Journal of The Korea Society of Computer and Information
Vol. 17 No. 6 , June 2012

2012-17-6-3-7

DHCP를 이용한 악성 봇 치료 기법

김 홍 윤*

A Malicious Bot Curing Technique Using DHCP

Hong-Yoon Kim*

요 약

본 논문에서는 악성 봇 치료 백신을 설치하지 않는 컴퓨터에게 DHCP 서버가 IP 주소를 제한적으로 공급하는 기법을 제안하여, 불편을 느낀 사용자들이 악성 봇 치료에 적극적으로 참여하도록 유도하고자 한다. DHCP 서버는 IP 주소를 제한적으로 공급하기 위하여 주기적으로 사용자 컴퓨터에게 백신 설치 확인 요청을 한다. 이 기법은 특정 시스템이나 조직에 종속되지 않아서 효율적인 악성 봇 치료가 가능하다.

▸ Keyword : 악성 봇, 백신, DHCP

Abstract

In this paper, a technique wherein the DHCP server has a restriction in providing the IP address to the computers that has no malicious bot curing vaccine is proposed, so that users will cooperate in the curing of malicious bot to avoid inconvenience. In order to provide restricted ip address periodically, the DHCP server makes a request of vaccine installation check for user's computer. Proposed technique is effective in the curing of malicious bot, because it does not depend on specific systems or organizations.

▸ Keyword : Malicious Bot, Vaccine, DHCP

• 제1저자 : 김홍윤 • 교신저자 : 김홍윤
• 투고일 : 2012. 05. 21, 심사일 : 2012. 06. 13, 게재확정일 : 2012. 06. 20.
* 한서대학교 컴퓨터공학과(Dept. of Computer Science, Hanseo University)

I. 서 론

인터넷이 전 세계로 활발하게 보급되면서 인터넷을 통한 각종 온라인 서비스를 편리하게 이용할 수 있게 되었다. 그러나 이러한 편리함의 역 기능으로 인터넷을 통한 사이버 공격이 국가 안보적인 차원에서 심각한 문제가 되고 있다[1]. 사이버 공격자들은 수천에서 수만 대의 좀비 PC 들로 구성된 악성 봇넷으로 주요 시스템에 DDoS 공격을 하고 공격 시스템 정보와 네트워크 이용경로 및 공격기법 등의 정보를 소멸시킴으로써 증거를 인멸한다.

이러한 DDoS 공격에 대응하기 위하여 7.7 DDoS 이후 인터넷진흥원과 전자통신연구원은 DDoS 탐지 및 악성 봇넷 탐지 기술과 악성코드 수집 및 분석 기술을 중심으로 국가적 통합 보안관제 체계를 구축하고 있다. 또한 네트워크 측면에서의 대응은 ISP에 통보하여 봇넷 C&C 서버로의 접속을 차단하고 네트워크 보안 장비를 이용하여 유해 트래픽을 차단하는 기법[2]을 사용하고 있다. 이 기법에서는 좀비 PC의 치료는 하지 않고 있다. 7.7 DDoS나 3.4 DDoS 사례와 같이 좀비 PC의 근본적인 치료를 하지 않은 환경에서, 통합 보안관제 체계와 ISP에서 대응하는데 한계가 있다[3].

좀비 PC를 근본적으로 치료하기 위하여 일본의 사이버클린센터 CCC(Cyber Clean Center)는 허니 넷을 공격하여 악성 봇을 전파한 IP 사용자에게 감염사실을 알리고, 사용자는 악성 봇 치료 홈페이지에 접속하여 백신 프로그램을 다운로드 받아 치료하였다. 악성 봇에 감염된 좀비 PC를 사용자가 백신으로 치료를 하도록 안내하여 악성 봇을 제거할 수 있어서 근본적인 취약점 제거가 가능하다는 장점이 있다.

그러나 이 기법은 사용자들의 비협조적인 참여로 감염 사실을 통보 받은 PC 중 30% 가량만 치료 페이지를 방문하여 치료하고 있다. 나머지 사용자들은 감염사실을 알고 있음에도 아무런 조치를 하지 않아, 좀비 PC가 여전히 악성행위를 수행하는 문제가 있다[4].

이 문제를 개선하기 위하여 본 논문에서는 사용자가 적극적으로 악성 봇 치료를 하는 기법을 제안한다. 이 기법에서는 악성 봇 치료에 비협조적인 사용자에게 IP 주소를 제한적으로 제공하여 사용자가 불편을 느끼는 환경을 제공한다. 이에 따라 불편을 느낀 사용자가 악성 봇 치료에 능동적으로 참여하도록 유도하고자 한다.

본 논문은 다음과 같이 구성되어 있다. 먼저 2장에서 DNS 싱크홀 차단 기법과 사이버클린센터 치료 기법등 기존의 악성 봇 대응 기법들의 장점 및 단점에 대해 살펴보고, 3장에서는 본 논문에서 제시한 사용자가 능동적으로 악성 봇을 봇 치료 하는 기법을 제시하며, 4장에서 기존 기법과 본 논문에서 제안한 기법을 비교 분석하고, 5장에서는 결론과 함께 본 논문을 마치도록 한다.

II. 봇 넷 대응 기법

주요 시스템에 DDoS 공격을 하는 악성 봇 대응 기법으로 봇 헌터(Bot Hunter), 봇 마이너(Bot Miner), 봇 스니퍼(Bot Sniffer) 등이 제안되었다. 그러나 봇 행위에 대한 프로파일을 주기적으로 갱신해주어야 하는 문제, 화이트 리스트 기반으로써, 봇 넷의 통신이 주요 화이트 리스트를 사용하여 이루어지거나, 암호화된 통신이 긴 주기를 가지는 봇 넷의 경우 탐지가 힘들다는 한계가 있다[5]. 또한 악성 봇도 빠른 속도로 진화하여 탐지/대응을 매우 어렵게 하고 있다. 감염 경로도 기존의 시스템 취약점을 이용한 방식에서, 웹, 이메일, 메신저 등 다양해지고 있다.

이에 따라 악성 봇을 국가적으로 대응하기 위하여 한국은 인터넷진흥원에서 DNS 싱크홀 시스템을 운영하고, 일본에서는 사이버클린센터 CCC(Cyber Clean Center)를 운영하고 있다.

1. DNS 싱크홀 차단 기법

한국인터넷진흥원에서는 국내 관련 업체와 협조하여 악성 봇에 감염된 좀비 PC를 해커가 조종하지 못하도록 해커와 좀비 PC의 연결을 차단하는 DNS 싱크홀 시스템을 운영하고 있다. DNS 싱크홀은 악성 봇에 감염된 좀비 PC가 해커와 연결을 시도할 때 해커의 시스템 대신 한국인터넷진흥원의 싱크홀 서버로 연결하도록 하여 해커로부터 악용당하지 않도록 해주는 시스템이다.

악성 봇은 취약점을 가지고 있는 PC에 전파되며, 감염 시 해커가 지정해 놓은 명령/제어 서버에 접속하여 해커로부터의 명령을 기다린다. 이렇게 악성 봇 감염 PC가 접속하는 해커의 서버를 악성 봇 명령/제어 서버라고 하며, 명령/제어 서버와 감염 PC 들로 구성된 네트워크를 봇 넷(Bot Network)이라고 한다. 악성 봇 명령/제어 서버는 이러한 악성 행위의 중심에 있으며, 악성 봇 명령/제어 서버의 차단만으로도 해커로부터의 명령 전달을 방지할 수 있어 악성 봇의 악성 행위를 효과적으로 막을 수 있다. 악성 봇에 감염된 좀비 PC가 명령/제어 서버에 접속하기 위해서는 <그림 1>과 같이 악성 봇 서버의 도메인에 대한 IP를 얻기 위하여 감염 PC가 사용하는

DNS 서버에 질의를 하게 된다. 이때 DNS 서버에서는 해당 도메인을 관할하는 DNS 서버에게 IP를 받아와서 감염 PC에게 알려주고 감염 PC는 응답받은 IP로 접속하는 과정을 거치게 된다.

그러나 악성 봇 DNS 싱크홀이 적용된 DNS 서버의 경우에는 사전에 악성 봇 명령/제어 서버로 알려진 도메인은 감염 PC로부터 DNS 질의를 받을 때 해당 도메인을 관할하는 DNS 서버에게 물어보지 않고 직접 특정 IP(싱크홀 서버 IP)를 응답하게 되고, 감염 PC는 해커의 서버 대신에 싱크홀 서버로 접속하게 된다. 악성 봇에 감염된 좀비 PC는 명령/제어 서버로의 접속이 차단되므로 더 이상 악성 행위를 할 수 없게 된다. 악성 봇 DNS 싱크홀은 감염 PC의 사용자가 보안에 대한 지식이 없더라도 감염 PC가 사용하는 DNS 서버를 운영하는 ISP에서 악성 봇 DNS 싱크홀을 사용하면 악성 봇에 의한 악성 행위를 차단 할 수 있는 장점이 있다.

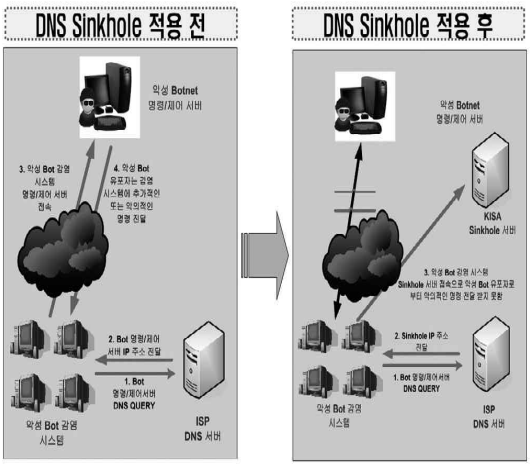

그림 1. DNS 싱크홀
Fig. 1. DNS Sinkhole

악성 봇 DNS 싱크홀 기법은 감염자의 참여 없이도 ISP의 협조만으로 악성 봇에 의한 악성행위를 차단할 수 있다는 장점이 있다. 그러나 악성 봇 DNS 싱크홀 기법은 감염자 PC가 치료되지 않고, 보안 취약점도 여전히 남아 있어서 또 다른 악성 봇에 쉽게 감염될 가능성이 있다. 근본적인 악성 봇 치료를 위해서는 일본 사이버클린센터 치료 기법과 같이 감염자 PC 자체의 취약점 제거하는 방안이 향후에 마련되어야 할 것으로 보인다[6].

2. 일본 사이버클린센터 치료 기법

일본 총무성과 경제산업성이 공동으로 봇넷, 악성 코드 대응·감축을 위한 사이버클린센터 CCC(Cyber Clean Center)를 운영하고 있다. CCC는 8개 ISP 및 마이크로소프트, 트렌드마이크로의 협조를 통해 운영되고 있다. CCC는 <그림 2>와 같이 3개의 그룹이 실무를 담당하여 운영한다.

(1) Telecom ISAC Japan 그룹

악성 봇 대책 시스템 운영을 담당한다. 좀비 PC가 유인용 Honeypot 위장 서버를 공격 하도록 하여 악성 봇에 감염된 시스템을 탐지한다. Honeypot에서 탐지된 악성 봇 자료와 샘플을 추출한다. 추출된 악성 봇 샘플은 JPCERT/CC 그룹에 전달하여 분석 한다. Honeypot을 공격한 악성 봇 IP 목록을 ISP에 전달하여 악성 봇의 경보 및 통지 시스템을 운영한다.

(2) JPCERT/CC 그룹

Telecom ISAC Japan 그룹에서 전달 받은 악성 봇 자료와 샘플을 이용하여 악성 봇 프로그램 분석 및 봇넷의 특성과 기술을 분석한다. 이 분석 정보를 토대로 마이크로소프트, 트렌드마이크로는 악성 봇에 대응하는 CCC 클리너 백신을 업데이트하고 IPA 그룹에 전달한다.

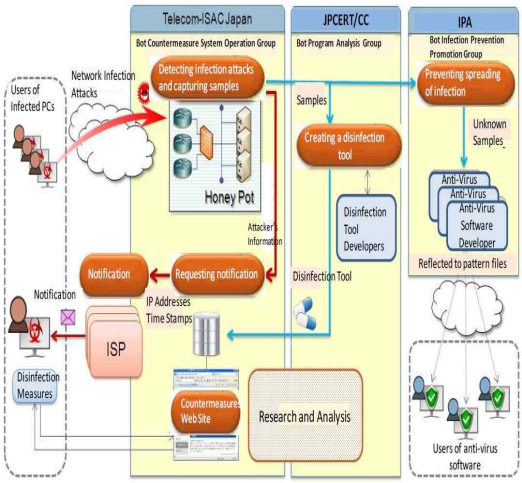

그림 2. CCC 업무 흐름도
Fig. 2. CCC Workflow

(3) IPA 그룹

악성 봇에 감염된 가입자 IP로 사용자 신원확인을 하고, JPCERT/CC 그룹에서 업데이트된 CCC 클리너 백신 설치 권고를 한다. 사용자는 CCC 치료 홈페이지에 접속하여 CCC 클리너 백신 프로그램을 무료로 다운로드 받아 악성 봇에 감염된 좀비 PC를 치료한다.

CCC 봇 넷 치료 기법은 악성 봇에 감염된 좀비 PC 사용자로 하여금 백신으로 치료를 하도록 유도하여 악성 봇을 제

거할 수 있고, 보안패치 등을 유도하는 경우 근본적인 취약점 제거가 가능하다. 특히 ISP가 해당 가입자에게 감염 여부를 알려줄 때 감염 통보를 받은 사용자 중 얼마만큼의 사용자가 CCC의 치료 홈페이지에 접속하여 전용백신을 다운로드하는지를 알 수 있는 장점이 있다.

그러나 이 기법은 감염이 확인된 후, 좀비 PC 치료 요청 e-mail을 수신한 PC 사용자 중에 30% 가량만 CCC의 치료 페이지를 방문하여 치료한다. 나머지 70%의 사용자는 감염 사실을 알고 있어도 아무런 조치를 하지 않아, 감염된 좀비 PC가 악성 행위를 계속하는 단점이 있다[4].

이러한 문제를 해결하기 위하여 본 논문에서는 악성 봇 치료를 사용자의 협조에 의존 하는 것이 아니라 악성 봇 치료를 감시하는 기법을 사용하여 해결 하고자 한다. 이 기법에서는 악성 봇 치료에 비협조적인 컴퓨터는 IP 주소를 제한적으로 제공하여 컴퓨터 사용자가 불편을 느끼도록 환경을 제공한다. 이에 따라 불편을 느낀 사용자가 악성 봇 치료에 능동적으로 참여하도록 유도하고자 한다.

III. DHCP를 이용한 봇 치료 기법

앞에서 살펴 본 바와 같이, 주요 시스템에 DDoS 공격을 하는 악성 봇에 국가적으로 대응하는 것은 필수적이다. 악성 봇 DNS 싱크홀 기법은 악성 봇 감염자 대부분이 보안에 대한 지식이 부족하고 백신 프로그램을 사용하지 않는 현실에서, 감염자의 참여 없이 ISP의 협조만으로도 악성 봇에 의한 악성행위를 차단할 수 있다는 장점이 있다. 그러나 악성 봇 DNS 싱크홀 기법은 감염자 PC를 치료하지 않아서 다른 악성 봇에 쉽게 감염된다. 근본적인 악성 봇 치료를 위해서는 사이버클린센터 치료 기법과 같이 감염자 PC 자체의 취약점을 제거하여야 한다[6]. 사이버클린센터 치료 기법은 악성 봇에 감염된 좀비 PC에 조치 요청한 PC 사용자 중에 30% 가량만 CCC의 치료 페이지를 방문하여 치료하고, 나머지 70%의 PC는 감염 사실을 알고 있어도 치료를 하지 않아서 여전히 악성 행위를 수행한다는 단점이 있다[4].

이러한 문제를 해결하기 위하여 본 논문에서는 사용자들이 적극적으로 악성 봇 치료를 하는 DHCP를 이용한 악성 봇 치료 기법을 제안한다. 이 기법에서는 악성 봇 치료에 비협조적인 컴퓨터에게 IP 주소를 제한적으로 제공하여 컴퓨터 사용자가 불편을 느끼도록 환경을 제공한다. 이에 따라 불편을 느낀 사용자가 악성 봇 치료에 능동적으로 참여하도록 유도하고자 한다.

DHCP를 이용한 악성 봇 치료 기법은 사용자 컴퓨터에 악성 봇 치료 백신 설치를 확인하는 클라이언트 소프트웨어와 이 설치 소프트웨어와 협력하여 봇 치료를 관리하는 서버 두 부분으로 나뉜다.

1. 백신 설치 확인 소프트웨어

악성 봇에 감염된 좀비 PC들을 치료하기 위해서 일본에서는 트렌드마이크로사가 CCC를 통하여 무료 백신을 제공하고 있다. 우리나라에서도 백신 업체와 협력하여 무료 백신을 제공하고 있다. 일반 사용자가 보호나라 홈페이지에서 악성 봇 감염 여부를 확인할 수 있다. 일반 사용자는 악성 봇 감염 여부를 확인하고, 악성 봇 무료 백신 다운로드 및 윈도우즈 보안 업데이트를 할 수 있다[3].

악성 봇 백신을 사용자에게 신속하게 배포하여 좀비 PC들을 치료하는 것은 매우 중요하다. 신속하게 배포하기 위하여 CCC에서는 ISP에 가입된 사용자 신상 정보를 이용하여 e-mail을 발송 및 전화 통보한다.

그러나 메일 주소 및 전화번호는 자주 바뀌기 때문에 통보가 힘든 점도 있고, 비협조적인 사용자들은 통보를 받더라도 치료를 하지 않는 문제가 있다. DDoS 공격을 하는 악성 봇은 주요 시스템에게는 치명적이지만 감염된 좀비 PC들에게는 별 해가 없어서 치료에 비협조적인 사용자가 많다.

본 논문에서는 <그림 3>과 같이 봇 치료 백신 설치여부를 관리 서버에게 보고하여 DHCP가 제한된 IP 주소를 할당하도록 한다. 클라이언트용 소프트웨어는 봇 치료 백신과 백신 설치 확인 소프트웨어 부분으로 나뉜다. 백신 설치 확인 소프트웨어는 주기적인 설치 확인 요청을 치료 관리 서버에 응답하는 간단한 구조로 되어있다.

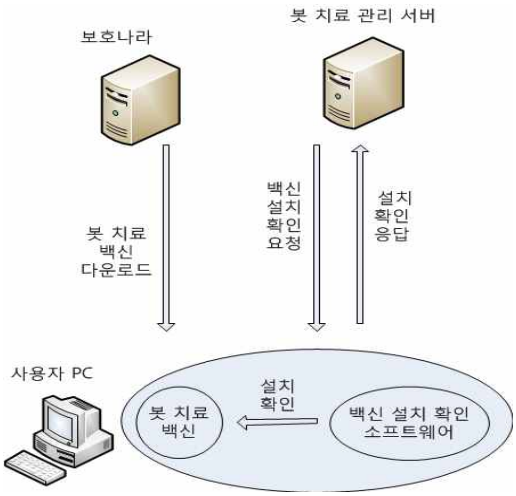

그림 3. 백신 설치
Fig. 3. Installation of Vaccine

2. 치료 관리 서버

DDoS 공격을 하는 악성 봇은 국가 주요 시스템에게 치명적이지만 봇에 감염된 좀비 PC들의 증상은 느끼지 못할 정도로 미미하다. 따라서 사용자들이 자신의 문제로 인식하지 못하고 좀비 PC 치료에 적극적으로 나서지 않고 있다. 본 논문에서는 <그림 4>와 같이 DHCP가 봇 치료 백신 설치여부 목록을 참조하여 제한된 IP 주소를 할당하도록 한다. 봇 치료 백신 설치여부 목록은 사용자 PC의 백신 설치 확인 소프트웨어가 제공한 정보로 봇 치료 관리 서버가 작성 한다.

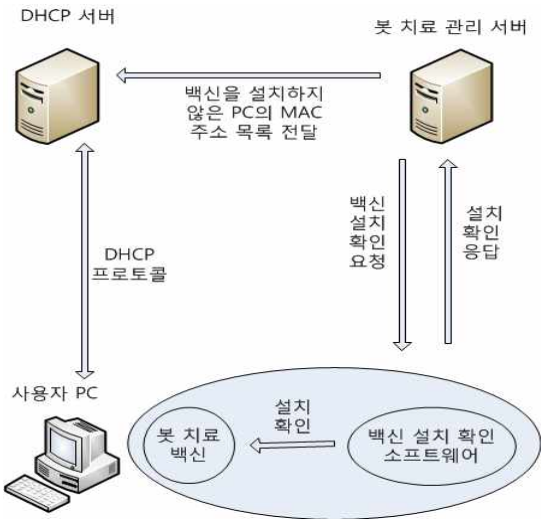

그림 4. MAC 주소 목록 전달
Fig. 4. Passing List of MAC Addresses

작성된 목록을 참조하여 DHCP는 봇 치료 백신을 설치하지 않은 PC에게 제한된 IP를 제공하는 불편한 환경을 만든다. 이 불편한 환경 때문에 봇에 감염된 사용자들은 악성 봇 치료를 자신의 문제로 느끼고 적극적으로 치료에 임하게 된다.

백신 설치 확인 소프트웨어가 설치되지 않은 컴퓨터에 DHCP가 제한적으로 IP 주소를 공급하려면 DHCP 서버 동작을 수정 하여야한다.

DHCP 서버와 클라이언트의 주요 동작은 아래와 같은 차례로 동작한다.

(1) DHCP_Discover : DHCP 클라이언트가 부팅이 되고 네트워크가 시작되면 DHCP 서버를 찾는 요청을 만들어서 패킷을 브로드캐스트 한다.

(2) DHCP_Offer : DHCP_Discover 메시지를 받은 DHCP 서버는 사용가능한 IP 주소 하나를 담은 DHCP 패킷을 만들고, 역시 네트워크에 브로드캐스트로 보낸다.

(3) DHCP_Request : DHCP 서버로부터 IP 주소를 받은 DHCP 클라이언트가 이 IP 주소를 사용할 수 있는 것은 아니다. DHCP 클라이언트는 서버로부터 할당 받은 IP 주소와 이 IP 주소를 임대해준 서버의 IP를 담은 패킷을 만들어서 네트워크에 다시 브로드캐스트로 보낸다.

(4) DHCP_Ack : DHCP 클라이언트의 DHCP_Request 브로드캐스트를 받은 DHCP 서버는 둘 중의 한 가지 작업을 한다. 자신이 보낸 IP 주소가 채택되지 않았다면 DHCP 서버는 다시 IP Database에 유지하고, 자신이 보낸 IP가 채택되었다면 IP 임대기간, DNS, Default Gateway, WINS 등의 DHCP 옵션 값을 담은 DHCP_Ack 패킷을 만들어서 최종적으로 브로드캐스트로 보낸다.

DHCP_Nack 메시지를 받은 클라이언트는 IP 주소를 받을 수 없는 것으로 정의한다[7].

백신 설치 확인 소프트웨어가 설치되지 않은 사용자 PC가 DHCP_Discover 메시지를 보내면 DHCP 서버가 DHCP_Offer 메시지 대신에 DHCP_Nack 메시지를 전송하도록 수정하여야 한다. 이러한 수정 작업을 쉽게 하기 위하여 봇 치료 관리 서버를 DHCP 서버에 함께 설치하였다.

DHCP 서버를 이용한 소프트웨어 개발을 쉽게 하기 위하여 마이크로소프트는 DHCP 서버 Callout API를 제공한다. Callout API는 개발자가 윈도우즈 서버에서 DHCP 서버의 사용자 정의 확장 기능 및 통계 모니터 등의 개발을 가능하게 한다[8]. Callout API를 사용하기 위해서는 Callout DLL을 다운로드하여 설치해야 한다. Callout API를 사용하기 위하여 MSDN에서는 아래와 같은 콜백 함수 들을 제공한다[9].

DhcpAddressDelHook
DhcpAddressOfferHook
DhcpControlHook
DhcpDeleteClientHook
DhcpHandleOptionsHook
DhcpNewPktHook
DhcpPktDropHook
DhcpPktSendHook

치료 관리 서버는 이러한 콜백 함수들을 이용하여 백신 설치 확인 소프트웨어가 설치되지 않은 사용자 PC가 DHCP_Discover 메시지를 보내면 DHCP 서버가 DHCP_Offer 메시지 대신에 DHCP_Nack 메시지를 전송하

도록 구성 하였다. DHCP_Offer 메시지 콜백 함수로는 DhcpAddressOfferHook가 제공되고 있다.

그러나 이 함수는 시급히 처리해야 하는 콜백 함수이므로 여기서 봇 백신 설치 확인 소프트웨어의 동작 여부를 묻는 메시지 요청을 하고, 백신 설치 확인 응답을 받을 시간이 없다. 따라서 치료 관리 서버는 백신 설치 확인 소프트웨어가 설치되지 않아서 IP 주소를 제한해야하는 MAC 주소 목록을 미리 마련해 놓았다. 이 MAC 주소 목록을 이용하여 DhcpAddressOfferHook 콜백 함수에서 DHCP_Offer 메시지와 DHCP_Nack를 선택적으로 보내도록 하였다.

IP 주소를 제한해야하는 MAC 주소 목록을 만들기 위해서는 DHCP_Ack 패킷에서 구할 수 있으나 Callout API에서는 따로 제공하지 않는다. 그 대신 DhcpPktSendHook 콜백 함수에서 송신할 패킷이 DHCP_Ack 패킷일 경우 여기서 클라이언트의 IP 주소와 MAC 주소를 구하고, 이 IP 주소를 이용하여 클라이언트용 백신 설치 확인 소프트웨어 동작 확인 이벤트를 발생시킨다.

이 이벤트에서 치료 관리 서버는 사용자 PC IP 주소로 봇 백신 설치 확인 소프트웨어 동작 확인 요청을 하고 응답을 받는다. 3번의 요청에도 응답이 없을 시에는 백신 설치 확인 소프트웨어가 설치되지 않은 것으로 간주 하고 IP 주소를 제한해야하는 MAC 주소 목록에 추가시킨다. MAC 주소 목록에 있는 사용자 PC는 IP 주소 제공에 제한을 받는다. 이 불편함은 본 논문에서 의도한 것 이지만 클라이언트용 백신 설치 확인 소프트웨어 설치 이후에도 해당 MAC 주소의 컴퓨터가 IP 주소를 못 받는 문제가 있다.

DHCP 클라이언트가 DHCP_Offer 메시지를 받지 못했다면 DHCP_Discover 메시지를 다시 브로드캐스트 한다. 네 번째 요청 이후에도 받지 못했을 때 사용자 클라이언트는 5분마다 다시 시도하게 된다.

이를 이용하여 DhcpAddressOfferHook 콜백 함수에서 해당 MAC 주소가 15번 이상의 호출이 있으면 MAC 주소 목록에서 삭제하도록 하여 클라이언트용 백신 설치 확인 소프트웨어 설치 후에 IP 주소를 재 할당 받도록 설계하였다.

IV. 기존 기법과의 비교 분석

악성 봇 감염자의 대부분이 보안에 대한 지식이 부족하고 백신 프로그램을 사용하지 않는 현실에서 악성 봇 DNS 싱크홀 기법은 효과적인 기법인 것으로 판단된다. 반면에 이 기법은 감염자 PC의 보안 취약점이 그대로 남아 있어서 다른 악성 봇에 쉽게 감염이 된다. CCC 봇넷 치료 기법은 악성 봇에 감염된 좀비 PC 사용자로 하여금 백신으로 치료를 하도록 유도하여 악성 봇을 치료한다. 그러나 이 방식은 좀비 PC 치료 요청 e-mail을 수신한 PC 사용자 중에 소수만 치료하고, 나머지 70% PC 사용자는 치료를 하지 않는 단점이 있다[4].

인캅스나 에스코트 등의 기업 보안 시스템은 NAC(Network Access or Admission Control) 기술을 이용한다. NAC 기술은 허가된 사용자가 아니거나 바이러스에 감염된 시스템은 네트워크의 접속을 차단하고 해당 조직이 요구하는 보안수준을 준수해야 네트워크의 사용을 허가한다. NAC 기술을 이용하면 대부분의 컴퓨터에 백신을 설치할 수 있으나, 이 방식은 사용자에게 심한 거부감을 일으켜 일반 사용자에게 사용하기 어렵다. 기업은 정보 유출 및 변조에도 큰 피해가 발생하므로, NAC 기술을 이용하여 <표 1>과 같이 메신저, 파일 전송, usb 사용 등에 제한을 한다. 이러한 사용 제한은 기업 및 조직의 정보 보호에 꼭 필요하지만 일반 사용자에게는 상당히 불편하다. 인캅스 프로그램이 깔려있는 노트북은 가정집또는 다른 지역으로 이동시에도 <표 1>과 같은 사용 제한으로 불편하다. 이에 따라 인터넷에 “인캅스 우회”, “인캅스 제거” 등 NAC 기술을 무력화시키는 방법들이 많이 소개되고 있다.

표 1. 2가지 방식(NAC, DHCP) 비교
Table 1. Comparison of Two Methods(NAC, DHCP)

방식	NAC 기술을 이용한 방식	DHCP를 이용한 방식
악성 봇 제거	가능	가능
설치가 안된 컴퓨터	방화벽으로 인터넷 사용 차단	DHCP가 인터넷 사용을 정기적으로 차단
사용자 인증	필요함	필요 없음
메신저, 이메일	사용 제한	제한 없음
파일 전송	사용 제한	제한 없음
usb, cd/dvd	사용 제한	제한 없음

기업의 클라우드 컴퓨팅 환경 구축으로 PC에서 노트북, 테블릿, 스마트폰 사용으로 바뀌는 현실에서 이러한 사용 제한은 큰 불편을 초래한다. 사이버 공격자들은 DDoS 공격을 하기위하여 기업보다 보안이 허술한 일반 사용자 컴퓨터를 악성 봇에 감염 시킨다. 이러한 상황에서 NAC 기술 보안 시스템에 대한 일반 사용자의 거부감은 심각한 문제가 된다.

이에 비하여 본 논문에서 제안한 백신 설치 확인 소프트웨어는 사용자의 인터넷 사용에 제한을 두지 않기 때문에 거부감이 적다. 백신 확인 소프트웨어가 없는 컴퓨터에 대해서 주기적으로 IP 주소를 제한적으로 공급하여 불편을 느낀 사용자가 악성 봇 치료에 능동적으로 참여하도록 유도하였다. 또한 백신 설치 확인 소프트웨어는 사용자의 인터넷 사용에 제

한을 두지 않기 때문에 NAC 기술의 사용자처럼 백신 확인 소프트웨어를 제거하거나 우회할 걱정이 없는 장점이 있다.

V. 결 론

악성 봇을 이용한 DDoS 공격에 정부 주요 기관이 유린당하고도 범인을 못 잡는 현실이 반복되고 있다. 공격 기법도 탐지가 힘들 정도로 교묘해 지고, 공격 속도는 방어가 힘들 정도로 빨라지고 있다. 이는 악성 봇의 약점이 명령/제어 서버에 접속하는 것이라 판단하고 이 연결을 끊기 위한 대응에 집중한 결과이다. 악성 봇은 이러한 대응을 회피하는 기법으로 계속 발전 중이며 이에 대응하는 기법들이 성공 할 수 있다는 확신이 들지 못하고 있다. 악성 봇에 대응하는 또 다른 기법은 봇 치료 백신으로 좀비 PC 자체를 치료하는 것이다. 현재의 방식은 이 백신 개발을 민간 업체에게 맡기고 백신의 설치는 사용자에게 협조를 구하는 방식이다. 민간 업체는 정부의 협조를 받아 공개용 백신을 제공하고 있으나 기능이 약하거나, 신속한 업데이트 기능이 떨어지는 한정판인 공개 백신을 제공하고 있다. 악성 봇의 피해가 심각한 상황에서 봇 백신은 일본처럼 무료로 나누어 주는 것이 필요하다. 악성 봇은 주요 시스템을 공격하지 사용자 PC를 공격하지 않으므로 사용자들이 감염 사실을 잘 알지도 못하고 봇 치료에도 비협조적이다. 심각한 DDoS 공격에 대응하기 위해서는 우수한 백신의 설치가 매우 중요하다.

본 논문은 이점에 주목하여 사용자 컴퓨터의 백신 설치를 감시하는 기법을 제안하였다. 백신 설치가 확인되지 않은 컴퓨터는 DHCP 서버가 주기적으로 IP 주소를 제한적으로 제공하여 사용자가 불편을 느끼는 환경을 제공한다. 주기적으로 IP 주소를 제공하지 않는 불편한 환경 때문에 사용자들이 자발적으로 봇 치료를 하도록 유도하였다. 이 불편한 환경이 사용자들에게 거부감이 들 수도 있다. 그러나 DHCP 프로토콜도 고정 IP 주소 환경에 비하면 불편하지만 대부분 사용자는 당연하게 받아들이고 있다. 본 논문에서 제안한 기법은 백신 설치가 확인된 PC는 아무런 불편을 느끼지 못하고, 확인이 불가능한 PC만 주기적으로 불편을 느끼도록 하였다.

참고문헌

[1] Y. H. Kim, “Theoretical Implication on Establishing the National Countermeasure System against Cyber Crime - Focusing on a Pattern of Cyber Terror -,” Journal of the Korea Society of Computer and Information, Vol. 14, No. 6, pp. 165-171, June 2009.

[2] M. S. Jang, J. I. Lee, C. S. Oh, “Harmful Traffic Control Using Sink Hole Routing,” Journal of the Korea Society of Computer and Information, Vol. 14, No. 4, pp. 69-76, April 2009.

[3] K. H. Kim, et al., “Accredited by the device identifier location-based security techniques,” Journal of the Korea Institute of Entertainment Industry Spring Conference, pp. 186-194, May 2011.

[4] Y. B. Kim, H. Y. Youm, “A New Bot Disinfection Method Based on DNS Sinkhole,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 18, No. 6(A), pp. 107-114, Dec. 2008.

[5] D. W. Kang, et al., “Recent trends and the corresponding technical studies malicious behavior of botnets,” Korea Institutes of Information Security and Cryptology, Vol. 19, No. 6, pp. 22-31, Dec. 2009.

[6] Y. B. Kim, et al., “Preventing Botnet Damage Technique and It’s Effect using Bot DNS Sinkhole,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 15, No. 1, pp. 47-55, Jan. 2009.

[7] J. H. Lee, et al., “The Address Detection Algorithm to Avoid DHCP NAK Loop Problem in Virtual LAN,” Journal of Korea Information Science Society Fall Conference, Vol. 29, No. 2, pp. 604-606, 2002.

[8] DHCP Server Callout API usage, *http://blogs.technet.com/b/teamdhcp/archive/2009/07/06/dhcp-server-callout-api-usage.aspx*

[9] DHCP Server Callout API Reference, *http://msdn.microsoft.com/en-us/library/windows/desktop/aa363373(v=vs.85).aspx*

저 자 소 개

김 홍 윤

1982: 인하대학교 전자계산학과 이학사.
1984: 인하대학교 전자계산학과 이학석사.
1996: 인하대학교 전자계산학과 이학박사.
현 재: 한서대학교 컴퓨터공학과 교수
관심분야: 센서 네트워크, 정보통신,
디지털 포렌식
Email : hykim@hanseo.ac.kr