情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

봇넷 기술 개요 및 분석

전 용 희*

요 약

어떤 조직이나 개인을 상대로 한 인터넷 자원에 대한 분산 서비스 거부 공격이 통상적인 위험이 되고 있다. 이런 공격은 봇넷이라는 수많은 감염되거나 침해된 좀비 머신을 통하여 이루어지고 있다. 우리나라에서는 홈네트워크의 구축으로 광대역 액세스를 가진 개인사용자의 호스트 컴퓨터가 주 공격대상이 될 수 있다. 특히 개인 사용자들은 인터넷 보안에 대한 낮은 인식과 제한된 방어 자원으로 인하여 공격자의 대표적인 타깃이 되고 있다. IRC(Internet Relay Chat) 네트워크를 이용하여 감염된 인터넷 호스트를 제어하고 관리하는 공격들이 증가하고 있어, 이에 대한 대책이 절실히 요구되고 있는 실정이다. 따라서 본 논문에서는 인터넷 호스트들을 감염시키고 원격에서 제어하는 악성 봇/봇넷의 기술 개요에 대하여 기술하고 분석하고자 한다. 또한 최근 증가하고 있는 P2P 봇넷에 대하여도 알아보고자 한다.

Ⅰ. 서 론

1999년에 IRC(Internet Relay Chat)-기반 백도어를 가진 첫 번째 멀웨어 표본 중 하나인 PrettyPark가 등장한 이래로, 봇넷은 네트워크-기반 공격을 위한 가장 많이 사용되는 공격 플랫폼으로 발전하여 왔으며, 최근 침해된 머신(즉, 좀비)의 대규모 네트워크를 이용한 공격이 증가하고 있다[1].

수천 개의 좀비 기계들로 구성된 봇넷이 광역화된 액세스를 이용하여 인터넷 자원을 대상으로 한 분산 서비스 거부(DDoS : Distributed Denial of Service) 공격이 빈번하게 발생되고 있다. 특히 많은 수의 좀비 호스트들을 관리하고 지시하기 위하여 IRC 네트워크를 이용한 공격이 많이 발생 하였다. 이러한 공격은 합법적인 IRC 트래픽을 가장하기 때문에, 공격자의 공격이 난해하고 탐지를 회피할 수 있게 된다. 봇넷은 보통 통신 프로토콜로 IRC를 사용하지만, HTTP나 peer-to-peer 기반 프로토콜과 같은 다른 프로토콜이 사용될 수 있다. 그러나 아직까지 봇넷에 의하여 통상적으로 사용되는 통신 프로토콜은 IRC라 할 수 있다. IRC-기반 봇넷은 공격자들에게 잉여성(redundancy), 확장성, 유연성을 제공해 주기 때문에 많이 사용된다. 게다가 IRC-기반 봇을 개발하기 위한 많은 지식베이스와 소스 코드가 존재한다. 그러므로 본 논문에서는 주로 IRC-기반 봇넷에 대하여 기술한다.

봇과 봇넷을 이용하여 공격자에 의하여 수행되는 악성 행위의 예로는 다음과 같은 것이 있다[2] :

- DDoS 공격 : 공격자에 의하여 악성 IRC 봇을 사용하는 주된 이유이다. 공격자는 봇넷을 이용하여 자신의 좀비 머신 부대에게 명령할 수 있다. 이를 통하여 타깃 서버에 대하여 대형 크기의 UDP 패킷 혹은 ICMP 요구 스트림을 전송하거나, TCP sync 요구를 범람시킴으로써 DDoS 공격을 지시한다.
- 이차적 지역 감염 : 봇을 설치함으로써 공격자는 희생 머신에 대하여 완전한 제어를 할 수 있게 되고, 공격자는 침해된 머신 상에 저장된 개인정보와 같은, 감염 호스트로부터 유익한 정보를 수집하기 위하여 키 로거(key logger)나 트로이 목마를 내려 받기하거나 설치할 수 있다.
- 대역폭 거래 : 해커 공동체 사이에 고속 봇의 대역폭을 거래할 수도 있다.
- 백도어 : 공격 후에 지속적인 접근을 유지하기 위하여 침해 머신 상에 백도어를 설치한다. 네트워크 내에 합법적인 IRC 트래픽이 있으면 더욱 그러하다. 합법적인 IRC 트래픽에 의하여 사용되는 것과 같은 원격 TCP 포트를 사용하기 위하여 봇을 구성할 수 있고, 탐지 기회를 감소시킨다.

* 대구가톨릭대학교 컴퓨터정보통신공학부 (yhjeon@cu.ac.kr)

- 불법 데이터 공유 : 악성 봇을 사용하여 파일 공유 네트워크의 일부로 만들거나, 특히 고속 인터넷 링크를 통하여 연결된 대용량 저장 공간을 가진 서버가 감염된 경우, 저장 공간을 불법 파일, 소프트웨어, 해적판 영화 등을 저장하기 위하여 사용한다.

본 논문에서는 봇넷 관련 정의, 악성 봇 감염에 포함된 요소들과 공격자에 의하여 감염된 머신들이 어떻게 사용되는지에 대하여 알아보고자 한다. 그리고 공격자가 감염시키고자 하는 타깃 시스템을 어떻게 선정하는지, IRC 채널을 통하여 감염된 시스템을 원격 제어하는 방법, 몇 개의 알려진 봇을 열거하고 그 특성을 알아보고, 동향 및 전망에 대하여도 제시한다. 그리고 악성 봇 행위를 탐지하고 대응하는 방법에 대하여 기술하고자 한다. P2P 봇넷에 대하여도 간략하게 기술한다.

Ⅱ. 관련정의 및 공격요소

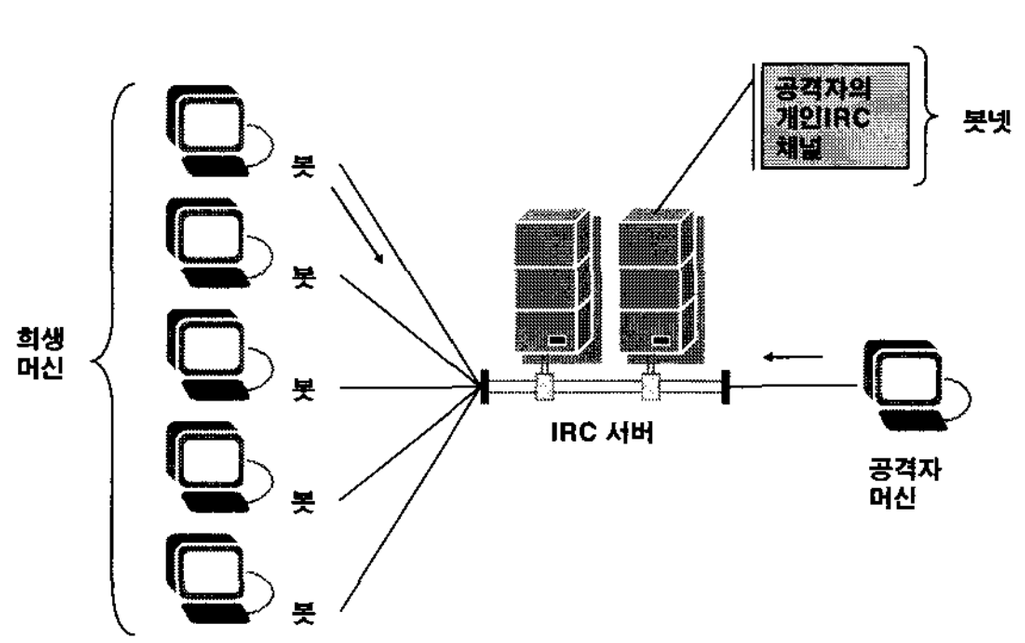
봇이란 용어는 로봇(robot)으로부터 유도되었으며, 봇 주인(Botmaster)으로부터 명령을 기다리는 감염된 머신이다. 봇은 자동화된 방법으로 미리 정해진 기능들을 수행하기 위하여 설계된 스크립트(script) 혹은 스크립트 집합을 묘사하기 위하여 사용되는 일반적인 용어이다. 이런 봇들의 네트워크가 봇넷(Botnet)이다. 따라서 봇넷은 감염된 혹은 침해된 기계들의 네트워크이다.

봇은 전통적인 DDoS 모델에서 에이전트와 유사한 개념이며, 감염 호스트들을 통제하기 위하여 공격자들은 기존의 핸들러(handler)에 해당하는 IRC 네트워크를 봇넷으로 이용한다. 대표적으로 봇은 표준 IRC 네트워크 서비스 포트와 외부 연결을 설정하며 공격자 개인 채널에 가입한다. 이와 같이 IRC 네트워크는 공격자에게 수백 개 혹은 수천 개의 봇을 통제할 수 있는 능력을 쉽게 그리고 융통성 있게 제공한다. 합법적인 IRC 트래픽으로 가장함으로써 공격을 난해하게 만들고, 시스템 관리자에 의한 공격 소스의 추적도 더욱 어렵게 만든다. 한 조사에 의하면 봇 감염의 주된 타깃으로 선정되는 희생자는 높은 대역폭과 높은 가용성을 가진 호스트로 알려져 있다[2]. 따라서 잠재적인 타깃은 기관들의 주요한 서버뿐만 아니라, 광대역 가정 가입자 및 인터넷 서비스 제공자들일 수 있다.

봇과 봇넷에 관련되는 대표적인 용어와 각각에 대한 간단한 정의 및 특성은 아래와 같다[2,3] :

- 봇(Bot) : 봇 주인으로부터 명령을 기다리는 감염 머신으로, 보통 어떤 기능들을 수행할 수 있는 실행 파일이다. 봇이 희생 머신에 설치될 때 자신을 구성 가능한 설치 디렉터리에 복제하고 매번 시스템이 부트될 때 구동 시스템 구성을 변경한다. 윈도우 플랫폼의 경우 봇은 자신의 인스턴스(instance)를 윈도우 현재 버전 메뉴에 추가하며, 압축된 봇의 보통 크기는 15 kb 이하이다. 중요한 점은, 봇은 운영체제나 애플리케이션에 대한 익스플로잇이 아니라, 웜에 의하여 운반되는 페이로드이거나 혹은 어떤 머신이 침해되면 백도어를 설치하기 위하여 사용되는 수단이라는 것이다. 공격자가 애플리케이션이나 운영체제의 취약성을 이용하여 악성 봇이 호스트 상에 설치되면, 해당 호스트는 감염되며 좀비(Zombie)라 한다.
- 봇넷(Botnet) : 제어 채널에 일단 연결되면 모든 봇은, 봇의 네트워크인 봇넷을 형성하며, 공격자 명령을 기다린다.
- 명령(Command) 및 제어 채널 : 봇 주인이 모든 봇에게 명령을 보내는 접속점역할을 하며, 통상 IRC 채널이 사용된다. 채널 이름과 인증하기 위한 패스워드 '키'로 구성된다.
- 공격자 : 봇을 구성하는 머신이며, 악성 봇을 설치하고, 지정된 IRC 채널에 봇이 일단 가입하면 제어하고 지시하기 위한 머신이다.
- IRC 서버 : IRC 서비스를 제공하기 위한 서버로써, 합법적인 공공 서비스 제공자이거나 다른 공격자의 침해된 머신일 수 있다.

[그림 1]은 위에서 기술한 요소들을 포함하고 있는 대표적인 IRC 봇넷 구성을 보여준다.



〔그림 1〕 대표적인 IRC 봇 공격의 요소

Ⅲ. 봇넷 공격 과정 및 대응기법

3.1 감염과 제어 과정

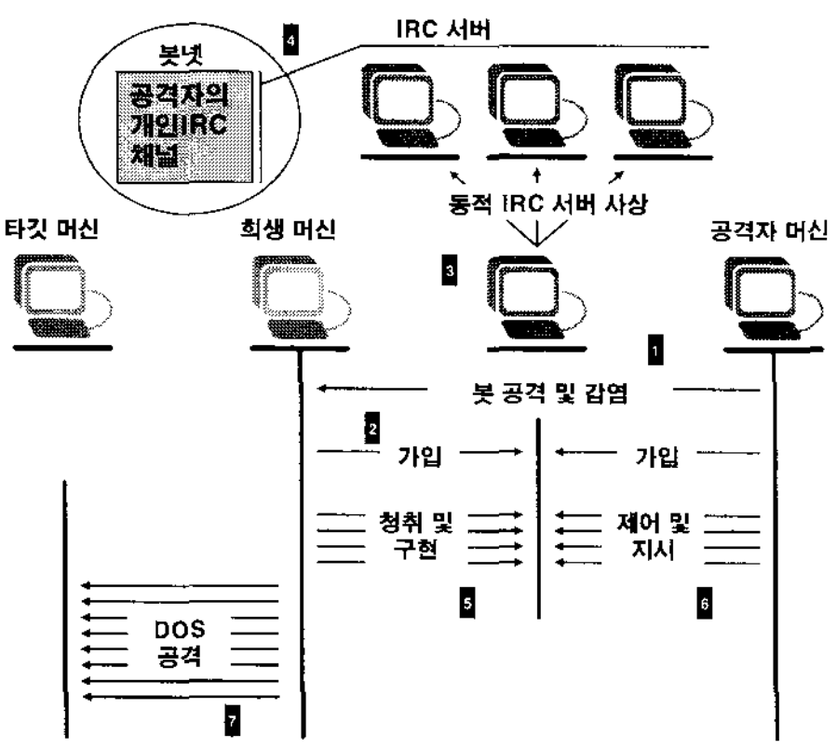
봇넷의 주요 목표는 아래의 세 범주로 묘사할 수 있다[4].

- 정보 분산 : 스팸 전송, DoS 공격 생성, 불법적으로 제어되는 소스로부터 허위 정보 제공.
- 정보 수확 : 신원 정보, 금융 자료, 패스워드 자료, 관계 자료(예, 전자 메일 주소) 및 기타 자료 획득.
- 정보 처리 : 패스워드 크래킹 같은 자료 처리

[5]에 의하면 봇의 감염 및 공격에 대한 방어는 방지, 탐지 및 대응과 같은 3 단계로 분류될 수 있다 :

- 방지 단계 : 사용자나 관리자가 시스템이나 네트워크를 봇 감염으로부터 예방할 수 있도록 취할 수 있는 대책을 추천한다. 이 단계는 사용자나 시스템 관리자가 봇 감염에 대하여 구현할 수 있는 예방적 대책을 개괄한다.
- 탐지 단계 : 머신 상이나 네트워크 내에서 악성 봇 활동을 식별하기 위하여 채택할 수 있는 대책을 기술한다. 의심되는 악성 봇 행위를 관찰하고 검증하기 위하여 사용될 수 있는 일반적인 지침을 제시한다.
- 대응 단계 : 봇 감염 머신이나 네트워크에 대응하여 취할 수 있는 행동을 추천한다.

봇넷의 공격 과정은 공격자의 숙련도에 의존하여 시작하며, 인터넷상에 이용 가능한 알려진 봇을 편집하거나, 희생 머신 상에 일단 설치되면 봇이 연결할 서버가 될 주요 구성 가능한 컴포넌트에 자신의 코드를 작성함으로써 행해진다. 공격자가 봇을 사용하여 희생 호스트를 공격하고 악성 봇으로 감염시키며, 봇을 통제하는 단계는 아래와 같다. [그림 2]는 봇의 감염과 제어 과정을 보여준다[2] :



〔그림 2〕 봇 감염과 제어 과정

[그림 2]의 각 단계별 설명은 아래와 같다.

1) 공격자는 어떤 운영체제나 응용의 취약성을 이용하거나 혹은 사용자를 속여서 봇 설치가 되도록 악성 프로그램을 실행하도록 함으로써 봇으로 희생 머신을 감염시키고자 시도한다. 공격자가 인터넷 호스트의 대량 그룹을 감염시키는 대표적인 방법은 최근에 밝혀진 취약성의 공격 코드를 이용하는 것이다. 이 과정은 알려진 취약성에 대하여 목표 서브넷을 스캔하고, 패치되지 않은 시스템을 공격하여 악성 봇으로 감염시키는 웜을 이용하여 자동화 될 수 있다. 희생 머신에 봇을 설치한 후, 디렉터리를 설치하기 위하여 자신을 복제하며 윈도우 플랫폼인 경우 레지트리 키를 갱신한다.
2) 봇은 임의로 생성된 이름을 가지고 IRC 서버에 연결을 시도한다. 봇은 공격자의 개인 IRC 채널에 가입(join)하기 위하여 인증 패스워드 '키'를 사용한다. 게다가 여러 경우에 공격자는 이런 활동을 위하여 공공 IRC 서버를 사용한다.
3) 공격자들은 가끔 다수의 IRC 서버들과 봇을 동적으로 사상하기 위하여 특정 서비스 제공자들을 이용한다.
4) 일단 봇이 희생 머신에 설치되면, 유일한 별명을 가지고 공격자의 채널에 가입하여, 공격자의 봇넷 군대의 일원으로 명령을 기다린다.
5) 이런 봇들이 IRC 채널에 가입할 때 공격자는 흔히 서버들에 로그인한다.
6) 복잡하고 때로는 암호화된 접근 패스워드를 사용하여 봇이 다른 것에 의하여 제어되지 못하게 보증하고, 누군가가 봇넷을 하이재킹하는 것을 어렵게 만든다.
7) 접근이 수락된 후, 공격자는 다른 목표에 대하여 공격을 개시하기 위하여 이 봇넷을 통하여 대량의 감염된 좀비들의 행동을 지시하거나 원격으로 제어한다. 혹은 악성 행위를 위하여 사용한다.

위에서 기술된 내용은 봇 감염과 제어의 단일 인스턴스를 위한 과정이며, 이 프로세스는 봇이나 좀비 머신의 군대

〔표 1〕 봇넷 자원 요구사항 및 측도

자원	측도
CPU 사이클	MIPS, 명령 목록
네트워크	Mbps, IP 목록, 포트 목록, 통신 그래프, 명령 지연
메모리	MB 저장, MB 정보, 값/비트
기타	시간 단위, 크기 단위 등

를 생성하기 위하여 대량의 호스트 상에 반복될 수 있다.

봇넷에 필요한 자원 및 측도는 [표 1]에서 보여준다[4].

3.2 대응기법

DNS 싱크홀 방법은 국내에서 적용하고 있는 봇 대응 시스템으로, 악성 봇에 감염된 PC가 유지하는 명령/제어 서버로의 연결을 차단함으로써 공격자로부터 감염 PC가 원격에서 조정되는 것을 방지하여 많은 수의 악성봇의 추가적인 활동을 막을 수 있는 방법으로 알려져 있다[6].

Ⅳ. Peer-to-Peer 봇넷

IRC-기반 봇넷은 어느 한 지점에서 중앙 명령 및 제어 위치를 가진 계층적인 방법으로 조직된 것으로 볼 수 있다. 이런 봇넷의 중앙 집중구조는 단일 실패점으로 제공될 수 있어, 공격자들은 더욱 더 탄력성 있는 구조로 이동할 수 있다. 이런 종류의 봇넷 구조의 하나로 P-to-P 기반 구조가 있다. P-to-P 구조에서는 명령 및 제어(C&C : Command and Control)를 위한 중앙점이 없다[4].

현재까지 잘 알려진 P-to-P 봇으로 Trojan.Peacomm 봇이 있다. 이 봇넷은 봇들을 제어하기 위하여 Overnet P-to-P 프로토콜을 사용한다. Overnet는 Kademlia-기반 프로토콜이며, 중요한 개념은 아래와 같이 요약 된다[4] :

- 통상적인 128-비트 수치 공간 사용
- 노드 ID는 그 수치 공간안에 존재
- 값들은 키들로 수치 공간에 사상됨.
- 키/값 쌍은 "가장 인접한" 노드에 저장됨.
- "인접"은 XOR 함수에 의하여 계산됨.
- 수치 공간 내의 각 버켓에 대하여 노드 목록 유지

감염 후 2차 주입이 P-to-P 네트워크로부터 자동적으로 다운로드 되며, 이것이 공격자로부터 감염 호스트로의 기본적인 통신 프리미티브를 제공한다. 이 P-to-P 통신 프리미티브가 공격자로 하여금 중앙 서버에 의존하지 않고도 감염 호스트를 임의로 업그레이드하고, 제어하고, 혹은 명령하도록 한다.

Ⅴ. 봇넷 사례연구, 동향 및 전망

5.1 사례연구

마이크로소프트 윈도우 플랫폼용으로 인터넷상에서 구할 수 있는 통상적으로 사용되는 악성 봇으로는 다음과 같은 것이 있다[2] :

- GTbot : 일명 W32.IRCBot이라고도 하며 윈도우 98, ME, NT, 2000 및 XP 등의 플랫폼에서 동작하며, 원격 접근 및 IRC 트로이 목마로 사용된다.
- Evilbot : GTbot과 같은 플랫폼에서 동작하며, 원격 접근, IRC 트로이 목마, 분산 DoS 툴 및 트로이 목마 다운로드용으로 사용된다.
- SlackBot : Backdoor.Slackbot, DDOS/ Slack 등의 별명을 가지고 있으며, IRC 소프트웨어와 함께 모든 윈도우 플랫폼에서 동작하며, Evilbot과 같은 용도로 사용된다.

5.2 동향

좀비 머신을 제어하기 위하여 IRC 네트워크를 사용하는 것이 DDoS 툴의 새로운 출현 및 동향의 하나로 보여진다. 대규모 봇 군대를 제어하기 위한 공격자 능력에 대한 IRC 네트워크의 영향을 아래와 같이 기술 한다[7] :

- 생존성(survivability) : 감염 시스템 상의 봇은 합법적인 IRC 네트워크 서비스 포트를 사용하여 공격자 IRC 채널에 대한 외향 연결을 설정하기 때문에, 단순한 네트워크 포트 스캐너로는 봇의 통신이 탐지되지 않는다. 이런 봇넷을 초대하기 위하여 공격자에 의하여 대규모 공공 IRC 네트워크가 사용되며 봇을 다수의 IRC 서버들에게 동적으로 사상하기 위하여 특정 서비스 제공자를 사용하기도 한다. 단일 봇 감염 머신의 발견은 공격자에 의하여 사용되는 한 개 이상의 IRC 서버와 채널명의 식별에 지나지 않을 수 있으며, IRC 서비스 제공자 네트워크로부터 설사 금지되더라도 봇넷

에 대한 접근을 유지할 수 있게 된다. 따라서 IRC 기반 봇넷은 전통적인 DoS 네트워크 모델보다 추적하거나 없애는 것이 어렵다.

- 감염 및 전파 : 공격자들이 취약성에 대하여 각 희생 머신을 스캐닝하고 봇을 설치하기 위하여 허점을 이용함으로써, 종단 운영체제를 위한 최근의 원격 익스플로잇을 사용하여 목표 네트워크 서브넷을 자동으로 스캔하고, 공격하고, 감염시키는 정교하고, 숙달된 웜을 위한 방법을 제시하였다. 그리하여 새로운 원격 익스플로잇이 공개적으로 이용가능하게 되는 경우 대규모 감염 시도 동향이 있다.
- 용도 : DDoS 공격 이외에 영화, mp3, 소프트웨어 등을 포함하는 해적판 지적 재산을 분배하기 위하여 IRC 채널 상에 파일 공유 네트워크의 일부로 봇 감염 머신들이 사용되는 경향이 증가되고 있다는 분석이다. 이에 대한 호스팅을 함으로써 해적판 지적 재산에 대한 통제나 소유권을 행사하게 된다.

[8]에서는 다음과 같이 세 단계로 이루어진 데이터 수집 방법을 사용하였다 :

- 멀웨어 수집
- gray-box 테스팅을 통한 바이너리 분석 : 네트워크 지문 생성 및 IRC-관련 특징 추출
- IRC와 DNS 추적기를 통한 IRC 봇넷의 추적

2006년 1월부터 아래와 같은 방법으로 데이터를 수집하였다 :

- 3 개월 이상의 기간 동안 지역 다크넷(darknet)에 포획된 트래픽 트레이스
- 3 개월 동안에 수집된 IRC 로그 : IRC 추적기에 의하여 방문되거나 하니넷 상에서 관측된 100 개 이상의 봇넷 채널로부터의 데이터를 포함한다.
- 45일 이상동안 65 IRC 서버를 추적한 DNS 캐시 히트의 결과

위의 관측으로부터 일반적인 봇넷 활동에 대한 이해를 얻기 위한 관점에서 결과들을 상호관련 시켰다. 분석 결과 봇넷이 원하지 않는 인터넷 트래픽에 대하여 주요한 원인을 제공하는 것으로 나타났다. 관측된 모든 악성 연결 시도 중 27%가 봇넷-관련 확산 행위에 직접적으로 기인하는 것으로 조사되었다. 또한 조사된 80만개의 DNS 도메인 중 11%에서 봇넷 감염의 증거가 발견되었으며, 이것은 봇넷 희생자들 사이의 높은 다양성을 보여준다. [표 2]는 모든 봇넷 인스턴스 사이에서 발행된 명령들의 상대 빈도를 보여준다.

〔표 2〕 봇넷에서 관측된 명령의 상대적 빈도

명령 유형	빈도 (%)
제어	33
스캐닝	28
번식(cloning)	15
마이닝	7
다운로드	7
공격	7
기타	3

318 개의 전체 악성 바이너리 중에서, 60%가 IRC 봇이며, 약간은 명령과 제어를 위하여 HTTP를 사용한 것을 보여준다. 주요한 네 가지의 지배적인 IRC 구조들은 아래와 같이 나타났음을 또한 보여준다 :

- 모든 봇이 단일 IRC 서버에 연결된다. 이 구조는 수백 온라인 사용자들을 가지는 소규모 클래스의 봇넷에 많이 있다. 서버 용량에 이를 정도의 봇넷을 이루며, 70%가 이 범주에 속하는 것으로 관측되었다.
- IRC 프로토콜의 서버 연결 능력을 이용하여, 다른 IRC 서버들이 많은 수의 사용자들을 지원하는 하나의 IRC 네트워크를 형성하기 위하여 연결될 수 있다. 서버 상태 메시지를 조사하고 다수의 서버가 사용 중인지를 봄으로써 브리지 구조를 추론하며, 분석 결과 봇넷의 30%는 다수의 서버들에 브리지(bridge) 되었음을 보여준다. 이 중에서 반은 단지 두 개의 서버 사이에서 브리지 되며, 브리지된 서버들 중 25%는 또한 알려진 공개 서버인 것으로 나타났다.
- 여러 개의 관련 없는 것으로 보이는 봇넷들이 면밀한 조사 결과, 작명 관습, 채널 이름 및 운용자의 사용자 ID에 대하여 비교하였을 때 아주 유사한 것으로 나타났다. 이는 대부분의 경우에 이런 봇넷들이 동일한 봇 마스터에 속한다는 것을 보여준다.
- 봇의 선택된 그룹들이 봇을 다른 IRC 서버로 계속하여 이동하도록 갱신된 바이너리를 다운로드

〔표 3〕 감염 벡터

형태	특징 요약
서버	원격 서비스의 적극적인 이용
클라이언트	클라이언트 프로세스의 수동적 이용
트로이 목마	우선권 프로그램의 신뢰 이용
물리적	물리적 컴퓨터 침해
기타	실행을 제어하기 위한 다른 방법

〔표 4〕 봇넷에 대한 공격자에 의하여 발행된 명령 분포

명령 범주	사건 수
확산	10,891
DDoS 공격	9,755
봇넷 번식(cloning)	5,621
다운로드/갱신	5,583
정보 절도	3,809
봇 로그인	1,863
서버 호스팅	398
봇 제어	780
기타	107

할 것을 명령 받은 여러 인스턴스가 관측되었다.

[표 3] 은 주요한 감염 방법에 대한 요약을 보여준다[4].

이와 비슷하게 [1]에서는 3,290개의 IRC-기반 봇넷을 탐지하고 공격자에 의하여 내려진 명령 분포를 [표 4]와 같이 보여준다.

[표 4]를 통하여 보면, 명령 확산이 가장 빈번한 용도라는 것을 알 수 있다. 그 이유는 봇넷의 크기를 키우기 위하여 추가적인 머신에 대한 침해를 시도하기 때문이다. DDoS 공격 범주에는 네트워크 상의 다른 컴퓨터를 공격하기 위하여 사용된 플러딩-관련 명령들이 포함된다. 봇넷을 가지고 이런 공격을 하는 것은 매우 효율적이며 두 번째를 차지한다. 봇넷 번식(cloning)은 DDoS 공격의 특별한 형식으로 공격자가 각 봇에게 희생 IRC 네트워크에 대규모 자손을 연결하도록 명령한다. 이 공격은 다른 IRC 서버에 대하여 효과적이다. 다운로드와 갱신 명령은 새로운 멀웨어를 분배하거나 새로운 소프트웨어 버전에 대하여 봇을 갱신하기 위하여 사용된다.

[9]에서는 독립적인 봇넷들의 네트워크인 "슈퍼-봇넷"의 가능성을 조사하였다. 봇넷들이 협동하도록 설계된다면, 슈퍼-봇넷으로 인한 새로운 위협이 발생할 수 있다는 것이다. 예를 들어, 공격자는 슈퍼-봇넷을 이용하여 선택된 목표에 대하여 거대한 DDoS 공격을 개시할 수 있으며, 또한 정보 전쟁과 사이버 테러에도 응용될 수 있는 가능성이 있다고 지적한다.

악성 봇의 국내 감염율은 2006년 평균 12.5%이며, 2007년 평균은 11.3%로 소폭 감소한 것으로 조사되었다[6]. 2007년 악성 봇의 가장 두드러진 특징은 악성 봇을 이용한 랜섬형 DDoS 공격의 증가로 분석되었다. 이 악성 코드는 특정 기업의 홈페이지를 대상으로 DDoS 공격을 수행하였고, HTTP에 기반한 악성 봇의 특징을 보여주었다. 따라서 기존의 취약점 스캔에 의한 봇 확산과 달리, 네트워크 트래픽을 증가시키지 않아 비밀스런 확산이 가능하며 적은 감염 PC 대수로도 공격이 쉽게 이루어질 수 있어 향후 DDoS 공격용 악성봇 등의 확산에 많이 이용될 것으로 예측하고 있다. 또 다른 특징으로는 악성봇에 대한 분석이 어렵도록 분석 회피 기술이 적극적으로 활용되기 시작했다는 점을 들고 있다.

5.3 국내 전망

한편 2008년 악성봇의 전망에 의하면, 지난해와 마찬가지로 홈페이지와 같은 악성코드 유포지를 통한 다운로드 사례가 더욱 증가할 것으로 전망하고 있다. 악성봇의 확산방법으로는 기존의 IRC 기반의 악성 봇보다는 웹을 이용한 HTTP 기반의 악성 봇이 더욱 증가하고 싱크홀 같은 중앙 서버로의 연결을 차단하는 방법을 우회할 수 있는 P2P 봇의 증가를 예상하고 있다.

또한 앞에서도 지적하였듯이 봇의 발견과 분석을 어렵게 하기 위한 분석회피 기술이 더욱 발전하고, 특정 목적을 위한 봇넷의 사례가 더욱 증가하고, 금전적 이득을 목적으로 하는 DDoS 공격, 게임 아이템 등의 탈취를 위한 개인정보 습득 등의 범죄가 더욱 증가할 것으로 예상하고 있다.

Ⅵ. 맺음말

ICMP와 UDP 플러딩, TCP Sync 플러딩 공격을 포함한 DoS 공격 기술들이 지속적으로 진화되어 왔다. IRC 네트워크 모델은 하부 기술에 대하여 별로 지식을 갖고 있지 않은 공격자에게 이미 알려진 봇을 이용하여 확장 가능한 자동화된 대규모 봇을 생성할 수 있도록 하였다.

봇의 전파와 감염 과정이 단축되고 자동화됨에 따라,

인터넷상에 높은 대역폭을 가진 항시 켜져 있는 호스트들, 특히 윈도우 기반 종단 사용자들에 대한 맹목적이고도 선택적인 공격의 증가를 초래하였다.

봇 공격의 주된 대상이 되는 타깃은 감시가 많이 되지 않고, 높은 대역폭을 가진 가정 컴퓨터나 대학 서버인 것으로 나타났으며, 다음과 같은 특성을 가지고 있다[2] :

- 고 대역폭 : 광대역 액세스 능력을 가진 머신들은 공격자에게 DDoS나 호스트 침해 파일 혹은 소프트웨어를 위하여 타깃 서버에 대하여 대량의 공격 대역폭을 제공하여 준다.
- 가용성 : 공격자는 그들의 명령을 수행하기 위하여 언제든지 이용 가능한 항시 켜져 있는 머신을 선호한다.
- 낮은 사용자 인식 및 감시 능력 : 봇 감염의 주 타깃은 인터넷 보안 인식이 낮고 접근제어 장치에 투자할 만한 자원을 갖고 있지 않은 사용자이다. 방화벽 같은 접근제어 장치가 없는 것 외에 운영체제나 애플리케이션을 제때에 갱신하지 않는 것도 공격자에게 시스템에 침투할 수 있는 기회를 제공하고, 식별이나 추적되지 않고 상당기간 동안 봇을 유지할 수 있게 해준다.
- 위치 : 공격자는 자신의 위치로부터 지역적으로 멀리 떨어진 머신을 공격 타깃으로 잡음으로써, 공격 추적을 상대적으로 어렵게 만들려고 한다.

위의 기준에 부합되는 대표적인 사용자는 광대역접속망을 가지고 있고 인터넷에 상시로 연결된 홈네트워크 사용자나 대학 서버가 될 가능성이 높다. 이런 측면에서 특히 홈네트워크 구축 사업을 적극적으로 추진하고 있는 우리나라에서 홈네트워크 보안과 각 가입자들의 컴퓨터보안에 대한 지대한 관심이 요구된다고 하겠다.

참고문헌

[1] Jianwei Zhuge et al., "Characterizing the IRC-based Botnet Phenomenon", Reihe Informatik, TR-2007-010, Dec. 2007.

[2] Ramneek Puri, Bots & Botnet : An Overview, GSEC Practical Assignment Version 1.4b, Aug. 2003, SANS Institute.

[3] Nicholas Albright, Researching Botnets, HTTP 자료.

[4] Julian B. Grizzard et al., "Peer-to-Peer Botnets : Overview and Case Study", http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/griz...

[5] Jones Jim, FEDCIRC, "BotNets : Detection and Mitigation", Feb. 2003. http://www.fedcirc.gov/library/documents/botNetsv32.dco

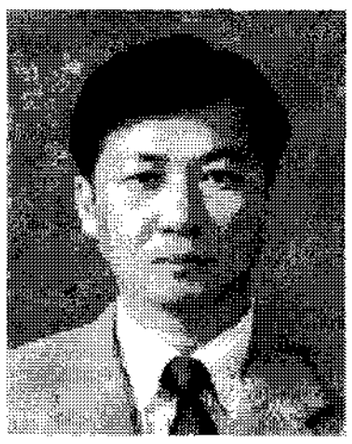
[6] 한국정보보호진흥원, "2007년 악성 봇 현황 및 2008년 악성 봇 전망", 정보보호뉴스, Vol 124, pp. 14-15, Jan. 2008.

[7] Jeff Carpenter, Chad Dougherty and Shawn Hernan, : "Continuing Threats to Home Users", CERT®Advisory CA-2001-20. Jan. 2001.

[8] Moheeb Abu Rajab et al., "A Multifaceted Approach to Understanding the Botnet Phenomenon", IMC'06, Oct. 2006, Brazil.

[9] Ryan Vogt and John Aycock, "Attack of the 50 Botnet", Dept. of Computer Science, University of Calgary, TR 2006-840-33, Aug. 2006.

〈著者紹介〉



전 용 희 (Yong-Hee Jeon)
종신회원

1971년 3월~1978년 2월 : 고려대학교 전기전자전파공학부
1985년 8월~1987년 8월 : 미국 플로리다 공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월 : 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월 : 삼성중공업(주)
1978년 11월~1985년 7월 : 한국전력기술(주)
1979년 6월~1980년 6월 : 벨기에 벨가톰사 연수
1989년 1월~1989년 6월 : 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월 : 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월 : 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재 : 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년 3월~2003년 2월 : 대구가톨릭대학교 공과대학장 역임
2004년 2월~2005년 2월 : 한국전자통신연구원 정보보호연구단 초빙연구원
2007년 1월~2007년 12월 : 한국정보보호학회 학회지 편집위원장
2008년 1월~현재 : 한국정보보호학회 부회장
<관심분야> 네트워크 보안, 웜 모델링 및 대응 기술, 통신망 성능분석