情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

대규모 컴퓨터 바이러스/웜의 공격시 "종합침해사고대응시스템"에서의 자동화된 역추적 절차

최 운 호*, 전 영 태**

요 약

본 논문에서는 최근 인터넷 환경에서 증가하고 있는 대규모 컴퓨터 바이러스/웜에 의한 침해사고 발생 시 네트워크 포렌식등에서 정의되어야할 정보와 이를 활용한 대량 트래픽을 발생시키는 시스템을 탐지하는 방안을 제안하였다. 이에 따라 종합 침해사고 대응 시스템에서의 자동화된 역추적 절차를 제시한다.

Ⅰ. 서 론

인터넷 사용자가 급증하면서 이를 이용한 각종 해킹, 악성 웜의 배포, 중요기반구조에 대한 사이버테러 등이 크게 증가되는 상황에서 각종 정보보호시스템이 개발되어 운용되고는 있으나, 현재 도입되는 수동적인 방어 시스템이나 ESM(기업통합정보보호관리시스템 : Enterprise Security Management)은 해킹이 시도된 후 이를 막기 위한 제품/서비스로 해킹 시도 자체를 방지하는 데는 한계를 가지고 있다.

이러한 이유로 불특정 다수를 대상으로 한 악성 웜의 배포 및 해커의 해킹 시도 자체를 제한할 수 있는 자동화된 "종합침해사고대응시스템"[1]을 개발하고자 하는 노력이 시도되고 있으며, 가장 확보가 필요한 기술로 역추적 시스템기술에 대한 관심이 날로 커지고 있으나, 비록 아직은 초보적인 수준으로 이에 대한 연구가 진행되기 시작하였다.[2]

최근 대두되고 있는 컴퓨터 포렌식 DB는 시스템에 중대한 위기가 발생했거나, 시스템 다운 등 막대한 피해를 보았을 경우 법적인 조치를 위한 근거자료로 이용될 수 있는 바, 침해사고 발생 시 컴퓨터 포렌식 DB를 근거로 증거를 제시하여 민/형사 재판상의 증거로 제시할 수 있게 되는 것이다. 이 문서는 디지털 증거 관련 재판 시 배심원들에게 배포되어 검사, 변호사들은 공신력 있는 기관에서 인정한 컴퓨터 포렌식 툴로 획득된 디지털 증거임을 강조하여, 법 효력을 가질 수 있음을 주장하는데 사용된다.[3]

본 논문에서는 인터넷환경에서 증가하는 대규모 컴퓨터 바이러스/웜의 공격에 의한 침해사고 발생 시 네트워크 포렌식 등에서 정의되어야할 정보와 이를 활용한 대량 트래픽을 발생시키는 시스템을 탐지하는 절차를 제안하였다. 본 논문의 구성은 먼저 2장에서 기존의 역추적기술에 대해 살펴보고 3장에서 컴퓨터 바이러스와 웜의 전파경로에 대해 연구하도록 한다. 그리고 4장에서는 네트워크 포렌식에서 수집되어야할 정보를 살펴보고 마지막으로 5장에서 자동화된 역추적 기술의 절차를 제시한다.

Ⅱ. 기존의 역추적 기술에 대한 연구

침입자를 역추적(Traceback)하는 노력은 여러 가지 방향으로 연구되고 있다. 시스템에 침입한 증거를 찾기 위해 시스템 로그 분석, Logging, Ingress Filtering, Link Testing, ICMP Traceback등이 있으며 또한 IP역추적 시스템에 대한 연구로서 라우터 기능을 이용한 형태, 로그 데이타를 이용하는 구조 혹은 링크를 테스트하여 추적하는 방식이 있다. 이를 구체적으로 살펴보면 다음과 같다.

* 금융결제원 금융 ISAC실 정보보호평가팀장 (tiger@kftc.or.kr)
** 고려대학교 정보보호 대학원 (jbacteria@hanmail.net)
한국정보보호학회 조기경보시스템연구회 WG05 "특이 웜/바이러스 전파경로 분석기법" 부운영자

1. 로그를 이용한 역추적 기술

역추적을 위해서는 기본적으로 시스템 로그를 활용하며, 로그와 이상 파일을 바탕으로 시스템에 침입이 있었는가를 밝히고, 침입이 있었다면 언제 어느 사용자가 어디에서 접근하여 이루어졌는가를 밝힌다.

이후 침입자가 접근한 시스템에 접근하여 그 시스템에서 로그를 검색하여 그 사용자의 원래의 출발지를 연속적으로 찾아가는 방식으로 침입자의 출발지를 추적하는 시스템이다.[4,5]

2. TCP 연결 역추적 기술[6]

TCP 연결 역추적 기술은 호스트기반 연결역추적 (host-based connection traceback) 기술과 네트워크기반연결역추적 (network-based connection traceback) 기술로 분류된다.

2.1 호스트 기반 연결 역추적 기술

호스트 기반 연결 역추적 기술은 역추적을 위한 모듈이 인터넷 상의 호스트들에 설치되는 역추적 기법으로 호스트에서 발생하는 로그 기록 등의 다양한 정보를 바탕으로 역추적을 진행하는 기술이다.

2.1.1 CIS[7]

CIS(Caller Identification System)는 사용자가 특정 시스템에 접속하고자 할 때, 해당 시스템은 한 시스템에 접속하기 위해서는 자신이 경유한 모든 시스템에 대한 목록을 제공해야 하는 것이다.

2.1.2 AIAA[8]

AIAA(Autonomous Intrusion Analysis Agent) 시스템은 침해를 당한 서버의 해킹 피해 분석과 추적을 위한 로그 분석을 에이전트를 이용해 자동화한 역추적 시스템이다.

2.1.3 패킷손실기반의 논리적 전송경로추정[9]

패킷손실기반의 논리적 전송경로추정 방법은 다수의 호스트가 임의의 IP주소로 목적지 호스트를 공격하는 분산서비스공격의 경우에 패킷의 전송경로를 역추적하기 위한 방법이다. 이는 동일 경로를 따라 전송되는 패킷들의 손실에는 상호 연관성이 있다는 점에 근거하였다. 목적지 호스트는 전송되는 트래픽에 대하여 패킷들의 전송상태 및 전체 손실률을 계산한 후 이를 바탕으로 소스호스트까지의 전송경로를 역추적 할 수 있기 때문에, 라우터의 특정기능이나 ISP의 도움 없이 목적지 호스트를 독자적으로 추론하는 장점이 있다.

2.1.4 JBPA[10]

JBPA(JVM Based Plug-in Agent) 시스템은 'Real Tracing'이 구현된 것으로, 웹브라우저 플러그인으로 사용되는 JVM(Java Virtual Machine)을 이용한 역추적 기법으로 호스트에 자바애플릿 형태의 에이전트를 탑재하여 접근하는 모든 접속(사용자)을 실시간으로 최초 접속지까지 역추적할 수 있다는 장점을 가지고 있다.

2.2 네트워크 기반 연결 역추적 기술

네트워크 기반 연결 역추적 기술은 네트워크 상에 송수신되는 패킷들로부터 역추적을 수행할 수 있는 정보를 추출하여 역추적을 수행하는 것으로 역추적 모듈이 네트워크 상에 송수신되는 패킷을 확인할 수 있는 위치에 설치되어야한다. 아직까지는 네트워크 상에서 얻을 수 있는 패킷으로부터 어떤 정보를 활용해야 공격 연결과 같은 연결에 속하는가를 판단할 수 있을지에 대한 알고리즘만이 제기되고 있는 상황이며, 액세스 네트워크를 기본으로 하기 때문에 현재의 인터넷 환경에 적용하는 데 많은 어려움이 있는 것이 사실이다.[11-16]

2.2.1 TCP sequence number의 증가정도를 이용한 알고리즘

TCP sequence number를 이용하는 알고리즘은 비록 송수신되는 데이터가 암호화 되더라도 데이터의 양은 크게 변하지 않는다는 점에 착안하여 sequence number의 증가 정도를 변동 폭의 조정을 통해 비교하고 연결 체인을 구성하는 알고리듬이다.

2.2.2 Sleepy Watermark Tracing(SWT)

Sleepy watermark 역추적 시스템은 침입에 대한 응답 패킷에 워터마크를 삽입하여 역추적을 수행한다.

2.2.3 BPBT[17]

BPBT(Browser Plug-in Based Tracing) 시스템은 'Real Tracing'이 구현된 것으로, 기존 호스트기반 'JBPA' 역추적기법이 호스트에 국한되며 JVM만 지원한다는 한계를 극복하기 위해 등장하였다. 이는 호스트 기반인 'JBPA'의 기능과 장점을 그

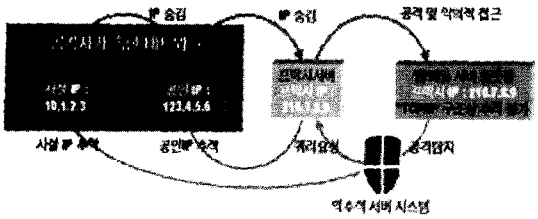


그림 1. Real Tracing 추적기법

대로 계승하면서 네트워크상에서의 역추적을 지원하고 추적성공률도 월등히 개선시키기 위한 노력의 일환으로 연구되고 있다.

3. 역추적 기술의 정의[6]

가. 역추적 : 사이버 범죄를 시도하는 공격자의 네트워크 상의 실제 위치를 탐색하는 기술

나. TCP 연결 역추적: TCP연결을 기반으로 우회공격을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기법

다. 연결 체인(Connection Chain): 컴퓨터 H_0의 한 사용자가 네트워크를 통해 다른 시스템 H_1으로 로그인하면, 두 시스템 H_0와 H_1간에는 TCP 연결 C_1이 생성된다. 이때, 같은 사용자가 시스템 H_1에서 H_2로, 또 H_3, …, H_n으로 로그인하게 되면, 각각의 해당 시스템들 간에는 TCP 연결 C_2, C_3, …, C_n이 같은 방식으로 생성되게 된다. 이때 이 일련의 연결들의 집합 $C = (C_1, C_2, \cdots, C_n)$를 연결체인이라 한다.

라. IP 패킷 역추적 : IP 주소가 변경된 패킷의 실제 송신지를 추적하는 기술이다.

4. 기타 역추적 기술들

4.1 마킹알고리즘기반 IP역추적에서의 공격근원지 발견기법[18]

DOS공격에 대응하는 하나의 방법으로 마킹알고리즘을 이용하여 공격경로를 찾아내고, 더 나아가 공격근원지의 MAC 주소를 알아냄으로써, 공격근원지를 찾는 방법이며, 이는 중간라우터가 패킷에 자신의 IP 주소를 표시하도록 하여 이를 토대로 공격경로를 역추적한다.

4.2 다중에이전트를 이용한 역추적시스템[19]

서버에서 스니핑과 스푸핑기법을 이용하여, 특정패킷을 전송하면, 각 네트웍에 존재하는 에이전트에서 그 패킷을 검출함으로써, 근원지 호스트까지의 연결경로정보를 획득하여 역추적서버로 하여금 공격 호스트를 검출하도록 한다.

4.3 네트웍에 대한 해킹공격에 대한 역추적[20]

이 방법은 기존 라우팅 프로토콜에서의 보안취약점을 분석한 해킹공격이 가능하다는 점에 착안한 것이다. 라우팅 테이블공격은 DDoS 공격보다 손쉽고도 파괴적이기 때문에 네트웍 AS시스템에서의 해킹/바이러스를 대처하고 이를 역추적 할 수 있도록 기존 라우터의 성능을 개선한 Secure Router 개발이 시급하다.

III. 컴퓨터 바이러스와 웜의 전파

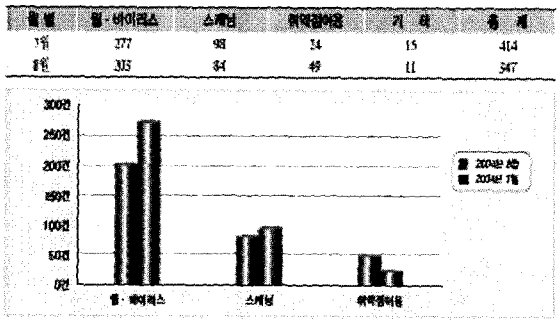


그림 2. 월간 국가/공공기관 해킹사고현황(NCSC, 2004. 8)

네트웍 운영자/시스템 운영자 그리고 정보보호담당자들은 1분기 정도에 몇 십종의 변종으로 나누어지는 각종 바이러스 및 웜에 대하여, 최초 전파자 혹은 조직 내의 최초 감염자들의 전파경로를 역추적하여, 이들을 근원부터 발견하여, 치료하고자 하지만 대부분 실패하고 있으며, 피해자이며 공격자로 변한 IP 혹은 공격자들은 차단시키는 기술을 고민하고 있어서, 최근의 바이러스/웜에 대해 상세한 전파경로를 확보하기 위한 분석이 필요하다.[19]

1. 컴퓨터 바이러스의 정의

최근 컴퓨터 바이러스는 윈도우 바이러스가 주를 이루고 있으며 윈도우용 실행파일 을 감염시켜 시스템에 악영향을 많이 일으키고 있다. 주로 감염된 시스템에 국한되던 피해에서 벗어나 네트워크에 공유된 컴퓨터까지 감염시켜 로컬 네트워크 전체의 피해로 확산되는 추세에 있다.

표 1. 컴퓨터 바이러스의 정의

구 분		특 징	현 재
감염 영역별	부트 바이러스	주로 하드디스크의 주 부트섹터(MBS)에 감염된 부팅디스크를 사용할 경우 감염됨 예) 브레인(1985)	윈도우 환경에서는 감염된 부팅디스크 사용이 일반적이지 않아 거의 사라진 상태임
	파일 바이러스	일반적으로 실행 가능한 파일(EXE, COM, DLL, SCR, PIF 등)에 감염됨	독립적인 형태의 파일 바이러스출현은 줄어들고, 인터넷 웜의 내부에 포함되는 형태로 나타나고 있음
※ 이외에 부트/파일 바이러스, 매크로 바이러스가 있음			
운영 체제별	Window 바이러스	Win3.1바이러스(NE) :16비트 코드로 작성 Win9x바이러스(PE) :32비트 코드로 작성 Win32 바이러스(PE) :NT 계열에서 정상적으로 메모리에 상주함	Win32/딸구.B 이후 큰 이슈가 되는 바이러스 등장하지 않음
	Linux /Unix 바이러스	Linux/Unix의 취약성을 이용해 제작되어 주로 웜의 형태를 띔 예)Linux/Lamen	Linux/Unix의 감염을 위한 신종 바이러스의 개수가 많지 않음
※ 이외에 도스, 자바, Palm 바이러스 등이 있음			

2. 웜의 정의

이메일의 첨부 파일을 통한 전파가 대부분이던 감염 경로에서 IRC, P2P, 메신저 등 감염 매체가 다양해지고 컴퓨터 바이러스와 결합함으로써 다양한 유형으로 피해를 일으키고 있으며 최근에는 Buffer Overflow 취약점을 이용한 웜의 등장으로 대량의 트래픽 공격으로 인해 국가 기간망의 다운까지 초래하고 있다.

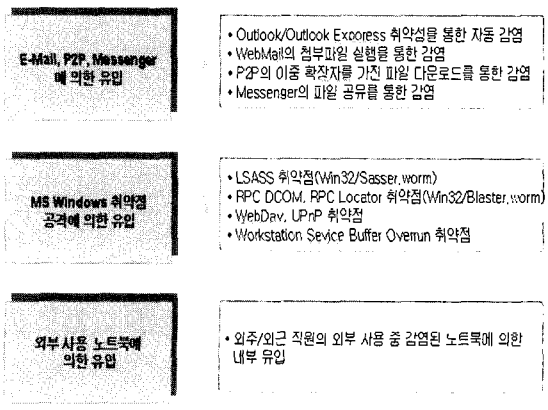


그림 3. 웜의 전파 경로

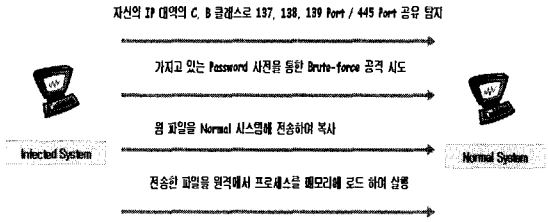


그림 4. 네트워크을 이용한 공격

3. 컴퓨터 바이러스와 웜의 감염 경로

컴퓨터 바이러스와 웜의 감염 경로가 다양해지고는 있지만 여전히 초기 확산의 단계에서는 이메일에 첨부된 웜에 의한 경우가 대부분이다. 이후 2차적으로 관리적 공유 폴더를 통한 내부 네트워크 시스템에 대한 감염이 시작되고 IRCBOT의 경우 3차적으로 DDOS 공격 등의 원격 공격으로 인해 피해 범위의 확산이 가능하다.

대표적인 웜의 감염 경로로 사용되는 Outlook / Outlook Express의 경우 취약점을 패치하지 않을 경우 제목을 클릭 하는 것으로 첨부된 파일의 실행 없이 감염이 가능하다. 웹메일의 경우 인터넷 익스플로러의 취약점이 패치 되었다면 대부분의 경우 첨부된 파일을 다운로드 후 실행하는 것으로 감염된다.

자신의 혹은 미리 정의된 IP 대역의 C, B, A 클래스 순서로 TCP 139, 445 포트를 통해 윈도우 NT 계열의 관리적 공유 연결을 스캐닝 하는 순간 대량의 트래픽 유발 및 많은 세션 연결로 인해 라우터, 스위치, ATM, 침입차단시스템 등의 네트워크 장비 및 정보보호 장비들이 다운되는 증상이 빈번하게 발생하고 있다.

4. 컴퓨터 바이러스와 웜의 대응 방법

네트워크 트래픽의 이상 증상을 일으키는 컴퓨터 바

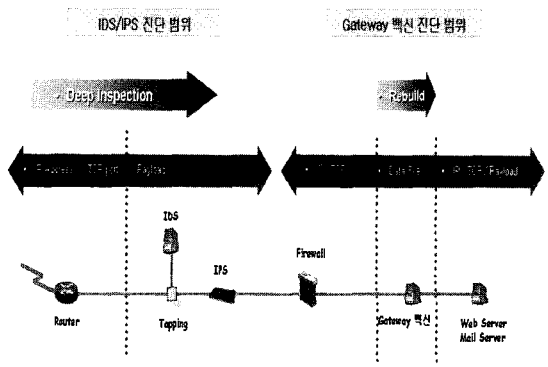


그림 5. 컴퓨터 바이러스와 웜 솔루션

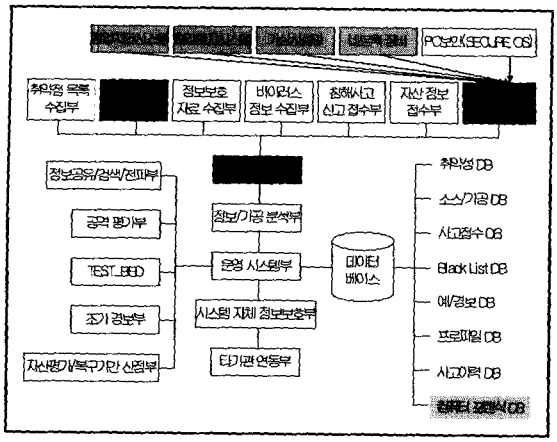


그림 6. 자동화된 침해사고대응시스템에서의 컴퓨터포렌식DB

이러스와 웜의 등장으로 IPS가 최근 크게 대두되고 있지만 아직까지 성능 면에서 불안정성을 가지고 있다.

Ⅳ. 컴퓨터 바이러스와 웜의 네트웍 포렌식

현재의 정보보호시스템은 ESM시스템과 연동되어 관리되는 추세이며, 네트웍으로 빠르게 확산되는 바이러스/웜 에 대한 가공/분석된 정보를 관련기관시스템으로 제공하고, 실제 시스템에 대한 대규모 공격사고가 예상되는 경우 공격평가를 통한 조기경보를 발령하여 예방활동을 수행하는 것이 필요하다.

이를 위해서는 과거 또는 현재 발생한 침해사고 정보를 관리하는 컴퓨터 포렌식 DB가 필요하다. 일반적으로 컴퓨터 포렌식 DB는 시스템에 중대한 위기가 발생했거나, 시스템 다운 등 막대한 피해를 보았을 경우 법적인 조치를 위한 근거자료로 이용될 수 있어야 한다. 이러한 포렌식 DB에 수집되는 정보들은 디지털 증거(Digital Evidence)를 쉽고, 빠르고, 정확하게 수집할 수 있어야 하는데, 이를 위해서는 컴퓨터 포렌식 툴이 사용된다. 이러한 컴퓨터 포렌식 툴에서 성능 이외에도 가장 중요시 되는 것은 수집된 증거가 신뢰성을 가질 수 있도록 뒷받침 할 수 있어야 한다는 것이다.

미국 NIST(National Institute of Standards and Technology) 산하 정보기술 연구소에서는 컴퓨터포렌식툴 검증(Computer Forensics Tool Testing - CFTT)[22] 프로젝트를 실시하고 있다.

이 프로젝트는 컴퓨터 포렌식 툴은 항상 목적한 결과를 정확하게 낼 수 있는지 검증할 수 있어야 하기 때문에 컴퓨터 포렌식 툴 검증 및 평가 방안을 제시하고 컴퓨터 범죄 수사관이 많이 사용하는 컴퓨터 포렌식 툴을 테스트하고 결과를 문서화하여 공개하고 있다.[3,23]

1. 네트워크 포렌식의 정의

네트워크 포렌식의 절차는 침해정보 수집체계에서 침해사고에 대한 규칙을 판단하고, 해당 이벤트를 확보하여 활용하며, 절차는 다음과 같다.

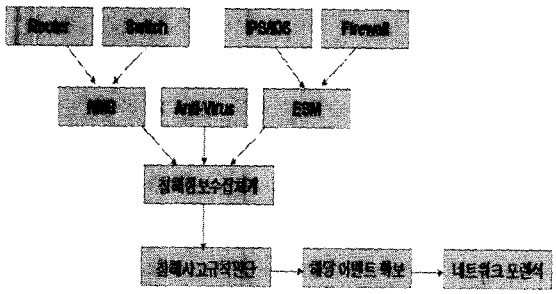


그림 7. 네트워크 포렌식 프로세스

2. 라우터 정보

라우터는 외부 네트워크와 내부 네트워크 분리 및 내부 네트워크의 브로드케스트 도메인을 분리하기 위해 사용되는 장비로 컴퓨터 바이러스와 웜의 포렌식을 위해서는 아래의 정보가 수집되어야 한다.

- 라우터의 상태 정보와 설정 정보
- 라우팅 프로토콜과 라우팅 테이블정보
- 라우터의 ARP Cache 정보
- 라우터의 local 로그와 네트웍 트래픽 로그 정보

```
Router# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
   Console logging: level debugging, 10 messages logged
   Monitor logging: level debugging, 0 messages logged
   Trap logging: level informational, 14 message lines logged
   Buffer logging: level debugging, 10 messages logged

Log Buffer (4096 bytes):

%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINK-3-UPDOWN: Interface Serial1, changed state to down
00:00:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed sta
te to up
00:00:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
 to up
00:00:14: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state
 to down
```

그림 8. 라우터 로그 정보

```
Switch (enable) sh logg
Logging buffer size          500
       timestamp option:     enabled
Logging history size         1
Logging console:             enabled
Logging server               disabled
       server facility:      LOCAL7
       server severity:      warnings(4)
Facility          Default Severity        Current Session Severity
--------------    ----------------------  ------------------------
cdp               4                       4
(...)
Heap Memory Log:
Corrupted Block = none

NVRAM log:
01  11/27/2000,22:12:11  convert_post_SAC_CiscoMIB Block 0 converted from version 7
(...)
Module 2 Log:
  Reset Count:  51
  Reset History: Sun Oct 14 2001, 03:36:07
                 Sun Oct 7 2001, 02:59:08
Module 3 Log:
  Reset Count:  4
  Reset History: Sun Oct 14 2001, 03:36:48
                 Sun Oct 7 2001, 02:59:51
                 Sun Oct 7 2001, 02:29:23
                 Sun Oct 7 2001, 02:22:30
```

그림 9. 스위치 로그 정보

3. 스위치 정보

스위치는 내부망에서 호스트들 간의 네트워을 형성하는 중계기의 역할을 한다. 스위치는 단순히 신호를 전달해주는 역할을 하는 허브와는 달리 전송될 메시지를 MAC address 와 일치하는 port 로 전달해주는 데이터링크(Data Link)계층 장비로 아래의 정보가 수집되어야 한다.

- MAC table
- VLAN(virtual LAN)

4. IPS/IDS 정보

IPS/IDS는 컴퓨터 바이러스와 웜에 의한 공격을 직접적으로 통제 할 수 있는 중요한 정보를 제공한다. 오용 탐지 기반의 IPS/IDS의 경우 Signature와 매칭되는 위험정보리스트가 중요하며 비정상 탐지 기반의 IPS/IDS의 경우 정상 상태값이 네트워크 포렌식에서의 프로파일 DB의 원시데이타로 사용된다.

- IPS/IDS의 상태 정보
- IPS/IDS의 정책 정보
- IPS/IDS 이벤트 로그와 로그 정보

5. 침입차단시스템(Firewall) 정보

침입차단시스템은 악의적인 공격자로부터 내부의 서버나 호스트들을 지키기 위한 보안관으로서의 역할

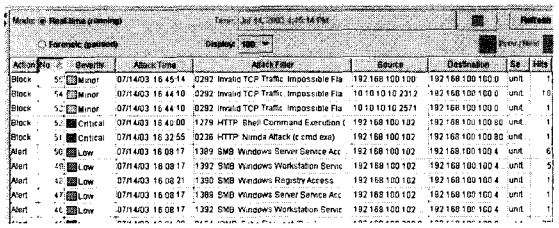


그림 10. IPS 필터 정보

을 한다. 내부로 접속하는 모든 네트워 트래픽은 침입차단시스템(firewall)을 통해서 접속하도록 허용하고 침입차단시스템에서는 지나는 모든 네트워 패킷의 IP address와 Port 번호 그리고 연결 상태를 기준으로 해당 패킷을 허용할지 거부할지를 결정하며 아래의 정보가 네트워크 포렌식에서 필요하다.

- 침입차단시스템의 상태 정보 및 설정 보
- 침입차단시스템의 로그

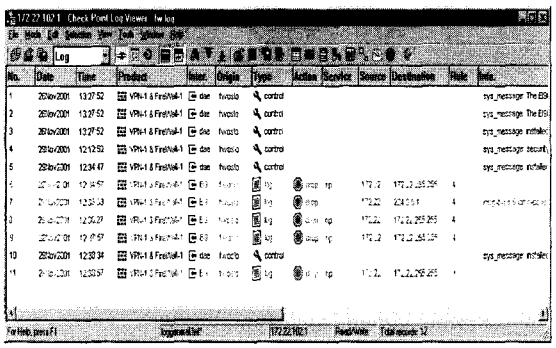


그림 11. 침입차단시스템 로그 정보

6. 기타 네트워크 장비 및 보안 장비 정보

네트워크 스캐너를 통한 네트워크 장애 관련 로그

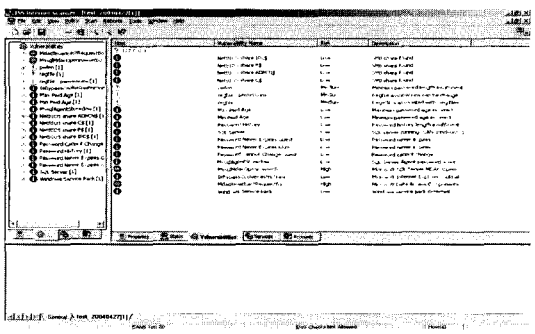


그림 12. 네트워크 취약점 정보

와 취약점 스캐너를 통한 취약점 로그 등의 정보도 추가적으로 필요하다. 기타 정보보호 장비인 VPN, SecureOS 등의 로그 정보도 부가적으로 자동화된 역추적을 위한 정보로 사용될 수 있다.

V. 자동화된 역추적 기술의 설계 및 기능

1. 침해 정보 수집 체계

네트워크 정보(Router, Switch), 정보보호 제품 정보(IPS/IDS, Firewall)와 안티바이러스 정보의 수집 시 많은 양의 정보[24]로 인해 침해 정보 수집의 체계적인 정립이 필요하다. 이러한 침해 정보 수집 체계는 네트워크 포렌식의 전체적인 성능을 좌우한다.

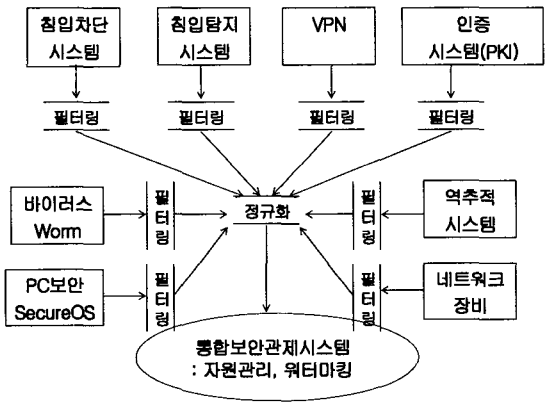


그림 13. 정보보호제품 이벤트수집 및 필터링

2. 침해 사고 규칙 판단

수집된 침해 정보가 미리 정의된 프로파일과 비교하여 비정상적인 경우 혹은 블랙리스트와 일치할 경우 침해 사고로 인식된다. 침해 사고 규칙에는 전문가 시스템에서 사용되는 인공지능 기법이 사용될 수 있다. 이를 침입준비단계, 공격단계, 사후 진행단계 등으로 시간에 따라 재분류하며, 공격수준(단계)을 산출한 후, 소스(Source) IP별, 인터넷 서비스 제공사업자(ISP)별, 국가별, 공격수법별, 기간별 등으로 분류·저장한다.

3. 해당 이벤트 확보

침해 사고로 판단되면 해당 IP, MAC 등 구별기준을 통해 최대한의 이벤트를 확보하는 장치를 마련해야 한다. 또한, 운영중인 정보보호제품, 예를 들면 침입탐지시스템(IDS)의 이벤트 중 위험도, 목적지(Destination) IP, 특정 소스(Source) IP, 특정 포트 등을 파악하고, 해당되는 이벤트를 블랙리스트(Black List) DB, IDS 사고이력 이력(History) DB 등으로 나누어 저장하며, 각 DB에서 추출된 데이터를 이용해 공격 평가 알고리즘을 적용하여 공격정도를 평가한다.

4. 자동화된 역추적 방안

컴퓨터 바이러스와 웜에 의해 대규모 악성 트래픽이 네트워크에 침해 사고를 일으키기 시작하면 침해 정보 수집 체계에 따라 악성 트래픽 정보가 각종 솔루션으로부터 수집되며 미리 정의된 침해 사고 규칙에 위배되면 최대한의 이벤트를 확보하여 악성 트래픽을 발생한 시스템의 위치를 역패스 구성을 통해 해당 시스템의 OS 및 백신의 최신 패치 여부를 확인하여 자동으로 패치를 푸쉬하며 이때에도 컴퓨터 바이러스나 웜이 해결되지 않는다면, 알려지지 않은 컴퓨터 바이러스나 웜으로 구별해 백신 회사로 해당 시스템의 정보를 자동으로 통보하는 시스템을 구성한다. 역추적 패스는 침해사고 규칙판단에 따라 Non-Spoof IP는 그대로 탐지하며 Spoof된 IP의 경우 MAC값을 기초로 침해정보수집체계의 로그를 기초하여 해당 시스템, 네트워크 장비를 탐지한다. 웜/바이러스에 의한 네트워크 트래픽을 발생시키는 시스템, 네트워크의 네트워크 차단을 통해 초기 네트워크, 보안 장비의 침해 사고를 예방하고 시스템의 경우 운영체제 정보 및 백신 최신 패치 적용 유무를 스캔하여 백신이 최신 패치가 되도록 자동으로 푸쉬한후 웜/바이러스에 감염된 시스템이 최신 버전의 백신으로도 해당 시스템이 안정화되지 않는다면 시스템의 각종 정보를 자동으로 백신 회사로 전송한다. 자동으로 전송된 웜/바이러스 감염 시

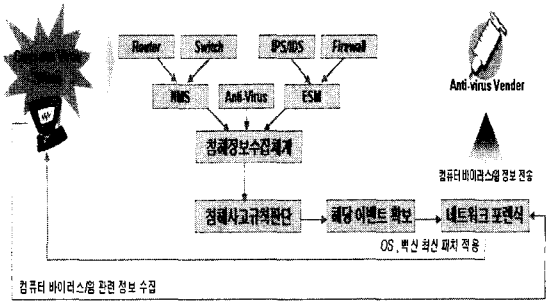


그림 14. 네트워크 포렌식 IP 역추적

스템의 정보를 기초로 백신 회사에서 분석이 끝난 후 제작된 최신 버전의 백신 엔진을 웜/바이러스에 감염된 시스템에 적용하여 안정화한다. 자동화된 역추적 프로세스상의 네트워크 포렌식은 웜/바이러스에 감염된 시스템의 운영체제 정보 및 백신 엔진 정보를 확인하고 패치를 업데이트 할 수 있는 기능이 있어야 한다. 위의 프로세스로 웜/바이러스에 감염된 시스템, 네트워크 장비의 초기 억제를 통해 네트워크의 가용성을 보장할 수 있다.

5. 네트워크 포렌식 IP 역추적시나리오

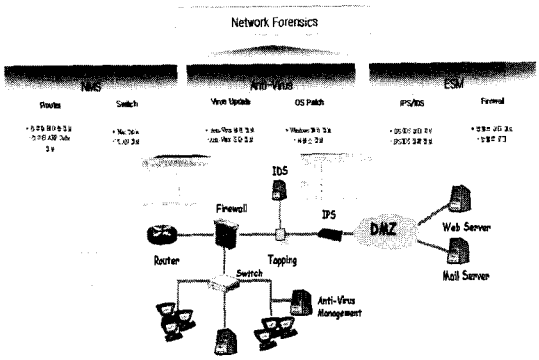


그림 15. 네트워크 포렌식 IP역추적 시나리오

웜/바이러스에 의한 네트워크 침해 사고의 유형은 크게 내부 네트워크의 감염된 시스템에 의한 경우와 외부 네트워크의 감염된 시스템에 의한 경우 2가지로 분류 할 수 있고, 내부 네트워크의 감염된 시스템에 의한 경우는 다시 정상적인 소스 IP를 가지는 경우와 스푸핑되는 IP를 가지는 경우 2가지로 분류될 수 있다.

가. 내부 네트워크의 웜/바이러스 감염된 시스템에 대한 역추적 시나리오

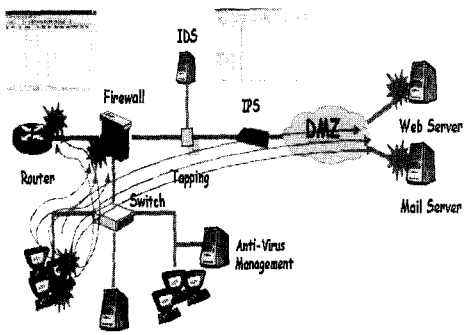


그림 16. 내부 네트워크에서의 IP 역추적 시나리오

(1) 1단계(Attack) : 웜/바이러스에 감염된 시스템에 의해 내부 네트워크의 게이트웨이시스템에 네트워크 연결 세션 증가

(2) 2단계(Detection) : 침해정보 수집체계중 ESM, NMS에서 웜/바이러스에 의해 감염된 것으로 추정되는 시스템의 IP를 탐지(IP가 고정되지 않고 지속적으로 변화하거나 스푸핑되는 경우 MAC어드레스의 비교를 통해 시스템 탐지) 및 Anti-Virus 시스템에서 웜/바이러스 진단 시스템의 로그 증가

(3) 3단계(Define) : 침해사고규칙판단에 따른 미리 정의된 프로파일 비교 및 블랙리스트 매칭을 통해 웜/바이러스에 의한 네트워크 침해 시스템을 규정

(4) 4단계(Traceback) : 침해사고규칙판단 결과에 따른 해당 IP정보 및 경로에 대한 수집 가능한 정보 확보를 통해 내부 네트워크의 감염된 시스템 역추적

(5) 5단계(Network Forensic) : 수집된 정보를 바탕으로 웜/바이러스 감염 IP에 PMS를 통한 OS 패치 및 백신 관리 시스템을 통한 백신 업데이트를 통해 알려진 웜/바이러스에 의한 공격 여부를 판단

(6) 6단계(Feedback) : 알려지지 않은 웜/바이러스에 의한 침해 사고일 경우 네트워 침해를 일으킨 시스템의 정보를 수집하여 백신 업체에 전송 후 분석된 자료를 통한 업데이트 피드백

나. 외부 네트워크의 웜/바이러스 감염된 시스템에 대한 역추적 시나리오

(1) 1단계(Attack) : 웜/바이러스에 감염된 외부 시스템에 의해 내부 게이트웨이 및 응용 시스템에 서비스 거부 등의 이상 증상 나타남

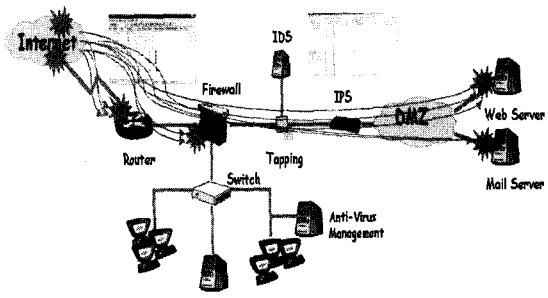


그림 17. 외부 네트워크에서의 IP 역추적 시나리오

(2) 2단계(Detection) : 침해정보수집체계에서 ESM, NMS에서 웜/바이러스에 의해 감염된 것으로 추정되는 시스템의 IP탐지 및 Anti-Virus시스템에서 웜/바이러스 진단 시스템의 로그 증가

(3) 3단계(Define) : 침해사고규칙판단에 따라 정의된 프로파일비교 및 블랙 리스트 비교를 통해 웜/바이러스에 의한 네트워크 침해여부를 규정

(4) 4단계(Traceback) : 침해사고규칙판단 결과에 따른 해당 IP정보 및 경로에 대한 수집 가능한 정보 확보를 통해 내부네트워크의 감염된 시스템 역추적

(5) 5단계(Network Forensic) : 네트워크 포렌식 DB의 프로파일 갱신 및 블랙 리스트 갱신을 통해 추후 이상 증상의 판단 결과로 재사용

다. 사후처리(postmortem) : 보안 최적 실행 방안의 최종 단계는 사후 처리로, 공격이 발생한 뒤 이를 해결하는데 가장 효과적인 방법은 무엇이었으며 어떤 것들이 개선되었는지를 검토하는 것이다. 사후 처리는 내부적으로 실시 되어야 할 뿐만 아니라 외부 조직과의 협력을 통해서도 진행되어야 한다.

Ⅵ. 결 론

사이버 공격은 어떠한 전조도 보이지 않는다. SQL 슬래머(Slammer) 웜이 2003년 1월 25일 등장한 이후 빠른 속도로 컴퓨터 바이러스/웜이 해킹 기술과 접목되고 있다. 이러한 위협에는 분산 서비스 거부(DDoS)를 비롯해 해커 공격에 이르는 모든 유형의 보안 정책 위반이 포함된다. 이러한 공격의 수준과 정교함이 높아지면서 더 이상 단순히 고객 네트워크와 데이터를 침해하는데 그치지 않고 인터넷 인프라 자체를 타깃으로 한 공격이 나타나고 있다. 점점 더 많은 서비스 사업자들이 음성을 포함한 통합 서비스를 제공함에 따라 네트워크 보안의 중요성도 높아지고 있다. 네트워크에 연결된 정상적인 컴퓨터를 감염시키기 위해 네트워크 스캐닝 시 대량의 트래픽이 발생하여 라우터, 침입차단시스템, 스위치 등 네트워크 장비들을 다운시키거나 장애를 유발하고 있다. 따라서 네트웍에 연결된 각종 장비의 정보를 기반으로 한 네트웍포렌식과 각종 통계를 기초한 블랙리스트 등의 연동을 통하여, 특정시기에 대량의 트래픽을 발생시키는 사이트 및 공격자/피해자 등을 자동적으로 가려내는 시스템이 강력하게 요구되고 있다.

본 논문에서는 자동화된 종합 침해사고 대응시스템에서 컴퓨터 바이러스에 의한 침해사고 발생 시 네트워크 포렌식 등에서 정의되어야할 정보와 이를 활용한 대량 트래픽을 발생시키는 시스템의 탐지 및 자동화된 역추적 방안에 대한 설계와 기능에 대한 개념을 제시하였다.

네트워크 포렌식과 연동된 자동화된 역추적 기술은 내부 네트워크 트래픽을 폭증시키는 시스템의 탐지에 새로운 대안이 될 수 있으며 기업에서 컴퓨터 바이러스/웜의 대처를 위한 컴퓨터 사용자의 책임성을 위한 자료로도 사용될 수 있다. 특히 네트워크 담당자에게는 고가용성 유지를 가능하게 하고 정보보호 담당자에게는 컴퓨터 바이러스와 웜에 의한 사고의 기초 자료로서 사용될 수 있으며, 자동화된 역추적 기술을 이용한 자동화된 컴퓨터 바이러스와 웜의 분석 및 치료 기술에 대해 고민해 보아야 할 것이다.

Ⅶ. WG05 소개

한국조기경보포럼의 WG05는 특이 웜 바이러스 전파경로 분석에 관련된 분과이다. 최근의 웜은 전파방법의 다양화 및 지능화, 네트워크 인프라의 고속화로 전세계 취약한 시스템의 90%을 10분 내에 감염시킬 수도 있다. 지난 1.25 대란때의 Slammer 웜이 30분내에 국내 모든 네트웍에 전파된 것으로 보아 그 심각성을 알 수 있을 것이다. 또한 과거에는 보안 취약점에 의한 패치가 나온 후 웜이 등장했으나 최근에는 거의 비슷한 시기에 출현하는등 웜 등장 주기가 점차 단축되고 있다. WG5는 이러한 문제점들에 대한 가장 시급한 과제로서 웜 전파 경로의 분석기법을 연구하고자 한다.

⊙ 연구 방향

- 내부 급속한 확산으로 인한 네트워크/서버 침해 억제 방법 연구
  - 패스워드 취약점 : 전체 시스템 패스워드 적용 방안 연구, 패스워드 정책 연구 등
  - 관리적 공유 대응 방안 연구 : 관리적 공유 해제 방안 적용 연구, NetBios 제한 방안 연구 등
  - 보안 패치 방안 연구 : 패치 매니지먼트 시스템 연구 등

⊙ 분과 운영

- 월 1회 오프라인 모임 및 온라인 모임을 통하여 연구 주제를 토론

· 개인별 희망 과제 부여 또는 분과내의 소규모 분과를 만들어 운영

참 고 문 헌

[1] 최운호, "국가 조기경보시스템 활성화를 위한 제안", 월간사이버시큐리티, 국가사이버안전센터 2004. 5

[2] Buchholz, Thomas E. Daniels, Benjamin Kuperman, Clay Shields, "Packet Tracker Final Report,"CERIAS Technical Report 2000-23, Purdue University, 2000.

[3] 김현상, 이상진, 최운호, 임종인 "자동화된 침해사고 대응시스템에서의 디지털증거 수집", 한국정보보호학회 하계학술대회, 2004년

[4] 한국정보보호센터 "불법 침입자 실시간 역추적 시스템 개발에 관한 연구"위탁과제보고서, 1998

[5] Karyn Pichnarczyk, Steve Weeber & Richard Feingold, Unix Incident Guide : How to Detect an Intrusion, CIAC-2305 R.1, Dec 1994.

[6] 최양서, 서동일, 손승원 "역추적 기술 동향: TCP Connection Traceback 중심" IT-FIND 주간기술동향, 2003년 1월, http://kidbs.itfind.or.kr.

[7] H.T. Jung et al. "Caller Identification System in the Internet Environment.," Proceedings of the 4th Usenix Security Symposium, 1993.

[8] Chaeho Lim, "Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis Agent," FIRST Conference on Computer Security Incident Handling & Response, 1999.

[9] 이준엽 외 4인, "IP역추적을 위한 새로운 접근 : 패킷손실기반의 논리적 전송경로 "한국정보보호학회논문지, 제12권3호, 2002.6.

[10] Steven R. Snapp, James Brentano, Gihan V. Dias, "DIDS(Distributed Intrusion Detection System), Motivation, Architecture, and An Early Prototype," Proceedings of the 14th National Computer Security Conference, 1991.

[11] K. Yoda and H. Etoh, "Finding a Connection Chain for Tracing Intruders," In F. Guppens, Y. Deswarte, D. Gollamann, and M. Waidner, editors, 6th European Symposisum on Research in Computer Security - ESORICS 2000 LNCS-1985, Toulouse, France, Oct. 2000.

[12] S. Staniford-Chen and L.T. Heberlein. "Holding Intruders Accountable on the Internet," In Proceedings of the 1995 IEEE Symposium on Security and Privacy, 1995.

[13] Y. Zhang and V. Paxson, "Detecting Stepping Stones," Proceedings of 9th USENIX SecuritySymposium, Aug. 2000.

[14] D. Schnackenberg, K. Djahandari, and D. Sterene, "Infrastructure for Intrusion Detection and Response," Proceedings of DISCEX, Jan. 2000.

[15] D. Schnackenberg, K. Djahandary, and D Strene, "Cooperative Intrusion Traceback and Response Architecture(CITRA)," Proceedings of the 2nd DARPA Information Survivability Conference and Exposition(DISCEXII), June 2001.

[16] 김병룡 외 3인, "마킹알고리즘기반 IP 역추적에서의 공격근원지 발견기법" 한국정보보호학회논문지, 제13권1호, 2003.2.

[17] 정종민 외 2인, "다중 에이젼트를 이용한 역추적 시스템 설계 및 구현" 한국정보보호학회논문지, 제13권4호, 2003.8

[18] 이형우, "DDoS 해킹공격 근원지 역추적 기술" 한국정보보호학회논문지, 제13권5호, 2003.10

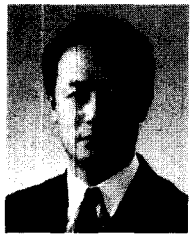
[19] 국가사이버안전센터, www.ncsc.go.kr, "월간 국가/공공기관 해킹사고현황 "월간사이버시큐리티 8월호, 2004.8

[20] NIST 컴퓨터 포렌식 툴 검증 프로젝트, http://www.cftt.nist.gov

[21] 박종성, 최운호, 문종섭, 손태식, "자동화된 침해사고대응시스템에서의 네트워 포렌식 정보에 대한 정의", 한국정보보호학회 논문지, 4월, 2004년도

[22] 전규삼, 최운호, "자동화된 침해대응시스템에서 Web을 기반으로 한 로봇에이전트에 대한 연구" 한국정보보호학회 하계학술대회, 2004년

〈著 者 紹 介〉



최 운 호 (Un-Ho Choi)
종신회원

1990년 : 광운대학교 학사
1995년 : 광운대학교 대학원 전자계산학과 석사
2004년 : 한세대학교 대학원 정보보호공학과 박사
1989년~1996년 : 한국전산원 선임연구원
1996년~2001년 : 한국정보보호진흥원 팀장
2002년~현재 : 금융결제원 금융ISAC실 정보보호평가팀장
2003년~현재 : 한국정보보호학회 이사
2004년~현재 : 한국정보보호학회 조기경보시스템연구회 위원장
2004년~현재 : 국가정보보안협의회 조기경보시스템연구회 위원장
〈관심분야〉 조기경보, 블랙리스트, 관제센터운영, 침해사고신고 자동화 등

전 영 태 (Jun-Young Tae)

2002년 : 명지대학교 학사
2002년~2004년 : (주)하우리 바이러스 분석실 연구원
2003년~현재 : 고려대학교 정보보호 대학원 석사과정
〈관심분야〉 컴퓨터 바이러스, 웜 전파경로 조기경보, 컴퓨터 포렌식, 데이터베이스 보안, 시스템 취약점 등