NAC 의 post-connect에서 행위정보를 사용한 악성코드 감염 호스트 탐지 시스템

한명묵† · 선종현††

요 약

NAC(Network Access Control)는 운영체제 보안 패치 미 적용 혹은 AV(Anti-Virus)미설치 컴퓨터 등 웜의 공격대상이 되어 내부망에 바이러스를 유포하는 엔드 포인트 사용자 보안에 대한 솔루션으로 개발되었다. 현재 시장에 상용화된 NAC 제품들이 경우 연결 전 보안기능(pre-connect)기술들은 많이 발전되어 있으나, 정상적인 인증을 통해 연결된 이후에 발생하는 위협을 탐지하는 위협 관리 기능(post-connect)이 대체적으로 부족한 상태이며, 이에 따라 Zero-day 공격, 악성코드 감염 등으로 NAC 사용자들이 지속적으로 피해를 입고 있는 상황이다.

본 논문에서는 이러한 post-connect단계에서의 문제점을 해결하고자 기존에 사용되던 단말에 대한 인증과 정책 위반 여부 검사 외에 각 단말이 발생시키는 트래픽 정보와 Agent를 통해 획득한 각 단말의 정보, 그리고 Network Scanner에서 획득한 Open Port와 네트워크 구성 변경 정보를 활용하여 정상 Behavior profile을 생성하고 이를 기반으로 악성코드 감염 시스템을 탐지하는 시스템을 제안한다.

주제어 : NAC, post-connect, malware, behavior profile

The Detection System for Hosts infected Malware through Behavior information of NAC post-connect

Myung-Mook Han† · Jong-Hyun Sun††

ABSTRACT

NAC(Network Access Control) has been developed as a solution for the security of end-point user, to be a target computer of worm attack which does not use security patch of OS and install Anti-Virus, which spreads the viruses in the Intra-net. Currently the NAC products in market have a sufficient technology of pre-connect, but insufficient one of post-connect which detects the threats after the connect through regular authentication. Therefore NAC users have been suffered from Zero-day attacks and malware infection. In this paper, to solve the problems in the post-connect step we generate the normal behavior profiles using the traffic information of each host, host information through agent, information of open port and network configuration modification through network scanner addition to authentication of host and inspection of policy violation used before. Based on these we propose the system to detect the hosts infected malware.

Keywords : NAC, Post-connect, Malware, Behavior profile

† 정 회 원: 경원대학교 IT대학 컴퓨터공학과 부교수
†† 정 회 원: 경원대학교 일반대학원 전자계산학과
논문접수: 2010년 10월 11일, 심사완료: 2010년 11월 16일
* 이 연구는 2010년도 경원대학교 지원에 의한 결과임.

1. 서 론

네트워크 접근제어(Network Access Control : NAC) 시스템은 내부 네크워크에 접근하는 단말기의 인가 여부, 단말기의 안정성 여부, 단말기의 규정 준수 여부에 따라 네트워크 접속 허가, 네트워크 격리, 치료 기능 등을 제공해 주는 시스템이며, 네트워크 보안과 사용자단의 보안을 해결할 수 있는 차세대 통합 보안 패러다임으로 각광받고 있는 기술이다. NAC는 크게 2가지 단계로 나눌 수 있는데, NAC가 사용자 접속을 허가·통제하기 위해 먼저 사용자의 단말기가 인가된 장치인지, 사용자 PC에 기업의 보안정책이 제대로 구현되어 있는지 확인하게 된다. 예를 들어 PC에 보안패치나 안티바이러스가 제대로 깔려 있는지, 패치는 항상 최신 업데이트를 유지하는지, 방화벽이 설치되어 있는지 등을 접속 이전에 점검하게 된다. 이러한 단말에 대한 인증을 수행하는 단계를 pre-connect 단계라고 하며, 인증을 과정 후 네트워크에 접속한 단말들의 트래픽을 모니터링하여 정책에 위배되는 통신 또는 유해 트래픽을 발생시키거나 허용하지 않는 프로그램이 설치되는 등 정책을 위반하는 단말을 격리하는 작업을 수행하는 단계를 post-connect 단계라고 한다.

현재 시장에 상용화된 NAC 제품들의 연결 전 보안기능(pre-connect) 기술들은 많이 발전되어 있으나, 정상적인 인증을 통해 연결된 이후에 발생하는 위협을 탐지하는 위협 관리 기능(post-connect)이 대체적으로 부족한 상태이며, 이에 따라 Zero-day 공격, 악성 코드 감염 등으로 인해 기업들이 지속적으로 피해를 입고 있는 상황이다. 특히, 악성 코드는 웜, 바이러스, 트로이목마, 백도어와 같은 공격을 포함하는 공격으로서 사용자의 의사와 이익에 반해 시스템을 파괴하거나 정보를 유출하는 등 악의적 활동을 수행하도록 의도적으로 제작된 소프트웨어를 말하는데, 이로 인해 개인정보가 유출되거나 DDoS공격을 수행하여 대역폭, 프로세스 처리 능력 및 시스템 자원을 고갈시킴으로써 정상적인 서비스를 제공하지 못하게 만드는 등 다양한 공격을 수행하게 된다. 이런 악성코드에 의해 내부망이 단말기가 감염된 경우, 자기 복제 및 네트워크 스캐닝을 통해 주변 단말기들을 파악한 후 악성코드를 전파해 나가기 때문에 네트워크 전체가 감염에 노출될 수 있다.

이 논문에서는 이러한 NAC의 post-connect단계에서의 효과적인 위협 관리 기능을 제공하기 위해 각 호스트들의 행위정보들을 사용하여 악성코드에 감염된 호스트를 탐지해 내는 방법을 제안한다.

2. 관련 연구

2.1 Nmap

엔맵(Nmap : 네트워크 매퍼)은 네트워크 조사와 보안 감사를 위한 무료 오픈소스 유틸리티다. 엔맵은 어떤 호스트가 네트워크에서 사용 가능하며, 그런 호스트가 어떤 서비스(애플리케이션 이름과 버전)를 제공하는지. 그런 호스트가 어떤 운영체제(그리고 운영체제 버전)를 운영하는지, 어떤 종류의 패킷 필터/방화벽이 사용되는지 등 수십 개의 특성을 결정하기 위한 새로운 방법으로 로우 IP 패킷을 사용한다. 엔맵은 거대한 네트워크를 재빨리 스캔하려고 설계됐지만 싱글 호스트 대상으로도 잘 동작한다[1][2].

2.2 트래픽 분석

트래픽의 모니터링을 통해 네트워크 내부의 트래픽 상태를 분석할 수 있는 방법은 크게 2가지 방법이 있다. 그중 한가지 방법은 네트워크 트래픽 모니터링을 위해 네트워크를 지나다니는 모든 패킷들을 미러링해서 네트워크 상태를 알아내는 패시브 모니터링 방법이다.

다른 한가지 방법은 네트워크 장비의 Flow Exporting 기능을 이용한 트래픽 정보 분석 방법이 있다. 네트워크 장비가 플로우(Flow)정보를 생성해야 하는 부담이 있어 고속 네트워크에서의 사용은 제한적이지만 네트워크 장비가 플로우 생성을 해주무로 트래픽 모니터링 시스템의 구조가 간단해 질 수 있다는 장점이 있다. 현재 많이 쓰이는 Flow exporting 방법은 CISCO의 Netflow가 산업체 표준으로 자리잡고 있고 플로우를 그래픽으로 표현하여 네트워크 상태를 분석하는 툴인 Flowscan등이 대표적이다[3].

본 논문에서는 통신사업자 같은 대형 네트워크

망이 아닌 중, 소형 네트워크 망을 대상으로 보다 효과적인 트래픽 정보를 수집하기 위해 미러링 방법을 사용하여 트래픽을 수집한 후 이를 재가공하는 방법을 사용했다.

2.3 Rule을 바탕으로 한 연관성 분석 방법

효과적인 이벤트들의 요약과 복잡한 패턴의 인식을 모적으로 연구되고 있는 방법으로 Stanford에서 개발한 Context 바탕의 이벤트 프로세싱이 있다. Rule을 바탕으로 한 연관성 분석 방법은 대규모 네트워크 침입을 초기에 탐지하고 대응시간을 줄일 수 있다는 장점이 있지만 많은 침입 시나리오 Rule과 조건이 설정되어야 한다는 단점이 있다. Stanford의 Context 바탕의 연관성 분석방법은 각 침입 시나리오에 따라 추상화된 모델을 생성한다. 시스템으로부터 보고되는 각 이벤트들을 추상화된 모델로 매칭시켜 침입을 탐지한다. 각 이벤트를 표현하는 방법으로 전달된 이벤트를 이벤트들 간의 시간관계와 인과관계에 의해 "if condition then statement"형태의 룰(rule)에 의해 처리한다[4][5].

3. 악성코드 감염 호스트 탐지 시스템

3.1 호스트 분석을 위한 요구 사항

본 논문에서 제안한 악성코드 감염 호스트 탐지 시스템이 갖추어야 할 조건은 다음과 같다.

첫째, 각 호스트들의 자원 정보를 여러 단위 시간 별로 나타낼 수 있어야 한다. 실시간의 5분 단위 정보를 토대로 시, 일, 주 단위의 누적된 정보를 통해 해당 호스트의 자원 사용에 대한 Behavior profile을 생성 및 해당 호스트의 패턴을 파악할 수 있다[11].

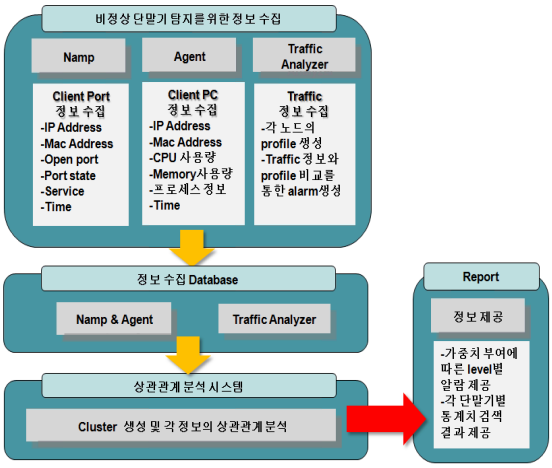
둘째, 각 호스트의 트래픽 정보를 여러 단위 시간별로 나타낼 수 있어야 한다. 실시간의 5분 단위 정보를 토대로 시, 일, 주 단위의 누적된 정보를 통해 해당 호스트의 트래픽 정보에 대한 Behavior profile을 생성 및 해당 호스트의 패턴을 파악할 수 있다.

셋째, 각 호스트의 Open port 정보 및 네트워크 구성 정보를 여러 단위 시간별로 탐지할 수 있어야 한다. 실시간의 5분 단위 정보를 토대로 시, 일, 주 단위의 누적된 정보를 통해 해당 호스트의 트래픽 정보에 대한 Behavior profile을 생성 및 해당 호스트의 패턴을 파악할 수 있다.

넷째, 비슷한 행동을 하는 호스트끼리 혹은 같은 일을 수행하는 부서끼리 그룹을 생성하여 그룹의 Behavior profile을 생성해야 한다. 앞에서 생성된 개인 Behavior profile을 통해 그룹 Behavior profile이 생성되며, 개인 Behavior profile과 그룹 Behavior profile을 통해 정상/비정상 여부를 판단할 수 있다. 또한 비정상으로 판단된 호스트들에 대해 각 이벤트들의 상관관계 분석을 통해 악성코드 감염 여부를 판단할 수 있어야 한다.

다섯째, 과거의 정보들을 확인할 수 있어야 한다. 모니터링 시스템의 사용자가 실시간 정보들을 계속해서 지켜볼 수는 없으므로, 특정 시점의 트래픽 현황을 파악하기 위해서 과거의 정보들을 저장해 놓아야 한다.

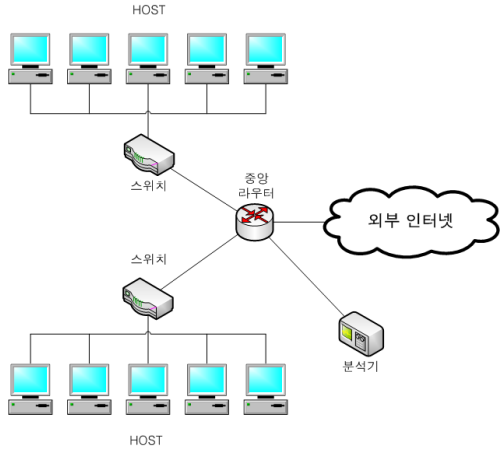
3.2 시스템 전체 구조



<그림 1> 전체 구성도

그림 1은 탐지 시스템의 구조를 보여준다. 본 시스템은 비정상 호스트를 탐지하기 위해 Nmap을 통해 Open port 정보와 인가되지 않은 채 네트워크에 접속한 노드를 탐지하기 위해 네트워크 구성 정보 변경 여부를 검사한다. 또한 각 호스트에 Agent를 설치하여 해당 호스트의 IP, MAC, CPU 사용량, Memory 사용량, 프로세스 정보, 시

간 정보와 같은 정보를 수집하게 된다.



<그림 2> 트래픽 분석기(AD 센서) 구조도

그림 2는 비정상 호스트를 탐지하기 위해 각 호스트들의 트래픽 정보를 수집하여 분석하는 분석기이다. 이러한 트래픽 분석기는 내부 네트워크의 비정상 트래픽을 탐지해야 하기 때문에 각 단위 네트워크의 스위치에 연결하여 트래픽 미러링을 통해 분석이 이루어지게 된다. 본 트래픽 분석기에서는 단순히 트래픽의 양뿐만 아니라 input/output 비율, 프로토콜별 사용 비율, 교환된 패킷의 평균 길이 등 미러링된 트래픽을 한차례 더 가공하여 정보수집 Database에 전달하게 된다.

정보수집 Database는 매 5분마다 3개의 파트에서 정보를 수집하게 된다. 5분으로 주기를 설정한 이유는 실시간 처리를 수행할 경우 부하가 크게 걸리기 때문이며, 일반적으로 웜과 같은 악성코드의 경우 10분 내외의 활동시간을 가지기 때문이다.

3.3 분석 시스템

분석 시스템에서는 정보수집 Database에서 수집된 정보를 바탕으로 각 호스트들에 대한 정상 profile을 생성하는 작업과, 이를 바탕으로 비정상 이벤트를 발생시키는 작업, 그리고 마지막으로 이러한 비정상 이벤트들간의 상관관계를 분석하여 악성코드 감염 여부를 판단하는 작업을 수행하게 된다.

우선, 정상 profile을 생성하는 부분부터 살펴보면 정상 profile은 호스트별 개인 profile과 해당 호스트가 속한 그룹 profile 2가지가 존재하게 된다. 개인 profile의 경우 호스트의 트래픽 정보, 자원 사용 정보, Open port 3종류로 나뉘게 되는데, 트래픽 profile의 경우 아래 표 1과 같은 feature들을 사용한다[6].

<표 1> 개인 트래픽 profile 생성에 사용된 feature

feature	내용
f_1	input/output 비율
f_2	프로토콜 사용 비율
f_3	교환된 패킷의 평균 길이
f_4	호스트 생성 트래픽 양

이러한 feature들은 이미 트래픽 분석기에서 가공되어 저장이 되며, 분석기에서는 이러한 각 feature들에 대해 누적된 데이터들을 통해 평균과 표준편차를 구하여 둘을 합하여 개인 profile을 생성하게 된다. 또한 profile 생성 시 악성코드에 감염된 호스트를 보다 효과적으로 찾기 위해 악성코드에 자주 사용되는 포트에 대한 profile과 전체 트래픽에 대한 profile을 따로 생성하게 된다. 이때 사용되는 포트는 표 2와 같다. 또한 시간 j당 호스트 i의 profile 생성은 다음 식 1과 같다.

$$Profile_i(j) = a_j + \sigma_j \quad \text{----------(1)}$$

자원사용 양과 Open port의 경우도 위 식 1을 따라 profile이 생성되게 된다.

<표 2> 개인 profile 생성에 사용되는 포트

포트 번호	서비스
21	FTP 포트
22	ssh 원격 로그인 포트
25	SMTP 포트(e-mail)
80	웹 접속용 서비스

그룹 profile의 경우 가장 중요한 것은 어떻게 호스트들을 Grouping 하느냐이다. 우리가 대상으로 하는 것은 NAC가 설치된 기업이나, 학교와

같은 단체의 네트워크에 대한 탐지이기 때문에, NAC 인증 과정 중 각 호스트들의 위치정보 혹은 부서나 해당 단말 타입과 같은 정보를 획득할 수 있다. 일반적으로 같은 부서의 경우 업무시간이나 업무의 유형이 비슷하기 때문에 그룹 설정 시 각 부서와 단말 타입(서버 타입, client)으로 그룹을 설정하였다. 또한 그룹 profile의 사용에 있어서 가장 중요한 점은 다양한 type의 정상 사용자들의 profile이 생성될 수 있다는 것이다. 이러한 점을 살리기 위해 그룹 profile 생성 시 아래 식 2와 같이 그룹에 속한 호스트의 profile 중 단위 시간당 가장 큰 값을 뽑아 그룹 profile을 생성함으로서 개인 profile만을 사용했을 시 발생할 수 있는 오경보를 줄일 수 있다.

$$\mathrm{P}rofile_i(j) = \forall m \in g\ MAX(\mathrm{P}rofile_m(j)) \text{ -(2)}$$

개인 profile 생성과 동일하게 특정 포트(표 2)와 전체 트래픽에 대한 profile 생성과 각 그룹에 속한 호스트들의 자원 사용 량에 대한 profile 그리고 네트워크 구성 정보 변경과 Open port에 대한 profile을 생성하게 된다. 이렇게 생성된 개인과 그룹 profile들을 사용하여 호스트들의 각 시간별 값과의 비교를 통해 비정상 호스트에 대해 이벤트를 발생시키게 된다.

악성코드 감염 여부를 판단하기 위해 분석 시스템은 각각의 호스트들에서 발생된 이벤트들을 수집하여 그들 간의 상관관계를 분석하게 된다. 상관관계 분석에는 Rule을 바탕으로 한 연관성 분석 방법을 사용하게 되는데, 이는 효과적인 이벤트들의 요약과 복잡한 패턴의 인식을 목적으로 연구되고 있는 방법으로, 대규모 네트워크 침입을 초기에 탐지하고 대응 시간을 줄일 수 있는 장점을 가지고 있다. PC Agent 와 Network Scanner, 트래픽 분석기에서 오는 정보들에 의해 발생된 이벤트들의 시간관계와 인과관계에 대해 정의를 하여 해당 정의에 해당하는 연속적인 이벤트가 발생할 경우 각각의 정의(룰)에 맞는 경보를 발생시킨다. 일반적으로 악성코드에 감염된 경우 대부분 일련의 과정을 거쳐 동작하게 된다. 최초 감염 시 해당 호스트에서는 파일을 생성하게 되고, 생성된 파일은 실행 되도록 컴퓨터의 레지스트리나 서비스에 등록되게 된다. 등록된 후에는 프로세스나 쓰레드, DLL Injection 등을 통해 동작하게 되며 네트워크를 통해 전파되기 위해 포트를 오픈하거나 특정 도메인 혹은 포트에 접속을 하게 된다. 그 후 보안기능 비활성화나 계정 정보 탈취와 같은 악성행위를 수행하는 것이 일반적인 악성코드에 감염된 호스트가 보이는 행동들이다. 이러한 이벤트들에 대해 시간 관계나 인과관계를 적용시켜 PC Agent, Network Scanner, 트래픽 분석기에서 취득한 정보를 바탕으로 분석 시스템에서 가중치를 부여하게 된다[4][5][7][8].

<표 3> 연관성 분석을 통한 위험도 부여 조건

위험도	내용
1	트래픽 이벤트가 발생하였을 경우 발생되는 경보
2	트래픽 이벤트가 발생하였으며, 해당 호스트로부터 Agent의 경보가 발생한 경우 발생되는 경보
3	트래픽 이벤트가 발생하였으며, 해당 호스트로부터 Agent 경보와 Open port 경보가 모두 발생 하였을 경우 발생되는 경보
4-1	트래픽 이벤트 중 생성 트래픽 양이 기존의 그룹 Profile보다 200%를 넘는 경우 발생되는 경보
4-2	보안 관련 프로세스가 kill된 경우 발생되는 경보
4-3	특정 port에서 이벤트 경보가 발생한 경우 발생되는 경보
4-4	프로토콜 비율 이벤트가 발생한 경우 발생되는 경보

이러한 Rule을 바탕으로 한 연관성 분석 방법은 많은 침입 시나리오 Rule과 조건 설정을 통해 정확도를 올릴 수 있다.

4. 시스템 구현 및 실험 결과

4.1 시스템 구현

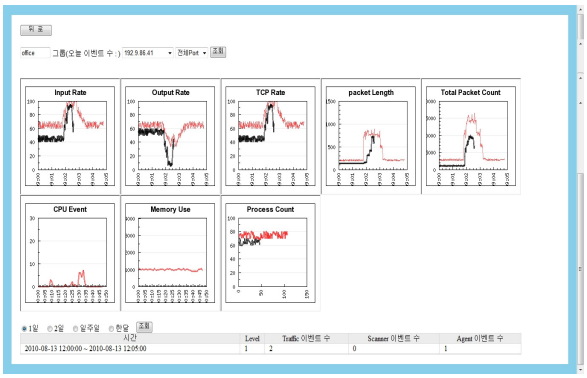
<표 4> 시스템 개발 환경

OS	Window 7
Web Server	Apache 2.2.3
Language	C#, PHP5
DB	MySql
Tool	Nmap

본 시스템의 개발 환경은 표 3과 같다. 윈도우 환경에서 Apache 웹서버를 사용하였고, DB는 Mysql을 사용하였다. 관리자용 웹 페이지는 PHP를 통해 구현하였고, 나머지 모듈들은 C#을 이용하여 구현하였다.

첫 화면은 다음과 같다. 기본적으로 각 그룹과 그에 해당하는 노드 수, 노드 상태, 인가 여부등을 알 수 있다.

<그림 3> 관리자 페이지의 main UI

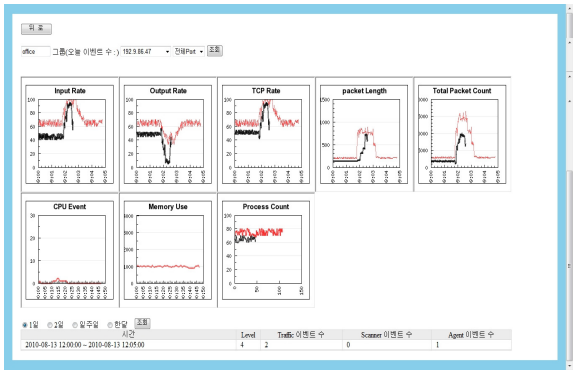


<그림 4> 관리자 페이지의 UI

각 그룹별 호스트들에 대한 input/output 비율과 TCP 비율, 패킷 길이, 패킷 량, CPU 사용 양, 메모리 사용 양, 사용되는 프로세스 양에 대한 모니터링을 제공하며 각 단위 시간별 발생된 이벤트들을 볼 수 있다. 또한 21, 22, 25, 80번 포트와 전체 트래픽에 대한 모니터링을 따로 제공하며, 1일, 2일, 일주일, 월 별로 과거 이벤트 정보에 대한 열람이 가능하다.

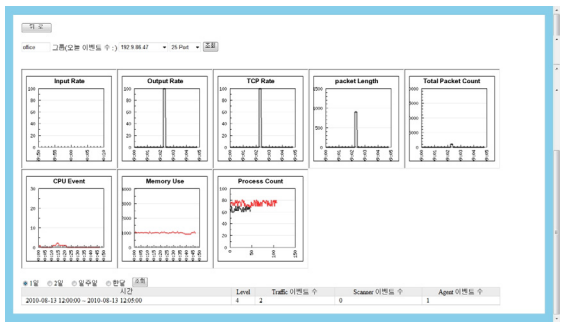
4.2 실험 및 분석

본 절에서는 논문에서 제시한 시스템을 학교 네트워크에 적용하여 특정 호스트에 대해 악성코드에 감염된것과 같은 환경을 조성하여 이를 탐지하는 실험을 수행하였다[9][10].



<그림 5> 악성코드에 감염된 행정실 노드의 전체 트래픽 정보

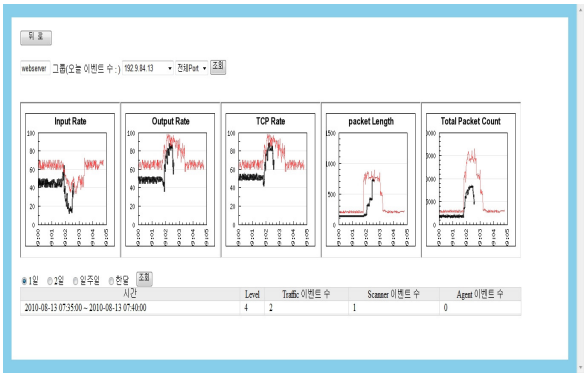
위 그림 5는 스팸메일을 발송시키는 악성코드(MyDoom.A)에 감염된것과 동일한 행동을 하도록 만들어진 호스트의 트래픽, 호스트 자원 사용양 정보와 발생된 이벤트를 보여주고 있다. 붉은색 선이 그룹 profile이며 검은색 선이 오늘 트래픽 정보를 나타내고 있다. 그림에서 볼 수 있듯이 트래픽 정보에서 눈에 띄는 점은 살펴볼 수 없다. 이는 MyDoom.A에 감염된 경우 1초당 0.15개의 메일을 SMTP를 통해 발송하기 때문에 업무시간 중에 작동할 경우 다른 트래픽 정보에 묻혀 단순히 트래픽의 양적인 변동이나 자원 양의 변화만으로는 탐지하기 힘들다. 아래 그림 6은 같은 호



<그림 6> 악성코드에 감염된 행정실 호스트의 25번 포트

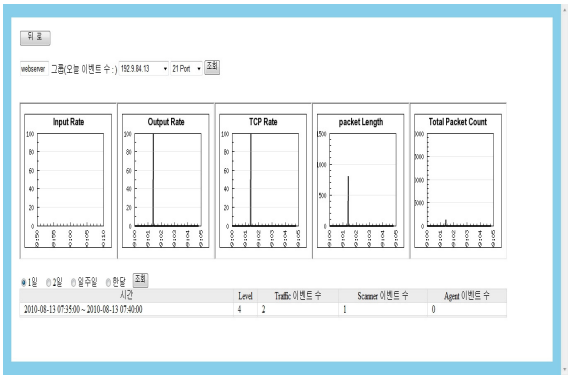
스트의 25번 포트의 트래픽 정보를 나타내고 있는데, 오전 12시쯤 output 비율과 TCP 비율이 급격히 증가하는 것을 볼 수 있다. 해당 호스트의 경우 일반적인 행정업무를 중심으로 수행하는 그룹이기 때문에 메일의 발송이 한정적이며, 학교에서는 25번 포트를 사용하지 않기 때문에 이러한

양적인 변화를 탐지를 통해 이벤트를 발생하게 된다. 분석 시스템에서는 이러한 특정 포트에 대해 가중치를 부여하게 되며 이는 관리자 UI아래에 위치하고 있는 이벤트 창에 나타나게 되어 관리자는 이를 통해 공격을 탐지하게 된다. 이와 같이 주요 포트에 대한 통계 정보를 따로 제공함으로서 보다 효과적으로 악성코드 감염 호스트를 탐지할 수 있다.



<그림 7> 악성코드에 감염된 서버의 전체 트래픽

위 그림 7은 웹 쉘에 감염된 서버의 트래픽 정보를 나타내고 있다. 웹 쉘 공격은 게시판이나 자료실과 같은 파일 첨부하는 기능을 포함한 웹 서비스 제공 서버에 악의적으로 제작된 스크립트 파일을 업로드하여 해킹하는 공격인데, 이러한 공격을 통해 서버 내 자료 유출이나 백도어 프로그램 설치 등 다양한 공격을 수행한다. 그림 7을 살펴보면 전체 트래픽 정보에서는 큰 문제점을 찾을 수 없다. 그러나 이벤트 창을 살펴보면 위험 레벨 4 이벤트가 발생한 것을 알 수 있다. 이벤트 내용을 살펴보면 Open port에 대한 이벤트와 트래픽 관련 이벤트가 다수 발생한 것을 알 수 있다.



<그림 8> 악성코드에 감염된 서버의 21번 포트

이러한 이벤트 정보를 바탕으로 21번 포트 트래픽 정보를 살펴보면 오전 7시 40분에 웹 서버에서는 사용하지 않는 21번 포트가 Open되어 이를 통해 파일 전송이 이루어진 것을 알 수 있다. 이러한 정보들을 통해 관리자는 해당 서버가 악성코드에 감염되어 정보가 유출되었다는 사실을 알 수 있다.

앞에서 살펴본 바와 같이 본 시스템을 통해 악성코드 감염 시스템을 탐지할 수 있었다. 또한 Bagle과 같은 메일형 웜이나 그 변종들에 대한 탐지와 보안 관련 프로세스 종료를 수행하는 봇형 악성코드에 대한 탐지도 가능하였다.

5. 결 론

본 논문에서는 네트워크 내 악성코드 감염 시스템을 탐지하는 시스템을 제안하였다. 제안된 시스템은 호스트의 자원 사용과 프로세스 탐지, 그리고 Open port와 네트워크 구성 변경 탐지, 네트워크 트래픽 분석을 통해 메일형 웜이나 보안 관련 프로세스 종료를 수행하는 악성코드들과 같이 트래픽 양이나 호스트에 직접적인 변화를 주는 악성코드 탐지가 가능하며 이를 실시간으로 관리자에게 알림으로서 빠른 대처가 가능하도록 하였다. 또한 시그니쳐 기반이 아니기 때문에 동일한 패턴을 보이는 신종, 변종 악성코드에 대한 탐지가 가능하다는 장점을 가지고 있다. 오탐지를 줄이기 위해 NAC의 그룹 정보를 바탕으로 호스트들을 묶어 다양한 정상 profile을 통해 탐지를 수행하였다. 또한 트래픽 정보에만 의존하지 않고 호스트들의 상태 변화 정보와 Open port, 네트워크 구성 변경 등에 대한 이벤트들을 Rule을 바탕으로 한 연관성 분석 방법을 통해 정확도를 높일 수 있었다.

시그니쳐기반이 아니기 때문에 공격을 탐지 했을 때 어떠한 공격인지 공격 명을 알 수 없다는 단점을 가지고 있다. 그렇기 때문에 위험 레벨과 이벤트 정보들을 통해 어떠한 공격인지 판단하는 것은 관리자의 능력에 의존할 수 밖에 없다는 단점을 가지고 있다. 향후 좀더 다양한 악성코드를 효과적으로 탐지하기 위해 Rule셋 추가와 더불어 특정 레벨 이상의 이벤트가 발생한 노드에 대한 자동적인 차단 정책을 적용하는것에 대한 연구가

필요하다. 또한 Agent에서 좀더 정확한 행위 정보를 얻기 위해 레지스트리 변경 탐지와 프로세스와 API에 대한 연구와 더불어 오탐율을 줄이기 위해 효과적인 Grouping에 대한 연구를 수행할 계획이다.

참 고 문 헌

[1] Fyodor, Gordon Lyon (2009). NMAP NETWORKING SCANNING. 에이콘 출판사

[2] http://nmap.org

[3] 정재훈, 이승윤, 김용진 (2001), 인터넷 트래픽 측정 방법 및 시스템, 전자통신동향분석, 제16권 제5호.

[4] Luis Perrochon, Using Context-Based Correlation in Network Operation and Management, work in process, <http://pavg.stanford.edu/cep/>

[5] Webke Lee. Salvatore J.Stolfo, Kui W.Mok (1999), A Data Mining Framework for Building Intrusion Detection Models, IEEE Symposium on Security and Privacy.

[6] Vanessa Frias-Martinez, Salvatore J. Stolfo, Angelos D. Keromytis, Behavior-Profile Clustering for False Alert Reduction in Anomaly Detection Sensor, 2008 Annual Computer Security Applications Conference

[7] 노태열, 노대종, 박승섭 (2006), 네트워크 트래픽 분석을 통한 웜의 특성과 탐지방법에 관한 연구, 한국인터넷정보학회 학술발표대회 논문집, 7(1). (35~39).

[8] 김재현, 강신헌 (2007), 네트워크 트래픽 특성을 이용한 스캐닝웜 탐지기법, 정보보호학회 논문지, 17(1), (57~66).

[9] MyDoom.A와 Doomjuice 웜 분석 및 대응 보고서, http://www.krcert.or.kr

[10] 웹쉘에 대한 방어, http://kr.ahnlab.com/

[11] V.Frias-Martinez and S.J.Stolfo and A.D.keromytis. Behavior-Based Access Control : A Proof-of-Concept, Information Security Conference(ISC), 2008

한 명 묵

1980 연세대학교 공과대학 (공학사)

1987 뉴욕공과대학교 컴퓨터공학과(공학석사)

1997 오사카시립대학교 정보공학부(공학박사)

2005~2006 죠지아공대 교환교수(GTISC)

1998~현재 경원대학교 IT대학 부교수

관심분야: Information Security, Intellignet System

E-Mail: mmhan@kyungwon.ac.kr

선 종 현

2009 경원대학교 컴퓨터공학과(학사)

2009~현재 경원대학교 일반대학원 전자계산학과(석사과정)

관심분야: Network, Information Security

E-Mail: sunjh82@naver.com