情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

DNS 싱크홀에 기반한 새로운 악성봇 치료 기법

김 영 백[1†], 염 흥 열[1‡]
[1]순천향대학교

A New Bot Disinfection Method Based on DNS Sinkhole

Young-Baek Kim[1†], Heung Youl Youm[1‡]
[1]SoonChunHyang University

요 약

악성봇은 DDoS 공격, 스팸메일 발송 등 다양한 악성행위를 하는 웜/바이러스 이다. 이러한 악성봇의 악성행위를 차단하기 위하여 국내외 많은 기관에서 노력을 기울이고 있다. 국내에서도 악성봇 DNS 싱크홀을 구축하여 악성봇에 의한 악성행위를 차단하고 있고, 일본에서도 CCC(Cyber Clean Center) 구축을 통하여 악성봇 감염 PC를 치료하고 있다. 그러나 악성봇 DNS 싱크홀은 감염 PC를 근본적으로 치료하지 못한다는 단점이 있고, CCC 또한 감염이 확인된 PC 중 30%만 치료가 되고 있는 문제점을 가지고 있다. 본 논문에서는 이러한 기존 기법들의 단점을 보완하고 장점을 취하여 악성봇에 의한 악성행위를 차단함과 동시에 근본적인 치료도 병행하는 방식으로 새로운 악성봇 치료기법을 제안 하였다.

ABSTRACT

The Bot is a kind of worm/virus that can be used to launch the distributed denial-of-service(DDoS) attacks or send massive amount of spam e-mails, etc. A lot of organizations make an effort to counter the Botnet's attacks. In Korea, we use DNS sinkhole system to protect from the Botnet's attack, while in Japan “so called” CCC(Cyber Clean Center) has been developed to protect from the Botnet's attacks. But in case of DNS sinkhole system, there is a problem since it cannot cure the Bot infected PCs themselves and in case of CCC there is a problem since only 30% of users with the Botnet-infected PCs can cooperate to cure themself. In this paper we propose a new method that prevent the Botnet's attacks and cure the Bot-infected PCs at the same time.

Keywords : Bot, Bot Disinfection, DNS sinkhole, CCC

Ⅰ. 서 론

악성봇은 스팸메일 발송, DDoS 공격 등 인터넷 상에서 다양한 문제를 일으키고 있다. 이러한 악성봇에 대하여 다양한 대응을 하고 있으나, 아직도 수많은 PC 들이 악성봇에 감염되어 있는 상태이다. 이렇게 악성봇에 감염된 PC는 PC 소유자의 의지에 상관없이 해커에 의해 조종당하여 악성행위를 수행하기 때문에 좀비 PC 라 부르기도 한다. 이러한 악성봇의 감염을 막고 악성행위를 차단하기 위하여 다양한 기법들이 활용되고 있다. 국내에서는 2005년부터 악성봇 DNS 싱크홀 운영을 통하여 악성봇 감염시 명령/제어 서버로의 접속을 차단함으로써 악성봇에 의한 악성행위를 효과적으로 차단한 바 있다. 또한 국외에서도 다양한 방법으로 악성봇의 악성

접수일 : 2008년 9월 16일; 수정일 : 2008년 11월 12일;
채택일 : 2008년 11월 24일
† 주저자, ybkim@kisa.or.kr
‡ 교신저자, hyyoum@sch.ac.kr

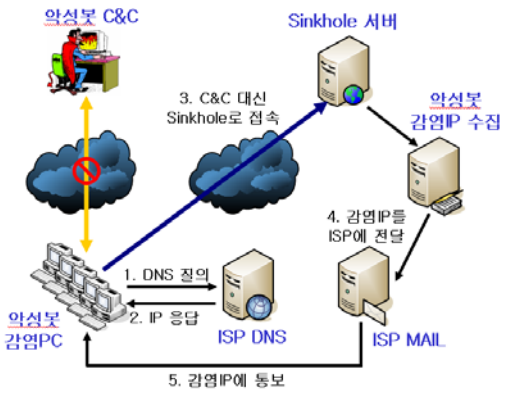
행위를 차단하고 있다. 일본에서는 악성봇 감염PC를 치료하기 위한 체계인 CCC(Cyber Clean Center)를 구축하여 악성봇에 감염된 사용자가 CCC 사이트를 방문하여 전용백신을 다운로드 하고, 다운로드한 백신을 이용하여 악성봇을 치료하도록 하고 있다.

본 논문에서는 기존 기법 중 DNS를 이용하여 악성봇 명령/제어 서버로의 연결을 차단함으로써 악성봇 감염PC의 악성행위를 막는 DNS 싱크홀 기법과, 일본에서 악성봇 감염PC를 치료하기 위한 체계인 CCC 기법을 비교하고, 기존 기법의 한계점을 극복한 새로운 악성봇 치료 기법을 제안하여 시스템의 구성을 설명하고, 마지막으로 기존 기법들과의 장단점을 비교하였다. 본 논문에서 제안하는 치료 기법은 2008년 연말에 실제 시스템으로 구축되어 서비스 예정이다.

Ⅱ. 기존 악성봇 치료 기법

2.1 악성봇 DNS 싱크홀을 이용한 악성행위 차단 기법

악성봇은 취약점을 가지고 있는 PC에 자동으로 전파되며, 감염 시 해커가 지정해 놓은 명령/제어 서버에 접속하여 해커로부터의 명령을 기다린다. 이렇게 악성봇 감염 PC가 접속하는 해커의 서버를 악성봇 명령/제어(C&C : Command and Control) 서버라고 하며, 명령/제어 서버와 감염 PC 들로 구성된 네트워크를 Botnet (Bot Network) 이라고 한다. 악성봇 명령/제어 서버는 이러한 악성행위의 중심에 있으며, 악성봇 명령/제어 서버의 차단만으로도 해커로부터의 명령 전달을 방지할 수 있어 악성봇의 악성행위를 효과적으로 막을 수 있다.



[그림 1] 악성봇 DNS 싱크홀 기법

DNS 싱크홀은 다음과 같이 동작한다. 악성봇 감염PC가 명령/제어 서버에 접속하기 위해서는 악성봇 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 감염PC는 응답받은 IP로 접속하는 과정을 거치게 된다.

그러나 [그림 1] 처럼 악성봇 DNS 싱크홀이 적용된 DNS 서버의 경우에는 사전에 악성봇 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, 감염PC는 해커의 서버 대신에 싱크홀 서버로 접속하게 된다. 이렇게 되면 악성봇은 감염 후 해커의 명령/제어 서버에 접속하여 악성 행위 명령을 전달받는데, 명령/제어 서버로의 접속이 차단되므로 더 이상 악성 행위를 할 수 없게 된다.

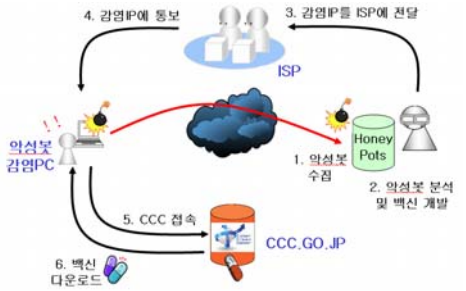
악성봇 DNS 싱크홀은 감염 PC의 사용자가 보안에 대한 지식이 없더라도 감염 PC 가 사용하는 DNS 서버를 운영하는 ISP에서 악성봇 DNS 싱크홀을 적용중이라면 악성봇에 의한 악성행위를 차단 할 수 있는 효과가 있다. 그러나 감염 PC에 악성봇이 치료되지 않고 그대로 남아 있으며, 감염 PC가 가지고 있는 보안 취약점 역시 해결되지 않고 남아 있어 또 다른 악성코드에 감염되는 것을 막을 수 없다는 단점이 있다. 이러한 단점을 보완하기 위하여 감염 PC 목록을 해당 ISP에 전달하고 있으나, 유동 IP의 경우 Timestamp로 실 사용자를 찾는데 시간이 오래 걸리고, 해당 사용자의 e-mail이 등록되지 않은 경우도 많으며, ISP의 기술지원 인력에 한계가 있다는 이유로 감염PC에 대한 조치가 잘 안되고 있는 실정이다.

2.2 일본 CCC(Cyber Clean Center)의 악성봇 치료 기법[4]

일본의 CCC는 [그림 2]와 같이 허니넷을 공격하여 악성봇을 전파한 IP 목록을 ISP에 전달하여 ISP가 해당 가입자에게 감염사실을 알리면, 가입자는 악성봇 치료 홈페이지에 접속하여 백신 프로그램을 다운로드 받아 치료하는 방식이다. 악성봇 감염 PC 사용자로 하여금 백신으로 치료를 하도록 함으로써 악성봇을 제거할 수 있고, 보안패치 등을 유도하는 경우 근본적인 취약점 제

거가 가능하다는 장점이 있다. 특히 ISP가 해당 가입자에게 감염여부를 알려줄 때 감염IP 별로 태그를 작성하여 이를 CCC의 치료 시스템 접속 URI에 삽입함으로써 감염 통보를 받은 사용자 중 얼마만큼의 사용자가 CCC의 치료 홈페이지에 접속하여 전용백신을 다운로드하는지를 알 수 있다. 2008년 7월 발표 자료에 따르면 [표 1] 6만 명 이상의 봇감염 PC에 조치요청 e-mail을 발송하여 그 중 30% 가량이 전용백신을 다운로드하였다.

그러나 CCC는 감염이 확인되어 감염사실을 통보한 PC 중 30% 가량이 CCC의 치료페이지를 방문하여 치료하고 있으므로, 나머지 70%의 PC는 감염사실을 알고 있음에도 아무런 조치가 이루어지지 않고 여전히 악성행위를 수행한다는 단점이 있다. 또한 전용 백신을 이용하여 치료하고 있으나 미처 패턴이 추가되지 못한 악성봇에 감염된 사용자는 이후 별다른 치료 방법이 없고, 허니넷을 공격하는 네트워크 전파형 악성봇을 중심으로 감염 PC를 확인하고 있어 HTTP봇이나 홈페이지를 통해 유포되는 봇에 대한 대응 능력이 떨어질 수 있다.



[그림 2] 일본 CCC 기법

[표 1] CCC 프로젝트 운영결과[4]

항목	2008년7월	총 누적
악성코드 수집 개수	655,320개	9,994,787개
악성코드 수집 uniq 개수	100,284개	494,661개
상용백신 미탐지 개수	302개	19,166개
전용백신 패턴 추가 개수	3,457개	14,880개
전용백신 버전 업데이트 회수	총 79회	
조치 e-mail 발송 개수	14,967개	288,393개
조치 대상자 수	5,506명	64,033명
조치 대상자 중 전용백신 다운로드율	30%	
전용백신 다운로드 총 수	15,952회	453,214회

Ⅲ. 싱크홀을 통한 악성봇 치료 기법 제안

제안 방식은 다음과 같이 진행된다. 싱크홀을 통하여 악성봇 감염 PC를 싱크홀 네트워크로 유도하면 싱크홀 네트워크에서는 감염 IP가 실시간으로 접속을 시도하게 되고 이를 악성봇 감염 IP 목록 DB에 저장한다. 이후 일반사용자가 홈페이지에서 악성봇 감염여부를 확인할 수 있는 “악성봇 감염PC 확인 홈페이지”를 구축하여 일반사용자의 접속을 유도한다. 일반사용자가 “악성봇 감염PC 확인 홈페이지”에 접속하면 접속한 사용자의 IP가 현재 악성봇 감염IP 목록 DB에 포함되어 있는지 여부를 확인하여 악성봇 감염 IP목록 DB에 해당 IP가 있는 경우 감염되었음을 알려주고 공개백신 및 윈도우즈 보안 업데이트를 안내한다. 윈도우즈 보안 업데이트의 경우 이미 개발하여 운영 중인 “PC 자동 보안 업데이트” S/W를 이용하면 보다 편리하게 윈도우즈 보안 업데이트를 수행할 수 있다. “PC 자동 보안 업데이트” S/W는 윈도우즈 보안 업데이트를 하지 않는 사용자 등을 대상으로 자동으로 윈도우즈 보안 업데이트를 설치해 주는 프로그램으로[그림 3] 보호나라 홈페이지 등에서 서비스 중이다[6]. 이를 이용하면 감염PC 사용자가 다시 MS 홈페이지 방문 등을 통하여 윈도우즈 보안 업데이트를 설치할 필요 없이 보다 손쉽게 설치가 가능하다.

[그림 3] PC 자동 보안 업데이트 S/W

공개백신으로 치료가 되지 않는 경우에는 별도로 “감염 파일 확인 S/W”를 다운로드 하도록 하여 감염된 파일을 “악성봇 감염PC 확인 홈페이지”를 통해 업로드

하도록 유도하고 이를 받아 백신회사에 전달함으로써 수일 안에 백신 프로그램에서 치료할 수 있도록 한다

3.1 싱크홀을 통한 악성봇 감염 PC 확인

악성봇 감염 PC가 싱크홀 네트워크에 접속하면 싱크홀 네트워크 앞단에 위치한 트래픽 수집 서버에서 접속 트래픽을 수집하여 악성봇 감염 IP 목록 DB에 저장한다. 저장하는 내역은 접속시간, 감염IP, 대상포트 등과 IRC 관련 채널 정보로 [표 2] 같다. 접속정보는 실시간으로 저장되므로 감염 PC 확인을 위해서는 최근 5분~10분 사이의 접속 IP를 확인하여 현재 “악성봇 감염PC 확인 홈페이지”에 접속한 IP와 비교하는 방식으로 진행한다. 초고속 인터넷 사용자가 많은 유동 IP의 경우 IP를 사용자에게 동적으로 할당되게 되는데, 5분~10분 사이에 이전 사용자가 인터넷 사용을 끊고 새로운 사용자가 PC를 켜서 같은 IP를 재할당 받아 “악성봇 감염PC 확인 홈페이지”에 접속하였을 가능성은 매우 적다. 따라서 악성봇 감염 IP 목록 DB에서 검색한 최근 5분~10분 사이의 접속 IP 목록에 “악성봇 감염PC 확인 홈페이지”에 접속한 PC의 IP가 있다면, 해당 PC는 악성봇에 감염되어 사용자 모르게 해커의 명령/제어 서버로 접속을 시도하다가 싱크홀 네트워크로 접속하게 되었음을 확인할 수 있다[그림 4].

또한 특정 기업이나 조직의 관리자의 경우 자신이 관리하고 있는 IP 대역의 PC들이 악성봇에 감염되었는지 여부를 확인하고 싶을 수 있다. 이러한 경우 “악성봇 감염PC 확인 홈페이지”에서 자신이 관리하고 있는 IP 대역을 입력하면 해당 대역의 IP 검색을 통하여 감염 PC의 목록을 표시하여 줄 수 있다.

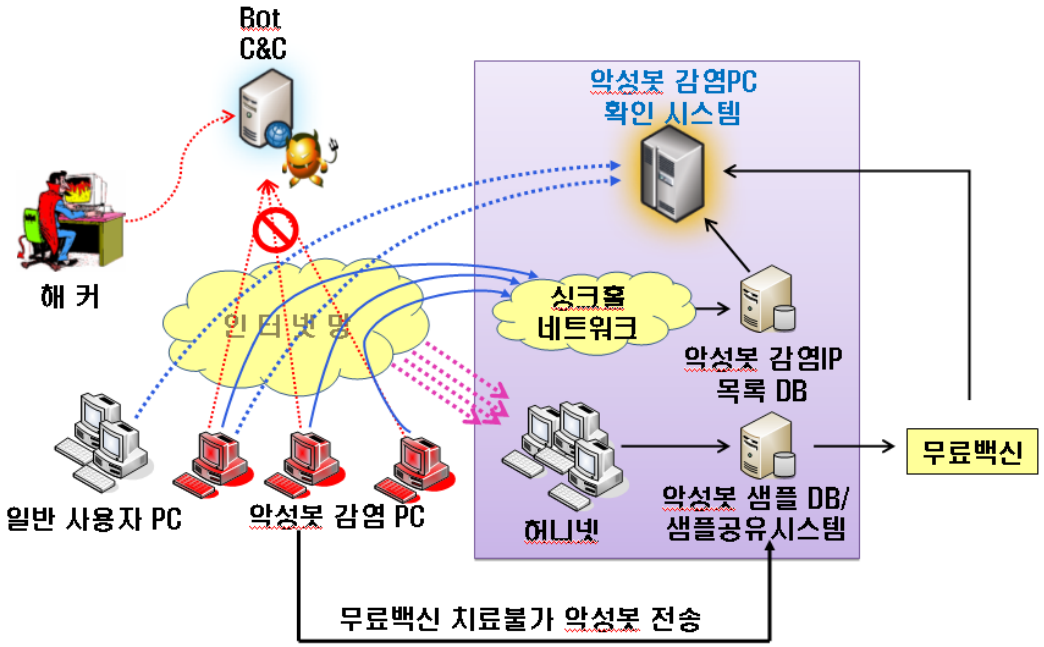
악성봇의 특성상 감염PC는 명령/제어서버에 접속하여 해커의 명령을 대기하게 된다. 만일 싱크홀 기법이 적용된 경우 감염PC는 싱크홀 서버에 감염PC가 접속하여 명령을 대기하게 되는데 장시간 대기하는 경우 발생하는 트래픽이 적어 최근 10분간의 악성봇 감염IP 목록 DB에 감염PC로부터 발생되는 트래픽(신규 패킷)이 기록되지 않을 수 있다. 그러나 접속 중인 싱크홀 서버의 네트워크 접속정보(netstat)를 확인하면 이미 접속되어 있음을 확인할 수 있으므로, 이런 경우에는 싱크홀 서버군[그림 5]에서 서버별 네트워크 접속정보 확인 하여 이를 서버별로 취합하여 네트워크 접속 현황을 확인하면 장시간 접속 중인 감염PC라 할지라도 감염유무를 확인할 수 있다. 따라서 감염 여부에 대한 검증은 악성봇 감염 IP 목록 DB와 서버별 네트워크 접속 정보 두 가지 모두 확인하여 둘 중 하나라도 IP가 확인되면 감염된 것으로 통보한다.

3.2 악성봇 감염 PC 치료

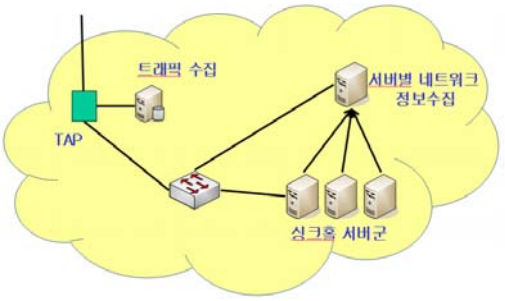
“악성봇 감염PC 확인 홈페이지”에 접속한 사용자가 감염되었음을 알게 되면 사용자는 무료백신 다운로드를 통하여 자신의 PC에 감염된 악성봇을 치료할 수 있다.

[표 2] 악성봇 감염 IP 목록 DB 스키마

시간	감염IP	소스포트	대상포트	채널명	채널키	사용자명	패스워드	닉네임
2008/09/12 03:00:30	IP1	2877	6667	-	-	-	-	oicvuf
2008/09/12 03:00:30	IP2	2753	7007	-	-	LOTTE_SVR	-	-
2008/09/12 03:00:30	IP3	3456	5555	-	-	-	-	KOR|9875829
2008/09/12 03:00:30	IP3	3456	5555	-	-	vskyazrm	-	-
2008/09/12 03:00:30	IP3	3456	5555	#ddos#	dreny	-	-	-
2008/09/12 03:00:30	IP4	4203	7007	-	-	LSHO_1301_CTS	-	-
2008/09/12 03:00:30	IP5	62057	7000	-	-	-	eeeeeeee	-



[그림 4] 제안하는 악성봇 치료기법



[그림 5] 싱크홀 네트워크 상세구조

싱크홀 구축을 위해 악성코드를 수집하는 단계에서 이미 백신업체에 악성코드에 대한 샘플이 전달되므로, 대부분의 악성봇을 치료할 수 있다. 하지만 치료하지 못하는 경우에는 감염 PC 사용자로 하여금 싱크홀 네트워크와 접속을 하고 있는 악성 파일을 “악성봇 감염PC 확인 홈페이지”로 업로드하게 유도하고, 이를 백신업체에 전달하여 백신엔진 업데이트를 요청하게 된다. 감염 PC 사용자는 별도로 작성된 “감염 파일 확인 S/W”를 통하여 해당 악성 파일을 확인할 수 있다. “감염 파일 확인 S/W”는 내부적으로 두 가지 기능을 수행하게 되는데, 네트워크 연결 현황을 확인하는 기능과 해당 네트워크 포트를 사용하는 프로세스를 확인하는 기능이다. 네트워크 연결 현황 확인을 통해 싱크홀 IP와 연결되어 있는 포트를 확인하고 해당 포트를 사용 중인 프로세스를 확인함으로써 악성봇에 감염된 파일명 및 경로를 감염 PC 사용자에게 알려준다. 감염 PC 사용자는 이렇게 확인된 파일을 “악성봇 감염PC 확인 홈페이지”로 업로드하면 된다.

악성봇 치료를 위해서는 악성봇이 가지고 있는 자체 삭제기능을 활용하여 싱크홀 네트워크에서 일괄 삭제 명령을 통해 삭제도 가능하다. 그러나 이러한 경우 감염 PC에 접근하여 파일을 삭제하는 것이기 때문에 좋은 의도라 할지라도 법적으로 문제가 될 수 있다. 또한 “악성봇 감염PC 확인 홈페이지” 접속 시에 감염된 파일을 확인해서 강제 삭제할 수도 있으나 이 역시 같은 이유로 바람직하지 않다. 따라서 본 논문에서는 최대한 감염 PC 사용자의 의지에 따라 악성봇을 치료하고 감염 파일을 확인할 수 있는 방법을 제안하였다. 또한 무료 백신으로 치료가 되지 않더라도 끝까지 해당 악성봇을 찾아 삭제할 수 있는 방법을 제시하였다.

Ⅳ. 제안방식과 기존연구 비교 및 특성 분석

제안방식은 악성봇 싱크홀을 통하여 유입되고 있는

[표 3] 제안방식과 악성봇 싱크홀, CCC 프로젝트 비교

	악성봇 싱크홀	CCC 프로젝트	제안방식
감염PC의 악성행위 지속 여부	해커의 명령에 의한 1차적인 악성행위 차단	치료된 30%에만 차단	해커의 명령에 의한 1차적인 악성행위 차단
사용자의 보안의식	관계없음	필수적	1차적으로는 관계없으나 근본적인 치료에는 필수적
악성코드 제거	불가능	가능	가능
백신 미탐지 악성코드 처리방법	없음	없음	제안방식으로 전송 후 무료백신 업데이트를 통해 사후 조치 가능
감염PC의 보안취약점	남아있음	MS 윈도우즈 보안 업데이트 사이트를 방문하여 업데이트	제안방식 홈페이지에서 “PC 자동 보안 업데이트 S/W" 이용 업데이트
감염PC 정보수집 방법	모든 C&C 접속 IP (네트워크웜, HTTP웜 등)	CCC의 허니넷을 공격하는 네트워크웜 전파 IP	모든 C&C 접속 IP (네트워크웜, HTTP웜 등)
감염PC 사용자의 감염확인 방법	ISP로부터 e-mail 수신 싱크홀 네트워크와 접속여부 확인	ISP로부터 e-mail 수신	ISP를 통한 e-mail 수신 싱크홀 네트워크와 접속여부 확인, 감염확인 홈페이지 방문

봇감염 IP를 이용하여 사용자가 방문하여 악성봇 감염 여부를 확인하고 치료할 수 있는 시스템으로 구축할 수 있다. 사용자 PC가 알려진 악성봇에 감염되었을 경우 사용자가 감염확인을 위해 “악성봇 감염PC 확인 홈페이지”에 방문하면, 싱크홀 시스템과의 접속유무를 확인하여 감염확인을 하게 된다. 감염이 확인되는 경우 무료백신으로 1차 치료를 하고, 치료가 되지 않는 경우에는 제공하는 “감염 파일 확인 S/W”로 감염된 파일을 “악성봇 감염PC 확인 홈페이지”로 업로드 하도록 유도한다.

제안방식은 국내 대다수 초고속 인터넷 가입자가 유동IP를 사용하는 것을 감안하여 최근 5분~10분 사이의 접속 기록만을 악성봇 감염 IP 목록 DB에서 조회하도록 하여 감염 여부 확인에 대한 신뢰성을 높일 수 있다. 그러나 감염 PC가 NAT를 통한 사설 IP를 사용하는 경우에는 악성봇 감염 IP 목록 DB에는 대표 IP만 저장되어 있으므로 오탐지 우려가 있다. 즉, 감염되지 않았음에도 동시간에 같은 NAT를 사용하는 다른 감염 PC가 싱크홀 네트워크에 접속 중이라면 감염된 것으로 통보할 수 있다. 따라서 “악성봇 감염PC 확인 홈페이지”에서는 NAT를 사용하는 경우 감염여부를 정확하게 알 수 없다고 알리는 것이 필요하다.

또한 CCC는 구조상 CCC의 허니넷을 공격하는 IP를 감염PC로 판단하여 조치하고 있다. 즉, 허니넷을 공격하지 않는(네트워크 취약점 스캔을 통하여 전파하지 않는) 악성봇에 감염된 경우에는 감염사실을 CCC에서 알 수 없다. 그러나 최근 취약한 PC 사용자가 해킹된 웹사이트를 방문시 다운로드 되어 감염되는 형태의 악성봇이 증가하고 있고, 네트워크 취약점 스캔을 통하여 전파되는 악성봇은 점차 줄어드는 추세이므로 CCC의 방식은 한계가 있다. 반면 제안방식에서는 감염을 위한 전파방법에 관계없이 알려진 악성봇 명령/제어 서버에 접속하는 IP를 싱크홀 네트워크로 우회시킨 후, 이를 악성봇 감염 IP 목록 DB에 저장하여 감염PC로 판단하여 조치하므로, 웹사이트를 통해 전파되는 악성봇이라 할지라도 악성봇 명령/제어 서버가 싱크홀에 적용되어 있다면 감염여부 확인이 가능하다.

제안방식은 싱크홀과 CCC를 혼합한 형태로서 감염PC의 1차적인 악성행위를 차단한 상태에서 해당 악성봇의 감염이 확인되면 치료할 수 있는 체계를 구축하고자 하였다. 악성봇 치료 후 윈도우즈 보안 업데이트를 유도함으로써 감염 PC가 가지고 있는 보안 취약점을 근본적으로 제거할 수 있다. 다만 싱크홀에 접속하지 않고 있는 감염 PC(알려지지 않은 악성봇에 감염된 감염PC)의 경우에는 악성봇 감염 확인 단계에서 감염되지 않은 PC로 조회되므로 감염되었다 할지라도 치료 등의 조치가 어렵다. 그러나 기존의 싱크홀 기법이나 CCC 기법 모두 알려진 악성봇에 대해서만 조치하는 방식이므로 제안하는 방식이 기존 방식보다 효과가 떨어진다고 보기는 어렵다[표 3].

또한 CCC는 악성봇에 감염된 감염 PC 목록을 CCC

에서만 알 수 있다. 이에 따라 감염PC 목록을 ISP에 전달하여 주고 ISP에서 감염 PC 사용자에게 알려주는 방식을 이용하고 있다. 제안방식의 경우 기본적으로는 감염 PC 목록이 악성봇 감염 IP 목록 DB에 저장되어 있지만, 감염 PC에서 네트워크 현황을 확인하여 보면 싱크홀 네트워크와 연결되어 있는 것이 확인되므로 간단한 프로그램으로도 감염PC 측면에서 감염여부가 확인이 가능하다. 즉 국내 주요 포털 사이트에서 공급하고 있는 툴바나 메신저 프로그램 등에 감염 PC 확인 기능을 추가하여 누구나 손쉽게 자신의 감염여부를 확인할 수 있으므로, CCC 센터에만 정보가 집중되고 관리되어 ISP를 통하여 e-mail을 수신해야 감염여부를 알 수 있는 CCC의 경우에 비하여 다양한 감염 확인 경로의 제공이 가능하다.

CCC 프로젝트의 경우 70%의 감염 PC가 악성봇에 감염되었다는 사실을 CCC와 ISP 모두 알고 있으면서도 감염 PC 사용자의 방문을 기다리는 수동적인 방법밖에는 취할 수 없었다. 이에 비해 악성봇 싱크홀은 감염 PC 사용자의 보안의식 정도에 관계없이 해당 ISP에서 싱크홀을 적용중이라면 감염 PC의 1차적인 악성행위가 차단되는 능동적인 대응 기법이었다. 제안방식은 악성봇 싱크홀과 같이 능동적인 방식으로 감염 PC의 1차적인 악성행위를 차단한 상태에서 추가적으로 어느 정도 보안의식이 있는 사용자의 경우 자신의 PC에 남아있는 악성봇을 삭제하고 윈도우즈 보안취약점을 제거할 수 있는 손쉬운 방법을 제공함으로써 보다 안전한 인터넷 사용에 기여할 수 있다. 또한 백신에서 미 탐지된 악성코드만을 선별하여 수집하는 방법을 구현함으로써 백신의 치료율을 높일 수 있는 부가적인 기능도 수행할 수 있다.

Ⅴ. 결론 및 향후 연구방향

본 논문에서는 기존 싱크홀 시스템과 일본 CCC의 장점을 더한 악성봇 치료 체계를 구축하는 방안을 제안하였다. 제안 기법은 악성봇의 악성행위를 차단한 상태에서 감염 PC에 대한 치료를 병행하므로 싱크홀의 단점인 근본적인 치료가 어려웠던 점과, CCC의 단점인 보안의식이 낮은 감염PC에 대한 악성행위 차단이 어려웠던 점을 보완하였다. 또한 조직의 전산 담당자를 위해 관리하는 IP 대역별 감염 PC를 확인할 수 있는 방안을 제시하였고 이를 이용하여 주기적으로 감염 PC 목록을 확인한다면 악성봇 감염 PC를 줄여 나갈 수 있을 것으로 기대된다. NAT를 사용하는 기업 사용자의 경우에도 감염 PC 사용자가 직접 자신의 PC에 대한 감염 여부 사용은 할 수 없더라도 “악성봇 감염PC 확인 홈페이지”에서 감염 PC의 IP 와 사용시간을 정확하게 통보해 주므로 전산 담당자가 보안장비 검색 등을 통하면 실제 사용자를 찾아낼 수도 있을 것으로 생각된다.

“악성봇 감염PC 확인 홈페이지”의 경우 홍보를 통한 사용자의 자발적인 방문이 필요할 것으로 생각된다. CCC의 경우 프로젝트에 참여한 ISP가 감염 IP로부터 사용자를 찾는 업무, 찾은 사용자에게 경고 메일을 보내는 업무, 사용자가 경고 메일에 대해 문의시 기술 지원 업무를 적극적으로 지원함으로써 감염을 통보한 IP의 30%가 CCC의 치료 홈페이지에 방문하여 전용백신을 다운로드하는 성과를 올렸다. 이는 ISP의 노력과 더불어 일본의 높은 보안의식을 반영하는 수치라고 할 수 있다. 본 논문에서 제시한 악성봇 치료 기법은 1차적인 악성행위는 차단한 상태에서 치료를 유도하고 있기는 하지만 근본적인 치료 및 감염 PC의 취약점 제거를 위해서는 사용자의 노력이 필요한 만큼 국내 인터넷 사용자의 보안의식을 높이기 위한 노력이 필요할 것으로 생각된다.

참고문헌

[1] 한국정보보호진흥원, “2007 정보시스템 해킹・바이러스 현황 및 대응”, 한국정보보호진흥원, pp. 41-73, 2007.

[2] F. Freiling, T. Holz, and G.Wicherski, “Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks”, In Proceedings of 10th European Symposium On Research In Computer Security (ESORICS05). Springer, July 2005.

[3] P. Baecher, M. Koeetter, T. Holz, M. Dornseif, and F. C. Freiling. “The nepenthes platform: An efficient approach to collect malware”, In Proceedings of 9th Symposium on Recent Advanses in Intrusion Detection (RAID'06), pages 165-184, 2006.

[4] Cyber Clean Center, Dec 2007, Internet: https://www.ccc.go.jp/
[5] Cyber Clean Center Activity Report, Dec 2006, Internet: https://www.ccc.go.jp/
[6] 보호나라 홈페이지, Internet: https://www.boho.or.kr/

<著者紹介>

김 영 백 (Young Baek Kim) 정회원
1995년 2월 : 순천향대학교 정보통신공학과 졸업
1997년 2월 : 순천향대학교 정보통신공학과 석사
1996년 12월~2000년 3월 : 한전KDN 주임
2002년 9월~현재 : 순천향대학교 정보보호학과 박사과정(수료)
2000년 4월~현재 : KISA 인터넷침해사고대응지원센터 해킹대응팀 선임연구원
관심분야 : 인터넷침해사고대응, 정보보호

염 흥 열 (Heung-Youl Youm) 종신회원
1981년 2월 : 한양대학교 전자공학과 졸업
1983년 9월 : 한양대학교 전자공학과 석사
1990년 2월 : 한양대학교 전자공학과 박사
1982년 12월~1990년 9월:한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사, (현)논문지편집위원장, (현)상임부회장
2003년 9월~2004년 3월 : ITU-T SG17/Q10 Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
2008년 10월~현재 : ITU-T SG17 부의장
2005년 3월~현재 : 국내 ITU-T SG17 국내 분과위원회 의장
2006년 11월~2008년 2월: (구)정보통신부 정책자문단 정보보호 PM
2006년 11월~현재 : (현) IITA 정보보호 PM
<관심분야> 네트워크 보안, IPTV 보안, USN 보안, 홈네트워크 보안, 응용보안, 이동통신보안