DNS 정보 검색 연동 기법을 이용한 침해 사고 예방 시스템 설계

김광섭* · 박영길** · 노승환*** · 김봉현****

Design of Infringement Accidents Preventing System Using DNS Information Retrieval Integration Method

Kwang-sup Kim* · Young-Gil Park** · Soong-hwan Ro*** · Bong-hyun Kim****

이 논문은 2012년도 경남대학교 학술연구장려금 지원에 의한 것임

요 약

최근 정보보안의 흐름은 사용자 중심으로 변화가 되고 있다. 이는 사용자가 인터넷을 하는 동안 정상적 및 비정상적으로 유입되는 유해한 파일에 의한 보안사고가 대부분이라는 의미이다. 따라서 본 논문에서는 DNS에 대한 신뢰성을 향상시키고 DNS를 이용한 시스템 제어를 통해 침해사고를 사전에 예방할 수 있는 보안 시스템을 설계하고자 한다. 즉 사용자 중심의 정보보안 시스템으로 사용자 컴퓨터에 감염된 유해 파일이 임의로 사이트를 접속하는 행위에 대하여 차단할 수 있는 방법을 제안하고자 한다.

ABSTRACT

Recently the flow of information security has become a user-centered change. This is mostly breach of security by the normal and abnormal entering harmful files during user internet. Therefore, we would like to design security system that breach of security can be prevented in advance to improve using the reliability of DNS and system control in this paper. In other words, we would like to suggest method can be block randomly to access the site which information security system of user-centric is breached harmful files infected in user computer.

키워드

DNS, 방화벽, 클라이언트 제어, 시스템 제어, 정보보안

Key word

DNS, Firewall, Client Control, System Control, Information Security

* 정회원 : 한국폴리텍대학 아산캠퍼스 정보통신시스템과 부교수
** 정회원 : 한밭대학교 멀티미디어공학과 박사과정
*** 정회원 : 공주대학교 정보통신공학부 교수
**** 정회원 : 경남대학교 컴퓨터공학과 조교수
(교신저자, hyun1004@kyungnam.ac.kr)

접수일자 : 2012. 04. 04
심사완료일자 : 2012. 04. 25

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.9.1955

Ⅰ. 서 론

컴퓨터 침해사고는 2005년 이후부터 신고 건수가 감소하고 있으나 매스컴의 대대적인 보도와 개인정보 유출에 대한 국민적 관심이 증가하고 있다. 또한, 침해사고에 대한 빈도수가 감소하였을 뿐 침해 강도 및 영역이 점차 증가하고 있다. 결국 개인의 프라이버시 침해에서부터 국가 경제 및 안보에까지 총체적으로 위협을 하고 있는 실정이다. 최근에는 악의적인 해킹이나 산업 스파이에 의한 정보유출, 내부 직원의 회사기밀, 고객정보 유출 등의 컴퓨터를 이용한 범죄가 급증하고 있다.

이와 같은 상황 속에서 침해사고가 발생하였을 경우 가해자보다 피해자가 더 많은 비난을 받는 사회적 분위기가 조성되고 있다[1]. 즉, 침해사고는 무조건 피해자의 과실이라는 인식이 강하기 있기 때문에 다양한 보안 솔루션들을 개발, 적용하여 완벽한 예방을 추구하려는 노력이 증가되고 있다.

그러나 보안 솔루션을 통해 침해사고 예방은 100% 완벽할 수 없다. 보안 솔루션은 특정 위협에 대한 통제에 불과하다. 즉, 보안 솔루션 역시 비즈니스 상 허용해야만 하는 접근경로에 대해서는 개방할 수밖에 없다.

또한 감시를 통한 탐지인 IDS(Intrusion Detection System)도 널리 알려진 패턴이나 명백한 비정상적 행위에 대한 탐지가 가능한 것이기 때문에 침입탐지 우회기법 등을 통한 침해사고 탐지에는 한계가 있다[2].

이와 같은 침해사고들에 대해 대응하는 입장에서는 우선 시스템에 대해 공격할 여지가 없도록 철저한 보안을 신경 쓰는 것부터 침해사고 발생 시 신속하게 대응하여 피해의 확산을 막는 것, 침해사고 분석을 통해 차후에 발생될 공격에 대해 취약점을 보강하고 공격자의 단서 및 증거를 확보하여 법적인 대응 시 증거자료로 쓰일 수 있도록 신뢰성 있는 데이터를 확보하는 것까지 주력해야 할 것이다[3][4].

또한 최근 보안사고의 대다수는 사용자가 인터넷을 하는 동안 정상적 및 비정상적으로 유입되는 유해한 파일이 보안의 취약함(개인정보 유출, 제3의 감염 경로, 유포지 경로 등등)을 주고 있는 실정이다. 이들 파일들은 독자적인 행위를 하는 것을 포함해서 개인의 정보를 수집하여 경제적인 이득을 취하는 사업자 또는 해커들에게 전달하도록 하고 있다[5][6]. 결과적으로 기존 정보보안 시스템에서 고민하고 있는 다양한 문제점인 가짜 도메인 접근에 따른 피싱 피해, 사용자도 모르게 설치되는 좀비에 의한 개인정보 유출 피해 및 유해파일에 의한 2차・3차 감염 피해 등을 기존에 개발, 운영되는 프로토콜을 활용하여 문제점을 해결하기 위한 것이다.

따라서 본 논문에서는 DNS(Domain Name System)에 대한 신뢰성을 향상시키고 DNS를 이용한 시스템 제어를 통해 침해사고를 사전에 예방할 수 있는 보안 시스템을 설계하고자 한다.

이를 위해 기존의 침해사고 예방 시스템에서 신뢰 DNS에 IP(Internet Protocol)정보를 요청한 내부 사용자의 정보와 요청 정보를 실시간으로 DNS 방화벽에 전달하여 정책을 자동으로 설정하고자 한다. 또한, 정상접근에 대한 확인절차를 거쳐 정상적인 접근일 경우 이를 허용하고 불법적인 접근에 대한 정보는 취합하여 해당 사이트에 대해 CERT(Computer Emergency Response Team) 팀에 전달하여 분석, 처리할 수 있는 시스템을 설계하고자 한다.

Ⅱ. 기존 시스템 현황 및 침해사고 유형

2.1. 기존 시스템 현황

현재 사용자가 웹 콘텐츠에 접근하는 기본적인 경로는 5단계에 걸쳐 이뤄지고 있다.

먼저, 1 단계에서 사용자가 접속할 웹 사이트를 브라우저를 이용하여 네이밍(www.aa.com)을 하고 실행한다. 2 단계에서 브라우저는 네이밍에 대한 IP정보 확인하기 위해 1차적으로 PC에 존재하는 host 목록을 확인한다. 3 단계에서 존재 유무의 결과를 알려주고 만약 존재하지 않으면 4단계를 수행한다. 4 단계에서는 2 단계에서 존재하지 않으면 사용자 PC에 등록되어 있는 DNS 주소를 확인하여 2 단계와 같이 IP정보를 요청한다. 마지막 5 단계에서 요청한 IP정보를 가지고 인터넷 경로를 찾아 해당 웹사이트에 접속하여 정보를 열람한다[7]. 그러나 이와 같이 보편적으로 운영되고 있는

인터넷 접근 및 시스템 관련 현황에 대한 문제점은 아래 표 1과 같이 지적할 수 있다[2][8].

표 1. 단계별 문제점
Table. 1 Step by step Problem

단계	정상적 절차	위험상황
1	사용자가 접속할 웹 사이트를 브라우저를 이용하여 네이밍을 하고 실행한다.	PC사용자의 경우 자신이 사용하는 브라우저에 대해서만 운영할 수 있어 외부에서 불법적으로 심어 놓은 불법 브라우저가 외부에 접근하는 정보는 확인 불가능하다.
2	브라우저는 네이밍에 대한 IP정보 확인하기 위해 1차적으로 PC에 존재하는 host 목록을 확인한다.	피싱과 같은 보안 사고의 원인이 되는 부분으로서 PC를 잘 아는 사용자가 아니면 자신이 접속한 사이트에 대한 신뢰성을 확인할 수 없다.
3	존재유무의 결과를 알려준다. 만약 존재하지 않으면 4단계 수행을 한다.	존재 유무를 확인하지 않는 것을 사용자는 모른다.
4	2단계에서 존재하지 않으면 사용자 PC 에 등록되어 있는 DNS 주소를 확인하여 2단계와 같이 IP정보를 요청한다.	가짜 DNS가 존재하여 사용자가 자신도 모르게 우회하여 외부에 접속토록 하여 안전한 DNS에 대한 확인이 필요하다.
5	요청한 IP정보를 가지고 인터넷 경로를 찾아 해당 웹사이트에 접속하여 정보를 열람한다.	가짜 사이트에 대한 정보가 없어 사용자는 가짜 사이트에 정보를 열람 또는 정보 입력 또는 자료 다운로드(ActiveX, 악성 코드 등등)를 수행한다.

2.2. 침해사고 유형

침해사고는 크게 공격방법에 따른 침해사고와 피해유형에 따른 침해사고로 분류할 수 있다. 공격에 따른 침해사고는 서비스 거부공격, 분산서비스 거부공격, 악성코드, 사회공학 및 프로토콜 취약점 공격으로 분류할 수 있다. 또한, 피해유형에 따른 침해사고는 계정 침탈, 스니핑(sniffing) 및 캐시 포이즈닝으로 분류할 수 있다[9][10].

공격방법에 따른 침해사고를 살펴보면, 서비스 거부공격(DOS, Denial of Service)은 대량의 접속을 유발해 해당 컴퓨터를 마비시키는 수법이다. 이 수법은 목표 서버가 다른 정당한 신호를 받지 못하게 방해하는 작용만 한다. 분산서비스 거부공격(DDOS, Distributed Denial of Service)은 특정 사이트에 동시에 수백만 대의 컴퓨터를 접속시켜 한꺼번에 접속량을 늘림으로써 해당 사이트를 마비시키는 수법이다.

즉, DOS 공격을 하나가 아닌 여러 개의 호스트가 담당하게 된다. 악성코드는 시스템 내에 설치되어 시스템의 정상적인 동작을 방해하거나 또는 사용자가 알아채지 못하는 상태에서 특정 작업을 수행하게 하는 프로그램이다. 대표적으로 바이러스, 백도어, 트로이 목마, 웜 등이 있다. 사회공학은 시스템이 아닌 사람의 취약점을 공략하여 원하는 정보를 얻는 공격 기법을 말한다. 마지막으로 프로토콜 취약점 공격은 프로토콜 최초 설계 시 불안전하게 설계된 부분이 있기 때문에 불안전한 부분을 공격자가 악용하는 것을 말한다[11].

피해유형에 따른 침해사고를 살펴보면, 계정침탈은 계정에 대한 관리를 소홀히 하여 인가되지 않은 외부의 다른 사람이 계정에 접근하여 심각한 문제를 발생시키는 것이다. 스니핑(Sniffing)은 네트워크상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미한다. 간단히 말하면 네트워크 트래픽을 도청하는 과정을 스니핑이라 할 수 있다. 마지막으로 캐시 포이즈닝은 DNS가 가짜의 응답(IP)을 하게하는 공격 수법이다.

즉, 가짜의 응답(IP)이 DNS를 통해서 웹에 접속되면 사용자가 알아채지 못하는 동안 피싱 사이트에 유도되게 하는 수법이다[12][13].

본 논문에서는 침해사고를 예방하기 위해 DNS에 대한 신뢰성을 향상시키고 DNS를 이용한 시스템 제어 방법을 적용한 침해사고 예방 시스템을 설계하였다.

Ⅲ. 시스템 설계

본 논문에서는 DNS에 대한 신뢰성 및 DNS를 이용한 시스템 제어를 통해 다양한 침해사고를 사전에 예방하기 위한 시스템을 설계하였다. 즉, 기존 인터넷 운영을 위한 안정적인 구조와 방법을 사용자가 정상적으로 안전하게 사용하도록 하는 솔루션이다. 따라서 사용자 컴퓨터에 새로운 무엇을 설치하여 인터넷을 안전하게 사용하는 솔루션이 아니라 인터넷 사용의 방법적인 기능을 인터넷 구간에 설치하여 사용자가 요구한 경우에만 인터넷이 되도록 하는 사용자 행위 중심의 솔루션이라고 보면 된다. 여기에 기존 활용하고자 하는 핵심 사항은 인터넷을 하기위한 필수 서비스인 도메인 시스템(DNS)과 침입차단시스템(Firewall)이다.

아래 그림 1은 기존의 시스템에 DNS 검사 장치를 추가하고 신뢰 DNS와 연동시켜 Dynamic DNS 정책을 설정하여 DNS 검색 결과 전송 및 내부에서 검색 요청한 정보에 대한 결과를 정상적으로 제어하는 절차가 추가된 것이다.

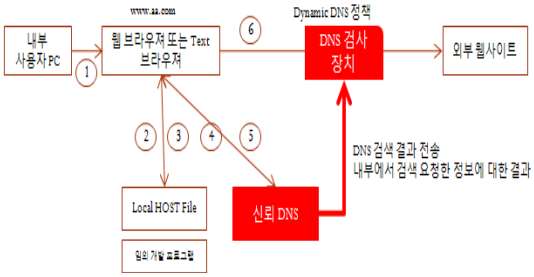

그림 1. 신뢰 DNS를 이용한 시스템 제어
Fig. 1 System Control Using Trust DNS

전체 시스템의 흐름은 다음과 같다. 1차 단계에서 사용자가 인터넷을 하기 위해 도메인 정보를 DNS 서버에 요청하여 IP 정보를 요청한다. 2차 단계에서 DNS 서버는 사용자에게 요청 받은 도메인 정보에 해당하는 IP정보를 제공한다. 3차 단계에서 DNS 서버는 요청한 사용자 정보와 요청한 도메인에 해당하는 IP정보를 실시간으로 DNS 방화벽에 전달하여 정책을 자동으로 설정하여 정상 접근에 대한 확인 절차를 거쳐 정상적인 접근을 허용한다. 만약 DNS 방화벽에 허용되지 않는 정책은 모두 차단과 로깅 정보를 수집 하도록 되어 있다.

마지막 단계에서 수록된 허용 및 차단 로그는 CERT 팀에 전달하여 허용 로그에 대해서는 통계자료를 만들어 감사 자료로 활용하고, 차단 로그에 대해서는 분석하고 다양한 자료(유해 사이트 자료, 좀비 사이트 자료 등)로 활용한다. 또는 불법사이트 목록 데이터베이스를 운영하여 정보공유로 활용한다.

시스템 내에서 존재하는 해당 기능은 타 보안 장비와 연동이 가능하며 예외처리는 관리자가 직접 입력한다. 아래 그림 2는 프로토콜 구성도를 나타낸 것이며 표 2는 DNS Type을 나타낸 것이다.

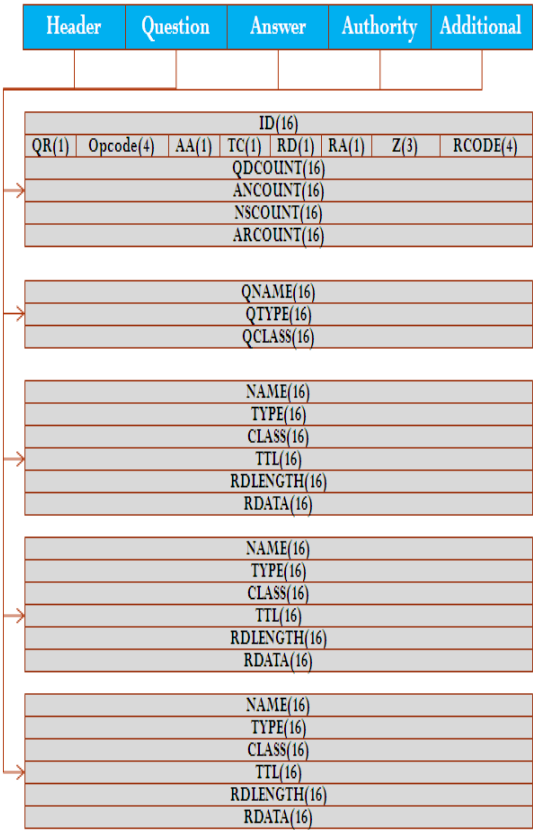

그림 2. 프로토콜 구성도
Fig. 2 Protocol Diagram

표 2. DNS Type
Table. 2 DNS Type

Type	Value	Meaning
A	1	a host address
NS	2	an authoritative name server
MD	3	a mail destination (Obsolete - use MX)
MF	4	a mail forwarder (Obsolete - use MX)
CNAME	5	the canonical name for an alias
SOA	6	marks the start of a zone of authority
MB	7	a mailbox domain name (EXPERIMENTAL)
MG	8	a mail group member (EXPERIMENTAL)
MR	9	a mail rename domain name (EXPERIMENTAL)
NULL	10	a null RR (EXPERIMENTAL)
WKS	11	a well known service description
PTR	12	a domain name pointer
HINFO	13	host information
MINFO	14	mailbox or mail list information
MX	15	mail exchange
TXT	16	text strings

아래 그림 3은 시스템 설계를 나타낸 것이며 그림 4는 개발에 필요한 흐름 절차를 나타낸 것이며 그림 5는 시스템 설치에 대한 예상 구성도를 나타낸 것이다. 전체 시스템은 DNS 구성, Dynamic 및 Static 침입차단시스템 구성, DNS Cacheing Time Clear ActiveX 구성으로 되어 있다.

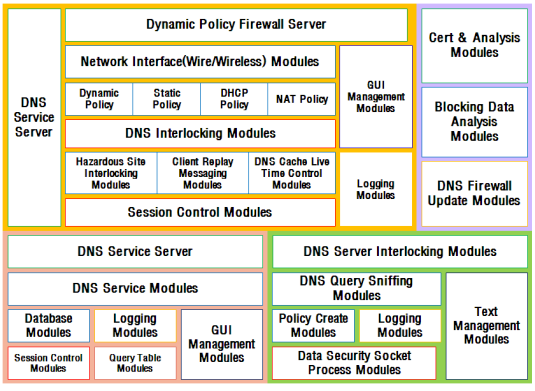

그림 3. 시스템 설계
Fig. 3 System Design

위의 그림 3은 DNS 방화벽 System 전체 구조도로 4개의 모듈로 구성되어 있다. 첫 번째는 방화벽(침입차단시스템) 모듈부로서 올바른 쿼리를 통하지 않는 외부 접근자에 대하여 차단하도록 되어 있으며, 두 번째는 DNS 시스템으로 DNS에 대한 정보 등록과 사용자 쿼리에 대한 응답처리 하도록 되어 있다. 세 번째는 DNS 시스템에 요청된 쿼리 결과에 대한 정보를 방화벽 모듈에 전달을 하도록 되어 있다. 네 번째는 방화벽에 의해 차단된 정보를 다른 시스템과 연계하여 사용할 수 있는 분석 및 로깅 모듈이다.

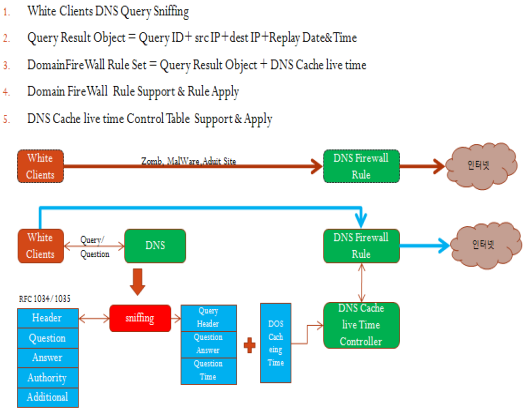

그림 4. 시스템 흐름도
Fig. 4 System Flow

위의 그림 4는 DNS 방화벽이 동작하는 동작 흐름을 표현한 것으로서 다음과 같은 단계로 동작한다.

① 사용자가 DNS시스템에 외부 접근에 대한 IP 정보 요청 쿼리를 한다.

② DNS 시스템은 사용자가 쿼리한 정보를 수집하여 사용자가 외부에 접근코자 하는 IP 주소와 사용자 주소 그리고 해당 쿼리가 유동 방화벽 테이블에 넣을 수 있게 객체를 만든다.

③ ②단계에 의해 만들어진 객체를 유동 방화벽 정책에 넣고 적용한다.

④ 사용자는 유동정책이 적용된 기간 동안 방화벽 장치를 통하여 쿼리한 사이트에 접속한다.

⑤ 예외 정책이나 우회 정책은 정적 정책을 넣어 사용하도록 한다.

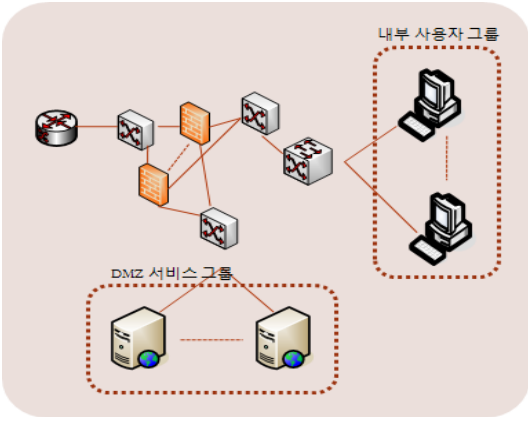

그림 5. 시스템 예상 구성도
Fig. 5 System Expectance Diagram

위의 그림 5는 개발된 DNS 방화벽이 실제 구성되는 예상 구성도로서 일반적인 방화벽 장치와 동일하게 라우팅 모드와 브리지 모드를 지원하도록 되어 있으면서 기능적으로는 일반 방화벽에서 제공하는 NAT(Network Address Translation) 기능을 포함하고 있다. Zone 구분으로는 내부사용자 영역, DMZ(Demilitarized Zone) 영역 그리고 외부사용자 영역을 관리할 수 있도록 구성이 가능하다. 또한, DNS 방화벽의 가장 큰 특징은 기존 방화벽 장치들은 주된 방화벽 기능에 단순 DNS 서비스를 제공토록 되어 있는데 저희가 개발코저하는 시스템은 두 개의 독립된 주장치(방화벽 장치, DNS 시스템)가 운영되는 구조로 인터로깅을 통한 연계 구조로 되어 있다.

Ⅳ. 시뮬레이션 분석

본 논문에서 제안한 방법은 기존 정보보안 시스템의 연구 방향들이 특별한 솔루션 개발에 중점을 두고 있는 것과는 달리 Domain To Host 검색 방법과 침입차단시스템의 연동 솔루션을 활용한 통합 위협 관리 시스템(UTM : Unified Threat Management)을 설계, 개발하는 것이다.

따라서 기존 정보보안 시스템에서 고민하고 있는 다양한 문제점인 가짜 도메인 접근에 따른 피싱 피해, 사용자도 모르게 설치되는 좀비에 의한 개인정보 유출 피해 및 유해파일에 의한 2차・3차 감염 피해 등을 기존에 개발, 운영되는 프로토콜을 활용하여 문제점을 해결하기 위한 것이다.

표 3. 기존 연구내용과의 비교
Table. 3 Comparison with Previous Research

구분	장점	단점
기존 연구/개발 내용 (좀비 PC탐지, 통합PC, PC 방화벽, 유해사이트 차단 등)	1. 단일시스템 개발 용이 2. 대규모 사이트 적용	1. 단편적인 보안구성 2. 피해에 대한 문제 해결 능력 부족 3. 원인 분석을 위해서는 별도 솔루션 도입 필요 4. 제품의 하드웨어 성능 편중 5. 종단 장치의 운영 환경에 민감 6. 지속적인 업데이트
제안 연구/개발 내용 (DNS 정보 검색 연동 기법을 이용한 침해사고 예방 시스템)	1. 연동 보안 구성 2. 분석이 용이 3. 소프트웨어적인 성능 4. 종단장치 운영에 영향 없음 5. DNS 정보교환 업데이트만 존재	1. 중/소규모 사이트 적용 2. 연동 설계에 따른 복잡성

정보보안에서 중요시 생각하는 부분은 비정상 패킷들이다. 이 패킷들 중에는 유해한 파일이 존재할 수 도 있고, 유해 사이트에 접속을 제공하는 패킷도 있을 것이다. 따라서 보안 솔루션 개발사들은 비정상패킷들을 대상으로 내부 또는 외부로 나가고 들어오는 패킷에 대하여 차단 및 제거하는 방법들을 개발하고 있다.

그러나 기존 방식들은 비정상 패킷에 대한 구분을 별도로 하지 않고 제조사에서 별도의 정보수집 또는 분석을 통하여 만들어진 자료를 데이터베이스화(패턴화)하여 관련 보안장비에 업데이트하여 적용하는 방법이 있는가 하면, 아무런 정보가 없는 보안장비에 사용자가 자신들의 사이트 상황에 맞게 정책을 적용하는 방법이 있다.

아래의 비교 실험에서 보는 바와 같이 DNS 쿼리를 하는 정보에 대해서는 정상적인 처리를 보이는 패킷들인 반면, DNS 쿼리를 하지 않는 패킷들은 비정상적인 패킷

으로 판단된다. 이는 정상과 비정상을 가려내는 방법이 DNS 쿼리를 통해서만이 가능하다 판단된다. 물론 DNS 쿼리를 하지 않는 방법도 있으니 이는 극히 제한적인 사항이라 비교 실험에서는 제외하였다.

비교 실험 결과에서 보는 바와 같이 평균 12% ~ 14% 정도가 비정상 패킷을 보이고 있다. 이에 대한 제어 방법으로 본 논문에서 제안하고 있는 DNS 정보 검색 연동 기법이 근본적인 해결 방법이라 생각된다.

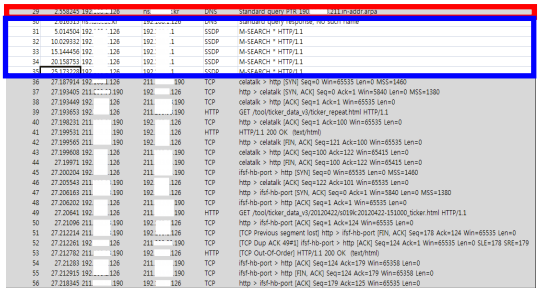

그림 6. DNS 패킷 데이터 수집
Fig. 6 DNS Packet Data Collecting

표 4. 패킷 분석 결과
Table. 4 Packet Analysis Result

수집 시간	전체 패킷	DNS 쿼리	DNS 정상 응답	DNS 비정상 응답	정상 패킷	비정상 패킷	정상 패킷 비율	비정상 패킷 비율
1분	90	10	6	4	66	11	73%	12%
5분	570	2	2	0	491	75	86%	13%
10분	1186	0	0	0	1015	171	86%	14%
15분	1560	2	2	0	1315	243	84%	16%
20분	2349	2	2	0	2032	315	87%	13%
평균	5755	16	12	4	4919	815	85%	14%

V. 결 론

최근 정보보안의 흐름은 사용자 중심으로 변화가 되고 있다. 이는 사용자 컴퓨터에 에이전트를 설치하여 사용자 컴퓨터로 들어오고 나가는 패킷들에 대하여 보안을 적용하는 상태이다. 이는 사용자 컴퓨터의 성능을 가중 시키는 실정이고 이는 바로 경제적인 영향을 미친다. 초기 관공서 기준의 사용자 컴퓨터에는 백신정도로 깔아 사용자가 취급하는 파일 또는 외부에서 유입되는 파일에 대하여 바이러스 감염 유무를 판단하고 치료하는 정도였다. 그러나 최근에는 최소 6개 이상의 컴퓨터 보호용 에이전트가 심어져 있는 실정이다. 모두 안전을 위하여 필요한 보호 장치이다. 이들 에이전트는 모두 중앙제어 또는 중앙정책을 적용하여 일괄 관리하는 수준이다. 이유는 사용자에게 제어권을 주면 위험성에 대한 보호 장치가 되지 않는다는 이유에서 제어권은 최소로 하고 있다.

그러나 사용자 중심이라고 하면 사용자가 선택을 할 수 있는 수준을 일반적으로 사용자 중심이라고 할 수 있다. 즉, 사용자가 인터넷을 하게 되면 본인이 직접 웹 브라우저에 접근하고자 하는 URL을 입력하여 해당 정보를 검색하여야 하는 것이라고 판단된다. 대다수 인터넷을 이용하는 또는 터미널 서비스를 이용하는 솔루션은 모두 이와 같은 사용자가 입력하는 형태로 작업을 한다. 결국 사용자 중심은 사용자가 원하는 정보를 취득 하기 위해 원하는 행위를 하는 것이다. 따라서 이를 근본적으로 해결하기 위해서는 사용자 중심의 행위 기반을 제어하는 형태만이 가능하다고 판단된다.

본 논문에서 제안한 방식인 DNS 정보 검색 연동 기법을 이용한 침해사고 예방 시스템은 최초의 사용자 중심의 정보보안 시스템으로 사용자 컴퓨터에 감염된 유해 파일이 임의로 사이트를 접속하는 행위에 대하여 차단할 수 있는 근본적인 해결 방법으로 판단된다.

참고문헌

[1] 전병규, “클라이언트/서버 기반의 침해사고 대응 시스템 구조의 설계,” 충주대학교 석사학위논문, 2007.
[2] 최상용, 해킹 사고의 재구성, 에이콘출판, 2012.
[3] 정익래, 홍도원, 정교일, “디지털 포렌식 기술 및 동향,” 전자통신동향분석, 제22권, 제1호, pp.97-104, 2007.
[4] 박재홍, Network Hacking & Security, 글로벌, 2003.
[5] 강영선, 최영우, “사이버 공격에 대비한 대학의 정보보안 현황 및 개선 방안,” 한국컴퓨터정보학회지, Vol16, No12, 2011.

[6] 황성준, “최근 인터넷 보안침해사고 동향분석과 대응방안 고찰,” 포항대 사회경제연구소 논문집, 제35권, 제1호, 2009.
[7] 김우한, 최중섭, 침해사고 분석 절차 가이드, 한국인터넷진흥원, 2006.
[8] 편집부, 기업정보보안 가이드, 화산미디어, 2012.
[9] 송대근, 해킹 침해사고 분석, 지앤선, 2009.
[10] 견병구, “침해사고 관리 방안에 관한 연구,” 성균관대학교 석사학위논문, 2011.
[11] 배상일, VIRUS DDOS, 샤프론, 2009.
[12] 고병수, 박영신, 최용락, 고명수, “보안 침해사고 대응을 위한 컴퓨터 포렌식스 기술 동향,” 한국인터넷정보학회, 제4권, 제1호, pp.37-46, 2003.
[13] 진양양, “윈도우 시스템 침해사고 분석 및 분석방법에 관한 연구,” 한서대학교 석사학위논문, 2011.

저자소개

김광섭(Kwang-Sup Kim)

1992년 서울산업대 전자공학과 공학사
2008년 공주대학교 전기전자정보공학부 공학석사
2004년 ~ 현재 공주대학교 정보통신공학부 공학박사수료
2003년 ~ 현재 한국폴리텍대학 아산캠퍼스 정보통신시스템과 부교수
※관심분야 : 네트워크 운용 및 관리, 네트워크 보안

박영길(Young-Gil Park)

2007년 한밭대 컴퓨터공학과 학사
2009년 한밭대 멀티미디어공학과 석사
2009년 ~ 현재 한밭대 멀티미디어공학과 박사과정
2010년 ~ 현재 한국폴리텍대학, 대덕대학 외래강사
※관심분야 : 네트워크 및 시스템 보안, 멀티미디어 보안, 영상처리

노승환(Soong-Hwan Ro)

1987년 고려대학교 전자공학과 공학사
1989년 고려대학교 전자공학과 공학석사
1993년 고려대학교 전자공학과 공학박사
1997년 한국전자통신연구원 초빙연구원
2003년 영국 버망엄대학교 초빙연구원
1994년~현재 국립공주대학교 정보통신공학부 교수
※관심분야 : 이동통신, Pervasive 컴퓨팅, 임베디드 시스템

김봉현(Bong-Hyun Kim)

2000년 한밭대 전자계산학과 학사
2002년 한밭대 전자계산학과 석사
2009년 한밭대 컴퓨터공학과 박사
2002년~2012년 한밭대, 충북도립대 외래강사
2012년 ~ 현재 경남대학교 컴퓨터공학과 조교수
※관심분야 : 생체신호분석, BIT융합기술, 차세대 컴퓨팅, e-Business