평판을 이용한 새로운 DDoS 공격 대응 방안 연구

신정화* · 신원**

A New Defense against DDoS Attacks using Reputation

Jung-hwa Shin* · Weon Shin**

이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임
[NRF-2009-351-D00082]

요 약

최근 증가하고 있는 DDoS 공격은 공격자가 피해 시스템을 공격하기 전에 미리 좀비PC를 확보해 두어야 한다. 좀비PC는 악성 코드에 감염되어 악성코드 제작자의 의도에 따라 명령을 수행하는 PC로 사용자 자신도 모르게 다양한 불법 행위에 악용된다. 이에 본 논문에서는 보안이 취약한 개인 PC가 좀비PC로 악용되는 경우를 감소시키고 좀비 PC 가능성이 있는 개인 PC의 인터넷 접속을 사전에 차단함으로써 DDoS 공격의 피해를 줄일 수 있는 방안을 제안하고자 한다. 제안 방안은 개별 PC의 평판을 계산하여 계속적으로 인터넷 접속을 허용할지 말지를 판정한다. 또한, 각종 실험을 통하여 좀비PC가 확산되는 양상과 제안 방안을 적용함으로써 DDoS 공격 감소에 어떠한 영향을 끼치는지 분석하였다.

ABSTRACT

The DDoS attacks which are increasing recently must have many zombie PCs before attacking targeted systems by attacker. A zombie PC is infected by attacker's malignant code and may be operated by the his/her special malicious purposes. But most users generally don't know that their PCs are infected and used as zombies by illegal activities covertly. In this paper, we propose a new scheme that decreases vulnerable PCs and isolates them from Internet before being zombie PCs. The proposed scheme point the reputations of connected PCs and decide whether their Internet connections are keeping continuously or not. Also We show the figures how to infect susceptable PCs to zombie PCs, and analyze the decrease effects of DDoS attacks adapted by the proposed scheme with various experiments.

키워드
디도스 공격, 좀비 PC, 봇, 평판

Key word
DDoS attack, Zombie PC, Bot, Reputation

* 정회원 : 부경대학교 (주저자)
** 정회원 : 동명대학교 (교신저자, shinweon@tu.ac.kr)

접수일자 : 2011. 04. 04
심사완료일자 : 2011. 06. 14

Ⅰ. 서 론

최근 주요 인터넷 사이트들에 대한 공격은 여러 개의 호스트에서 IP망을 통해 특정 서버에 대량의 트래픽을 보내는 방식으로 공격 하고자 하는 서버를 다운시키거나 네트워크를 마비시켜 서비스를 중단시키는 분산 서비스 거부(Distributed Denial of Service, 이하 DDoS) 공격을 사용하고 있다. DDoS 공격은 최근에 발생한 신종 공격 기법이 아니다. 이미 1990년대 말부터 발생하기 시작하여 지난 2000년 야후, 아마존 등 유명 웹사이트에 대한 대대적인 DDoS 공격이 발생하였고, 막대한 피해자가 발생하기도 했다.

DDoS 공격은 공격자가 피해 시스템을 공격하기 전에 미리 좀비(zombie)PC를 확보해 두어야 하며, 이를 기반으로 공격자가 공격 명령을 내리면 좀비PC 또는 서버들이 일제히 피해 시스템에 다량의 트래픽을 보내어 서버를 다운시키거나 네트워크를 지연시켜 서비스를 불가능하게 만든다. 즉, 수 만에 달하는 여러 대의 컴퓨터를 동작하게 하여 특정 웹 사이트에 동시에 접속함으로써 해당 사이트의 시스템 과부하를 유발해 정상적인 서비스를 할 수 없는 상태가 되도록 만든다[1][2].

좀비PC는 악성 코드에 감염되어 악성코드 제작자의 의도에 따라 명령을 수행하는 PC를 말하며 로봇 프로그램의 일종인 악성 봇(Bot)에 감염되어 사용자 자신도 모르게 다양한 불법 행위에 악용된다[3]. 악성 봇에 감염된 좀비PC는 사용자도 모르게 DDoS 공격에 이용돼 특정 사이트로 대량의 트래픽을 전송하는 역할을 한다. 또한 좀비PC는 사용자가 모르는 사이에 다른 사람에 의해 원격 조정되며, DDoS 공격뿐만 아니라 불법 프로그램의 유포, 스팸메일 발송, 개인 정보 유출 및 스파이웨어 설치 등에 악용될 수 있다. 이 중 특히 DDoS 공격이 최근 들어 더욱 심각해지고 있는 실정이다.

2009년 7월 7일 청와대, 국회, 국방부, 국가정보원까지 국가 주요기관 26개 사이트가 무차별적인 DDoS 공격을 받았다. 한국경제연구원의 'DDoS 사이버 테러의 피해와 대책' 보고서에 따르면 7.7 DDoS 대란의 금전적인 피해금액은 최소 363억 원에서 544억 원에 이를 것으로 추정하고 있다[4]. 2011년 3월 3일~4일 이틀간 청와대, 국가정보원을 포함해 은행, 증권사 등 국내 40개 주요 대형 웹 사이트를 대상으로 한 DDoS 공격이 또다시 발생했다[5]. 국가, 사회 기능의 전산 시스템 의존도가 높아지면서 사이버테러에 의한 피해는 향후 다양한 형태로 발생할 것으로 예상된다.

최근 지능화되고 고도화된 형태의 DDoS 공격을 쉽게 탐지하고 차단하기가 어렵지만 DDoS 공격에 이용되는 좀비PC의 수를 줄이는 것만으로도 DDoS 공격의 피해를 최소화할 수 있을 것이다. 따라서 DDoS 공격을 사전에 차단하기 위한 방법으로 개인 PC의 보안을 강화하여 좀비PC가 되지 않도록 예방하는 것이다. 이는 곧 보안이 취약한 개인 PC가 좀비PC로 활용될 가능성이 높다는 것을 의미한다.

이에 본 논문에서는 개인 PC의 평소 보안 업데이트 여부에 따라 가중치를 부여하고 평판(Reputation)을 계산하여 좀비PC 가능성이 있는 개인 PC의 인터넷 접속을 차단하여 개인 PC가 좀비PC로 악용되는 경우를 감소시키고자 한다. 평판은 객체의 과거 행동에 대한 피드백을 수집하여 객체의 신뢰도 평가를 목적으로 사용하는 정보이다[6]. 인터넷 서비스 제공 업체(Internet Service Providers, 이하 ISP)는 개인 PC가 인터넷 접속을 요청할 때 해당 PC의 평판을 참조하여 인터넷 접속을 차단하거나 허용 여부를 결정하여, DDoS 공격의 피해를 줄일 수 있음을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 네트워크 접근 제어 방법을 살펴보고 3장에서는 좀비PC 가능성이 있는 개인 PC의 인터넷 접속을 차단하여 개인 PC가 좀비PC로 악용되는 경우를 감소시키기 위한 제안 방안을 설명한다. 4장에서는 실험을 통해 제안 방안의 효율성을 살펴보고, 5장에서 결론을 맺는다.

Ⅱ. 관련연구

한국인터넷진흥원의 2011년 1월 인터넷 침해사고 동향 및 분석 월보에 따르면 좀비PC망인 봇넷의 국내 감염률은 지난해 전 세계에서 평균 1% 정도였으며 1월에는 0.5%로 분석됐다. 하지만 좀비PC 감염 위협은 상당히 높은 수준으로 나타나 좀비PC를 만들기 위한 악성코드 전파를 목적으로 하는 TCP/455 및 TCP/139 포트에 대한 스캔 비율이 계속적으로 높은 수준을 유지하고 있는 것으

로 확인되었다[7]. 이에 보안 업계와 전문가들은 사용자들의 컴퓨터가 좀비PC가 되는 것을 막기 위해 운영체제 등의 보안 업데이트 패치를 최신 상태로 유지하고 보안 소프트웨어를 실시간으로 사용해야 한다고 권고하고 있다.

또한, 네트워크 접근 제어(Network Access Control, 이하 NAC)는 네트워크에 접근하는 접속 단말의 보안성을 강제화할 수 있는 보안 인프라(하드웨어 및 소프트웨어)로써 2009년 발생한 7.7 대란 이후 DDoS 공격의 원동력인 좀비PC의 방지, 네트워크 액세스 단의 보안 강화가 시급한 보안 선결책으로 떠오르면서 비인가 사용자의 접근 제어, 백신 업데이트 기능을 가진 NAC 솔루션 도입이 활발히 진행되고 있다[8]. NAC의 핵심 기능은 내부 네트워크를 접근하는 단말기에 대한 인증 및 통제로 허가되지 않거나 웜, 바이러스 등 악성코드에 감염된 PC 또는 노트북, 모바일 단말기 등이 회사 네트워크에 접속되는 것을 원천적으로 차단해 시스템 전체를 보호하는 기법이다.

그러나, NAC 솔루션을 이용할 경우 기업 내 PC는 기업 관리자에 의한 통제가 가능하지만 보안이 미비한 일반 개인 사용자의 접속을 제한하는 것은 현실적으로 무리가 있다. 이에 본 논문에서는 평판(Reputation) 개념을 활용하여 좀비PC로 동작하거나 좀비PC 가능성이 있는 개인 PC의 인터넷 접속을 차단하는 방법을 제안하고자 한다.

Ⅲ. 평판을 이용한 DDoS 공격 대응 방안

본 논문에서는 DDoS 공격에 대한 대응 방안으로 좀비PC 가능성이 있는 PC들의 인터넷 접속을 사전에 차단하기 위해 평판 개념을 적용하여 좀비PC의 인터넷 접속을 차단하는 방법을 제안한다. 평판은 객체의 행동을 기반으로 계산되는 값으로 실생활에서 미래에 일어날 객체의 행동을 예상하는데 도움을 줄 수 있다. 또한 평판은 객체가 미래에 어떻게 행동하는가에 영향을 미치므로 객체는 자신의 평판을 현재 상태로 유지하거나 향상시키기 위해 정당하게 행동하려고 할 것이다.

제안 방안에서는 평판이 가지는 이러한 성질을 참조하여 개인 PC가 평소 백신 프로그램을 설치하고 주기적으로 운영체제 보안 업데이트와 백신 업데이트, 실시간 감시를 수행하고 있는지 여부를 확인한 후 업데이트 종류별로 가중치를 부여하여 평판을 계산한다. 인터넷서비스제공업체(ISP)는 인터넷 접속을 요청하는 개인 PC들의 평소 보안 업데이트 상태를 알 수 없기 때문에 좀비PC 가능성이 있거나 좀비PC로 동작 중인 PC라 하더라도 인터넷 접속 차단이 어려운 경우가 많다.

이에 제안 방안에서는 개인 PC가 인터넷 접속을 요청할 때 ISP는 먼저 해당 PC의 평판을 확인하고 인터넷 접속을 허용하거나 차단한다. 그림 1은 본 논문에서 제안하는 평판을 이용한 DDoS 공격 대응 방안의 기본 동작을 나타내고 있다. 사용자 PC에서 ISP로 인터넷 접속 요청이 들어올 때 ISP 내에 존재하는 에이전트에 의해 사용자 PC의 평판을 확인한다. 평판이 1보다 크거나 같다면 보안 어플리케이션 설치 및 보안 업데이트 적용이 적절한 상태이므로 인터넷 접속을 허용하고, 그렇지 않은 경우 보안 업데이트가 미흡한 상태로 판단하여 인터넷 접속을 차단한다.

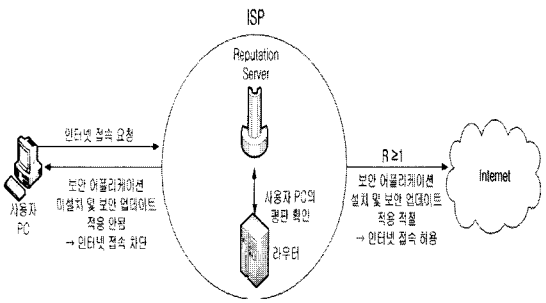

그림 1. 제안 방안의 동작 방식
Fig. 1 Overview of proposed scheme

ISP 내에서 일어나는 세부적인 동작을 살펴보면 다음과 같다. 개인 PC가 인터넷 접속을 요청할 때 ISP 내에 존재하는 에이전트는 먼저 표 1에 명시된 보안 점검 항목들의 설치 여부를 확인한다.

표 1. 보안 점검 항목
Table. 1 Security check list

보안 점검 항목	파라메터	가중치
(1) 운영체제 및 어플리케이션의 보안 업데이트 … A	α	0.50
(2) 보안 어플리케이션 설치 ① 보안 어플리케이션의 최신 업데이트 … B ② 보안 어플리케이션의 실시간 감시 기능 동작 … C	β γ	0.25 0.25

ISP 내의 에이전트는 표 1의 보안 점검 항목의 설치 여부를 기반으로 표 2와 같이 8가지 경우로 나누어 개인 PC의 보안 설정 상태를 점검한다.

표 2. 보안 점검 항목에 따른 분류
Table. 2 Classified groups by security check list

Case	A	B	C	가중치	그룹
1	○	○	○	1.00	G1
2	○	○	X	0.75	G2
3	○	X	○	0.75	
4	○	X	X	0.50	G3
5	X	○	○	0.50	
6	X	○	X	0.25	G4
7	X	X	○	0.25	
8	X	X	X	0.00	G5

보안 설정 상태에 따라 표 1에 명시된 가중치를 부여하고 식 (1)을 이용하여 해당 PC의 평판을 계산한다.

$$R=\alpha+\beta+\gamma \tag{1}$$

식 (1)의 계산 결과를 식 (2)에 적용하여 인터넷 접속을 요청한 PC의 보안 상태 값이 t이상일 경우 인터넷 접속을 허용하고, 미만인 경우는 인터넷 접속을 차단한다.

$$\begin{cases} R \geq t, & \text{인터넷 접속 허용} \\ R < t, & \text{인터넷 접속 차단} \end{cases} \tag{2}$$

예를 들어, $t=0.50$인 경우 표 2에 명시된 보안 점검 항목의 설치 여부를 결정 트리(Decision Tree) 형태로 표현하면 그림 2와 같다.

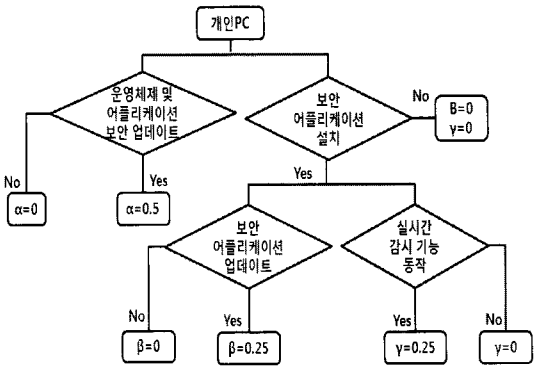

그림 2. 보안 점검을 위한 결정 트리 표현
Fig. 2 Decision tree for security check

Case 1의 경우 운영체제 및 어플리케이션 보안 업데이트를 수행하고 보안 어플리케이션 설치 후 최신 업데이트를 수행하였고 실시간 감시 기능까지 동작시키고 있다. 식 (1)의 계산에 따라 '1.0'의 평판을 가지므로 인터넷 접속이 가능하다. Case 3의 경우 운영체제 및 어플리케이션 보안 업데이트를 수행하고 보안 어플리케이션 설치 후 최신 업데이트는 않고 실시간 감시 기능만 동작시키고 있지만 식(1)의 계산에 따라 '0.75'의 평판을 가지므로 인터넷 접속이 가능하다. Case 5의 경우 운영체제 및 어플리케이션 보안 업데이트를 수행하지 않고 보안 어플리케이션 설치 후 최신 업데이트를 수행하고 실시간 감시 기능을 동작시키고 있지만 식 (1)의 계산에 따라 '0.50'의 평판을 가지므로 인터넷 접속이 가능하다. Case 7의 경우 운영체제 및 어플리케이션 보안 업데이트를 수행하지 않고 보안 어플리케이션 설치 후 최신 업데이트를 수행하지 않고 실시간 감기 기능을 동작시키고 있지만 식 (1)에 의해 '0.25'의 평판을 가지므로 인터넷 접속이 차단된다.

Ⅳ. 실험 및 분석

제안 방안에 대한 실험을 수행하기 위해 다음과 같이 가정한다. 첫째, SI 모델[9]과 개선된 SI 모델[10]에 따라

좀비PC가 확산한다고 가정하고 확산율은 시간당 백만분의 1로 둔다. 둘째, 좀비PC가 국내 인터넷 환경에서 확산하고, 해당 네트워크의 호스트의 취약성을 이용하여 확산한다고 가정한다. 셋째, 각 호스트는 평균 인터넷 속도를 최대 대역폭으로 하는 단일 네트워크로 구성되었다고 가정한다. 참고로, 2011년 2월 Akamai에서 조사한 인터넷 평균 속도 측정 결과에 따르면 한국이 17.632Mbps로 조사되었다[11].

4.1. 기본 조건에서 좀비PC 확산 실험

그림 3은 취약한 전체 호스트 수(N)를 $N=100,000$으로 두고, 최초 악성 봇 감염 호스트 수를 1대로 두고 SI 모델에 의해 현재 우리나라의 인터넷 평균 속도에 맞추어 확산 실험한 결과이고, 그림 4는 감염된 호스트가 발생하는 트래픽을 나타낸다.

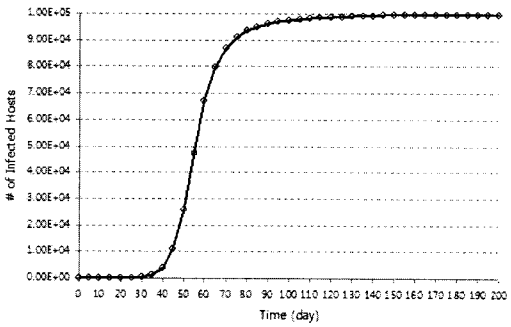

그림 3. 좀비PC의 확산
Fig. 3 Spread of zombie PCs

취약한 100,000대의 PC가 시간당 1/1,000,000 비율로 감염된다고 가정하면, 약 200일 후에 모두 감염된다는 사실을 그림 3에서 확인할 수 있다.

지난 7.7 대란에서 발생한 트래픽을 적용하여 분석하여 보면, 각 호스트 당 64~256 바이트의 패킷을 초당 1,800개 발생시켜 150개의 커넥션을 설정하여 20개 정도의 사이트에 전송하는 것으로 조사되었다. 즉, 한 호스트가 한 사이트에 초당 8개의 커넥션을 열고 64~256 바이트의 패킷을 90개 전송하므로 각 사이트에 46,080~184,320비트를 전송하는 것을 확인할 수 있다. 이를 실험한 결과 모든 감염 호스트가 발생시키는 트래픽의 하한과 상한은 그림 4와 같다.

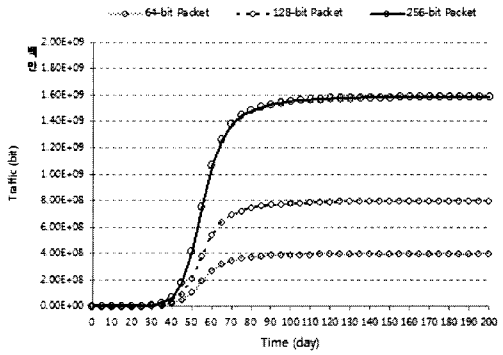

그림 4. 좀비PC의 확산에 따른 발생 트래픽
Fig. 4 Spreading traffics of zombie PCs

4.2. 그룹별 좀비PC 확산 실험

표 2의 보안 점검 항목에 따라 구분된 그룹 G1~G5에서 좀비PC 확산 실험 결과는 그림 5와 같고 발생 트래픽은 그림 6과 같다.

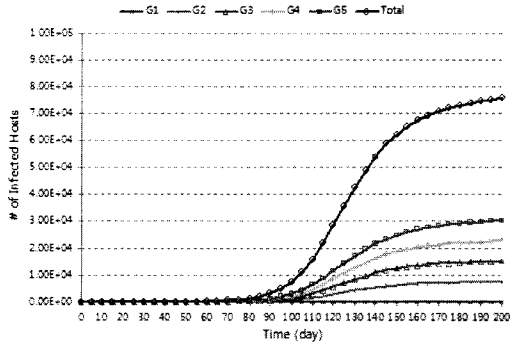

그림 5. 그룹별 좀비PC 확산
Fig. 5 Spread of zombie PCs by groups

표2의 보안 점검 항목에 따른 여러 가지 경우를 G1~G5 다섯 그룹으로 나누어 앞의 실험과 같은 조건으로 실험한 결과 G1 그룹은 안전하므로 감염되지 않는 그룹이고, G2~G5는 보안 설정 상태에 따라 각기 다른 속도로 좀비PC가 확산되는 것을 확인할 수 있다.

앞의 실험과 마찬가지로 모든 감염 호스트가 발생시키는 트래픽은 그림 6과 같다.

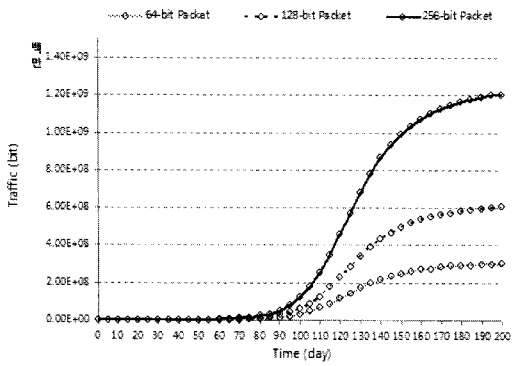

그림 6. 좀비PC 확산에 따른 그룹별 발생 트래픽
Fig. 6 Spreading traffics of zombie PCs by groups

4.3. 그룹별 좀비**PC** 확산 차단 실험

제안 방안을 적용하여 취약한 PC를 R에 의해 시간당 백분의 1 비율로 150일 시점에 차단한다고 가정하면, 그 결과는 그림 7과 같다.

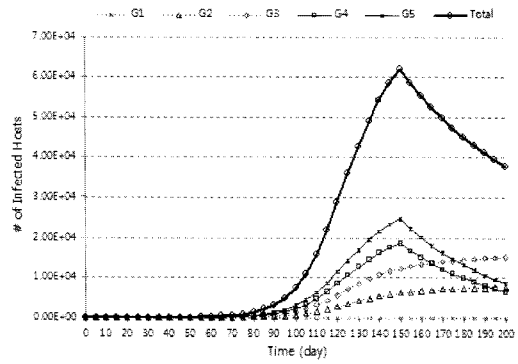

그림 7. 제안 방안을 적용한 좀비PC 확산 차단
Fig. 7 Spread of zombie PCs by proposed scheme

$t=0.3$의 경우 제안 방안을 적용하면, 좀비PC 확산율이 가장 높은 G4($R=0.25$)와 그룹 G5($R=0.00$)의 좀비PC 확산이 감소하므로 증가세가 전체적으로 줄어들고 있음을 확인할 수 있다.

제안 방안을 적용하여 좀비PC 확산을 차단하면 $t=0.3$의 경우 그림 8과 같고, $t=0.6$의 경우 그룹 G3 ($R=0.50$), 그룹 G4($R=0.25$), 그룹 G5($R=0.00$)의 좀비PC의 확산이 감소하고, $t=0.9$의 경우 G1 ($R=1.00$)을 제외한 모든 그룹의 좀비PC 확산이 감소한다. 즉, t를 높이면 높일수록 전체적인 좀비PC 확산의 감소세가 증가함을 확인할 수 있다.

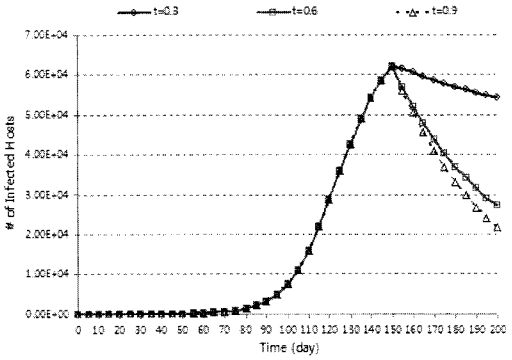

그림 8. t에 의한 좀비PC 인터넷 연결 차단
Fig. 8 Internet connection of zombie PCs by t

V. 결 론

초고속 인터넷을 제공하는 통신사나 주요기반시설을 운영하는 기업・공공기관 등에는 상당한 사이버 보안 대책이 마련되어 있지만 최근 악성코드에 감염된 개인 PC, 즉 좀비PC를 악용해 DDoS 공격이나 PC 내 자료 유출, 스팸 발송 등 2차 공격을 감행하기 때문에 적절한 대응이 어렵다. 인터넷의 발달과 정보의 공유로 악성코드나 웹 해킹의 피해는 날이 갈수록 심각해지고 있다. 피해 유발 기능이 점점 더 악성화 되어 가는 것은 물론이고 안티 백신 프로그램이나 침입탐지시스템 등 보안 제품으로부터 자신을 숨기고 보호하려는 자기방어 기능이 포함된 지능적 악성코드들도 점점 늘어가고 있다. 결국 이에 대응하는 보안 기술의 발전도 중요하겠지만 PC를 사용하는 사용자들의 노력이 절실히 요구된다. 기본적이지만 실천이 되지 않고 있는 백신 프로그램 설치와 윈도우 보안 업데이트만으로도 자신의 PC를 DDoS 공격으로부터 안전하게 관리할 수 있을 것이라 생각된다.

참고문헌

[1] T. Peng, C. Leckie, K. Ramamohanarao, "Survey of Network-based Defense Mechanism Countering the DoS and DDoS Problems," ACM Computing Surveys, Vol. 39, No. 1, April 2007.

[2] J. Mirkovic, P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM COmputer Communication Review, Volume 34, Issue 2, pp. 39-53, April 2004.

[3] E. Cooke, F. Jahanian, and D. McPherson, "The Zombie Roundup: Understanding, Detecting, and Distrupting Botnets," In Proceeding of Usenix Workshop on Steps to Reducing Unwanted Traffice on the Internet(SRUTI'05), pp.39-44, 2005.

[4] 한국경제연구원, "DDoS 사이버 테러의 피해와 대책," 2010

[5] 보안뉴스, http:/www.boannews.com

[6] S. Marti, H. Garcia-Molina, "Taxonomy of Trust: Categorizing P2P Reputation Systems," Computer Networks, Volume 50, Issue 4, pp.472-484, 2006.

[7] 인터넷 침해사고 동향 및 분석 월보, 한국인터넷 진흥원, 2011년 1월

[8] 노철우, 강경태, 이지웅, 전재현, "NAC(Network Access Control)을 이용한 컴퓨터 네트워크 보안 플랫폼 구성," 한국콘텐츠학회 춘계 종합학술대회 논문집, 제7권 제1호, pp.8-11, 2009.

[9] H. W. Hethcote, "The Mathematics of Infectious Diseases," SINA Review, Vol. 42, No. 4, pp.599-653, 2000.

[10] 신원, 이경현, "인터넷 환경에서 웜 확산 모델의 제안과 분석," 정보보호학회논문지, 제16권, 제3호, pp.165-172, 2006

[11] http://www.akamai.com

저자소개

신정화(Jung-Hwa Shin)

2011.3~현재 부경대학교 전자정보통신연구소 연구원
2006. 8 부경대학교 전자계산학과 이학박사

※관심분야 : P2P 보안, 평판 관리, 봇넷

신원(Shin, Weon)

2005.3~현재 동명대학교 정보보호학과 부교수
2002.3~2005.1 (주)안철수연구소 선임연구원

※관심분야 : 악성코드 확산, 디지털 포렌식, 소프트웨어 보안