情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

악성 봇넷 별 트래픽 분석을 통한 탐지 척도 선정

장 대 일,[1†] 김 민 수,[2] 정 현 철,[3] 노 봉 남[1‡]
[1]전남대학교, [2]목포대학교, [3]한국인터넷진흥원

Selection of Detection Measure using Traffic Analysis of Each Malicious Botnet

Dae-il Jang,[1*] Minsoo Kim,[2] Hyun-chul Jung,[3] Bong-Nam Noh[1‡]
[1]Chonnam National University, [2]Mokpo National University, [3]Korea Information Security Agency

요 약

최근 발생하는 인터넷 상의 악성 행위는 많은 부분 악성 봇넷과 관련이 있다. DDoS 공격이나 스팸 발송, 악성코드 전파, 개인 정보 유출, 피싱 등 대부분의 악성 행위들이 봇넷에 의해 행해지고 있다. 이러한 봇넷을 탐지하고자 네트워크 단에서 악성 봇넷 탐지 시스템이 활발히 연구되고 있지만, 특정한 프로토콜이나 행위, 공격을 수행하는 봇넷에만 적용 가능하다는 단점을 가지고 있다. 이에 본 논문에서는 악성 봇넷을 탐지하기 위한 척도 선정에 관한 연구를 진행하였다. 연구를 위해 악성 봇넷의 트래픽을 수집 및 분석하여 분석된 네트워크 트래픽의 특징에 기반 한 척도를 선정하였다. 본 연구를 통해 악성 봇넷을 탐지하는데 도움이 될 수 있을 것으로 기대한다.

ABSTRACT

Recently malicious activities that is a DDoS, spam, propagation of malware, steeling person information, phishing on the Internet are related malicious botnet. To detect malicious botnet, Many researchers study a detection system for malicious botnet, but these applies specific protocol, action or attack based botnet. In this reason, we study a selection of measurement to detec malicious botnet in this paper. we collect a traffic of malicious botent and analyze it for feature of network traffic. And we select a feature based measurement. we expect to help a detection of malicious botnet through this study.

Keywords: Botnet, Traffic Classification, Botnet Detection

I. 서 론

봇넷은 악의적인 공격자들에 의해 조종되는 시스템인 악성 봇들의 네트워크이다[1]. 공격자들은 원격으로 시스템을 제어하면서 DDoS, 스팸 메시지 발송, 피싱, 개인정보 탈취 등 각종 악성 행위를 한다[2]. 봇넷이 좀비 시스템을 제어하기 위해서 중앙집중형, 계층형, P2P형, 랜덤형 등 다양한 방법들이 사용된다[3]. 중앙집중형은 좀비 시스템을 제어하기 위해 하나 이상의 명령제어 서버를 두고 좀비 시스템에 명령을 하달하는 방식이다. 명령 하달 시, 좀비 시스템이 명령제어 서버로 접근하는 폴링(polling)형, 명령제어 서버가 좀비 시스템에 명령을 하달하는 푸쉬(push)형이 있다. 중앙집중형 구조의 경우 구현은 쉽지만 탐지도 쉽다는 단점을 갖는다[4]. 초기의 많은 봇넷들이 중앙집중형 구조를 갖는다. 계층형 구조는 명령 제어 서버와 좀비 시스템 사이에 프록시를 둠으로써 탐지를 어렵게 한다. 프록시 간에 P2P 통신을 함으로써 실제 명령제어 서버를 감추고, 좀비 시스템은 프록시 서버

접수일(2010년 7월 8일), 게재확정일(2010년 10월 27일)
† 주저자, daels@lsrc.jnu.ac.kr
‡ 교신저자, bbong@jnu.ac.kr

의 제어를 받는 것처럼 보이게 한다[5]. 이러한 노력으로 중앙집중형 구조의 단점을 회피하려 하지만, 지속적인 모니터링으로 명령제어 서버를 탐지 후 차단할 경우 봇넷의 활동을 차단할 수 있다. 이러한 계층형 구조를 갖는 봇넷으로는 웨일덱 봇넷이 있다. P2P 구조는 각 좀비 피어들이 다른 피어들과 통신을 통해 명령을 전파한다. 때문에 명령의 전파 속도는 느리지만 탐지 및 봇넷의 차단이 쉽지 않다. 스톰 봇넷이나 컨피커 봇넷이 대표적인 P2P 봇넷이다. 랜덤형 구조는 앞서 설명한 봇넷의 구조와는 달리 초기 감염시 네트워크를 스캔하여 다른 감염된 좀비 시스템 혹은 명령제어서버를 찾는다[3]. 즉, 악성코드를 분석하여도 명령 체계 및 봇넷의 구조를 알 수 없다는 장점을 지닌다. 하지만 랜덤형의 경우 봇넷을 구성하는 것 자체가 쉽지 않아 아직까지 발견된 랜덤형 구조의 봇넷은 발표되지 않았다.

이에 본 논문에서는 악성 봇넷을 탐지하기 위한 척도 선정하고 각 봇넷에 적용하여 악성 봇넷을 탐지하기 위한 기준을 제시하였다. 이를 위해 각 봇넷의 트래픽을 분석하여 봇넷 트래픽의 특징을 추출하고 봇넷의 세션별 특징을 분류하기 위해 C4.5가 생성한 의사결정트리를 사용하였다. 그 결과 선정된 척도에 기반한 각 봇넷 별 탐지 기준을 만들어 낼 수 있었다.

본 논문의 2장에서는 시스템 구조에 대한 설명을 하고, 3장에서는 C4.5 알고리즘을 이용한 의사결정트리 생성과정을 설명한다. 4장에서는 각 봇넷에 대한 탐지 결과를 설명하고, 5장에서는 결론 및 향후 전망에 대해 언급한다.

II. 관련연구

악성 봇넷은 인터넷 상에서 수행되어지는 많은 악의적인 행위를 수행하고 있고, 이를 해결하기 위해 DNS 정보를 이용[6]하거나 악성 봇넷의 행위 순서[7]를 이용하는 방법, 허니팟을 이용[8,9,10]하는 등 많은 연구가 진행되고 있다.

DNS 트래픽의 그룹 행위를 이용한 봇넷 탐지 연구[6]에서는 단위 네트워크에서 동일한 봇넷에 감염되었을 때 비정상적인 DNS 트래픽 증가를 이용하여 악성 봇넷을 탐지한다. 하지만 이러한 경우 악성 봇넷이 하드코드된 아이피를 사용하면 해당 탐지 시스템을 사용할 수 없게 된다. 봇헌터[7]는 스노트 룰에 기반하여 인바운드와 아웃바운드 트래픽을 분석하여 봇넷의 생명주기와 트래픽이 일치하면 봇을 탐지하는 방법이다. 악성 봇넷의 각 각의 행위트래픽을 프로파일링한 후 프로파일과 일치하는 트래픽의 양이 임계치를 넘어가면 악성 봇으로 탐지한다. 하지만 이러한 경우 변종에 대한 대비나 행위 간에 시간이 길어질 경우 탐지가 어려워진다. 봇 스니퍼[11]는 화이트리스트를 기반으로 의심스러운 트래픽을 걸러낸 후 아이피와 포트 쌍을 토대로 유사한 트래픽을 탐지하는 방법을 사용한다. 프로토콜 및 포트에 독립적이지만 암호화된 통신을 이용할 경우 탐지가 어려워진다. 봇콥[12]은 페이로드 시그니쳐와 n-그램 알고리즘을 이용하여 악성 봇넷을 탐지하는 연구이다. 페이로드의 비트 스트링의 특징을 이용하여 시그니쳐를 생성하고 일반 트래픽으로부터 구분되는 의사결정트리를 생성하였다. 하지만 IRC 봇넷에 한정하고 있어 대부분의 봇넷이 HTTP와 P2P 프로토콜을 사용하고 있는 현재 상황에 적합하지 않다.

III. 악성봇넷 트래픽 분석

본 논문에서는 악성 봇넷을 탐지를 위한 척도를 선정하기 위해 6종의 악성 봇넷의 트래픽을 분석하였다. 이를 위해 가상 머신(vmware)에 윈도우즈 XP sp3를 설치한 후 감염되지 않은 상태에서 임의로 악성 봇 샘플을 실행시킨 후 와이어샤크를 이용하여 네트워크 트래픽을 수집하였다.

[표 1]의 6개 봇넷이 척도 선정을 위해 트래픽을 분석한 봇넷으로 사용하는 프로토콜을 나열한 것이다. 상당히 다양한 프로토콜이 사용하는 것을 확인할 수 있다. 이때 탐지 척도 선정을 위해 DDoS 공격에 사용하는 ICMP나 SMB 프로토콜 등은 제외하기로 한다. 이는 DDoS 공격의 경우 스팸 메시지나 개인정보

[표 1] 봇넷 별 사용 프로토콜 및 수집된 세션 수

봇넷	프로토콜	수집된 세션 수
보박스 (Bobax)	HTTP, SSL, Own Protocol	22,740
브리도랩 (Bredolab)	DNS, SMTP, HTTP, Own Protocol	9,071
컨피커 (Conficker)	HTTP, UDP, SMB	13,567
게그 (Gheg)	SSL, Own Protocol	24,680
넷봇 (Netbot)	UDP, ICMP, Own Protocol	5,355
웨일덱 (Waledac)	HTTP, DNS, SMTP, DCERPC, FTP	49,814

탈취와는 다르게 매 순간 공격자가 트래픽량을 조절하거나 프로토콜을 변경할 수 있기 때문이다. [표 1]에서처럼 각 봇넷의 트래픽은 매우 다른 성향을 보인다. 통신을 위한 프로토콜에서부터 C&C와의 연결주기, 공격 내용, 바이너리 및 탬플릿 다운로드 등 각각의 행위가 서로 다른 방법으로 진행된다.

먼저 보박스 봇넷은 여러 개의 C&C가 존재하는 멀티서버형 구조를 하고 있고, C&C에는 다운로드 서버를 포함하여 각 서버별 통신주기 및 다운로드 받는 바이너리나 탬플릿의 크기를 분석하였다. 그리고 각 봇넷별 스팸 엔진에 따라 스팸 메시지 발송 량 및 탬플릿에 따라 스팸 메시지의 크기가 달라지기 때문에 스팸 메시지 발송량 및 평균 크기를 측정하였다. 이와 유사하게 스펨 메시지를 발송하는 브리도랩 봇넷과 웨일덱 봇넷의 워커봇을 분석하였다[5,13].

컨피커 봇넷은 분석한 봇넷 중 유일하게 확산을 위한 트래픽이 발생하여 TCP 445 포트를 비롯한 SMB 프로토콜에 대한 분석을 진행하였다. 이때 연결되지 않은 TCP 트래픽이 매우 많이 발생하고, 연결된 후 발생하는 트래픽도 매우 규칙적이기 때문에 컨피커 봇넷을 탐지하기 위한 척도로 사용될 수 있다. 또한 다른 봇넷에 사용되지 않은 랑데부 프로토콜에 대한 분석도 같이 진행되었다. 게그 봇넷은 다른 좀비 시스템과의 연결 및 C&C와의 통신에 대한 트래픽 위주로 분석하였다. 게그 봇넷은 SSL을 이용하여 통신을 하고 각 봇들과 TCP를 이용하여 문자열을 전송하는데 이때 다른 서버 정보나 활동에 필요한 데이터를 전송한다. 게그 봇넷이 이런 한 행위를 할 때 TCP 데이터의 크기나 외부 아이피 연결 시 DNS를 사용하지 않는 등의 행위가 발견 되었다. 웨일덱 봇넷은 계층형 구조를 갖는 봇넷으로 프록시 봇과 워커봇으로 구분할 수 있다[5]. 앞서 설명했다시피 워커봇의 경우 일반적인 스팸 봇넷과 동일한 형태를 지니고 있다. 프록시 봇은 워커봇이나 하위 프록시 봇의 요청을 받아 상위 프록시 봇이나 C&C 서버로 연결해주는 역할을 한다. 이때 프록시 봇은 가상 서버 역할을 하기 때문에 인바운드 패킷의 원격지 포트가 80번 포트인 것은 중요한 척도가 될 수 있다. 또한 프록시 봇을 거쳐 질의에 대한 응답을 받기 때문에 일반적인 웹요청에 비해 세션 지속시간이 길어지게 된다.

[표 2]의 각 행위는 악성 봇넷 탐지를 위해 특정 행위를 분석한 것이다. 일반적인 사용자 기반의 통신에서 발생하지 않는 규칙적인 통신이나, DNS에 기반하지 않는 웹 질의, 동일한 크기의 파일을 여러 번 다운로드 하는 등의 행위를 위주로 분석하였다. 주소대역 같은 경우 악성 봇넷의 C&C 서버나 바이너리 다운로드 서버가 주로 외국에 있다는 것에 착안하여 주소 대역을 분석하였다.

[표 2] 악성 봇넷 별 행위 패턴 분석

행위 \ 봇넷	보박스	브리도랩	컨피커
C&C 연결 주기	300~400초	20분	30~60초
사용 포트	80, 443,	80	80, 445
DNS	DNS & Hard-Coded IP	DNS	Hard-Coded IP
다운로드 파일 크기 (byte)	1,223 8,704 7,680	1,089,115 666,431 581,044	-
주소 대역	국외	국외	국내 및 국외
공격 패킷 량	66pps	136pps	-
행위 \ 봇넷	게그	넷봇	웨일덱
C&C 연결 주기	150초 70~260초	설정가능 (고정)	200~400초
사용 포트	443,	80	21, 80
DNS	Hard-Coded IP	DNS or Hard-Coded IP	Hard-Coded IP
다운로드 파일 크기 (byte)	-	-	717,861
주소 대역	국외	임의	국내 및 국외
공격 패킷 량	-	임의조정 가능	56pps

IV. 탐지 척도 선정

4.1. 탐지 척도 선정

분석된 트래픽을 통해 선정한 척도는 총 12개로 다음과 같다.

- AddressA

AddressA는 세션이 시작할 때 근원지 아이피 주소를 이용한 척도이다. AddressA는 로컬 아이피 주소와 같은 네트워크에 해당하는 아이피 주소, 원격 주소로 집합을 정하여 데이터를 분류한다. 이는 주로 감염된 호스트를 분리하기 위해 사용된다.

• AddressB

AddressB는 세션이 시작할 때 목적지 아이피 주소를 이용한 척도이다. AddressB는 AddressA와 같은 방법으로 데이터를 분류한다. 근원지 아이피에서 특정 서버 혹은 호스트로의 연결 관계를 파악하기 위해 사용된다.

• PortB

PortB는 원격지 포트 정보를 이용한 척도이다. C&C 서버와 통신할 때 많이 사용되는 80(HTTP)번, 443(HTTPS)번, 8080번 포트를 한 클래스로 정의하였다. 악성 봇넷 중 많은 봇넷이 스팸 메일을 발송하는 행위를 하기 때문에 25(SMTP)번 포트를 하나의 새로운 집합으로 정의하였다. 이 외의 포트는 1024를 기준으로 1024보다 작은 예약된 포트를 사용하는 집합과 1024보다 큰 포트를 사용하는 집합으로 나눈다. PortB는 특정한 포트를 사용하는 봇넷을 판별하는 척도가 된다.

• Session

session은 세션의 연결 유무를 이용한 척도이다. session은 SYN 패킷 이 전송된 후 응답 여부를 가지고 판단한다. 하드코드된 아이피를 사용하는 봇넷의 경우 C&C 서버 혹은 좀비 시스템이 셧다운되어있을 때 SYN패킷만 발생하는 빈도가 감염되지 않은 호스트에 비해 많이 발생하기 때문에 세션의 연결유무를 하나의 척도로 사용한다.

• DNS

DNS는 DNS 질의 유무를 이용한 척도이다. 많은 봇넷들이 DNS 질의가 아닌 하드 코딩된 아이피 주소를 이용하여 통신을 시도한다. DNS는 봇넷들이 하드코딩된 아이피 주소를 사용하는지 판별할 수 있는 척도가 된다.

• Duration

duration은 세션이 유지되는 시간을 이용한 척도이다. duration은 C&C 서버와 통신하는 주기가 불규칙적이지만 통신을 하면 세션이 유지되는 시간이 일정한 봇넷들을 판별할 수 있는 척도가 된다.

• Connection Interval

Connection Interval은 한 세션이 시작한 후 다음 세션이 시작할 때까지의 시간을 이용한 척도이다. Connection Interval은 C&C 서버와 주기적으로 통신하는 봇넷을 판별할 수 있는 척도가 된다.

• byteA

byteA는 하나의 세션동안 근원지 호스트에서 원격지 호스트로 전송하는 데이터의 크기를 이용한 척도이다. byteA는 통신을 할 때 일정한 데이터 크기의 데이터를 사용하는 봇넷을 판별할 수 있는 척도가 된다.

• byteB

byteB는 하나의 세션동안 원격지 호스트에서 근원지 호스트로 전송되는 데이터의 크기를 이용한 척도이다. byteB도 byteA와 같은 척도로 사용된다.

• Count

Count는 세션이 유지되는 동안 근원지 호스트와 원격지 호스트사이에서 전송된 총 패킷 총 수를 이용한 척도이다. Count는 스팸 메일 발송 등 공격을 수행하거나 통신을 하는 경우 일정한 수의 패킷이 발생하는 봇넷을 판별할 수 있는 척도가 된다.

• Average

Average는 세션이 유지되는 동안 발생한 패킷들의 평균 데이터 크기를 이용한 척도이다. 봇 사이의 통신에서 주고받는 데이터의 양이 평균에서 크게 벗어나지 않아 척도로 선정하였다.

• Nation

Nation은 로컬 호스트가 접근을 시도하는 아이피 주소의 대역 정보를 이용한 척도이다. 많은 봇넷들이 국외에 있는 아이피 주소로 접근을 한다. Nation은 국외 아이피 주소를 이용하여 접속을 시도하는 봇넷들을 판별할 수 있는 척도가 된다.

선정된 12개의 척도는 〔표 3〕과 같은 분류 기준을 갖는다. 분류 기준을 토대로 악성 봇넷의 트래픽에서 정보를 추출한 후 데이터 셋을 생성한다. 생성된 데이터 셋은 다음과 같은 형태로 구성되어 있다.

0, 2, 0, 1, 1, 4.7489, 0.0057200000, 1864, 59310 ,75, 815, 1, bobax

데이터 셋이 위와 같이 구성된 이유는 이후 C4.5를

〔표 3〕 변수 집단화

변수 명	집단	값
Address	0	Host 같은 서브 마스크
	1	Host가 소속된 네트워크와 같은 Class
	2	0과 1에 속하지 않은 나머지
Port	0	TCP 80, 443, 8080
	1	TCP 25
	2	0, 1에 속하지 않은 TCP 1024 미만
	3	TCP 1024 이상
Session	0	미 연결
	1	연결
DNS	0	미 사용
	1	사용
Nation	0	국내
	1	국외
Duration	-	범위를 갖는 정수
Connection Interval	-	범위를 갖는 정수
ByteA	-	범위를 갖는 정수
ByteB	-	범위를 갖는 정수
Count	-	범위를 갖는 정수
Average	-	범위를 갖는 정수

통해 악성 봇넷 트래픽에 대한 의사결정트리를 구축하여 각 봇넷 별 탐지 규칙을 생성하기 위해서이다.

4.2. 탐지 규칙 생성

각 봇넷의 트래픽 분석 결과와 선정된 탐지 척도를 토대로 각 봇넷의 탐지 규칙을 생성한다. 이때 생성된 각 봇넷 별 데이터 셋과 전남대 학내에서 수집된 일반 트래픽 데이터 셋을 트래이닝 데이터로 생성하여 C4.5를 이용하여 의사결정트리를 생성하였다. 생성된 의사결정트리에서 각 봇넷의 탐지 규칙을 추출한다. 아래의 〔표 4〕는 보박스 봇넷의 탐지 규칙이다.

보박스 봇넷 탐지 결과를 보면 세션간격, 통신 내용의 크기 및 평균, 세션 연결 간격 등이 주로 사용되는 것을 볼 수 있다. 1번 규칙은 C&C에 접근하는 행위에 대한 규칙이고 2번 규칙은 탬플릿을 다운받는 행위에 대한 규칙이다. 아래의 〔표 5〕는 게그 봇넷의 트래픽을 탐지하기 위한 규칙이다. 게그 봇넷의 경우 알려지지 않은 포트를 사용함으로써 IP 주소와 포트를 이용하고 세션 및 DNS를 이용하지 않은 연결 정보를 이용하여 탐지 규칙을 생성하는 것을 확인할 수 있다.

〔표 4〕 보박스 탐지 규칙

순번	속성	값
1	DNS	미사용
	다음 세션 간격	41.3351 이하
	A->B 크기	2272~3850바이트
	패킷 평균 크기	589바이트
	국가	외국
2	세션 지속 시간	4.6197~10.1852
	다음 세션 간격	0.000594이상
	패킷 평균 크기	205바이트
	국가	외국

〔표 5〕 게그 봇넷 탐지 규칙

순번	속성	값
1	근원지 주소	2 (외부 아이피)
	목적지 포트	3 (1024 이상)
	세션 지속시간	9.0474 이하
	패킷 평균 크기	30~57
2	목적지 주소	2 (외부 아이피)
	목적지 포트	0 (SSL)
	DNS	미사용
	세션 지속시간	4.6197 이하
	a->b 크기	470 이상
	b->a 크기	608 이하
	패킷 개수	12 이상
	패킷 평균 크기	129 이하

각 봇넷의 탐지 규칙 생성 결과 각 봇넷이 사용하는 척도가 상이한 점이 존재하였다. 이는 각 봇넷을 탐지하기 위해 다양한 척도를 적용해야 함을 보여준다.

V. 탐지 실험

총 6개의 악성 봇넷에 대해 탐지 실험을 한 결과는 〔표 6〕과 같다. 각각 악성 봇넷에 해당하는 트래픽을 새로 수집하여 실험 데이터 집합을 구성하였다. 수집 환경은 초기 데이터 수집 환경과 동일하고, 일반 트래픽의 데이터와 혼합한 데이터를 가지고 탐지 규칙에 대한 실험을 수행하였다.

보박스 봇넷과 브리도랩 봇넷을 제외한 4종의 봇넷에서는 매우 높은 탐지율을 보였다. 여기에서 보박스 봇넷과 브리도랩 봇넷은 C&C와의 통신 이외에 스팸 메시지를 발송하는 트래픽이 포함되어 규칙간의 간섭

〔표 6〕 악성 봇넷 탐지 결과

봇넷	True Positive	False Positive	ROC Area
보박스	0.763	0.048	0.966
브리도랩	0.812	0.064	0.962
컨피커	0.974	0.022	0.992
게그	0.988	0.001	0.998
넷봇	1	0	1
웨일텍	0.994	0.002	0.998

이 발생한 것으로 분석되었다. 하지만 넷봇이나 웨일텍 봇넷처럼 TCP 80 포트에서 동작하는 봇넷의 탐지율이 매우 높은 것을 토대로 보박스나 브리도랩 봇넷에서 스팸 트래픽을 제외하면 높은 탐지율을 보일 것으로 기대한다.

탐지 실험의 결과 본 논문에서 악성 봇넷을 탐지하기 위해 선정한 12개의 척도는 유용함을 알 수 있었다. 하지만 스팸 메일 발송 등 공격 과정에서 유사한 트래픽을 발생할 경우 탐지 규칙간에 간섭이 발생하기 때문에 이를 보완할 수 있는 다른 수단이 필요하다.

VI. 결 론

최근 악성 봇넷은 매우 빠르게 진화하고 있고, 각종 악성 행위들이 대부분 봇넷을 통해 행해지고 있어 악성 봇넷에 대응할 수 있는 기술이 국가적인 요구사항이 되고 있고, 그에 따라 산학연의 각 기관에서 많은 연구가 진행되고 있다.

본 논문에서는 악성 봇넷의 규모와 C&C를 탐지할 수 있는 기술을 개발하기 위해 악성 봇넷의 현황과 동향을 분석하고 주요 악성 봇넷의 샘플을 수집하여 정적, 동적 분석을 통해 악성 봇넷의 특징을 추출하였다. 이를 위해 총 6가지의 주요 악성 봇 샘플을 분석하여 특징을 추출하고, 추출된 특징을 기반으로 악성 봇넷을 탐지하기 위한 척도를 선정하였다. 선정된 척도를 가지고 탐지 규칙을 생성하여 탐지 성능을 실험해 보았다. 그 결과 보박스 봇넷과 브리도랩 봇넷을 제외한 봇넷들은 97%이상의 탐지율을 보였다. 이러한 결과로 선정된 척도들이 탐지를 위해 중요한 역할을 할 수 있다고 말할 수 있다. 하지만 이러한 연구의 결과는 새로운 악성 봇넷에 대해 탐지가 힘들다는 단점을 갖는다. 이를 위해 향후 규칙에 기반한 탐지 척도가 악성 봇넷의 진화에 대응하기 위해 허니넷과 연동을 통해 탐지 규칙을 자동으로 업데이트할 수 있는 시스템을 구축하고자 한다.

참 고 문 헌

〔1〕 Wikipedia, "Botnet," http://en.wikipedia.org/ wiki/Botnet, 21 August 2009

〔2〕 Symantec Internet Security Threat Report, ,http://www.symantec.com/business/theme.jsp?themeid=threatreport, Volume XIII: April, 2008

〔3〕 Evan Cooke, Farnam Jahanian, and Danny McPherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets," Proc. of Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI '05), Jul. 2005.

〔4〕 Gunter Ollmann, "Botnet Communication Topologies," Damballa, Jun. 2009

〔5〕 Dae-il Jang, Minsoo Kim, Hyun-chul Jung, and Bong-Nam Noh, "Analysis of HTTP2P Botnet - Case Study Waledac," MICC2009, pp. 535-538, Dec. 2009.

〔6〕 H. Choi, H. Lee, H. Lee, and H. Kim, "Botnet detection by monitoring group activities in DNS traffic," in Proceedings of the 7th IEEE International Conference on Computer and Information Technology (CIT '07), pp. 715-720, October 2007.

〔7〕 Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong, and Wenke Lee, "BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation," 16th USENIX Security Symposium, pp.1-16, Aug. 2007.

〔8〕 M.A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," In Proceedings of the 6th ACMSIGCOMM Conference on Internet measurement, pp.41-52, 2006.

〔9〕 V. Yegneswaran, P. Barford, and V. Paxson, "Using honeynets for internet situational awareness," In Proceedings of the 4th Workshop on Hot Topics in

Networks(HotNets IV), Nov. 2005.

[10] F. Freiling, T. Holz, and G. Wicherski. "Botnet tracking: exploring a root-cause methodology to prevent Denial of Service attacks," In Proceedings of 10th European Symposium on Research in Computer Security (ESORICS'05), pp. 319-335, Sep. 2005.

[11] Guofei Gu, Junjie Zhang, and Wenke Lee., "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," College of Computing Georgia Institute of Technology, NDSS'08, Feb. 2008.

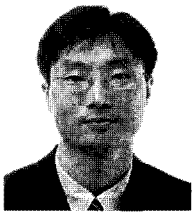
[12] Wei Lu, Mahbod Tavallaee, Goaletsa Rammidi and Ali A. Ghorbani "A.BotCop: An Online Botnet Traffic Classifier," 2009 Seventh Annual Communications Networks and Services Research Conference(CNSR'09), pp 70-77, May 2009

[13] 장대일, 김민수, 정현철, 노봉남, "HTTP기반의 브리도랩 봇넷 분석," 한국정보과학회 2009 가을 학술발표논문집 제36권 제2호(D), pp. 62-66, 2009년 11월

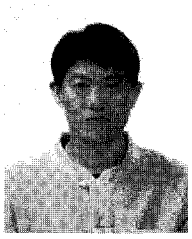
〈著者紹介〉

장 대 일 (Dae-il Jang) 학생회원
2008년 8월: 전남대학교 컴퓨터공학과 학사
2010년 8월: 전남대학교 정보보호협동과정 석사
2010년 9월 ~ 현재: 전남대학교 정보보호협동과정 박사과정
〈관심분야〉 봇넷 탐지, 시스템 보안, 해킹 등

김 민 수 (Minsoo Kim) 종신회원
1993년: 전남대학교 전산통계학과 졸업(학사)
1995년: 전남대학교 대학원 전산통계학과(이학석사)
2000년: 전남대학교 대학원 전산통계학과(이학박사)
2000년~2001년: 한국정보보호진흥원 선임연구원
2005년~현재: 목포대학교 정보보호학과 조교수
관심분야: 시스템 보안, 네트워크 보안, 정보보안, 신경망 등



정 현 철 (Hyun-chul Jung) 종신회원
1989년 3월 ~ 1996년 2월: 서울시립대학교 전산통계 학사
1997년 3월 ~ 1999년 8월: 광운대학교 전자계산 석사
1996년 7월 ~ 현재: 한국인터넷진흥원 팀장
관심분야: 네트워크 보안



노 봉 남 (Bong-Nam Noh) 종신회원
1978년 2월: 전남대학교 수학교육과 졸업(학사)
1982년 2월: KAIST 대학원 전산학과 졸업(석사)
1994년 2월: 전북대학교 대학원 전산과 졸업(박사)
1983년 ~ 현재: 전남대학교 전자컴퓨터공학부 교수
2000년 ~ 현재: 시스템보안연구센터 소장
관심분야: 정보보안, 시스템 및 네트워크 보안 등