DBpia

논문 12-37B-11-13

한국통신학회논문지 '12-11 Vol.37B No.11
http://dx.doi.org/10.7840/kics.2012.37B.11.1082

DNS 트래픽 기반의 사이버 위협 도메인 탐지

임 선 희◆, 김 종 현°, 이 병 길*

Detecting Cyber Threats Domains Based on DNS Traffic

Sun-Hee Lim◆, Jong-Hyun Kim°, Byung-gil Lee*

요 약

최근 사이버 공간에서는 대규모 사이버 공격들을 위해 봇넷(Botnet)을 형성하여 자산 손실과 같은 경제적 위협뿐만 아니라 Stuxnet과 같은 국가적으로 위협이 되고 있다. 진화된 봇넷은 DNS(Domain Name System)를 악용하여 C&C 서버와 좀비간의 통신 수단으로 사용하고 있다. DNS는 인터넷에서의 주요 인프라이고, 무선 인터넷의 대중화로 지속적으로 DNS 트래픽이 증가되고 있다. 반면에, 도메인 주소를 이용한 공격들도 증가되고 있는 현실이다. 본 논문에서는 지도 학습 기반의 데이터 분류 기술을 이용한 DNS 트래픽 기반의 사이버 위협 도메인 탐지 기술에 대해 연구한다. 더불어, 개발된 DNS 트래픽을 이용한 사이버위협 도메인 탐지 시스템은 대용량의 DNS데이터를 수집, 분석, 정상/비정상 도메인 분류 기능을 제공한다.

Key Words : DNS, botnet, DDoS, cyber security, Classification

ABSTRACT

Recent malicious attempts in Cyber space are intended to emerge national threats such as Suxnet as well as to get financial benefits through a large pool of comprised botnets. The evolved botnets use the Domain Name System(DNS) to communicate with the C&C server and zombies. DNS is one of the core and most important components of the Internet and DNS traffic are continually increased by the popular wireless Internet service. On the other hand, domain names are popular for malicious use. This paper studies on DNS-based cyber threats domain detection by data classification based on supervised learning. Furthermore, the developed cyber threats domain detection system using DNS traffic analysis provides collection, analysis, and normal/abnormal domain classification of huge amounts of DNS data.

Ⅰ. 서 론

봇넷(botnet)은 악성코드 봇(bot)에 감염된 다수의 컴퓨터들이 네트워크로 연결되어 있는 형태로서, 분산서비스거부공격(distributed denial of service), 부정클릭(click fraudulence), 스팸(spam), 개인정보 유출(identity theft)과 같은 다양한 공격들의 60%이상이 봇넷을 통하여 이루어지고 있다. 이러한 공격들은 단순한 사고가 아닌 자산 손실과 같은 경제적으로도 위협뿐만 아니라 Stuxnet과 같은 국가적 위협으로 대두되고 있다.

봇넷은 자유자재의 권한을 가진 봇마스터(botmaster), 악성코드 즉 봇 프로그램에 감염된 좀비(zombie), 명령/제어를 내리는 C&C(command

※ 본 연구는 방송통신위원회 정보보호 원천기술개발 사업의 일환으로 수행하였음. [2012/10912-06002, 전역적 협력기반의 통합보안제어 시스템 개발]
◆ 주저자 : 한국전자통신연구원 사이버융합보안연구단, capsunny@etri.re.kr, 정회원
° 교신저자 : 한국전자통신연구원 사이버융합보안연구단, jhk@etri.re.kr, 정회원
* 한국전자통신연구원 사이버융합보안연구단, bglee@etri.re.kr, 정회원
논문번호 : KICS2012-08-404, 접수일자 : 2012년 8월 31일, 최종논문접수일자 : 2012년 10월 31일

www.dbpia.co.kr

and control) 서버가 네트워크로 연결되어 있다. 좀비들은 봇마스터에 의해 원격 조종되며 각종 악성 행위를 수행할 수 있는 수천에서 수십만대의 봇에 감염되어 C&C 서버와 지속적으로 명령 및 제어 메시지를 통해 통신한다.

초기의 봇넷은 채팅 프로그램에서 많이 사용하던 IRC(internet relay chat)를 이용한 중앙집중형 구조의 봇넷이 주를 이루었다. 중앙집중형 구조의 봇넷은 하나의 C&C서버가 다수의 좀비PC들을 명령/제어하기 때문에 C&C서버의 탐지 및 차단으로 다량의 좀비PC들을 유실함으로써 공격자 입장에서는 커다란 손실을 갖게 된다. 이러한 중앙집중형 구조의 문제점을 해결하기 위해, 일반 사용자들이 많이 사용하는 웹 프로토콜 HTTP를 적용하거나, 모든 좀비PC들이 C&C 서버 역할을 수행할 수 있는 분산형 명령/제어 방식, 즉 P2P 봇넷 구조로 진화하고 있다[1].

또한, 최근 봇넷 기술에서는 C&C서버와 좀비PC 간의 접근 방법으로 악성코드인 봇 프로그램에 고정(static) IP 주소를 하드코딩 방식이 아닌 DNS(domain name system) 서비스를 이용하여 도메인 주소로 접근 하는 방법을 사용하고 있다. 더욱이, 도메인 네임에 IP 주소가 동적으로 다양하게 변경되는 DDNS(dynamic DNS) 서비스 혹은 FastFlux 기법을 적용하고 있다.

이러한 전역적 네트워크 환경에서의 대규모 사이버 공격의 원인이 되는 봇넷들이 진화하고 있다. 특히, DNS 서비스를 이용한 사이버 위협들이 빈번하게 자주 발생되고 있는 현실이다.

DNS 서비스는 사용자들에게 보다 편리하게 인터넷에 접근하기 위한 네트워크 인프라 서비스이다. 특히, 스마트폰의 보급과 확산으로 인터넷 이용자수가 급변하게 증가하고 있고, 오락, 기업, 소셜미디어, 검색, 쇼핑 등을 제공하는 스마트폰 어플리케이션으로 인한 DNS 트래픽양이 급속하게 증가하고 있다. 반면에 DNS 서버를 통한 DDoS 공격만으로도 전역적 네트워크 사이버 위협에 커다란 파장을 일으킬 것으로 예상되고 있고, DNS 서비스를 악용한 봇넷 기술들이 발생함으로써 DNS 트래픽 분석을 기반으로 사이버 위협 탐지 기술에 대한 연구가 필요하게 되었다. 하지만, DNS 서비스가 일반 사용자 인터넷 서비스의 QoS와 맞물려 있기 때문에 DNS 트래픽 기반의 침입탐지시스템(IDS), 침입방지시스템(IPS)으로 사이버 위협에 대한 탐지 및 대응이 쉽지 않다[2].

본 논문에서는 DNS 트래픽을 수집 및 모니터링하여 지도학습(supervised learning)기반의 데이터 분류(classification) 기술을 통해 사이버 위협 도메인을 분류하고자 한다. 본 논문에서의 사이버 위협 도메인은 좀비PC들이 C&C서버와 명령 및 제어 메시지를 송수신하기 위해 접속하는 C&C서버의 도메인 주소이다. 봇넷을 형성하기 위해서는 악성코드인 봇 프로그램으로 감염시켜야 한다. 이러한, 봇 프로그램으로 감염된 좀비PC들의 행위들은 일반 사용자의 도메인 질의 패턴과 다르게 봇 프로그램이라는 특성상 특정 패턴을 가지게 될 것이다. 이러한 점을 가정하여, 본 논문에서는 봇에 감염된 좀비PC에서 질의되는 비정상 DNS 트래픽과 일반 사용자에서 질의되는 정상 DNS 트래픽을 수집 및 지도학습 과정을 통해 정상/비정상 도메인 질의 패턴을 분석하여 사이버 위협 도메인을 분류하고 사이버 위협 도메인의 비정상도(abnormality)를 도출한다. 본 논문은 실제 발생된 DNS 위협 사례와 DNS 기반의 봇넷 기술에 대해 Ⅱ장에서 기술하고, Ⅲ장에서는 본 논문에서는 제안하는 사이버 위협 도메인 분류 기술에 대해 설명한다. 또한, Ⅳ장에서 개발된 사이버 위협 탐지 시스템의 기능, 구현 및 실험 결과에 대해 기술한다.

Ⅱ. 관련 기술

2.1. DNS 위협 사례

최근 DNS 서비스를 이용한 사이버 위협들이 빈번하게 발생하고 있다. 다음 사례들과 같이 DNS 서버를 이용하여 제 3의 서버에 DDoS 공격을 진행하는 방식 혹은 DNS 설정을 변조하여 사용자의 개인정보 유출, 혹은 서비스 중단이 발생되고 있다.

- DNS Changer(2012.07.09.) : 악성코드에 감염되어 공격자가 운영하는 DNS서버로 연결되도록 설정. 전 세계 35만여대의 PC가 인터넷 접속 이상이 발생할 가능성 보도
- BIND Zero-Day(2012.11.16.) : DNS BIND 애플리케이션에 크래쉬가 발생하여 DNS서비스가 중지되는 제로데이(Zero-Day, CVE-2011-4313) 공격 발생
- DNS Spoofing과 Phishing을 결합한 공격(2011.1.09.) : 공격자는 미리 해당 사이트의 도메인 주소를 바꾸기 위해 DNS 관리업체의 아이디와 패스워드를 탈취하여 자신들이 만든 DNS로 이동하게 하고, 이 DNS는 다시 피싱 페이지

www.dbpia.co.kr

로 연결하는 방식. 국내 유명 커뮤니티 사이트 "ppomppu.co.kr"과 인터넷신문 "투데이코리아(todaykorea.co.kr)"가 해킹 공격을 받아 많은 사용자 정보들이 유출

- DNS Hijacking(2010.1.12.) : 중국 대형포털 사이트 바이두(http://www.baidu.com/) 도메인을 신청한 미국 도메인 제공 사이트(http://www.register.com/) 쪽에 불법 수정
- 아마존, 월마트 DNS DDoS 공격(2009.12.23.) : 아마존, 월마트, 익스피디아(인터넷 여행사)등 미국의 유명 인터넷 쇼핑몰이 DDoS 공격을 받아 다운. DNS서비스 제공업체인 미국 캘리포니아 주 팔로알토와 산호세에 있는 뉴스타의 DNS에 1시간여 동안 공격 받음
- Reflector 공격(2006) : 네임서버를 제3의 공격 대상 서버를 공격을 위해 사용하는 방식으로 DNS 질의에 사용되는 패킷이 통상 약 70바이트 크기를 갖는데 비해 그 응답메시지의 패킷을 최대 4196바이트 크기를 갖는 경우를 만들 수 있어 질의 트래픽 대비 약 60배로 증폭된 응답 트래픽을 유발하는 것이 가능하다는 점을 이용한 공격
- DNS Cache Poisoning 공격(2005.03.03.) : 각 도메인의 IP 주소를 변조하는 기법으로 정상적인 사이트로 접속하지 못하고 공격자가 만들어 놓은 진짜와 매우 유사한 사이트로 접속하도록 유인하여 로그인 정보 등을 탈취하는 위협

2.2. DNS 기반의 봇넷 기술

봇넷 기술들은 탐지 및 대응을 회피하기 위해 DNS서비스를 악용한 봇넷 기술들이 나타나고 있다.

2.2.1. DNS서비스로 C&C서버의 도메인네임 질의

악성코드 봇 프로그램에 C&C서버의 주소를 하드코딩된 IP주소가 아닌 도메인 주소로 접근하는 방법이다. C&C서버의 도메인 주소에 접근하는 좀비PC들은 DNS 서버에게 C&C 서버의 도메인 주소를 질의하고, 좀비PC들은 DNS서버로부터 응답받은 도메인 주소의 IP 주소로 접근을 시도한다. 더불어, 최신의 진화된 봇넷들은 DNS 쿼리를 정상 사용자와 유사한 패턴으로 랜덤하게 질의한다거나 도메인네임에 대응하는 IP주소가 계속 변경되는 DDNS 서비스 혹은 Fast-Flux기법을 통해 봇넷 탐지가 어려워지고 있다[3].

2.2.2. DNS 트래픽으로 명령/제어 전송

DNS 트래픽 페이로드에 명령/제어 메시지를 포함하여 전송하는 Feederbot이 발생되었다. 이러한 방법은 명령/제어 메시지 전달 채널로 DNS 데이터를 사용하거나 은닉채널로 DNS 데이터를 암호화하였을 경우는 탐지가 어려워진다. 또한, DNS서비스는 사용자들에게 인터넷 서비스로서 중요한 역할을 하기 때문에 DNS 데이터를 침입탐지 시스템에서 차단하기는 어렵다[4].

Ⅲ. 사이버 위협 도메인 분류 기술

전역적 네트워크에서의 대규모 사이버 위협이 되는 봇넷 탐지 기술은 중앙집중형 구조의 특징을 기반(IRC, HTTP 프로토콜)으로 탐지하는 BotSniffer[5]와 특정 프로토콜 기반의 봇넷 탐지인 BotSniffer의 문제점을 해결하기 위한 데이터 마이닝 기반의 탐지기술 BotMiner[6], DNS 트래픽 기반의 봇넷 그룹 행위 분석 기반의 탐지[3,4,8,9] 기술들이 연구되었다. 하지만, 이러한 선행 기술들은 봇넷의 특정 행위를 중심으로 탐지하기 때문에 특정 행위를 회피하는 봇넷은 탐지하지 못한다는 문제점을 가지고 있다.

본 논문에서는 DNS트래픽을 수집 및 분석하여 지도학습(supervised learning) 기반의 데이터 분류(classification) 방법을 이용하여 봇넷에서의 C&C서버와 좀비PC간의 DNS 서비스를 이용한 비정상 네트워크 행위를 탐지하고, 사이버 위협 도메인 즉 C&C 서버를 추출한다. 그림 1은 DNS 트래픽을 패시브 모니터링(passive monitoring)하여 사이버 위협 도메인을 탐지하기 위한 네트워크 구조도로 DNS 서버로 입출력되는 트래픽을 미러링하여 DNS 트래픽을 모니터링한다. 본 논문의 DNS 트래픽 분석 시스템은 DNS 서버의 인/아웃 트래픽을 수집, 분석하고, 비정상 행위 트래픽을 분류함으로써 사이버 위협 도메인을 탐지한다. 즉, 사이버 위협 도메인 탐지 시스템은 도메인 네임에 대한 질의를 하는 쿼리(query) 메시지와 쿼리 메시지에 대응하는 쿼리 응답 메시지에 해당하는 RR(resource record) 메시지를 통해 DNS 트래픽을 분석한다.

www.dbpia.co.kr

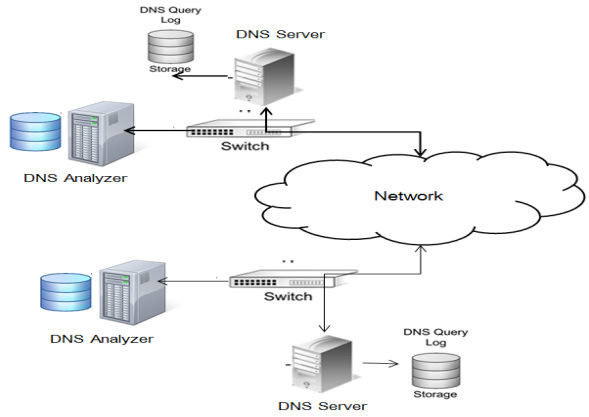

그림 1. DNS 트래픽 분석 시스템 네트워크 구성도
Fig. 1. Network architecture of DNS traffic analysis system

선행 연구에서는 비정상 행위인 봇넷의 특정 행위인 주로 사용하는 프로토콜, 순간적인 트래픽 증가, DDNS 사용, 한정된 소스 포트에서의 도메인 주소 질의들을 비정상 행위로 정의하였다. 하지만, 특정 봇넷 그룹 행위 기반의 탐지 기술은 행위에서 벗어나는 봇넷은 탐지가 어렵다는 한계점을 가지고 있다.

본 논문에서는 그림 2와 같이 DNS 트래픽 기반의 정상/비정상 트래픽을 수집 및 데이터 셋(dataset)화하고, 지도학습(supervised learning) 방법으로 수집된 데이터로 학습하여 분석 성분들을 추출 및 분류 알고리즘을 통해 분류한다. 더불어, 네트워크 행위에 대한 비정상도를 도출한다. 그림 2는 지도학습 기반의 데이터 분류 단계들이다.

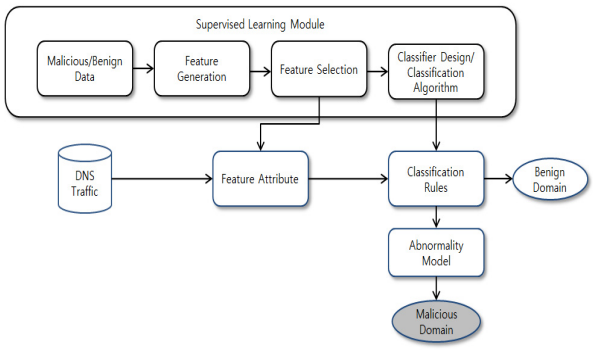

그림 2. 지도학습 기반의 데이터 분류 단계
Fig. 2. Data classification steps based on supervised learning machine

3.1. 데이터 수집 및 학습 데이터

본 논문에서는 3가지 실험을 통해 비정상 행위를 하는 DNS 데이터를 수집하였다.

1차 실험에서는 외부네트워크와의 연결을 단절시킨 상태에서 악성코드를 실행시키고 내부 네트워크에 수집되는 패킷을 수집하였다. 2차 실험에서는 외부 네트워크와 연결된 상태에서 악성코드를 실행시키고 외부의 통제되지 않은 C&C 서버와 통신하는 패킷을 수집하였다. 이 실험에서는 좀비 PC가 외부의 통제되지 않은 C&C서버에게 감염되었음을 알리는 패킷을 송신하고, 이 패킷을 수신받은 C&C서버가 좀비PC들을 자신들의 봇넷에 포함시킬 것을 고려하여 실험하였다. 3차 실험에서는 외부 네트워크와 연결된 상태에서 통제하에 있는 C&C 서버와 악성코드를 실행시키고 C&C 서버에서 좀비에게 공격명령을 내리고 외부로 공격이 이루어지는 패킷을 수집하였다.

1차 실험에서는 외부네트워크와의 연결이 단절되어 DNS 서버의 질의가 실험망 이상의 상의 DNS 서버로 질의되지 못하는 문제점을 가지게 되었고, 2차 실험에서 외부의 통제되지 않은 C&C서버의 접근이 거의 미비하였다. 본 실험 결과의 수집 데이터 양은 1차 실험 패킷 수(633,170), 2차 실험 패킷 수(839,718), 3차 실험 패킷 수(2,421,275)로 3차 실험만이 DNS 트래픽 분석을 위해 효과적으로 이용 가능하였다.

3.2. 파라미터 구성을 위한 학습 및 실험 데이터 구성

본 논문에서는 파라미터 구성을 위하여 수집된 폐쇄망 데이터와 정상 DNS 쿼리 패킷 데이터를 혼용하였다. 수집된 폐쇄망 실험 데이터에서는 악성 데이터 중 DNS 패킷 데이터가 아닌 라우팅 관련 패킷, 이더넷 장치의 브로드캐스팅 메시지를 제외한 데이터에서 DNS 서버로 유입되는 데이터를 선별하였다. 선별된 데이터 중 커널, 혹은 전송에서 발생한 프라그먼트 패킷은 소거하였으며, 학습 단계의 공격 데이터로 사전 분류하였다.

정상 데이터는 일반적인 SSL 암호화 통신 및 허가된 클라이언트의 요청에만 응답하는 통신 구조인 Skype사의 DNS 데이터를 이용하였다.

전체 공격 및 정상 데이터에서 분석의 정확도를 기대하기 위하여 10회 라운딩 학습을 시도 하고, 10회 실험을 반복하였으며, 도출된 결과 오차범위 3% 이내 검증으로 정확도를 확인하였다.

학습과 실험 두 단계의 데이터는 공격과 정상 비율을 데이터 분류에서 주로 사용하는 비율인 7:3 비율로 구성하였다. 그림 3은 분류 시스템을 위한

www.dbpia.co.kr

실험 데이터 수집 및 실험 데이터 구성을 위한 모델링 단계이다.

3.3. 분석 성분 추출(Feature Selection)

비정상 도메인을 분류하기 위해 구성된 학습 및 실험 데이터로부터 주요 분석 성분(feature)을 추출하기 위해 통계 기법인 주성분분석(PCA, principal components analysis)을 실험하였다. 주성분분석은 대응되는 성분을 이용하여 데이터의 주성분 및 성분의 성향을 분석할 수 있는 방법이다. 주성분분석(PCA)는 입력데이터의 상관 행렬(correlation matrix)의 고유값(eigen value), 고유벡터(eigen vector)값을 계산하여 고유값이 높은 차순의 성분들이 비정상 도메인의 성향을 나타내는 주성분으로 유의성이 보장된다[10].

본 논문에서는 DNS 트래픽 기반의 정상 쿼리와 비정상 쿼리의 성향을 분석하기 위해 DNS 트래픽에서 획득할 수 있는 최대 정보들인 DNS 트래픽 헤더 데이터 및 DNS 트래픽의 IP 패킷 속성에 해당되는 모든 성분들을 주성분분석(PCA) 한 결과 UDP 패킷에서의 소스포트, CRC 값, 패킷 길이, IP 패킷의 플래그값, 식별자, CRC 값, 패킷길이, TTL값이 도출되었다. DNS헤더에서는 식별자 속성이 비정상 도메인을 분류하기 위한 효과적인 파라미터 구성으로 참조된다[11].

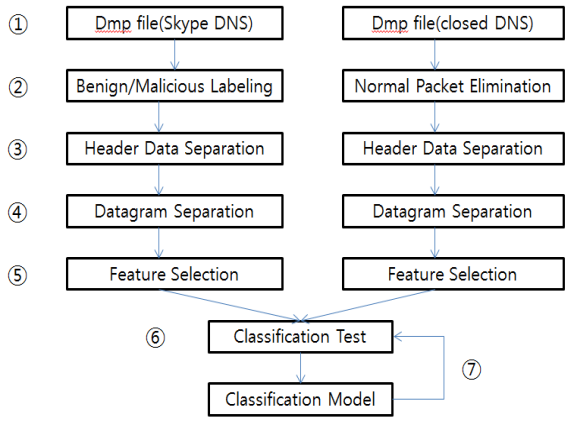

그림 3. 데이터 수집 및 실험 데이터 구성을 위한 모델링 과정
Fig. 3. Modeling steps of data collection and experimental data configuration

3.4. 분류기(Classifier)

최근 DNS 트래픽은 기존 인터넷 이용자의 증가와 더불어 스마트폰의 보급과 확산으로 무선 인터넷 접속량의 증가로 인해서 최근 5년간 DNS 쿼리 수가 200% 증가되고 있는 현실이다. 2011년 1분기 기준 일평균 570억 쿼리양을 기록하고 있어 DNS 트래픽 분석에서는 대용량 처리가 요구된다.

본 논문에서는 초당 5만쿼리 이상의 실시간 DNS 트래픽 수집을 고려하여 대규모 데이터베이스에 적용되어도 높은 정확성과 속도가 가능한 베이지안 분류기를 적용하였다.

단순 베이지안 분류기(Naïve Bayesian Classifier)는 통계적 분류기로서, 주어진 튜플이 특정 클래스에 속할 확률인 클래스의 소속 확률을 예측한다[10]. 이때, 단순 베이지안 분류기는 주어진 클래스의 한 속성 값이 다른 속성의 값과 상호독립임을 가정한다.

m개의 클래스 $C_1, C_2, ..., C_m$와 n개의 데이터 속성 $A_1, A_2, ..., A_n$ 으로 구성되는 튜플에 대한 n개의 측정값으로 표현되는 n-차원의 속성 벡터 $X = (x_1, x_2, ..., x_n)$이 있다.

실데이터 X 분류는

$\arg max_{C_j \in C} P(C_j) \prod_{k=1}^{n} P(x_k | C_j)$ 최대값을 갖는 클래스로 분류된다.

Ⅳ. 사이버 위협 도메인 탐지 시스템

본 논문의 DNS 트래픽 기반의 비정상 도메인 탐지 시스템은 데이터 수집 및 모니터링 기능, 화이트/블랙 리스트 처리 기능, 비정상 도메인 탐지 기능으로 그림 4와 같이 시스템이 구성된다.

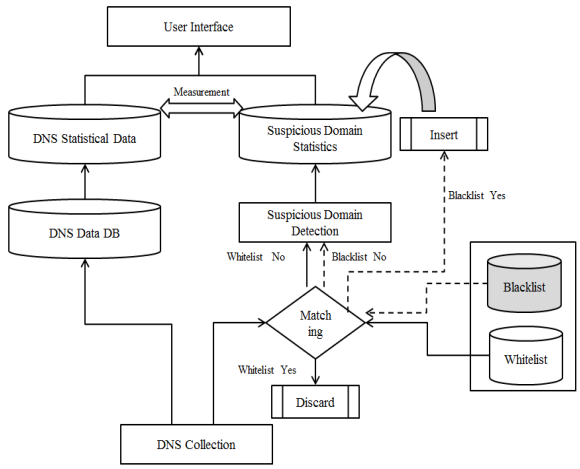

그림 4. DNS 트래픽 기반의 사이버 위협 도메인 탐지 시스템 구조
Fig. 4. Cyber threats domain detection system structure based on DNS traffic

4.1. DNS 트래픽 모니터링

본 시스템은 DNS 서버의 질의(query), 응답(resource record) 트래픽을 수집 및 모니터링하여

www.dbpia.co.kr

통계 데이터를 도출하는 기능이다. DNS 트래픽은 초당 5만쿼리 이상이 DNS 서버에게 질의하면 그에 대한 응답처리를 해야 한다. DNS 데이터 모니터링을 하기 위해서는 대용량의 데이터 처리가 중요하다. 모니터링을 위한 주요 기능으로는 다음과 같은 통계 데이터를 도출한다.

- 단위시간당 전체 트래픽 통계
- 단위시간당 DNS 질의 통계
- 단위시간당 DNS 응답 통계
- DNS 질의 시간 차 통계
- 평균 TTL 값 통계
- 질의 도메인 TOP N
- 응답 오류 값(RCODE) 통계

4.2. 화이트 리스트/블랙리스트 기능

화이트리스트는 포털 사이트(portal site)와 같이 전역적으로 잘 알려진 정상 도메인들의 리스트로써[13], DNS 수집 단계에서 필터링한다.

블랙리스트는 전역적으로 잘 알려진 비정상 도메인들의 리스트로서, 수집기에서 비정상 도메인 탐지 전에 사전 처리한다. 이러한 화이트/블랙리스트 기능은 탐지 모듈의 오버헤드를 줄여줌으로써 성능이 향상될 뿐만 아니라 오탐(false positive) 혹은 미탐(false negative)를 방지한다.

4.3. 사이버 위협 도메인 탐지

비정상 도메인을 탐지 시스템은 학습 단계(learning step)와 분류 단계(classification step)로 구분된다. 학습단계에서는 훈련용 데이터를 분석한다. 사전에 학습된 데이터를 통해 분석성분들을 추출하여 수집된 DNS 트래픽을 분류 알고리즘(classification algorithm)을 통한 분류규칙(classification rule) 즉 분류기를 모델링하여, 의심 도메인을 질의하는 쿼리를 분류한다. 이때, 각 분류기는 최대우도(maximum likelyhood) 개념을 기반으로 분포를 추론하며, 각 특성의 상관 관계 및 추론 분포를 기반으로 파라미터 추출이 된다. 추출된 파라미터는 분류 기준으로서 비정상 쿼리를 분류하는데 이용한다. 각 파라미터의 정량적 위치에서 상대 분포를 확인하며, 각 클래스별 상태 분포 정상 분포 i, 비정상 분포 j 에서 $i=0\sim1, j=0\sim1, i+j=1$의 기본 확률 값으로 도출한다. 도출된 i,j를 이용하여, $j\geq0.5$의 경우 좀비 노드로 분류하며, 해당하는 노드에서 질의하는 도메인 주소를 비정상 도메인으로 분류한다.

4.4. 비정상 도메인 비정상도(abnormality) 도출

본 논문에서는 확률값 i,j을 이용하여 좀비 노드를 분류하고, 좀비 노드에서 질의되는 도메인 정보를 도출하여, 도메인(D_j^n, j: 좀비 노드, n: 도메인 식별자)의 발생 횟수를 카운팅($Count(D_j^n)$)한다.

구체적으로, 정상 확률의 분포와 비정상 확률의 분포의 사후 확률을 $p(i), p(j)$로 정의하고, 악성에 대한 $p(j)$가 0.5 이상인 노드에서 질의되는 DNS 쿼리 데이터의 도메인 D_j^n를 확인한다. 비정상 도메인 D_j^n는 이전에 탐지된 비정상 노드에서 도출된 도메인과 비교하여, 동일한 도메인들이 탐지되었을 경우 보다 위험한 도메인으로 확인할 수 있다.

이와 같이, 비정상도를 정량화하여, 위험도를 정량적으로 도출하기 이전에 다음과 같은 과정을 수행해야 한다.

① 비정상 확률의 분포의 사후 확률$p(j)$을 확인

② 쿼리 데이터의 도메인(D)를 확인하고, 확인된 도메인(D)과 기존의 좀비 노드에서 발생한 도메인을 비교하는 과정

③ 좀비 노드에서 발생한 도메인을 도메인별 발생 횟수 ($Count(D_j^n)$) 도출

도메인의 비정상도는 다음 식 (1)과 같이 도메인별 비정상 확률의 평균값으로 도출한다.

$$Abnormality_n(D_j^n)=\frac{Abnormality_{n-1}(D_j^n)*(k-1)+P(j')}{k},$$
$$k=count(D_j^n)\ \text{현재까지 측정된 도메인의 수} \quad (1)$$

4.5. 시스템 개발 및 실험

4.5.1. 시스템 개발

사이버 위협 탐지 시스템의 사용자 인터페이스는 데이터 모니터링 기능 및 사이버 위협 도메인 탐지 기능으로 크게 구분된다. 대용량 데이터 처리를 위해 개발 시스템 사양은 표 1과 같다.

표 1. 개발 시스템 사양
Table 1. Development system specification

System	System Specification
Main CPU	2.4GHz/6Core/12MB Cache/16G Memory
OS	Redhat Enterprise 5.0
Interface	Gigabit server adapter
DBMS	Oracle Enterprise

www.dbpia.co.kr

그림 5는 수집데이터의 모니터링 및 통계 데이터(단위시간당 전체 트래픽 통계/단위시간당 DNS 질의 통계/단위시간당 DNS 응답 통계/DNS 질의 시간 차 통계/평균 TTL 값 통계/질의 도메인 TOP N/응답 오류 값(RCODE) 통계)를 나타낸다. 그림 5를 통해 DNS서버로 입출력되는 DNS 트래픽의 상황을 모니터링 할 수 있다.

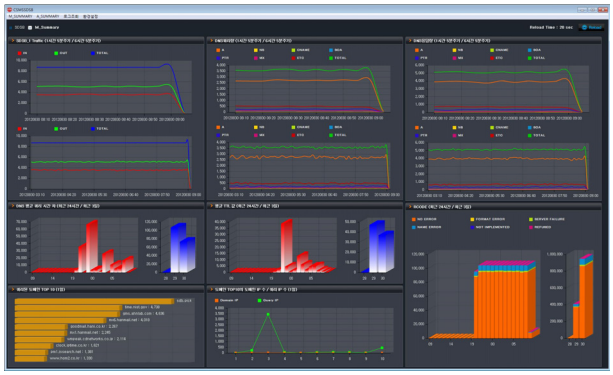

그림 5. DNS 트래픽 모니터닝 및 통계 데이터 사용자 인터페이스
Fig. 5. User interface of DNS traffic monitoring and statistical data

그림 6은 사이버 위협 도메인 탐지 결과와 위협 도메인과 정상 도메인간의 비교 통계 데이터들을 나타내는 사용자 인터페이스이다. 특히, 그림 6은 탐지된 비정상 도메인에 대한 통계 데이터를 포함한 도메인당 쿼리 IP, IP당 쿼리 도메인, 도메인 IP 평균 변화, 도메인당 TTL 값들의 정상 도메인과 비정상 도메인간의 비교 통계 데이터를 통해 정상 도메인과 비정상 도메인간의 특징을 도식화할 수 있다. ISP 망에서의 덤프(dump)한 DNS데이터를 tcpreplay로 일정 트래픽양으로 전송하여 테스트한 결과이다.

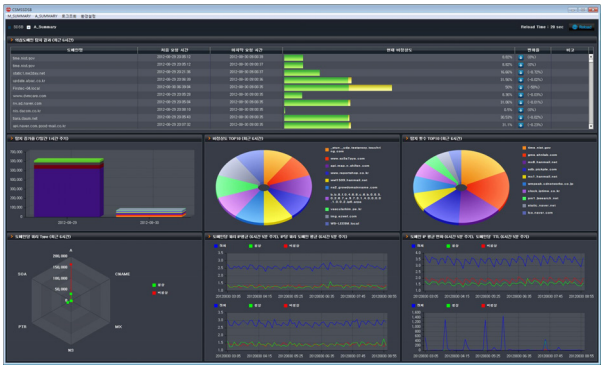

그림 6. 사이버위협 도메인 탐지 및 통계 데이터 사용자 인터페이스
Fig. 6. User interface of Cyber threats domain detection and statistical data

4.5.2. 실험결과

본 개발 시스템의 실험을 위해 첫 번째로는 실험 단계의 데이터는 공격과 정상 비율을 데이터 분류에서 주로 사용하는 비율인 7:3 비율로 구성한 데이터로 실험한 결과 우리가 예측가능한 사이버 위협 도메인 탐지를 99%이상의 결과가 도출되었다. 두 번째 실험으로는 ISP망에서의 발생되는 DNS 트래픽으로 실험한 결과 수집 데이터 1,501,824개의 도메인에서 79,214(18.9%)의 사이버 위협 도메인을 탐지하였다.

V. 결 론

최근 봇넷 기술은 C&C서버와 좀비간의 통신을 위해 DNS 서비스를 이용한 기술들이 증가되고 있다. 반면에, DNS 서비스는 인터넷 서비스를 위한 편리하면서도 중요한 네트워크 인프라 서비스로써, DNS 서비스에 보안 측면을 위한 DNS 트래픽 차단과 같은 대응 방법은 네트워크 서비스의 QoS를 감소시키는 것임으로 적용이 어려운 현실이다. 하지만, 최신 봇넷과 같은 DNS서비스를 이용한 네트워크에서의 비정상 행위들이 빈번하게 발생함에 따라, 본 논문에서는 DNS 트래픽 기반의 비정상 행위에 대한 분류 시스템을 개발 및 실험하였다, 특히, 본 논문의 분류 시스템에서는 기존의 알려진 악성 좀비의 행위부터 알려지지 않은 악성 좀비의 행위까지 DNS 쿼리를 질의하는 좀비의 행위를 확인하여 비정상치를 확인한다. 대부분의 봇넷 형식의 악성코드 및 악성 행위가 짧은 시간적 주기로 변경되기 때문에 기존의 악성 행위의 탐지 기반 또는 대부분의 네트워크에서 사용 중인 시그너쳐 기반의 탐지 기술이 한계를 가지게 된다. 본 논문에서 제안된 사이버 위협 도메인 탐지 시스템은 지도 학습 기반의 DNS 트래픽 분석을 통한 사이버 위협 도메인을 탐지함으로써 지속적인 정상 및 비정상에 대한 학습 기반으로 변화되는 봇넷의 행위 변화와 관계없이 지속적인 관제 및 탐지가 가능하다.

References

[1] S. Lim, J. Kim, B. Lee, "A Study on the Prediction and Analysis of Cyber Threats", *in Proc. KICS*, vol. 48, pp. 125-126, 2012.

[2] L. Bilge, E. Kirda, C. Kruegel,M. Balduzzi, "EXPOSURE: Finding malicious domains using passive dns analysis", *in Proc. of the Annual Network and Distributed System*

www.dbpia.co.kr

Security (NDSS 2011), Feb. 2011.

[3] H. Choi, H. Lee, H. Lee, H. Kim, "Botnet detection by monitoring group activities in DNS traffic", *in 7th IEEE Int. Con. Computer and Information Technology 2007. (CIT 2007)*, pp. 715 – 720, Oct. 2007.

[4] J. Dietrich, C. Rossow, F. Freiling, On Botnets that use DNS for Command and Control, Retrieved Jun., 01, 2012, from http://www.syssec-project.eu/media/page-media/3/dietrich-ec2nd11.pdf.

[5] G. Gu, J. Zhang,W. Lee, "BotSniffer: Detecting botnet command and control channels in network traffic", *in Proc. of the 15th Annual Network and Distributed System Security Symposium (NDSS 2008)*, Feb. 2008.

[6] G. Gu, R. Perdisci, J. Zhang,W. Lee, "BotMiner: clustering analysis of network traffic for protocol-and structure-independent botnet detection", *in Proc. of the 17th conference on Security symposium, 2008*, pp. 139 – 154, Aug. 2008.

[7] R. Villamarín-Salomón, J. C. Brustoloni, "Bayesian bot detection based on DNS traffic similarity", *in Proc. of the 2009 ACM symposium on Applied Computing*, pp. 2035 – 2041, Mar. 2009.

[8] R. Villamarín-Salomón, J. C. Brustoloni, "Identifying botnets using anomaly detection techniques applied to DNS traffic", *in Consumer Communications and Networking Conference 2008 (CCNC 2008)*, pp. 476 – 481, Jan. 2008.

[9] H. Tu, Z. Li,B. Liu, "Detecting botnets by analyzing DNS traffic", *Intelligence and Security Informatics*, pp. 323 – 324, Apr. 2007.

[10] J. Han and M. Kamber, Data Mining: Concepts & Techniques, 2nd Ed., Elseviser Inc., 2007.

[11] S.H Lim, J. Cho, J.H. Kim, B.G. Lee, "Feature Selection with PCA based on DNS Query for Malicious Domain Classification", *Computer and Communication Systems*, vol.1, no.1, pp. 55-60, Oct. 2012.

임 선 희 (Sun-Hee Lim)

1999년 2월 고려대학교 컴퓨터학과 학사
2005년 2월 고려대학교 대학원 정보보호학과 공학석사
2010년 8월: 고려대학교 대학원 정보보호학과 공학박사
2010년~현재 한국전자통신연구원 선임연구원
<관심분야> 무선이동통신보안, 정보보호, 사이버보안, 융합보안기술

김 종 현 (Jong-Hyun Kim)

2000년 오클라호마주립대 컴퓨터학과공학석사
2005년 오클라호마주립대 컴퓨터학과공학박사
2005년~현재 한국전자통신연구원 선임연구원
<관심분야> 정보보호, 사이버보안, 역추적기술

이 병 길 (Byung-gil Lee)

1991년 경북대학교 전자공학과 졸업 학사
1993년 경북대학교 대학원 전자공학과공학석사
2001년 경북대학교 대학원 전자공학과공학박사
2001년~현재 한국전자통신연구원 융합보안연구팀 팀장(책임)
<관심분야> 융합보안기술, 사이버보안기술, 홈랜드보안기술

www.dbpia.co.kr