情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

"종합침해사고대응시스템"에서의 블랙리스트 추출방법과 관리방안 연구

박 광 철*, 최 운 호**, 윤 덕 상***, 임 종 인*

요 약

정보화에 대한 의존도가 심화됨에 따라 사이버상의 테러는 기업과 국가안보를 위협하는 단계에까지 이르렀으나 아직까지 이를 방어하기 위한 정보보호시스템은 침해사고에 대한 정보가 공유되지 못하고 독립되어 운영되고 있는 실정이다. 이에 기업과 국가는 물론 전세계에서 발생되는 실시간 위협 상황에 대해 조기분석과 대응을 위한 정보공유의 필요성이 무엇보다 강조되고 있다. 본 논문에서는 종합침해사고대응시스템에서 침해사고에 대한 실시간 분석 및 대응을 위한 중요자원인 블랙리스트 DB 구축방법과 관리방안을 제시하였다. 인터넷상에서 광범위하고 지속적인 공격을 시도하는 공격 IP정보를 효율적으로 판별하고 추출한 IP를 실시간으로 자동대응할 수 있는 모델을 제안하였으며 사고 시나리오를 통해 검증하였다.

Ⅰ. 서 론

현재의 사이버 공격은 해킹의 파괴성과 바이러스의 전염성이 결합된 '웜 바이러스'의 형태로 더욱 고도화되고 있으며, 서버 및 개인 컴퓨터의 성능이 향상되고 초고속 인터넷망이 널리 보급되면서 웜의 전파속도가 기하급수적으로 증가하고 국가적 규모의 경제적 피해와 사회혼란을 야기시킬 만큼 피해가 대형화 되어가고 있는 추세다.

최근 보안취약점이 발견된 후 이를 악용하는 웜 바이러스가 급격히 증가하고 있다. 지난 2001년 9월 18일 등장해 세계 각국을 공포에 떨게 만든 님다 바이러스는 보안 취약점이 발견된 후 336일 후에 바이러스가 나왔지만 지난해 1월 25일 우리나라 인터넷을 마비시킨 슬래머 바이러스는 SQL서버 취약점 발견 후 185일 만에 등장했다. 또 작년 8월 11일부터 기승을 부린 블래스터 바이러스는 그 주기가 더욱 짧아져 윈도의 보안 취약점이 발견 후 26일밖에 걸리지 않았다. 심지어 지난 3월 20일 처음 나타난 위티 바이러스는 특정 보안제품에 있는 보안 취약점이 발견한 지 불과 이틀 만에 만들어질 만큼 주기가 급속히 짧아지고 있다.

이처럼 주기가 갈수록 빨라지면서 보안 취약점이 발견되자마자 바이러스가 등장해 보안 패치 파일을 설치할 시간적 여유가 없게 돼 피해가 커지는 이른바 제로데이(zero-day)의 가능성이 현실로 나타날 수 있다는 우려마저 제기되면서 이를 효과적으로 방어할 수 있도록 체계정비와 대처방법에 대한 연구가 절실히 요구되고 있다

현재 우리나라의 국가사이버안전활동은 민간·공공 등 국가 전분야에서 사이버위협에 대한 효율적인 사전 예방활동과 사고 발생시 신속한 대처로 피해를 최소화하고자, 국가안전보장회의(NSC)를 정점으로 국가사이버안전센터(NCSC : National Cyber Security Center)를 설립하고, 국가·공공부분은 NCSC, 국방부분은 국방정보전대응센터, 민간부분은 인터넷침해사고대응지원센터를 설립하여 체계적인 대응을 하고 있다.

또한 개별적으로 운영되고 있는 정보보호시스템에 대한 관리와 전문인력으로 구성된 정보보호 조직운영

* 고려대학교 정보보호 대학원(muryo@dreamwiz.com, jilim@korea.ac.kr)
** 금융결제원 금융 ISAC실 정보보호평가팀장 (tiger@kftc.or.kr)
*** 시큐아이닷컴 침해사고대응센타 보안서비스팀 (yoondark@orgio.net)
한국정보보호학회 조기경보시스템연구회 WG04 "침해사고 신고 및 정보공유 표준화" 운영자

을 위해 전사 혹은 전국적인 종합침해사고시스템을 구축하고 운영해야 할 필요성이 제기되고 있다. 이에 본 논문에서는 종합침해사고대응시스템에서 침해사고에 대한 실시간 분석 및 대응을 위한 중요자원인 블랙리스트 DB를 구축하고 관리하는 방안에 대해 연구하였다. 본 논문은 인터넷상에서 광범위하고 지속적인 공격을 시도하는 공격IP 정보를 효율적으로 판별하고 추출된 IP를 실시간으로 자동대응할 수 있는 모델을 제안하는데 목적이 있다. 본 논문의 구성은 제2장에서 종합침해사고대응시스템에 대해 설명하였다. 제3장에서는 블랙리스트의 추출방법 및 관리방안을 제시하고 사고 시나리오를 통해 제안모델을 검증하였다. 제4장에서는 제안된 모델에 대한 장단점과 향후 발전방향에 대해 정리하였다.

Ⅱ. 종합침해사고대응시스템

1. 종합침해사고대응시스템의 이해

현재 사이버위협으로부터 정보자산을 방어하기 위해 다수의 침입차단시스템, 침입탐지시스템, 바이러스백신 등 각종의 정보보호시스템이 설치되고 있다. 그러나 이러한 각종 정보보호시스템은 여러 불법적인 행위에 대한 대응 및 패치방법 등이 서로 공유되지 못하고 각각 기관·기업별로 독립되어 운영되고 있는 실정이다.

이러한 문제점에 대응할 목적으로 ESM(Enterprise Security Management : 기업통합 정보보호 관리시스템)이 개발되었고 기존의 다양한 정보보호 솔루션들을 통합하여 하나의 화면에서 모니터링하는 방법을 제공하게 되었다.

하지만 ESM의 경우에도 너무 많은 이벤트가 발생하므로 이벤트를 일정한 방법으로 필터링하더라도 연관관계나 사고대응 업무를 처리하기에는 불편함이 상존하였다. 이는 더 많은 전문인력의 투입을 요구하였으며, 대부분 인원부족으로 방치되어 사용되고 있다.

또한 ESM은 보안 이벤트간 연계분석, 상관관계 분석을 수행하지만 사용자의 요구를 충분히 반영하지 못하고 있으며 아직도 많은 양의 데이터와 분석근거 부족으로 즉각적인 침해사고 대응, 공격평가, 조기예·경보 등의 대응은 엄두를 내지 못하고 있다.

따라서, 이러한 사이버 상에서의 효율적인 침해대응이 가능한 종합침해사고대응시스템의 필요성이 제기되고 있다. 이는 개인이나 민간의 IT정보, 회사의 정보보호관련 취약성 정보 등을 원격지에서 상호간에 공유함과 동시에 해킹, 바이러스, 사이버테러 등의 침해사고에 종합적으로 대응할 수 있도록 구성된 정보공유 및 분석센터(ISAC : Information Sharing & Analysis Center) 형태의 전사적 종합침해사고대응시스템의 구축을 의미한다.

2. 종합침해사고대응시스템의 구성

종합침해사고대응시스템은 여러 기관 시스템과 연동되어 전국적인 혹은 전사적인 시스템 및 네트워크, 어플리케이션, 인터넷서비스 등과 관련된 정보보호 정보를 수집하고 이를 가공·분석하여 데이터베이스로 관리하도록 한다. 또한 필요한 경우 가공·분석된 정보를 관련기관시스템으로 제공하고 실제 시스템에 대한 공격사고가 예상되는 경우 공격평가를 통한 조기경보를 발령하여 예방활동을 수행할 뿐 아니라 자체적인 정보보호 수단을 구비하는데 목적이 있다.

이러한 목적을 달성하기 위해 종합침해사고대응시

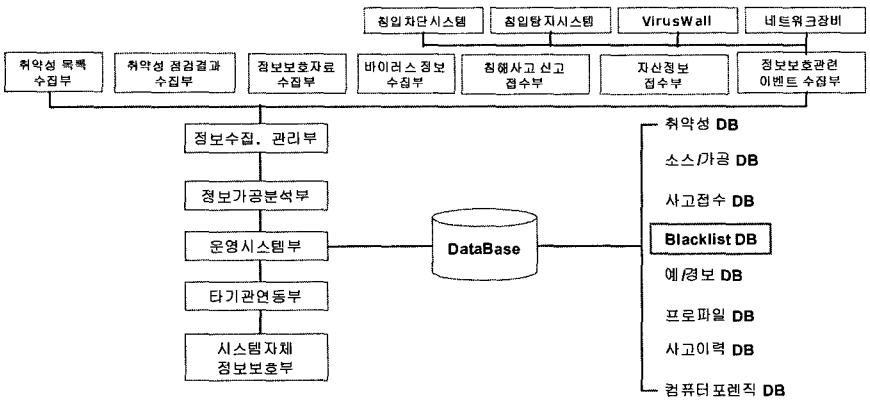


그림 1. 종합침해사고대응시스템의 구성

스템은 보호대상이 되는 컴퓨터시스템 및 네트워크, 어플리케이션, 인터넷 서비스 등과 관련된 보안정보를 수집하고 원시 데이터를 저장하는 정보수집관리부와 분석알고리즘을 이용하여 수집된 보안정보를 가공 및 분석하고 분석결과를 저장·관리하는 정보가공분석부, 가공분석된 보안정보를 하나이상의 보호대상 시스템으로 전달하는 정보공유·검색·전파부, 필요한 보안정보를 소정 형식으로 출력하는 디스플레이부를 포함한 운영시스템부, 시스템 자체의 정보보호를 위한 시스템 자체 정보보호부, 취약성 정보를 저장하는 취약성 데이터베이스부, 외부 시스템과의 신뢰성 있는 정보공유를 위한 타기관 연동부를 포함한다.

본 논문에서는 종합 침해사고 대응방법을 구현하는데 필요한 각종 정보를 종류별로 저장하고 있는 데이터베이스부에서 침해사고 정보 중 상습적으로 발생하는 이벤트를 선별·저장하는 blacklist DB에 대해 연구될 것이다. 블랙리스트 DB는 취약성 목록 및 침해사고 정보중 동일한 공격기법, 비슷한 유형, 일정기간 일정 횟수 이상의 반복공격, 동일ISP, 공격대상 Port의 일치 등의 기준을 적용하여 분석하고 주요공격기법 및 피해 등을 고려해 심각한 침해사고 또는 취약성과 관련된 정보를 선별·저장한다.

Ⅲ. 블랙리스트 추출방법과 관리방안

1. 블랙리스트의 개념 및 관리 필요성

인터넷에서 어떠한 공격이 발생하고 있는지, 어떤 새로운 공격이 나타났는지, 또는 이러한 공격이 자신의 사이트에 얼마나 위협적인지 등에 대한 정보는 실시간으로 제공되어야 한다.

지금까지의 보안 시스템은 "소 잃고 외양간 고치기" 식의 사고대응 방법을 제공하고 있다. 항상 새로운 공격이 널리 확산되고 나서야, 이에 대응하는 방법이 제공되고 있는 실정이다. 이를 극복하기 위해서는 현재 인터넷에서 어떠한 공격이 발생하고 있는지, 어떤 새로운 공격이 나타나고 있는지 등에 대한 정보를 실시간으로 분석 할 수 있어야 한다.

블랙리스트는 각각의 로그수집 에이전트에서 탐지한 공격시도 정보를 실시간으로 수집하여 종합적으로 분석함으로써 새로운 공격이 널리 확산되기 이전에 보다 빠른 대응을 할 수 있도록 하는데 목적이 있다.

인터넷 상에서 광범위하고 지속적인 공격을 시도하는 공격 IP정보를 수집하고 이를 분석하여 각각의 유관기관과 정보공유를 하게 되며 기관은 통지된 정보를 근거로 Firewall 등에서 미리 공격자를 차단함으로 인터넷 상의 실시간 위협에 대응할 수 있다.

2. 블랙리스트 추출방법

2.1 정보수집 모델

블랙리스트 추출을 위해 최우선의 선결과제는 얼마나 신뢰할 수 있는 데이터를 실시간으로 수집할 수 있느냐의 문제이다. 각종 로그수집 Agent로부터의 정보는 가공·분석을 위해 신뢰할 수 있는 수준이어야 하며, 분석에 필요한 최적의 정보만을 위해 정규화되고 축약되어 한다.

그림 2는 블랙리스트 작성을 위해 필요한 침해사고 정보의 수집 모델을 도식화 하였다. 각 기관의 침입차단시스템, 침입탐지시스템 등의 보안장비에서 생성되는 로그는 로그수집기를 통해 모아진다. 이기종 시스템 또는 보안장비에 특성에 따라 다양한 형식으로 생

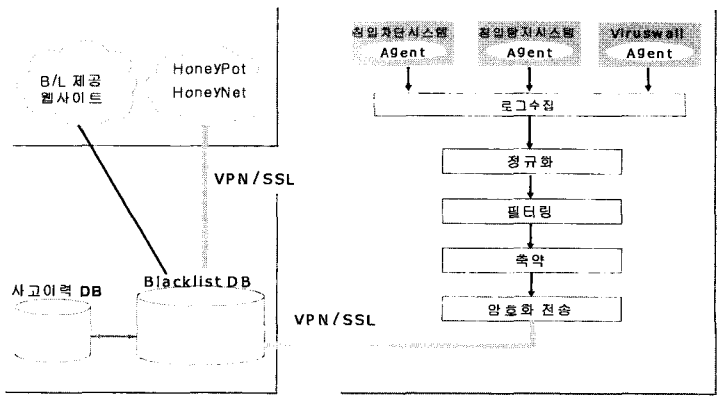


그림 2. 블랙리스트 추출을 위한 정보수집 모델

표 1. 수집로그 정보

Log Name	Full Name	Description
p_code	position code	데이터 수집처를 구별하기 위한 고유코드번호
s_num	sensor number	데이터 수집을 위해 설치된 agent의 고유번호
equipment	equipment name	데이터가 수집되는 장비의 종류(F/W, IDS 등)
date		로그발생 시간
so_ip	source ip address	공격이벤트의 출발지 주소
de_ip	destination ip address	공격이벤트의 목적지 주소
de_port	destination port	목적지 포트
proto	protocol	사용된 프로토콜명. (TCP, UDP, ICMP 등)
in/out	inbound / outbound	inbound(외부->내부), outbound(내부->외부)
action		패킷의 차단/허용여부 판별(drop, allow)
e_name	event name	공격이벤트의 탐지명

성된 로그들은 정규화 과정을 거치게 되며, 분석에 필요한 정보를 위해 필터링(filtering)과정이 수행된다.

또한 중복되는 로그기록에 대한 축약과정을 거쳐 최적의 데이터로 가공되며, 데이터 기밀성 보장을 위해 신뢰할 수 있는 네트워크(VPN/SSL)를 사용하여 수집되어 진다.

객관적이고 정확한 블랙리스트 작성을 위해 침해사고에 대한 정보수집처는 다양화되어져야 한다. SANS, Mynetwatchman 등과 같은 블랙리스트 정보를 제공하는 웹사이트에서 수집로봇을 통해 정보가 수집되며, honeynet 등의 시스템에서 수집되는 정보 또한 블랙리스트 작성에 유용하게 이용될 수 있다. 또한 기존 사고이력에 대한 정보 또한 블랙리스트 작성에 참조된다.

2.2 블랙리스트 추출조건

본 절에서는 각 에이전트로부터 취합되는 raw data로부터 어떻게 의미있는 블랙리스트 정보를 생성하는지에 대한 방법에 대해 고찰해 보고자 한다. 블랙리스트 추출을 위한 기본적으로 수집되어야 할 정보는 표 1과 같이 정의한다. 위에서 획득되어져야할 정보들은 각 단말 에이전트에서 수집된 정보를 정규화하고 필터링하여 필요부분만 추출한 축약된 로그로 무엇보다 정보의 신뢰도와 적시성이 요구된다. 먼저 대량으로 수집되는 공격시도정보로부터 블랙리스트를 추출하기 위한 조건을 다음과 같이 고려해 볼 수 있다.

- □ 탐지되는 이벤트의 수
- □ 수집되는 에이전트의 수
- □ 탐지되는 에이전트수의 증감
- □ 공격이벤트에 대한 신뢰도 적용

수집되는 에이전트 수는 공격지의 범위를 측정하여 타 기관으로의 전파여부를 판단하는 중요 잣대가 될 수 있으며, 탐지되는 에이전트 수의 증감을 통해 공격자의 공격확대범위를 추정할 수 있는 중요 자료가 된다. 하지만 현재 정보보호시스템을 통해 수집되는 로그정보는 100% 블랙리스트를 위한 분석에 적용될 만큼 신뢰도를 갖지 못한다. 특히 IDS 에이전트로부터 수집되는 로그들은 IDS의 false positive한 탐지 이벤트로 인해 정확한 블랙리스트 IP 추출에 장애가 될 수 있다. 이를 개선하기 위해서 수집되는 장비와 이벤트에 따라 신뢰도를 다르게 적용할 필요성이 있다.

표 2는 에이전트에서 수집되는 정보보호장비에 따

표 2. 수집로그에 대한 신뢰도 평가

신뢰도	이벤트 수집장비	판단근거
3	FireWall	실제공격에 대한 차단로그로 공격판단을 위한 신뢰성이 높음
2	VirusWall	탐지 이벤트에 대한 오탐의 가능성이 적음
	IPS	실시간 차단정책으로 인해 탐지룰 적용이 엄격함으로 신뢰성 증대
	IDS	실제 공격가능성이 높은 것으로 정의되어진 공격이벤트
1	IDS	오탐의 가능성이 높은 것으로 정의되어진 공격이벤트

른 신뢰도 적용 순위를 가정해 보았다.

표 2와 같이 다양한 장비에서 수집된 로그정보들에 대해 신뢰도를 판정하고 블랙리스트 판별에 적용함으로 실제 블랙리스트를 정보공유하는 것은 물론 해당 정보를 각 기관에 실시간으로 자동적용 시킬 수 있는 모델을 구현 가능토록 한다.

3. 블랙리스트 대응관리

3.1 블랙리스트에 대한 대응관리

정형화된 추출조건에 의해 생성한 블랙리스트는 다양한 방법으로 활용되고 대응할 수 있다. 본 논문에서는 생성된 블랙리스트를 단순히 정보공유 목적을 위해 웹사이트에 게시하는 수동적인 대응에 그치기보다 시스템적으로 자동적용되어 대응할 수 있는 모델을 제시하고자 한다.

자동적이고 실시간 대응을 위해서는 블랙리스트의 신뢰도가 관건이며, 이를 위해 적용순위를 두었다. 객관적인 적용순위 산출을 위해 다음 사항이 고려된다.

- □ 사고이력 DB와의 연동을 통한 상관관계 분석
- □ 자동수집로봇을 통해 인터넷상에 등재된 블랙리스트 수집

기존 침해사고이력 DB와의 연동은 중복되는 공격지에 대한 다양한 정보를 제공하며, 이에 대한 발빠른 대응을 가능토록 한다. 또한 인터넷상에 등재된 블랙리스트를 자동수집로봇 등을 통해 수집하여 블랙리스트 생성에 참조한다면 설치된 에이전트를 통해 수집되는 정보의 한계를 어느 정도 극복할 수 있을 것이다.

표 3. 가중치 적용모델

적용순위 값	적용 모델
2이상~3	실시간 자동적용
1이상~2미만	자동적용(한시적)
0~1미만	관리자에 의한 수동적용

블랙리스트에 대한 시스템적 대응을 위해 다음과 같은 사항들이 참조된다.

- □ 신뢰도
- □ 단위시간당 총 count수
- □ 단위시간당 탐지된 Agent수
- □ 기존시간 대비 최근시간대의 Agent수의 증감
- □ 사고이력 여부

이를 통해 산출할 수 있는 적용순위에 대한 기준은 다음과 같이 정의한다.

적용순위 값 = 신뢰도(1~3)*가중치+단위시간당 총 count수 등급(1~3)*가중치+단위시간당 탐지된 Agent수 등급(1~3)*가중치+기존시간 대비 최근시간대의 Agent수의 증감 등급(1~3)*가중치+사고이력 등급(1~3)*가중치 (가중치의 총합 = 100%)

4. 사고시나리오에 따른 블랙리스트 생성 및 적용등급 판정

본 절에서는 앞서 정의한 블랙리스트 추출방법이 실제 적용가능한지를 사고 시나리오 작성을 통해 증명하고자 한다. 침해사고에 대한 공격유형은 표 4와 같이 분류하였다. 사고 시나리오는 제시된 모든 공격유

표 4. 침해사고에 대한 공격유형 모델

type	so_ip	de_ip	attack name	service name	description
A	■	■	■		단일공격자에 의한 단일시스템으로의 특정공격수행
B	■	■		■	단일공격자에 의한 단일시스템으로의 특정서비스공격
C	■	■			단일공격자에 의한 단일시스템으로의 공격
D		■	■		단일시스템으로의 특정공격 수행
E	■		■		단일공격자에 의한 특정공격 수행
F	■			■	단일공격자에 의한 특정 서비스의 공격
G		■		■	단일시스템으로의 특정 서비스 공격
H	■				단일공격자에 의한 무작위 공격
I		■			무작위 소스로부터 단일시스템으로의 공격
J			■		무작위 소스로부터 무작위 대상으로의 특정공격

기관코드	Sensor	date	So_IP	So_Port	De_IP	De_Port	Protocol	in/out	action
0001	1	2004-10-18 10:50:00	61.76.160.213	2965	192.168.1.100	4899	tcp	in	drop
0011	45	2004-10-18 10:50:00	61.76.160.213	2967	192.168.2.100	4899	tcp	in	drop
0041	101	2004-10-18 10:50:00	61.76.160.213	2975	192.168.4.100	4899	tcp	in	drop
0032	301	2004-10-18 10:50:00	61.76.160.213	2977	192.168.5.100	4899	tcp	in	drop
0044	405	2004-10-18 10:50:00	61.76.160.213	2981	192.168.7.100	4899	tcp	in	drop

그림 3. 사고시나리오 : 침해사고 로그 1

표 5. 블랙리스트 추출을 위한 적용순위 판정 1

수집장비	이벤트명	신뢰도	count수	Agent수	Agent수의 증감(60분)	사고이력	공격유형
F/W	4899/tcp drop	3	4,500	4	4(10)	2	f

형에 대해 작성되어야 하나 본 절에서는 침해사고의 대표적인 공격유형 3가지를 통해 실제 블랙리스트 추출과정을 도출하고자 한다.

이 사고 시나리오에서는 블랙리스트 추출과 적용순위 산출을 위해 정의된 산출식에서 다음과 같은 가중치를 적용하였다. (여기에서 등급분류와 가중치 계산을 위해 적용되는 값들은 경험에 의해 최적화 될 수 있는 값들로 사용자 정의에 의해 변경 적용될 수 있는 값이다.)

□ 신뢰도
- 등급 : 1,2,3
- 가중치 : 40%

□ 단위시간(5분)당 총 count수
- 등급
  1 : 1~1,000 미만
  2 : 1,000이상~10,000 미만
  3 : 10,000 이상
- 가중치 : 15%

□ 단위시간(5분)당 탐지된 Agent수(총 100개)
- 등급
  1 : 1
  2 : 2~5
  3 : 6 이상
- 가중치 : 15%

□ 기준시간(60분) 대비 최근시간(5분)의 Agent 수의 증감(%)
- 등급
  1 : 10% 이내
  2 : 10~30% 이내
  3 : 30% 이상
- 가중치 : 15%

□ 사고이력 여부(건수)
- 등급
  1 : 1건
  2 : 2~4건 이내
  3 : 5건 이상
- 가중치 : 15%

4.1 사고시나리오에 따른 블랙리스트 생성예 1

단일 공격자는 특정 대역의 전산망을 대상으로 RAdmin Tool 설치시 기본적으로 오픈하는 4899포트를 스캐닝함으로써 RAdmin 프로그램이 운용중인 시스템을 찾고 있다. 해당 공격이벤트는 다수의 기관과 에이전트에서 수집되고 있으며, 수집되는 에이전트의 수가 단위시간 대비 증가(4개) 추세에 있으며 기존에 2번의 사고이력을 가지고 있다.

- 적용순위 산출식 : 적용순위 값 = 신뢰도(1~3)*가중치+단위시간당 총count수 등급(1~3)*가중치+단위시간당 탐지된 Agent수 등급(1~3)*가중치+기존시간 대비 최근시간대의 Agent수의 증감 등급(1~3)*가중치+사고이력 등급(1~3)*가중치=적용순위 (가중치의 총합 = 100%)
- 계산값 : 3*0.4+2*0.15+2*0.15+3*0.15+2*0.15 =2.65
- 적용순위 : 실시간 자동적용

4.2 사고시나리오에 따른 blacklist 생성예 2

웜 바이러스에 감염된 공격자는 특정 대역의 전산망을 대상으로 윈도우 취약점 및 타 웜 바이러스의 감염 후 오픈하는 백도어 포트를 스캐닝하고 있다. 해당 공격이벤트는 단위시간에 하나의 기관의 에이전트에서

기관코드	Sensor	date	So_IP	So_Port	De_IP	De_Port	Protocol	in/out	action
0011	45	2004-10-18 12:15:00	203.236.211.21	3166	192.168.1.100	135	tcp	in	drop
0011	45	2004-10-18 12:15:00	203.236.211.21	3157	192.168.1.100	139	tcp	in	drop
0011	45	2004-10-18 12:15:00	203.236.211.21	2935	192.168.1.100	6129	tcp	in	drop
0011	45	2004-10-18 12:15:00	203.236.211.21	2865	192.168.1.100	1025	tcp	in	drop
0011	45	2004-10-18 12:15:00	203.236.211.21	2410	192.168.2.100	139	tcp	in	drop

그림 4. 사고시나리오 : 침해사고 로그 2

표 6. 블랙리스트 추출을 위한 적용순위 판정 2

수집장비	이벤트명	신뢰도	count수	Agent수	Agent수의 증감(60분)	사고이력	공격유형
F/W	135, 139, 1025, 6129/tcp drop	3	13,455	1	1(10)	0	e

기관코드	Sensor	date	So_IP	So_Port	De_IP	De_Port	attack_Name	in/out
0011	45	2004-10-18 12:15:00	203.236.211.21	3166	192.168.1.100	80	http iis webdav unlock	in
0011	45	2004-10-18 12:15:00	203.236.211.21	3157	192.168.1.100	80	http status.cgi	in
0011	45	2004-10-18 12:15:00	203.236.211.21	2935	192.168.1.100	80	http download.cgi	in
0011	45	2004-10-18 12:15:00	203.236.211.21	2865	192.168.1.100	80	http register.asp	in
0011	45	2004-10-18 12:15:00	203.236.211.21	2410	192.168.2.100	80	tcp syn flooding	in

그림 5. 사고시나리오 : 침해사고 로그 3

표 7. 블랙리스트 추출을 위한 적용순위 판정 3

수집장비	이벤트명	신뢰도	count수	Agent수	Agent수의 증감(60분)	사고이력	공격유형
IDS	http ...	2	2,543	2	2(10)	0	b

수집되고 있다.

- 적용순위 산출식 : 적용순위 값 = 신뢰도(1~3)*가중치+단위시간당 총count수 등급(1~3)*가중치+단위시간당 탐지된 Agent수 등급(1~3)*가중치+기존시간 대비 최근시간대의 Agent수의 증감 등급(1~3)*가중치+사고이력 등급(1~3)*가중치 (가중치의 총합 = 100%)
- 계산값 : 3*0.4+3*0.15+1*0.15+1*0.15+0*0.15=1.95
- 적용순위 : 한시적 자동적용

4.3 사고시나리오에 따른 blacklist 생성예 3

임의의 공격자는 특정 대역의 전산망을 대상으로 웹 서비스의 오픈여부 및 관련 취약점을 scanner tool을 이용하여 탐색하고 있다. 해당 공격이벤트는 한개의 기관과 다수의 에이전트에서 수집되고 있다.

- 적용순위 산출식 : 적용순위 값 = 신뢰도(1~3)*가중치+단위시간당 총count수 등급(1~3)*가중치+단위시간당 탐지된 Agent수 등급(1~3)*가중치+기존시간 대비 최근시간대의 Agent수의 증감 등급(1~3)*가중치+사고이력 등급(1~3)*가중치 (가중치의 총합 = 100%)
- 계산값 : 2*0.4+2*0.15+2*0.15+2*0.15+0*0.15=1.7
- 적용순위 : 한시적 자동적용

Ⅳ. 결론 및 추후 연구방향

현재의 사이버 공격은 웜과 해킹의 특성이 결합되어 고도화되고 있으며, 초고속 인터넷망이 널리 보급되면서 전파속도가 기하급수적으로 증가하고 국가적 규모의 경제적 피해와 사회혼란을 야기시킬 만큼 피해가 대형화 되어가고 있는 추세다.

이에 대응하기 위해 ISAC, CERT 등 다수의 사이버공격 대응기구가 설립되고 있으며, 정보공유 및 공동대응체계 구축을 위해 부단히 노력해 가고 있는

중이다. 하지만 대응조직의 활성화 및 공동대응체계 구축은 초기단계에 머무르고 있는 추세이며 국가차원 또는 전세계에서 발생되는 실시간 위협상황에 대한 조기분석 및 대응의 필요성이 제기되고 있다.

본 논문에서는 자동화된 '종합 침해사고 대응시스템'에서 사이버 침해사고에 대한 조기경보 및 대응을 위해 중요한 구성요소가 될 blacklist DB를 추출하는 방법을 제시하고 이를 활용하는 방안에 대해 시나리오 작성을 통한 새로운 모델을 제안하였다.

이 모델은 네트웍에 연결된 각종 장비의 정보를 기반으로 한 블랙리스트 등의 연동을 통하여, 특정시기에 대량의 트래픽을 발생시키는 사이트 및 공격자 등을 자동적으로 가려내고 차단하는 시스템을 구현하는데 일조할 것이다. 또한 광범위하고 지속적인 공격은 물론 새로운 공격 위협에 대한 실시간 분석 및 대응을 실현하고 침해사고에 대해 자동화된 대응을 가능하게 할 것이다.

하지만 본 논문에서 다룬 블랙리스트 추출방법과 관리방안에 대한 제안은 몇가지의 문제점을 극복해야 할 것이며 이는 추후에 연계될 연구에서 발전시켜 나가야 할 부분이다.

본 논문에서 제안한 신뢰도, 적용순위 산출을 위한 기준설정 값들은 사용자에 의한 임의의 수동설정 값으로 경험적인 수치에 의존하고 있다. 이를 객관적으로 증명할 수 있는 다양한 테스트와 분석연구가 있어야 한다. 또한 IP Spoofing Attack, NAT, DHCP 사용 IP에 대한 대응 및 관리방안에 대해서도 관련 연구가 필요할 것이다.

V. WG 04 소개

한국조기경보포럼의 WG 04는 침해사고 신고 및 정보공유 표준화를 담당하는 분과이다. 이 분과에서는 서로 다른 기술수준을 보유하고 있는 각 기관의 정보보호 담당자들 사이에 표준화된 정보공유 채널을 통해 전문가와 비전문가들이 자유롭게 침해정보를 공유하고 사회적으로 큰 영향을 줄 수 있는 침해사고 징후를 조기에 탐지, 공유토록 하여 상호 대응능력을 향상 시키고 더 나아가 범국가적인 표준 침해사고 대응시스템을 디자인 하는 분과이다. 현재까지 미국이나 유럽 등 선진화된 침해사고 공유시스템을 운영하고 있는 국가들의 수준 및 대응체계를 분석하고, 국내의 침해사고 대응시스템의 실체파악을 통해 국내 환경에 맞는 침해사고 공유 모델을 연구하고 있다.

⊙ 연구 방향

- 국내 침해사고 신고 및 대응 체계의 문제점 분석 및 개선방향 연구
- 해외 선진 국가들의 침해사고 대응체계 벤치마킹
- 국가기관 및 산학연을 연계한 범국가적 침해사고 대응모델 디자인
- 익명성이 보장된 침해사고 신고체계 연구
- 표준화된 침해사고 분석용 데이터베이스 구축
- 기타 침해사고 대응체계와 관련된 논문 및 최근 동향 연구

⊙ 분과 운영

- 월 1회 오프라인 모임 및 온라인 모임을 갖고 연구 주제를 토론
- 희망 과제를 부여하고 자유롭게 발표
- 각종 세미나를 통한 정기연구 결과 발표

참 고 문 헌

[1] 안정모, 조진성, 정병수, "대규모 네트워크 환경을 위한 통합 침입탐지 시스템", 한국통신학회, 2004.7.

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

[3] 손우용, 송정길, "통합보안 관리시스템의 침입탐지 및 대응을 위한 보안 정책 모델", 한국컴퓨터정보학회, 2004.6.

[4] 김현상, 이상진, 최운호, 임종인 "자동화된 침해사고 대응시스템에서의 디지털 증거 수집", 한국정보보호학회 하계학술대회, 2004.

[5] 박종성, 최운호, 문종섭, 손태식, "자동화된 침해사고대응시스템에서의 네트웍 포렌식 정보에 대한 정의", 한국정보보호학회 논문지, 2004.7

[6] 전규삼, 최운호,"자동화된 침해대응시스템에서 Web을 기반으로한 로봇에이전트에 대한 연구", 한국정보보호학회 하계학술대회, 2004.

[7] 국가정보보호백서, 국가정보원, 2004.

[8] 침해사고대응팀 구축·운영 지침서, 한국정보보호진흥원, 2004.

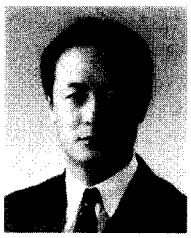
[9] Steven R. Snapp, James Brentano, Gihan V. Dias, "DIDS(Distributed Intrusion Detection System) ? Motivation, Architecture, and An Early Prototype,"

Proceedings of the 14th National Computer Security Conference, 1991.
[10] 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.
[11] Y. Zhang and V. Paxson, "Detecting Stepping Stones," Proceedings of 9th USENIX Security Symposium, Aug. 2000.
[12] D. Schnackenberg, K. Djahandari, and D. Sterene, "Infrastructure for Intrusion Detection and Response," Proceedings of DISCEX, Jan. 2000.
[13] 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.

〈著 者 紹 介〉

박 광 철 (Kwang-Chul Park)

2004년 : 고려대학교 정보보호 대학원 졸업(석사)
〈관심분야〉 조기경보, 블랙리스트 구성 및 관리



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

윤 덕 상 (Deok-Sang Yoon)
정회원

1989년 2월 : 고려대학교 수학과 졸업
2005년 2월 : 고려대학교 정보보호대학원 정보보호학과 졸업
1991년 7월~2000년 3월 : 삼성SDS 그룹IS실 개발자, 보안관리자
2000년 4월~현재 : 시큐아이닷컴 침해사고대응센타 팀장
〈관심분야〉 정보보호, 컴퓨터 네트워킹

임 종 인 (Jong-in Lim)

1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1986년 3월~2001년 1월 : 고려대학교 자연과학대학 정교수
2001년 2월~현재 : 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
〈관심분야〉 정보보호 이론, 정보보호 정책