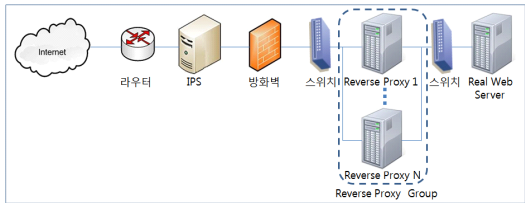
멀티벡터의 공격형태는 공격자가 악성코드를 감염시켜, 내부 네트워크의 취약점을 분석하게 된다. 취약점에 따라 정보수집 및 정보유출 관련 PC와 DDoS 공격 PC를 지정하게 된다.

3.2 Reverse Proxy Server Group을 이용한 DDoS 방어[23]

Reverse Proxy는 실 서버 앞에 위치하여 마치 실 서버처럼 동작하므로, 사용자와 공격자는 실 서버의 중요한 정보(O/S, 시스템 자원, IP 주소 등)를 알 수 없으며 Reverse Proxy를 실 서버로 착각하게 된다. (그림 2)은 Reverse Proxy를 이용한 DDoS 방어의 일반적 시스템 구조이다.

(그림 2) Reverse Proxy를 이용한 DDoS방어

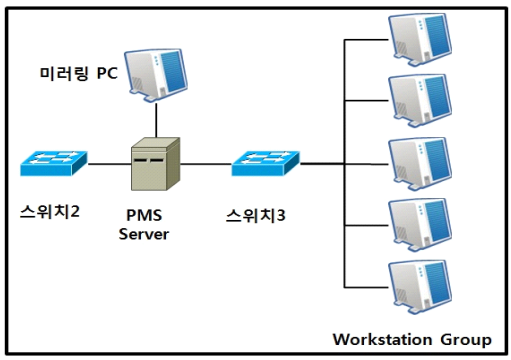
Reverse Proxy를 사용하는 이유는 공격자가 공격을 감행하더라도 모든 공격은 프락시 서버가 받게 되어, 프락시 서버가 다운되더라도 실 서버는 공격에 직접 노출되지 않기 때문에, 시스템 구성 정보만 변경하면 언제든지 즉각적인 서비스가 가능하다. (그림 3)은 이러한 Reverse Proxy 서버를 Group화하여 구성한 시스템 구조이다.



(그림 3) Reverse Proxy Group를 이용한 DDoS방어

3.3 패치관리시스템 서버

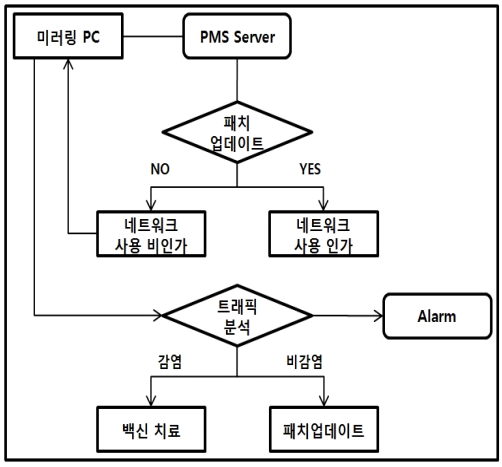
(그림 4)는 패치관리시스템 구성도로 내부 Workstation Group의 패치설정을 관리하게 된다.



(그림 4) 패치관리시스템 관리 서버 구성

(그림 5)는 패치관리시스템 Server의 운영 Flowchart로, 패치업데이트의 유무에 따라 네트워크 사용에 제한을 주게 된다. 네트워크의 제한을 받게 된 PC는 미러링 PC를 통하여 트래픽 분석을 하게 된다.

트래픽분석을 통하여 해당 PC의 이상유무를 확인하게 되고, 감염여부에 따라 치료 및 패치업데이트를 하게 된다. 또한 패치 업데이트에 대한 Alarm을 주게 된다.



(그림 5) 패치관리시스템 Server 운영

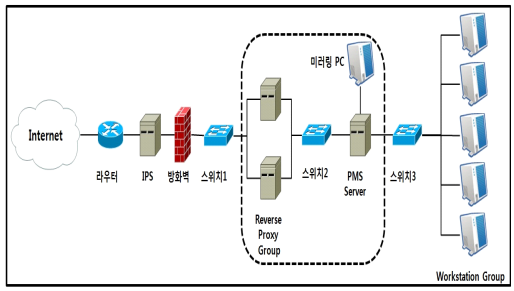
4. 제안 시스템 구현 및 평가

4.1 제안 시스템 구현

(그림 6)는 멀티벡터 공격을 방어하기 위한 Reverse Proxy Group과 PMS의 시스템 구성을 나타낸 것이다.

제안 시스템은 외부의 DDoS 공격에 대하여, Reverse Proxy Group을 활용하여 효과적인 방어를 하게 된다.

또한 내부의 악성코드 감염에 대하여, 최선의 방어방법인 보안패치 및 백신 설치유무를 확인하여, 내부의 정보유출 및 좀비PC의 형태를 차단하게 되는 시스템 구성이다.



(그림 6) 제안 시스템 구성

4.2 제안 시스템 평가

제안 시스템의 평가를 위하여 Workstation Group에 5대의 PC를 연결하여, 일반적인 구조와 제안된 구조를 비교분석하였다.

<표 1>은 제안 시스템의 비교 및 평가를 나타낸 것이다.

일반적 구조에서는 사용자가 일반적으로 보안패치 업데이트가 이루어지지 않은 상태이고, 제안된 구조에서는 자동으로 중요업데이트 및 제로데이 취약점 패치 업데이트하게 된다.

또한 평가를 위해 미러링 PC를 연결하여 트래픽을 분석 및 백신으로 감염숫자를 확인하였다.

분석결과 제안된 구조에서는 악성코드 감염, 좀비PC, 특정이상행위를 하는 PC가 나타나지 않았고, 일반적인 구조에서는, 5대 모두 악성코드에 감염되었고, 2대는 좀비PC로 과도하게 트래픽이 생성되었다.

<표 1> 제안 시스템 비교 분석

구분	일반적 구조	제안된 구조
중요업데이트	×	자동
제로데이 취약점 업데이트	×	자동
악성코드감염	5	0
좀비PC	2	0
특정이상행위	3	0

또한 미러링 PC에서 패킷분석을 한 결과 특정이상행위로 <표 2>와 같은 행위가 나타났다.

<표 2> 특정이상행위

Layer	이상행위
L2	· 특정 Port Open · 주기적 특정 IP/사이트 접속
L3	· 특정 사이트 SYN 패킷 급증 · 특정 사이트 TCP/UDP 패킷 급증
L7	· HTTP Get Flooding · HTTP Post Flooding

5. 결 론

본 연구는 기존의 DDoS 공격의 형태가 멀티벡터 형태의 공격으로 발전함에 따라, DDoS 공격 및 악성코드 감염의 복합적 공격에 대한 대응방안을 제시하고자, Reverse Proxy Group과 PMS를 이용한 멀티백터 DDoS 공격 방어시스템 구축방안에 대하여 연구하였다.

제안 시스템의 평가를 위하여 Workstation Group에 5대의 PC를 연결하여, 일반적인 구조와 제안된 구조를 비교분석하였다.

분석결과 제안된 구조에서는 악성코드 감염, 좀비PC, 특정이상행위를 하는 PC가 나타나지 않았지만, 일반적인 구조에서는, 5대 모두 악성코드에 감염되었고, 2대는 좀비PC로 과도하게 트래픽이 생성되었다.

또한 미러링 PC에서 패킷분석을 한 결과 Layer 2, 3,7에 대하여 특정 Port가 Open 되거나, 특정사이트에 SYN 패킷이 급증 및 HTTP Get/Post Flooding이 일어났다.

따라서, 멀티벡터 공격에 대하여 Reverse Proxy Group과 PMS를 구축한다면, DDoS 공격을 감소시키거나 분산시키고 내부적으로 악성코드에 대한 관리한다면, 멀티벡터 공격을 보다 효율적으로 방어할 수 있을 것이다.

참고문헌

[1] C. P. Pfleeger, and S. L. Pfleeger, security in Computing, Prentice hall, 2003.

[2] H. Carvey, "Malware analysis for windows administrators", Digital Investigation, Col.2, pp.19-22, 2005.

[3] N. Idika, and A. P. Mathur, "A Survey of Malware Detection Techniques", Research, Dept. of Computer Science, Purdue Univ., 2007.

[4] 김태형 외, “Intel VT 기술을 이용한 Xen 기반 동적 악성코드 분석 시스템 구현 및 평가”, 정보과학회, Vol.37, No.5, pp.304-313, 2010.

[5] Jose Nazario, "Defense and Detection Strategies against Internet Worms", Artech House, 2004.

[6] 박남열 외,“우회기법을 이용하는 악성코드 행위기반 탐지 방법”, 정보보호학회, Vol.16, No.3, pp.17-28, 2006.

[7] Jelena Mirkovic, “D-WARD : Source-End Defense Against Distributed Denial-of Service-Attacks", Ph. D. Dissertation, Computer Science, UCLA, 2003.

[8] Jelena Mirkovic and peter Reiher, “A Taxonomy of DDoS Attack and DDoS Defence Mechanisms”, ACM SIGCOMM Computer Communication

Review, pp.32-39, 2004.
[9] 서진원 외, “다단계 방어기법을 활용한 DDoS 방어시스템 설계”, 한국정보보호학회, Vol.22, No.3, p.681, 2012.
[10] 구자현, “서비스 거부 공격(Denial of Service)의 유형 및 대응”, 주간기술동향, 1377호, p.6, 2008.
[11] 김태원 외, “패킷 카운팅을 이용한 DoS/DDoS 공격 탐지 알고리즘 및 이를 이용한 시스템”, 한국시뮬레이션학회, Vol.19, No.4, pp.153-154, 2010.
[12] Takeshi Yatagai, “Detection of HTTP GET Flood Attack Based on Analysis of Page Access Behavior”, PACRIM, pp.232-235, 2007
[13] M. Srivatsa et al, “Mitigating Application Level Denial of Service Attacks on Web Servers”, ACM Transactions on WEB, Vol.2 Issue.3, 2008.
[14] 강신범 외, “프록시 서비스를 통한 범죄 위협과 프라이버시 보호에 관한 연구”, 정보보호학회, Vol.22, No.2, pp.318-319, 2012.
[15] 임차성 외, “SSL MITM 프록시 공격에 대한 효과적 방어방법”, 한국정보과학회, Vol.16, No.6, pp.693-694, 2010.
[16] 민동욱 외, “보안패치 자동분배를 위한 패치 DB 자동구성 방안”, 한국정보과학회, Vol.31, No.1, pp.367-369, 2004.
[17] 손태식 외, “안전한 패치분배시스템 구조 설계”, 한국정보화학회, Vol.29, No.2, pp.559-561, 2002.
[18] 이상원 외, “일반화된 보안패치 분배 및 관리 시스템을 위한 프레임워크 설계”, 한국정보과학회, Vol.31, No.2, pp.502-504, 2004.
[19] 김윤주 외, “확장성을 고려한 계층적 패치 분배 시스템 프레임워크 설계”, 한국정보과학회, Vol.31, No.1, pp.199-201, 2004.
[20] Chuan-Wen Chaang, Dwen-Ren Tsai, Jui-Mi Tsai, "A cross-site patch management model and architecture design for large scale heterogeneous environment", Security Technology 2005, CCST '05 3pth, IEEE, pp.41-46, 2005.
[21] Taeshik Shon, Jongsub Moon, Chelwon Lee, EulGyu Im, JungTaek Seo, "Safe Patch Distribution Architecture in Intranet Environments", Securtiy and Management 2003, pp.455-460, 2003.
[22] 이인용 외, “패치관리시스템의 효율적인 구성요소에 관한 연구”, 한국방송공학회, Vol.2008, pp.21-24, 2008.
[23] 신상일 외, “Proxy Server Group과 Dynamic DNS를 이용한 DDoS 방어 구축 방안”, 한국융합보안학회, Vol.12, No.6, pp.101-106, 2012.

[저 자 소 개]

김 민 수(Min-Su Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2012년 현재 경기대학교
산업보안학과 박사과정

email : fortcom@hanmail.net

최 경 호(KyongHo Choi)

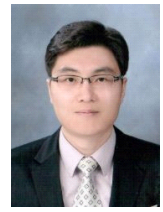
2002년 경기대학교 경제학사
2005년 경기대학교 경제학석사
2008년 경기대학교 정보보호학박사
2012년 경기대학교 연구교수
(산업기술보호특화센터)

email : cyberckh@gmail.com

신 상 일(Sang-Il Shin)

2004년 컴퓨터공학사
2007년 컴퓨터공학석사
2011년 현재 경기대학교
산업보안학과 박사과정

email : sishin69@hanmail.net



이 대 성 (Daesung Lee)

1999년 2월 인하대학교
전자계산공학과 학사
2001년 2월 인하대학교
전자계산공학과 석사
2008년 2월 인하대학교
정보공학과 박사
현재 부산가톨릭대학교
컴퓨터공학과 조교수

email : xdilemma@naver.com

김 종 민(JongMin Kim)

2012년 경기대학교 산업보안학과
박사과정

email : dyuo1004@gmail.com

이 동 휘(DongHwi Lee)

2000년 경기대학교 컴퓨터과학과
(이학사)
2003년 경기대학교
정보보호기술공학과(공학석사)
2006년 경기대학교 정보보호학과
(정보보호학박사)
2011년~2012년 5월 University of Colorado Denver, Dept. of Computer Science and Engineering
현재 경기대학교 산업보안학과

email : dhclub@naver.com

김 귀 남(Kuinam J. Kim)

미국 캔자스대학(학사)
미국 콜로라도주립대학(석사)
미국 콜로라도주립대학(박사)
현재 경기대학교 융합보안학과 교수

email : harap123@daum.net