인터넷 채팅 환경에서 악성 Bot 탐색 시스템

이동훈O* 하경휘* 최진우* 우종우* 박재우** 손기욱** 박춘식**
*국민대학교 컴퓨터학부
**국가보안기술연구소
{dhlee^O, khha, jwchoi, cwwoo}@cs.kookmin.ac.kr, guru@etri.re.kr

A System for Detecting Malicious Bot in Internet Relay Chat

Donghun Lee^O* Kyounghui Ha* Jinwoo Choi* Chongwoo Woo*
Jaewoo Park** Kiwook Sohn** Chunsik Park**
*School of Computer Science, Kookmin University
**National Security Research Institute

요 약

최근 악성코드들의 주요한 특징 중 하나는 악성코드와 해킹기법이 결합된 형태이며 기존의 악성코드들 보다 더욱 공격 성향을 내포하고 있다는 점이다. 이러한 악성코드에는 대표적으로 IRC를 이용하는 Bot 계열 악성코드들이 있으며 해킹과 결합되어 그 피해 또한 스팸성 악성코드들보다 심각하다. 또한 이러한 악성코드들은 다양한 변종이 신속하게 제작 및 유포되고 있어, 백신을 이용한 방어만으로는 적절히 대처할 수 없다는 문제점을 가지고 있다. 본 논문에서는 IRC를 이용하는 공격성 악성코드들을 분석하고, 이들 악성코드들을 효과적으로 탐색하여 감염 여부를 판단할 수 있는 악성 Bot 탐색 시스템의 설계 및 구현에 관하여 기술한다.

1. 서론

일반적으로 악성코드란 사용자의 의사와 이익에 반해 시스템을 파괴하거나 정보를 유출하는 등의 악의적인 활동을 수행하도록 제작된 소프트웨어를 의미한다[1]. 최근 악성코드의 특징은 해킹과 결합하여 공격기능을 내포하고 있으며 그 전파속도가 매우 빠르다는 점이다. 이러한 악성코드의 대표적인 사례로는 **Bot** 계열 악성코드들을 들 수 있으며 그 피해는 점차 증가하고 있다[2].

[표 1] 악성코드의 전파방법과 감염벡터

Infection Vector	Beginning of 2003	End of 2003	Change
Internet Worms	10	30	+200%
Mass-mailers	80	98	+23%
Mailers	9	17	+89%
Network Shares	41	79	+93%
P2P(KaZaA)	9	21	+133%
AVKill	20	35	+75%
DDOS	3	15	+400%
Bot-Net	2	9	+350%
Self Updating	11	25	+127%
Spoofed Email	10	18	+80%
BackDoor	18	38	+111%
Instant Messenger	7	12	+71%

[표 1] 은 악성코드에 의해 증가된 전파 방법과 감염벡터를 수치화 한 표이다[3]. [표 1]에서 보는 바와 같이, **IRC** 채널을 사용하는 **Bot** 계열 악성코드의 증가와 이로 인한 분산 서비스 거부 공격**(Distribute Daniel of Service)**이 급격히 증가한 것을 확인할 수 있다. 이들 악성코드의 공격형태는 특정 포스트에 대한 스캐닝, 시스템 사용자 정보를 포함한 각종 정보 유출, 특정 호스트로 분산 서비스 거부 공격, 특정 호스트의 취약성 공격 등을 들 수 있다.

본 논문에서는 이러한 악성코드들에 의한 피해 감소를 목적으로 **Bot** 계열 악성코드를 탐색할 수 있는 악성 **Bot** 탐색 시스템의 설계 및 구현에 관하여 기술한다. 특히, 백신이 갱신되기 전에 이미 수많은 변종들이 제작 유포되기 때문에 단순히 백신에만 의존하기 보다는 이러한 탐색 시스템을 활용하여 감염여부를 신속히 판단하는 것도 피해감소를 위한 주요한 대처 방안으로 활용될 수 있을 것이다.

2. 관련연구

IRC를 이용하는 **Bot** 계열 악성코드를 이해하기 위해서 다음과 같이 **IRC**에 대한 기본 개념을 기술하였고, 악성 **Bot**의 기능을 자세히 분석하였다.

2.1. IRC(Internet Relay Chat)

IRC는 클라이언트/서버 기반의 인스턴트 메시징 서비스 **(Instant Messaging Service)** 중 하나이다. **IRC** 프로토콜**(RFC 1459)**은 **TCP/IP**를 사용하며 주로 **6667**번 포트**(Port)**를 사용한다[4][5]. **IRC**는 일반적으로 다음의 세 가지 특징을 가지고 있다[6].

- **IRC** 채널 내의 사용자는 유일한 사용자 대화명을 가져야 하며, 한 명 이상의 **"Channel Operator"**라는 사용자가 존재한다.

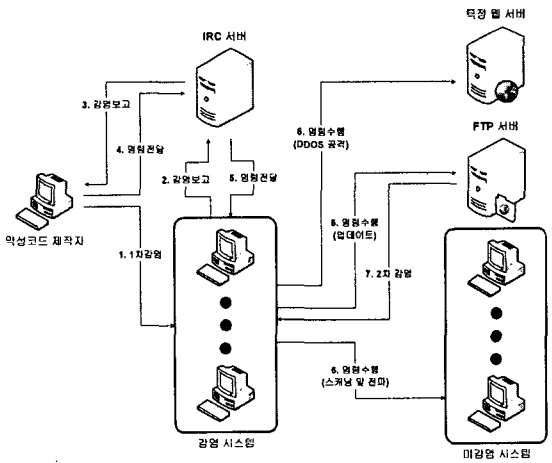
- IRC는 사용자 사이에 실행할 수 있는 스크립트를 포함하는 메시지 교환이 가능하여 DCC(Direct Channel Connections)를 사용한 P2P(Peer-to-Peer)로도 실행 가능하다.
- IRC는 Bot이라는 자동화된 프로그램을 사용하여 IRC 클라이언트를 실행할 수 있다.

IRC는 mIRC, Pirch, ircII, WSIRC, ChatMan, Virc 등과 같은 IRC 서버에 접속할 수 있는 클라이언트 프로그램이 필요하며 그 중 mIRC가 대표적이다.

2.2. IRCbot

악성코드와 해킹이 결합된 형태의 악성코드 대부분은 Bot 계열 악성코드들이다. Bot이란 프로그램 또는 사용자가 수행하는 일련의 동작들을 자동으로 수행하는 프로그램을 의미한다[7][8]. Bot 계열 악성코드들은 윈도우즈 패스워드 취약점이나 윈도우즈 보안 취약점 이외에도 다양한 방법을 사용하여 전파되고 IRC 채널에 자동으로 접속하여 공격자로부터 분산 서비스 거부 공격이나 시스템의 정보 유출, 특정 호스트의 취약성 공격, 악성코드들의 업데이트 등에 대한 명령을 전달받아 수행한다[9].

초기 Bot 계열 악성코드들은 단순한 Syn-Flooding의 공격 방법을 사용하였으나 현재는 Syn-Flooding 이외에 HTTP-Flooding, ICMP-Flooding, UDP-Flooding 등과 같이 여러 공격 방법을 사용하고 있다.



[그림 1] Bot 계열 악성코드의 동작 과정

[그림 1]은 Bot 계열 악성코드들이 공격자에 의해 명령을 전달 받아 분산 서비스 거부 공격과 같은 공격 작업을 수행하는 과정을 도식화한 것이다. Bot 계열 악성코드의 수행 절차는 다음과 같다.

1. 패스워드 취약점이나 윈도우즈 취약성 등을 이용하여 Bot 계열의 악성코드를 전파
2. Bot을 사용하여 IRC 채널에 접속하여 시스템 감염을 공격자에게 보고
3. IRC 채널을 통해 시스템 감염 여부를 확인
4. IRC 채널을 통해 공격자의 공격 명령을 전달
5. IRC 채널을 통해 공격자의 공격 명령을 접수
6. 감염된 시스템에서 특정 명령 수행(DDoS 공격, 악성코드 업데이트, 스캐닝 및 악성코드 전파)

Bot 계열 악성코드로는 Gaobot, IRCBot, Korgo, SdBot, Agobot 등이 대표적이다. IRCBot, Agobot 과 같은 대부분의 Bot 계열 악성코드는 공격자에 의해 미리 생성한 IRC 채널에 접속하여 공격자의 명령을 전달 받아 수행하는 공통된 특징을 내포하고 있다.

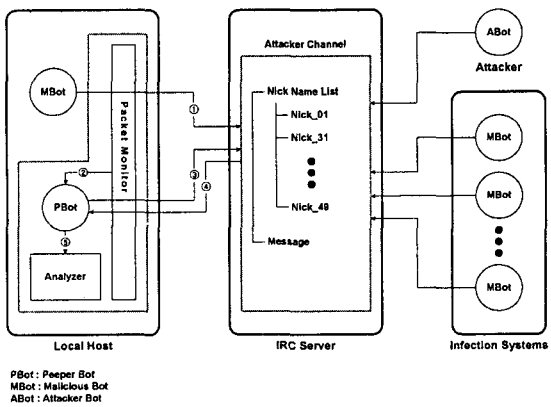
3. 설계

본 연구의 시스템은 Bot 계열 악성코드들이 내포하고 있는 공통된 특징들에 착안점을 두고 설계하였다. 공통된 특징은 크게 세 가지로 나타나며 다음과 같다.

첫 번째, Bot 계열 악성코드들, 또는 이들로부터의 변종 악성코드들의 동작 과정 중, 일련의 공통된 작업이 존재한다는 점이다. 즉 Bot 계열 악성코드들은 실행 초기 단계에서 IRC 서버에 접속하고, IRC 서버 내의 특정 채널에 진입하여 공격자의 명령을 수신하기 위한 대기 과정을 공통적으로 수행 한다는 것이다.

두 번째, Bot 계열 악성코드가 사용하는 IRC 채널 내의 사용자 대화명이 일정한 패턴을 가지고 있다는 점이다. IRC 채널 내에서 사용자 대화명은 유일성을 가진다. Bot 계열 악성코드가 IRC 서버에 접속하여 채널에 진입하기 위해서 유일성을 가지는 사용자 대화명을 생성하게 된다. 그러므로 Bot 계열의 악성코드는 일정한 패턴을 가지는 사용자 대화명을 생성한다.

세 번째, Bot 계열 악성코드들이 공격자의 명령에 대해 동일한 작업을 수행한다는 점이다. 배포된 악성코드들은 동일한 프로그램이기 때문에 IRC 채널에 접속해 있는 악성코드들은 공격자의 명령에 동일한 작업을 수행하고 동일한 메시지를 IRC 채널을 통해 공격자에게 전달한다.



[그림 2] 시스템 구조

[그림 2]는 위에서 언급한 세 가지 특징들을 고려하여 설계된 시스템의 전반적인 흐름을 도식화 한 것이다. 본 시스템은 악성 Bot이 전송하는 패킷의 캡쳐 및 분석을 담당하는 Packet Monitor 모듈, IRC 채널의 정보를 수집하는 PBot(Peeper Bot) 모듈, 수집한 정보를 분석하여 악성 Bot을 탐지할 수 있는 Analyzer 모듈로 구성된다.

시스템의 수행은 다음과 같이 진행된다. 우선 MBot (Malicious Bot)은 악성코드에 의해 수행되어 IRC 채널에 접속하고 공격자의 명령을 기다린다. 공격을 지휘하는 ABot은 MBot에게 공격자의 특정 명령을 전달한다(①).

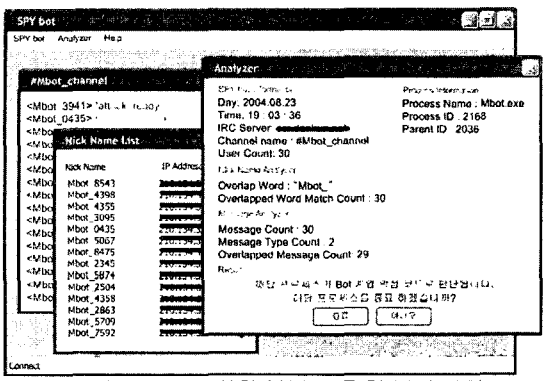
Packet Monitor 모듈은 패킷 모니터링을 수행하여 시스템 내에서 IRC 채널에 접속을 시도하려는 패킷들을 발견하면 그 패킷들을 분석한다. 주로 IRC 서버의 주소, 사용자 대화명, 접속 채널명, 채널 암호 등의 정보를 분석하여 PBot 모듈에게 그 정보를 전달한다(②).

IRC에 접속을 시도하려는 프로세스가 Bot 계열 악성코드인지를 판단하기 위해서는 IRC 채널 내의 정보(사용자 대화명 목록과 메시지 정보)를 획득해야만 한다. PBot 모듈은 Packet Monitor 모듈이 제공한 정보를 사용하여 IRC 채널에 접속하고 IRC 채널이 공격자가 생성한 채널인지 판단할 수 있는 정보를 수집을 수행한다(③, ④).

Analyzer 모듈은 PBot 모듈이 수집한 정보를 전달받는다(⑤). PBot 모듈에게서 전달받은 사용자 대화명 목록의 대화명을 분석하여 일정한 패턴 유무를 판단하고 메시지 정보를 분석하여 메시지의 동일성을 판단한다. 이와 같은 정보들을 기반으로 공격자가 생성한 IRC 채널인지 판단할 수 있다. 즉 대한 감염 여부를 식별할 수 있다.

4. 구현

본 시스템은 MFC의 C++ 언어를 사용하여 윈도우즈 XP 환경에서 구현 하였고 임의의 IRC 채널과 Bot을 생성하여 실험하였다.



[그림 3] PBot에 의한 정보 획득 및 분석 화면

[그림 3]은 Bot 계열 악성코드의 패킷을 분석하여 IRC 채널에 접속한 PBot이 수집한 정보와 그 정보를 분석한 화면이다. 분석 화면은 메시지 정보, 사용자 대화명 목록, 분석 정보의 세 화면으로 구성되어 있다.

1. 메시지 정보 화면은 PBot이 수집한 채널 내의 메시지 정보를 출력한다.
2. 사용자 대화명 목록 화면은 채널 내에 접속한 사용자의 사용자 대화명과 IRC 서버에 접속한 IP를 출력한다.
3. 분석 정보 화면은 Bot 계열 악성코드의 특징을 분석한 정보를 및 Bot 계열 악성코드에 감염여부를 출력한다. 감염되었을 경우, 경고화면과 해당 프로세스를 종료하도록 한다.

5. 결 론

최근 피해가 급증하고 있는 Bot 계열 악성코드들은 공격성향을 가지며 그 변종들이 기존의 백신보다 훨씬 빠르게 제작 및 유포된다는 점에서 그 대처 방안이 시급하게 대두되고 있다.

본 논문에서는 이러한 Bot 계열 악성코드들과 그 변종들 사이에 공통된 특징을 분석한 정보를 기반으로 Bot 계열 악성코드의 탐지가 가능한 시스템 환경을 설계 및 구현하였다.

본 연구의 시스템은 갱신된 백신이 방어해 주기 이전에 신속히 악성코드를 탐지할 수 있으며 더 나아가 공격자가 생성한 IRC 채널 내에서 획득한 IP 정보 등을 활용하여 IRC 채널 내에 접속되어 있는 감염 시스템의 대처 방안에 관한 연구도 진행될 수 있을 것이다.

참 고 문 헌

[1] F. Cohen, "Computer viruses-theory and experiments", Computers and Security, Vol. 6, p22-35, 1987.

[2] 한국정보보호진흥원, "2004년 07월 해킹바이러스 통계 및 분석 월보", available at http://www.krcert.org/, 2004.

[3] B. Hughes, "WildTrends 2003: A Look at Virus Trends in 2003 and a Few Predictions for 2004", available at http://www.slyck/misc/TruSecure%20Report.pdf, 2003.

[4] J. Oikarinen and D. Reed, "Internet Relay Chat Protocol", available at http://www.ieft.org/rfc/rfc1459.txt?number=1459, 1993.

[5] C. Kalt, "Internet Relay Chat: Architecture", available at http://www.irchelp.org/irchelp/rfc/rfc2810.txt, 2000.

[6] J. Jim, "BotNets: Detection and Mitigation", available at http://www.fedcirc.gov/library/documents/botNetsv32.doc, 2003.

[7] R. Puri, "Bots & Botnet: An Overview", available at http://www.sans.org/rr/papers/36/1299.pdf, 2003.

[8] R. A. Grimes, "Malicious Mobile Code", O'REILLY, ISBN 1-56592-682-X, 2001.

[9] 한국정보보호진흥원, "Agobot(rbot) 최신 변종 분석 보고서", available at http://www.krcert.org/, 2004.