한국항행학회 논문지 제17권 제6호 2013년 12월 (JKONI 17(6): 816-822, Dec. 2013)

사이버공격 탐지를 위한 클라우드 컴퓨팅 활용방안에 관한 연구

A Study on Cloud Computing for Detecting Cyber Attacks

이준원*, 조재익**, 이석준***, 원동호*

Jun-Won Lee*, Jae-Ik Cho**, Seok-Jun Lee***, Dong-Ho Won*

요 약

최근 악성코드의 다양화와 변종 발생 주기가 기존대비 지극히 단시간에 이루어지고 있으며, 네트워크 환경 또한 기존 보다 그 속도와 데이터 전송량이 급격히 증가하고 있다. 따라서 기존 침입 탐지 연구 및 비정상 네트워크 행위 분석 연구와 같이 정상과 비정상 네트워크 환경을 구성하여 데이터를 수집·분석하는 것은 현실적으로 환경 구성에 어려움이 많다. 본 논문에서는 기존 단순 네트워크 환경이 아닌 근래 많이 연구가 진행되고 서비스가 활발히 이루어지고 있는 클라우드 환경에서의 악성코드 분석 데이터 수집을 통하여 보다 효과적으로 데이터를 수집하고 분석하였다. 또한 단순한 악성 코드 행위가 아닌 DNS 스푸핑이 포함된 봇넷 클라이언트와 서버를 적용하여 보다 실제 네트워크와 유사한 환경에서 악성 코드 데이터를 수집하고 분석하였다.

Abstract

In modern networks, data rate is getting faster and transferred data is extremely increased. At this point, the malicious codes are evolving to various types very fast, and the frequency of occurring new malicious code is very short. So, it is hard to collect/analyze data using general networks with the techniques like traditional intrusion detection or anormaly detection. In this paper, we collect and analyze the data more effectively with cloud environment than general simple networks. Also we analyze the malicious code which is similar to real network's malware, using botnet server/client includes DNS Spoofing attack.

Key words : Packed technique, Malicious code, Zombie client, Automatic analysis, Anti-malware

I. 서 론

2011년 안전행정부에 의해 발간된 국가정보화 백서에 따르면 우리나라는 세계최초로 인터넷 보급률이 80%를 넘었고, 스마트 폰 가입자가 1,000만 명을 넘어섰으며 인터넷 사용자 수는 무려 3,700만 명 이상이다. 또한 2010년 UN이 전 세계 192개국을 대상으로 실시한 전자정부 평가에서 한국이 1위를 차지하기도 하였다. 이와 같이 국가정보화는 선진국 수준에 이르고 있으나 이에 따른 정보보호대책은 상대적으로 미흡하여 국가·공공분야 전산망을 대상으로 한 해킹사고는 2008년까지 약 6,500여건이나 발생하였고, 매년 증가 추세에 있다. 해킹공격 수법도 점차 지능화·첨단화·조직화 되어 가고 있으며, 공격목적 또한 해커 개인의 실력을 과시하기 위한 단순공격에서 국가기밀이나 첨단산업기술 등 정보절취 또는 국

* 성균관대학교 컴퓨터공학과 (Division of Computer Engineering, Sungkyunkwan University)
** 삼성전자 책임연구원(Samsung Electronics)
*** 아주대학교 컴퓨터공학과 석박사통합과정(Division of Computer Engineering, Ajou University)
· 제1저자 (First Author) : 이준원(Jun-Won Lee, tel : +82-31-290-7213, email :damooki@naver.com)
· 접수일자 : 2013년 11월 12일 · 심사(수정)일자 : 2013년 11월 12일 (수정일자 : 2013년 12월 21일) · 게재일자 : 2013년 12월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.6.816

가정보통신망 마비를 노린 사이버정보전 양상으로까지 변화하고 있어 국가안보에 직접적인 위협요인으로 대두되고 있다.[1]

점점 보안 위협이 증가하는 반면에 인터넷 환경은 스마트폰, 스마트 태블릿 등 스마트기기의 폭발적인 성장과 와이브로(WiBro), 롱텀에볼루션(LTE) 등 새로운 통신방식의 적용으로 인해 'always connected' 환경으로 성장하여 해커들의 공격 루트는 무궁무진 하다고 볼 수 있다. 또한, 국가·공공분야 행정환경도 오프라인, 제한된 비공개 업무환경에서 점차 인터넷 기반의 공개 서비스로 진화함에 따라 정보보호 환경은 날로 취약해져가는 추세이다. 그 결과 국가 사이버 보안 취약성은 기존의 침입탐지·차단, 인증 및 암호화 등의 정보보호기술 및 시스템 운용만으로는 사이버 공격이나 취약요인에 대해 완벽히 대처할 수 없는 한계상황에 직면해 있다.

이러한 사이버 보안 취약요인을 해결하기 위해 세계 각국은 사이버 공격 대응책 마련에 국가의 총력을 기울이고 있는 실정이다. 미국은 사이버 보안 5대 전략을 발표하고 2010년 5월 사이버 사령부를 창설하여 미 전역은 물론 세계 사이버 공간 방어에 총력을 경주하고 있다. 유럽은 '네트워크정보보안청'을 출범시켜 유럽 전역에 대한 사이버 위기관리체계를 구축하고 국가 간 보안정보 공유를 강화하고 있는 실정이다.[2]

본 논문에서는 이러한 상황에서 다양한 형태의 사이버 공격을 탐지하고 실행 검증 할 수 있는 클라우드 컴퓨팅 기반의 테스트 베드 방안을 제안하고 검증하였다.

본 논문은 2장에서 다양한 보안 위협과 최근 사이버 공격 형태를 알아보았다. 3장에서는 클라우드 기반의 악성공격 탐지 방안을 제시하였고, 4장에서는 실험을 통해 제안 방법을 검증하였다. 5장에서는 결론 및 향후 연구 방향을 제시하였다.

Ⅱ. 관련연구

2-1 최근 보안 위협 동향

그림 1. 모바일 4대 영역별 보안위협[3]
Fig. 1. Security threats of four major mobile domains

(가) 모바일 디바이스 위협

스마트폰 및 스마트 패드의 보급이 증가함에 따라 네트워크의 영역은 더 넓어졌다. 언제 어디서나 스마트 디바이스를 이용하여 인터넷에 접속할 수 있으며, 그것은 곧 스마트 디바이스가 위협 대상이 될 수 있다는 것이다. 특히 대부분의 스마트폰은 PC의 운영체제를 모바일기기에 맞게 수정하여 설계하기 때문에 그 구조는 PC와 비슷하고, 이는 해커의 입장에서 전혀 새로운 공격 방식을 고안하지 않아도 보다 쉽게 공격할 수 있는 가능성이 열려 있는 것으로 볼 수도 있다. 모바일 디바이스 사용률이 높아질수록 중요 데이터들이 모바일 디바이스로 옮겨질 것이고, 금융거래 등 보안에 민감한 서비스들도 모바일 디바이스로 집중될 것이다. 따라서 네트워크를 통한 공격은 모바일 디바이스를 이용하거나 모바일 디바이스를 대상으로 할 수 있다.

(나) SNS(소셜 네트워크 서비스) 위협

2010년부터 SNS를 통해 악성코드를 전파하는 사례가 종종 발생하고 있다. SNS는 데이터가 확산되는 속도가 매우 빠르고, PC·모바일기기·스마트TV 등 다양한 기기에서 접속이 가능하므로, 다양한 대상을 타겟으로 하는 공격 경로가 될 수 있다. 대부분의 공공기관이나 대기업에서 사용하는 업무용 PC에서도 SNS이용이 제한되지 않고, 악성 웹페이지로 링크 유도, SNS의 플랫폼상의 사용자 어플리케이션을 통한 악성코드 배포 등이 가능하기 때문에 SNS 사용 및 관리에 있어 주의할 필요가 있다. 또한 여러 SNS 서비스를 위장한 악성 페이지 및 악성 어플리케이션이 등장하여 사용자들에게 위협이 되고 있다.

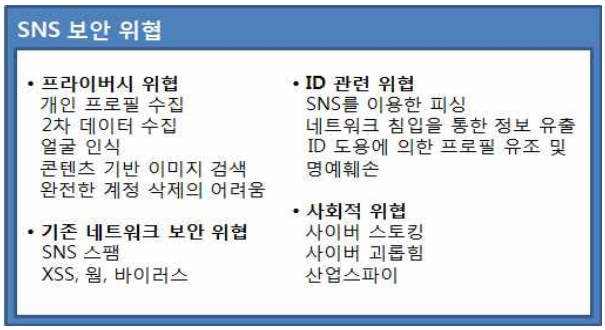

그림 2. SNS 보안 위협[4]
Fig. 2. Security threats of SNS

(다) 사회 기반시설을 겨냥한 공격

2010년 스턱스넷(Stuxnet)은 사회 기반 시설이 사이버 공격 대상이 될 수 있음을 증명하였다. 사이버 미사일이라고도 불리는 스턱스넷(Stuxnet)은 이란의 원자력 발전소 제어시스템(SCADA)을 감염시켜 원심분리기 오작동을 유발하였고, 이 사례는 외부와 차단된 폐쇄망이라고 생각해 외부로부터의 공격에 안전하다고 여겨지던 발전소·교통·전기·수도 등과 같이 국가적으로 크게 문제가 될 수 있는 사회 기반 시설의 제어시스템도 충분히 위협 받을 수 있는 대상이 될 수 있다는 것을 보여주었다.

(라) 클라우드, 가상화 기술 위협

세계적으로 클라우드 열풍이 불고 있고, IBM이 '2011 글로벌 CIO 스터디'를 통해 전세계 3,000여명의 최고정보관리 책임자(CIO)를 대상으로 조사한 결과 이들의 60%가 향후 5년이내 클라우드 컴퓨팅 도입을 준비하고 있다고 하였다. 우리나라 또한 안전행정부를 중심으로 '클라우드 기반 범정부 IT 거버넌스 추진계획'을 발표하고 2015년까지 관련 인프라를 구축한다는 계획을 갖고 있다. 이처럼 기업뿐 아니라 정부 기관들도 점차 가상화 혹은 클라우드로 업무 환경을 전환하는 추세이다. 클라우드에서는 클라우드 플랫폼 자체가 악성행위 경유지로 이용되는 사례도 있으며, 클라우드 스토리지의 중요 데이터 유출 사례도 있다. 클라우드의 사용이 많아질수록 이러한 위협도 더 다양해지고, 빈도수도 증가할 것이다. 따라서 보안 위협에 대비해야 할 필요가 있다.

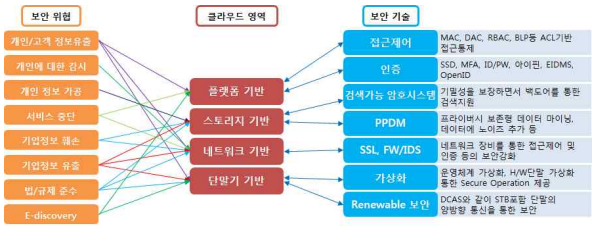

그림 3. 클라우드 보안 위협 및 보안 기술[5]
Fig. 3. Security threats and security techniques of cloud system

2-2 사이버 공격 형태의 동향

(가) 지능형 타겟 위협 (APT, Advanced Persistent Threat)

APT 공격은 개인 해커가 아닌 일련의 범죄 그룹에서 정부 혹은 특정회사의 기밀을 획득하거나 금전을 목적으로 특정 사이트 혹은 기업을 표적으로 삼고 지속적으로 해킹 공격을 하는 것을 말한다. 이는 사회공학, 컴퓨터 취약점 이용, 시스템접근 및 권한 획득, 파일을 여러 개로 나누어 비정기적으로 유출하는 등 크게 4단계의 공격을 수행한다. APT 공격의 주요한 목적은 경제적, 정치적 및 전략적 이득을 위한 정보를 훔치는 것으로 특징은 대상 시스템을 점령해 필요 시 다시 방문하기 쉽도록 구축하기도하며, 오랜 기간 특정 목적을 위해 공격이 진행되어도 인지하지 못한 채 지나갈 수 있다는 점이다.

한두 가지의 보안 솔루션으로는 다계층적인 APT 공격을 막을 수 없으며, 최근 사이버 공격은 특정 기관이나 기업을 겨냥한 지속적인 위협의 성격을 띠고 있기 때문에 보다 철저한 다계층적인 보안 계획 수립이 필요한 실정이다.

○ APT 공격방법

먼저 공격자는 공격 대상에 대해 스피어-피싱을 하기 위한 직원을 찾아낸다. 회사의 주요간부·관리자 등 중요정보에 접근권한이 있는 직원을 찾고, 신뢰하는 사람으로부터 오는 메일 등으로 위장하여 악성코드를 포함시켜 전송하거나, 제로데이 공격 취약점이 있는 첨부파일이나 링크를 포함하여 공격 루트를 얻어낸다. 시스템에 접근한 뒤에는 접근권한 상승을 위한 공격을 수행하여 네트워크 및 시스템 접근권한을

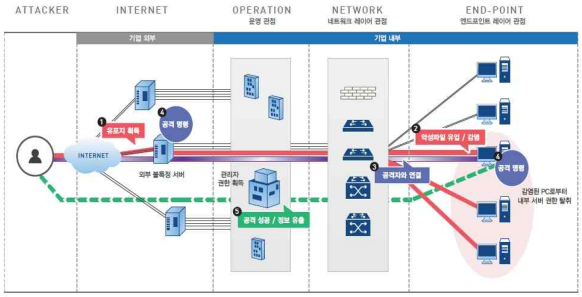

그림 4. APT 공격 진행 프로세스[7]
Fig. 4. APT attack model

얻고, 데이터를 훔쳐 대상 서버 내부에 암호화하거나 압축하여 저장한 뒤 작은 파일로 쪼개 비정기적으로 유출시키는 방법이다.[6]

○ APT의 특성
- 다중 계층 공격(Multi-Layered 공격)
- 네트워크-PC등 총체적인 자원을 활용한 복합적인 공격
- 사회공학적인 요소 필요
- 시스템이 눈치채기 어려움

(나) 인터넷 위협의 대형화 및 조직화

○ 단순한 해킹으로부터 조직화된 공격으로의 변화

과거의 단순한 해킹·웜 등은 감소하는 추세이나, 국가기밀·대기업 등의 서비스 거부 혹은 금품탈취를 위한 영리목적성 공격은 증가하고 있다. 7.7 DDoS나 스턱스넷(Stuxnet) 사례처럼 사전에 치밀한 계획을 갖고 공격 시나리오를 기획하여 웜·바이러스·사회공학 등이 동시적으로 발생하는 복합적이고 지능적이고 조직적인 공격이 증가하는 추세이다.

○ 현실세계와의 연계성 증가 및 대규모의 피해

사이버 공격이 사이버 상에서 종료 되는 것이 아니라 공격받은 기업 및 국가의 이미지 추락 및 경제적인 손실, 개개인의 프라이버시를 침해하는 대규모의 개인정보 유출 사례가 증가하는 추세이다. 개인정보가 유출되는 규모는 몇 천, 몇 만 명이 아닌 천만 단위 이상의 개인정보가 유명 포털사이트, 대기업의 온라인 게임 네트워크 등을 통해 유출되는 사례가 빈번히 일어나고 있다.

Ⅲ. 제안하는 클라우드 기반 탐지 방법

(가) 네트워크 데이터 수집

DNS 서비스 쿼리, 감사 데이터 종류의 로그 데이터, 입출력 바운드의 네트워크 패킷 데이터를 1,000개 호스트 규모로 구성된 중규모 네트워크의 서비스 DNS 전후에서 수집을 목표로 하였다. 수집은 상세 수집 대상을 구조화 하고, 수집에 따른 수집 체계와 검증 체계를 수립하여 최소화된 오류범위 내에서 수집한다. 수집에서는 커널 손실률 2%이내 및 네트워크 장비에서의 패킷 손실률 5%이내를 목표로 하였다.

(나) DNS 데이터 분석, 탐지

수집된 네트워크 패킷 데이터는 알려진 대표적 침입 탐지 시스템으로 검증하여 악성 여부가 포함된 패킷 데이터를 구분하여 분리한다. 분리에는 봇넷 관련 악성 행위, 기타 악성 행위, 정상을 구분하여 봇넷 관련 악성 행위와 정상 상태를 실험 대상 데이터로 선정한다. 선정된 데이터와 DNS 시스템 데이터를 시간적 단위를 이용하여 비교 분석한 후 악성 행위와 관련된 패킷 데이터와 관련된 DNS 시스템 데이터를 구분하여 분리한다. 분리된 데이터를 기계 학습 탐지 데이터로 사용하며, 학습과 정상은 일반적 범주의 정상·공격 분포 비율로 학습·테스트하여 탐지를 수행하고, 탐지 결과의 효과에 따라 DNS 시스템 데이터 및 패킷 데이터의 선택 성분을 변환, 치환, 분류, 성분 선택 조절을 통해 분류 성능을 최적화한다.

(다) 좀비 PC 행위 분석, 탐지

DNS 관련 데이터를 이용하여 탐지 성능을 확인하고, 보다 정확한 데이터를 구성하여 탐지 성능을 증대시키기 위하여 폐쇄망 실험을 한다. 폐쇄망 실험에서는 좀비 PC를 양산 시킬 수 있는 악성 코드를 수십 대 규모의 소규모 네트워크에서 가상 DNS를 설치한 후 강제로 감염시킨다. 이때 호스트 중 일반적 정상 서비스의 서버, DNS 서버, 기본적 허니팟 시스템을 포함시켜 예측할 수 없는 행위나 추가적 동작에 대해서도 모니터링 할 수 있도록 한다. DNS 시스템과 관련하여 중규모 네트워크에서 수집한 경우와 동일하게 데이터를

수집하며, 수집된 데이터를 이용하여 탐지 실험을 한다. 탐지 성능 효과를 기대하기 위해서 기존의 중규모 네트워크 기반의 데이터 셋과 폐쇄망 기반에서 구성된 데이터 셋을 상호 비교하여 추가적 성분이나 데이터의 변환, 치환, 분류, 성분 선택 조절을 한다.

(라) 데이터 셋 생성

중규모 실제 네트워크 및 소규모 폐쇄 실험망에서 수집된 데이터를 이용하여 추후 DNS 쿼리 기반 사이버공격의 탐지 연구에 사용하고, 추후 예측 모델의 신뢰성 있는 기반 데이터를 데이터 셋으로 구성한다. 구성된 데이터 셋은 악성 행위 침입 탐지 실험의 성능으로 확인한다.

(마) 공격 탐지 연구

구성된 데이터 셋의 효과적 성분 선택을 위해 통계적 성분 영향도를 Factor Analysis를 이용하여 확인하며, Principal Component 를 선택한다. 이때 Principal Component 의 Eigen Value 는 전체 영향도의 95%이상을 기준으로 한다. 또한 전체 구성된 데이터의 성분에 있어서 성분 간 데이터의 독립성을 확인하기 위하여 상관관계 분석을 시도하며, 결과에 따라 성분 선택을 조정한다. 정리된 데이터 셋을 이용하여 DNS 쿼리 기반 사이버 공격을 분류하기에 적합한 공격 탐지 모델을 구성한다.

공격 탐지 모델은 DNS 쿼리의 양상이 빠른 시간에 변화되는 점을 감안하여 업데이트 가능한 복합적 기계학습 기반 탐지 모델을 구성하며, 현재까지 고려중인 구성은 다음과 같다.

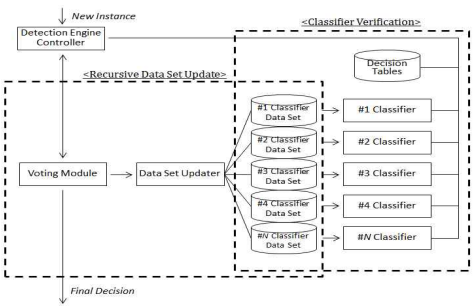

그림 5. 공격 탐지 모델 구성도

Fig. 5. System architecture of attack detection model

각 분류기의 성능에 따라 효과적 성분을 조정하고, 데이터를 변환하여 탐지 성능을 최종적으로 최적화 한다.

Ⅳ. 실험 및 검증

(가) 실험환경구성

본 논문에서 제안한 공격 탐지 모델을 실험하기 위해 다음과 같은 사양으로 실험 환경을 구성하였다.

○ Server

CPU : AMD Phenom II x6 1055T
Memory : DDR3 4GB
HDD : S-ATA2 : 500GB

○ DNS Server

Model : LG-Z10KG
CPU : Intel E4600
Memory : DDR2 2GB
HDD : S-ATA2 320GB

○ Switch

Cisco Catalyst 2950 (WS-C2950G-48-EI)

○ Clients

- Model : Samsung-DMR150

CPU : Intel E8400
Memory : DDR2 2GB
HDD : S-ATA2 130GB

- Model : LG-Z10KG

CPU : Intel E4600
Memory : DDR2 2GB
HDD : S-ATA2 320GB

- Model : Samsung-BP50

CPU : P4-Dual Core 3.2 Ghz
Memory : DDR2 1GB
HDD : S-ATA 130GB

- Model : Samsung-BP55

CPU : Pentium D Dual Core 3.4Ghz
Memory : 512M
HDD : S-ATA 130GB

(나) 네트워크 구성도

제안하는 공격 탐지 모델 실험의 네트워크 구성도는 다음 그림과 같다.

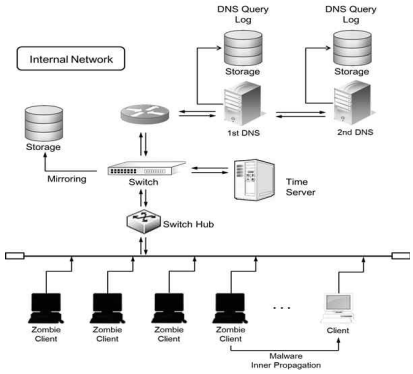

그림 6. 제안 모델 실험 환경 네트워크 구성도
Fig. 6. Network configuration of test environment

표 1. 제안 모델 실험 환경 네트워크 주소 구성
Table 1. Network address configuration of test environment

	Time Svr	1stDNS	2ndDNS		
192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.4		
		Client	Client	Client	Client
		192.168.1.13	192.168.1.14	192.168.1.15	192.168.1.16
Client	Client	Client	Client	Client	Client
192.168.1.21	192.168.1.22	192.168.1.23	192.168.1.24	192.168.1.25	192.168.1.26
Client	Client	Client	Client	Client	
192.168.1.31	192.168.1.32	192.168.1.33	192.168.1.34	192.168.1.35	
Client	Client	Client	Client	Client	Client
192.168.1.41	192.168.1.42	192.168.1.43	192.168.1.44	192.168.1.45	192.168.1.46
Client	Client	Client	Client		
192.168.1.51	192.168.1.52	192.168.1.53	192.168.1.54		

실험에서는 전체 클라우드 노드에서 발생되는 패킷 데이터를 수집하는 Mirror 서버와 실제 네트워크 구성과 유사한 환경을 구성하기 위해 포함시킨 가상 1차 DNS·2차 DNS를 포함하였으며, 전체 가상 노드의 패킷 수집 시간을 정확하게 기록하기 위하여 Time 공유 시스템 노드, 기타 그 밖의 클라이언트로 구성하여 봇넷 클라이언트를 배치하였다. 패킷은 0.1% 이하의 손실률로 수집되었으며, 각 가상 노드에

표 2. 각 노드별 수집 패킷 수 및 수집 시간
Table 2. Packet count and packet collection times of each nodes

	Packet count	First packet	Last packet
Mirror	387,619,316	2011-07-29 11:00:03	2011-08-01 11:08:11
1st DNS (000.000.217.192)	2,421,275	2011-07-29 10:59:44	2011-08-01 11:15:34
2nd DNS(000.000.217.193)	2,398,922	2011-07-29 11:00:22	2011-08-01 11:16:46
Bot server (000.000.217.204)	3,685,171	2011-07-29 11:01:39	2011-08-01 06:39:11
Client21 (000.000.217.198)	3,351,240	2011-07-29 11:01:36	2011-08-01 06:07:57
Client22 (000.000.217.199)	28,873,821	2011-07-29 11:01:38	2011-08-01 11:02:18
Client24 (000.000.217.204)	19,444,043	2011-07-29 11:01:38	2011-08-01 11:00:59

서 발생된 패킷의 수와 전체 Mirror 노드에서 수집된 패킷의 수 또한 0.1% 이하의 오차 범위 내에서 수집되었다.

V. 결 론

본 논문에서는 근래 많이 이용되고 있고, 사설 네트워크 구성이 유연한 클라우드 환경을 네트워크 악성 행위 데이터 수집을 위한 시험 환경으로 구성하였다. 논문에서의 실험은 실제 소규모 네트워크 환경과 유사한 네임서버 시스템 노드와 전체 패킷 발생 시간을 기록하고 이후 비교하기 위해서 시간 동기화 시스템 노드, 그리고 봇넷 클라이언트 감염을 위한 일반 노드를 가상화하여 구성하였다. 실험 결과 실제 네트워크 환경에서와 같은 네트워크 패킷 데이터가 수집되었으며, 손실률 또한 최소화 되어 효과적인 네트워크 데이터 수집이 가능하였다.

향후 본 논문의 실험 결과 및 환경 구성을 이용하면 기존과 같은 소규모 네트워크를 실제 구성하지 않고도 악성코드 행위에 대한 네트워크 패킷 데이터 기반연구, 악성코드 행위분석 등에 보다 효과적인 환경을 클라우드 환경 하에서 구성할 수 잇다. 향후 필요

한 연구로는 클라우드 기반 악성코드 탐지 및 분석 등이 있다.

Reference

[1] SungKyong Eun, "Cloud Computing Security Technology", *No.20-2, Review of KIISC,* 2010.

[2] Taehyung Kim, Inhyun Kim, Changwoo Min, Yeongik Eom, "The Trends of Cloud Computing Security Technology", *No.30-1, Communications of the Korea Information Science Society,* 2012.

[3] Korea Communicaions Commission, MOSPA, MOTIE, 2011 National Information Security White Paper, p.305, 2011.

[4] Boan News, "Enhancing the security of SNS is what we need to do", http://www.boannews.com/media/view.asp?idx=22775, Sep 2010.

[5] Trend Micro 2011 Security News, http://kr.trendmicro.com/kr/about/events/eventcalendar/event/20110803045254.html, Aug 2011.

[6] ITL-SANS KOREA, “Summary of Intelligent Persistence Hacking APT attack”, May 2011.

[7] Ahnlab Web Document, “[Special Report] Revealed APT attack secrets”, Oct 2011.

[8] Wenke Lee, Salvatore J. Stolfo, "A framework for constructing features and models for intrusion detection systems", *ACM Trans. Inf. Syst. Secur. 3,* 2000

[9] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", *44th Hawaii International Conference on System Sciences 2011.*

[10] W. Jansen, and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", January, 2011

이 준 원 (Jun-Won Lee)

1985년 : 한양대 전자공학학사
1996년 : 연세대 전자공학석사
2005년 : 한국인터넷진흥원 연구원
2006~현재 : 성균관대 컴퓨터공학 박사과정
관심분야 : 악성코드 분석, 해킹사고 조사 및 분석, 보안관제

조 재 익 (Jae-Ik Cho)

2005년 : 동국대학교 컴퓨터학과 학사 졸업
2008년 : 고려대학교 정보보호대학원 석사 졸업
2012년 : 고려대학교 정보보호대학원 박사 졸업
2012년~현재 : 삼성전자 시스템LSI 책임연구원
관심분야 ; 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지

이 석 준 (Seok-Jun Lee)

2011년 : 아주대학교 학사 졸업
2011년~현재 : 아주대학교 대학원 석박사 통합과정
관심분야 : 비정상행위 탐지, 스마트그리드 보안, 디지털 포렌식

원 동 호 (Dong-Ho Won)

1976년~1988년: 성균관대학교 전자공학과(공학사, 공학석사, 공학박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 일본 동경공업대 객원연구원
1988년~2003년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
현재 : 성균관대학교 전자전기컴퓨터공학과 교수, 한국정보보호학회 명예회장
관심분야 : 정보보호, 암호이론, 정보이론