DNS Response Policy Zone 을 이용한 DNS 싱크홀 운영 방안 연구

최재영*, 오상석**, 민성기**
*고려대학교 컴퓨터정보통신공학과
**고려대학교 컴퓨터정보통신공학과
e-mail : jayforest@gmail.com, ssoh94@korea.ac.kr, sgmin@korea.ac.kr

A Study on DNS sinkhole operation using DNS Response Policy Zone

Jae-Young Chio*, Sang-Seok Oh**, Sung-Gi Min**
* Dept of Computer and Communication Engineering, Korea University
** Dept of Computer and Communication Engineering, Korea University

요 약

최근 악성봇은 해커에 의해 원격 조정되어 명령에 의해 스팸메일 발송, DDoS 공격 등의 악성행위를 수행하는 웜/바이러스이다[2]. 악성봇은 이전의 웜/바이러스와 달리 금전적인 이득을 목적으로 하는 것이 많아 작게는 일상생활의 불편함으로부터 크게는 사회적, 국가적으로 악영향을 주고 있다. 국내에서는 이러한 위험을 방어하기 위한 효과적인 대응 방법으로 DNS 싱크홀을 운영 하고 있다. 본 논문에서는 DNS 싱크홀 운영 중 수집한 봇 명령/제어 (Command and Control, C&C) 도메인을 Internet Service Provider (ISP) DNS 싱크홀 시스템에 적용하는 과정에서 나타나는 문제점을 효과적으로 해결 하기 위한 DNS Response Policy Zone(RPZ)을 이용한 DNS 싱크홀 운영 방안을 제시 하였다.

1. 서론

악성봇은 해커에 의해 원격 조정되어 명령에 의해 스팸메일 발송, DDoS 공격 등의 악성행위를 수행하는 웜/바이러스 이다. 악성봇은 이전의 웜/바이러스와 달리 금전적인 이득을 목적으로 하는 경우가 많은 반면 감염사실을 피해자가 인지하기 쉽지 않아 피해가 심각한 실정이다. 이에 대한 대응 방안으로는 해커의 명령을 전달하는 명령/제어 서버의 차단이 필요하다[1]. 이러한 악성봇의 감염을 막고 악성행위를 차단하기 위하여 다양한 기법들이 활용되고 있다. 이 중 악성봇 DNS 싱크홀 기법이 국내에서 적용하고 있는 봇 대응 시스템으로 한국인터넷진흥원(KISA)과 국내 Internet Service Provider (ISP)가 협조하여 2005 년부터 운영 중에 있다[1].

DNS 싱크홀 운영 측면에서 두 가지 핵심적인 주요한 요소가 있다. 첫째, 봇 명령/제어(Command and Control, C&C) 도메인의 수집 둘째, DNS 싱크홀 시스템에 얼마나 신속하게 적용하느냐 하는 것이다. 현재 봇 C&C 도메인 자동 수집을 위한 방법이 활발히 연구되고 있는 반면, DNS 싱크홀 시스템 적용은 아직까지 큰 변화 없이 정적으로 이루어지고 있다. 이렇게 운영되고 있는 DNS 싱크홀 시스템 적용을 실시간 동적 업데이트로 발전 시키기 위해서 DNS Response Policy Zone(RPZ)을 이용한 DNS 싱크홀 운영 방안을 제안한다.

이 논문의 구성은 다음과 같다. 제 2 장에서는 현재 국내에서 운영 되고 있는 DNS 싱크홀 운영 방법과 DNS Response Policy Zone 을 분석한다. 제 3 장에서는 이 논문에서 제안하고자 하는 DNS RPZ 을 이용한 DNS 싱크홀 운영 방법을 기술한다. 제 4 장에서는 앞서 제안한 운영방법을 실험으로 통해 결과를 확인한다. 마지막으로 제 5 장에서는 결론을 내리고 DNS 기술에 대한 새로운 트랜드와 변화에 따른 향후 연구 방향에 대해 기술하였다.

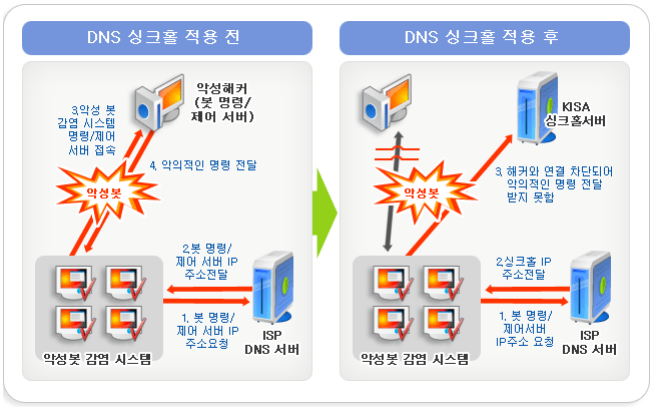
2. 관련연구

2.1 DNS 싱크홀

악성봇은 취약점을 가지고 있는 PC 에 자동으로 전파되며, 감염 시 해커가 지정해 놓은 명령/제어 서버에 접속하여 해커로부터의 명령을 기다린다. 이렇게 악성봇 감염 PC 가 접속하는 해커의 서버를 악성봇 C&C 서버라고 한다. 악성봇 C&C 서버는 이러한 악성행위의 중심에 있으며, 악성봇 C&C 서버의 차단만으로도 해커로부터의 명령 전달을 방지 할 수 있어 악성봇의 악성행위를 효과적으로 막을 수 있다[1, 2].

이러한 악성봇의 감염을 막고 악성행위를 차단하기 위하여 다양한 기법들이 활용되고 있다. 이 중 악성봇 DNS 싱크홀 기법이 국내에서 적용하고 있는 봇 대응 시스템으로 다음과 같이 동작한다. 악성봇 감염

PC 가 명령/제어 서버에 접속하기 위해서는 악성봇 서버의 도메인에 대한 IP 를 얻기 위하여 감염 PC 가 사용하는 DNS 서버에 질의를 하게 된다. 이때 DNS 서버에서는 해당 도메인을 관할하는 DNS 서버에게 IP 를 받아와서 감염 PC 에게 알려주고 감염 PC 는 응답 받은 IP 로 접속하는 과정을 거치게 된다.



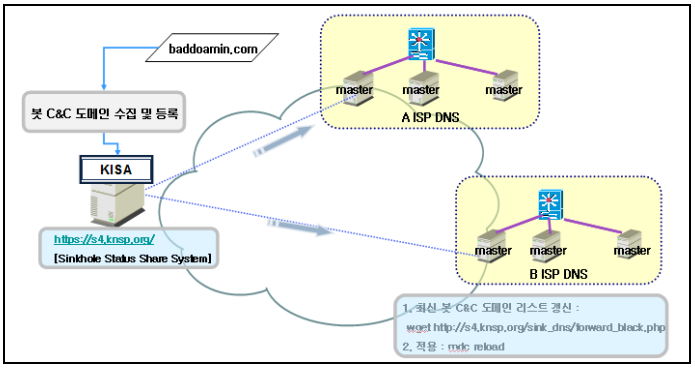
(그림 1) DNS 싱크홀 적용 개념도, 출처:KISA[3]

그러나 (그림 1)처럼 악성봇 DNS 싱크홀이 적용된 DNS 서버의 경우에는 사전에 악성봇 C&C 서버로 알려진 도메인은 감염 PC 로부터 DNS 질의를 받을 때 해당 도메인을 관할하는 DNS 서버에게 물어보지 않고 직접 특정 IP(싱크홀 서버 IP)를 응답하게 되고, 감염 PC 는 해커의 서버 대신에 싱크홀 서버로 접속하게 된다. 이렇게 되면 악성봇은 감염 후 해커의 C&C 서버에 접속하여 악성 행위 명령을 전달받는데, C&C 서버로의 접속이 차단되므로 더 이상 악성 행위를 할 수 없게 된다. 악성봇 DNS 싱크홀은 감염 PC 의 사용자가 보안에 대한 지식이 없더라도 감염 PC 가 사용하는 DNS 서버를 운영하는 ISP 에서 악성봇 DNS 싱크홀을 적용 중 이라면 악성봇에 의한 악성행위를 차단 할 수 있는 효과가 있다[2].

2.2 DNS 싱크홀 운영 방법 분석

DNS 싱크홀 운영의 필수적인 요소는 지속적인 봇 C&C 도메인 수집 함께 수집된 C&C 도메인을 DNS 싱크홀 시스템에 즉시 적용해야 한다. 봇 C&C 도메인 수집을 위해 KISA 에서 지속적으로 악성코드 수집시스템과 허니넷 (honeynet)의 DNS 로그 및 기타 방법으로 C&C 도메인을 수집하고 있다[4]. 수집된 봇 C&C 도메인은 KISA 웹사이트인 Sinkhole Status Share System (S4)에 등록 되어 ISP 에 제공 하고 있다[3]. 현재 약 2000 여개의 도메인이 등록 되어 있으며, 국내 ISP 에서는 S4 에 등록된 봇 C&C 도메인을 특정 주기마다 파일로 다운로드 받아 DNS 싱크홀 시스템에 적용 하는 방식으로 운영되고 있다.

봇 C&C 도메인을 DNS 싱크홀 시스템에 적용 하는 방법은 다음과 같다. 봇 C&C 도메인을 DNS config 파일에 로컬존으로 추가 후 DNS 에 새로운 config 를 읽어 들이도록 하고 있다. 수천 개의 봇 C&C 도메인을 운영중인 ISP DNS config 파일에 로컬 존 으로 추가하는 불편함이 있다. 따라서 KISA 에서 해당 봇 C&C 도메인 배포파일을 미리 DNS config 파일 형식으로 만들어 제공 하고 있으며, ISP 에서는 배포 파일이름을 DNS config 에 include 시켜 놓은 상태에서 일정 주기로 해당 파일을 다운로드 받아 업데이트 한 후 DNS 에 새로 읽어 들이게 하고 있다.



(그림 2)KISA DNS 봇 C&C 도메인 전파 방법

KISA 는 다양한 경로로 봇 C&C 도메인을 수집 하고 있으며 매일 약 1~2 의 새로운 봇 C&C 도메인을 탐지하고 이를 S4 시스템에 등록 하고 있다[4]. 따라서 봇 C&C 도메인 리스트는 빈번하게 업데이트 되고 있다.반면, ISP 에서는 특정 주기마다 봇 C&C 도메인 리스트 파일을 다운로드 하여 이를 DNS 싱크홀에 적용 함으로써 새로운 봇 C&C 도메인이 DNS 싱크홀에서 동작한다. 즉 KISA 에서 C&C 도메인을 탐지 하고 S4 에 실시간 등록 했다 하더라고 해당 도메인이 ISP DNS 싱크홀에 적용되기 까지는 일정 시간이 소요되는 문제점이 있어 악성봇의 악성행위 차단 공조 효과가 떨어진다.

2.3 DNS Response Policy Zone(RPZ)

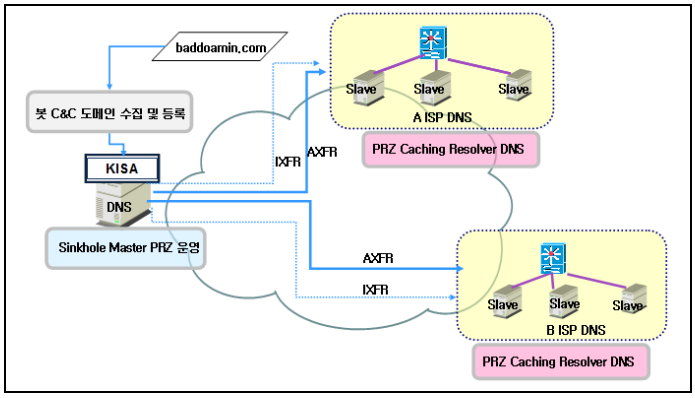
DNS RPZ 는 인터넷 범죄에 대항 하는 특수한 목적으로 Internet Systems Consortium(ISC)[5]에서 만들어 졌으며 ISC BIND9 에 구현되었다.

예를 들면, kisa-sinkhole 라고 불리는 RPZ 에서 www.attack.com.kisa-sinkhole 의 Resource Record Set (RRset)은 www.attack.com을 찾으려는 요청에도 응답한다. 즉 www.attack.kisa-sinkhole 과 www.attack.com 은 동일한 응답 값을 반환한다. 그러므로 하나의 RPZ 에 봇 C&C 도메인을 하위 도메인으로 등록하여도 봇 C&C 도메인에 대한 요청을 로컬 존에서 처리할 수 있다. 또한 DNS RPZ 는 일반적인 DNS 존 정책을 따른다. RPZ 는 서버간 존트랜스퍼가 되고 (DNS AXFR/IXFR) 거래서명(DNS TSIG)에 의해 보호될 수 있으며 실시간 변경 알림(NOTIFY)으로 신속히 처리 된다. DNS RPZ RRset 은 일반적인 규칙에 따라 와일드카드가 될 수 있다. 예) *.attack.com.kisa-sinkhole 은 attack.com 의 모든 서버도메인을 위한 응답에 영향을 준다. 이것은 도메인과 그 하위 도메인 모두에게 영향을 주기 위해서는 정책이 해당도메인과 그 와일드카드 하위도메인 모두에 적용된다는 것을 의미한다.

BIND9 에서 RPZ 적용은 DNS config 옵션인 "response-policy" 으로 동작 한다.

3. DNS RPZ 이용한 DNS 싱크홀 운영 방안 제안

기존 DNS 싱크홀 운영 방식은 KISA 에서 수집한 봇 C&C 도메인을 웹서버를 통해 ISP 에 제공한다고 앞서 설명하였다. ISP 에서는 KISA 에서 제공하는 사이트에서 특정 주기 마다 해당 파일을 다운로드 하고 이를 DNS 싱크홀에 적용하여야 한다. 본 논문에서 제안하는 방법은 KISA 에서 Master DNS RPZ 을 운영하고 ISP 에서는 Slave DNS RPZ 운영하여 KISA 에서 수집한 봇 C&C 도메인을 DNS 존트랜스퍼 방식으로 ISP DNS 에 봇 C&C 도메인을 동기화 한다.



(그림 3) DNS RPZ 를 이용한 DNS 싱크홀 운영 방안

즉 KISA 싱크홀 DNS 를 Master RPZ 로 운영하고 IPS DNS 싱크홀을 Slave RPZ 로 한번만 설정 하게 되면 이후 새로 수집된 봇 C&C 도메인은 S4 서버 대신 (그림 3)에서와 같이 싱크홀 Master RPZ 존파일에만 추가 하면 된다. 봇 C&C 도메인 동기화를 위해서는 Master RPZ 존파일의 시리얼값을 증가 시킨 후 존파일을 새로 읽게 되면 ISP DNS 에서는 Master DNS SOA 값의 변경 여부를 체크 하여 자동으로 존 트랜스퍼를 하게 된다. 즉 기존방식과 다르게 ISP 에서 봇 C&C 도메인 추가에 관여하지 않아도 자동으로 봇 C&C 도메인이 ISP 싱크홀 DNS 에 추가 된다.

Master DNS RPZ 에서 실시간 변경사항을 Slave DNS RPZ 에 전달 할 수 있어 KISA 에서 수집한 봇 C&C 도메인이 실시간 ISP DNS 싱크홀에 적용되어 악성봇에 의한 악성행위를 효과적으로 차단 할 수 있다.

4. 실험 및 결과

본 실험은 DNS RPZ 가 구현된 BIND 9.8.0[6]을 사용하였다. 첫째, DNS RPZ 에 현재 DNS 싱크홀에서 운영되고 있는 봇 C&C 도메인 약 2 천 여 개를 하위 도메인으로 추가 한 후 DNS RPZ 가 현재와 동일한 DNS 싱크홀로 정상 동작 하는지 확인 하였다. 둘째, DNS Master RPZ 에서 DNS Slave RPZ 로 정상적인 존 트랜스퍼가 이루어 지는지 확인 하였다.

4.1 DNS RPZ 존 생성 및 봇 C&C 도메인 추가

DNS config 의 named.conf 에 (표 1)과 같이 RPZ 를 위한 옵션을 추가 하여 싱크홀 용 DNS RPZ 을 만들었으며 싱크홀 존파일에 현재 운영중인 봇 C&C 도메인을 추가 하였다.

(표 1) DNS RPZ 설정 Config 및 Zone file

```
#-------------------------------
# DNS RPZ
#-------------------------------
options {
      response-policy {
            zone "kisa-sinkhole";
      };

};
zone "kisa-sinkhoke" {
          type master;
          file "kisa-sinkhole.zone";
};
```

```
#-------------------------------
# kisa-sinkhole.zone file
#-------------------------------
$TTL 21600
@     IN    SOA     ns1.kisa-sinkhole. root.kisa.org. (
                    2011031701
                    21600
                    1800
                    604800
                    21600 )
                    IN          NS          ns1
;; Static Address for NS Server
ns1                   IN          A           127.0.0.1

0a.yi.org          IN          A          211.233.91.10
0c.yi.org          IN          A          211.233.91.10
0x0.b0b.org        IN          A          211.233.91.10
apld.ma.cx         IN          A          211.233.91.10
aq.dyns.be         IN          A          211.233.91.10
                  ---------- 중략----------
```

4.2 DNS Master RPZ / Slave RPZ 구성

3 장에서 제시 한 것과 같이 싱크홀 Master RPZ DNS 는 KISA 에서 운영하고 ISP 에서는 싱크홀 Slave RPZ 로 운영 한다. (표 2)는 Master RPZ / Slave RPZ 동기화 실험을 위한 config 다.

(표 2) Master RPZ / Slave RPZ 구성 config

```
#-------------------------------
# Master RPZ
#-------------------------------
options {
      response-policy {
            zone "kisa-sinkhole";
      };

};

zone "kisa-sinkhoke" {
          type master;
```

```
        file "kisa-sinkhole.zone";
        also-notify {192.168.0.2;};
};
```

```
#------------------------------
# Slave RPZ
#------------------------------
options {
      response-policy {
            zone "kisa-sinkhole";
      };

};
zone "kisa-sinkhoke" {
        type slave;
        masters {192.168.0.1;};
        file "kisa-sinkhole.zone";
};
```

4.3 실험 결과

DNS RPZ 생성 (kisa-shinkhole zone)후 봇 C&C 도메인을 서버 도메인으로 추가 하여 실험한 결과 봇 C&C 도메인에 대한 응답 값이 현재 운영 중인 DNS 싱크홀과 일치 하였다. 그리고 DNS Master RPZ / Slave RPZ 로 구성 시 Slave DNS 에서 정상적인 존트랜스퍼가 이루지는 것을 확인 하였다. 특히 notify 옵션을 이용 할 경우 Master RPZ 의 변경 내용이 실시간으로 Slave RPZ 에 적용되는 것을 확인 할 수 있었다.

5. 결론

DNS 싱크홀 운영을 통하여 악성봇 감염시 C&C 서버로의 접속을 차단함으로써 악성봇에 의한 악성행위를 효과적으로 차단하고 있다. 매일 새로운 봇 C&C 도메인들이 출원하고 있고 KISA 에서 수집한 봇 C&C 도메인을 ISP DNS 싱크홀에 적용하는 일은 매우 중요 하다. 그러나 현재의 방식은 도메인에 대한 존을 강제로 추가하는 방식으로 봇 C&C 도메인이 새로 수집 될 때 마다 정적으로 ISP DNS 에 적용해주어야 하는 문제점을 가지고 있다.

본 논문에서는 KISA 에서 Master DNS RPZ 을 운영하고 ISP 에서는 Slave DNS RPZ 운영을 제시 하였다. KISA 에서 수집한 봇 C&C 도메인을 Master DNS RPZ 에만 업데이트 하면 모든 ISP DNS 싱크홀 시스템에 동적으로 실시간 적용되어 보다 효과적인 악성봇에 의한 악성행위를 차단을 할 수 있다.

향후 과제로 DNS 기술에 대한 새로운 트랜드와 변화에 대해 연구할 계획이다.

참고문헌

[1] 김영백, 이동련, 최중섭, 염흥열 “ DNS 싱크홀 적용을 통한 악성봇 피해방지 기법 및 효과”, 학술저널, 컴퓨팅의 실제 및 레터 제15권 제1호, 한국정보과학회, pp. 47~55, 2009

[2] 김영백, 염흥열” DNS 싱크홀에 기반한 새로운 악성봇 치료 기법”, 학술논문, 제 18 권 제 6(A)호, 한국정보보호학회, pp. 107~114, 2008

[3] https://s4.knsp.org/

[4] 정현철, “ Botnet C&C Handling with DNS Sinkhole” 한국인터넷진흥원

[5] Internet Systems Consortium (ISC), http://www.isc.org/

[6] http://www.isc.org/software/bind