Journal of Korea Multimedia Society Vol. 15, No. 2, February 2012(pp. 226-233)

윈도우시스템에서 새로운 선택적 에이전트 공격 기술에 관한 연구

김연우†, 임영환††, 박원형†††

요 약

최근에 발생한 3.4 DDoS 사이버 테러에서 볼 수 있듯이 사이버테러의 유형은 점점 복합화, 지능화, 대형화 되어가고 있고 사이버 위협 대상도 국가 전체로 확대되고 있다. 미래 사이버 테러를 대비하기 위해 기존에 시도되지 않았던 새로운 공격기법에 대해 미리 예상하고 구현하여 아직 드러나지 않은 시스템의 취약점을 공격자보다 앞서 인식할 필요가 있다. 본 논문에서는 윈도우 시스템에서 레지스트리 변조를 통해 사이버공격을 하는 것처럼 보이게 하는 새로운 사이버테러 공격 기법에 대해 연구한다. 제안하는 새로운 공격기법은 시스템의 레지스트리 default ttl값을 패킷의 송수신 시 필요한 값보다 작은 값으로 변조하여, 이동 중인 패킷이 중간에 폐기되도록 함으로써 에이전트(Agent)의 네트워크 연결을 제한한다.

A Study on New Selective Agent Attack Technology in Windows System

Yeong Woo Kim†, Young Hwan Lim††, Won Hyung Park†††

ABSTRACT

Recently, Like we saw with 3.4 DDoS Cyber Terror, a behavior of cyber terror becomes increasingly more complicated, sophisticated and larger, and there has been largely damage on industry, the general economy. For responding cyber terrors which occur in the future, we should recognize security holes of system which isn't exposed yet before attacker in advance as we anticipate and implement new technique of cyber attack which not exist hitherto. We design and implement a new technique of cyber attack; it seems to us that a server denies agent' service by altering value of registry in windows system. Network connections of agent are restricted to the new technique we suggest as the a value of registry is changed to a less value than a necessary value and there has happened packet loss by attacker.

Key words: Cyber Terror(사이버 테러), DoS Attack(서비스거부공격), Registry(레지스트리)

1. 서 론

우리나라는 인터넷 이용자 3,000만 명, 초고속 인터넷 가입자 1위, 무선 인터넷 사용 급증 등 최고 수준의 IT인프라를 자랑하며 정보화 시대를 선도하고 있다. 하지만 정보통신의 발달로 인해 국경의 개념이 희박해지고 우리의 생활과 관련된 모든 것이 사이버 공간과 융합되어감에 따라 컴퓨터 바이러스, 스팸메일 등 사이버테러로 인한 정보시스템의 파괴나 마비 또는 중요 정보의 누출과 같은 정보화의 역기능이

※ 교신저자(Corresponding Author) : 박원형, 주소:서울시 노원구 공릉동 서울과기대 프론티어관 303-1호, 전화: 02)970-6465 E-mail : infosecure@seoultech.ac.kr
접수일 : 2011년 8월 9일, 수정일 : 2011년 10월 10일
완료일 : 2012년 2월 28일

† 준회원, 고려대학교 정보보호대학원
(E-mail : ywkim0817@hanmail.net)
†† 준회원, 서울과학기술대학교 IT정책대학원
(E-mail : yhlim@seoultech.ac.kr)
††† 정회원, 서울과학기술대학교 산업정보시스템공학과

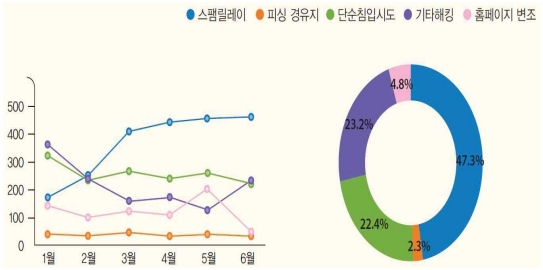

그림 1. 국내 인터넷 침해사고 현황[1,2]

심각한 문제점으로 부각되고 있다. 그림 1과 같이 최근 1년 동안 한국인터넷진흥원(KISA)에서 처리한 해킹사고는 해마다 증가추세를 보이고 있으며, 인터넷 이용 증대와 더불어 사이버테러 및 그 피해 규모는 더욱 증가할 것으로 보인다. 아래 표 1은 국내에서 발생한 대규모 사이버테러 현황을 나타내고 있다.

2003년에 발생한 '1.25 인터넷 대란'을 통해 알 수 있듯이 컴퓨터 바이러스는 네트워크로 연결되지 않은 이전의 컴퓨팅 시대보다 빠른 속도로 전파되었고, 9시간 동안 전국 인터넷망이 마비되는 사태가 발생하였다. 또한 2009년 7월 7일과 최근 발생한 3.4 DDoS공격은 청와대, 국회, 국방부, 국정원까지 국가 주요기관 26개 사이트가 무차별적 DDoS(Dis- trib-uted Denial of Service) 공격을 받았다. 위 사례에서 보듯이 국가·사회 기능의 전산시스템 의존도가 높은 우리나라는 사이버위협에 취약할 수밖에 없고 그에 따른 피해는 점점 커질 것으로 예상된다. 지금까지의 DDoS공격은 개인 사용자 PC의 보안 취약성을 이용하여 개인 사용자 PC를 좀비PC로 만든 후 다수의 좀비PC들로 하여금 대상 서버를 공격함으로써 네트워크 자원을 소모시키는 공격이 대부분 차지하고 있다. 본 논문에서 제안하는 새로운 공격기법은 특정 사이트를 공격하는 것이 아닌 취약한 개인 사용자 PC 즉, 에이전트를 공격하여 네트워크 서비스를 사용하지 못하게 함으로써 경제적·사회적 혼란을 유발한다. 다음은 새로운 개념의 에이전트 사이버 공격기법의 원리와 그 위험성에 대하여 알아보기에 앞서 기존 DDoS공격 및 TTL의 정의와 원리에 대해서 알아본다.

2. 관련연구

2.1 DDos공격

분산서비스거부(DDoS)공격이란 인터넷 서비스를 제공하는 기업(기관)의 운영 서버(웹서버, DNS서버 등)와 네트워크 장비(라우터, 스위치 등)에 임의의 조작된 공격성 트래픽을 전송하여 시스템 자체를 지연 혹은 마비시켜 사용자들이 인터넷 서비스를 이용할 수 없게 만드는 것을 말한다.

모든 인터넷 사용자는 TCP/IP 프로토콜을 이용하여 임의의 데이터 패킷을 발송자의 IP 주소(Source IP)를 가지고 목적지의 IP 주소(Destination IP)로 발송할 수 있다. 이때 이 IP주소에 대한 특별한 인증절차 없이 무제한적으로 대규모의 데이터 패킷을 전송할 수 있다는 것이 문제이며, DDoS 공격은 이러한 취약점을 악용하는 공격이다. 이는 공격 목표 호스트로 대량의 네트워크 트래픽을 발생시켜 대상 호스트의 네트워크 서비스 기능을 일시적 또는 완전히 정지시키는 공격의 유형으로 일반적인 DoS 공격보다 훨씬 더 강력한 파괴력을 지닌다[3]. DDoS 공격은 수백 혹은 수천 개의 좀비 시스템들을 이용해서 공격의 목적이 되는 시스템을 공격하는 형태를 띠고 있다. 수많은 좀비 시스템들은 공격 명령이 떨어지면 일제히 대상시스템을 공격하고 결국, DDoS 공격은 엄청난 볼륨의 패킷들을 발송하거나 불완전한 형태의 요청 패킷을 발송하여 공격 대상이 되는 네트워크 장비나 서버가 정상적인 서비스 요청을 받아들일 수 없는 상태, 혹은 자신의 능력으로 처리할 수 있는 용량을 초과하여 처리 불능의 상태에 이르게 한다.

표 1. 국내 사이버테러와 피해액 현황[3]

구 분	내 용
2003. 1. 25	마이크로소프트 윈도우 서버의 취약점을 이용한 슬래머 웜. 국내 8,800여대 PC 감염
2004. 7. 13	중국에서 유입된 악성프로그램으로 국회와 한국국방연구원 등 10개 기관 전산망 피해
2008. 2. 5	사이버 쇼핑몰 옥션에서 이용자 1,081명의 개인정보와 100만 명의 계좌번호 유출
2009. 7. 7	북한의 DDoS 공격에 의한 주요 정부기관, 민간 인터넷 사이트 공격, 장애발생
2011. 3. 4	북한의 DDoS 공격에 의한 주요 정부기관, 민간 인터넷 사이트 공격

표 2. IP 패킷 구조[4]

Version	IHL	Type Of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				

2.2. 시스템의 IP 헤더 구조와 TTL(time-to-live) 옵션

시스템에서의 IP 헤더 구조에 내포된 TTL(time-to-live)은 8 비트 길이의 IP패킷 헤더 내에 있는 패킷의 유효갯수를 나타내는 값으로, 최대 255까지의 정수 값으로 표시된다.TTL이 필요한 이유는 패킷의 무한루핑을 방지하기 위한 값으로서, 패킷이 버려지기 전에 허용되는 라우터의 통과횟수를 의미한다.

패킷이 라우터를 통과할 때마다 TTL값은 1씩 감소하게 되고 TTL값이 0이 되면, 라우터에서는 해당 패킷을 버리고, 재전송 여부를 결정하기 위해 ICMP 메시지가 발신 호스트로 보낸다. 일반적으로 TTL값은 운영체제에 따라 달라지는데 아래 표 3과 같다.

네트워크상의 거리가 먼 호스트에 패킷을 전송할 경우 적당한 큰 값으로 설정하여 패킷을 보내지 않으면 패킷이 목적지에 도달하기도 전에 폐기되기 때문에 정상적인 네트워크의 연결은 불가능하게 된다.

표 3. 운영체제별 TTL값 [5,6]

운영체제	ICMP Request 패킷	ICMP Reply 패킷
리눅스커널 2.2 이상	255	64
리눅스커널 2.0	64	64
FreeBSD	255	255
솔라리스	255	255
HP-UX	255	255
윈도우 95	32	32
윈도우 98	128	32
윈도우 NT	128	32
윈도우 2000	128	128
윈도우 XP	128	128
윈도우 VISTA	128	128
윈도우 7	128	128

3. 선택적 사이버 공격 기술

3.1 에이전트(Agent) 사이버 공격

취약한 PC를 봇넷으로 악용하여 특정 웹사이트 서버의 자원을 소모시키는 등 원활한 서비스를 하지 못하도록 공격하는 DDoS공격과 달리, 에이전트 공격은 개인의 PC를 직접 공격하여 네트워크 사용을 제한하는 Host기반의 서비스거부공격 기법이다.

에이전트 사이버공격은 패킷의 TTL(time-to-live)값이 0이 되면 폐기된다는 점을 악용하여, 사용자의 요청 패킷이 목적지(웹서버)까지 도달하지 못하고 중간에 폐기되도록 TTL값을 필요한 값보다 작은 값으로 변조한다.

패킷이 중간에 폐기되면 사용자와 목적지(웹서버)가 서로 연결이 되지 않아 사용자는 서비스 사용이 불가능하게 되고 이는 곧 기존의 DDoS공격을 받은 것과 유사한 효과를 나타나게 한다. 그리고 에이전트 공격으로 인해, 국내망을 유지한 채 오직 해외망만 단절시킬 수 있는데, 이것은 기존의 DDoS 공격과 차별화되는 피해양상으로 아래에서 자세히 다룬다.

3.2 에이전트(Agent) 사이버 공격

네트워크상에서 에이전트 공격이 어떻게 이루어지는 살펴보면 전반적인 흐름은 그림 2와 같다.

표 4는 그림 3의 흐름도 상에서 발생되는 사건에 대해 순차적으로 간략하게 설명하고 있다.

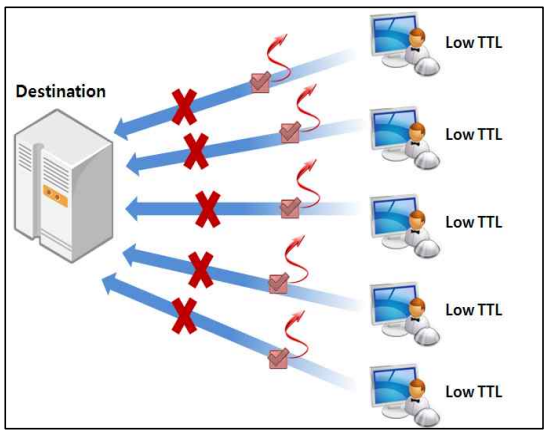

그림 2. 에이전트 사이버 공격 개념

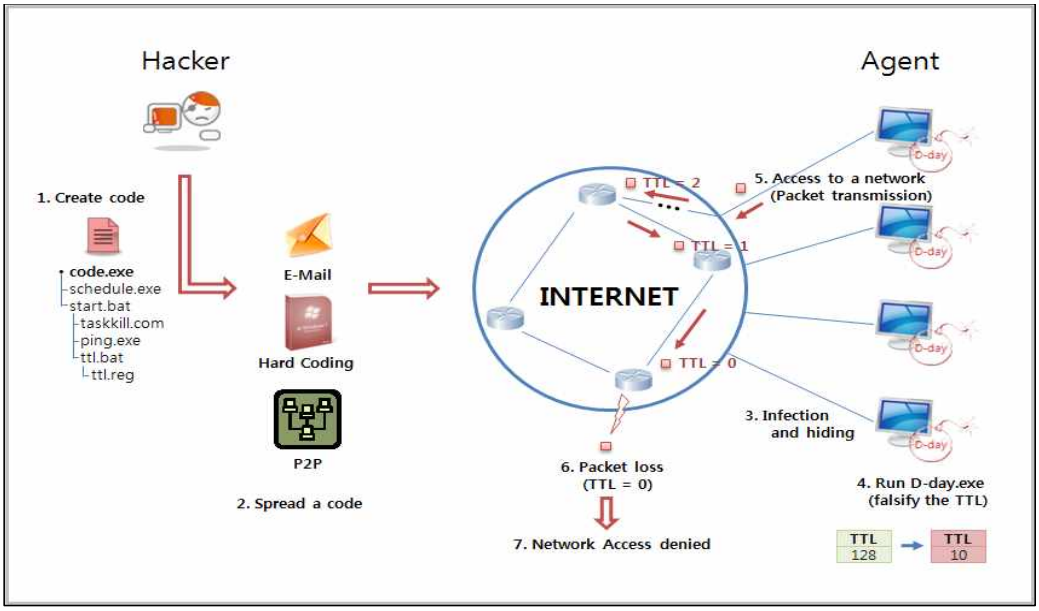

그림 3. Agent 공격 흐름도

표 4. 에이전트 공격의 흐름 순서

① 해커는 악성코드를 제작하고 다양한 경로(P2P, 웹 디스크 등)를 통해 악성코드 배포 ② 최초 감염 시 공격이 곧바로 실행되지 않으며 D-day까지의 잠복기간을 가짐 ③ D-day가 되면 TTL변조를 위해 숨겨진 악성코드 실행 ④ 감염된 에이전트에서 목적지 A로 네트워크 접속을 시도 ⑤ 패킷이 목적지까지 가지 못하고 손실(TTL값이 0이 되어 폐기) ⑥ 네트워크 사용 불가

다음은 위와 같은 에이전트 공격을 수행하기 위해서 필요한 악성코드의 구조와 역할, 그리고 동작에 대해 구체적으로 알아본다.

4. 호스트시스템에서 에이전트 사이버 공격 구현 및 평가

4.1 Agent 사이버공격 테스트 환경

테스트 환경은 아래 그림 5와 같이 구성하였다. Windows XP Professional SP3, Vista Home Edition 등 다양한 감염서버를 두고 실험하였으며 최신 윈도우 업데이트를 모두 완료한 상태이다. 또한

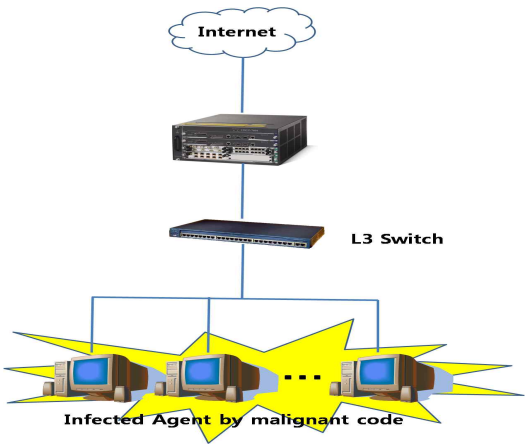

그림 5. 악성코드 테스트 환경 구조

우분트 리눅스, VMWare 기반의 안드로이드폰을 설치한다.

악성코드에 감염되고 공격이 실행되는 동안 백신 프로그램의 탐지는 전혀 나타나지 않았다. 아래 그림 6은 세계적으로 많이 사용되고 있는 백신 프로그램을 사용하여 우리가 작성한 악성코드 파일을 검사하여 나타난 결과이다. 대부분의 백신 프로그램에서 탐지하지 못하였고, 탐지가 된다 하더라도 치명적인 악성코드로 인식하지 못하였다. 이는 기존의 사이버테러에서 사용되었던 악성코드와 다르게 지극히 정상

그림 6. 다양한 백신 프로그램을 통한 공격 탐지 결과[7]

적인 코드로 이루어져 있기 때문인 것으로 이것은 백신 프로그램의 탐지를 자연스럽게 우회할 수 있게 하고 신속한 대응을 어렵게 한다. 즉, 이는 개인 PC 사용자들을 중심으로 한 공격 피해자들의 인터넷장애 현상을 상당시간 지속시킬 뿐만 아니라, 부차적으로 발생하는 경제적 손실 또한 증가시킨다.

4.2 윈도우시스템에서 사이버 공격 구현

윈도우에서 TTL 값을 변조 하기 위해서 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]의 레지스트리 를 변조해야 한다. 그림 7의 ping테스트 결과 Localhost의 TTL값이 128이므로 패킷의 송· 수신이 원활하여 인터넷을 이용하는데 지장이 없음을 알 수 있다.

TTL 값의 변조를 위해 그림 8과 같이 Tcpip\Parameters의 레지스트리에 DefaultTTL이라는 값이 추가되었다. 설정된 값은 10으로 그림 9의 ping 테스트 결과 TTL 값이 10으로 바뀌어있음을 알 수 있다. 이렇게 되면 TTL값이 필요한 값보다 작아 송신 패킷이 목적지까지 가지 못하고 소실되어 인터넷

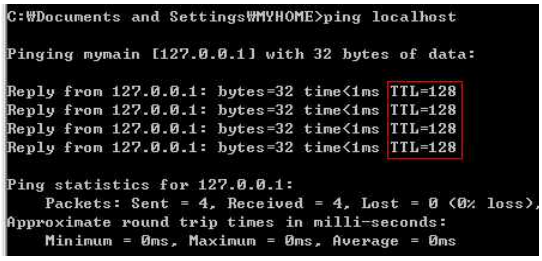

그림 7. Localhost ping 테스트

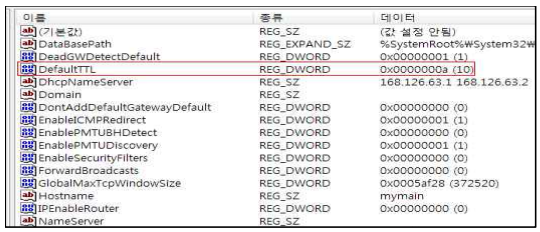

그림 8. 변조된 레지스트리 정보

그림 9. Localhost ping 테스트[8,9]

을 사용할 수 없게 된다.

에이전트 사이버공격으로 인한 인터넷 단절 현상은 간단한 ping테스트를 통해 쉽게 원인을 찾을 수 있다. 그리고 실제 인터넷에 접속하면 네트워크의 접속 제한으로 접속되지 않는다.

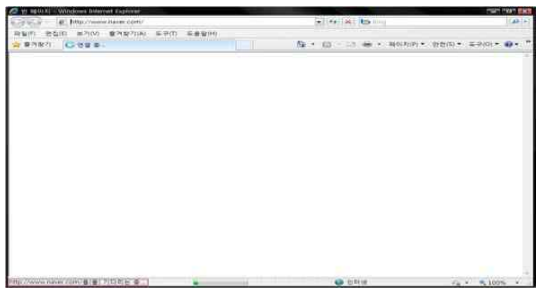

그림 10. 네트워크 접속 실패

4.3 호스트시스템에서 선택적 Agent 사이버공격 평가

에이전트 사이버공격은 위와 같이 감염된 사용자의 네트워크 마비 이외에도, 국내망과 해외망에서 요구되는 TTL값의 차이를 이용하여 오직 해외망만을 단절시킴으로써 네트워크상에서의 국제적인 고립상태를 만드는 공격도 수행될 수 있다.

아래의 표 5는 각 국가별로 선정된 대표적인 포털사이트를 나열한 것으로, 이를 바탕으로 TTL값에 따른 접속여부에 대해 분석했다.

실제 접속분석 결과 아래 그림 11과 같이 TTL값이 9에서 24일일 경우 국내외 사이트에 접속할 수

표 5. 국가별 포털 사이트 접속 여부

구분	사 이 트	국가
국내	www.bok.or.kr www.kbstar.com www.wooribank.com www.hanabank.com www.paran.com www.yahoo.co.kr www.freechal.com www.nate.com www.lycos.co.kr www.korea.com www.netian.com www.president.go.kr	한국
해외	www.google.com www.yahoo.com www.bankofamerica.com www.usbank.com www.nhk.co.jp www.boj.or.jp www.baidu.com www.boc.cn www.barclays.co.uk www.bundesbank.de www.indiatimes.com www.anz.com	미국 미국 미국 미국 일본 일본 일본 일본 영국 독일 인도 호주

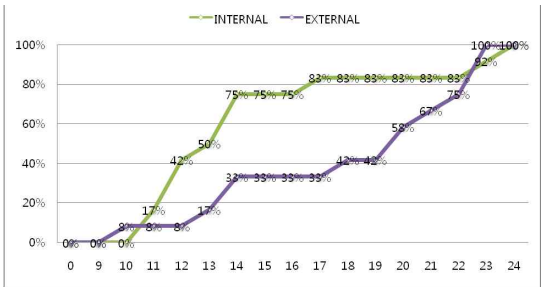

그림 11. 국내외별 TTL값에 따른 접속률

있었다. 이 중 TTL값이 17이상일 경우 접속률이 80%이상 되었으며, 해외 사이트는 TTL값 23이상이 되어야만 100% 접속이 가능하였다.

이러한 결과는 스케줄링기법과 접목되어 실제

표 6. 내부망과 외부망구분에 따른 접속여부

	접속 가능	접속불가능	합 계
국내	26	4	30
해외	11	9	20
합계	37	13	50

Agent공격 발생 시 피해 지속시간 및 대응시간을 현저히 증가시키는 중요한 요인이 된다.

다음은 통계적 기반의 가설검증이다. 귀무가설(H_0)과 대립가설(H_1)를 수립한다[10].

H_0 : 망구분과 접속여부는 연관성이 없다.
H_1 : 망구분과 접속여부는 연관성이 있다.

귀무가설을 간단히 표현하자면 '차이가 없을 것이다'라고 요약할 수 있다. 다르게 표현하면 "망구분과 접속여부는 무관할 것이다(독립성 검정)" 또는 "국내망과 해외망의 접속여부는 동일할 것이다(동질성 검정)"라고 할 수 있다[10].

문제에서는 내부망과 외부망의 종류와 접속 여부는 둘 다 질적 변수이고 이런 경우 두 질적 변수에 대한 독립성 여부, 즉 관련성 여부를 조사하는 검정통계량이 관측빈도와 기대빈도의 차를 이용해서 구한 카이제곱 통계량이다. 카이제곱 통계량의 경우 자유도는 각 변수의 수준수가 각각 r과 c 일 때 $(r-1)\times(c-1)$이 된다. 그러므로 자유도는 $(2-1)\times(2-1)=1$이 된다.

χ^2값은 자유도에 따라서 다양한 분포함수를 형태를 지니게 되는데 자유도가 커질수록 분포는 오른쪽으로 기울어지게 된다.

따라서 자료로부터 구한 χ^2값이 $\chi^2_{(r-1)(c-1),0.05}$ 값보다 작으면 관측빈도와 기대빈도의 차이를 우연히 발생한 차이를 보고 귀무가설을 채택하고, 자료로부터 구한 χ^2 값이 $\chi^2_{(r-1)(c-1),0.05}$ 값보다 그 차이가 우연으로 보기에는 너무 큰 차이이므로 "두 망 구분에 대한 접속여부의 차이가 없다"는 귀무가설을 기각한다. 이제 자료로부터 χ^2 값을 구해보면 관측빈도와 기대빈도는 다음과 같다.

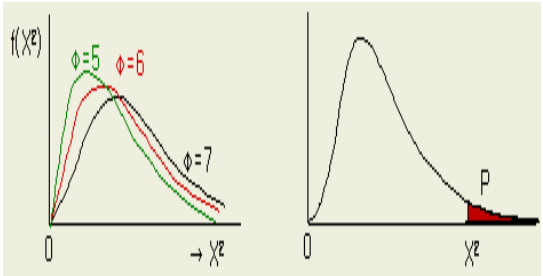

그림 12. χ^2 분포

표 7. 선택적 Agent 공격의 관측빈도 기대빈도

	접속 가능	접속불가능	합계
국내	26	4	30
해외	11	9	20
합계	37	13	50

표 8. 선택적 Agent 공격의 기대빈도

	접속 가능	접속불가능	합계
국내	22.2	7.8	30
해외	14.8	5.2	20
합계	37	13	50

χ^2값은

$$\chi^2 = \frac{(26-22.2)^2}{22.2} + \frac{(4-7.8)^2}{7.8} + \frac{(11-14.8)^2}{14.8} + \frac{(9-5.2)^2}{5.2}$$

= 6.254 이 된다.

유의수준 5%에서 기각치는 $\chi^2_{(r-1)(c-1),0.05} = \chi^2_{1,0.05}$=3.84 이다 자료에서 구한 χ^2값은 6.254로 기각치인 3.84보다 크므로 자료에서 나타난 두 망구분에 따른 접속여부 차이가 우연한 차이라고 보기에는 큰 차이이므로 “망구분과 접속여부는 연관성이 없을 것이다.”는 귀무가설은 기각된다. 즉, 내부망과 외부망과의 접속여부 연관성이 있는 것으로 확인 되었다.

5. 결 론

본 연구에서는 다수의 에이전트(좀비PC)를 이용한 웹서버로의 공격을 통해 해당 웹서버의 네트워크 자원을 소모시킴으로써 네트워크를 마비시키는 DDoS공격과는 달리 에이전트를 직접 공격하여 개개인 PC의 네트워크를 사용을 제한하는 새로운 사이버공격기법을 제안하였다.

제안한 에이전트 사이버공격기법은 개인 PC의 레지스트리 변조를 통해 PC에서 송신되는 패킷의 TTL값을 임의적으로 변경하여 패킷이 목적지까지 도달하지 못하고 중간에 폐기되도록 유도한 것으로, 송신되는 모든 패킷이 네트워크 중간에서 폐기되기 때문에 감염된 에이전트는 인터넷 사용이 불가능하게 된다. 특히, 스케줄링기법을 활용한 특정 시간의 인터넷 서비스 제한을 통해 에이전트 사이버공격의 효과를 극대화 할 수 있다.

에이전트 사이버공격을 구현하여 분석한 결과, 다수의 백신 프로그램에서 해당 공격을 탐지하지 못하는 것으로 나타났다. 뿐만 아니라 TTL값에 따라 부분적으로 인터넷 사용이 불가능한 현상이 나타남에 따라 공격의 파괴력을 높이고 더욱 혼란을 야기할 수 있다. 국민들의 저조한 보안의식으로 인한 개인 PC의 보안이 취약한 현실을 미루어볼 때, 사회 공학적 기법과 접목되어 에이전트 사이버공격이 국내에서 대규모로 감행될 경우 경제・사회적으로 큰 혼란을 유발할 수 있다. 따라서, 개인 PC의 직접적인 에이전트 사이버 공격에 대비한 대응방안에 대해 적극적으로 연구해야 한다. 향후에 라우터, IPTV, IP전화, 스마트폰 등을 공격하는 방법으로 진화될 제2, 제3의 사이버테러를 방지하기 위해서 국가차원의 사이버위협을 종합적으로 수집・분석하여 사전 방어대책을 수립해야 한다.

참 고 문 헌

[1] 인터넷침해대응센터, 인터넷침해사고동향 및 분석월보 7월호, http://www.krcert.or.kr, 2010.8

[2] 인터넷침해대응센터, 인터넷침해사고동향 및 분석월보 7월호, http://www.krcert.or.kr, 2011.8

[3] 이장균, 사이버테러의 상시 감시체제를 구축하자, 현대경제연구원, 2009.

[4] W. Richard Stevens, *TCP/IP Illustrated*, Addison-Wesley Professional. Vol.1. 1993.

[5] Default Time To Live(TTL) values, http://www.binbert.com/blog/2009/12/default-time-to-live-values/, 2009.12

[6] 정태명, 엄정호, 한영주, 박선호, 사이버 공격과 보안기술, 홍릉과학출판사, 2009.

[7] 바이러스·악성 S/W 검사 서비스, www.virustotal.com, 2011. 7

[8] ICMPmessages, http://www.networksorcery.com/enp/protocol/icmp.htm, RFC, 2011

[9] The Story on the PING Program, http://ftp.arl.mil/~mike/ping/html, 2008.

[10] 황현식, 통계적 가설검정, 통계교육원(http://sti.nso.go.kr), 2007.

김 연 우

현재 고려대학교 정보보호대학원 정보보호정책(석사수료)

관심분야 : 보안관제, 보안정책, 침해사고대응

임 영 환

2008년 서울과학기술대학교 산업대학원 정보산업공학과 석사

현재 서울과학기술대학교 IT정책전문대학원 산업정보시스템전공(박사과정)

관심분야 : 융합보안, 네트워크보안, 디지털포렌식

박 원 형

2009년 경기대학교 정보보호학과 (이학박사)

2011년 서울과학기술대학교 산업정보시스템공학과(겸임교수)

현재 극동대학교 정보경영학과 (전임교수)

관심분야 : 보안관제기술, 융합보안, 윈도우포렌식