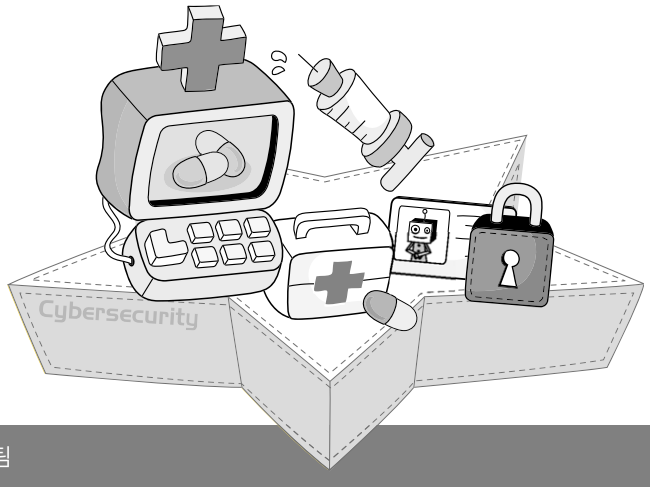
봇넷(Botnet) 동향 및 대응기술 현황

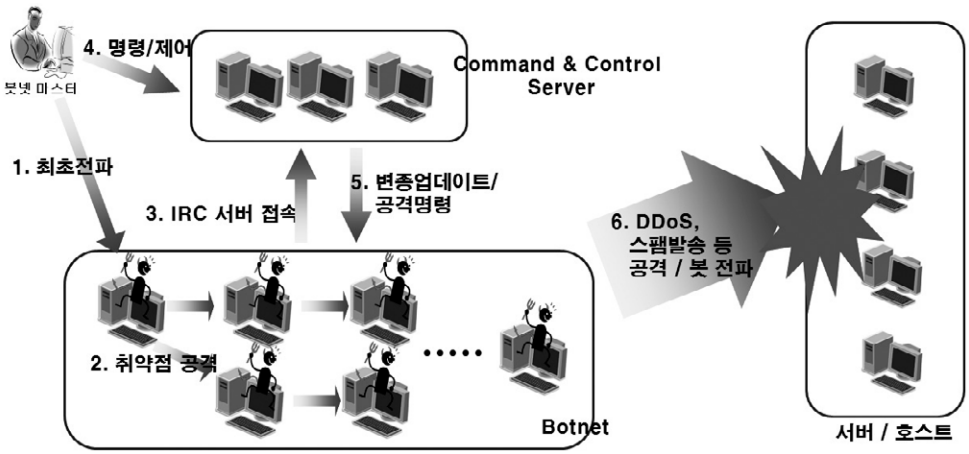


임 채 태 • 한국정보보호진흥원 응용기술팀

현재 사이버 공간에서는 수많은 위협들이 대두되고 있다. 제3자의 개인정보를 갈취 또는 수집하여 악용하고, 불특정 다수를 향해 음란, 광고메일을 유포하고 금전적 이익을 보거나, 또는 경쟁사의 정보화 기기의 서비스를 못하게 하는 등 인터넷상의 위협요인들은 산재해 있다. 이러한 사이버 피해가 두드러지는 가운데 새로운 위협적 요소가 인터넷을 장악해 나가고 있는데 그것이 바로 봇넷이며, 가장 심각한 네트워크 위협으로 봇넷과 분산서비스 거부공격(DDoS) 공격이 선정되었다.(Arbor Networks, 2007)

1. 봇넷이란?

악성 소프트웨어인 봇에 감염된 다수의 컴퓨터들이 네트워크로 연결되어 있는 형태를 봇넷(Botnet)이라 한다. 즉, 봇들을 자유자재로 통제하는 권한을 가진 봇마스터에 의해 원격 조종되며 각종 악성행위를 수행할 수 있는 수천에서 수십만 대의 악성프로그램인 봇(Bot)에 감염된 컴퓨터들이 네트워크로 연결되어 있는 형태를 봇넷이라 한다.



[그림 1] 봇넷의 구성 및 공격시나리오

2. 봇넷 분포 및 피해 동향

봇넷은 1993년에 EggDrop으로 처음 나온 이후로 최근 10년간 Forbot, PBot, Toxbot, Machbot, PHP Bot, Storm Bot 등으로 진화한 봇이 출현하였으며, 최근에는 너무 많은 변종 봇이 출현하면서 대응을 매우 어렵게 하고 있으며(매일 5,000개의 신규 악성코드 출현, TechNewsWorld, 2007), 전 세계적으로 C&C 서버(Command & Control, 봇 좀비들에게 명령을 내리고 제어하기 위한 서버)와 악성 봇은 광범위하게 분포하고 있고 특정 지역적에 밀집되는 양상을 보이고 있다. 이는, 초고속 인터넷이 잘 갖추어진 환경에서는 기존에 비해 1/10의 PC들만 이용해도 더욱 강력한 DDoS와 같은 공격이 가능하기 때문이며, 초고속의 인터넷 인프라가 잘 갖추어져 있는 국내 지역은 봇넷 감염지로 선호되는 지역이다.

※ 2007년 2월, 미국의 2개 루트서버가 봇넷을 통한 DDoS 공격으로 5시간 동안 서비스 장애가 발생하였을 당시, 이중 61%가 한국에서 발송되었음

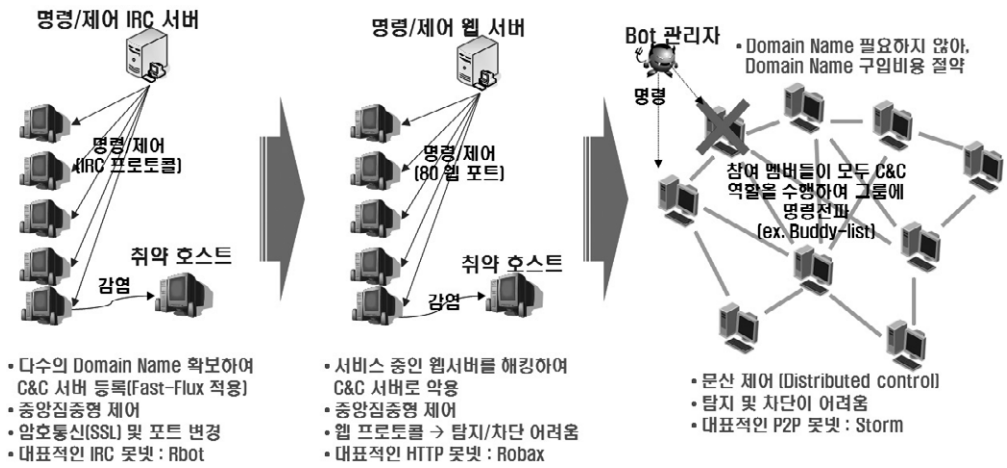
세계적으로 봇에 감염되어 좀비 PC로 바뀌는 PC의 수가 지속적으로 증가하고 있으며 봇넷의 규모 또한 커지고 있다. TCP/IP 프로토콜 공동 창시자인 Vint Cerf는 전 세계 컴퓨터의 약 11% 정도인 1억~1억 5천 컴퓨터가 봇 악성코드에 감염되어 공격 수행에 사용될 것으로 예상하였으며, 현재까지 알려진 가장 큰 봇넷은 Storm 봇넷으로 230,000개의 좀비들로 연결되어 있는 것으로 알려져 있다.

봇넷으로 인한 공격이 더욱 심각해지는 이유는 범죄화 양상을 띠고 있는데 있다. 2007년 발생한 아이템 거래업체 서비스 장애 유발 및 현금요구 협박 사고에서와 같이 서비스 장애유발을 빌미로 서비스 업체에

협박하여 금품 갈취하거나, 개인/금융 정보 수집 및 스팸 발송 등을 통하여 대가를 받는 사고가 빈번하게 발생하고 있다.

3. 봇넷의 특성 및 진화

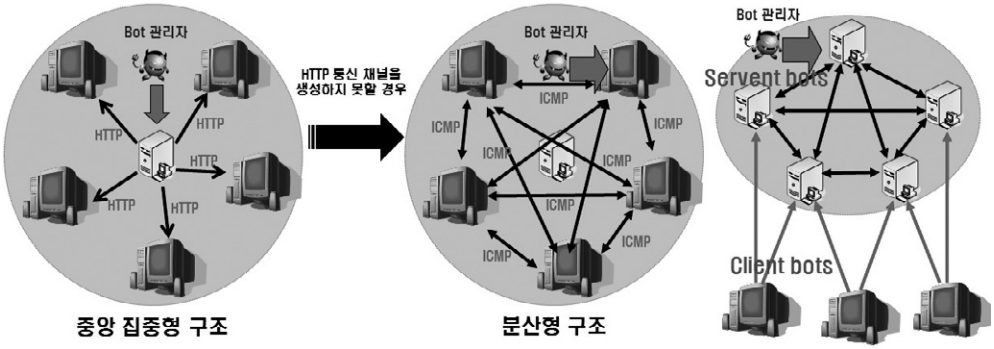
봇은 웜/바이러스, 백도어, 스파이웨어, 루트킷 등 다양한 악성코드들의 특성을 복합적으로 지니며, 봇넷을 통해 DDoS, Ad-ware, Spyware, 스팸발송, 정보불법 수집 등 대부분의 사이버 공격이 가능하다.



[그림 2] 봇넷 명령/제어 방식의 진화

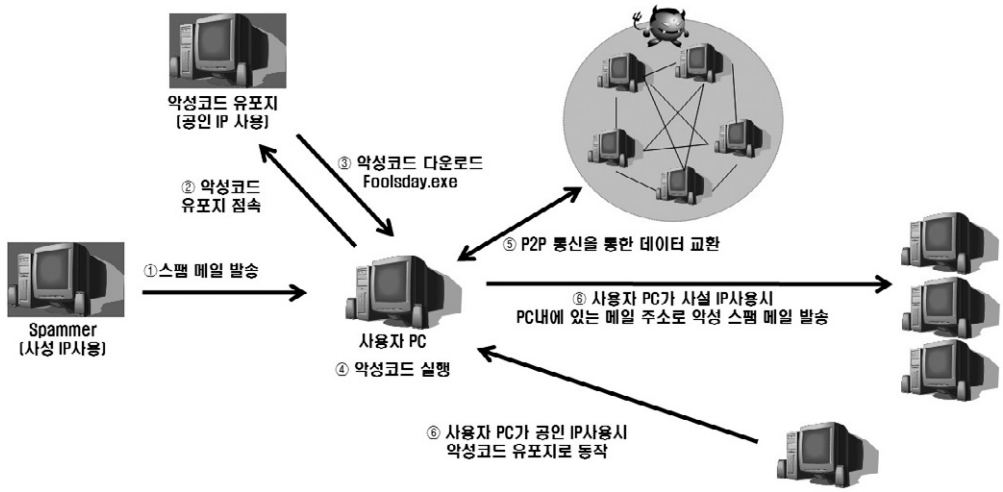
초기의 봇넷은 구조가 유연하고 널리 사용되는 IRC의 특성을 이용한 IRC 봇넷이 주를 이루었었다. 하지만, 탐지 및 대응을 보다 어렵게 하기 위해 웹 프로토콜인 HTTP를 기반으로 하거나, C&C라는 중앙집중형 명령/제어 방식(IRC, HTTP 봇넷)에서 탈피하여, 모든 좀비들이 C&C가 될 수 있는 분산형 명령/제어 방식(P2P 봇넷)의 봇넷으로 진화하고 있다.

더 나아가, 명령/제어를 위해 2가지 이상의 프로토콜을 사용하는 하이브리드 형태로 진화하고 있다. 최근 등장한 MayDay 웜의 경우, [그림 3]과 같이 두 가지 프로토콜을 사용하거나, 다수의 중앙 집중 포인트(C&C서버)가 존재하고 중앙 집중 포인트는 P2P 방식으로 연결되는 하이브리드 형태로 진화하고 있다.



[그림 3] 하이브리드 명령/제어 방식

명령/제어 방식의 진화와 함께, 악성코드도 빠른 속도록 진화하여 탐지/대응을 매우 어렵게 하고 있다. Packing/압축/암호화 기술, VM(Virtual Machine)/디버거/샌드박스 탐지 우회 기술, 악성코드를 숨기기 위한 RootKit 기술 등이 적용되어 봇에 대한 탐지 및 분석을 매우 어렵게 하고 있으며, 감염경로 또한 기존의 시스템 취약점을 악용한 방식에서, 웹, 이메일, 메신저 등 다양한 수단으로 다양해지고 있다.



[그림 4] Foolsday 봇 전파 및 스팸 발송 절차

최근 이슈가 된 봇넷으로는 Mayday 봇, Foolsday 봇이 있으며, Mayday 봇의 경우, 2가지 이상의 프로토콜을 사용하는 하이브리드 형태로 진화된 양상을 보였으며, Foolsday 웜은 storm 웜의 변종으로 2008년 만우절을 전후로 발견되었다.

4. 봇넷 대응 기술 현황

대응 기술은 적용 대상에 따라, PC상에서 악성 봇 프로그램 설치 및 행동을 기반으로 탐지/분석하는 호스트 기반과 봇 좀비 및 C&C로부터의 네트워크 트래픽을 기반으로 탐지/분석하는 네트워크 기반으로 구분되며, 기술 특성에 따라 시그니처 기반과 행위기반으로 구분될 수 있다.

1) 봇넷 대응 기술 현황

호스트를 대상으로 탐지/분석하는 기존 상용 기술들을 정리하면 아래표와 같다.

〈표 1〉 호스트 대상 기존 상용기술 특성

	시그니처 기반	행위 기반
제품 및 특징	○ AntiVirus, 백신 솔루션 등 – 시그니처 기반 상용 솔루션 – 악성코드에 대한 시그니처를 바탕으로 예방, 검색, 치료하는 종합 서비스를 제공	○ Sandbox – 가상머신(Virtual Machine)를 이용하여 컴퓨터에서 파일을 실행하여 행위 분석 ○ Nepenthes(공개툴) : 취약점들을 emulate 한 후에 침투 악성코드 분석
한계점	○ 신종/변종 악성코드에 대한 탐지 어려움 ○ 패킹, 압축, 암호화 등 다양한 회피기술의 사용으로 인한 탐지 어려움 ○ 커널레벨에서 구동되는 악성코드에 대한 탐지/대응이 어려움	○ 오탐 및 미탐 발생 ○ VM, 샌드박스, 디버거 탐지 등 다양한 회피기술의 사용 ○ 커널레벨에서 구동되는 악성코드에 대한 탐지/대응이 어려움

네트워크를 대상으로 탐지/분석하는 기존 상용 기술들을 정리하면 아래 표와 같다.

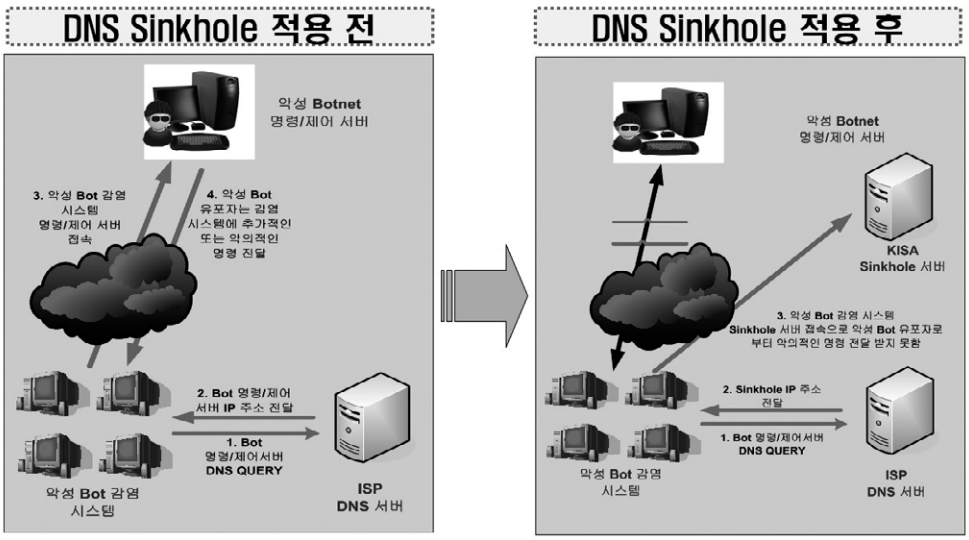
〈표 2〉 네트워크 대상 기존 상용기술 특성

	시그니처 기반	행위 기반
제품 및 특징	○ 봇넷 전용 네트워크 솔루션 ※ 최근 들어, 외국에서 전용장비가 출시되고 있음 ○ IDS, IPS, F/W 상용 제품	○ 봇넷 전용 네트워크 솔루션 – 네트워크 트래픽을 분석하여 봇넷을 탐지하고, 봇넷으로부터의 공격을 차단
한계점	○ 알려진 시그니처 기반 공격 탐지/대응 ○ 봇넷 전체구성, 봇 좀비 분포 및 과거 봇넷의 변동사항 등 정보 파악 어려움	○ 스텔스 스캔, 채널암호, 명령/제어패턴 변경 등 기법 적용으로 오탐/미탐 발생
	○ HTTP 및 분산형 P2P 봇넷에 대한 탐지/대응 어려움 (최근, HTTP 봇넷에 대한 일부 탐지/대응 기능이 탑재된 솔루션이 출시되었음)	

최근 들어, 봇넷의 심각성이 부각되면서 국제적으로 연구가 활성화되고 있는 추세이지만, 대체로 IRC 봇넷 중심으로 진행되어 왔으며, HTTP 및 P2P 봇넷에 대해서는 현황 및 특성에 대해서만 다루어져 왔다. IRC 봇넷에 대한 기존 대부분의 연구들은 채널 암호화, 스텔스 스캐닝, 명령/제어 패턴 변경, DNS 스푸핑 등을 통해 회피가 가능하고 오탐발생의 소지가 있으며, 최근 등장하는 HTTP/P2P 신규 봇넷에 대한 대응이 미흡한 수준이다.

2) 국내 봇넷 대응 현황

한국정보보호진흥원에의 봇넷 대응은 국제적인 Best Practice로 받아들여지고 있다. 그 대응을 살펴보면, Honeynet DNS 로그, 악성코드 수집시스템, 외부 사이트, 사고분석(KrCERT/CC)를 통해 봇C&C 정보를 수집하고, 이를 업체 및 사업자와 공유하고 있으며, 아래 그림과 같이 DNS 싱크홀을 운영하여 C&C 서버와 봇 좀비간의 통신을 단절시켜 공격에 악용되는 것을 방지하고 있다.



[그림 5] DNS 싱크홀

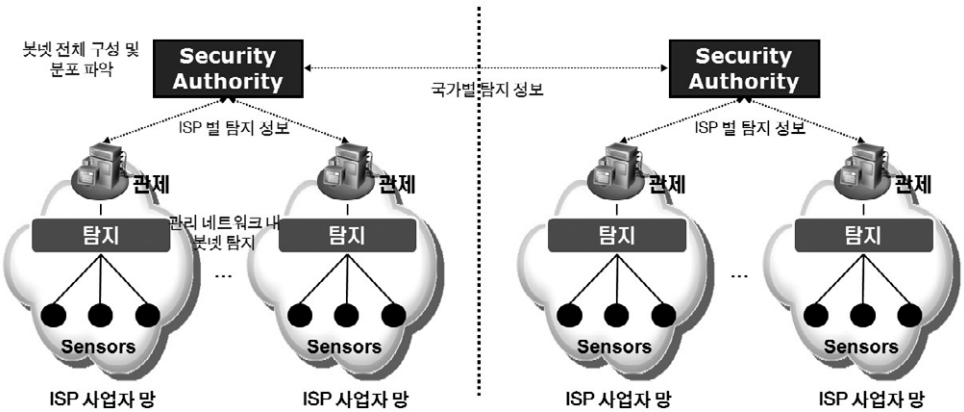
국내 대응은 국제적으로 좋은 모델이지만, HTTP/P2P 탐지 및 대응에는 어려움이 있으며, DNS 싱크홀을 우회할 수 있는 기술이 등장하고, 악성코드 분석도구를 우회하는 지능형 봇의 지속적인 증가로 탐지 및 대응을 어렵게 하고 있다.

5. 국제적인 공동대응 및 표준화

앞서 살펴본 바와 같이 봇 C&C(Command & Control) 서버와 봇 좀비들이 전세계적으로 광범위하게 분포하고 있으며 특정 지역에 밀집되는 양상을 보이고 있다. 이러한 상황에서 봇넷을 탐지하기 위해서는, ISP 사업자들이 탐지한 단편적인 탐지 정보들이 취합될 때 비로소 봇넷의 정확한 구성(C&C 서버, 봇 좀비)을 파악할 수 있으며, 구성상의 변동사항에 대한 추적이 가능하다. 또한, 봇넷을 통한 사이버 공격을 탐지하는 경우, 봇넷 구성정보를 기반으로 보다 조기에 정확하게 탐지가 가능하다. 예를 들어, 봇넷을 통한 DDoS 공격을 실행하는 경우, 기존의 대응 시스템에서는 트래픽이 집중되는 피해자가 위치하는 영역에서 탐지가 가능하였으나, 봇넷 구성정보를 알고 있는 경우, 봇 좀비들이 위치하는 ISP에서 조기에 탐지가 가능하다.

봇넷에 대응하기 위해서는, 봇 좀비들이 사이버 공격에 악용되지 않도록 봇넷 구성 자체를 와해시키거나, C&C 서버의 명령/제어를 단절함으로써 공격을 수행하지 못하도록 하는 대응이 가능하다. 탐지에서와 마찬가지로 봇넷 구성정보에 기반하여 ISP 및 국가간 협력이 수반되어야 효과적인 대응이 가능하다. (예: C&C가 위치한 ISP에서 C&C로의 접근을 차단)

따라서, 점차 심화되는 봇넷 위협에 효과적인 탐지 및 대응을 위해서는 ISP 및 국가간 정보 공유 및 공조대응이 필요성에 대한 공감대를 기반으로 관련 국제 표준화가 마련되어야 한다.



[그림 6] 봇넷 탐지 정보 공유

6. 맺음말

인터넷에 대한 의존도가 점차 심화되는 상황에서의 향후 침해사고는 지금과는 다른 엄청난 파급효과를 유발할 수 있다. 따라서, 안전한 인터넷 환경을 만들기 위해 인터넷의 최대 위협으로 인식되고 있는 봇에 대한 대응이 시급한 실정이다. 하지만, 현재의 기술은 봇넷의 진화속도에 뒤쳐져 있는 것이 현실이고, 기존과는 다르게 ISP 및 국가간 상호 협력이 요구된다.

기술 측면에서는 아무리 다양한 변종이 등장하더라도 탐지할 수 있는 지능적이며, 능동적인 탐지 기술과, 봇넷의 구성 및 분포와 공격을 조기에 정확히 파악할 수 있는 모니터링 기술과 봇넷의 구성을 와해하거나, 사전에 공격을 차단할 수 있는 대응기술 개발이 필요하다. 또한, 봇넷은 하나의 사업자 영역이 아닌 국제적으로 분포됨에 따라 국제적인 공조가 필요하므로, 이를 위해 체계적인 봇넷 탐지 및 대응 프레임워크와 공조를 위한 절차 및 방법에 대한 국제 표준화가 선결되어야 할 것이다.

IT강국으로서의 위상을 이어갈 수 있도록 인터넷 기반을 튼튼히 할 수 있는 봇넷 탐지 및 대응 기술과 표준이 조속히 마련되어야 할 것이며, 더불어, 정보보호 기술 및 산업측면에서 국제적인 정보보호 기술 우위를 선점하고, 신규 시장을 창출하고, 표준화를 주도하여 국가 위상을 제고할 수 있는 기회를 제공하고 있으므로, 이러한 기회를 잘 활용할 수 있어야 할 것이다. TTA

정보통신용어해설

모바일 지갑
Mobile Wallet, 一紙匣 [통신서비스]

휴대폰을 신용카드처럼 사용하는 서비스로서 물품 구매시 전용칩이 내장된 휴대폰을 무선 리더기에 인식시키기만 하면 결제가 가능한 서비스이다. 모바일 지갑에 대해서는 사용에 대한 비용문제와 보안문제로 휴대전화분실이나 개인정보 유출문제 등의 해결과제가 남아 있다.