인터넷 웜 CodeRed의 공격기법 분석 및 대응현황

한국정보보호진흥원 전완근 · 임재명
한서대학교 이중식 · 이종일 · 김홍윤*

1. 서 론

웜(Worm)은 수년 전에만 해도 플로피 디스크 등을 통해 일부 PC들에게 컴퓨터바이러스에 감염되어 피해를 주는 정도로 소규모적인 컴퓨터바이러스의 전염성을 가지고 있었다. 그러나 최근에는 네트워크상에 접속된 대량의 컴퓨터에 의존하는 정보화 사회가 도래되고 이동코드 형태의 프로그램의 개발과 보급이 확대되면서 인터넷을 통하여 생물학적 바이러스 질병처럼 인터넷 기반의 컴퓨터바이러스는 자기 자신을 복제하거나 번식하는데 단시간에 감염시킬 수 있는 전염성을 갖추게 되었다[1].

특히, 1990년 후반부터 시작된 인터넷 열풍으로 E-mail 사용이 빈번해지면서 E-mail은 웜의 유용한 전파수단이 되기 시작했다. E-mail을 통한 전파법은 기존의 어떤 방법보다 효과적으로 짧은 시간에 웜을 확산 시켜주었다. 이로 인하여 매크로 바이러스 제작에 열을 올리던 많은 바이러스 제작자들에 의해 자신의 바이러스와 웜에 이메일(전자우편) 기능을 추가한 인터넷 웜이 제작되어 졌다.

최근 들어 급증하고 있는 인터넷 웜은 인터넷을 통해 사용자의 간섭 없이 자동으로 웜을 전파시키는 등 감염속도가 급격히 빨라졌으며 국내에 유입된 미켈란젤로, 멜리사 바이러스, ExploreZip, 러브레터 등과 같은 웜바이러스 경우에서처럼 수 시간 또는 수일 내에 인터넷을 통해 전 세계에 유포되어 하루만에 수백 만대의 PC에 막대한 피해를 입히고 있는 실정이다. 또한 인터넷 웜은 취약점 스캔, 자동공격, 빠른 확산을 특징으로 하고 있으며, 기존에 있던 솔라리스 등 유닉스 기반의 서버시스템이 아닌 윈도우 운영체제 시스템 기반으로 공격의 초점이 맞추어 지고 있다. 그 중에서 가장 대표적인 인터넷 웜이 Code Red[2]이다. 이 CodeRed 웜은 백도어, 트로이목마, 웜 등 복합적인 기능을 함께 지니고 있다.

CodeRed 웜은 2001년 7월 처음으로 출현하여 IIS(Internet Information Server)의 보안 취약점[3]을 지닌 윈도우 NT/2000 웹서버를 대상으로 하는 해킹 공격이 시작되어 만 하루만에 전 세계 370,000여대 이상의 시스템이 피해를 입었고, 국내에서도 4만 여대의 시스템이 피해를 당하였다. 또한 8월에는 백도어 및 트로이목마 기능이 포함된 새로운 변종의 CodeRed 웜의 공격까지 더하여 4,000여개의 기관이 해킹 피해를 당하는 등 CodeRed 웜의 피해는 기하급수적으로 늘어만 갔다.

특히, CodeRed 웜으로 인한 피해가 다른 기관들보다 기업과 교육기관들은 더 큰 피해를 컸던 이유는 기업이나 대학의 연구소 등에서 주로 웹 서버로 윈도우 NT/2000 시스템을 많이 사용하고 있다는 점과 그러한 웹 서버의 보안관리를 할 수 있는 기술력이나 인력 등이 거의 없다는 점 때문이었다.

이에 본고에서는 먼저 최근 인터넷을 통해 급증하고 있는 웜의 종류와 기본적인 형태에 대해서 살펴보고, 3장에서는 Code Red 웜의 공격 대상인 IIS가 지닌 취약점에 대한 버퍼오버플로우 공격기법과 전체적인 CodeRed 웜에 대한 공격 방법을 기술하고, 4장에서는 라우터나 스캐너 등을 이용한 CodeRed 웜의 공격 대응현황에 대해서 알아보고, 5장에서는 결론을 맺는다.

2. 웜의 종류와 형태

해킹 기술을 응용하기도 하며 원격 시스템으로의 전파라는 점에서 웜은 바이러스보다 그 전파속도가 강하다고 할 수 있고 가장 위험한 유형이라고 할 수

* 종신회원

있다. 바이러스 제작도구들이 인터넷에 유통되면서 다양한 악성프로그램변종들이 출현하고 있다. 그러나, 컴퓨터 바이러스와 웜의 정의에 대해서는 아직까지 일치된 하나의 명확한 이론이 없는 실정이다. 그리고, 현재 나타나고 있는 웜의 형태를 보면, DOS 시절의 단순한 형태의 웜이 아닌 복합화되는 양상을 띠고 있다. 또한, 최근에는 계속적으로 공개되는 새로운 취약성에 대한 공격 모듈을 쉽게 추가하고 업데이트가 가능하도록 웜이 구현되어가고 있다[4].

2.1 웜의 전파방법에 따른 분류

웜은 많은 전파를 목적으로 하는 경우가 많으며 웜에서 사용되는 전파방법에 따라 이메일, 호스트 컴퓨터, 네트워크 웜과 같은 세 가지 유형으로 나눌 수 있다[5].

표 1 웜의 전파방법에 따른 분류

컴퓨터 웜	
전파방법	이메일 웜
	호스트 웜
	네트워크 웜

2.2 웜의 네트워크 범주에 따른 분류

지난 몇 년간 인터넷 웜의 다른 유형들이 개발되면서 컴퓨터 웜은 로컬 네트워크를 통해 전파되는 네트워크 웜과 인터넷과 같은 글로벌 네트워크를 통해 전파되는 인터넷 웜으로 나눌 수 있다.

표 2 웜의 네트워크 범주에 따른 분류

컴퓨터 웜	
네트워크 범주	인터넷 웜
	네트워크 웜

2.2.1 인터넷 웜

인터넷 웜은 다시 PC사용자의 감염원인 행위에 따라서 몇 가지 그룹으로 분리할 수 있는데 주로 이메일의 메시지를 읽음에 의해 행동하는 웜, 파일을 열어 봄으로써 행동하는 웜, 아무런 행위 없이도 자동으로 행동하는 웜으로 나눌 수 있다. 이메일 웜은 전파되는 속도에 따라서 Slow mass-mailers, Fast mass-mailers로 분류된다. Slow mass-mailers 웜은 감염된 사용자가 메일을 보내는 시점에 웜을 전송하는 반면에 Fast mass-mailers는 한번에 여러 메일 사용자에게 웜을 보낸다.

표 3 이메일 웜의 전파속도에 따른 분류

컴퓨터 웜	
전파속도	Slow mass-mailers
	Fast mass-mailers

이메일 웜은 전파방법으로 시스템에 이미 설치되어 있는 이메일 클라이언트를 사용하는데 마이크로소프트의 아웃룩과 아웃룩 익스프레스와 같은 특정 메일 클라이언트의 주소록에 등록된 모든 사용자에게 메일을 동시에 송신하는 것이 대부분이다. 따라서 어느 한 명이 감염되면 그 사람의 이메일 주소록에 있는 다른 사람들의 컴퓨터까지 바이러스에 감염될 위험이 있으며, 이렇게 연쇄적으로 웜이 확산될 경우 엄청난 숫자의 컴퓨터들이 바이러스에 걸리게 된다.

Loveletter나 Navidad 바이러스처럼 사람들의 감성을 자극하는 문구를 첨가하거나 음란사진이나 동영상이라는 문구를 사용해 호기심을 유발하는 경우가 많으며, 또한 최신 바이러스 백신이라고 가장해서 바이러스에 겁먹은 사람들의 별다른 의심 없이 첨부파일을 열도록 유도하는 등 다양한 방법을 사용하고 있다.

2.2.2 네트워크 웜

네트워크 웜은 로컬 네트워크를 통하여 전파되는 웜으로 다음과 같은 단계로 구성된다.

▲ 공유 드라이브 찾기
▲ 드라이브 매핑하기
▲ 웜을 복사하고 실행하기

일반적으로 복사된 웜의 실행은 즉각적으로 일어나지 않고 윈도우 시작 시 자동실행 될 수 있는 시작 폴더와 같은 특정 디렉토리에 복사해놓는 경우가 많다. 따라서 시스템이 재시작 될 경우에 설치된 웜이 자동으로 실행된다.

네트워크 웜의 하나인 넷로그(Netlog)[6]는 먼저 전파하려는 대상을 찾기 위해 임의의 IP를 설정하여 검색한 후 서브넷 시스템 전체에서 C드라이브 전체를 공유해 놓은 시스템을 찾아낸다. 그 후 해당 드라이브를 J드라이브로 설정하고 윈도우와 윈도우 시작

폴더에 파일을 복사해 놓으면 다음 윈도우 시작 시 자동으로 실행되어 감염된다.

이외에도 최근 등장하는 인터넷 웜 중에서 윈도우 웜이 큰 비중을 차지하여 플랫폼에 따라 윈도우에서 활동하는 윈도우 웜과 윈도우 외에 다른 플랫폼에서 활동하는 Non-윈도우 웜으로 분류할 수 있다. 윈도우 웜은 이메일이나 뉴스레터, IRC, MSN 메신저와 같은 채팅 프로그램, 그밖에도 Gnutella, IIS 등을 이용하고 있으며, Non-윈도우 웜은 리눅스나 솔라리스와 같은 유닉스 시스템과 매킨토시에서 활동하는 유닉스의 러브레터 개념의 모리스(Morris) 웜, 최초로 큰 규모의 피해를 주었던 리눅스 라멘(Ramen) 웜, 솔라리스의 에스어드민(Sadmind), 매킨토시의 심슨(Simpson)과 같은 것이 있다.

2.3 웜 바이러스의 형태

웜은 DOS 시절에도 존재했지만 당시 프로그램 복사는 플로피디스크와 통신을 통한 프로그램 복사가 고작이었다. 따라서 일반 사용자들의 PC가 웜에 감염되는 일은 거의 없었다. 웜이 다른 컴퓨터로 복사될 가능성이 제한적이었기 때문이다.

그러나, 1990년 후반부터 시작된 인터넷 열풍으로 이메일 사용이 빈번해지면서 이메일은 웜의 유용한 전파수단이 되기 시작했다. 대부분의 개인 사용자 컴퓨터의 운영체제가 윈도우로 통일되면서 웜들이 전 세계로 퍼졌다. 이메일을 통한 전파법은 기존의 어떤 방법보다 효과적이었다. 짧은 시간에 널리 퍼진 걸 알게 된 바이러스 제작자들은 이메일을 통한 바이러스 전파 아이디어를 받아들였고, 매크로 바이러스 제작에 열을 올리던 많은 바이러스 제작자들은 자신의 바이러스와 웜에 이메일 기능을 추가하게 됐다. 이에 따라서 DOS 시절 단독으로 존재하면서 복사를 통하여 플로피디스크 등을 통하여 전파되었던 단순한 형태의 웜에서, 웜과 바이러스 또는 웜과 백도어(트로이목마) 등의 기능이 혼합되어 인터넷이나 이메일을 통하여 유포되고 있는 형태로 변하고 있다.

그 대표적인 예가 바로 I-Worm_MTX [7]웜이다. I-Worm_MTX 웜은 웜과 바이러스와 백도어(트로이목마)의 기능을 동시에 지니고 있다. MTX 웜 바이러스의 구조에서 주요부분을 차지하고 있는 바이러스코드 부분은 Win32 실행 파일을 감염시키며 웜 부분에서는 전자우편을 통하여 보내지는 메시지에 감염된 첨부 파일을 보내도록 하고, 설치된 백도어를 통하여 감염이 된 시스템에 플러그인을 다운로드받아 자체의 기능을 업그레이드하거나 시스템 정보를 외부로 유출한다.

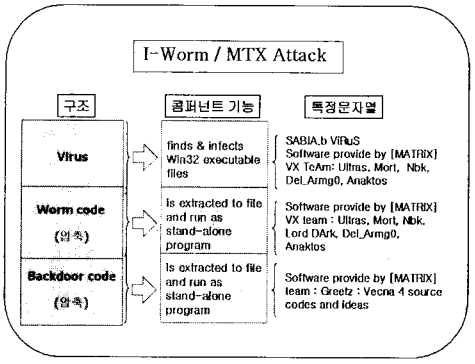


그림 1 MTX 웜 바이러스의 구조

3. 인터넷 웜 CodeRed의 주요 공격기법

인터넷상에서 크게 문제화되고 있는 해킹기법 중의 하나가 버퍼오버플로우이다. CodeRed에서 사용된 기법은 윈도우즈 IIS 서버가 지닌 취약점인 ida.dll 대상으로 버퍼오버플로우 공격을 하여 감염·전파되었다.

3.1 IIS(Internet Information Service) 취약점과 버퍼오버플로우

인터넷 웜은 시스템을 감염시키고 나면 다른 취약점이 있는 시스템을 찾기 위해 네트워크를 스캔(Scan)한 후 자동적으로 취약점이 있는 시스템을 공격대상으로 하여 감염시키면서 전파된다. CodeRed는 바로 WindowNT/2000시스템의 웹서비스로 많이 쓰이고 있는 IIS가 가지고 있는 IIS Indexing Service DLL 파일을 대상으로 버퍼오버플로우 공격이 이루어졌다는 것이다. IIS 확장 응용프로그램인 ISAPI DLL중 하나인 ida.dll 파일은 IIS 설치과정에서 여러 가지 ISAPI 확장 기능 중 Index Server의 구성요소인 중 하나로, 입력된 URL을 처리하는 기능을 하는데, 바로 이 코드의 일부분에 검사하지 않은 버퍼를 포함시킴으로써 공격을 당하게 되었다.

기본적으로 ISAPI 응용프로그램 또한 시스템의 권한으로 돌아가게 되고, ISAPI hook이 불려지게 되

면, IIS는 그 일을 하는 스레드를 낮은 권한으로 돌리게 되는데 바로 이점을 CodeRed 웜이 이용한 것이었다. CodeRed가 사용한 취약점은 IIS 4.0과 5.0 버전에 설치된 ISAPI 확장기능에서 원격 버퍼오버플로우이었으며, 이에 대한 exploit code가 인터넷상에 이미 공개되어있는 상태여서 쉽게 공격을 할 수가 있었다.

3.2 인터넷 웜 CodeRed의 공격분석

현재까지 알려진 CodeRed는 두 가지 종류가 있다. CodeRed I 의 경우에는 감염된 WindowNT/2000 시스템의 메모리에 100개의 쓰레드를 만들어 특정주기를 가지고 백악관 홈페이지를 서비스거부 공격하고, 영문 시스템일 경우엔 웹 페이지에 "Hacked by Chinese!"를 출력하도록 되어있다. 이와는 달리 CodeRed II는 중국어 버전일 경우엔 600개의 쓰레드를 만들어서 공격을 한 후에 웜기능뿐만 아니라 트로이목마를 설치하고 재부팅하여 메모리 상주된 웜을 사라지게 하는 역할을 수행하였다. 따라서 언제든지 자유롭게 감염된 시스템을 통제할 수 있는 백도어와 트로이목마 기능을 새로 포함하고 있었다.

3.2.1 CodeRed I 의 공격과정

CodeRed I 의 공격과정은 크게 CodeRed 감염루틴, 웹 페이지 해킹루틴, 미국 백악관의 웹 사이트 www.whitehouse.gov 공격루틴 3순서로 나뉘어져 있다. 세부적인 순서는 다음과 같다.

3.2.1.1 CodeRed 감염순서

CodeRed의 공격은 먼저 취약점이 있는 시스템에 대한 감염이 이루어지며 모두 8단계로 이루어졌다.

Step 1. .ida 공격에 취약한 웹서버에서 감염은 HTTP GET 요구(exploit 코드포함)가 실행되어 지면서 시작된다. .ida 오버플러우 공격에 성공하면, 최초의 HTTP 요청패킷에 포함되어 있는 CodeRed 웜 코드로 점프하게 된다.

Step 2. CodeRed 웜 코드 실행을 위해 스택영역을 확보한 후 218h 바이트 크기 CCh로 채운다. 그 후 점프 테이블로 이동하여 웜 함수를 초기화시킨다.

Step 3. RVA lookup 기법을 사용하여 IIS가 사용하고 있는 함수인 GetProcAddress의 시작 주소를 구한다. 그리고, GetProcAddress로 LoadLibraryA 시작 주소를 구한다. 이 함수를 이용하여 CodeRed 웜이 사용할 모든 함수의 dll 파일들을 로드하여 실행시킨다(예를 들면 WS2_32.dll을 로드하여 socket, connect, send, recv, closesocket 함수를 실행한다).

Step 4. 이 시스템을 공격하는 웜에게 WriteClient (Internet Server API) 함수를 이용하여 이 호스트가 이미 감염 됐음을 알린다.

Step 5. CodeRed 웜은 이미 실행중에 있는 스레드의 수가 100 이하이면 새로운 스레드를 생성하고, 100 이면 **웹페이지 해킹순서**로 제어를 옮긴다.

Step 6. c:\notworm 파일이 있으면 다른 IP 주소에 대해 더 이상 연결시도를 하지 않는다. 그러나, 파일이 존재하지 않으면 Step 7을 지속한다.

Step 7. 시스템의 현재 날짜가 20 UTC 보다 클 경우엔 **DDOS 공격순서** step 1로 간다.

Step 8. CodeRed 웜은 80포트가 열린 IP 주소를 대상으로 자신을(.ida 웜) 보낸다. 전송을 완료하면 소켓을 닫고, Step 6으로 제어를 옮긴다.

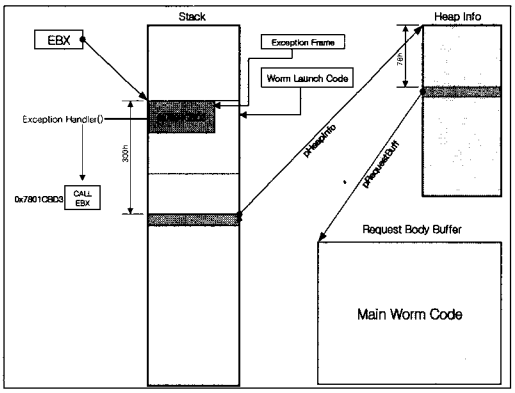


그림 2 CodeRed의 버퍼오버플로우 공격[10]

3.2.1.2 웹 페이지 해킹순서

CodeRed에 의한 웹 페이지 해킹은 영문시스템일 경우에만 이루어지며 해킹을 당한 홈페이지에 "Hacked by Chinese!"를 출력하도록 되어있다.

Step 1. 로컬시스템의 코드페이지 값이 0x409(영문시스템)이면 Step 2로 가고 아니면 **CodeRed 감염순서**의 Step 6으로 간다.

Step 2. 실행중인 스레드는 2시간동안 휴면한다.

Step 3. CodeRed 웜은 윈도우즈 hooking 기법을 사용하여 저장된 w3svc.dll의 TcpSockSend 주소를 웜 안에 있는 주소를 가리켜 "Hacked by Chinese!"을 클라이언트에게 보여주게 된다.

Step 4. 이 스레드는 10시간동안 휴면을 한다. 10시간이 지나면 이 쓰레드는 원래의 상태로 되돌리고

CodeRed 감염순서의 Step 6으로 되돌아간다.

3.2.1.3 DDOS 공격 순서

CodeRed의 목표인 www.whitehouse.gov에 대한 웜의 DDOS공격은 다음과 같다.

Step 1. CodeRed 웜은 패킷을 보내기 위해 소켓을 생성한 후 www.whitehouse.gov에 연결되면 80 포트로 100K 바이트 크기의 데이터를 한번에 1 바이트씩 보낸다.

Step 2. 패킷을 보낸 후 4시간 30분 동안 휴면시간이 지난 면 Step 1로 제어를 옮겨 공격을 되풀이한다[8].

3.2.2 CodeRed II의 공격과정

CodeRed II의 경우엔 기존의 CodeRed 웜과 같은 취약점을 이용하여 새로운 시스템을 감염시킨 후 5단계에 걸쳐서 공격한다.

Step 1. 현재 감염된 시스템의 IP 주소를 획득한다. 이는 웜 유포를 위한 공격대상 시스템을 선정하는데 사용된다.

Step 2. 감염된 시스템의 언어가 중국어(Taiwanese 또는 PRC)인지 점검한다.

Step 3. 위 과정이 이전에 실행되었는지 점검하여, 실행되었다면 유포단계로 간다.

Step 4. "CodeRed II"라는 atom의 존재여부를 검사하여, 있으면 sleep 상태로 들어가고, 없으면 새로 생성한다. 이는 이미 감염된 시스템을 재감염시키지 않기 위한 루틴이다.

Step 5. 비 중국어인 경우 300개의 스레드를, 중국어인 경우 600개의 스레드를 생성하고 웜 유포를 위한 공격에 들어간다[9].

4. CodeRed 웜의 공격 대응현황

CodeRed 웜의 공격에 대한 대응방법으로는 여러 가지가 있다. CodeRed 전용스캐너를 이용하여 CodeRed 웜으로 인한 공격대상이 되는 윈도우 NT/2000에서 IIS 4.0, IIS 5.0이 가지고 있는 버퍼오버플로우 취약점을 보완하여 미연에 방지하거나, 또는, 백신을 이용하여 치료하는 방법, 네트워크 장비인 스위치나 라우터 등에서 제공해주는 필터링기능을 이용하는 방법 등 여러 가지가 있을 수 있다.

4.1 백신제품과 CodeRed 전용스캐너

CodeRed 웜으로 인한 공격에 대한 근본적인 방법은 윈도우 NT/2000에서 IIS 4.0, IIS 5.0이 가지고 있는 버퍼오버플로우 취약점을 보완하는 것이다. 만일 CodeRed 웜에 이미 감염이 되었거나, 감염여부를 알고 싶은 경우에는 국내외의 백신제품이나 CodeRed 전용스캐너 등을 이용하여 탐지 및 치료하는 것도 대응에 한 방법이 될 수가 있다.

이미 CodeRed 웜에 감염된 증상이 나타날 경우에는 안철수 연구소 혹은 하우리 등의 국내외 백신제품을 이용하여 감염시 생성되는 파일과 변경되거나 새로 생성된 레지스트리들을 제거하여 치료하면 된다. 만일, eEye.com와 같은 사이트에서 개발한 CodeRed 전용스캐너[11]들을 이용하여 대응할 수도 있다. 이와 같은 도구들은 윈도NT/2000뿐만 아니라 윈도98에서도 사용이 가능하며, GUI형식으로 되어 있고, 검사할 내부 IP 대역과 CodeRed가 사용하는 특정 포트번호를 지정하여 자동으로 스캔하여 각 사이트 내에서 감염 가능한 혹은 감염된 시스템을 자동으로 찾아낸 후 보안조치를 할 수 있기 때문에 편리하다. 물론 국내 백신업체 사이트에서도 CodeRed 전용스캐너를 구할 수 있다.

4.2 방화벽과 L7 스위치

CodeRed와 같은 네트워크를 통한 대규모 공격 가능성은 이전부터 제기되어 왔다. 네트워크를 통해 정상적 서비스를 방해하는 형태인 '분산 서비스 공격' 이 알려진 이후, 야후와 이베이 등 대형 사이트 공격에 실제로 2년 전에 사용되었다. 그러나, CodeRed의 경우는 자동으로 배포되는 웜이기 때문에 순식간에 전 세계의 시스템에 자동으로 침투해 9시간만에 25만대 이상의 서버에 침투했고, 그로 인한 피해는 시간이 갈수록 기하급수적으로 늘어났다. CodeRed 웜과 같은 새로운 개념의 네트워크 공격은 다음과 같은 특성을 지니고 있다.

▲ 자동화된 공격

자동화된 공격방법으로 프로그램이 직접 공격을 수행한다. 이와 같은 자동화된 공격은 순식간에 공격을 끝내기 때문에 기존의 방화벽 · 침입탐지시스템의 조합으로는 대처하기 힘들다.

▲ 대규모 네트워크 부하 유발

짧은 시간 안에 가능한 한 많은 공격 대상을 찾아내기 위해, 수많은 시스템들을 빠르게 스캔해야만 한

다. 이러한 스캔 시도들은 그 자체가 네트워크 가용량을 떨어뜨리는 서비스 거부 공격의 형태를 띤다.

▲ 최신 취약점을 이용한 빠른 공격

항상 해킹을 시도할 때는 최근에 공개되거나 혹은 공개되지 않은 취약점들을 이용해 공격을 시도함으로써 취약점을 패치할 시간적 여유가 훨씬 줄어들었다.

이러한 CodeRed의 공격특성으로 인하여 네트워크를 보호하고 동시에 네트워크 성능 및 가용성을 유지시켜야 하는 해결책들을 필요로 한다. 그러나 일부 라우터 장비에서 제공하고 있는 패킷 필터링[12]이나 접근제어리스트 등 방화벽으로는 지속적으로 증가하는 다양한 외부 공격의 위협으로부터 기업을 보호하거나 애플리케이션의 가용성 및 성능을 보장하기에는 아직 역부족이다.

그러나, 자체 복제와 빠른 속도로 확산되는 CodeRed와 같은 공격들에 대해서 L7 스위치를 사용할 수 있다. 이 스위치는 URL, 컨텐츠 등의 인지가 가능할 뿐만 아니라 세션 컨트롤이 가능하고, dynamic port 와 유동되는 IP와 위장된 패킷까지 차단하기 때문에 공격 트래픽을 잡아내어 CodeRed 웜과 같은 인터넷 웜에 대한 대응에 어느정도 효과적이다.

5. 결 론

21세기에 접어들면서 획일화된 네트워크 구조와 운영체제 그리고 응용프로그램들도 인터넷의 환경으로 동질화되고, 기존의 유닉스 계열의 시스템보다 훨씬 더 보안상에서 취약한 윈도우 계열의 시스템으로 운영체제가 확산되면서 인터넷 웜에 의한 공격이 급증하는 등 그 파괴력 또한 커지고 있다. 또한 인터넷에 연결된 수 많은 취약한 시스템을 공격하여 자기 자신을 복제하면서 전파되는 인터넷 웜은 최근의 컴퓨터 보안 문제에 있어 가장 큰 문제로 여겨지고 있다.

이러한 인터넷 웜의 가장 대표라고 할 수 있는 CodeRed 웜은 마이크로소프트의 웹서버를 해킹 경유지로 이용하여 시스템에 피해를 주는 웜으로, Windows 인덱스 서비스의 .ida 취약점을 이용하여 확산되며, 80 포트(http)를 이용하여 전파된다. 그리고 기존의 웜이나 바이러스처럼 특정 파일이 복사되는 형태가 아닌 메모리에 상주하는 형태로 감염된다. 이러한 공격특성을 가진 CodeRed 웜에 대한 대응 방안은 아직 현저하게 미비한 형편이다. 일부 라우터 장비에서 제공하고 있는 패킷 필터링이나 접근제어리스트 등 방화벽 기술로는 지속적으로 증가하는 다양한 외부 공격의 위협으로부터 기업을 보호하거나 애플리케이션의 가용성 및 성능을 보장하기에는 아직도 안심할 수가 없는 실정이다.

이에 본고에서는 최근 급증하고 있는 인터넷 웜의 기본적인 종류와 형태, 그리고 대표적인 웜인 CodeRed를 분석해 보고, 그에 대한 대응 현황도 살펴보았다. 앞으로 이러한 빠른 전파력과 강력한 파괴력을 지닌 인터넷 웜의 공격에 대한 침입방지와 차단 기능을 동시에 가진 자동화된 제품들이 개발되어야 하고 또한, 대규모의 네트워크부하를 유발하는 인터넷 웜의 공격에 대처하기 위한 훨씬 빠른 처리 속도와 알려지지 않은 공격을 탐지하기 위한 연구들을 집중적으로 해야 할 것이다.

참고문헌

[1] David Harley 저, 이동표 역, Viruses Revealed, 교학사, 2002.7.

[2] 하도윤, 이현우, Code Red 인터넷 웜 재 확산, http://www.certcc.or.kr/paper/incident_note/2001/in2001_009.html

[3] Microsoft Security Bulletin MS01-033, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

[4] 이필원, 해킹 & 바이러스 특명 사이버테러를 진압하라, 아이북스, 2002. 2.

[5] V. Bontchev, Methodology of Computer Anti-Virus Research, Doctor Thesis, University of Hamburg 1998, p.23

[6] VBS/NetLog 웜 경보, http://www.certcc.or.kr/cvirc/Alert/36/Netlog.html

[7] 전완근, I-Worm_MTX 분석 보고서, http://www.certcc.or.kr/paper/tr2001/tr2001-03/I-Worm-MTX.html

[8] .ida "CodeRed" Worm, http://www.eeye.com/html/Research/Advisories/AL20010717.html

[9] CodeRed II Worm Analysis, http://www.eeye.com/html/Research/Advisories/AL20010804.html

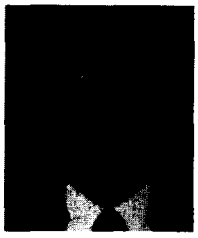
[10] Bruce McCorkendale & Peter Szor, "Code Red Buffer Overflow," Symantec Virus Bulletin,

2001.9.
[11] http://www.mines.uidaho.edu/ftp/pub/msdos/windows/utils/CodeRedScanner.EXE
[12] 전완근 외, 네트워크 필터링기법을 통한 CodeRed 웜 대응방법, http://www.certcc.or.kr/paper/tr2001/tr2001-08/CodRed%20Worm%20Virus.html

전 완 근

1998 한서대학교 전산정보학과(이학사)
2000 한서대학교 전산학과(이학석사)
2000~현재 한국정보보호진흥원 해킹바이러스상담지원센터 연구원
관심분야 : 컴퓨터 바이러스, 해킹, 인터넷 라우팅
E-mail : wkjeon@kisa.or.kr

임 재 명



1981 한양대학교 전자공학과(학사)
1983 한양대학교 전자공학과(석사)
1991 한양대학교 전자공학과(박사과정 수료)
2000~현재 한국정보보호진흥원 해킹바이러스상담지원센터 센터장
관심분야 : BIOS, 인터넷 네트워크 트래픽, QOS, RTOS, 컴퓨터 해킹, 바이러스
E-mail : jmlim@certcc.or.kr

이 중 식

2000 한서대학교 컴퓨터과학과(이학사)
2002 한서대학교 정보보호공학과(공학석사)
2002~현재 한서대학교 시간강사
관심분야 : 컴퓨터 바이러스, 정보보호, 네트워크 보안
E-mail : jslee@hanseo.ac.kr

이 종 일

2000 한서대학교 물리학과(이학사)
2002 한서대학교 정보보호공학과(공학석사)
2002~현재 한서대학교 시간강사
관심분야 : 정보보호, 무선 인터넷 보안
E-mail : jeeplee@hanseo.ac.kr

김 홍 윤

1982 인하대학교 전자계산학과(학사)
1984 인하대학교 전자계산학과(석사)
1996 인하대학교 전자계산학과(박사)
1995~현재 한서대학교 컴퓨터통신공학과 부교수
관심분야 : 인터넷 라우팅, 컴퓨터 바이러스, 인터넷 보안
E-mail : hykim@hanseo.ac.kr