www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2012.17.3.117

활성 포렌식 기술을 이용한 좀비 PC 탐지시스템 모델

Detection System Model of Zombie PC using Live Forensics Techniques

홍준석(Jun Suk Hong)*, 니오박(Neo Park)**, 박원형(Won Hyung Park)***

초 록

2009년에 발생한 7.7 DDoS(Distributed Denial of Service) 공격에 이어 2010년 3월 4일에도 주요 기관 사이트를 대상으로 대규모의 DDoS 공격이 발생 하였다. 악성코드 제작과 배포는 누구나 쉽게 좀비 PC를 양산할 수 있게 되고 DDoS 공격기법이 지능화・고도화되어 감에 따라서 DDoS 공격을 대응하는 보안담당자의 어려움은 점점 커져가고 있다. 정상 PC에서 좀비 PC로 감염되어 호스트에서 발생하는 변조내용을 분석하여 활성 포렌식 기술로 점검해야 하는 항목이 무엇인지 연구한다. 본 논문에서는 PC 보안관제시스템 구축 및 운영 방안에 대하여 다루었으므로 해당 시스템을 도입하려는 기업에게 좋은 기준서로 활용될 수 있다.

ABSTRACT

There was a large scale of DDoS(Distributed Denial of Service) attacks mostly targeted at Korean government web sites and cooperations's on March 4, 2010(3.4 DDoS attack) after 7.7 DDoS on July 7, 2009. In these days, anyone can create zombie PCs to attack someone's website with malware development toolkits and farther more improve their knowledge of hacking skills as well as toolkits because it has become easier to obtain these toolkits on line, For that trend, it has been difficult for computer security specialists to counteract DDoS attacks. In this paper, we will introduce an essential control list to prevent malware infection with live forensics techniques after analysis of monitoring network systems and PCs. Hopefully our suggestion of how to coordinate a security monitoring system in this paper will give a good guideline for cooperations who try to build their new systems or to secure their existing systems.

키워드 : 좀비 PC, 활성 포렌식, 보안관제시스템
Zombi PC, Live Forensics, Security Monitoring System

* 주저자, 성균관대학교 정보통신대학원 정보보호전공 공학석사
** 극동대학교 유비쿼터스학과 전임교수
*** 교신저자, 극동대학교 정보경영학과 전임교수
2012년 08월 16일 접수, 2012년 08월 27일 심사완료 후 2012년 08월 28일 게재확정.

1. 서 론

과거에는 해커 스스로의 실력과시와 장난의 목적으로 해킹이 이루어지던 것과는 달리 최근의 해킹기술은 금전적·정치적·군사적인 목적을 가지고 해킹이 발생하고 있다. 작년 4.8 현대캐피탈 해킹에서 볼 수 있듯이 사용자 개인의 중요 정보는 해커들의 주요 표적이 되었고 나아가 기업과 공공기관 심지어 국가를 표적으로 한 공격이 이루어지고 있다. 작년 발생한 3.4 DDoS 공격, 4.12 농협 전산망 해킹, 2010년 9월 이란에서 발생한 스턱스넷이 대표적인 사례이다[1].

DDoS 공격은 지난 2009년 7월 7일에 이어 2011년 3월 4일 다시 한 번 대규모 형태로 발생하면서 정보보안업계의 큰 화두로 떠올랐다. 더불어 netBot Attacker, zeus와 같은 악성코드 제작 툴킷의 공개로 인해 DDoS 공격의 대중화 시대를 맞으면서 이제 DDoS 공격은 간헐적인 것이 아닌 상시적인 위협으로 우리에게 다가오고 있다. 중국발 6.9 성전과 폭로전문 웹사이트 위키리크스 공격, 경쟁 온라인 게임 사이트 공격 등이 대표적인 예이다[2, 3]. 그래서 본 논문은 호스트를 대상으로 하는 좀비 PC 탐지시스템에서 관제해야 할 항목을 선정 및 분석하고 효과적인 구축 및 운영 방안에 대해서 연구한다.

2. 관련 연구

2.1 서비스거부(DoS) 공격 기술

DoS 공격은 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다. 특정 target에게 수많은 트래픽을 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나 tcp 연결을 위해 필요한 서버의 자원을 고갈시키는 등의 공격이 이 범위에 포함된다. 기본적인 DoS 공격은 여러 가지 방법들이 사용되어 왔으며 최근에는 protocol을 이용하여 공격하는 형태로 변형되고 있다. DoS 공격의 유형으로는 대표적으로 아래 6가지를 말할 수 있다[4, 5].

기본적 공격방법을 응용한 분산서비스거부(DDoS) 공격은 여러 대의 Agent가 Target을 향해 일제히 DoS 공격을 하게 만드는 해킹 방식의 하나이다[6]. Client가 명령을 내리면 각 Agent에서 Target을 향해 많은 분량의 패킷을 동시에 전송한다. 이처럼 Agent를 여러 개의 시스템에 설치하고 이 Agent를 제어하여 공격을 실행함으로써 보다 강력한 공격을 시도할 수 있으며 IP 스푸핑을 사용하여 공격자에 대한 역추적 공격트래픽의 차단을 어렵게 만드는 공격 형태이다.

DDoS 공격을 주시해야 할 이유는 다른 공격의 사전 작업으로 이용되어 피해가 발생할 가능성이 크기 때문이다. 또한 최근 변형된 공격방법으로 DRDoS 공격[6]이 있는데 DDoS 공격 방법의 단점인 좀비 PC를 이용하지 않으면서 target에게 피해를 줄 수 있다는 장점이 있다[7, 8]. 기존의 DDoS 공격 방법에 비하여 향상된 공격 특성으로 인하여 DDoS 공격의 변형이 발생할 가능성이 아주 높기 때문에 이러한 변화된 공격에도 안전하게 방어하기 위한 방법이 절실히 요구된다. DRDoS 공격을 DDoS 공격보다 발전된 공격방법이라

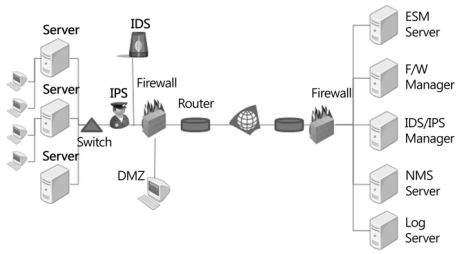
할 수 있는 가장 큰 내용은 반사 서버의 활용이다[9].

좀비 PC란 악성코드에 감염되어 악성코드 제작자의 의도에 따라 명령을 수행하는 PC를 뜻한다. 즉, '사용자가 모르는 사이에 해커의 원격 조정을 받는 PC'로 원격지에 있는 악성코드 제작자의 명령에 의해 조정된다는 의미에서 좀비라는 용어로 불리게 되었다. 악성코드 형태로 이메일, 액티브X, 공유사이트 등등에 심어져 일반 PC에 감염이 된다. 이것은 DDoS 공격에 이용돼 특정 target으로 대량의 트래픽을 전송하는 역할을 한다. 또한 해커가 원할 경우 PC에 담긴 개인정보를 빼내거나 시스템을 손상시킬 수도 있다. 이처럼 수많은 PC가 운영자도 모르는 사이에 해킹의 도구로 이용되고 있다.

2.2 기존 보안관제시스템 기술

기존 보안관제시스템은 아래와 같이 5가지의 시스템을 운영하고 있다[10].

- 침입차단시스템(Firewall System) : 인터넷에 접속되어 있는 네트워크를 불법적인 침입으로부터 보호하기 위해 게이트웨이에 설치되는 접속제한 시스템으로 방화벽이라고도 한다. 침입차단시스템은 웹 방화벽, 네트워크 방화벽, PC 방화벽으로 등으로 구성한다.
- 침입방지시스템(IPS, Intrusion Prevention System) : 시스템 및 네트워크 자원에 대한 다양한 형태의 침입행위를 실시간 탐지, 분석 후 비정상으로 판단된 패킷을 차단해 네트워크 위협을 사전에 방지하는 시스템이다.
- 통합보안시스템(UTM, Unified Threat Management) : 다중 위협에 대해 보호 기능을 제공할 수 있는 포괄적 보안제품을 의미하며 방화벽, 안티바이러스, 스팸필터를 하나의 패키지로 통합되어 있는 제품이다.
- 위협관리시스템(TMS, Threat Management System) : 국내·외 최신 취약점 정보와 보안 트랜드, 정밀 분석된 네트워크 트래픽 및 공격 형태를 상관 분석해 인터넷 웜, 바이러스, 해킹 등의 사이버공격을 예측하고 판단하여 보다 능동적으로 대응할 수 있는 체계적인 위협관제 및 대응시스템이다.
- 패치관리시스템(PMS, Patch Management System) : 시스템의 보안 취약점을 보완하기 위하여 배포되는 보안패치 파일을 원격에서 자동으로 설치, 관리해 주는 시스템이다.



〈그림 1〉 보안관제시스템 구성도[11]

2.3 기존 보안관제시스템의 문제점

기존의 보안관제시스템은 규모가 큰 네트워크 내의 중요 서버들을 대상으로 시행되어 왔다. 이러한 구조는 좀비 PC가 유발하는

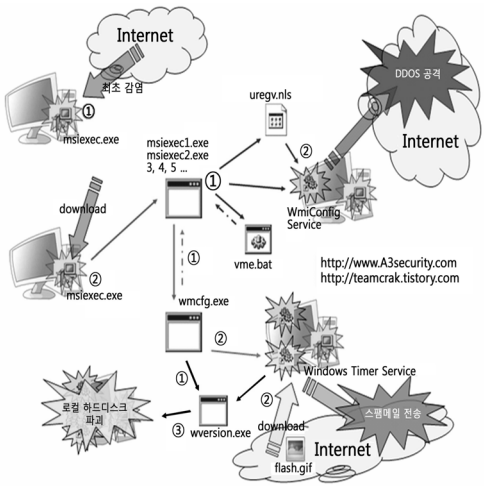
DDoS 공격을 원천적으로 봉쇄하는 것이 불가능 할 뿐만 아니라 DRDoS 공격 등 변화된 신종 공격에는 매우 취약하다. 또한 침입탐지 시스템은 민감성이 매우 중요하다. 특정 탐지나 공격의 패턴을 민감하게 감지할 수 있어야 고도의 네트워크 해킹 기법들에 대응할 수 있다. 그렇지만 이러한 민감성은 일반적으로 발생할 수 있는 트래픽들, 예를 들어 일부 nat 장비에서 발생하는 “port 0”과 같은 이벤트나 한 기업에서 프록시 캐시를 사용하는 경우는 “port scan”이라는 특정의 이벤트들로 감지할 수도 있다. 이를 false positive라고 한다. 말 그대로 하면 “잘못된 양성반응”이라고 할 수 있다. 이러한 false positive는 모든 침입탐지시스템에서 일반적인 현상이므로 충분한 customize가 필요하게 된다. 따라서 세션 차단 기능 또는 라우터나 firewall 연동 시에 주의 깊게 정의를 하여야 하며 만약 이런 false positive에 대해 정의하지 않는 경우 일반적인 서비스에 큰 장애를 유발하게 된다.

앞서 다룬 기존의 보안관제시스템 한계점들을 보완하기 위해서는 호스트에서 원천적으로 공격을 탐지해 신속히 대응하기 위한 좀비 PC 탐지시스템이 필요하다. 이 호스트에서의 대응 기술은 감염이 되었을 시에 특정 패턴 및 로그를 분석해 그 차이를 분석하고 탐지하는 것이 핵심이다. 소프트웨어 측면에서 볼 때 Agent가 각 호스트마다 설치돼야 한다는 점에서 백신의 경우와 동일한 선제조건이 있다. 하지만 백신에 비해 공격자를 검출하는 판단기준인 사용자 비정상 행위기반[12]의 요소를 수집 분석하는 등 기존 수천 개의 탐지룰이 없어도 쉽게 탐지가 가능하다는 장점이 있다. 또한 각 Agent가 중앙관제 시스템으로 연결되어 악성코드에 감염된 내용, DDoS 연결세션, 그리고 레지스트리 변경 등을 바로 알 수 있고 그에 따라 실시간으로 대응 할 수 있는 능동적인 방어 체계가 실현될 수 있다.

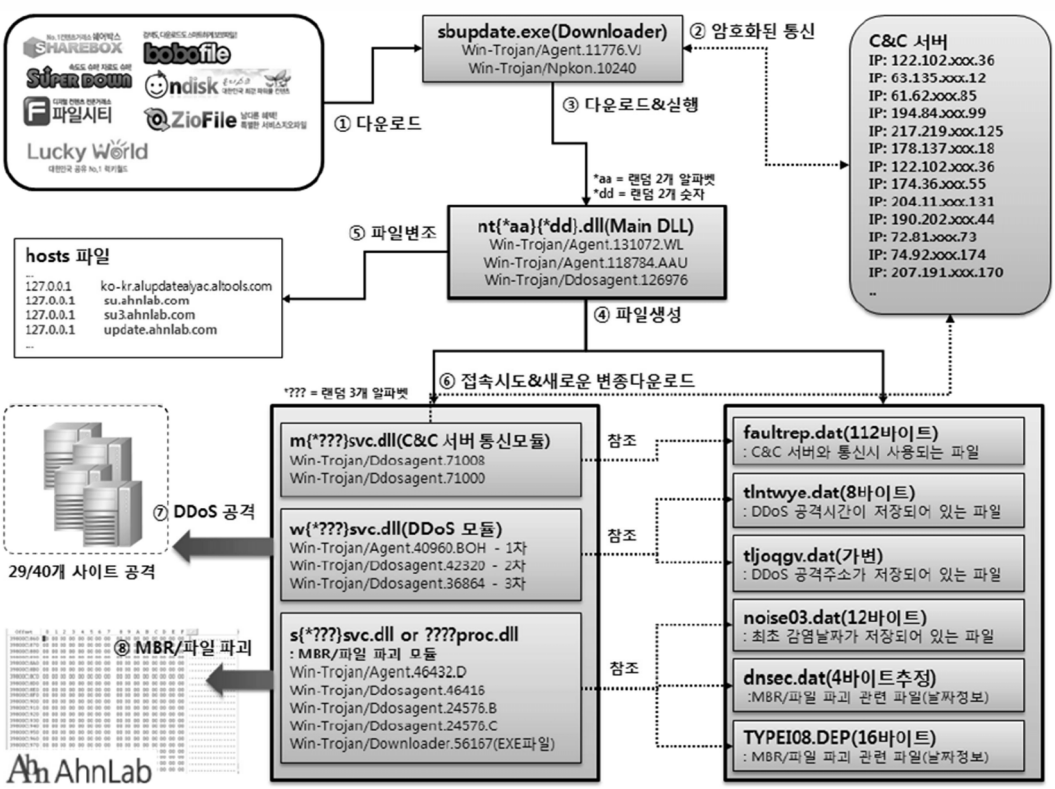
3. 주요 DDoS 공격 사고 분석

3.1 7.7 DDoS 공격과 3.4 DDoS 공격 분석

2009년 7월 4일 미국 주요 사이트들을 대상으로 공격이 시작되었으며 국내 최초공격은 7월 7일 오후 6~7시경 네이버메일 서비스에서 발견되었다. 이후 정부, 대기업 등을 중심으로 주요 대상으로 하여 7월 10일 자정까지 공격이 계속되었다. 악성코드는 명령 제어 서버로부터 공격목표를 전달받는 것이 아니라 감염 시 생성되는 공격목표 설정 파일



〈그림 2〉 7.7 DDoS 공격 흐름도



〈그림 3〉 3.4 DDoS 공격 흐름도[15]

을 기반으로 자동공격을 수행하였다[13].

2011년 3월 4일 오전 10시와 오후 6시 30분에 국내 다수의 웹사이트를 대상으로 DDoS 공격이 발생하였다. 7.7 DDoS 공격 때와 마찬가지로 DDoS 공격, C&C 통신, mbr 파일을 파괴하는 기능을 가지고 있다.

3.4 DDoS 공격은 과거 발생한 7.7 DDoS 공격에서와 같이 국내 웹 하드를 이용한 점을 비롯하여 DDoS 공격 대상 리스트를 비롯한 공격 시나리오들이 매우 유사하며 백신 업데이트 방해, 하드디스크 파괴 기능 강화 등 여러 문제점을 보완하였다. 다음의 <그림 3>은 3.4 DDoS 공격의 흐름을 나타낸다[14].

3.2 7.7 DDoS 공격과 3.4 DDoS 공격 차이점

3.4 DDoS 공격이 7.7 DDoS 공격과 비교하였을 때 두드러지게 나타나는 차이점은 공격하는 사이트가 늘어났다는 점과 치료를 방해할 목적으로 백신 업데이트 및 홈페이지 접근을 방해하는 기능을 추가했다는 것이다. 다음의 <표 1>는 7.7 DDoS 공격과 3.4 DDoS 공격의 차이점을 나타낸다[15].

3.4 DDoS 공격과 7.7 DDoS 공격간의 유사점 중 가장 큰 특징은 전반적인 공격 시나리오가 유사하다는 것이다. 이번 공격도 이전

처럼 공공기관을 대상으로 하였으며 공격이 끝나면 하드디스크를 파괴하는 특징을 가지고 있다. 그리고 해커들은 익명네트워크인 TOR를 사용하여 지령명령과 경유지에 접속하기도 한다[16].

〈표 1〉 7.7과 3.4 DDoS의 차이점[15]

구 분	7.7 DDoS 공격 (2009년 7월 7일)	3.4 DDoS 공격 (2011년 3월 4일)
공격 대상	청와대 등 국내 주요 사이트 23곳	청와대 등 정부 사이트, 네이버 등 국내 주요 국가 사이트 및 주한 미군 등 40곳
공격 시간	7~9일 3일 간 오후 6시에 다음날 6시까지	4일 오전 10시, 오후 6시 30분에 시작, 공격 종료 시점 불확실
대상	닷넷 프레임워크 기반 윈도우 2000/xp/2003	모든 윈도우 운영체제
파일 구성	같은 파일 구성으로 여러 차례 공격	공격에 따라 파일 구성이 달라짐
명령 변경	변경 없이 일관되게 진행	대응에 따라 명령을 변경함
치료 방해	없음	호스트 변조로 백신 업데이트 및 홈페이지 접근 방해
하드 디스크 손상 시점	마지막 DDoS 공격 날인 10일 자정 손상. 당시 백신을 설치하지 않은 PC는 시스템 날짜를 이전으로 바꿔야 했음	시스템 날짜를 감염 시각 이전으로 바꾸거나 감염 시각을 기록한 noise.dat 파일을 삭제할 경우 감염 후 7일 밤 9시경을 기해 즉시 손상되는 것으로 변경
좀비 PC 수	115,044대	77,207대
대응 방식	제대로 준비되지 않은 상태에서 대대적 혼란 야기	7.7 DDoS 이후 기업/기관의 준비가 있었고 보안 업체와 유관 기관과의 협조로 피해 최소화

4. 좀비 PC 탐지시스템의 구성 및 평가

4.1 좀비 PC 탐지시스템 수집 항목

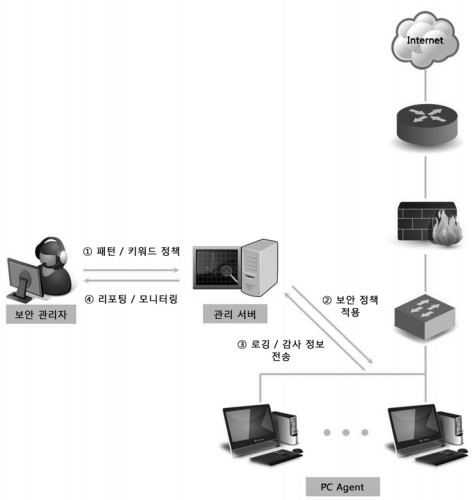
제안하는 호스트기반 좀비 PC 탐지시스템은 활성 포렌식 기술을 이용하여 총 5가지 항목에 대해 악성코드 정보수집을 시행한다.

첫째, Hosts 파일의 변조의 유무에 주목한다. Hosts 파일은 DNS서버가 구현되기 이전의 운영체제로부터 사용되던 것으로서 네트워크 상의 도메인 주소와 IP 주소의 매핑을 목적으로 한다. 현재는 대부분의 시스템에서 DNS 서버로부터의 정보와 이로부터 얻은 DNS캐시를 바탕으로 도메인 주소와 IP 주소를 매핑하기 때문에 Hosts 파일의 존재 이유는 이제 없어졌다고 볼 수 있다. 이러한 Hosts 파일은 공격자가 호스트를 의도된 사이트로의 리다이렉션 등의 방법으로 공격하는 취약점이 될 수 있다. 좀비 PC 탐지시스템에서는 정상적인 Hosts 파일의 MD5 해쉬값과 관제대상 PC의 해쉬값을 비교해서 Hosts 파일의 무결성 여부에 대한 검사를 실시하고 이상징후 발생 시 빠르게 대응한다. 둘째, ARP 캐시 테이블의 변조 유무에 주목한다. ARP 캐시 테이블은 통신을 하기 위한 ip 주소와 MAC 주소의 매핑을 위한 테이블 데이터를 담고 있는 캐시 데이터이다. 최근에는 교신을 하는 당사자들의 단말상의 ARP 캐시 테이블 정보를 공격자가 자신들의 MAC주소를 삽입, 변조해서 네트워크 상에서 교신되는 패킷을 스니핑 하거나 스푸핑해서 정보를 갈취하고 있다. 이로 인해 자신도 모르게 정보 침해 사고를 당하는 경우가 빈번해졌다. 위와 같은 arp 캐

시 테이블 변조 공격에 대응하기 위해 좀비 PC 탐지시스템에서는 평소 arp 캐시 테이블의 값을 수집하여 이상 징후 발생 시 빠르게 대응한다. 셋째, HTTP Header 내 User-Agent 값의 변조 여부에 주목한다. User-Agent 값은 PC가 서버 측에 PC의 시스템 버전, 웹브라우저 종류 등을 제공해서 상황에 맞는 서비스를 제공받기 위한 정보이다. 공격자는 User-Agent 값을 변조함으로써 좀비 PC의 개체수를 파악할 수 있고, 취약점을 가지고 있는 특정 버전의 브라우저를 사용하여 접속하는 사용자들을 악성코드에 감염시킬 수 있다. 공격자의 User-Agent 변조 공격에 대응하기 위해 좀비 PC 탐지시스템에서는 레지스트리에 6곳에 저장되어 있는 이 값을 추출하여 변조 여부를 감시하고 이상 징후 발생 시 빠르게 대응한다. 넷째, 호스트상의 네트워크 연결정보의 이상 징후 발생 여부에 주목한다. 네트워크 연결 정보는 netstat 콘솔 명령어 등으로 알 수 있다. 이때 기본 서비스 포트 이외에 의심스러운 포트가 listening 상태로 되어있을 수 있고 또는 established 상태의 연결 중 백그라운드 상에서 알 수 없는 특정 서버로 접속을 시도한 것이 있을 수도 있다. 제안하는 탐지시스템에서는 이러한 공격 징후를 사전에 정책으로 설정해 놓고 그 조건에 부합한다면 이상 징후 발생으로 인식하고 대응한다. 다섯째, 레지스트리 정보의 이상 징후 발생 여부에 주목한다. 윈도우 운영체제에 관련된 모든 데이터베이스는 레지스트리에 모인다. 이러한 레지스트리에 공격자가 임의의 수정을 통하여 단순히 사용자의 시스템을 운용불능의 상태로 만드는 등의 피해를 입힐 수 있고, 여기에 좀 더 지능적인 기법을 가미하면 PC를 보안상 더욱 취약하게 만들 수 있다. 좀비 PC 탐지시스템에서는 이러한 레지스트리를 악의로 변조하는 행위를 감지하고 신속하게 대응한다.

4.2 좀비 PC 탐지시스템 구성 및 설계

좀비 PC 탐지시스템은 아래의 그림과 같이 각종 정책을 설정하고 보안관제를 수행하는 관리 서버와 실질적인 보안 서비스를 수행하는 각 호스트의 Agent들로 구성된다. 보안관리자가 패턴/키워드 정책을 관리서버에 등록하게 되면 각 호스트의 Agent상에 보안정책이 적용이 되고 호스트의 Agent상으로부터 로깅/감사정보가 관리서버로 전송되게 된다. 이 정보를 보안관리자는 리포팅/모니터링 방식으로 실시간 확인 할 수 있다.



〈그림 4〉 좀비 PC 탐지시스템 구성도

좀비 PC 탐지시스템은 아래의 <표 2>와 같이 크게 4가지의 절차가 반복 순환한다. 보

안관리자가 탐지 패턴, 운용 정책 등을 설정하며, 관리 서버를 중심으로 각 PC Agent에 정책을 적용한다. 각 PC Agent에서는 관리 서버로 로깅/감사 정보를 전송하게 되며 보안관리자는 관리 서버로 모아진 각종 로깅/감사 정보를 모니터링하고 대응한다.

〈표 2〉 좀비 PC 탐지시스템 운영 절차

절차	설명
① 패턴/키워드 정책	보안관리자가 탐지 패턴, 운용 정책 등을 설정한다.
② 보안정책 적용	관리 서버를 중심으로 각 PC Agent에 정책을 적용한다.
③ 로깅/감사 정보	각 PC Agent에서는 관리 서버로 로깅/감사 정보를 전송한다.
④ 리포팅/모니터링	보안관리자는 관리 서버로 모아진 각종 로깅/감사 정보를 모니터링하고 대응한다.

서버사이드의 시스템 구성은 아래의 <그림 5>와 같다. 서버사이드 시스템은 PC Agent를 원격제어 할 수 있는 원격제어와 Agent를 설치 유도하여 관리하는 설치유도, 서버사이드 시스템을 관리하는 서버관리, 서버와 PC Agent를 연동 관리해 주는 연동관리, 특정 키워드 및 패턴을 통해 좀비 PC를 탐지할 수 있게 해 주는 키워드/패턴관리, 좀비 PC 탐지 시 알려주는 알림기능, 좀비 PC 탐지 시스템에서 발생하는 로그를 관리해 주는 로그 관리, 보안정책을 설정하고 관리해 주는 보안정책 관리, Agent 설정 및 Agent 업데이트 등을 관리 해 주는 관리 부문을 포함하여 총 9가지 부문으로 구성되어 있다.

클라이언트사이드의 시스템 구성은 아래의 <그림 6>과 같다. 클라이언트사이드 시스템은 특정 프로그램 실행을 제어 및 관리 해 주는 프로그램 실행 제어, Agent의 패치 및 버전을 관리해 주는 패치관리, 좀비 PC 감염여부를 사용자가 직접 확인 할 수 있는 사용자 UI, 사용자 및 허가 받지 않은 인가자의 Agent 무단 삭제를 방지하는 자체 보호, 암호화를 통해 서버사이드 시스템과 통신할 수 있게 해 주는 암호화, 시스템의 설정을 제어 해 주는 시스템 설정 제어, 패턴/키워드 검색이 가능하게 해 주는 내용기반 차단, 사고 발생 시 감사 자료로 활용 할 수 있는 감사로깅으로 총9개 부문으로 구성할 수 있다.

〈그림 5〉 서버사이드 시스템 구성도

〈그림 6〉 클라이언트사이드 시스템 구성도

4.3 좀비 PC 탐지시스템 분석 및 평가

좀비 PC 탐지를 위해 정보유출형 악성코드를 분석 및 적용하여 호스트에서 발생할 수 있는 다양한 정보유출형태를 탐지하는 실험을 연구한다.

아래 <표 3>는 정보유출형 악성코드 샘플 10종을 분석한 결과이다.

〈표 3〉 정보유출형 악성코드 샘플 파일 정보

	제작시간	유포 사이트	진단명
1	2012/05/02 13:48	194.183.224.73/out/svchost.exe	Poison Ivy
2	2012/04/30 16:15	188.40.168.128/e.exe	Zeus Trojan
3	2012/04/30 16:15	ryactive.com/media/video.avi.exe	Zeus Trojan
4	2012/04/24 08:32	manticore.cullhed.com/img/shadow.exe	Trojan Bebloh
5	2012/04/09 20:41	camrl.com/xCHZNdw.exe	Zeus Trojan
6	2012/03/02 16:33	www.gnnet.co.kr/fss/lsase.exe	Trojan
7	2011/12/24 09:40	thatsmytopper.com/upd.exe	Trojan
8	2011/12/04 03:00	privatetube.onlinetubes24.com/codec.exe	Trojan
9	2011/12/04 03:00	remix.onlinetubes24.com//applet.exe	Trojan
10	2011/11/25 13:40	signum-kzt.ru/img/Flash/postcard.exe	IRC Backdoor

제안하는 탐지시스템에 정보유출 악성코드 샘플 10종에 적용하여 각 항목에 대한 실험을 하여 이에 대한 적용 및 결과에 대해 설명한다. 탐지시스템에 관련된 기존 침입차단시스템과 침입탐지시스템을 본 논문에서 제안한 탐지시스템의 특징을 비교 분석하고 성능을 평가한다. 단, 실험시 제약사항으로 기존 알려진 정보유출형 악성코드 샘플 10종으로 평가를 진행하였으며, 2가지 실험 시스템과 제안하는 탐지시스템 모델간의 성격과 다소 차이가 있음을 알린다.

〈표 4〉 3가지 탐지시스템 성능 실험 평가

순서	악성코드 실행파일명	침입차단 시스템		침입탐지 시스템		제안하는 탐지 시스템	
		탐지	차단	탐지	차단	탐지	차단
1	svchost.exe	X	X	O	X	O	O
2	e.exe	X	X	O	X	O	O
3	video.avi.exe	X	X	X	X	X	X
4	shadow.exe	X	X	O	X	O	O
5	xCHZNdw.exe	X	X	O	X	O	O
6	lsase.exe	X	X	O	X	O	O
7	upd.exe	X	X	O	X	O	O
8	codec.exe	X	X	O	X	O	O
9	applet.exe	X	X	O	X	O	O
10	postcard.exe	X	X	X	X	O	O

위 <표 4>를 기반으로 성능 측정을 위하여 악성코드 탐지율(DR, Detection Rate)을 구하였다.

$$DR = \frac{\sum_{i=1}^{n} P_i}{\sum_{i=1}^{n} N_i} \quad (1)$$

수식 (1)에서 I는 악성코드의 개수, P는 각 측정된 항목을 의미한다.

이를 통해 아래 <표 5>와 같이 각 기능성과 성능평가를 진행하였으며, 탐지율과 검증단계에 대한 비교 분석 결과를 도출 할 수 있었다.

본 실험을 통해 침입차단시스템과 침입탐지시스템을 비교해 보면 제안하는 보안관제 시스템과 차이를 확인할 수 있다. 침임차단시스템은 탐지기능은 전혀 없으며 포트기반으로 차단만 하기 때문에 악성코드 샘플을 모두 탐지 및 차단하지 못하였다. 또한, 기존 침입탐지시스템은 알려진 악성코드 시그니처를 스노트 기반으로 탐지정책이 주입되어 있기 때문에 새로운 악성코드나 탐지정책에 없는 시그니처가 있다면 탐지가 불가능 하다.

또한 침입탐지시스템은 탐지만 하고 차단을 할 수 없는 구조적인 문제가 있다.

본 연구에서 제안하는 보안관제스템은 악성코드 감염시 행위기반으로 탐지하기 때문에 대부분 악성코드를 감지하고 감지된 PC는 사용을 중단시키는 정책을 사용하므로 정보유출을 사전에 차단할 수 있다. 또한, 샘플 악성코드 중에 1개 악성코드는 자가 삭제 기능을 가지고 있어 탐지 및 차단하기 어려운 부분이 있었으나, 90% 이상 탐지 및 차단되어 다른 탐지시스템보다 더 좋은 결과를 얻을 수 있었다. 따라서 본 논문에서 제안하는 탐지시스템을 활용하여 정보유출형 악성코드 탐지 및 사전 차단까지 할 수 있었다.

5. 결 론

본 논문에서 제안한 탐지시스템 모델을 통해 인식이 낮았던 호스트 기반의 보안관제 개념을 정립하고 기존의 기업들도 자사의 시스템에 이러한 개념을 구축, 운용하여 다수의 좀비 PC를 이용한 공격의 위협에 대한 근본적인 해법을 제시하고 추후에 생길 수 있는 다른 호스트 기반의 취약점에 대해 예방을 할 수 있을 것이다. 정보화 사회에서의 사이버 공격은 이제 간과할 대상이 아닌 무기를 사용한 실제 전쟁과 동등하게 취급하고 신속하게 대응해야 한다. 본 논문에서 제시한 탐

〈표 5〉 각 탐지시스템 비교지표 분석 결과

비교지표 \ 진단시스템		침입차단시스템	침입탐지시스템	제안하는 탐지시스템
기능성	호환성	네트워크 전용	네트워크, 호스트 선택 가능	호스트 전용
	점검기능	포트위주의 차단정책	해킹, 악성코드 탐지정책	PC에서 악성코드 행위기반 탐지
	진단방식	기본 포트 차단	시그니처 기반	행위기반 점검
신뢰성	점검속도	1초(1개 진단시)	3초(1개 진단시)	14초(1개 진단시)
	탐지율	0%	45%	90%
	검증단계	1단계	1단계	5단계

지시스템 모델을 통해 7.7, 3.4 DDoS 사이버 공격 위협을 예방하고 사회적 불안 요소와 경제적 비용 손실을 해결함으로써 국가 경쟁력을 강화할 수 있을 것으로 기대한다.

참 고 문 헌

[1] 장영준, 차민석, 정진성, 조시행, “악성코드 동향과 그 미래 전망”, 한국정보보호학회, 제18권, 제3호, pp. 1-16, 2008.

[2] 안철수 연구소, “DDoS 공격 동향과 전망”, 월간 安, pp. 4-15, 2011.

[3] 정석화, “DDoS 범죄 수법 및 대응방안”, 경찰청 사이버 테러대응센터, 2011.

[4] 이창훈, “공격 형태와 기술적 특징 분석 및 효율적 대응방안”, 한국CSO협회포럼, 2011.

[5] 양대일, “정보보안개론”, 한빛미디어, 2009.

[6] 서상욱, “Detection and Protection of DoS/DDoS Attacks in WiBro System”, 한국정보통신대학교, 2009.

[7] 선재훈, “효과적인 DRDoS 공격 차단을 위한 LA-BGP 기법 연구”, 경기대학교 박사학위논문, 2010.

[8] 하재철, 김환구, 오수현, “네트워크 보안”, 미래컴, 2008.

[9] 서동현, “DDoS 공격의 방어를 위한 효율적인 동적패킷 필터링”, 아주대학교 석사학위논문, 2009.

[10] 정순홍, “사이버위협 위험도 판정을 통한 정보보호활동 우선순위 결정에 관한 연구”, 고려대학교 석사학위논문, 2010.

[11] 오자영, “보안관제서비스란 무엇인가?”, 보안뉴스, 2006. 12. 25.

[12] 이창훈, “사용자행위분석 통한 능동적 방어체계가 해답”, 보안뉴스, 2011. 3. 23.

[13] A3Security, “7.7 DDoS 분석”, 2009.

[14] 이스트소프트 알약보안대응, DB 분석팀, “3.3 DDoS 악성코드에 대한 분석 보고서”, 2011.

[15] 안철수 연구소, “3.4 DDoS 분석보고서”, 2011.

[16] 박광철, 박원형, 임종인, “GEOIP를 이용한 익명 네트워크에서 통신 속도 향상을 위한 성능 개선에 관한 연구”, 한국전자거래학회, 제16권, 제4호, 2011.

저 자 소 개

홍준석 (E-mail : jun0817@kaits.or.kr)
2012년 성균관대학교 정보통신대학원 정보보호전공 (공학석사)
현재 한국산업보안기술협회 중소기업지킴센터 보안관제팀장
관심분야 보안관제정책, 침해사고대응, 보안취약점분석

니오박 (E-mail : neopark@kdu.ac.kr)
2002년 건국대학교 토목공학과 학사
2008년 미국 유타주립대학교 컴퓨터사이언스학과
2nd B.S. coursework
2010년 미국 유타주립대학교 컴퓨터사이언스 대학원 M.S
현재 극동대학교 유비쿼터스학과 전임교수/정보관리처장
관심분야 융합보안, 보안프로그래밍, 네트워크보안

박원형 (E-mail : whpark@kdu.ac.kr)
2002년 서울과학기술대학교 산업정보시스템공학과 (공학사)
2005년 서울과학기술대학교 정보산업공학과 (공학석사)
2009년 경기대학교 정보보호학과 (이학박사)
2011년 서울과학기술대학교 산업정보시스템공학과 겸임교수
현재 극동대학교 정보경영학과 전임교수
관심분야 보안관제기술, 윈도우포렌식, 산업보안