서비스 거부 공격형 웜 바이러스 모니터링 및 차단 시스템

김지환[0] 김성조
중앙대학교 컴퓨터공학과
{jhkim[0], sjkim}@konan.cse.cau.ac.kr

Monitoring and Filtering System for DoS Attack Style Worm Virus

Ji-Hwan Kim[0] Sung-Jo Kim
Dept. of Computer Science & Engineering, Chung-Ang University

요 약

인터넷 사용의 급증과 함께 Code-Red나 Nimda와 같은 서비스 거부 공격형 웜 바이러스가 급격히 확산되고 있으며 이로 인한 피해가 급증하고 있다. 이러한 웜 바이러스는 대부분 일정 패턴의 HTTP 요청을 가지고 있으며 이러한 HTTP 요청 패턴을 확인하면 현재 감염된 클라이언트를 확인 할 수 있다. 그러나 새로운 웜 바이러스의 출현 시에는 기존에 분석한 요청 패턴만으로는 감염된 클라이언트의 확인이 불가능하다. 따라서 본 논문에서는 프락시 서버를 이용하여 실시간으로 바이러스 패턴을 분석하여 그 HTTP 요청 패턴과, 감염된 클라이언트 정보를 관리자에게 전송하며 자동으로 해당 클라이언트 및 해당 패턴에 대한 요청을 차단하여 바이러스의 확산을 막는 시스템을 제안한다.

1. 서 론

코드레드(Code-Red), 님다(Nimda) 같은 서비스 거부 공격형(DoS : Denial of Service) 웜 바이러스(Worm Virus)의 확산으로 인하여 컴퓨터 사용자들의 피해는 급격하게 증가하고 있다. 이러한 웜 바이러스는 사용자가 인지하지 못한 상태에서 감염이 되며, 감염된 컴퓨터는 새로운 숙주가 되어 바이러스를 확산시킨다. 이러한 서비스 거부 공격형 웜 바이러스들은 일정한 패턴을 가지는 수많은 HTTP 요청을 발생시키므로 네트워크 자원을 고갈시키고, 또한 네트워크를 통해 확산되므로 감염 속도가 매우 빠르다는 특징이 있다[1][2]. 따라서 실시간 적으로 바이러스 감염을 체크하여 치료 및 패치를 하는 것은 매우 중요한 일이다.

일반적인 바이러스 치료 프로그램들은 예약 검사 및 포트 검사를 통하여 바이러스 유입을 막는 방법을 사용하고 있다. 그러나 대부분의 백신 프로그램들은 이미 알려진 바이러스에만 적용이 가능하며 새로운 바이러스가 출현 시에는 즉각적인 대처가 불가능하여 이미 많은 클라이언트들이 감염된 이후에야 치료할 수 있다. 따라서 이미 알려진 서비스 거부 공격형 웜 바이러스뿐만 아니라 새로 출현한 바이러스에도 즉각적인 대처가 가능한 시스템 개발이 요구된다.

본 논문에서는 프락시 서버(Proxy Server)를 사용하여 클라이언트로부터의 모든 HTTP요청을 분석하여 서비스 거부 공격형 웜 바이러스로 인한 HTTP 요청으로 의심되는 요청 패턴과 그 요청을 한 클라이언트의 정보를 관리자에게 알려주며, 해당 HTTP 요청 및 클라이언트의 모든 요청을 차단하여 효과적으로 바이러스의 추가적인 감염을 차단할 수 있는 기법을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 바이러스 패턴과 프락시를 이용한 차단 방법에 대해 살펴보고, 3장에서는 본 논문에서 제시하고자 하는 프락시 서버를 이용한 웜 바이러스 모니터링 및 차단 시스템에 대하여 각 데몬 별로 상세히 기술한다. 마지막으로 4장에서는 결론과 향후 연구 방향에 대하여 논의한다.

2. 기반 연구

2.1 바이러스 패턴

웜 바이러스들은 일정한 패턴을 가지는 HTTP 요청을 하게 되는데 그 요청은 다른 정상적인 웹에 대한 요청이 이루어지지 못할 정도로 그 요청이 빈번하게 이루어진다[1][2]. <표 1>은 현재 잘 알려진 서비스 거부 공격형 웜 바이러스가 유발하는 HTTP 패턴을 보여주고 있다.

<표 1> 웜 바이러스 HTTP 요청 패턴

웜 바이러스의 HTTP 요청 패턴
www
x
www.worm.comaccept
accept

바이러스가 감염되는 경우 바이러스로 인한 요청의 발생 비율은 전체 HTTP 요청 발생 비율중에서 상당한 양을 차지하게 된다. <표 2>는 프락시 서버의 로그를 분석하여 1분당 120개의 클라이언트로부터 1초당 총 150개의 요청을 받는 경우에 200000번의 HTTP 요청 중에서 웜 바이러스로 인한 요청 회수를 측정한 결과이다.

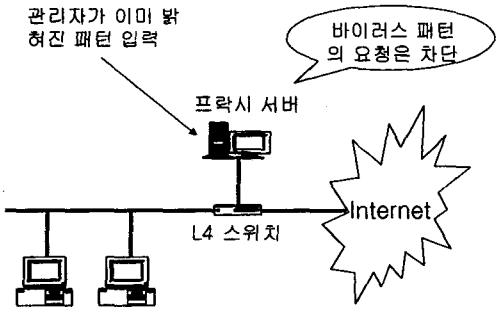
3개의 감염된 클라이언트에서 전체 HTTP 요청의 82%에 이를 정도로 심각한 네트워크 자원의 낭비가 발생하는 것을 확인할 수 있다.

<표 2> 웜 바이러스로 인한 HTTP 요청 비율

	요청 수	요청 비율
Client A	29192	14.60%
Client B	127537	63.77%
Client C	6645	3.32%
합 계	175586	81.69%

2.2 프락시 서버를 이용한 차단

<표 1>과 같이 웜 바이러스로 인하여 발생되는 HTTP 요청의 경우 일정한 패턴을 가지므로 관리자가 그 패턴을 찾아 요청을 막게 하면 외부망으로 바이러스가 확산되는 것을 차단할 수 있다. 즉 프락시 서버에서 일정 패턴의 요청에 대한 필터링을 수행하여 외부로 바이러스가 확산되는 것을 차단하는 방법이다.



(그림 1) 프락시 서버를 이용한 웜 바이러스 차단

그러나 이러한 방법은 관리자가 일일이 바이러스 패턴들을 확인하여 입력해야만 하는 단점이 있다.[3][4]. 더욱이 새로운 요청 패턴을 가지는 웜 바이러스의 경우 바로 적용이 불가능하며, 바이러스의 확산을 위해서는 단지 패턴을 차단하는 것만이 중요한 것이 아니라 이미 감염된 클라이언트를 확인하여 치료하는 것이 중요하므로 이에 취약점을 가지고 있다.

따라서 본 논문에서는 이미 밝혀진 패턴을 관리자가 입력하여 차단하는 기능 이외에 주기적으로 프락시 서버의 로그를 확인하여 웜 바이러스의 공격 패턴으로 의심되는 요청을 차단하고 그러한 요청을 발생시킨 클라이언트의 정보를 관리자에게 알려주는 시스템을 제안한다.

3. 웜 바이러스 실시간 모니터링 및 차단 시스템

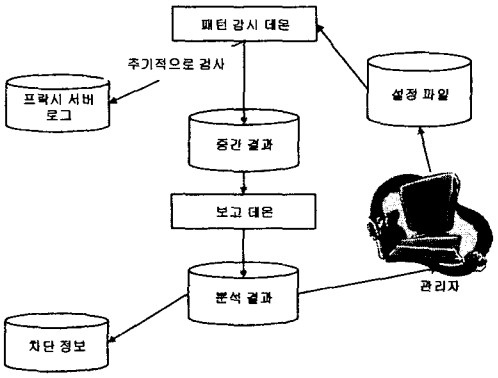
본 논문에서 제안한 시스템에 적용 가능한 웜 바이러스는 다음과 같은 요건을 가정한다.

▷ HTTP 요청을 빈번하게 발생시킨다.

▷ HTTP 요청에는 일정한 패턴을 가지고 있다.

본 논문에서 제안한 방법은 프락시 서버를 이용한 방법으로서 L4 스위치에서 모든 HTTP 요청을 프락시 서버로 전달하며 전달된 모든 HTTP 요청을 감시하여 웜 바이러스 패턴과, 감염된 IP를 검사하는 방식을 사용하고 있다. 모든 HTTP 요청은 프락시 서버의 로그에 저장이 되며 감시 시스템은 주기적으로 로그를 분석하여 의심되는 패턴을 찾아내게 된다.

시스템의 전체 구성은 (그림 2)와 같다. 프락시 서버에서 주기적으로 패턴 감시 데몬, 보고 데몬등이 동작을 하여 로그를 분석하여 바이러스 패턴을 감지하며, 그 결과를 관리자에게 알려주며 그 결과를 기반으로 하여 바이러스의 HTTP 요청 패턴 및 감염된 클라이언트로부터의 모든 요청을 차단한다.



(그림 2) 시스템 구성도

3.1 패턴 감시 데몬

패턴 감시 데몬은 로그를 분석하여 클라이언트들이 요청한 URL들과 해당 URL을 요청한 모든 클라이언트의 IP주소들을 얻는다. 이를 URL기준으로 바이너리 트리(Binary Tree)에 저장을 하며 이때 요청한 모든 클라이언트의 IP도 같이 저장한다.

<표 3> 요청 패턴과 IP를 저장하기 위한 자료구조

```
typedef struct _ip_node {
        struct _ip_node     *left,*right;
        unsigned long       requestCount;
        int                 ip_size;
        char                ip[0];
} IPNode,*pIPNode;

typedef struct _url_node {
        struct _url_node    *left,*right;
        unsigned long       requestCount;
        int                 url_size;
        pURLNode            ip_root;
        char                urp[0];
} IPNode,*pIPNode;
```

이 데몬에 의하여 모든 요청에 대한 분석이 종료가 되면 보고 데몬이 동작을 한다.

3.2 보고 데몬

보고 데몬에서는 패턴 감시 데몬에서 분석한 자료중에서 바이러스로 의심되는 요청 패턴과 이를 요청한 IP를 차단 DB에 저장을 한다. 바이러스로 의심되는 패턴은 다음과 같은 조건을 만족한 경우이다.

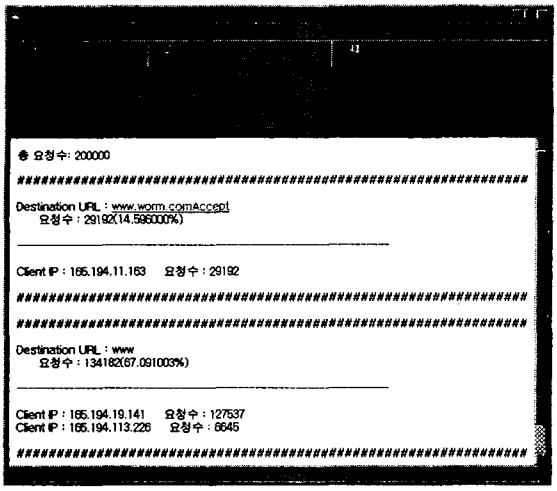
▷ 전체 요청 중 일정 비율 이상을 차지하는 경우

▷ 바로 이전의 검사 결과에 비하여 급격하게 증가한 경우

<표 5> 보고 데몬의 처리과정

```
for(all url_node in binary tree)
{
    if( url_node->requestCount  >
                        user define threshold_value)
    {
        to_administrator(url_node->url, url_node->ip);
        to_filtering_db(url_node->url, url_node->ip);
    }
}
```

그리고 분석한 결과를 정리하여 (그림 3)과 같이 관리자에게 메일로 그 결과를 전송한다.



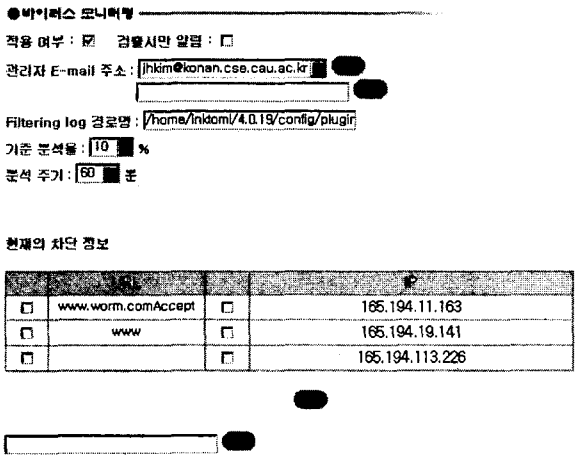
(그림 3) 관리자에게 전송된 분석 결과

3.3 차단 데몬

차단 데몬은 바이러스에 의한 요청을 차단하는 역할을 수행한다. 이 데몬에서는 보고 데몬에서 결정된 차단 DB를 기반으로 하여 바이러스로 의심되는 패턴과, 바이러스에 감염된 것으로 의심되는 클라이언트의 모든 HTTP요청을 차단하여 외부로 바이러스가 확산되는 것을 차단한다.

3.4 관리자 인터페이스

일부 패턴의 경우 정상적인 웹 요청임에도 불구하고 일시적으로 많은 사용자의 요청이 발생하는 경우 본 시스템에서는 바이러스로 인한 요청 패턴으로 인식할 수 있다. 따라서 (그림 4)와 같은 인터페이스를 제공하여 시스템 설정 및 관리자가 차단되는 패턴의 추가 및 삭제가 가능하도록 하였다. 또한 이 인터페이스를 통하여 관리자는 보고 데몬에서 사용할 임계값과 관리자의 메일 주소등을 설정할 수 있다.



(그림 4) 관리자 인터페이스

4. 결 론

본 논문에서는 프락시 서버를 이용한 웜 바이러스 모니터링 및 차단 시스템을 제안하였다. 새로운 패턴이 발생하는 경우에도 해당 패턴에 대한 분석이 가능하며 바이러스가 감염된 클라이언트를 차단함으로서 바이러스 확산을 막을 수 있는 장점이 있다. 그러나 웜 바이러스로 인한 요청이 아님에도 불구하고 사용자들에 의한 요청이 많은 경우 바이러스로 인한 요청으로 인식 될 수 있으며, 임계값이 관리자에 의해 설정되므로 너무 낮은 값이거나 높은 값으로 설정한 경우 효과적인 시스템 적용이 불가능하다.

향후 연구 과제로는 바이러스 요청이 아님에도 불구하고 특정 URL에 대한 요청이 급격하게 발생한 경우의 해결방법과, 임계값을 관리자가 설정하지 않고 현재의 요청 특성에 맞도록 시스템이 설정하는 방법에 대한 연구가 필요하다.

참고문헌

[1] "Code-Red 바이러스 정보" http://home.ahnlab.com/smart2u/virus_detail_848.html

[2] "정보보호진흥원" http://www.certcc.or.kr/

[3] "네트워크 필터링기법을 통한 Code Red 웜 대응방법" http://www.certcc.or.kr/paper/tr2001/tr2001-08/CodRed%20Worm%20Virus.html

[4] "엔콤정보시스템의 님다 차단 솔루션" http://www.encom.co.kr/about_htm/press_link5.htm