해커의 공격에 대한 실시간 보안공조시스템 연구

박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study of Real Time Security Cooperation System Regarding Hacker's Attack

Dea-Woo Park*

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

E-mail : *prof1@paran.com

요 약

중국의 해커가 제3국으로 한국IP를 우회 접속하여 전자상거래사이트를 해킹하여, 대포계좌로 금융피해를 입히는 한 침해사고가 났었다. 7.7 DDoS공격은 국가의 주요사이트를 마비시킨 해커의 공격사건이었다. 본 논문에서는 해커의 침해사고와 DDoS공격에 취약점 분석을 한다. 해커의 공격에 대한 전조 증상 및 공격 연관성 분석을 통하여 실시간으로 Red, Orange, Yellow, Green에 속하는 위험등급을 나눈다. 해커에 대한 블랙리스트를 작성하여 실시간으로 공격을 차단 방어하는 보안공조시스템을 연구한다. 침해사고 후 패킷에 대한 역추적과 탐지를 통해 포렌식 자료를 생성하고 법정에서 책임소재의 증거로 확정하는 연구를 하여 국가 침해사고 대응과 포렌식 기술 발전에 기여한다.

ABSTRACT

Chinese hackers hack the e-commerce site by bypass South Korea IP to connect to the third country, finance damaging a violation incident that fake account. 7.7.DDoS attack was the case of a hacker attack that paralyzed the country's main site. In this paper, the analysis is about vulnerabilities that breaches by hackers and DDoS attacks. Hacker's attacks and attacks on the sign of correlation analysis is share the risk rating for in real time, Red, Orange, Yellow, Green. Create a blacklist of hackers and real-time attack will be studied security and air conditioning systems that attacks and defend. By studying generate forensic data and confirmed in court as evidence of accountability through IP traceback and detection about packet after Incident, contribute to the national incident response and development of forensic techniques.

키워드

Hacking, Vulnerability, DDoS, Blacklist, Forensic

Ⅰ. 서 론

2009년 2월 25일 해킹에 의한 옥션 이용자 1천 81만명의 개인정보가 유출되고, 2009년 7월 7일 청와대 등 주요 정보기관 및 금융기관 인터넷 사이트가 해커들의 DDoS 공격[1]에 의해 마비되고, SQL Injection 공격, XSS 등 가장 많은 Web 공격[2] 등 사이버테러의 발생으로 국가 차원의 사이버 보안에 대한 중요성이 대두된다.

특히 국가 IT 인프라에 대한 DDoS 공격에 대해서는 종합적인 실시간 보안 방어 시스템이 미흡하여, 실시간으로 공격해 오는 DDoS 공격의 대응에는 어려움이 있다. DDoS 공격을 방어하기 위한 침해사고대응센터의 경우는 실시간 공격이벤트정보 확보와 원격 공격자에 대한 신속한 원인분석이 어려워 결과적으로 실시간 방어에 어려움이 있다.

DDoS 공격을 방어하고 역추적하기 위해서는 빅팀서버(Victim Server)[3]와 연결된 네트워크 단에서의 실시간 DDoS 공격을 방어하면서 조기경보를 관련 네트워크 시스템에 전달하여야 하고, 실시간 방어도 공조를 통한 유기적 시스템으로 해야 한다. 즉 DDoS 공격을 유발시키는 좀비 PC(Zombi PC)[4] 뿐만 아니라, 중간경유지를 거치면서 위조된 IP주소[5]를 사용하는 원격지 해커들의 소재지를 파악하여 블랙리스트[6]에 올리고, 보안 정책 수정하여 실시간 방어시스템을 구축하지 않으면, 해커들은 새로운 유형의 사이버 공격을 개발하여 DDoS 공격을 할 것으로 예상된다.

따라서 본 논문에서는 지능화되고 다양화되고

있는 DDoS 공격에 대한 네트워크 장비 및 보안 장비를 연구하고, DDoS 공격이벤트에 대한 분석을 실시간으로 실시하여 원격지에서 조정하는 해커들의 소재지를 파악하여 블랙리스트에 올리고, 보안 정책 수정하여 실시간 방어시스템을 구축하는 연구를 한다.

Ⅱ. 본 론

2.1. DDoS 공격 등 침해사례

사이버테러 유형이 점차 복합화, 지능화, 대형화되며, 공격의 결과 침해 피해 대상도 개인과 기업으로 확대되는 추세이다[7]. 최근 그림 1처럼 중국으로부터 해커가 제3국으로 우회접속을 하여 한국IP로 접속하여 쇼핑몰 219개 사이트에 대한 해킹을 하여 대포통장을 유통하여 금융 사고를 일으킨 침해사고가 났었다. 표 1은 침해사고 주요 현황이다.

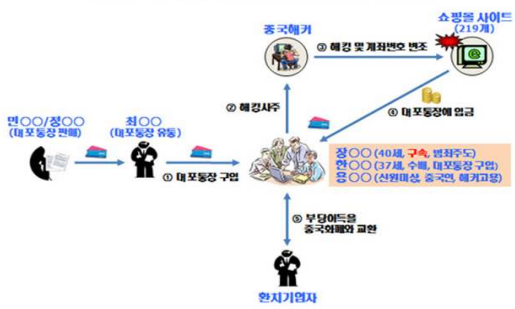

그림 1. 전자상거래 침해사고사례

표 1. 침해사고 주요 현황

일자	침해사고 주요 현황
2003. 1.25.	"1.25 인터넷 대란"으로 '슬래머 웜' 바이러스에 의해 전 세계 7만 5천대 및 국내 8천 800여대의 컴퓨터가 감염
2009. 2.5.	해킹에 의해 옥션 이용자 1천 81만 명의 개인정보 유출
2009. 7.7.	청와대 등 주요기관 웹사이트와 일부 포털 등이 DDoS 공격을 받아 다운

2.2. 보안시스템 기술 개발 현황

차세대 네트워크 보안은 단순 모니터링 및 보안정책을 적용하는 형태에서 네트워크 전체를 보안 제어 영역으로 확장 될 전망이다.

보안관리 시스템(Security Management System)의 발전 방향도 단순한 보안 장비(Security Device)에만 그치지 않고 IT 인프라, 애플리케이션, 트랜잭션, 비즈니스에 대한 통합 관리를 지향한다[8].

관리 대상과 범위에 따라 기존 관제장비로는 표 2와 같이 SMS(System Management), NMS(N-etwork Management), ESM(Enterprise Security Management)[9]이 대표적이며, 현재 ESM장비가 NMS/SMS의 주요기능을 흡수함과 더불어 TMS(Threat Management System) 및 UTM(Unified Threat Management)[10] 등과 같은 보안솔루션과 결합이 진행 중이다.

표 2. SMS, NMS, ESM 시스템 비교

분류	SMS	NMS	ESM
관리 대상	시스템	네트워크	네트워크, 시스템, 보안장비
관리 목표	가용성 확보, 성능관리, 장애관리 등	가용성, 트래픽 관리, 장애관리 등	위협요소 탐지 및 대응을 위한 망 보안체제 구축 등
주요 특징	가용성 확보, 배포관리, 업무효율성과 생산성 증대	트래픽 모니터링, SNMP 기반의 장애, 성능관리	발생 보안이벤트를 연계 분석 및 대응기능, SMS, NMS 등과 일부 기능이 중복

또한, 네트워크 보안 제품은 Firewall, IPS(Intrusion Prevention System), VPN(Virtual Private Network)[11]이 전용 기기로 공급되다가 DPI(Deep Packet Inspection) 기술에 기반 한다. 최근에는 방화벽, 안티바이러스 소프트웨어, 콘텐츠 필터링 및 스팸 필터 등 기능이 하나의 패키지로 통합되어 있는 통합 보안 시스템인 UTM(Unified Threat Management)으로 진화하고 있다.

Ⅲ. 해커의 공격과 보안공조시스템 분석

3.1. 해커에 의한 DDoS 공격과 침해사고 분석

좀비 PC와 중간감염자들로 부터 DDoS 공격을 유발시키는 침해사고 뿐만 아니라, 중간경유지를 거치면서 위조된 IP주소를 사용하는 해커들을 블랙리스트에 올리고, Real IP 역추적을 하기위한 실시간 보안공조시스템을 구축하려면 침해사고와 DDoS 공격에 대한 분석이 필요하다.

표 3에서 2009년과 2010년의 사고에서 해커의 공격에 의한 해킹으로 인한 침해사고가 많음을 보여주고 있다.

표 3. 침해사고 통계 요약

구분	2009년 총계	2010			2010 총계
		1	2	3	
웜 바이러스	10,395	932	1,302	1,085	3,319
해킹신고 처리	21,230	898	1,076	1,053	3,027
스팸 릴레이	10,148	154	317	222	693
피싱 경유지	988	78	106	116	300

단순 침입시도	2,743	232	230	345	807
기타해킹	3.,031	223	233	267	723
홈페이지 변조	4,320	211	190	103	504
악성 봇(Bot)	1.0%	0.6%	0.6%	0.7%	0.6%

3.2. 실시간 보안공조 시스템 기능 분석

실시간 보안공조시스템을 구성하려면 다음과 같은 기능이 필요하다.

- 해커의 공격 근원지/숙주사이트/좀비PC 등의 블랙리스트 생성과 검색 기술 확보(잠재적 공격의 근원지/숙주사이트/좀비PC 관련 정보 수집/정규화/검색/저장, 악성코드의 유포경로 확보 및 실시간 검사 및 모니터링을 통한 악성코드 실행 상황 분석, 속성정보별 연관성 분석을 통한 네트워크 보안상황을 인지).
- 침해사고 대응 전문가들 사이에 실시간 공격 정보를 공유하는 프레임워크 구축(국가 간, 지역 간, 행정구역별로 협력기반으로 정보의 공유와 정보프레임워크 모델링, 실시간 공격 정보의 공유를 위한 표준 데이터 모델링 필요).
- 정보공유 프레임워크 기반의 데이터 교환 포맷 및 전달 프로토콜(침해사고에 대한 정보의 수집/정규화/검색/저장, 공격 정보의 공유와 객체 기술, 공격 정보 교환 형식의 국내표준 제정, 안전한 연결기반의 정보를 전달하는 프로토콜 구축).
- 정보공유 프레임워크 기반의 통합보안제어시스템 구축(공격 보안 이벤트 및 네트워크 이벤트간의 공격 정보의 연동 기술, 실시간 공격 정보공유를 위한 시스템 연동 및 적합성 검증. 응용 가능성의 영역 정의 및 시범 서비스 개발 및 운용).

Ⅳ. 실시간 보안공조시스템 구성

4.1. 실시간 보안공조시스템 네트워크 구성

그림 2처럼 인터넷과 내부 네트워크 사이에 설치된 Firewall과 VPN이 있고, DMZ에 보안공조시스템(패킷수집서버 포함)을 설치한다.

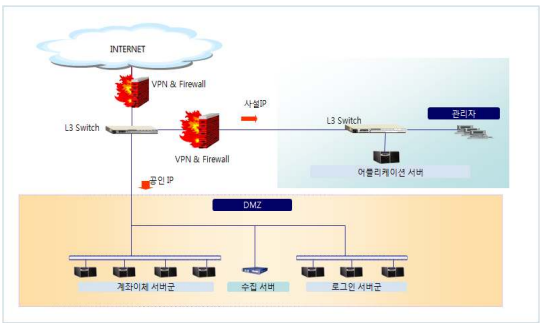

그림 2. 실시간 보안공조시스템 네트워크 구성

내부 네트워크 Firewall 안쪽에 어플리케이션과 관리자모듈을 설치한다.

4.2. 실시간 보안공조시스템 프로세스 구성

해커의 공격에 대한 외부 네트워크 보안 연계 시스템들과의 실시간 보안공조시스템에 관한 프로세스는 그림 3과 같다.

네트워크 내외부에서 시스템정보, 식별자, IP정보, 브라우저 정보, 유동 IP지역정보 등의 정보를 수집한다. 정보 저장은 Web과 WAS서버를 통한 정보는 수집서버에서 실행하고 로그기록과 블랙리스트 등의 통계를 작성한다.

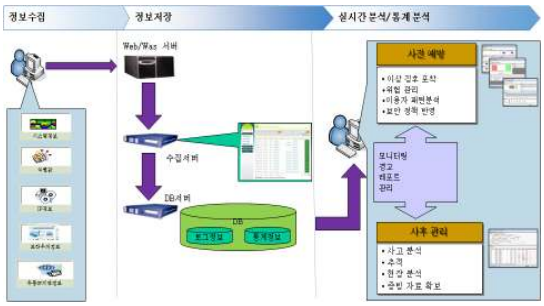

그림 3. 보안공조시스템 프로세스 구성

실시간 보안공조시스템은 수집된 접속자의 IP, port, 서비스, Application 정보를 수집하고, 수집된 정보의 분석 통계 등을 통하여 발생할 수 있는 위협 요소를 사전에 분석 포착하여, Red, Orange, Yellow 위험등급을 나누어 실시간으로 전파 및 방어를 통한 대응을 한다. Yellow 위험등급이상은 실시간 분석을 실시하고, Red등급은 침해사고에 대한 실시간 대응을 먼저 수행하면서 패킷을 분석하여, 관련 기관의 보안시스템에 대한 보안정책을 전파한다.

4.3. 실시간 보안공조시스템 역추적 구성

SQL Injection 공격, XSS 등 가장 많은 Web 공격의 경우 그림 4처럼 웹 접속자 Real IP획득을 위한 유해 게시물 처리를 이용한 보안공조시스템 역추적 구성을 하였다.

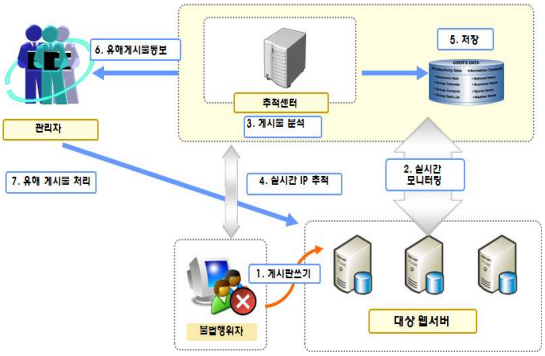

그림 4. 보안공조시스템 역추적 구성

웹페이지 및 게시판 페이지에 추적시스템의 Agent를 설치하여 Real IP 추적 및 게시판에 대한 글쓰기를 탐지하여 추적한다.

4.4 포렌식 자료 생성

DDoS 공격의 숙주자나 좀비 PC로 감염된 PC가 웹 접속자로 패킷을 분석해 보면 실제 공격자인 해커의 추적이 어렵다. 일단 숙주자나 좀비 PC를 압수 수색 후에 사용자에게 사인을 하도록 하고, 해시함수를 적용하여 복사본을 만든다. 증거 시스템은 휘발성과 비휘발성 데이터 수집을 통해 로그 원본성을 입증하고 EnCase나, DEAS Forensic Tool을 이용하여 증거자료의 합법성을 확보 한 후에, 압수자 입회하에 분석을 하고 원 자료를 찾아내어 감염시킨 악성 코드에 대한 출발지 주소와 응용계층에서의 활동 등 감염 원인에 대한 분석을 하여야 한다.

또한 공격자는 DDoS 공격의 성공 여부를 파악하기 위해 실제로 정상적인 상태에서 공격대상에 접속 하여 가용성을 확인해야 하므로, 로그 기록과 분석하여 유사도를 매치시키면서 공격자를 찾아낸다. 이 경우에도 포렌식 수사 절차를 준수하고 법정에서 증거로 인정을 받을 수 있도록 무결성 검증 매뉴얼에 의한 포렌식 분석 작업을 실시하고 보고서를 법정에 제출한다.

Ⅴ. 결 론

본 논문에서는 IT 인프라에 해커에 의한 DDoS 공격과 침해사고를 분석하고 보안공조 시스템을 구축하기 위한 종합적인 실시간 보안 방어 시스템에 해커의 공격에 대한 전조 증상 및 공격 연관성을 분석하고, 실시간 보안공조시스템 기능을 분석하였다. 이를 대응하기 위해 인터넷과 내부 네트워크 사이에 설치된 Firewall과 VPN이 있고, DMZ에 보안공조시스템(패킷수집서버 포함)을 설치하고 수집된 정보의 분석 통계 등을 통하여 발생할 수 있는 위협 요소를 사전에 분석 포착하여, Red, Orange, Yellow 위험등급을 나누어 실시간으로 전파 및 방어를 통한 대응이 가능한 실시간 보안공조시스템 프로세스를 구성하고 웹 접속자 Real IP획득을 위한 유해 게시물 처리를 이용한 보안공조시스템 역추적 구성을 하였다.

향후 연구로 실시간 보안공조 시스템을 사용하여 Red, Orange, Yellow 위험등급을 나눈 보안정책에 대한 세부적인 사항과 그에 맞는 각 기관별 실시간 고역대응에 관한 매뉴얼과 보안 가이드라인에 대한 연구가 필요하다.

참고문헌

[1] 이형우, "DDoS 해킹 공격 근원지 역추적 기술", 한국정보보호학회, 제 3권 제 5호, pp.104-112, 2003. 10.

[2] K. K. Mookhey, "Nilesh Burghate, Detection of SQL Injection and Cross-site Scripting Attacks",http://www.securityfocus.com/infocus/1768

[3] 박대우, 서정만, "TCP/IP 공격에 대한 보안 방법 연구", 한국컴퓨터정보학회, 제 10권 제 5호, pp.217-226, 2005. 11.

[4] 안성호, 강창구, 최용락, "Agent와 협력을 통한 DDoS 공격대응 메커니즘", 한국인터넷정보학회, pp.333~336, 2009. 10.

[5] “Reducing the Energy Consumption of Ethernet with Adaptive Link Rate(ALR)”, Chamara Gunaratne, IEEE Transaction on computers, Vol. 57, No. 4, 2008.

[6] 이인희, 박대우, "VoIP 취약점에 대한 스팸 공격과 보안에 관한 연구", 한국컴퓨터정보학회지, 제 14권 제 2호, pp.215-224, 2006. 12.

[7] 최정호, "사이버테러리즘의 변천방향과 한국의 대응", 국방안보학술회의, pp.155-172, 2008. 4.

[8] 박대우, 임승린, "해커의 공격에 대한 지능적 연계 침입방지시스템의 연구", 한국컴퓨터정보학회, 제 11권 제 2호, pp.351-360, 2006. 5.

[9] 정연서, 류걸우, 장종수, "네트워크 보안을 위한 ESM 기술 동향", ETRI, 2001.

[10] McAfee. “White Paper_Host and Network Intrusion Prevention", http://www.mcafee.com/us/local_content/white_papers/wp_host_nip.pdf, February, 2005.

[11] 신대규, "DDoS 대응 패러다임의 변화", 한국정보보호진흥원, 2009.