Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.12.1849

명령제어서버 탐색 방법 - DNS 분석 중심으로

천양하*

A Study of Command & Control Server through Analysis - DNS query log

Yang-Ha Cheon*

요 약

서비스 거부공격, 즉 DDoS(Destribute Denial of Service) 공격은 정상적인 사용자가 서비스를 이용하지 못하도록 방해하는 공격 기법이다. DDoS 공격에 대응하기 위해서는 공격주체, 공격대상, 그리고 그 사이의 네트워크를 대상으로 다양한 기법들이 연구개발 되고 있으나 모두 완벽한 답이 되지 못하고 있는 실정이다. 본 연구에서는 DDoS 공격이 발생하는 근원지에서 공격의 사전 준비작업 혹은 공격에 이용되는 봇이나 악성코드 등이 발생시키는 네트워크 트래픽의 분석을 통해 발견된 악성코드 및 봇을 제거하거나 공격 트래픽을 중도에서 차단함으로써 DDoS 공격에 대해 효율적으로 대응하는 방법을 개발하는 것을 목적으로 한다.

ABSTRACT

DOS attack, the short of Denial of Service attack is an internet intrusion technique which harasses service availability of legitimate users. To respond the DDoS attack, a lot of methods focusing attack source, target and intermediate network, have been proposed, but there have not been a clear solution. In this paper, we purpose the prevention of malicious activity and early detection of DDoS attack by detecting and removing the activity of botnets, or other malicious codes. For the purpose, the proposed method monitors the network traffic, especially DSN traffic, which is originated from botnets or malicious codes.

키워드

Command and control server, DNS query, DDoS Defense, botnet, C&C Server
명령제어서버, DNS 질의, DDoS 방어, 봇넷, C&C 서버

Ⅰ. 서 론

21세기 보안시장은 보안을 위한 또 다른 보안 정책을 도입하는 다단계적 솔루션을 구현한다. 기존의 정보 보안 솔루션과 장비를 지속적으로 구현하면서 추가적인 솔루션 적용을 통해서 공격 목적과 공격 대상에 대한 분리를 통해 단계적으로 방어를 한다[1].

네트워크측면에서 정보침해는 트래픽을 과다하게 발생시켜 네트워크의 기능을 마비시키는 것이 가장 일반적인 유형이다[2].

또한 대상, 범위, 침해방법, 침해로 인한 파급효과, 사회적 문제 야기 등 엄청난 결과를 가지고 온다[3].

최근 발생하는 개인정보탈취 해킹사고는 모두 악성코드에 감염된 PC를 통해서 내부망에 침투를 한 후에 자료를 탈취해가는 공격 방법을 사용하고 있다. 이렇듯 악성코드에 감염된 PC는 외부에서 공격자의 조종을 받아 내부망에 심각한 위협이 되고 있다. 이를 방어하기 위해서는 PC가 감염되지 않게 철저한 대비

* 교신저자(corresponding author) : 용인대학교(yangha00@yongin.ac.kr)
접수일자 : 2013. 10. 27 심사(수정)일자 : 2013. 11. 25 게재확정일자 : 2013. 12. 16

책을 세우는 것이 중요하다. 악성코드에 감염된 PC에 의한 공격을 방어하는 또 다른 방법은 감염된 증상을 파악하여 감염PC를 탐지하는 방법이다. 이것은 감염PC가 가지는 일반적인 네트워크 행위를 기반으로 분석하여 감염PC를 탐지하는 것이며 보안 관리자들 사이에서 좋은 방법으로 인식되고 있다.

공격자가 운영하는 명령제어 서버 역시 인터넷에서 동작하므로 도메인을 가지고 운영이 되며 감염PC는 공격자의 명령제어서버로부터 명령을 수신하기 위해서는 우선 명령제어서버에 접속하기 위해서 반드시 DNS에 질의를 해야 하기 때문이다. 수많은 클라이언트들이 질의하는 DNS 로그를 분석하여 이상 징후를 판별하고 분석결과 나타난 악성 도메인에 대해 상호분석을 수행하여 공격자가 사용하는 명령제어서버를 판별할 수 있게 된다. 그러므로 본 논문에서는 인터넷을 이용하는 모든 단말기들이 반드시 사용해야 하는 DNS(Domain Name System)의 로그를 분석해서 이상 징후를 판단하고 감염PC를 판별하는 기법을 제시한다.[4]

II. 탐지 기법

2.1 좀비PC 탐지 기법

2.1.1 서명기반 탐지 기법

좀비PC의 서명과 행동을 파악, 파악된 지식을 기반으로 좀비PC를 탐지하는 방법으로 대표적인 예로 Snort가 있다. 이러한 시그니처 기반 탐지 방법은, 기존에 발견된 좀비PC나 악성 코드에 대해서는 높은 탐지율을 보이는 장점이 있지만 새로운 좀비PC가 DDoS 공격에 사용되었을 경우 이에 대한 사전 정보가 없기 때문에 탐지가 불가능하다는 단점이 존재한다.

다른 탐지 기법으론 좀비PC의 IRC 닉네임으로 좀비PC임을 판단하는 기법이 있다. 좀비PC들의 IRC닉네임이 일반 사용자PC의 닉네임과 차이점이 존재한다는 점에 착안한 기법이다. 하지만 이러한 탐지 기법은 제한적인 방법이다. 공격자가 좀비PC의 IRC 닉네임을 일반 사용자 PC와 비슷하게 생성하면 탐지가 어렵고, IRC 기반 좀비PC가 아닐 경우에는 탐지가 불가능하다.[5]

2.1.2 허니넷을 이용한 탐지 기법

허니넷을 이용하여 좀비PC를 탐지하는 기법은 허니팟을 이용하여 좀비PC를 잡아낸 후 그 좀비PC를 분석한 결과를 바탕으로 악성코드와 통신을 주고 받는 네트워크 트래픽을 분석하여 C&C 서버나 좀비PC를 찾아내는 방법이다.

이러한 방법은 오탐율이 낮고, 전문 지식이 없더라도 좀비PC를 탐지해 낼 수 있다는 장점이 있다. 하지만 이러한 방법은 좀비PC의 종류가 많아지면 그 종류의 개수만큼 허니팟의 개수가 필요하다. 네트워크 트래픽이 커질수록 허니팟이 많이 필요하게 되기 때문에 일반적인 사용자나 영세기업에서 사용할만 한 방법이 아니다.

2.1.3 이상 행위 탐지 기법

이상 행위 탐지는 네트워크 트래픽의 이상한 점, 집중된 트래픽이나 평소 사용하지 않던 포트를 사용하는 등 일반적인 사용자와 다른 행동을 보이는 것을 을 좀비PC로 의심하고 탐지하는 방법이다. 이상기반 탐지는 새로운 좀비PC라 하더라도 탐지가 가능하기 때문에, 서명 기반 탐지 기법의 단점을 해결한 탐지 기법이다. 하지만 일반적인 사용자와 다른 행동을 보여야 탐지가 가능하기 때문에 좀비PC가 아무런 행동을 하지 않으면 탐지가 불가능하다.[4] 이러한 점을 해결하고 좀비PC뿐만 아니라 C&C 서버까지 알아낼 수 있는 방법을 제시하였다.

2.2 C&C 서버 탐지 기법

2.2.1 트래픽 분석을 이용한 C&C 서버 탐지

Gu[6]등이 제안한 BotMiner는 같은 네트워크상에 속한 좀비PC들이 유사한 트래픽을 발생하거나 유사한 악성행위 패턴을 보이는 것을 이용하여 좀비PC를 탐지한다. 그러나 좀비PC가 되는 순간 C&C 서버를 탐지하는 것이 아니라 이미 감염된 좀비PC의 그룹 행위를 기반으로 C&C 서버를 탐지하고 있으므로 실시간으로 탐지하기에는 어려움이 있다.

봇넷 트래픽 특성 분석 연구[6]에서는 C&C 서버가 좀비PC에 감염된 호스트의 명령이나 제어를 위

해 IRC서버를 이용하는 점을 이용하여, 이때 발생하는 DNS 트래픽을 이용한 C&C 서버 탐지 시스템을 제안하였다. 처음 좀비PC에 감염된 후 IRC 서버에 접속할 때와 C&C 서버에서 이주할 때, IRC 서버의 IP 주소가 변경된 경우 등에서 발생하는 DNS 쿼리를 이용하여 C&C 서버를 일정 수준 탐지할 수 있지만, HTTP/P2P C&C 서버를 탐지하는 데에는 한계가 있다.

2.2.2 좀비PC 행위 분석을 통한 C&C 서버 탐지

좀비PC의 행위 분석을 통한 C&C 서버 탐지 기술의 경우, 허니넷, 백신 샘플 공유 사이트 등을 통해 수집된 좀비PC의 샘플을 가상환경에서 실행한 다음 네트워크 행위를 모니터링해서 C&C 서버를 탐지하는 기술이다.[7][8]

III. 좀비PC 및 C&C 탐지시스템 구축

3.1 DNS와 악성행위의 연관관계

DNS은 현대 인터넷 서비스의 한 근간을 이루고 있는 Domain-to-IP 서비스를 제공함과 더불어, 서비스를 제공하는 네트워크 내의 서버 및 사용자 PC의 네트워크 활동을 개괄적으로 살펴볼 수 있는 위치에 있는 요소이기도 하다.

DNS가 DDoS 공격에 연관되는 경우는 크게 3가지이다.

첫 번째 대다수의 DDoS 공격의 원인인 악성코드가 공격 준비단계나 감염확산 단계에서 DNS를 이용한다는 것이다.

두 번째는 DNS 서비스와 그 네트워크 인프라가 DDoS 공격의 직접적 공격의 도구로서 악용되는 형태의 공격이 존재한다.

세 번째로는 DNS 자체가 DDoS의 공격의 대상이 된다. DDoS 공격의 근원지를 분류하는 접근방법에서 볼 때, 세 번째의 연관성은 첫 번째 경우의 악성코드를 탐지하고 대응함으로써 포괄적으로 보호 될 수 있는 사항으로 둘 수 있다.

3.1.1 DDoS 공격을 수행하는 악성코드의 DNS 이용

봇은 사용자 컴퓨터에 감염되어 활동하는 악성코드이다. 다수의 봇은 봇넷이라는 네트워크를 이루어 공격자의 명령에 의해 DDoS 뿐 아니라 다양한 형태의 공격을 수행한다. DDoS 공격을 발생시키는 근원지의 대다수는 이 봇에 감염된 PC이다.

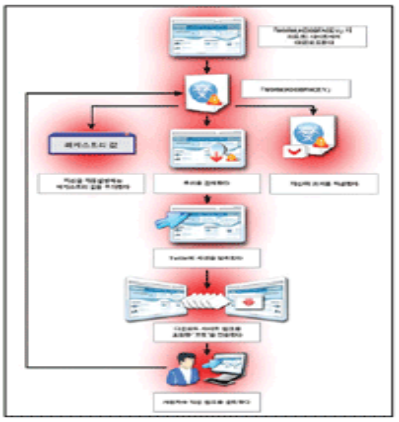

그림 1. 봇넷을 통한 감염 경로
Fig. 1 Infection through a botnet

감염된 PC는 실제 봇코드를 인터넷을 통해 다운로드하고 자신이 감염된 사실을 봇마스터에게 알리기 위해 명령 및 제어 채널에 접속한다. 이후 채널을 통해 봇 마스터로부터 명령을 전달 받고 공격을 수행하게 된다. 이렇게 채널에 접속하여 봇 마스터로부터 명령을 전달받고 공격을 수행하게 된다. 이렇게 채널에 접속하여 봇 마스터로부터의 명령을 받아 악성행위를 수행하는 감염PC의 네트워크가 봇넷이다. 이러한 일련의 네트워크 행위에서 악성코드 역시 DNS를 이용해야 한다.[10]

3.1.2 DDoS 공격 도구로서 DNS 서버 이용

DNS의 NS(Name Server)는 그 컴퓨팅 자원과 네트워크 대역 등이 공격도구로서 사용되기도 한다. 이 경우 DDoS 공격은 분산된 여러 대의 공격지로부터 NS를 거쳐 공격 대상지에 도달하고, NS는 패킷의 크기를 증가시켜 DDoS 공격의 위력을 강화시키는 역할과 더불어 피해자가 공격 근원지를 찾기 힘들게 하는 효과까지 부여한다. 이러한 공격 형태를 Amplification 공격이라 한다.

3.2 DNS를 이용한 좀비PC 탐지 기법

광범위한 네트워크를 대상으로 보안기법을 적용하는 데에 있어 물리적으로 분산되어 있고 그 수가 적지 않은 라우터 혹은 소규모 지역 ISP와 비교하여 DNS는 방어기법의 설치가 용이할 뿐만 아니라 넓은 범위에서 모여드는 정보를 집중된 한곳에서 관찰하고 고나리할 수 있다는 장점을 가진다. DNS는 서비스 권역 내에서 가장 중앙 집중적인 구조를 가지고 있다. DNS 서비스를 제공하는 네트워크의 범위만큼 그 관리 범위에 포함되어 넓은 지역의 사용자 및 기관들이 그 혜택을 받을 수 있다.

Ⅳ. 좀비PC 및 C&C 탐지 시스템 설계

4.1 설계 방법 및 시스템 개요

좀비PC 및 C&C 탐지 시스템은 가장 추상화된 수준의 시스템 배치에서 시스템 내부에서 각기 독립된 기능을 수행하는 모듈과 각 모듈의 내부의 기능, 기능 간의 데이터 흐름과 알고리즘의 수준으로 점차적 세부 설계를 하는 방식을 사용하였다.

제안하는 시스템은 DNS 서버에 들어가거나 서버로부터 나오는 DNS 트래픽을 입력받아 처리하는 구조를 가지고 있다.

좀비PC 및 명령제어서버 탐지 시스템을 중심으로 정보의 입출력 및 주변 시스템과의 연동관계를 고려한 것이다. 시스템의 핵심 기능인 명령제어서버 및 좀비PC 탐지 기능은 비정상 트래픽의 분류, 악성행위의 탐지, 주변 시스템과의 연동으로 수행되며, DNS 서버를 통해 봇에 감염된 좀비PC와 최종적으로 명령/제어 서버(Command & Control Server) 목록을 추출하도록 한다.[6][11]

4.2 좀비PC 및 C&C 탐지 시스템의 상세설계

좀비PC 및 C&C를 탐지하기 위해서는 공격을 수행하는 봇과 같은 악성코드에 감염된 PC와 이를 통제하는 명령제어 서버를 찾는 것이 주된 과제라고 할 수 있다. 시스템의 주 탐지 대상이 되는 DDoS 공격 코드, 봇넷, 악성코드, DNS 캐쉬 포이즈닝 공격 도구 등의 DNS 이용행위 중 정상 사용자와 구분되는 비정상적 특징을 보이는 행위들을 분석한 결과 [표 1]. 표 2, 표 3과 같았다.

표 1. DDoS 공격 코드의 비정상적 DNS 특징
Table 1. DNS unusual feature of DDoS attack code

Subject	DNS Unusual feature	Marker
DDoS Attack Code (A1)	Target Discovery	B11
	RR Request	B12
	Simultaneous use of the DNS service attack code group	B13

표 2. 봇/봇넷의 비정상적 DNS 특징
Table 2. DNS unusual feature of Bot/Botnet

Subject	DNS Unusual feature	Marker
Bot/Botnet (A2)	Periodic C&C Ping/Pong	B21
	Domain group access	B22
	C&C Channel Migration	B23
	Avoid detection for multi-domain IP	B24
	TTL	B25

표 3. 악성코드의 비정상적 DNS 특징
Table 3. DNS unusual feature of malicious code

Subject	DNS Unusual feature	Marker
Malicious code (A3)	Domain group access	B31
	Duplicate / repeat service calls	B32
	Phishing, Pharming for Domain/IP	B33

비정상 DNS 악성행위를 탐지하는데 사용하는 과정은 다음과 같다.

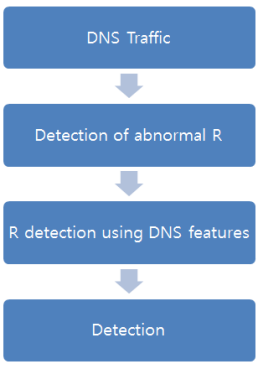

그림 2. 비정상 행위 탐지 과정
Fig. 2 Malicious behavior detection process

좀비PC 및 C&C 탐지 시스템은 수집된 DNS 트래픽으로부터 악성이용 IP/Domain 탐지 시스템으로 비정상 DNS 트래픽을 분류하여 악성행위를 분류, 탐지하고 이를 기반으로 악성 IP 및 Domain 정보를 추출한다.[4]

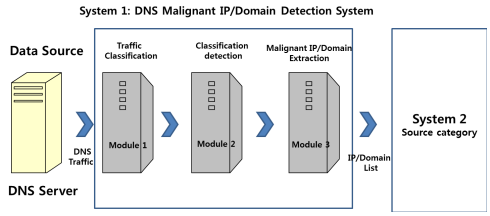

그림 3. 시스템 1 구조도
Fig. 3 System 1 structure

3개의 모듈로 구성되어 있으며 각각의 모듈은 비정상 트래픽 분류, 악성행위 탐지, 악성 IP/Domain 추출의 기능을 담당하고 선행 모듈의 출력이 후방 모듈의 입력이 되는 선형배치를 이루고 있다.

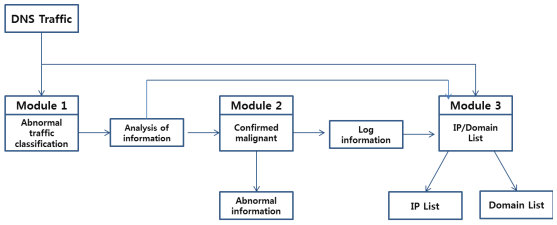

그림 4. 자료 흐름도
Fig. 4 Data flow diagram

그림 4는 시스템1의 내부의 자료 흐름을 도식한 것이다. 이것은 DNS 트래픽을 입력으로 제공받아 각 모듈 간의 처리를 거쳐 최종적으로 시스템 2의 입력이 되는 IP, Domain 리스트를 출력한다.

모듈 1에서는 총 8개의 Rule Checker가 평행하게 동작하도록 설계하였다. Rule Checker들은 DDoS 공격코드, 봇넷, 악성코드 감염 공격 등에서 나타나는 DNS 이용형태 중 정상 사용자와 비교하여 이상 행위를 검사하여 경고한다.[4]

대응 대상으로 삼는 4가지의 행위는 각기 다른 목적으로 DNS를 사용하지만 그 과정 중에 나타나는 비정상 트래픽의 특징은 유사하여, 정의한 8개의 비정상 행위들이 단독적 혹은 복합적으로 나타나는 것으로부터 악성행위의 존재를 판별할 수 있다.

모듈 2는 모듈 1에서 분류된 악성 행위에 대한 규칙과 실제 트래픽을 이용하여 상세 분석을 수행한다. 입력된 비정상 DNS 트래픽에 대한 패턴을 분석하여 DB에 저장된 DDoS, Botnet, 악성코드, DNS 캐시 포이즈닝과 관련된 트래픽과 비교, 확인 작업을 거쳐 어떤 종류의 악성 행위인지 판별한다 알려진 패턴 혹은 새로운 패턴의 악성코드, 보넷 리스트와 이용된 DNS 트래픽 정보를 추출하도록 한다.

패턴으로 사용하는 트래픽의 특성은 아래 표 4와 같다.[4]

표 4. 트래픽 패턴 유사도 평가 요소
Table 4. Traffic pattern similarity evaluation factors

	factor	Ratings	Range
i	Interval	Packets and the regularity of the time interval between packets	0.0-1.0
r	Repeat	Repeat the same query generation	0.0-1.0
p	Path	Similarity of the same quality source	0.0-1.0
b	similarity	The same source group similarity query generation	0.0-1.0

Ⅴ. 좀비PC 및 C&C 탐지시스템 실험 결과

본 장에서는 설계 시스템의 기술검증을 위해 실제 네트워크 트래픽에 적용하여 결과를 도출하였다. 실험은 DNS서버에서 수집된 트래픽을 사용하였다. 실험의 결과로서 탐지된 도메인들은 봇 등의 C&C 또는 배포 도메인으로 의심되는 도메인들이며, 이미 알려진 봇넷의 도메인 또는 주요 악성도메인 경고 사이트들에서 지목된 도메인들이 다수 발견되는 것을 볼 수 있었다.

5.1 시스템 1의 DDoS 공격근원지 탐지 결과

시스템 1의 악성도메인 탐지 성능을 실험하기 위해 실제 네트워크 DNS 트래픽을 대상으로 총 3차례에 걸쳐 시스템의 실험을 수행하였다.

표 5는 실험 결과 도출된 C&C의심 도메인들과 그

평가 척도인 유사도, 그리고 그 정보가 확인된 도메인들의 정보를 정리한 도표이다. 탐지 결과는 국내에 봇넷의 C&C 도메인으로 알려진 경우, Known, 공식적으로 알려지지 않았지만 그 악성 행위가 확인되어 각종 보안사이트에서 C&C로 지목된 경우 Unknown으로 구분하였다.[4]

표 5. 시스템 1 실험 결과
Table 5. System 1 results

Domain	Similarity	Results	ect
bosam	0.9900	Botnet	Drop
shiyansend.zyns	0.9800	Botnet	
vwidget	0.9732	Normal	
shiyansend.solaris	0.9700	Botnet	
desktop2.google	0.9697	Normal	
drsunbo2	0.9530	Botnet	Drop
180.96.114.125	0.9511	Normal	
weather	0.9464	Normal	
clock.iptime	0.9464	Botnet	

Ⅵ. 결 론

본 논문에서는 좀비PC를 생성하는데 주체가 되는 악성코드들의 활동을 탐지함으로서 감염PC를 탐지하고 그 활동을 제한하거나 차단하는데 활용할 수 있는 C&C 탐지 기법을 제안하였다. 이러한 탐지 방법 개발을 통하여 대규모 DNS 환경에서 넓은 네트워크 범위에 걸쳐 악성코드와 DDoS를 일으키는 공격코드, 봇넷의 활동, DNS에 대한 공격들을 탐지하고 그 정보를 제공함으로써, 이를 활용하여 악성코드의 확산과 활동을 제한하고, 이로부터 잠재적 정보유출 위험과 경제적 손실을 예방 할 수 있다. 제안한 좀비PC 및 C&C탐지 방법은 DNS를 이용하여 악성코드들의 활동과 명령제어서버를 분류하는데 필요한 정보를 넓은 범위에 걸쳐 획득하고, 이를 기존의 시스템과 연동하여 그 효과를 증대시킬 수 있도록 설계되었다. 원격접속을 통한 내부망 정보유출을 수행하는 악성봇을 비롯한 악성행위들을 분석하고 정상적 트래픽과 분류하는 기법을 개발함으로서, 기본의 악성행위 뿐 아니라 그와 유사한 행위들을 폭넓게 탐지하여 네트워크의 전체적 보안의 강화효과를 기대해 볼 수 있다.

감사의 글

본 논문은 2013년도 용인대학교의 지원으로 이루어졌습니다.

참고 문헌

[1] Woo-seok Seo, Moon-seog Jun, “A Study on Security Hole Attack According to the Establishment of Policies to Limit Particular IP Area”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 5, No. 6, pp 625-630, 2010. 12.

[2] Young-Dong Kim. “Performance of VoIP Traffics over MANETs under DDoS Intrusions”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 6, No. 4, pp. 43-48, 2011. 07.

[3] Woo-Seok Seo, Jae-Pyo Park, Moon-Seog Jun, “A Study on Methodology for Standardized Platform Design to Build Network Security Infrastructure”, The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 7, No. 2, pp 203-211, 2011. 12.

[4] Yang, JongHyu, “An Empirical Study of Detection Technique for Zombie PC through Analysis of DNS Query Behavior”, Department of IT Policy and Management Graduate School, Soongsil University, 2013.

[3] J. R. Binkley, S. Singh. “An algorithm for anomaly-based botnet detection", In Proceedings of USENIX SRUTI'06, pp. 43-48, 2006.

[4] G Gu, "BotMiner: clustering analysis of network traffic for protocol-and structure-independent botnet detection." Proceedings of the 17th conference on Security symposium. 2008.

[5] Villamarin-Salomon, Ricardo, and Jose Carlos Brustoloni. “Bayesian bot detection based on DNS traffic similarity", Proceedings of the 2009 ACM symposium on Applied Computing. ACM, 2009.

[6] Goebel, J., Holz, T. Rishi, "Identify bot contaminated hosts by IRC nickname evalu-

ation", In Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, p. 8, 2007.
[7] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. "BotHunter: Detecting malware infection through ids-driven dialog", In Proceedings of the 16th USENIX Security Symposium (Security'07), 2007.
[8] http://www.boannews.com/media/view.asp?idx=22777&kind=1
[9] J. R. Binkley, S. Singh, " An algorithm for anomaly-based botnet detection", In Proceedings of USENIX SRUTI'06, pp. 43-48, 2006.

저자 소개

천양하(Yang-Ha Cheon)

2010년 성균관대학교 대학원 정보통신학과 졸업(공학석사)
2013년~숭실대학교 IT정책경영학과 박사과정
숭실대학교 베어드학부 외래 교수
용인대학교 교육대학원 전산학 교수
※ 관심분야 : 모바일 콘텐츠, 빅데이터, 정보보안