분석보고서	'09. 11. 06. 작성

악성 봇 분석과 예방

(Analysis Malicious Bot & Protection)

작성자 : 영남대학교 @Xpert 이화진

ghkwls0308@ynu.ac.kr

- 목 차 -

1. About 봇

1) 봇의 정의

악성 봇(Malicious Bot)이란 사용자의 PC를 감염시켜, 감염된 PC와 시스템을 해커가 마음대로 조종할 수 있게 하는 악성코드의 일종입니다.
봇이라는 명칭은 마치 로봇과 같이 컴퓨터를 외부에서 조종한다는 유래했습니다.

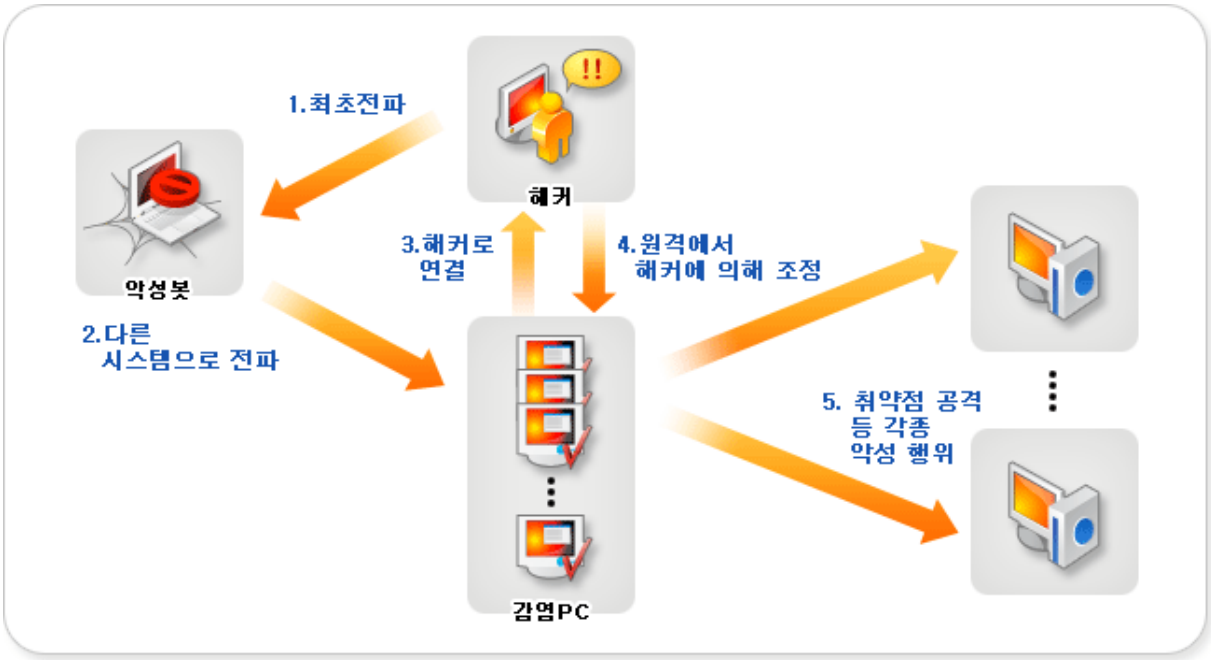
즉 봇에 감염된 컴퓨터는 악의적인 제3자로부터 여러 명령을 받아 조종됩니다.
현재 무수히 많은 봇 유형이 존재하고 있으며 매일 새로운 종이 출현하고 있는데 특히 변종이 많고 감염 여부도 일반인들이 쉽게 인지할 수 없어 치료하기가 쉽지 않습니다.

2) 봇의 특징

일반적으로 윈도우 시스템의 취약점을 악용하는 악성 봇은 웜처럼 자동으로 전파되는 특징을 가지고 있으며, 대개 악성 봇에 감염된 컴퓨터는 특정 사이트의 서비스거부공격을 비롯해 불법 프로그램을 유포하거나, 스팸메일 발송, 개인정보 유출, 애드웨어 및 스파이웨어 설치 등에 악용된다. 무엇보다 악성 봇에 대한 우려의 목소리가 높은 것은 악성 봇 프로그램의 소스가 해커들 사이에서 공유되거나 제작자간에 거래됨에 따라 수많은 변종이 양산되고 있고, 또 지능화되고 있어 사용자가 적절한 대응책을 마련하는데 어려움이 있다는 점이다.

3) 봇의 동작원리

해커에 의해 제작된 악성 봇은 윈도우와 같은 운영체제의 취약점을 가진 PC나 바이러스 백신 등이 설치되지 않은 PC를 대상으로 삼게 된다. 해커는 Botnet C&C(Command & Control)라고 불리우는 서버를 구축한 후 악성 봇에 감염될 PC를 스캐닝해 이 중 취약점 패치가 이뤄지지 않았거나, 바이러스 백신 프로그램이 설치되지 않은 PC를 감염시켜 BotNet C&C의 명령 즉, 해커의 명령을 받는 '좀비 PC'로 만들어 버린다.



특히 최근에는 복잡한 전파방법을 이용하기보다는 MSN 등과 같은 인스턴트 메신저를 이용해 봇을 전파하거나 운영체제가 아닌 응용 프로그램의 취약점을 이용하는 경우도 증가하고 있는 것으로 알려져 있다. 또, 하나의 취약점만을 이용한 전파방법에서 진화해서 동시에 몇 개의 취약점을 악용해 전파하는 등 보다 지능화되는 추세를 보이고 있다는 점이 특징이다.

이 좀비 PC에게 공격자가 중앙제어서버 프로그램으로 봇들에게 명령을 내리면 수많은 PC가 해당 서버로 접속을 시도하거나 악성 트래픽을 유발하는 패킷을 발생시켜 전송하게 되면 서버가 마비되는 것이다.

2. 악성 IRC 봇

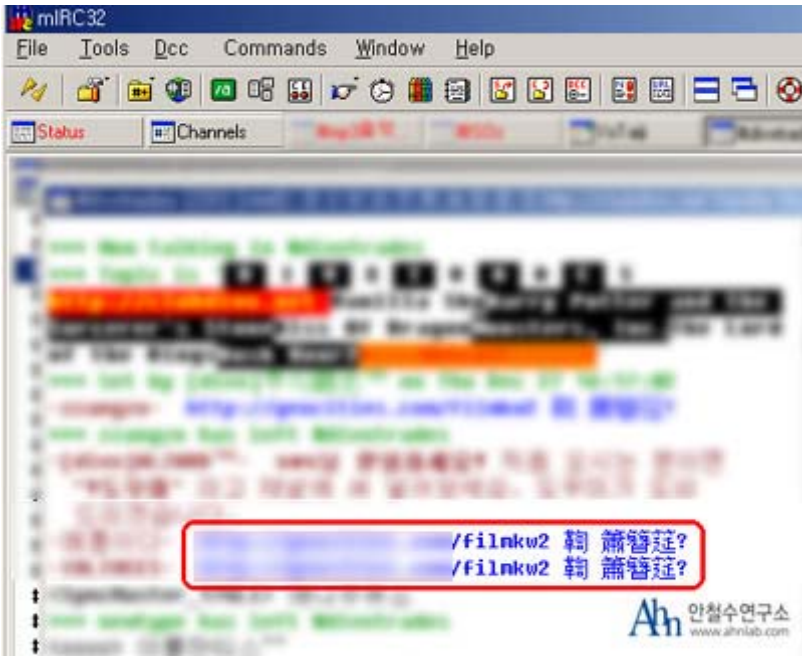
1) 정의

IRC(Internet Relay Chatting)는 일종의 채팅 서비스이며 대화를 위해서는 IRC 서버에 접속해야 한다.
IRC서버에 접속하는 프로그램은 IRC클라이언트라 부르며 윈도우에서는 mIRC가 가장 널리 사용된다. 보통 IRC클라이언트에는 스크립트를 처리할 수 있는 기능이 있고 mIRC 클라이언트에도 막강한 스크립트 기능을 포함하고 있으며 이를 IRC봇으로 부르고 있다.

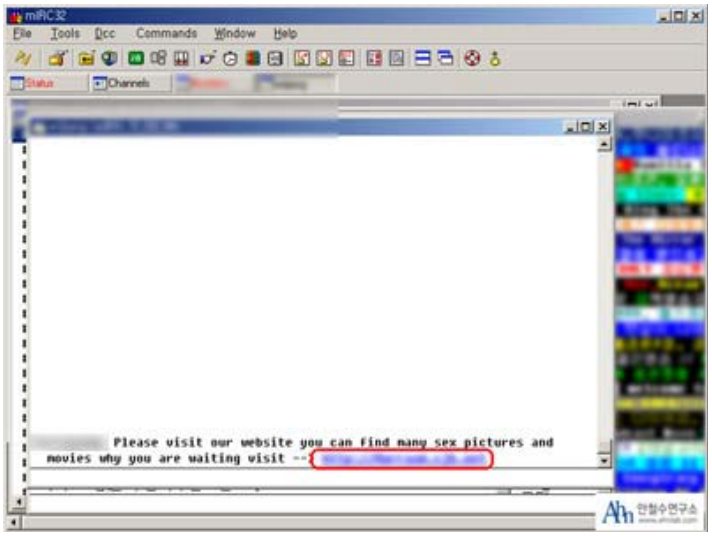
2) 동작 원리

악성 IRC봇은 IRC채널에서 채널 방장이 접속자들에게 특정 명령을 내릴 수 있고 클라이언트들이 해당 명령을 수행할 수 있는 기능을 악용한다. 이런 명령을 수행하기 위해서는 미리 정해진 IRC서버, 채널, 명령어가 필요하다. 보통 접속 서버주소는 제작자가 직접 프로그램 속에 지정한다.

감염된 컴퓨터는 사용자 몰래 특정 IRC서버에 접속해 특정 방에서 대기하며 방장의 명령이 오기를 대기한다. 악성 IRC봇은 여러 사람이 제작, 배포 하는 것으로 보이며 구 버전의 악성IRC봇은 공격이 내려지는 채널이 IRC 서버 관리자에 의해 폐쇄되는 경우 전파 외에는 다른 일은 하지 못하는 경우도 존재한다.

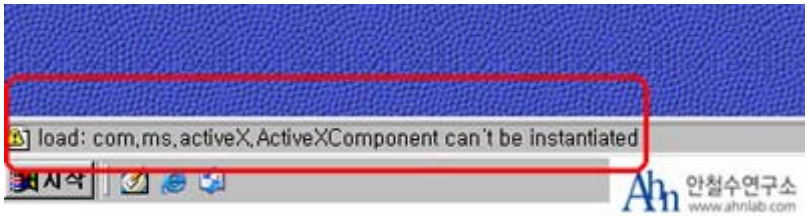


- 채널에 접속시 (URL을 mIRC 의 자동 인사말 기능을 이용하여 채널에 접속시 출력)



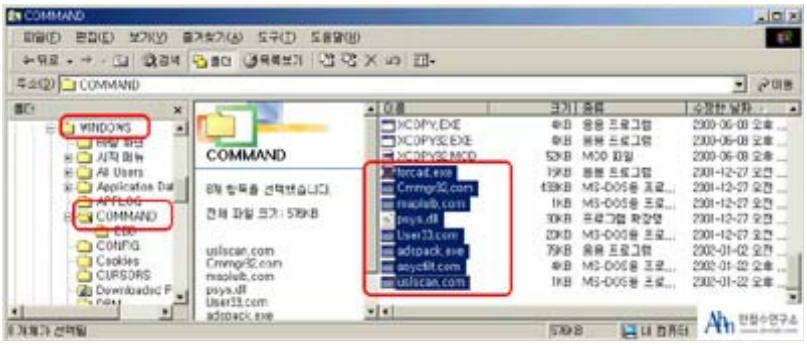
- 채널에 퇴장시 (URL을 채널에서 퇴장시 1:1 채팅 창을 오픈)

- 출력 URL 은 조금씩 다르며 다르며 웹 사이트 접속시 사용자의 시스템에 루트에 ROL.VBS 파일을 생성 하고 동영상을 가장한 웜을 다운받아 실행하게 된다. 현재까지 알려진 파일 이름은 Maram.avi.exe 이지만 다른 형태로도 존재할 수 있다.



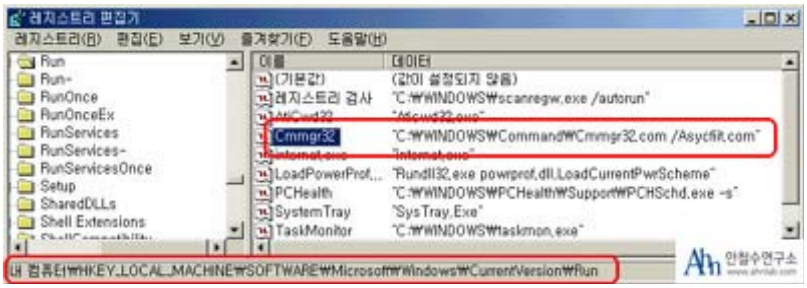
- 인터넷 익스플로러가 보안패치 되어 있다면 다음과 같은 메시지가 인터넷 익스플로러 하단에

출력되면서 감염되지 않는다.

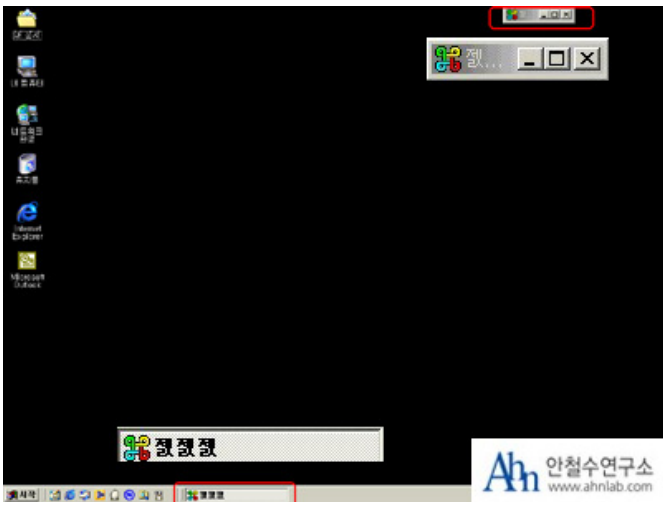


- 파일을 실행하면 윈도우의 Command 폴더 (일반적으로 C:₩Windows₩Command)에 다음과 같은 파일이 생성된다.

FORCAD.EXE 파일은 실행되면 컴퓨터를 꺼버리는 기능을한다. CMMGR32.COM 은 부팅시 자동으로 실행되도록 레지스트리를 변경해 등록된다. ASYCFIIT.COM 파일은 텍스트 파일로 mIRC의 환경설정 파일이다.나머지 파일은 백도어나 웜에서 사용하는 데이터 파일이다.

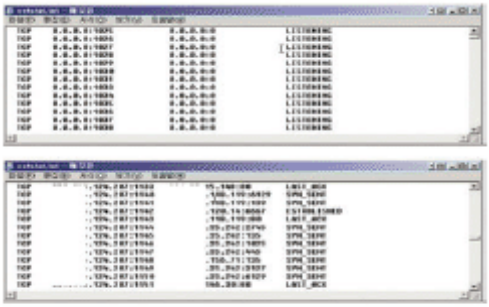


- HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run 에 Cmmgr32 생성

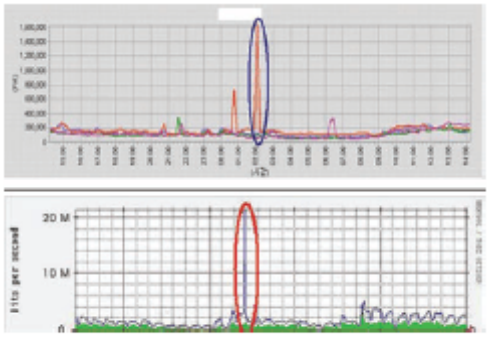


- 윈도우가 시작될 때마다 mIRC가 실행되므로 몇 초간 실행되는 그림을 볼 수 있다.

3) 증상

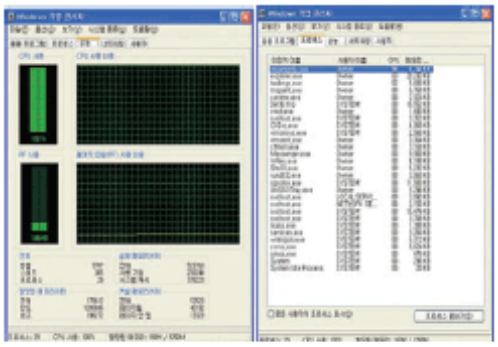


네트워크 연결 화면



특정 사이트에 대한 서비스 거부 공격시 트래픽 증가

- 불필요한 네트워크 트래픽이 발생한다.
다른 시스템을 감염시키거나 네트워크를 통한 공격을 위해 네트워크 트래픽이 발생한다.



CPU 사용률이 100%까지 증가

- CPU 사용률이 100%까지 올라가면서 컴퓨터가 느려진다

3. 악성 봇 현황

전 세계 악성 봇 감염추정 PC중 국내 감염 PC 비율이 16.9%에 달하고 있다. 전 세계 봇 감염 추정 PC는 9월에 일평균 6만여대에서 10월에는 5만여대로 16% 감소했지만, 국내 사정은 오히려 9% 증가해 봇 감염율이 4%가량 늘어난 것이다.

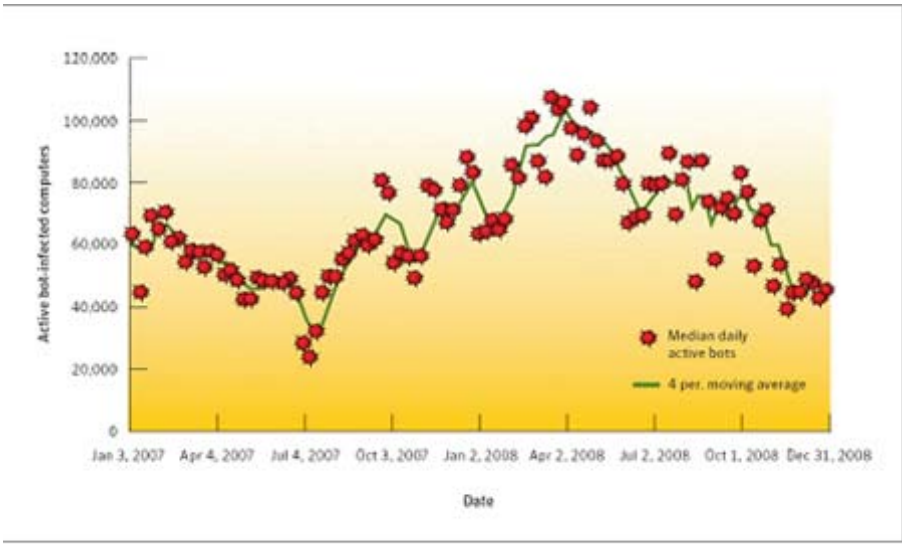
한국정보보호진흥원(KISA)은 월보에서 “국내의 경우 TCP/139, 80, 135 포트에 대한 감염시도 트래픽이 많았다. 허니넷에 유입된 웜들을 분석한 결과 주로 Mybot, Sdbot 등이 국내에서 활발한 활동을 하고 있었고,
봇의 전파에 사용된 주요 포트는 NetBIOS 관련 포트인 445, 139, 135와 웹 관련 80포트, MS-SQL 관련 포트인 1433 등으로 지난달 Top5를 차지한 포트들이 그대로 주요 포트로 사용되고 있다.

○ 악성 Bot의 전파에 이용되는 주요 포트 목록

포트	관련 취약점 및 웜/악성 Bot
80	WebDAV (MS03-007) 취약점, Agobot, Polybot 등
135	RPC DCOM 취약점(MS03-026, MS03-039), Polybot, Spybot 등
139	NetBIOS Brute force login attempts
445	LSASS(MS03-026, 039, 049 등) 취약점, Agobot, Polybot, Spybot, Zotob, IRCBot, SDBot 등
901	NetDevil 취약점 이용 Bot
903	NetDevil2 취약점 이용 Bot
1023	Sasser Backdoor 취약점 이용 Bot
1025	DCOM (MS03-026) 취약점 이용 Bot
1080	MyDoom.F 취약점 이용 Bot
1234	SubSeven 취약점 이용 Bot
1433	MS-SQL Login Brute force 취약점 이용 Bot

포트	관련 취약점 및 웜/악성 Bot
2556	Bagle, Bagle2
2745	Bagle, Bagle2
3127	MyDoom.A
3140	Optix Backdoor, Mockbot 등
3176	MyDoom.AB 등
5000	UPNP (MS01-059)
5554	Sasser ftpd Backdoor
6129	Dameware, Mockbot 등
9898	Dabber Backdoor
12345	SubSeven
17300	Kuang2

무엇보다 악성 봇의 가장 큰 문제는 악성 봇 프로그램의 소스가 해커들 사이에서 공유되거나 제작자간에 거래됨에 따라 수많은 변종이 양산돼 사용자가 적절한 대응책을 마련하기가 어렵다는 것이다.
악성 봇의 공격이 심각한 문제로 대두될 수밖에 없는 또 하나의 문제는 공격의 파괴력이 엄청나다는 것 외에도 감염 여부를 쉽게 알아내기가 힘들다는데 있다.



[그림 5] 전세계 일평균 활동중인 악성 봇 감염 PC수

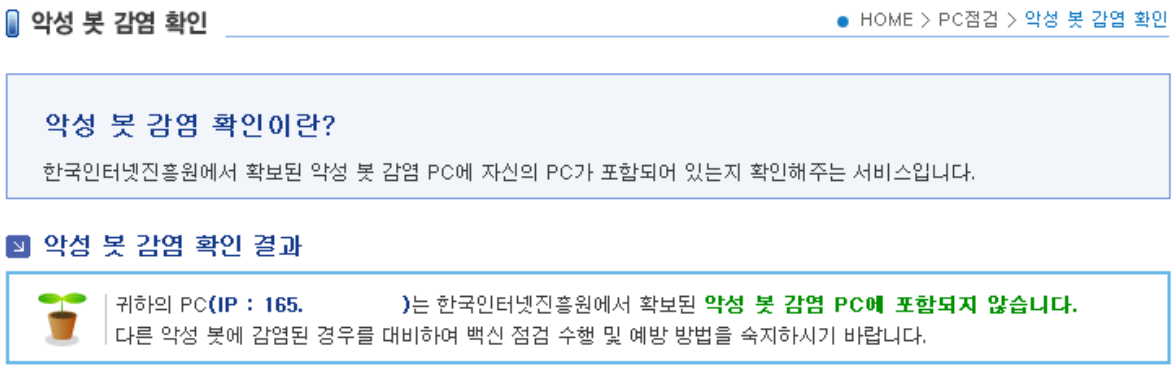
최근의 악성 봇은 일반적인 웜이나 바이러스에 감염 후 나타나는 증상처럼 PC 사용과정에서의 속도 저하나 접속 장애 등의 문제를 일으키지 않기 때문에 일반 사용자들이 봇의 감염여부를 알아내기가 쉽지 않다는 것이 전문가들의 공통된 의견이다. 또 최근에는 악성 봇이 백신 프로그램이나 다른 보안 프로그램을 공격해 강제 종료시키거나 백신 프로그램의 업데이트를 차단함으로써 자신의 존재를 은폐하기도 해 사용자에게 더욱 위협적인 존재가 되고 있다.

4. 예방방법

- 정보보호 5대 실천수칙 실천하기

수칙1 자동 보안패치 설정하기
수칙2 백신 프로그램 또는 개인 방화벽 등 보안 프로그램을 설치
수칙3 컴퓨터의 로그인 패스워드는 8자리 이상의 영문과 숫자로 구성 3개월 마다 변경
수칙4 신뢰할 수 있는 웹사이트에서 제공하는 ActiveX 프로그램 설치하기
수칙5 공인인증서 USB 저장 등 금융 정보 안전하게 관리하기

보호나라 웹사이트(http://www.boho.or.kr)를 방문하여 쉽고 간단하게 내 PC가 악성봇에 감염됐는지 여부를 확인해 볼 수 있다.
보호나라 웹사이트에 접속하여 [PC 점검] ->[악성 봇 감염확인]을 클릭하면 악성 봇 감염 확인 결과를 바로 알 수 있다.



5.참고문헌

- 보호나라 http://www.boho.or.kr/index.jsp
- 안철수 연구소 악성코드 분석가 차민석 님 글
- 안철수 연구소 바이러스/스파이웨어
- 보안뉴스 www.boannew.com
  [월간 시큐리티월드 통권 제147호]
- IT전문블로그 www.blog.naver.com/itexpert 2007