情 報 保 護 學 會 誌
第19卷 第 6號, 2009. 12

최근 봇넷의 악성 행위 동향 및 대응 기술 연구

강 동 완*, 임 채 태*, 정 현 철*

요 약

최근의 컴퓨터 통신 기술은 인터넷 기반으로 이루어지고 있으며 정치・경제・문화 등 사회 전 분야에 있어서 주요 기반 인프라를 구축하는데 없어서는 안 되는 핵심 요소 기술로 자리 잡았다. 이러한 인터넷상에서 기존의 악성코드와는 차별화 되는 외부 공격자의 명령・제어를 받는 악성 네트워크인 봇넷이 인터넷 서비스의 보안 위협으로 등장하게 되었다. 최근의 봇넷은 매우 빠르게 진화하고 있으며 봇넷을 이용한 스팸 메일, 개인 정보 탈취, 금품 갈취형 분산 서비스 거부 공격 등은 사이버상의 공격을 주도하는 주요 이슈로 부상하였다. 본 연구에서는 이러한 봇넷의 악성 행위 동향과 함께 이에 대응할 수 있는 기술에 대해서 방향을 제시하고자 한다.

Ⅰ. 서 론

최근의 통신 기술의 발전은 정치・경제・문화 등 사회 전 분야에 있어서 주요 기반 인프라를 구축하는데 없어서는 안 되는 핵심 요소 기술로 자리 잡았다. 하지만 정보통신기술의 비약적인 발전에서 오는 순기능과 동시에 발전한 역기능으로써 정보기술을 악용하는 해킹, 웜・바이러스 등 사이버상의 각종 위협 요소 또한 첨단화・고속화・광역화되고 있는 것도 현실이다. 지난 1.25 인터넷 대란 및 7.7 분산 서비스 거부 공격 때의 피해에서도 보는 바와 같이 사이버 위협의 파괴력이 이제는 단순한 서비스 마비나 경제적 손실을 넘어 나아가 국가 안보까지 위협하는 심각한 단계에까지 이르렀다.

또한 과거의 사이버 공격은 단순한 호기심과 해커들의 실력 과시용 퍼포먼스로 여겨졌지만 근래에는 경쟁사에 대한 분산 서비스 거부 공격(DDoS:Distributed Denial-of-Service)과 사용자들의 금융 정보등의 기밀정보 탈취, 광고성 스팸메일의 대량 발송 등 불법 행위를 대행해주고 경제적 이득을 취하려는 목적으로 바뀌어가고 있다.

이러한 보안 위협 가운데 최근 이슈화 되고 있는 봇넷은 종래의 바이러스나 웜, 스파이웨어 등을 모두 포괄할 수 있다. 봇넷은 단순히 해커가 악성 코드를 만들 당시에 결정된 행위 이외에 외부 다른 객체와의 통신을 통해서 다양한 악성 행위를 할 수 있는 명령을 받아 수행하는 거대한 악성 네트워크 집단이다.

따라서 현재 봇넷의 심각성을 주지하고 많은 연구가 이루어지고 있지만 특정 인터넷 서비스 제공자 망의 봇넷만을 탐지하여 봇넷의 전체적인 구성 및 분포를 파악하기 어려운 점이 있고, 많은 변종 등으로 인해 다양한 봇넷을 탐지할 수 있는 방법이 절실한 상황이다.

Ⅱ. 봇넷의 개요

봇은 로봇(robot)의 줄임말로, 사용자나 다른 프로그램 또는 사람의 행동을 흉내내는 대리자로 동작하는 프로그램을 의미한다. 인터넷상에서, 가장 보편적으로 존재하는 봇들은 스파이더, 크로울러라고도 불리는 프로그램들로서, 웹사이트들에 주기적으로 방문하여 검색엔진의 색인을 위한 콘텐츠를 모아오는 일을 한다. 또한 게임에 이용되거나 IRC(Internet Relay Chat) 채널 봇, 사람과 대화를 하는 봇(Chatterbot) 등 다양한 용도로

본 연구는 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발사업의 일환으로 수행하였음. [2008-S-026-02, 신종 봇넷 능동형 탐지 및 대응 기술]

* 한국인터넷진흥원(Korea Internet & Security Agency) (lupin428@kisa.or.kr)

인터넷에서도 널리 이용되고 있다.

하지만 악성 봇은 악의적 의도를 가진 소프트웨어로써, 이에 감염된 시스템을 드론(drone) 및 좀비(zombie) 시스템이라고 한다[2]. 이러한 봇들이 다수가 모여 서로 네트워크를 이룬 형태를 봇넷이라고 하며, 봇넷은 공격자인 봇 마스터(Bot Master)에 의해 원격에서 C&C(Command & Control) 서버를 통해 명령·제어가 이루어지며, DDoS 공격, 개인정보 수집, 피싱, 악성코드 배포, 스팸메일 발송 등 다양한 악성행위에 이용되고 있다.

최근 봇넷은 주기적 업데이트, 실행 압축 기술, 코드 자가 변경, 명령 채널의 암호화 등의 기술을 사용하여 탐지 및 회피가 어렵도록 더욱 교묘해지고 있다. 또한, 봇넷은 그 소스가 공개되어 있어 수천 종의 변종이 발생하고 있으며, 전문적인 지식을 가진 사람이 아니더라도 봇 생성 툴을 이용하여 쉽게 봇 코드를 생성하거나 제어할 수 있어, 쉽게 봇넷을 만들고 이용할 수 있기 때문에 문제점이 심각하다. 이러한 봇넷을 구성하는 봇 좀비들은 국가의 구분 없이 전 세계의 인터넷 서비스 제공자 망에 분포되어 있어 국가 간의 공조 없이는 봇넷을 대응하기 어려운 것이 현실이다.

Ⅲ. 봇넷의 발전 동향

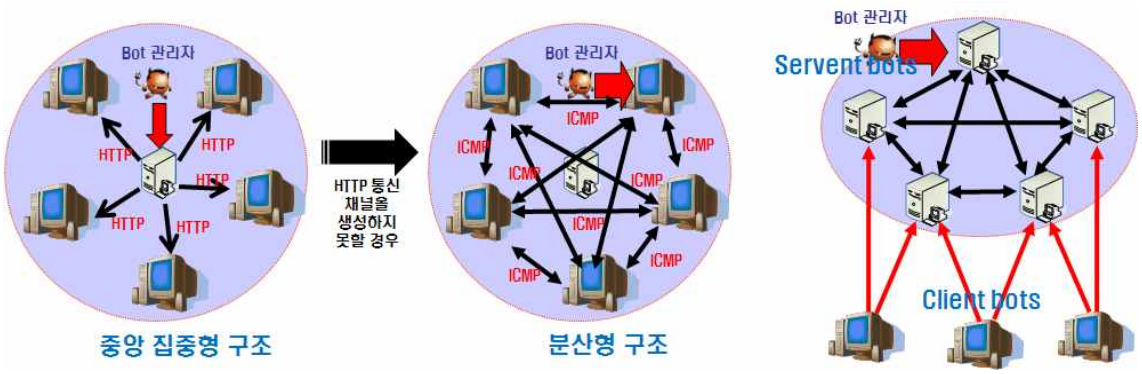
최근의 봇넷은 초기 단순한 형태의 공격 행위 및 구조에서 벗어나 탐지를 우회하거나 어렵게 하는 다양한 방어적인 기술들을 가지고 발전하고 있다. 본 절에서는 이러한 봇과 봇넷의 주요한 구성 모델과 전파·감염 행위, 공격·방어 행위의 발전 동향에 대해 알아본다.

1. 봇넷의 구성 모델

봇넷은 통신에 사용하는 프로토콜과 좀비 시스템과 이를 제어하기 위한 C&C서버간의 네트워크 구성에 따른 토폴로지로 분류될 수 있다. 먼저 봇넷이 사용하는 프로토콜로써 IRC를 사용하는 IRC 봇넷과 HTTP(Hyper-text Transfer Protocol)를 사용하는 HTTP 봇넷, 그리고 자체적으로 독립된 프로토콜을 사용하는 C/S(Client/Server) 봇넷으로 구분될 수 있으며, 네트워크 토폴로지에 따라 중앙 집중형과 분산형, 그리고 중앙 집중형과 분산형이 함께 구성되는 하이브리드형이 있다. 초기의 봇넷들은 당시 인터넷 채팅에서 많이 사용되었던 IRC를 사용하는 Virut, Sdbot, Rbot과 같은 IRC 봇넷에서 시작되었지만, IRC를 사용하는 봇넷이 탐지가 비교적 용이하고 IRC 서버의 차단으로써 쉽게 무력화되는 단점으로 인해서 점차 다른 형태의 프로토콜로 발전하기 시작하였다[6]. HTTP 프로토콜은 포트를 가지고 서비스의 구분이 어려우며, 네트워크에서 행위의 구분이 어렵다는 점을 이용하여 HTTP를 사용한 Bobax, Cutwail, Padobot, Kraken, Srizbi와 같은 HTTP 봇넷이 나타나게 되었으며, HTTP 뿐만 아니라 독자적인 프로토콜을 가지고 봇넷을 구성하는 Netbot과 같은 C/S(Client/Server)봇넷이 등장하게 되었다.

네트워크 토폴로지에 따라서는, 중앙에 독립적인 C&C 서버가 존재하여 명령/제어하는 구성을 중앙 집중형이라고 하며, 이와 달리 P2P 방식으로써 C&C 서버의 도움 없이 좀비 시스템끼리 상호 연결되어 동작하는 네트워크 구성을 분산형으로 분류한다.

현 시점에서의 봇넷이 사용하는 프로토콜에 따른 분류는 많은 봇넷들이 다양한 프로토콜을 함께 사용한다



[그림 1] 네트워크 구성에 따른 봇넷의 분류

는 점을 감안할 때 주요한 분류 기준이 되기 어려운 것이 현실이며, 네트워크 토폴로지에 따른 분류가 보다 현실적인 분류 기준이라고 볼 수 있는데, 최근의 대부분 봇넷들은 단일 계층이 아닌 다양한 레이어를 두고 복합적인 하이브리드 방식으로써 봇넷을 구성하고 있다.

2. 봇넷의 전파 및 감염 모델 동향

봇넷은 자신의 네트워크 구성에 참여하는 봇넷 감염된 개체인 좀비 시스템을 확보하기 위해 다양한 전파 및 감염 행위를 한다. 주요한 전파 경로는 다음을 들 수 있다.

- 스팸 메일 발송
- 좀비 시스템에 의한 네트워크에서의 취약점 스캔
- USB 메모리 장치에서의 자동 실행

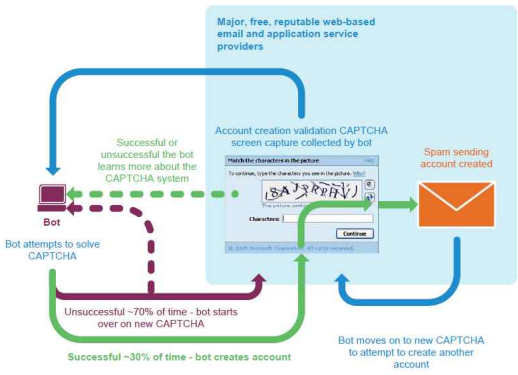
특히 스팸을 이용한 전파 방법은 사용자로 하여금 메일에 포함된 이미지나, 외부 서버에 접속할 수 있는 URL 링크, 그리고 첨부된 실행파일에 의해 악성 코드를 시스템에 감염시키게 된다. 스팸 메일은 공격자가 스스로 전파하기도 하며, 봇넷에 의해 발송되기도 한다. 최근의 스팸은 국세청을 사칭하거나, 소셜 네트워크 사이트인 Facebook의 사용자 암호를 설정하라는 내용등의 지능적인 내용으로 발송되고 있다[12].

최근의 스팸 메일은 단순히 악성코드가 첨부된 형태가 아닌 사용자들로 하여금 정상적인 소프트웨어인 것처럼 가장하여 사용자에 의해 쉽게 컴퓨터에 설치되도록 하는 가짜 보안 소프트웨어(Rogue Security Software)로

[그림 2] Bredolab 봇넷에 의한 facebook 스팸 메일

[그림 3] Rogue Security Software

전파·감염 되기도 한다. 일반 사용자들은 실제 보안상의 문제가 있는 것처럼 실행하게 되고, 이 가짜 보안 소프트웨어는 실제 보안 소프트웨어처럼 시스템을 점검하고, 검사하는 UI를 가지고 있어, 검사 결과를 사용자에게 보여준다. 검사 결과는 몇몇 악성코드에 감염된 것처럼 보이며, 이를 치료하기 위해 별도의 지불 과정을 요구하기도 한다. 몇몇 가짜 보안 소프트웨어들은 사용자 개인정보를 탈취하기 위한 키로깅 기능과 백도어를 설치하는 경우도 있고, 주기적인 외부 서버와의 업데이트 스케줄을 가지고 있어, 기능을 업데이트 할 수 있다. 또한 자체적인 스팸 발송이 아닌 정상적인 웹 메일 계정을 사용하는 시도도 보이며, 이를 위해서 봇넷은 자체적으로 CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)를 해킹하기도 한다.

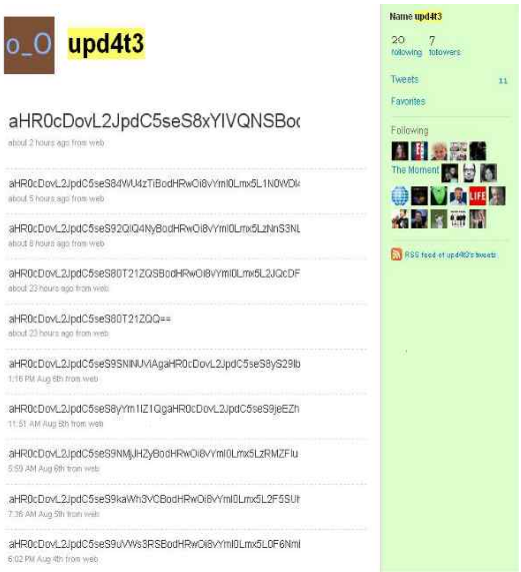


[그림 4] CAPTCHA를 해킹하는 주요 과정

3. 봇넷의 명령 제어 채널 동향

봇넷을 공격자가 제어하기 위해서는 봇넷과 통신할 수 있는 별도의 제어 채널을 형성해야 하는데, 초기 IRC 봇넷의 경우에는 IRC 서버가 그 역할을 하였다. 하지만 IRC 프로토콜을 사용하지 않는 HTTP 봇넷의 경우에는 IRC 서버가 아닌 별도의 웹서버가 사용되었다. 최근에는 봇넷의 생존성을 높이기 위해 특정한 C&C 서버에 의존하지 않는 P2P 프로토콜을 사용한 봇넷의 구성이 주가 되고 있으며, C&C 서버의 수도 하나가 아닌 여러 C&C가 역할별로 분할되어 사용되는 것이 일반적이다.

최근 봇넷들에서 인터넷상에서 소셜 네트워크 서비스 (SNS:Social network service)인 Facebook이나 구글 그룹스, twitter등을 사용한 명령・제어 방식도 등장하고 있다. 이는 정상적인 서버를 악용하는 경우로써, 네트워크 상에서는 정상적인 웹 접근처럼 보이지만, 실제 웹 페이지를 확인하면, 실제 사람이 사용하지 않는것을 알 수 있다. 이와 같이 최근 들어 다양한 SNS 사이트가 생겨남에 따라 이러한 개인 사이트를 사용한 명령・제어 채널이 악용되고 있다.



[그림 5] C&C로 악용된 SNS인 Twitter 사이트

4. 봇넷의 공격 행위 및 방어 행위 동향

4.1 봇넷의 공격 행위 동향

봇넷은 다수의 감염된 시스템인 좀비가 네트워크로 구성된 악성 네트워크이다. 이는 외부 공격자에 의해 명령 제어 채널을 유지하며 공격자의 명령을 받는다. 일반적으로 봇넷은 기존의 대부분의 악성코드들이 수행하는 모든 행위를 할 수 있다. 봇넷으로 수행할 수 있는 주요 악성행위는 다음과 같다.

- 스팸메일 발송
- 개인정보 탈취
- 부정 클릭 공격
- 특정 사이트에 대한 분산 서비스 거부 공격

특히 스팸의 경우, 봇넷 자신의 전파를 목적으로 이루어지기도 하지만, 피싱 사이트 및 가짜 보안 소프트웨어를 배포하여 금전적인 이득을 취하는 공격행위도 이루어진다. 또한 수신자의 지리적인 위치 정보를 사용하여 본문 내용의 도시명을 해당 국가로 바꾸어 놓는다던가, 특정한 사회적인 이슈에 대한 내용을 발송함으로써 그 효과를 높이고 있다. Symantec에 따르면 2008년에 전체 스팸의 81.2%를 차지했던 봇넷에 의한 스팸 발송은 2009년 87.7%로 증가한 상태이다.

부정 클릭 공격과 관련하여, Click Forensics에 의해 실제 검색 페이지 대신 가짜 검색 페이지로 연결시키는 Bahama 봇넷의 심각성과 위험성이 2009년 10월 발표되었다. Bahama 봇넷은 DNS Poisoning 기법을 이용하여 검색 엔진(구글, 야후, 빙)을 공격하도록 설계되었는데, 스폰서 링크의 Click Counter를 우회하고 특정 타 광고 네트워크를 거쳐 감으로 인해서, 검색 업체에 금전적 피해를 줌과 동시에 공격자가 광고이익을 받도록 한다.

또 다른 주요 공격인 DDoS는 인터넷을 기반으로 하는 금융권 및 전자상거래 기업들에게 큰 위협이 되고 있다. 최근에는 이러한 DDoS 공격에 특화된 Netbot과 같은 공격 툴이 등장하여 비전문가도 쉽게 DDoS 공격을 할 수 있고, 네트워크 인프라가 좋은 국내의 경우, 적은 수의 좀비 시스템으로도 대량의 DDoS 공격을 할 수 있기 때문에 큰 문제가 되고 있다.

4.2 봇넷의 방어 행위 동향

봇넷을 제어하는 공격자는 봇넷의 일부가 된 좀비 시스템이 지속적으로 좀비 시스템으로의 역할을 수행할 수 있도록 유지하기 위해 사용자에게 탐지되지 않도록 하거나 탐지가 되었다고 하더라도 즉각적으로 대응하지 못하도록 다음과 같은 방어 기술을 가진다.

- 탐지가 어려운 시스템 커널 영역에서 루트킷
- 활동에 방해가 되는 보안 소프트웨어 종료
- 안티 디버깅 및 안티 가상화 기술, 실행 코드에 대해 압축, 암호화 및 다형성 코드 사용
- 정상 프로세스 내에서 동작함으로써 탐지가 되더라도, 핵심 프로세스인 경우 차단이 매우 어려움
- DNS의 TTL 값을 매우 짧은 주기로 설정하여, 네임 서버의 IP 및 서버의 IP를 계속 바꿔주는 방법을 사용하여 고정된 C&C를 사용하지 않도록 하는 FastFlux 기술 사용
- 많은 C&C에 번갈아 가며 접속하여 특정 서버를 C&C라고 판단하기 어렵게 하는 행위
- 사용자의 컴퓨터에서 DNS 쿼리를 후킹하여 보안 관련 사이트 및 업데이트를 위한 웹 접속을 막는 행위

이와 같은 방어 행위는 봇넷의 탐지 및 치료를 어렵게 하는 요인이며, 감염 후 치료도 상당히 어려워지는 원인이 된다. 실제로 Conficker의 경우 대부분 보안 관련 웹사이트의 접속이 불가하여, 백신의 업데이트도 이루어 지지 않고, 다른 보안 관련 커뮤니티 및 관련 보안 사이트도 접속되지 않아서, 별도의 새로운 페이지에서 전용 백신을 받아 치료해야 했다.

Ⅳ. 최근 주요 봇넷 동향

2008년에 활동하던 봇넷 중 일부는 보안 업체의 대응에 의해 몇몇 봇넷은 와해되기도 하였다. 2008년 9월, 2년여 동안의 활동을 마치고 스톰 봇넷은 사망 판정을 받았다. 주요 원인으로 P2P 기반의 악성 봇넷이었기 때문에, 다른 악성 봇넷이 스톰 봇넷을 수정하여 사용하는 것이 쉽지 않았고, 마이크로소프트사의 악성 소프트웨어 제거 도구에 의해 한 번에 수십만 대의 악성 봇들이 사망함으로써 쇠퇴의 길로 접어들었다[11].

또한 지난 11월 가장 많은 스팸 메일을 발송하는 봇넷을 호스팅하는 것으로 알려진 ISP인 McColo의 폐쇄 이후 전 세계 스팸 메일의 절반이 넘는 50~70%의 스팸 메일이 감소하였다. McColo 폐쇄 후 봇넷은 다시 꾸준히 스팸 메일의 양을 늘려나갔으며, 2009년 6월 스팸 메일에 이용된 ISP 업체인 Pricewert를 폐쇄하여 스팸 메일의 양이 15% 감소하였다. 이때 스팸 메일을 발송하는 봇넷인 Mega-D 봇넷이 C&C를 이전하지 못하고 더 이상의 활동을 할 수 없는 사망 판정을 받았다[11]. 또한 Cutwail의 경우 ISP Pricewert의 폐쇄로 일시적인 쇠퇴를 겪었지만 폐쇄 이후 수 시간 만에 원래 봇넷 크기의 1/3까지 복원하여 수천 명에게 스팸 메일을 발송하였다[13].

이 외에 2009년에도 다양한 봇넷이 활동하였는데, 대부분 규모가 거대화되는 특징을 가진다. 2008년도에 가장 규모가 큰 봇넷이었던 스톰(Storm)이 20만대의 좀비 시스템을 가지고 있고, 이후 크라켄(Kraken)이 40만대 이상의 좀비 시스템을 가지고 있다고 발표[10]되었지만, 현재 봇넷의 규모는 하나의 봇넷 당 좀비 시스템의 수가 백만대를 넘어서고 있는 상황이다[8]. 본 절에서는 Waledac, Koobface, ZeuS등 주요 봇넷에 대해서 알아본다.

1. Waledac

1.1 개요

웨일덱(Waledac)은 2008년 말에 스팸 발송을 하는 봇넷으로 알려졌다. 웨일덱의 경우 최신 이슈를 사용하는 사회공학적 방법의 스팸 메일을 통한 전파를 하며, 다양한 암호학적 방법이 사용된 하이브리드 형태의 HTTP 봇넷이다.

1.2 주요 특징

웨일덱 봇넷의 주요 특징은 다음과 같다.

- HTTP2P(P2P over HTTP) 사용
- 암호 통신을 위해 RSA, AES, Base64등 다양한 암호화 기법 사용
- C&C 서버와 중계 역할을 하는 Proxy bot과 실제

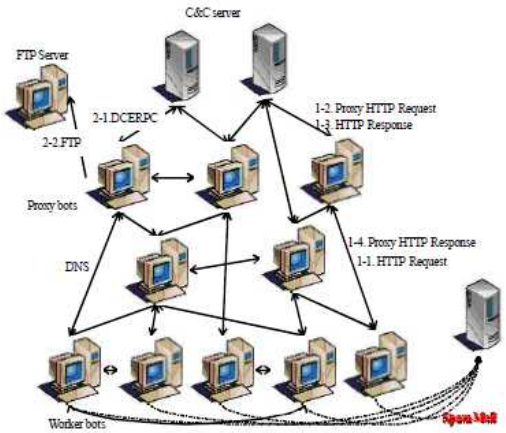
적인 공격(Spam Mail 발송)을 하는 Worker bot으로 구성되는 계층적 구조를 가짐

◦ Spam Mail을 통한 사회공학적인 방법으로 확산

웨일덱의 구조는 다음 [그림 6]과 같이 계층적인 구조를 가지는 하이브리드 형태를 이루고 있다. 실제적인 악성행위를 하는 Worker bot은 C&C와 직접적인 통신을 하지 않으며, 중간에 P2P 통신을 하는 프록시 서버 그룹과 통신하게 된다.

Proxy bot은 Worker bot과 다른 프록시 봇, 혹은 C&C와의 통신을 중계하는 역할을 한다. 웨일덱에 처음 감염 되었을 때 좀비 피어는 하드 코드된 아이피로 접근을 시도한다. 연결이 되면 HTTP를 이용하여 통신을 하면서 키 교환을 한 후 좀비 피어의 정보를 보내고 다른 좀비 피어에 대한 정보를 얻는다. 물론 이 과정은 RSA, AES, OpenSSL, bzip2 압축, Base64 인코딩 등을 사용하여 암호화 한다.[4] 그 후 다른 좀비와 연결을 유지한다. 웨일덱의 Proxy bot은 주로 HTTP를 이용하여 통신하면서도 악성 HTTP 봇넷과는 달리 전송하거나 받는 데이터의 양의 차가 매우 크고, 연결 범위가 매우 넓은 P2P의 형태를 띄고 있다.

Worker bot의 경우, 실질적인 스팸 발송을 하는데, 하드코드된 IP에 접속을 시도하고, 좀비 피어에 설정되어 있는 DNS에 서버를 질의하고 win.jpg라는 실행파일을 다운 받는다. 그 후 다른 서버에 접근하는데 바로 구글로 리다이렉트한 후, 하드 코드된 mx.google.com에 연결을 시도하는데 이것은 Proxy bot이 스팸 메시지를 보낼 수 있는 환경인지를 검사하는 단계인 것으로 볼 수 있다. 이후 비정상적으로 DNS MX 쿼리가 많이 발생하고, 스팸 메일을 발송한다.

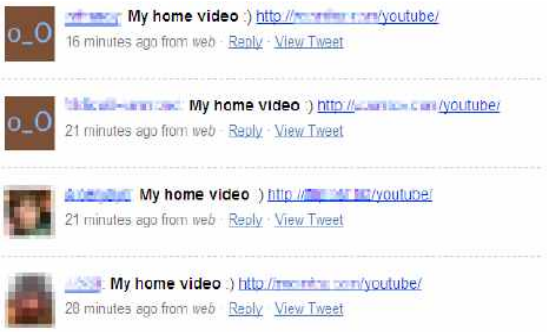


[그림 6 waledac 봇넷 구조

2. Koobface

2.1 개요

Kooface는 웹기반 악성 봇넷으로, HTTP(Hypertext Transfer Protocol) 프로토콜을 이용하는 중앙 집중 형 네트워크 구조를 가지고 있다. 다양한 기능을 가진 봇넷으로써 각각 기능에 따른 컴포넌트를 다운받아 설치하여 동작하는 구조를 가지고 있다. 최초의 Koobface는 구글(Google) 리더에 유튜브 동영상으로 위장하여 동영상에 필요한 코덱 다운로드를 요청하며 봇넷 감염을 유도한다.



[그림 7] Koobface의 Twitter 스팸 메시지

2.2 주요 특징

Kooface는 Cutwail, 과 마찬가지로 다양한 기능이 여러 파일에 나누어 제작되었으며, 감염된 좀비 시스템들은 C&C 서버로 정기적인 간격으로 폴링(polling) 하여 공격자와의 연결을 유지한다. 공격자가 C&C 웹 서버 상에 명령을 올려놓게 되면 좀비 시스템은 공격자의 명령을 응답(response) 받게 되고 명령에 따라 좀비 시스템들은 공격자가 지정한 피해 시스템으로 공격을 시도하게 되는 방식으로 명령체계를 구성한다. 전파 방식으로는 이동식 저장장치, 이메일의 첨부 파일이나 인스턴트 메신저의 파일 전송 기능을 통하여 유포되기도 하며, 공유된 네트워크 드라이브를 통하여 확산되기도 한다.

이 악성코드는 Facebook, MySpace, Twitter등의 SNS를 통해 유포되는 특성을 가지고 있다[9]. Koobface를 구성하는 주요 컴포넌트는 다음과 같다.

- Koobface downloader : 실제 악성행위를 하지 않고, 나머지 구성요소를 받기 위한 다운로더의 역할만 수행
- Social network propagation : 감염된 PC에서 이용한 SNS 사이트의 사용자 친구 혹은 멤버들에게 악성코드가 포함된 페이지로의 링크를 메일이나 텍스트 메시지를 이용해 전송
- Web Server component : Koobface는 감염된 PC를 봇넷의 일부로 두기 위해 웹서버 기능을 할 수 있도록 만들기도 하는데, 프록시 서버로 이용하거나, 가짜 YouTube 사이트 서비스를 제공하는 중계 서버로 사용
- Ads Pusher and rogue antivirus(AV) installer: 광고나 가짜 보안 소프트웨어를 받도록 하는 컴포넌트
- Data Stealer : 감염된 PC의 사용자 ID와 패스워드, 프로필 정보, 이메일 정보를 그림파일로 만들어 외부 C&C 서버로 전송
- Rogue Domain Name System(DNS) Change : 정상적인 DNS 서버 대신 감염된 DNS 서버로 연결을 변경하여 정상적인 페이지로의 접근을 피싱 사이트로의 접근으로 변경

3. Zeus

3.1 개요

최근 러시아 Black Market에서는 Crimeware의 판매가 성행하면서 취약점에 대한 Exploit을 담고 있는 Crimeware 배포를 위한 Kit을 판매가 성행하고 있다. 이와 같은 Crimeware에서 발전한 ZeuS Botnet은 최초 러시아에서 만들어져 Botnet의 규모만큼 영향력은 상당히 큰 편이다. 그러므로 ZeuS Botnet에 대한 다양한 사례들이 언급되고 있으며 러시아 Black Market에서 가장 잘 팔리는 Botnet 중 하나이다.

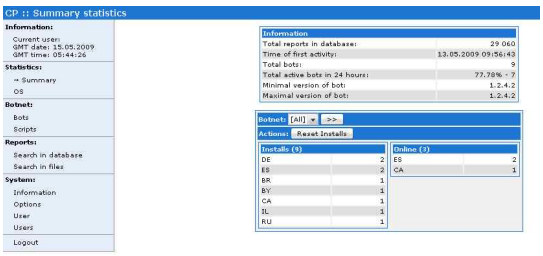
3.2 주요 특징

ZeuS는 본래 은행 정보를 수집하기 위한 악성코드를 만들기 위해 사용되는 Toolkit이며, Botnet을 구성하기 위해 필요한 악성코드를 생성하고 생성한 Botnet을 관리하는 기능을 제공한다. 그러나 ZeuS는 업데이트를 통해 다양한 프로토콜을 사용하여 사용자의 은행 정보뿐만 아니라 기타 금융 사이트 정보, 사용자 개인정보들을 수집한다.

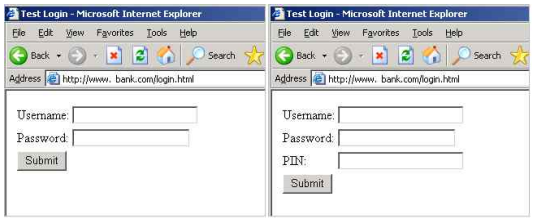
ZeuS Control Panel은 여타 Botnet과 동일하게 Botmaster가 Bot들을 제어하고 Bot들에게 명령을 내리기 위해 사용한다. ZeuS Control Panel은 PHP로 구성되어 있어 IIS와 Apache등에서 사용할 수 있으며 MySQL과 연동가능하다. 그러므로 ZeuS Control Panel Code를 Web Server에 복사하면 ZeuS Control Panel Install Page에 접근하여 설치할 수 있다.

ZeuS Bot이 정보수집 Bot으로써 역할을 수행하기위해 Web Page Injection을 수행하는데, 다운로드 받은 Dynamic Config에서 정의한 Web Site에 접근할 때, 동적으로 Form을 추가하여 사용자의 개인정보를 탈취한다.

최근 ZeuS와 Bredolab를 통해 FaceBook 사용자 패스워드를 Reset했다는 스팸 메일이 첨부파일과 함께 발송되고 있는데, 이들 스팸은 서로 각자의 봇들을 제외한 다른 봇을 제거하는 기능을 구현하고 있어, 봇넷간의 배타적인 동향도 보이고 있다.



[그림 8] ZeuS Botnet Control Panel



[그림 9] ZeuS 봇넷의 Web Page Injection 결과

Ⅴ. 봇넷의 향후 전망 및 대응 방향

1. 봇넷의 향후 전망

최근의 봇넷은 다양한 암호학적 기법과 함께 사회 공학적인 방법을 가지고 그 파급력을 극대화 하고 있다. 특히 점점 P2P 네트워크를 기반으로 생존력을 극대화 하여 봇넷의 탐지 및 대응을 어렵게 하고 있으며, CAPTCHA 같은 방어 기술을 보다 능동적으로 무력화 하려는 경향이 가속화 될것으로 보인다.. 또한 다양한 암호 알고리즘을 사용한 암호 통신과 호스트 시스템에서의 다양한 무력화 기법 및 은닉 기법들이 일반화 되어 분석이 더욱 어려워 질 것으로 전망된다.

통신 환경에 있어 스마트 폰의 보급화에 따라 SNS는 모바일 사용자까지 수용할 수 있는 서비스로 확대 되고 있다. 모바일 환경에서는 무선의 특징으로 유선에서의 인터넷 환경보다 전파가 용이한 특성이 있으며, 이러한 모바일 환경은 봇넷이 구성되기에 좋은 환경이 되고 있다. 실제로 모바일 환경에서 동작하는 심비안 운영체제 기반에서 Sexy Space 악성 코드는 가입자 정보나 네트워크 정보를 탈취하여 외부 서버에 전송하고, 감염된 모바일 폰에 등록된 사용자들에게 SMS 스팸 메시지를 발송하는 등, 봇넷으로써의 가능성을 확인할 수 있다[7].

2. 봇넷의 대응 동향

2.1 학계

봇넷을 위한 대응기술로써 이미 기존에 봇 헌터(BotHunter), 봇 마이너(BotMiner), 봇 스니퍼(BotSniffer) 등이 제안되었다. 하지만 봇 행위에 대한 프로파일을 주기적으로 갱신해주어야 하는 문제, 화이트 리스트 기반으로써, 봇넷의 통신이 주요 화이트리스트를 사용하여 이루어지거나, 암호화된 통신 및 C&C와의 긴 주기를 가지는 봇넷의 경우 탐지가 힘들다는 단점이 있다.

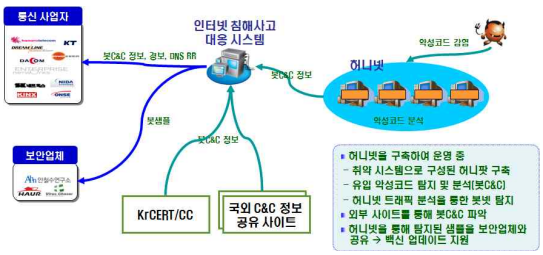
또한 DNS 쿼리를 기반으로 한 탐지 방법[1,3]이 제안되었는데, 이는 최근의 봇넷들이 DNS 쿼리가 아닌 하드 코드된 IP로 직접 통신을 하거나 DNS Fastflux를 사용하는 경우, 궁극적인 탐지 방법으로 보기 어렵다.

2.2 산업계

산업계에서는 크게 두 업체가 봇넷을 위한 전용 솔루션을 상용화 하여 대응하고 있다. Damballa와 FireEye에서 솔루션을 개발하여 상용화 하였는데, Damballa 솔루션의 경우 하나의 기업에 설치되어 모든 트래픽을 모니터링 하여 봇넷을 탐지하는 방식으로 대응하고 있으며 FireEye 솔루션의 경우, 회사에서 관리하는 중앙 데이터베이스 기반으로 탐지하며, 하나의 기업에 설치되어 모든 트래픽을 모니터링하고, 가상화 기법을 통해 봇넷을 탐지하는 방식으로 대응하고 있다.

2.3 정책

국내에서 한국인터넷진흥원(KISA) 인터넷 침해사고대응지원 센터에서는 봇넷에 대응하기 위해 DNS Sinkhole을 운영하고 있다[5]. Honeynet DNS 로그, 악성코드 수집 시스템, 외부 사이트, 사고분석(KrCERT/CC) 등에서 수집된 봇넷 C&C 서버 정보를 받아 이미 알려진 봇넷 C&C 서버의 도메인명을 질의하는 봇들의 DNS 질의를 ISP/IDC 사업자들과의 협력으로 DNS 싱크홀로 이용되는 서버의 IP 주소를 응답해 주도록 하였다. 봇넷 C&C 서버의 도메인명은 각종 여러 기관과 허니넷을 통하여 수집되고, 이들은 DNS 서버들의 블랙리스트에 기록된다. 이는 봇넷 확산을 원천적으로 방지할 뿐만 아니라 국내 봇 감염률 통계에도 유용하게 활용되고 있지만 최근 DNS 쿼리 이외의 하드 코드된 IP에 접속하는 경우와 정상적인 웹 사이트를 C&C로 사용하는 경우에는 대응이 어려운 점이 존재한다. 현재 KISA에서는 이러한 대응과 함께 일반 사용자들로 하여금 스스로 감염 여부를 확인할 수 있는 감염 확인 서비스도 제공하고 있다.



[그림 10] KISA의 봇넷 Sinkhole 정책

3. 봇넷에 대한 향후 대응 기술 방향

봇넷이 점차 발전함에 따라 탐지 기술 또한 다변화해야 한다. 특히 유연하고 확장성 있는 탐지 방안과 함께 컴퓨터 호스트 시스템 및 네트워크 단에서의 탐지 및 대응이 동시에 이루어 져야 하며, 이들의 탐지 정보를 관제할 수 있는 중앙 시스템이 요구된다. 그리고 이들 관제 시스템간의 정보 공유를 통해 국지적으로 산재되어 있는 봇넷에 대응할 수 있다. 현재까지의 봇넷의 발전 동향에 대응하여 아래의 기술적인 요인들에 대해 선결되어야 한다.

◦ 능동적 봇넷 탐지 기술

봇넷이 활동하기 전에 봇넷의 구성에 대해 탐지 할 수 있어야 한다. 최근의 봇넷들은 대부분의 공격 시간이 2시간 이내로써, 공격을 한 후에 다시 변형적인 공격을 하는 경우도 존재하여 최초 이러한 봇넷이 구성되는 단계에서 탐지하여 선제적인 대응을 할 수 있어야 한다.

◦ P2P 봇넷에 대한 탐지 기술

기존의 중앙 집중형 방식에서 점차 분산화 되고, 하이브리드 형태의 구성을 가지는 봇넷에 대응하기 위해 중앙 집중형 뿐 아니라, P2P 형태의 피어 네트워크를 탐지할 수 있어야 한다. 이를 위해서는 호스트 시스템 단에서의 악성코드 분석 정보를 분석하여 초기 피어 리스트에 대한 정보와 네트워크 단에서 단일 노드에서의 다수 목적지에 대한 유사 행위를 그룹 공간 및 시간 공간상에서 분석하여 P2P 네트워크를 탐지할 수 있는 종합적인 분석 시스템이 요구된다.

◦ 다양한 채널에서의 악성 코드 수집 기술

최근의 봇넷은 직접적인 시스템에 대한 공격 보다 스팸 메일과 피싱 사이트에 의해 전파・감염되는 것이 일반적이다. 이를 위해서는 현재의 허니팟 이외에 능동적으로 메일을 수집하고 웹 사이트를 분석하여 악성 코드를 탐지하는 기술이 요구된다.

◦ 그룹 행위 기반의 봇넷 탐지 기술

봇넷의 기본적인 특징은 다수의 좀비 시스템이 동일한 행위를 한다는 점이다. 이는 곧 그룹행위를 의미하며, 프로토콜 및 네트워크 토폴로지에 독립적인 봇넷의 특징으로 볼 수 있다. 이러한 그룹 행위를 기반으로 봇넷의 프로토콜과 네트워크 토폴로지에 상관없이 봇넷을 탐지할 수 있는 고도화된 기술이 요구된다.

◦ 지능화된 악성 코드 분석 기술

봇넷을 구성하기위해 시스템을 감염시키기 위한 악성코드는 탐지가 되지 않고, 분석을 어렵게 하기 위해 다양한 기법을 사용한다. 이러한 지능적인 악성 코드의 방어적 기법을 무력화하기 위해서는 악성 코드가 수행하는 행위 기반의 분석 기술이 필요하며, 악성 코드가 분석 환경이 가상 환경임을 알 수 없도록 하는 진화된 가상 분석 환경이 요구된다.

Ⅵ. 결 론

최근 악성 봇넷은 금전적 이익을 목적으로 혹은 불특정 다수를 대상으로 공격을 진행하고 있어 악성 봇넷에 대응할 수 있는 기술이 국가적인 요구사항이 되었고, 그에 따라 학계, 기업계 그리고 국가 연구 기관에서 많은 연구가 진행되고 있다.

인터넷 인프라에 대한 국가의 의존도가 높아지는 현 상황에서, 봇넷에 의한 침해 사고는 엄청난 파급 효과가 있을 수 있다. 봇넷의 기술이 점차 진화하고 있지만, 그에 따른 대응기술은 그 속도를 따라가지 못하는 것이 현실이다. 또한 봇넷은 인터넷에 존재하는 거대 네트워크로써 국가 간 및 ISP 간의 협력 없이는 대응이 어려운 점이 있다.

따라서 국제적 공조가 필요한 만큼 봇넷 대응 기술 및 절차에 관한 표준 기술의 개발이 선행되어야 하며, 더불어 봇넷이 구성되는 시점에서 능동적인 봇넷을 탐지하고 그 구성을 와해시킬 수 있는 대응 기술이 필요한 시점이다.

참고문헌

[1] Antoine Schonewille, Dirk-Jan van Helmond, “The Domain Name Service as an IDS,” A Research Project for the Master System and Network Engineering at the University of Amsterdam, February 2006.

[2] Basudev Saha, Ashish Gairola., “Botnet: An Overview,“ CERT-In, June 2005.

[3] Hyunsang Choi, Hanwoo Lee, Heejo Lee,

Hyogon Kim, “Botnet Detection by Monitoring Group Activities in DNS Traffic,” IEEE Int'l Conf. Computer and Information Technology (CIT), 2007.

[4] Jonell Baltazar,Joey Costoya, Ryan Flores, “Infiltrating WALEDAC Botnet's Covert Operations,” TREND MICRO, 2009

[5] KISA, “KISA Botnet Mitigation Activity,” Fourth International Botnet Task Force Conference, France, April 2006.

[6] Markus J, Zulfikar R., “Crimeware: Understanding New Attacks and Defenses,” Addison Wesley Professional, ISBN 0-321-50195-0, April 2008.

[7] 김동빈, "휴대전화 봇넷 등장?...휴대전화 이용한 DDoS 공격 우려정보보호," 보안뉴스, http://www.boannews.com/media/view.asp?idx=17182&kind=1, July, 2009.

[8] Ellen Messmer, “America's 10 most wanted botnets,” Damballa, http://www.networkworld.com/news/2009/072209-botnets.html?page=1, July, 2009

[9] Jose Nazario, “Twitter-based Botnet Command Channel,” http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/, August, 2009.

[10] Kelly Jackson Higgins, “New Massive Botnet Twice the Size of Storm,” Dark Reading, http://www.darkreading.com/document.asp?doc_id=150292, April, 2008.

[11] Joe Stewart, "Spam Botnets to Watch in 2009," SecureWorks, http://www.secureworks.com/research/threats/botnets2009, January, 2009.

[12] Websense, “Malicious Facebook Password Spam,” http://securitylabs.websense.com/content/Alerts/3496.aspx, October, 2009.

[13] WebUser, “Cutwail botnet 'recovers quickly',” http://www.webuser.co.uk/news/news.php?id=285193, June, 2009.

<著者紹介>

강 동 완 (Kang Dongwan)
정회원

2007년 2월 : 순천향대학교 정보기술공학부 졸업
2009년 2월 : 순천향대학교 컴퓨터학과 석사
2009년 1월~현재 : 한국인터넷진흥원 연구원
<관심분야> 봇넷 탐지, 네트워크 보안, 신뢰 컴퓨팅 보안

임 채 태 (Im Chaetae)
정회원

2000년 2월 : 충남대학교 컴퓨터과학과 졸업
2003년 2월 : 포항공과대학교 컴퓨터과학과 석사
2003년 3월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 네트워크 보안, 시스템 해킹보안, VoIP 보안, 이동통신

정 현 철 (Jeong Hyuncheol)
정회원

1996년 2월: 서울시립대학교 전산통계 졸업
1998년 8월: 광운대학교 전자계산 석사
1996년 7월~현재: 한국인터넷진흥원 팀장
<관심분야> 정보보호, 네트워크 보안, 무선랜 보안, VoIP 보안