Global Incident Trends 분석기술 동향

윤 영 태* 류 재 철** 박 상 서* 박 춘 식*

◈ 목 차 ◈

1. 서 론

바이러스와 달리 알려진 취약점을 통해 자기 전파(Self Propagation) 기능을 가지는 웜 형태의 악성코드는 일반 사용자 네트워크의 지연 및 심지어 네트워크 기반구조 마비 상태로까지 이어지는 커다란 피해를 가져왔다. 이러한 사례는 최초의 모리스 웜에서부터 최근 인터넷 마비 상태를 가져온 슬래머 웜, 마이둠 웜에서 쉽게 찾아볼 수 있다.

웜은 전파방법 및 피해형태에 따라 많은 변화가 있어왔는데 최근 웜은 다중 취약점 이용, 다중 플랫폼 전파 , 0-day 전파 등과 같은 특징을 보이고 있다. 악성코드 방어를 연구하는 보안분야의 전문가들은 이러한 웜으로 인한 피해는 계속해서 발생할 것으로 예측하고 있으며, 그 형태도 급속한 전파와 함께 다형성(Polymorphic) 특성을 가짐에 따라 탐지 및 대응이 더욱 어려워질 것으로 예상하고 있다[1][6].

이러한 웜 및 해킹에 대한 특성을 평가하는 방법으로는 코드 분석 방법과 웜 샘플 확보를 통해 재연함으로써 시연을 해보는 방법, 가상 시뮬레이션 기법, 침입차단시스템, 침입탐지 시스템과 같은 네트워크 보안시스템으로부터 발생되는 로그를 분석함으로써 관리대상 네트워크에 대한 사고 분석 방법 등이 고려될 수 있다.

* 국가보안기술연구소
** 충남대학교 정보통신공학부 교수

하지만, 위에 열거한 방법의 경우 현재의 피해 현황 및 진행상황을 평가하기에는 부족하게 된다. 실제 네트워크 환경에서의 사고 진행상황을 평가하기 위한 방법으로 트렌드 분석이 이용되게 되며, 본 논문에서는 웜이나 특정 취약점을 이용하기 위한 스캔 동작 등을 분석 탐지하는 글로벌 트렌드 분석 기술 동향에 소개하고자 한다. 2장에서는 글로벌 사고 트렌드 분석 사이트를 대상으로 현재 수행되고 있는 기술에 대한 분류를 기술한다. 3장에서는 트렌드 분석 서비스를 제공하는 사이트의 분석구조 및 기술 동향에 대해 살펴보고, 4장에서 결론을 맺도록 한다.

2. 글로벌 사고 트렌드 분석 기술

2.1 트렌드 분석 개요

보안분야에서 트렌드(Trend)란 용어는 취약성 분석 기술, 바이러스, 침해사고 대응 등 다양한 분야 및 인터넷 사고 분석 및 통계 정보를 제공하고 있는 여러 사이트에서 사용되고 있다. 본 논문에서는 서로 다른 공간 및 다수의 사이트로부터 발생되는 센서의 로그를 수집하여 인터넷 사고와 관련된 현황을 자동으로 분석하고, 축적된 분석데이터와의 비교를 통해 변화되는 패턴을 분석하는 글로벌 사고 트렌드 분석에 초점을 맞추고자 한다.

CERT/CC 분석 센터에서는 [2]에서 정보보호 트렌드 분석에 대한 모델을 제시하면서 트렌드 분석에 대

해, 시간상에서 변화하고 있는 주된 이벤트 패턴을 분석하는 것으로 정의하고 있다. 또한, 미 공군에서 SBIR 계약을 통해 NetSquared, U.C.Davis 대학과 추진해온 트렌드 센서(Trend Center) 프로젝트에서는 마이크로소프트사의 SQL 서버에 대한 취약점이 발표된 후 6개월 후에 슬래머 웜이 피해를 가져왔음을 경고하면서, 위협환경에 대한 분석정보 뿐만 아니라 위협이 될 수 있는 취약점 정보를 파악함으로써 기존의 " 탐지대응" 방식의 패러다임에서 "예측예방" 형태의 대응 패러다임으로 전환하기 위한 방법으로 트렌드 분석을 확장하였다[3].

트렌드 분석기술은 보안경보를 위한 기초 데이터를 자동으로 제공할 수 있는 장점을 제공하게 되는데, 기존의 보안경보는 침해사고 대응조직 또는 보안업체를 통해 신고되는 데이터를 분석함으로써 문제의 파급효과에 따라 위험레벨을 전파하도록 하였다. 또한, ESM 시스템이나 보안관제 기술에서는 침입탐지시스템과 같은 센서들로부터 관리대상 네트워크에 대해서만 이벤트를 수집·분석하고 있다. 하지만 최근의 위협동향은 새로운 취약점을 이용 네트워크를 통해 전파되는 특성을 가지고 있어 관리대상 네트워크에 대한 이벤트 수집만으로는 위협상황을 파악하기 어렵기 때문에 최근의 위협상황에 대처하기에는 한계점이 있다. 따라서, 전세계적 센서로그를 분석하여 자동화된 보안경보와 사고의 진행현황 등을 판단할 수 있는 글로벌 트렌드 분석기술이 요구되게 되었다.

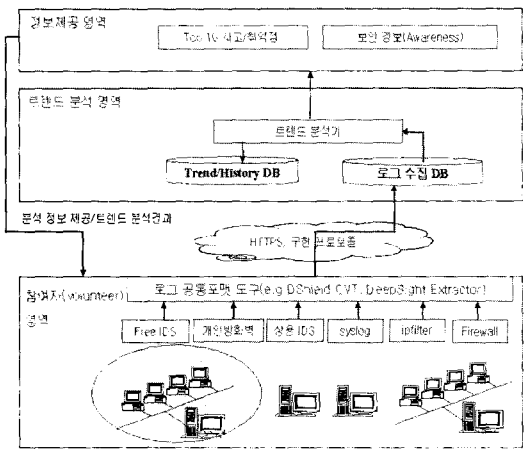
2.2 글로벌 사고 트렌드 분석 모델

트렌드 분석을 수행하는 대표적인 곳은 SANS의 ISC(Internet Storm Center), DShiled와 DeepSight 등을 들 수 있다. 이들 사이트에서 제공하는 트렌드 분석 모델은 그림 1에서와 같이 센서가 위치한 참여자(Volunteer) 영역, 센서로부터 수집된 정보를 중앙에서 분석 및 저장을 수행하는 분석 영역, 웹에 기반하여 분석결과를 공개하는 정보제공 영역으로 나누어 볼 수 있다. 참여자 영역은 각 서브넷에 위치한 방화벽, 개인방화벽, IDS 등과 같은 다양한 센서들로부터 발생되는 로그정보를 트렌드 분석 사이트와의 정보제공 동의를 통해 로그정보를 분석사이트에 제공하게 된다.

참여자 영역에서는 다양한 센서들이 위치함에 따라 생성되는 로그 정보들이 서로 다른 형식으로 발생되게 되는데 다양한 형식에 대한 전처리 과정을 수행할 수 있도록 트렌드 분석사이트에서는 이들 로그정보를 공통화된 포맷으로 변경하는 도구를 제공하고 있으며 DShiled CVT, DeepSight Extractor 등이 대표적이다[12][13]. 또한 로그정보에 포함된 주소정보에 대한 프라이버시 문제를 최소화하기 위해 HTTPS를 이용하거나 별도 구현된 보안프로토콜을 이용하여 정보를 전송하게 된다.

분석영역에서는 참여자 영역에서 전달된 로그정보를 저장하기 위한 로그 수집 DB, 상호연관 분석된 정보를 저장하기 위한 트렌드 데이터베이스 및 히스토리 데이터베이스를 이용하고 분석된 정보를 정보영역에 제공하게 된다.

정보제공 영역은 대부분이 웹에 기반한 서비스를 제공하게 되는데 수집된 로그를 상호연관 분석하여 생성된 TOP 10 리스트 및 공격 위험성에 대한 심각성(Severity)을 분류하여 경보와 관련된 정보를 제공하게 된다.



(그림 1) 글로벌 트렌드 분석모델

2.3 트렌드 분석 분류

글로벌 트렌드 분석을 수행하고 있는 사이트들은

각기 제공하는 정보 및 자료 수집 방법에 따라 크게 IDS 와 같은 침입로그를 분석하여 포트 기반 TOP 10 리스트 형식의 정보를 제공하고 것과 트래픽 기반 네트워크 상황을 파악하는 형태로 구분해 볼 수 있다.

ISC의 경우 하루에 3,000만 건의 이벤트를 처리하는 것으로 알려져 있는데, 이러한 대량의 로그를 얼마나 빠르게 분석하는 것이 글로벌 트렌드 분석의 문제점으로 제기될 수 있다. 또한, 기존 사이트에 대한 트렌드 분석 현황에 대한 분류를 보면 대표적인 트렌드 분석사이트인 ISC의 경우 포트에 기반한 센서 이벤트의 수를 가지고 분석을 수행하게 되는데 포트정보에 기반한 분석의 경우 CVE나 Bugtraq 등에서 제공하는 취약점과의 연계를 시킬 수 없기 때문에 랜덤하게 전파되는 웜의 경우에는 탐지가 용이하지만 특정 목적을 지니고 정교한 전파를 수행하는 웜의 경우에는 포트정보에만 의존해서는 탐지하기 어려운 단점을 가지고 있다.

따라서 트렌드 분석기술에서는 이러한 대량의 로그를 얼마나 빠르게 분석하고 이종 로그정보를 Bugtraq [18]이나 CVE[19]와 같은 공통된 취약점 정보와 상호 연관 시키는 기술이 요구되게 된다.

(표 2) 트렌드 분석 분류

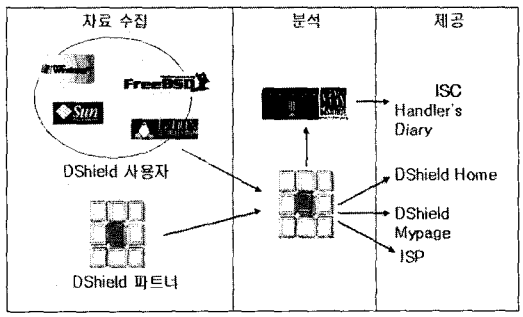
트렌드 분류		자료 수집	대표적인 사이트
포트기반	Top10 리스트 포트기반	센서(IDS, FW)	ISC, DShiled
	Warning서비스 사건연관	센서(IDS, FW)	DeepSight TMS(상용) DeeSight Analyzer
트래픽 기반	트래픽 이상상태	트래픽 정보	CAIDA, InternetPulse

3. 글로벌 트렌드 분석 사이트

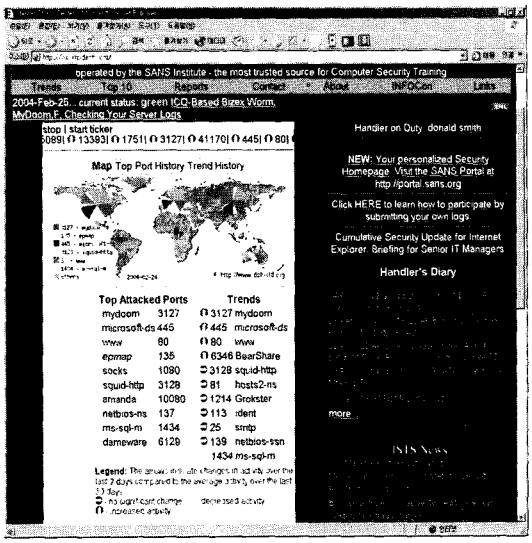
3.1 인터넷 스톰 센터(ISC)

Incidents.org/ISC는 전세계의 3000여개 이상의 침입차단시스템 및 IDS로 부터 수집된 이벤트 데이터를 전달받아 상호연관성을 분석하여, 발생 가능한 인터넷 위협을 조기에 탐지함으로써 보안 경보를 제공하고 분석결과에 대해 보안 공동체에 제공하는 것을 목적으로 하고 있다.

ISC는 그림 2에서와 같이 dshield.org로 부터 수집된 데이터를 제공받아 분석을 수행하게 되는데 ISC 데이터베이스에는 하루에 약 3,000만 건 이상의 이벤트가 전달되고 데이터에 대해 공격 빈도가 높은 포트번호, 공격 빈도가 높은 주소등을 분석하여 분석된 결과를 웹을 통해 그림 3과 같은 형태로 공개하고, Green, Yellow, Orange, Red와 같이 4 단계로 구성되는 인포콘(Infocon) 경보 체계를 운영하고 있다. 또한, 일별 책임자(Handler)를 운영함으로써 주의가 요구되는 위협에 대한 분석자료를 제공하고 있다[4][11].



(그림 2) ISC 트렌드 분석모델



(그림 3) ISC 정보제공 서비스

ISC에서는 포트스캐닝에 대한 트렌드 분석결과를 얻어내기 위해 기본적으로 세가지 테이블을 가지고 있으며 모든 테이블은 표 2에서와 같은 어트리뷰트를 가지고 있다[4].

(표 2) ISC 테이블 어트리뷰트 설명

어트리뷰트	설명
Port	수집된 로그에서 카겟 포트
Sources/Rarget/ Reports	지난 30일간의 서로 다른 근원지/목적지/리포트된 총 개수
Trend	지난 33일간의 데이터와 최근 2일간의 변화율
Error	Trend 계산에 대한 에러
Service	포트번호에 대한 서비스 이름

근원지 테이블은 지정된 포트에 대한 서로 다른 근원지 주소 변화를 보여주게 되며, 목적지 테이블에서는 지정된 포트에 대한 서로 다른 목적지 주소 변화를 관리하며, 리포트 테이블에서는 지정된 포트에 대해 수집된 로그엔트리의 총 개수를 관리하기 위해 사용된다[11].

(표 3) 근원지(Source) 테이블

port	Avg. Sources/Day	Current Sources	Trend	error	service
3127	203	16957	5.738083	0.136116	mydoom
1027	506	1715	2.534618	0.097590	icq
1080	502	1296	2.261827	0.101388	socks

(표 4) 목적지(Target) 테이블

port	Avg. Targets/Day	Current Sources	Trend	error	service
3127	2191	173943	5.738083	4.869053	mydoom
1027	9003	33277	1.802253	0.015215	squid-http
1080	19949	56408	1.534352	0.010550	SubSeven

(표 5) 리포트(Report) 테이블

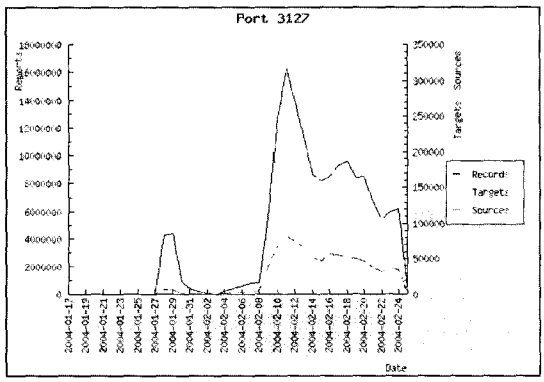
port	Avg. Targets/Day	Current Sources	Trend	error	service
3127	52866	3167387	4.801898	0.006251	mydoom
1080	4674	336778	2.683656	0.007036	socks
3128	28240	198656	2.659825	0.009065	squid-http

테이블에서 trend(t) 값과 error(terr) 값에 대한 계산 방식은 다음과 같다.

$$s = R/r$$
$$t = \ln((r_p/R_p)\ s)$$
$$terr = sqrt(s/r_p + s/R_p)$$

R = 모든 리포트 수
r = 최근 2일간의 리포트 수
R_p = 특정 포트(p)에 대한 모든 리포트 수
r_p = 특정 포트(p)에 대한 최근 2일간의 리포트 수

이와 같이 계산된 trend 값은 하루 단위로 계산되어 그림 4와 같이 각 포트별 증감 변화율을 확인할 수 있게 된다.

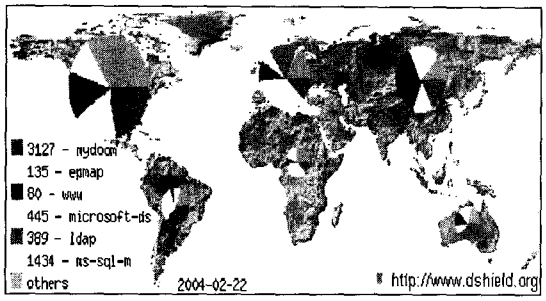


(그림 4) 포트 트렌드 분석 그래프

3.2 DShield

DShiled.org에서는 인터넷에서 발생하는 공격상황에 대한 데이터를 수집하여 공격상황에 대한 트렌드를

찾아내고 더 발전된 형태의 침입차단시스템 규칙을 마련하는 것을 목적으로 한다[12]. DShild에서는 포트에 기반한 근원지, 목적지, 프로토콜 정보를 수집하여 그림 5와 같이 탐지된 로그의 포트정보와 지역정보를 연계하여 분석결과를 제공하며, 표 6과 같은 분석결과를 제공한다.



(그림 5) 지역별 포트 발생 빈도 그래프

(표 6) ISC 테이블 어트리뷰트 설명

제공정보	설 명
Top 10 Most Wanted	DShield DB에 따라 Top 10 공격자 정보
Top 10 Port	Top 10 확인된 포트
Port Report	30일간의 포트에 대한 리포트
IP Info	IP 어드레스에 대한 정보
Subnet Report	서브넷 단위에 대한 최근 요약정보
Block List	IP 주소 블랙 리스트

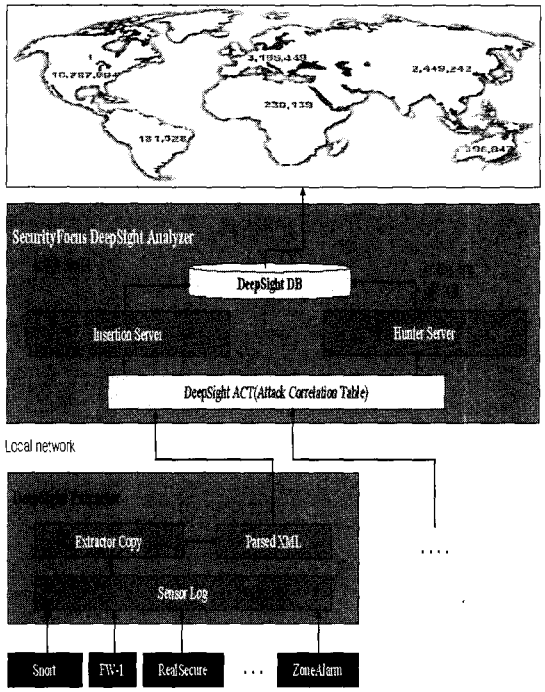
Dshield에서는 참여자 영역의 센서정보를 공통 포맷으로 전달받기 위하여 DShiled CVT와 같은 클라이언트 프로그램을 제공하고 센서로그 정보를 표 7과 같이 공통된 로그 형식으로 변형하여 수집한다. 공통 로그 형식은 날짜 및 시간정보, Author 필드에는 정보를 제공하는 등록된 사용자 ID, count 필드는 제출되는 로그의 수, IP 주소 정보와 필드 정보를 차례로 의미하고 있다. 이와 같이 DShiled에서는 포트에 기반한 로그를 분석할 수 있으며 Author 정보를 통해 사전에 등록된 GMT 존 정보를 이용하여 지역정보와 연관된 결과를 제공할 수 있다.

(표 7) DShiled 공통 로그 형식

Date	2004-02-21
Time(GMT)	01 : 45 : 54
Author	0
Count	1
Source IP Source Port	192.168.239.001 1254
Destination IP	192.168.239.016
Destination Port	139
Protocol	6
Flag	S

3.3 DeepShight Analyzer

DeepSight는 시큐리티포커스에서 운영하고 있는 트렌드 분석사이트로 19,000 이상의 참여자로부터 데이터를 수집 분석하고 있다[13]. DeepSight 구조는 그림 6과 같이 Extractor 프로그램을 통해 참여자 네트워크

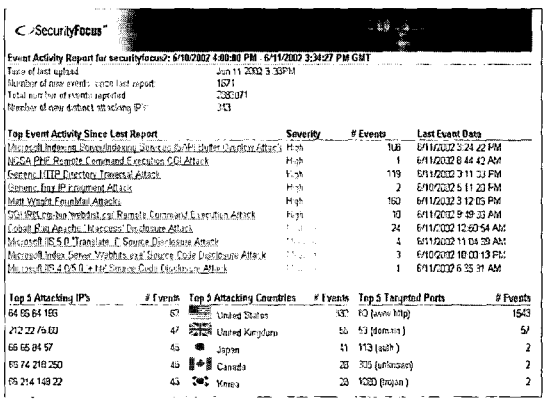


(그림 6) DeepSight 트렌드 분석 모델

의 센서 로그를 공통 형식으로 변환하여 XML 형식으로 데이터를 구성하게 된다. 생성된 로그 XML 파일은 DeepSight Analyzer로 전달되고 Insertion 서버와 Hunter 서버를 통해 DeepSight DB에 저장되게 된다. Insertion 서버에서는 전달된 데이터의 적합성을 검증함으로써 잘못 구성된 레코드를 삭제하는 과정을 수행한 다음 데이터베이스에 레코드를 추가하는 기능을 수행하게 되며, Hunter 서버는 로그정보에 포함된 IP 주소에 대한 호스트 이름과 ISP를 식별하여 데이터베이스에 추가하는 역할을 수행하게 된다. 또한, Extrator와 Analyzer의 통신은 사용자 인증 과정과 함께 HTTPS를 통해 암호화된 통신을 통해 전송된다.

DeepSight Analyzer를 통해 수집 분석된 데이터는 서비스 가입자로부터 전달된 데이터에 대한 이벤트 유형별, 목적지 포트별, 근원지 주소별, 근원지 도메인, 국가별, ISP 별로 통계 정보를 제공하고 있다. 따라서, ISC와 같은 글로벌 트렌드를 제공하지는 않고 있으며 별도의 상용 솔루션인 TMS(Thread Management System)에 가입을 통해 유료 서비스로 경보서비스를 받을 수 있다[7].

DeepSight에서는 ISC와는 달리 정보수집 시 센서로부터 사고 이벤트 ID를 전달받아 SecurityFocus에서 운영중인 BugTraq ID와 상호연관 시킴으로써 서비스 포트에 기반한 Top 10 리스트를 제공하는 것이 아니라 그림 7과 같이 실제 이벤트에 연관된 분석을 수행함으로써 이벤트에 기반한 분석서비스를 제공하는 것이 특징이다.

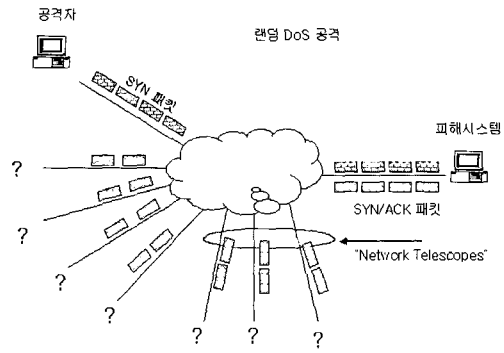


(그림 7) DeepSight 트렌드 분석 결과

3.4 CAIDA

CAIDA는 글로벌 인터넷의 효율적 관리를 목적으로 인터넷 트래픽 측정(Metric)을 위한 연구와 트래픽 데이터의 수집 및 분석, 트래픽 시각화 등을 연구하고 있다[14]. CAIDA에서는 트래픽에 대한 분석 연구를 통해 최근 이슈가 되고 있는 서비스거부공격, 인터넷 웜 등에 대한 분석결과를 발표하고 있는데, [9]에서 Network Telescopes를 통해 원격으로 보안관련 문제점을 분석할 수 있는 방법을 발표하였다.

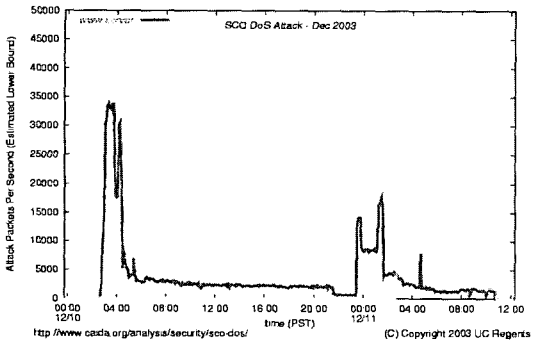
Network Telescopes는 스푸핑된 어드레스로 공격되는 서비스거부 공격과 랜덤하게 전파되는 웜에 감염된 호스트, 호스트 및 포트 스캐닝에 대한 탐지 기능을 수행한다. Network Telescopes에서 서비스거부 공격을 탐지하는 기법은 그림 8에서와 같이 공격자가 랜덤하게 스푸핑된 어드레스를 이용하여 피해 컴퓨터에 연결 패킷(SYN)을 전송하게 되면 피해 컴퓨터에서는 연결응답(SYN/ACK)을 패킷을 스푸핑된 어드레스로 전송하게 된다. 이때 Network Telescopes에서는 랜덤목적지를 가지는 패킷 트래픽을 분석함으로써 DoS 공격이 발생하고 있음을 탐지하게 된다.



(그림 8) Network Telescopes DoS 분석 개념

실제로 2003년 SCO를 대상으로 DoS 공격이 발생한 경우 그림 9에서와 시간대별 공격된 패킷 수를 측정 할 수 있었다.

CAIDA에서는 이와 같이 네트워크 트래픽 분석도구인 AutoFocus, FlowScan 등을 통해 코드레드, 슬래머 웜 등에 대한 트래픽 분석결과를 발표하였다.



(그림 9) SCO DoS 공격 트래픽 분석 결과

3.5 기타 트렌드 분석 사이트

앞에서 언급된 대표적 사이트 이외에도 Internet Pulse[15], MyNetWatchMan[16], Internet Traffic Report [17]와 같은 곳에서도 트렌드 분석을 수행하고 있는데, 대부분이 2장에서 언급된 트렌드 분석 분류 범주에 포함되고 있으며 네트워크 트래픽에 기반한 이상 상태를 감지 기법 및 에이전트 기반의 데이터 수집을 하고 있다.

4. 결론

본 논문에서는 글로벌 사고 트렌드 분석을 수행하는 대표적인 사이트들에서 수행하고 있는 기술에 대한 동향 분석을 수행하였다. 글로벌 트렌드 분석은 분산 IDS에서 사용되는 기술을 기반으로 구성되지만 센서 영역에서 이기종 로그의 상호연관 기술과 함께 전 세계에 분포된 센서로부터 발생되는 방대한 로그를 실시간으로 분석할 수 있는 기술이 요구되는 것을 알 수 있다.

현재의 트렌드 분석은 피해 현황 및 진행상황을 평가할 수 있는 방법으로 활용될 수 있으나 앞으로는 취약성 정보 및 분석기술을 연관시킴으로써 사고트렌드를 예측할 수 있는 기술로 발전할 것으로 판단된다.

참고문헌

[1] CERT Coordination Center, "Overview of Attack Trends", 2002.4

[2] Tim Shimeall, Phil Williams, "Models of Information Security Analysis", CERT Analysis Center

[3] Senthilkumber G Cheetancheri, "Worms : How to stop them ? - An Analysis of various response strategies to computer worms", U.C.DAVIS, 2003

[4] Vinod Yegneswaran, Paul Barford, Johannes Ullrich, "Internet Intrusion: Global Characteristics and Prevalence", SIGMETRICS '03, 2003. 6

[5] Louis Perrochon, Stanford Univercity, "Enlisting Event Patterns for Cyber Battlefield Awareness"

[6] Ed Sjoudis, "The Coming Super Worms", NIAL Conference V, 2003. 7

[7] Symantec DeepSightTM Services, Threat Management System

[8] Cliff C.Zou, Luxin Gao, "Monitoring and Early Warning for Internet Worms", Univ. Masschusetts, Technical Report: TR-CSE-0301

[9] David Moore, "Network Telescopes", USENIX LISA, 2003.10

[10] Todd Herblin, "Trend Center: Accelerating SANS GIAC"

[11] Internet Storm Center, http://isc.incidents.org

[12] DShiled, http://www.dshiled.org

[13] DeepSight, http://anzlyzer.securityfocus.com

[14] CAIDA, http://www.caida.org

[15] Internetpulse, http://www.internetpulse.com.

[16] MynetWatchMan, http://www.mynetwatchman.com

[17] Internet Traffic Report, http://www.internettrafficreport.com

[18] Bugtraq, http://www.securityfocus.com/archive/1

[19] CVE, http://cve.mitre.org

◐ 저 자 소 개 ◑

윤 영 태

1995년 충남대학교 컴퓨터과학과 졸업(학사)
1997년 현대전자 정보시스템 사업본부
1999년 충남대학교 컴퓨터과학과(이학석사)
1999년~현재 국가보안기술연구소 선임연구원
관심분야 : 네트워크 정보보호, 보안운영체제

류 재 철

1988년 Iowa State University(전산학 석사)
1990년 Northwestern Univercity(전산학 박사)
1991년~현재 충남대학교 정보통신공학부 교수
관심분야 : 인터넷 보안

박 상 서

1991년 중앙대학교 전자계산학과(공학사)
1993년 중앙대학교 전자계산학과(공학석사)
1996년~1998년 국방정보체계연구소 선임연구원
1999년~1998년 국방과학연구소 선임연구원
2000년~현재 국가보안기술연구소 선임연구원
관심분야 : 정보전

박 춘 식

한양대학교 전자통신과(석사)
일본 동경공업대학 전기전자공학과(공학박사)
1982년~1999년 한국전자통신연구원 책임연구원
2000년~현재 국가보안기술연구소 책임연구원
관심분야: 암호이론, 통신이론, 정보이론