Botnet의 자가 형성에 대응한 효율적인 방어책에 대한 연구

조주형*, 김용*, 황은영*, 박세현*

*중앙대학교 전자전기공학부

황현욱*, 배영철*, 윤영태*

*한국전자통신연구원 부설 국가보안기술연구소

A Study of an effective Defence against self-configuring Botnets.

Joo-Hyung Jo*, Yong Kim*, Eun-Young Hwang*, Se-Hyun Park*

*School of EE Engineering, Chung-Ang University, Seoul, Korea.

Hyunuk Hwag*, Byungchul Bae*, Youngtae Yun*

*Electronics and Telecommunications Reasearch Institute National Security Reasearch Institute

요 약

유행처럼 시도하던 DDoS 공격, 특정 목적을 위한 트로이 목마, 스팸메일을 통한 악성코드 유포, 개인 정보 유출 등 악의적인 공격들이 공격자에 의해 조종당하는 Bot에 의해 쉽게 이루어지고 있으며, 특별한 해결방안이 있는 것도 아니다. 이러한 Bot들이 공격자를 통해서가 아닌 자체적으로 P2P 네트워크를 자가 형성하여 공격한다면 탐지는 더욱 어려워지게 된다. 이와 같은 자가 형성에 대응한 효율적인 방어책을 로컬 시스템 간의 네트워크 모니터링 에이전트를 도입하여 해결하고, 에이전트들이 자가 형성하여 실시간으로 Bot에 대한 정보를 공유하고, 이 정보를 기반으로 시스템을 감시하여 Bot을 탐지하는 방어책에 대해 본 논문에서 기술한다.

I. 서론

Bot은 트로이 목마로 활용되거나 웜, 바이러스, 애드웨어, 스파이웨어 등을 설치하기 위한 목적으로 많이 사용되고 있다. 또한 피싱을 통해 스팸메일을 뿌려 미리 만들어 둔 위장 사이트를 방문하도록 유도해 개인 금융정보를 탈취, 금융 정보 등을 통째로 가로채는 행위가 일어나고 있다. 위와 같이 최근 금전적인 이득을 취하기 위한 공격자들은 보안 취약점이 발견된 임의의 PC를 좀비 PC처럼 만들어 추적이 쉽지 않게 만들고 이들을 거느리고 공격자가 자유자재로 제어할 수 있도록 한다. 이러한 목적으로 최근 사용되고 있는 공격기법이 악성 Bot이다. 공격자는 수천에서 수만에 이르는 시스템을 해킹하여 악성 Bot을 설치하고, 이 악성 Bot들을 네트워크로 묶어 동시에 제어함으로써 자신의 목적을 위해 충실히 따르는 좀비 시스템을 보유하게 되는 것이다. 이는 곧 Botnet이 공격자들의 제 3의 악의적인 행위를 하기 위한 클라이언트 부대가 되어 주는 것이다.

II. 본론

2.1 Botnet의 개요

Bot은 제어를 위해 IRC(Internet Relay Chat) 채널을 이용하며 이미 해킹당해 해커에 의해 제어당하는 시스템을 말하며, 스스로 움직이지 못하고 인간에 의해 제어당하는 기계인 로봇과 마찬가지로 '악성 Bot'은 해커에 의해 제어당하는 시스템을 말한다. 기존의 Bot들은 제어를 위해 IRC채널을 이용하는 경우가 많다. IRC 채널는 다수의 사용자들과 텍스트 메시지와 파일을 공유하며, 한 클라이언트의 사용자가 다른 클라

<본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(중앙대학교 홈네트워크 연구

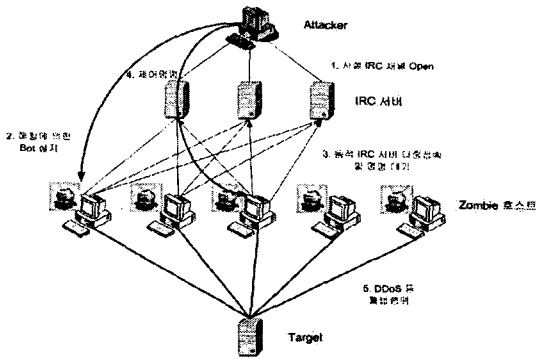
이언트 상에서 실행 가능한 메시지를 전송하는 용도이기 때문에 공격자가 IRC을 통해 Bot들에게 명령을 내리는 경로로 사용하게 되는 것이다. 이렇게 공격자가 소유한 IRC 채널에 연결하여 감염된 호스트를 'Bot'이라고 하고, IRC 채널에 연결된 Bot들로 이루어진 네트워크를 'Botnet'이라고 한다. 즉 Botnet은 공격자로부터 명령을 기다리며 명령을 받으면 군 조직처럼 행동하는 분산된 구조라 볼 수 있다.

2.2 공격

구분	악성 Bot/Botnet	트로이목마	DDoS 전용 툴
	다수시스템 동시제어 가능		다수시스템 동시제어 가능
악의적인 행위	DDoS 공격, 정보유출, 백도어, Warez 사이트 운영, 스팸발송, 피싱 등 대단히 다양	개별 시스템의 파일 시스템 제어, 프로세스제어, 백도어, Key Logging 등	DDoS 공격
주요 제어 포트	주로 IRC 포트 (6665~6669/TCP)	종류별로다양 (BackOrifice: 31337/TCP, NetBus: 12345/TCP 등	종류별로다양 (Trinoo: 1524, 27665, 27444/TCP, 31335/UDP)
종류	Agobot, rbot, rxbot, sdbot 등	BackOrifice, NetBus, SchoolBus 등	Trinoo, TFN2K 등

[표 1] 대표적인 Bot의 예

악성 Bot은 트로이목마 프로그램들과는 달리 다수의 좀비 네트워크를 형성하여 동시에 제어할 수 있고, 네트워크의 트래픽을 마비시키는 DDoS 전용 툴과는 달리 다양한 악의적인 행위를 할 수 있다. 제어에 사용되는 포트도 IRC 포트를 이용하여 탐지가 대단히 어려운 특징을 지니고 있다. 그리고 수없이 많은 변종들로 인해 보안 업체에서도 대응이 쉽지 않은 것이 사실이다. IRC 채널을 통한 Bot의 소스코드는 대부분 공격자 성향에 따라 기능을 추가, 삭제할 수 있도록 구현되어 있다. 따라서 새로운 취약점이 나올 경우 기존의 소스 코드에 취약점 공격 코드만 추가하면 쉽게 변종 제작이 가능하다는 점에서 더욱 대응이 어려워지고 있다.



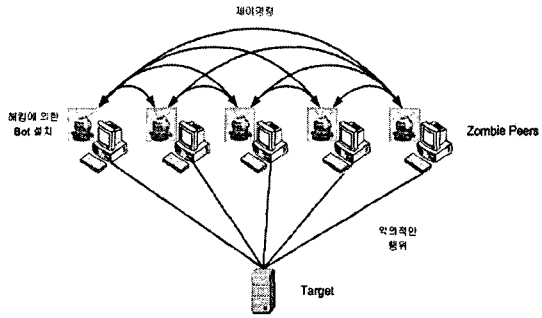
[그림 1] Bot 감염 및 공격절차

일반적으로 악성 Bot을 설치하기 위해 시스템을 해킹하는 다양한 방법들이 사용된다. 시스템을 해킹한 후에 해킹 피해 시스템에 대한 지속적인 접근을 위한 백도어로써 Bot을 설치한다. 이후 공격자는 악의적인 공격을 목적으로 사설 IRC 채널을 개설하고 Bot에 감염된 시스템들에게 접속 명령을 내린다. Bot들이 IRC 채널에 접속을 하게 되면 Botnet이 형성된다. 이러한 과정을 거쳐 Botnet이 형성되면 공격자는 IRC 채널을 통해 join한 Bot들을 제어할 수 있게 된다. 이 채널을 통해 대표적으로 DDoS 공격, 악의적인 시스템 제어, 정보유출을 통한 불법적인 거래, E-mail 스팸을 통한 악성코드 유포 등을 실행한다.

2.3 Botnet의 자가 형성

최근 들어 Bot이 몸집을 자꾸 줄여나가고 있다. 이는 침입탐지 망에 걸리지 않기 위해서다. 이와 같이 공격자들의 명령을 받는 일반 네트워크 Botnet은 네트워크를 한데 모으고자 하는 해커의 수가 증가하면서 좀비 컴퓨터의 보안을 유지하려는 경쟁이 더욱 치열해지고, 따라서 더 많은 수의 감염된 컴퓨터를 축적하기 위해 Bot의 몸집을 줄여나가는 형식으로 진화하고 있다. 또한 이는 고속 인터넷을 사용하는 가정 사용자들이 자신들의 컴퓨터 보안을 유지하기 위해 더 많은 조치를 취하고 있기 때문이기도 하다. 그 외에 Bot의 진화 중 본 논문에서 다루고자 하는 Bot의 진화는 바로 Bot들이 스스로 네트

워크를 자가 형성하여 Botnet 스스로 악의적인 행위를 하는 것이다. 이러한 구조는 공격자로부터 공격명령을 받는 서버-클라이언트 구조가 아니라 P2P 네트워크를 구성하여 P2P 기술의 장점을 살렸기 때문에 IRC 채널의 중앙 서버 감시를 피할 수 있으며, 좀 더 정교하고 복잡하다는 문제를 갖는다.



[그림 2] Bot의 자가 형성 구조

위 [그림 2]에서 보여주고 있듯이 사전에 설치된 Bot은 스스로 다른 원격의 시스템에 자기와 같은 혹은 변종의 Bot을 설치하여 Bot들 간에 명령을 내리거나 군집적으로 악의적인 행위를 할 수 있는 것이다. 이렇게 네트워크를 자가 형성한 Botnet은 특정한 서버가 없기 때문에 특정 포트의 트래픽 모니터링 같은 대응책으로는 Bot 탐지가 어려우며, Bot들이 형성한 네트워크의 다른 Bot들에게 백신 프로그램에 대한 자신들의 방어를 위해 별도의 드라이버를 설치, 분배하는 방법으로 은폐 기능을 구현할 수 있다. 이러한 자가 형성된 Botnet을 한 로컬 시스템 관리자가 탐지, 방어한다는 것은 불가능에 가까우며, 이는 다른 방어책의 접근을 필요로 하고 있다.

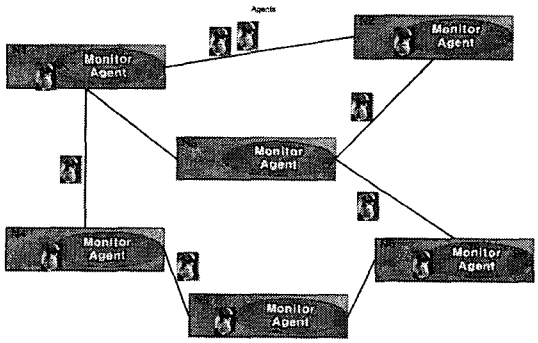
2.4 대응책

Bot 및 Botnet은 수십에서 수만까지 사용자 PC가 마치 군 조직처럼 구성되어 명령을 기다리는 서버-클라이언트 구조로 운영되고 있기 때문에 이를 한 순간에 제거하거나 대응하는 것은 쉽지 않다. 하지만 현재까지의 Botnet들은 특정한 웹사이트로부터 Bot 코드를 다운로드 받거나, 특정한 동적 도메인 네임 또는 IP 주소를 가진 Bot 서버로부터 제어를 받는 특성을 가지고 있다. 이러한 특성을 바탕으로 로컬 시스템에서는 다음과 같은 탐지가 필요하다.

- 비정상 IRC 트래픽 실시간 감시
- Bot 공격 트래픽 감시
- 비정상 DNS 질의 감시

위와 같은 감시를 통해 로컬 시스템에서는 Bot 감염 서버를 제거하고 시스템의 보안패치를 자동적으로 실행하여야 한다. 감염된 Bot들 간에 연결이 되어있기 때문에 이 연결고리를 제거함으로써 다수의 Bot들을 공격자가 잃게 할 수 있다. 감시가 된 Bot에 대한 백신을 업데이트하고, 새로운 Bot이 발견될 때마다 개인 방화벽의 데이터베이스를 갱신해야 한다.

그러나 앞에서 설명하였듯이 Bot들이 IRC 서버를 거치는 서버-클라이언트 구조가 아니라 순수 P2P 형태로 Botnet이 자가 형성되면 탐지가 더욱 어려워진다. 이에 대한 대응책의 기본 구조는 네트워크 포트 모니터링을 통해 특정 포트들의 트래픽 증가를 관찰하며 스스로 신뢰된 Peer들과 정보를 공유하며 Bot들의 침입을 막고 감시된 Bot들은 제거 하는 에이전트가 필요하다.



[그림 3] Monitor Agent의 자가 형성

[그림 3]에서와 같이 본 논문에서 제시하는 시스템의 에이전트는 다른 원격 시스템의 에이전트와 P2P 네트워크를 자가 형성한다. 그리고 다음과 같이 요청된 연결을 3단계로 나누어 연결을 받아들일 것이지, 블록킹을 할 것인지를

에이전트 스스로 결정해야한다.

- Acceptable : 연결을 받아들임
- Excludable : 연결을 블록킹함
- Questionable : 이웃 에이전트의 정보참조

각 포트의 연결을 모니터링하여 위와 같이 3단계의 과정을 나누어 실행한다. 이 에이전트들은 특히 Bot들 간에 명령이 오갈 수 있는 IRC 채널의 디폴트 포트인 6667/TCP 포트에 대한 트래픽 변화량을 집중적으로 관찰하며 동시에 다른 시스템들의 에이전트들과 모니터링한 결과를 공유하여 반영한다. 또한 사용자가 모르게 열려있는 포트들은 자동적으로 닫고, 열린 포트에 대해서는 패턴을 분석하여 해당 포트에서의 트래픽량 폭증 등이 발생할 경우 그 포트를 의심하여 블랙리스트에 올린다. 의심이 되거나 혹은 에이전트의 리스트에 확인이 되지 않은 연결은 다른 에이전트의 리스트를 참고하여 연결을 받아들일 것이지 혹은 블록킹을 할 것인지를 자동적으로 결정한다. 이런 과정을 거쳐 자가 형성된 에이전트 간에는 각각의 리스트가 자동적으로 갱신이 되며 최신의 정보를 갖고 네트워크를 모니터링하게 된다.

Bot들 간에 Botnet이 자가적으로 형성이 되려면 먼저 공격자 또는 Bot이 원격의 시스템에 접속하여 Bot을 설치하여야 하기 때문에 시스템 접속을 위해 백도어를 먼저 설치하게 된다. 일단 공격자의 백도어가 열리고 Bot이 설치되면 시스템 안에서의 Bot들 간의 자가 형성은 감지하기란 어렵다. Botnet이 자신이 거느린 Bot들을 늘리기 위해 각 Bot에 명령하거나 악의적인 행위를 하기위해 주기적으로 특정 취약점 또는 이미 만들어진 백도어를 공격하게 하여 다른 시스템들을 감염시킨다. 따라서 이때 특정 포트들에 비정상적인 트래픽 증가를 에이전트에서 탐지하여 Bot을 탐지할 수 있다.

본 논문에서 제시하는 Bot에 대한 보안 전략은 인터넷 이웃, 즉 다른 Peer간에 의존하는 방법이다. 각 Peer의 에이전트는 접속을 요청하는 host의 보안 레벨을 정의하고, 응답하기 위한 서비스 레벨 또한 정립시켜야 한다. 신뢰된 Peer의 에이전트에서 Bot에 대하여 비상 이벤트를 보내주면 각 보안, 서비스 레벨을 갱신하는 단계가 필요하다. 이 시스템은 주기적으로 방화벽, 안티스파이웨어 등과 데이터를 공유하여 Bot에 대한 최신 정보로 모니터링을 한다.

III. 결론

Bot은 현재 인터넷 환경에서 가장 큰 보안 위협 중의 하나이다. 이 Bot들은 서버-클라이언트 구조 또는 자가 형성을 통하여 특정 공격자가 없는 P2P 구조로도 Botnet을 형성할 수 있기 때문에 인터넷상에서 발생되고 있는 각종 범죄를 위한 인프라 역할을 수행한다고 말할 수 있다. 앞서 살펴본 바와 같이 특히 Bot들이 자가 형성하여 P2P Botnet을 형성한다면 탐지와 대응은 쉽지만은 않다. 하지만 앞에서 기술한 각 로컬 시스템의 모니터링 에이전트가 다른 시스템의 에이전트 간에 자가 형성을 하여 Bot에 대한 정보를 공유하여 Bot을 탐지 할 수 있으며 자가 형성을 통해 보다 쉽게 Botnet의 연결고리를 찾아 다수의 Bot을 파괴하는 역할을 수행 할 수 있다.

[참고문헌]

[1] Gregory P, Schaffer, "Worms and Viruses and Botnets, Oh My! : Rational Responses to Emerging Internet Threats.", IEEE Security & Privacy, Volume 4, May/June, 2006.

[2] Knowing Your Enemy: Tracking Botnets, research report, The Honeynet Project & Research Alliance, 13 Mar. 2005; www.honeynet.org/papers/bots.

[3] Ramneek Puri, "Bots & Botnet: An Overview", GSEC Practical Assignment Version 1.4b, August, 2