DNS 싱크홀 적용 안내서

2011. 10.

KISA 한국인터넷진흥원
Korea Internet & Security Agency

인터넷침해대응센터

< 목 차 >

1. DNS란? 1
1.1 DNS 정의 1
1.2 DNS 사용 전・후 비교 1

2. DNS 싱크홀 소개 4
2.1 개요 4
2.2 적용 효과 4

3. 가입 방법 6
3.1 가입 대상 6
3.2 가입 절차 6

4. DNS 싱크홀 적용 방법 8
4.1 Windows 계열 8
1) 구성 파일 8
2) 적용 방법 8
3) 적용 확인 15
4.2 Unix 계열 16
1) 구성 파일 16
2) 적용 방법 16
3) 적용 확인 19
4) 자동 업데이트 19

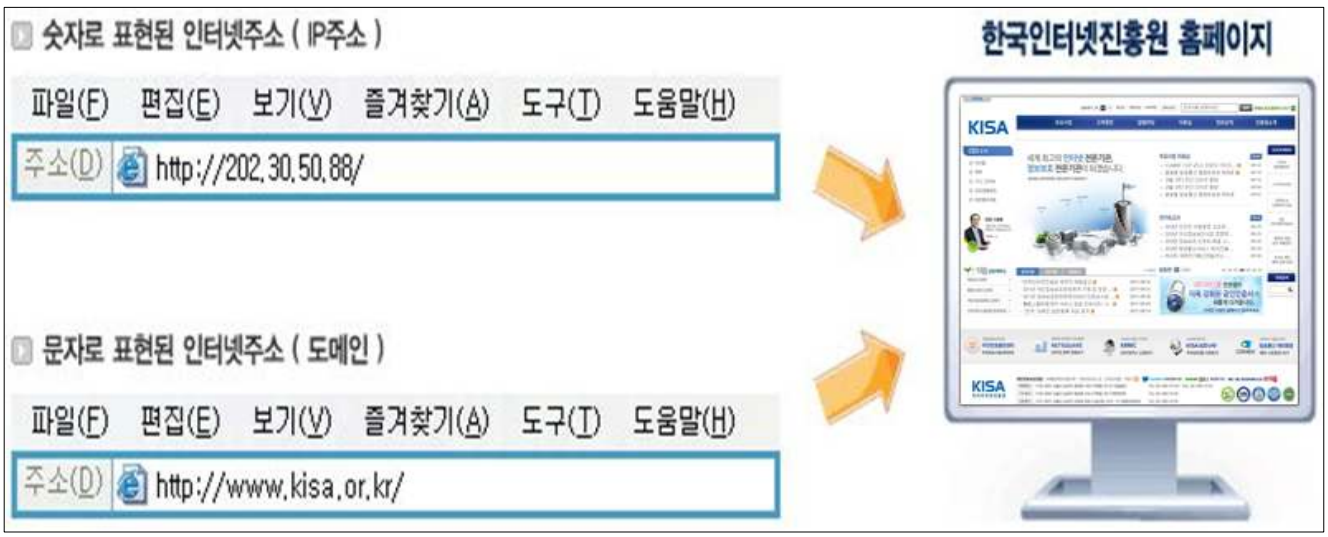
[부록] 용어 설명 20

1. DNS란?

1.1 DNS 정의

o DNS는 Domain Name System의 약어로 특정 호스트에 접속하기 위해 숫자로 된 IP주소를 일일이 기억하지 않고 도메인 네임(ex : kisa.or.kr) 만으로도 가능하게 하기 위해 도메인 네임을 IP로 전환시켜주는 시스템이다.

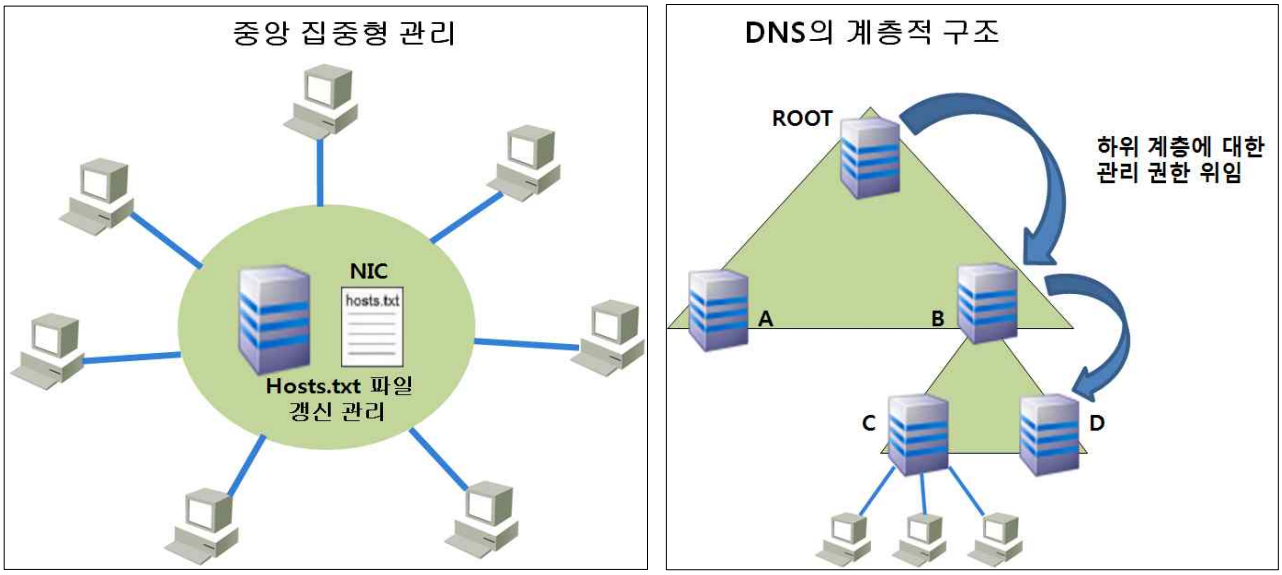
o 집배원이 집 주소를 알아야 우편물을 배달할 수 있는 것처럼 원하는 사이트에 접속하기 위해서는 접속 할 사이트의 IP주소를 알아야 한다. 숫자로 된 복잡한 IP주소를 외우지 않아도 DNS를 이용하면 도메인 네임 만으로 원하는 사이트에 접속할 수 있게 된다.



< DNS를 이용한 웹페이지 접속 >

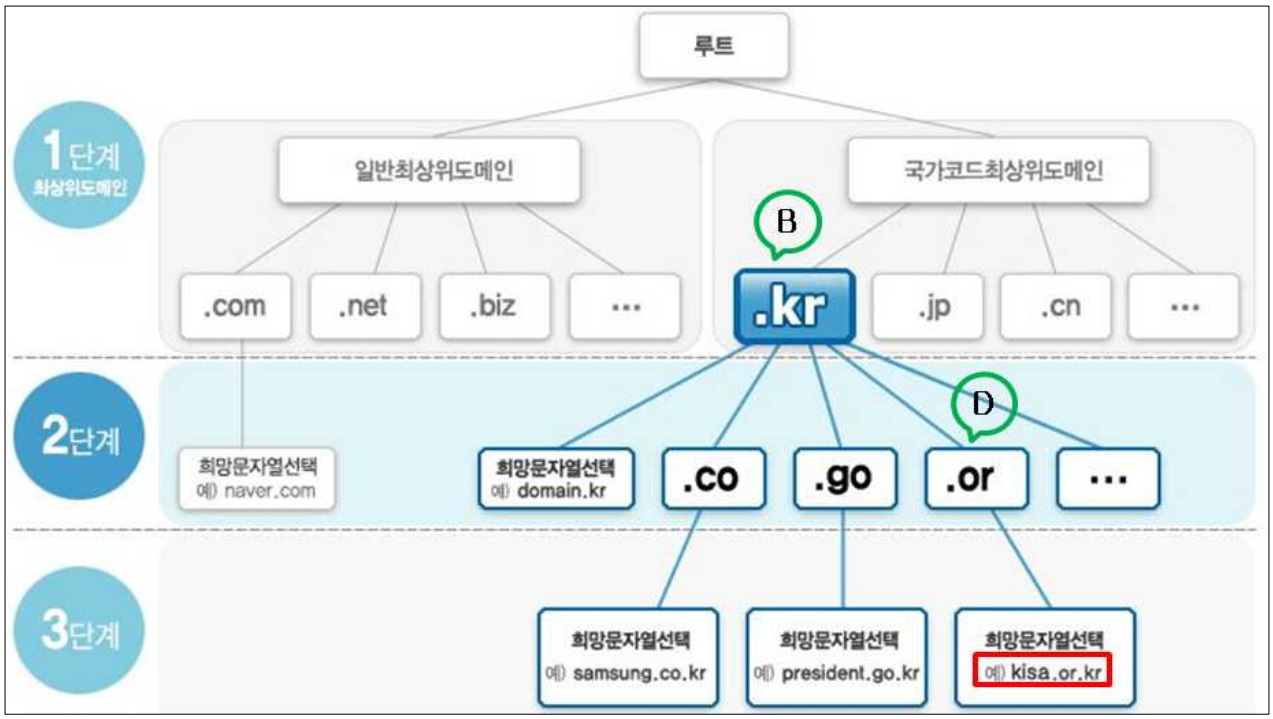
1.2 DNS 사용 전·후 비교

o 초창기 소수의 호스트들만 연결되었던 환경에선 각 호스트에 대해 숫자 형식의 네트워크 주소를 Hosts.txt 파일에 저장하여 직접 사용하였다. 그러나 점차 호스트의 수가 늘어나면서 보다 이해하기 쉽고 기억하기 쉬운 이름 체계 및 관리 방안의 필요성이 커지게 되었다. 이는 보다 광범위한 범주에서 사용될 수 있는 도메인 네임 체계로 발전하여 현재의 인터넷 네임 체계인 DNS가 등장하는 계기가 된다.



< DNS 사용 전 · 후 비교>

o DNS를 사용하지 않는 환경에서는 네트워크 주소를 직접 사용해야 원하는 호스트와 통신할 수 있었다. 즉, 특정 호스트가 어떤 IP 주소를 가지고 있는지, 어떤 서비스를 제공하는지를 사전에 알지 못하면 해당 호스트로 접근할 수 없었다. 그러나 수많은 호스트가 존재하는 인터넷 상에서 DNS를 사용하면 상황은 달라진다.



< DNS의 계층적인 네임 체계>

o DNS는 계층적인 네임 체계를 제공하므로 한국인터넷진흥원의 웹 사이트에 대한 접근을 원하는 경우, 전 세계적인 인터넷 기반 정보 서비스인 www(World Wide Web)와 한국인터넷진흥원의 영문 표기인 kisa (Korea Internet & Security Agency), 기관용 도메인인 or(Organization), 그리고 한국 국가 도메인인 kr(Korea)을 조합하여 www.kisa.or.kr을 도메인 네임으로 사용하여 접속을 시도함으로써 한국인터넷진흥원의 호스트로 접근이 가능하다.

www	kisa	or	kr
서비스명	기관명	기관 종류	국가명

< 도메인 네임의 의미 >

2. DNS 싱크홀 소개

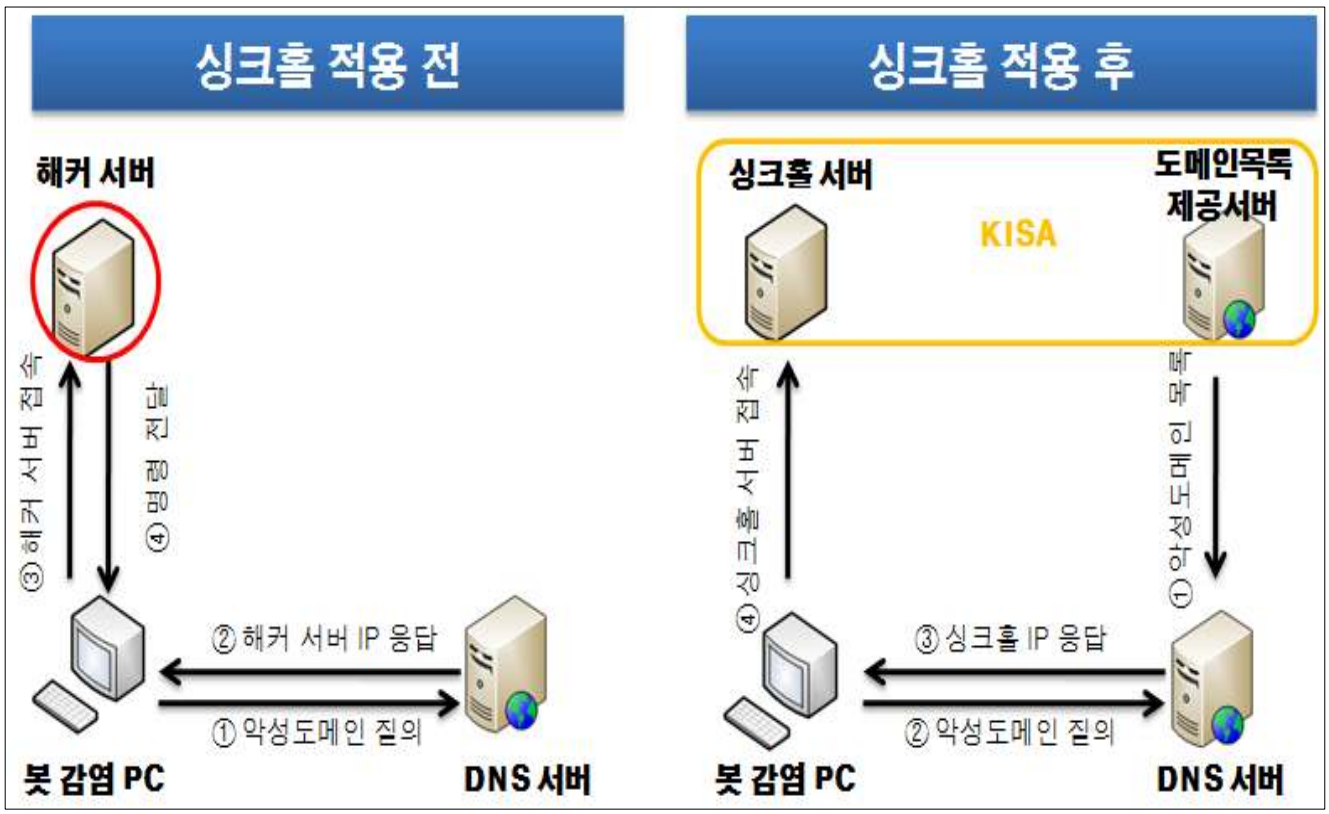
2.1 개요

o 해커들이 도메인을 악용하여 좀비PC들을 조종하기 위한 명령/제어 서버(이하 C&C)로 이용하고 있다.

o 한국인터넷진흥원(이하 KISA)에서는 이에 대한 대응 및 피해 확산 방지를 위한 기반환경을 조성하고자 DNS 싱크홀을 운영하고 있다.

o DNS 싱크홀이란 국내 주요 ISP와 협력을 통해 악성봇에 감염된 PC가 해커의 명령을 받기 위해 C&C로 연결을 시도할 때 C&C 대신 싱크홀 서버로 우회시켜 더 이상 해커로부터 조종 명령을 받지 않도록 해주는 시스템이다.

2.2 적용 효과



< DNS 싱크홀 적용 전·후 비교>

o DNS 싱크홀의 동작 과정은 다음과 같다.

※ 사전 단계로, KISA에서 배포한 C&C 목록을 ISP 등 DNS 싱크홀 적용기관의 DNS 서버에 업데이트하는 작업이 필요하다.

① 악성봇에 감염된 PC가 싱크홀이 적용된 DNS에 C&C에 대한 질의를 요청한다.

② DNS는 좀비 PC의 C&C 질의에 대해 싱크홀 IP 주소를 반환한다.

③ 이를 통해 악성봇에 감염된 PC는 C&C IP가 아닌 싱크홀 서버 IP로 우회 접속되어 해커의 명령/제어로부터의 피해를 방지할 수 있다.

3. 가입 방법

3.1. 가입 대상

o KISA는 민간분야 정보보호를 담당하는 기관으로, DNS 서버를 자체적으로 운영하고 있는 기관을 대상으로 DNS 싱크홀 서비스를 제공하고 있다.

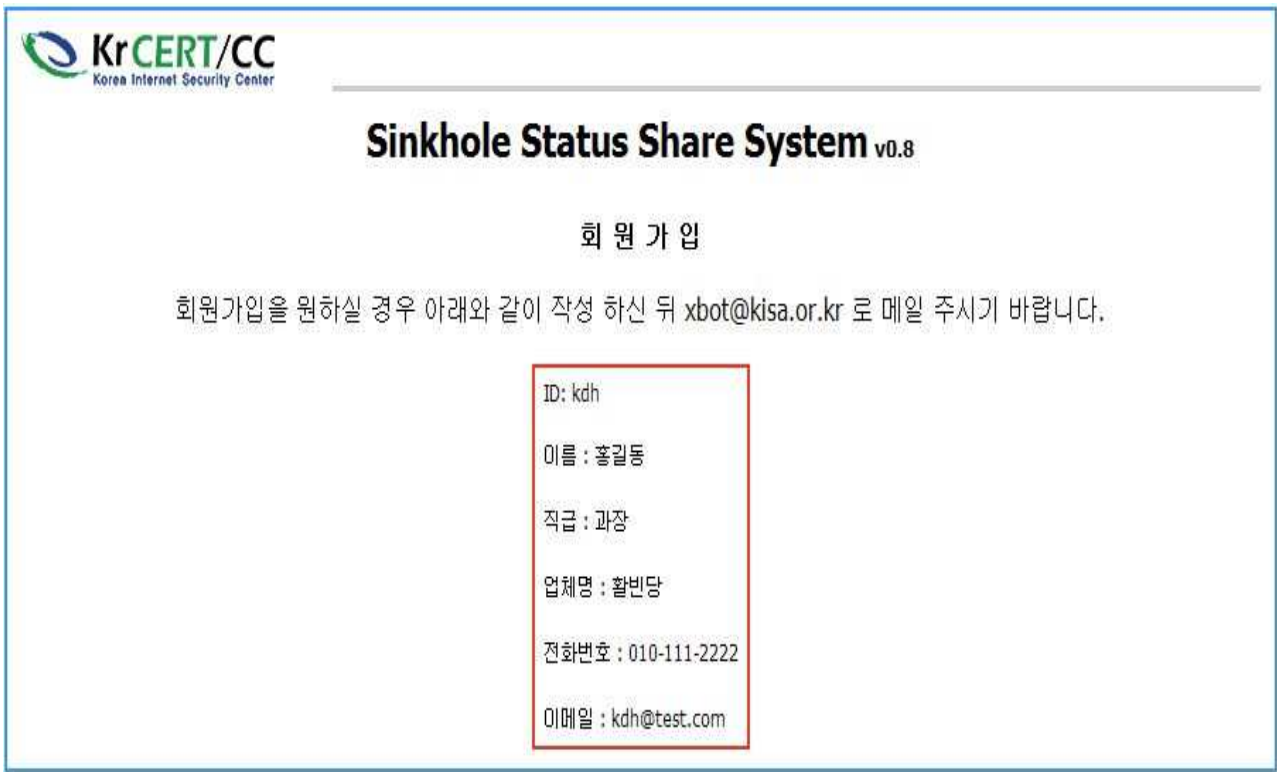
3.2. 가입 절차

o 싱크홀 적용기관과 KISA와의 체계적인 정보공유를 위해 Sinkhole Status Share System(이하 S4)을 개설하여 회원제로 운영 중이며, 가입 절차는 아래와 같다.

- 싱크홀 이용자 포탈사이트 : https://s4.knsp.org

o 회원가입 및 싱크홀 적용 절차

① S4 사이트 접속 후 [회원가입]을 클릭한다.



< S4 회원가입 페이지 >

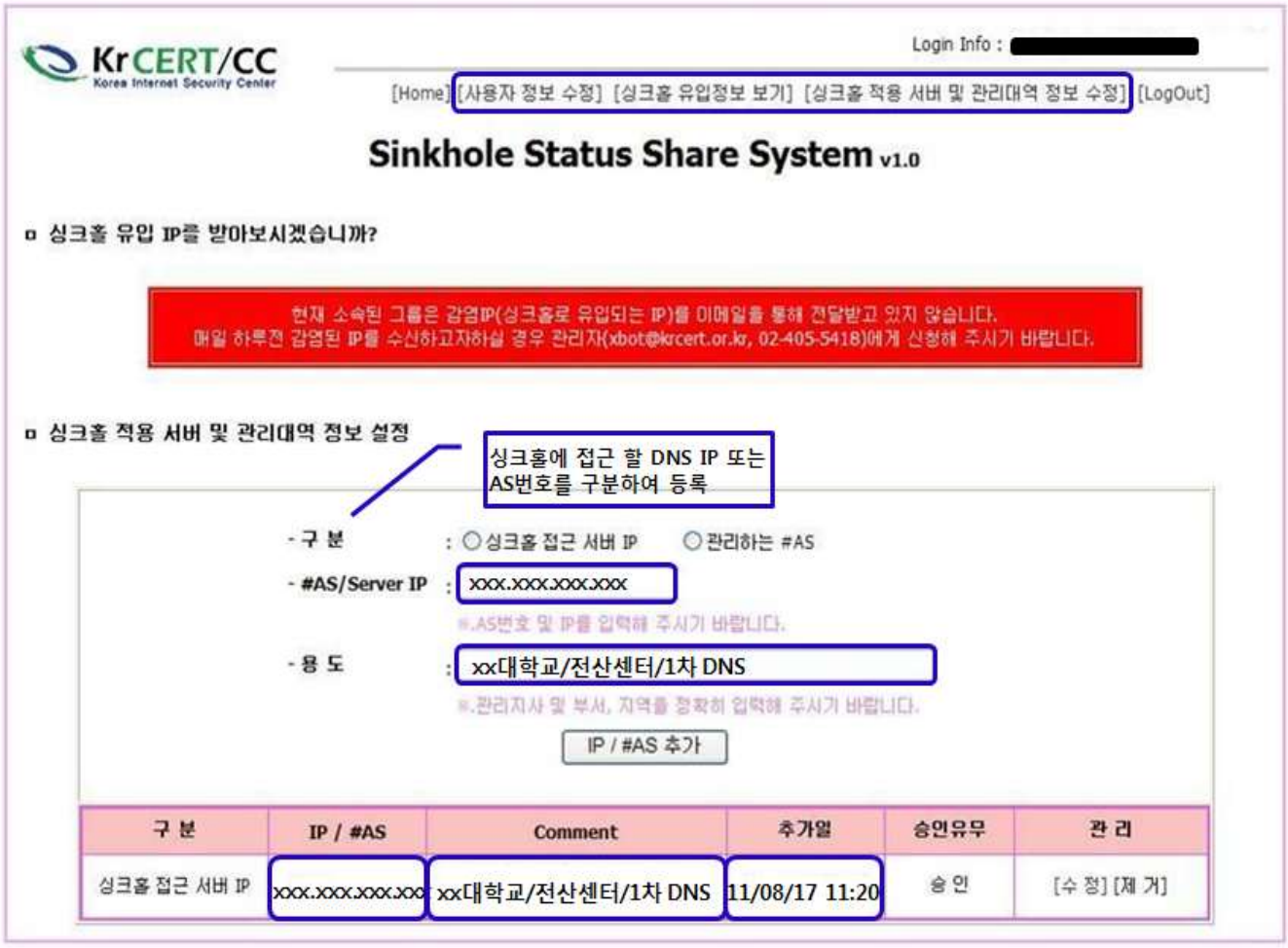
② 양식에 맞게 기입 후 xbot@kisa.or.kr로 메일을 보내면 관리자가 확인 절차를 거쳐 회원가입을 완료한다.

③ 패스워드는 관리자가 임의로 설정하여 메일을 통해 알려주며 로그인 후 메뉴 상단의 [사용자 정보 수정]에서 수정할 수 있다.

④ [싱크홀 적용서버 및 관리대역 정보 수정]에서 싱크홀 적용 할 DNS 서버 IP 및 AS번호를 등록한다.

- AS번호를 등록하면 하루 전 감염된 IP를 이메일로 수신 가능하다.

※ 사전에 관리자에게 연락하여 이메일 수신할 계정정보 제공 필요



< S4 싱크홀 적용 서버 및 관리대역 정보 수정 페이지 >

⑤ IP 등록 후 관리자가 등록 승인을 하면 '싱크홀 적용방법'을 참고하여 악성 도메인 목록을 다운로드 및 적용한다.

※ 문의 및 기술지원(Tel : 02-405-5478, Email : xbot@kisa.or.kr)

4. DNS 싱크홀 적용 방법

4.1 Windows 계열

싱크홀 시스템의 동작 원리는 좀비 PC가 C&C에 대한 질의 요청 시 해당 DNS 서버에서 C&C에 대한 IP주소 대신 싱크홀 서버 IP주소를 매핑 함으로써 C&C를 차단한다.

본 절은 Windows 서버 2000, 2003 환경에서 DNS 싱크홀 적용을 위한 설명이며, 설명의 용이성을 위해 아래 구성 파일과 같은 사항을 가정한다.

1) 구성 파일

o 싱크홀 적용을 위한 DNS 서버 설정 파일

- DNS가 설치된 디렉토리 : %SystemRoot%\system32\DNS

  ※ 설정 작업 시 탐색기를 열어 해당 디렉토리로 이동

- 싱크홀 적용 zone 파일 이름 : xx.com

  ※ C&C 질의에 대해 싱크홀 IP로 우회시키기 위한 설정 파일로 S4 사이트 Home에서 다운로드 가능

- 악성 도메인 설정 파일 : boot

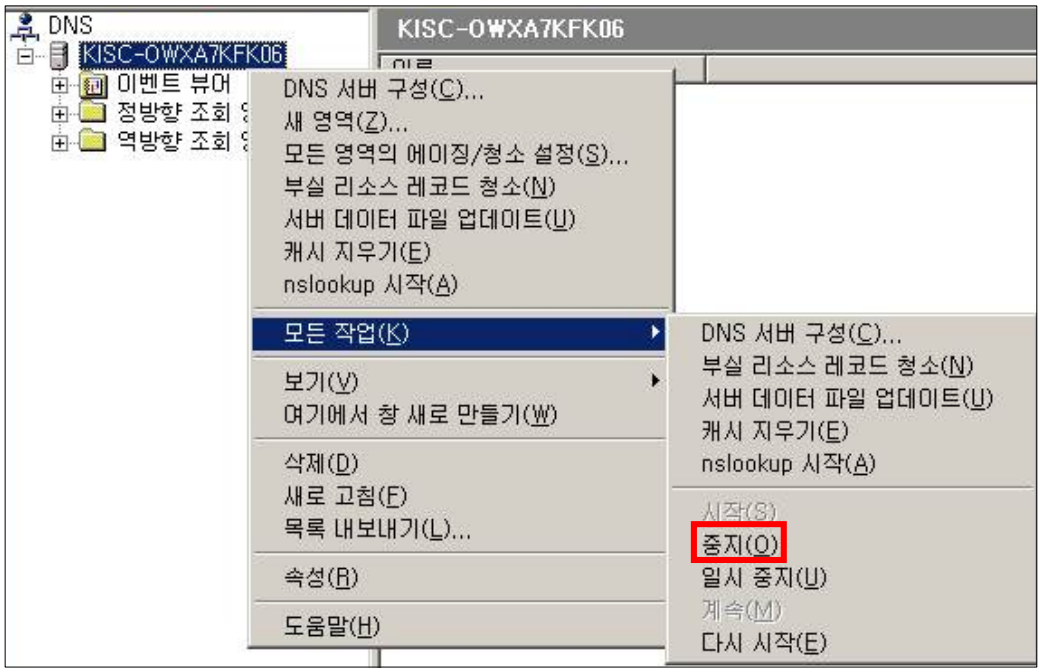
  ※ C&C 목록을 저장 할 파일로 경로는 %SystemRoot%\system32\DNS\boot

o 운영 시스템별로 DNS 설치 디렉토리를 반드시 확인 후 적용 할 것

2) 적용 방법

o Windows DNS 설정 백업

- "시작 → 관리도구 → DNS"로 이동하여 DNS 관리 도구를 열어 좌측에 DNS 서버를 선택한 뒤 "우측 버튼 → 모든 작업 → 중지"를 선택한다.

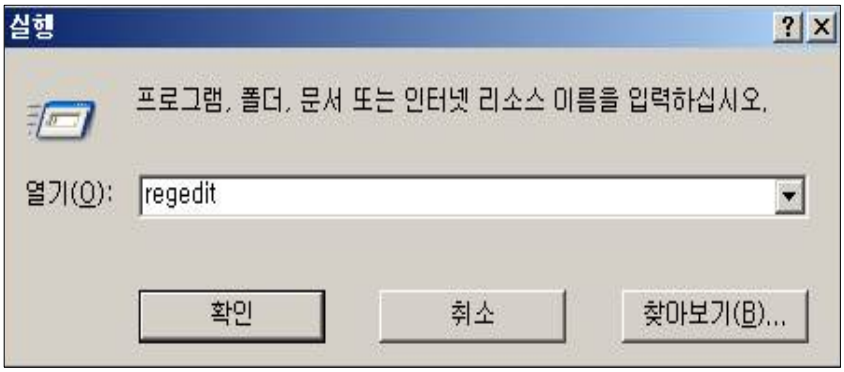


o DNS 텍스트 파일 백업

- 탐색기를 열어 "%SystemRoot%\system32\DNS"로 이동한 뒤 이 폴더 전체를 안전한 곳에 복사한다.

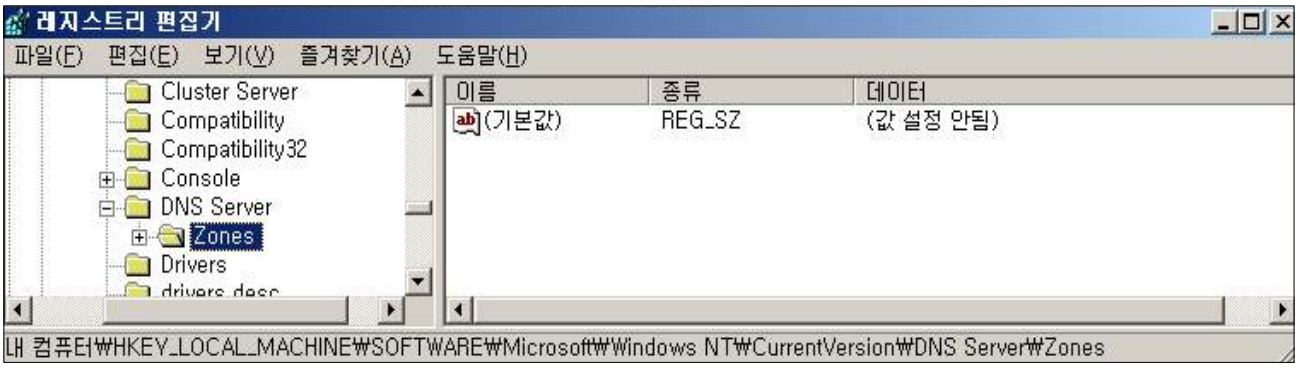
o DNS 레지스트리 백업

- "시작 → 실행"에서 regedit 입력 후 확인을 클릭하여 레지스트리 편집기를 연다.

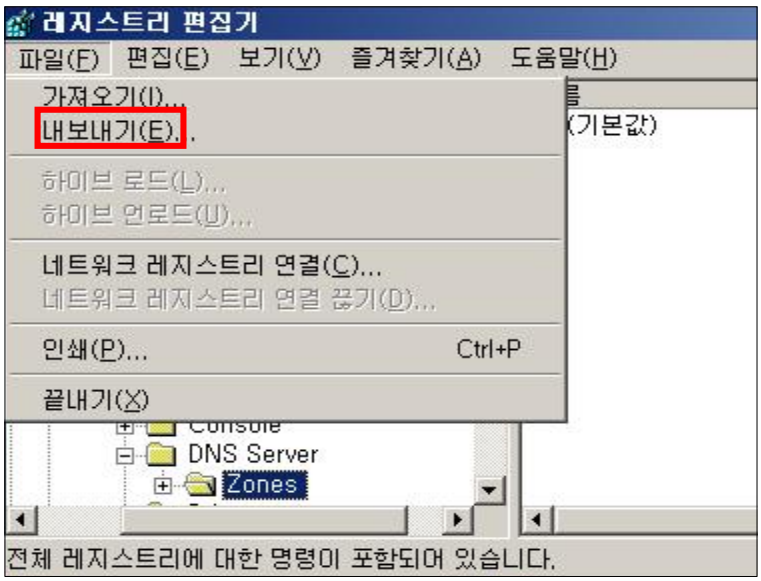


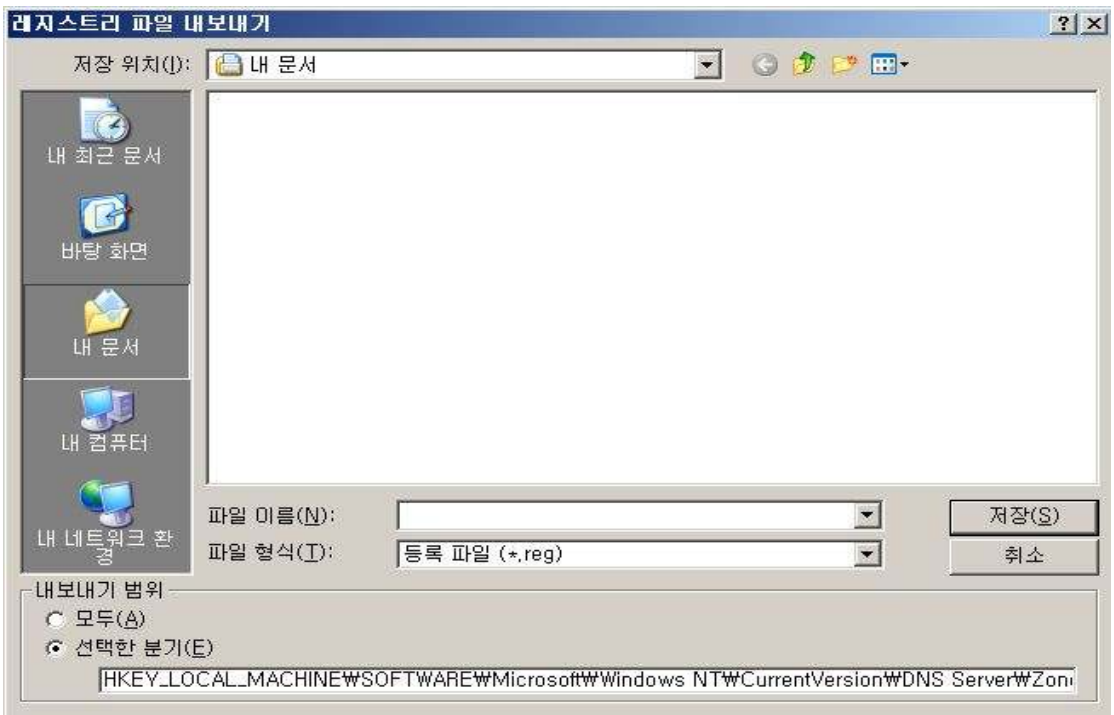
- 아래와 같은 레지스트리 키로 이동하여 Zones 항목을 선택한다.

Windows Server 2000	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Zone
Windows Server 2003	HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\DNS Server\Zones



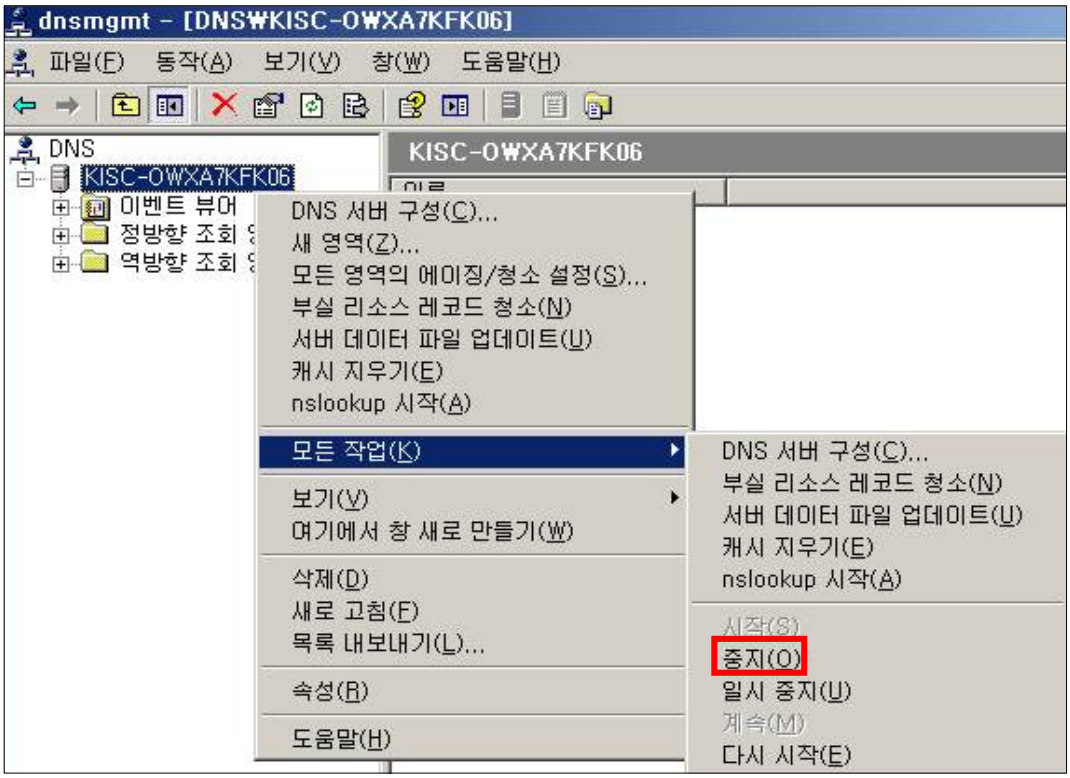
- 레지스트리 편집기 메뉴의 Registry를 선택하고 “Export Registry File” (내보내기)을 선택한다. 파일을 저장하는 위치를 물어보는 대화상자가 나타나면 안전한 곳에 레지스트리를 보관한다.





o Windows DNS 설정 복원

- 관리도구의 서비스 콘솔에서 DNS Server를 중지 시킨다.

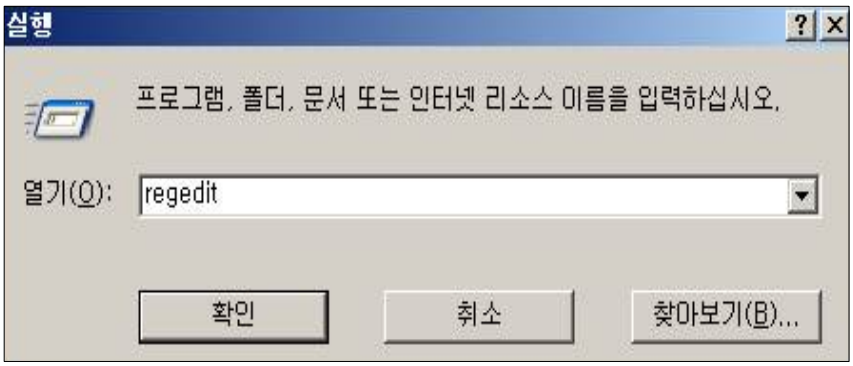


o DNS 파일 복원

- 백업해 두었던 DNS 텍스트 파일들을 탐색기를 열고 “%SystemRoot%\System32\DNS”로 이동하여 모두 복사한다.

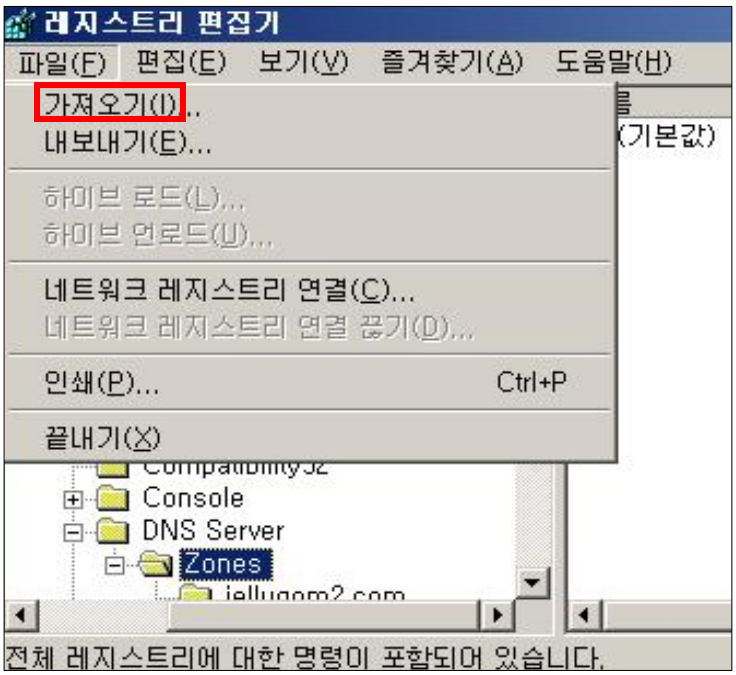
o DNS 레지스트리 복원

- 레지스트리 편집기를 연다.



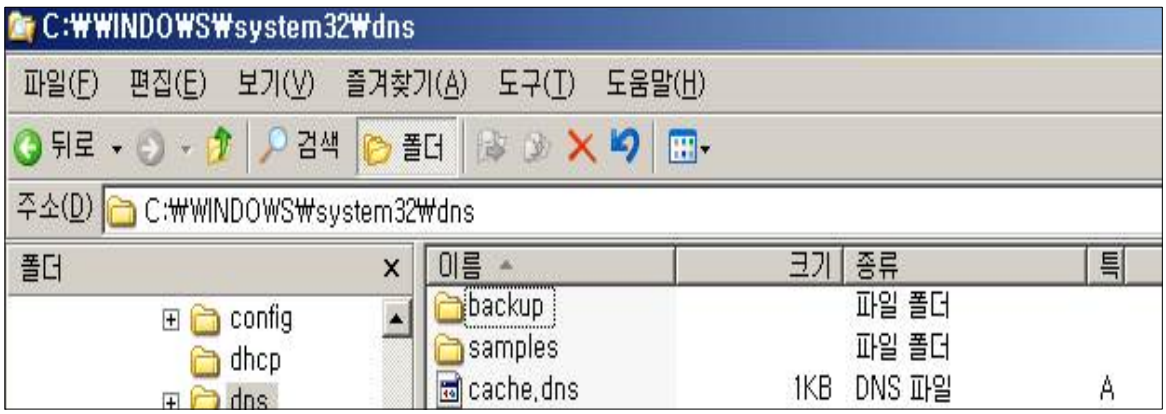
- 아래와 같은 레지스트리 키로 이동하여 Zones를 클릭하고 Regisrty 메뉴에서 “Import Registry File”(가져오기)을 선택하여 레지스트리를 복구한다.

Windows Server 2000	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Zone
Windows Server 2003	HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\DNS Server\Zones



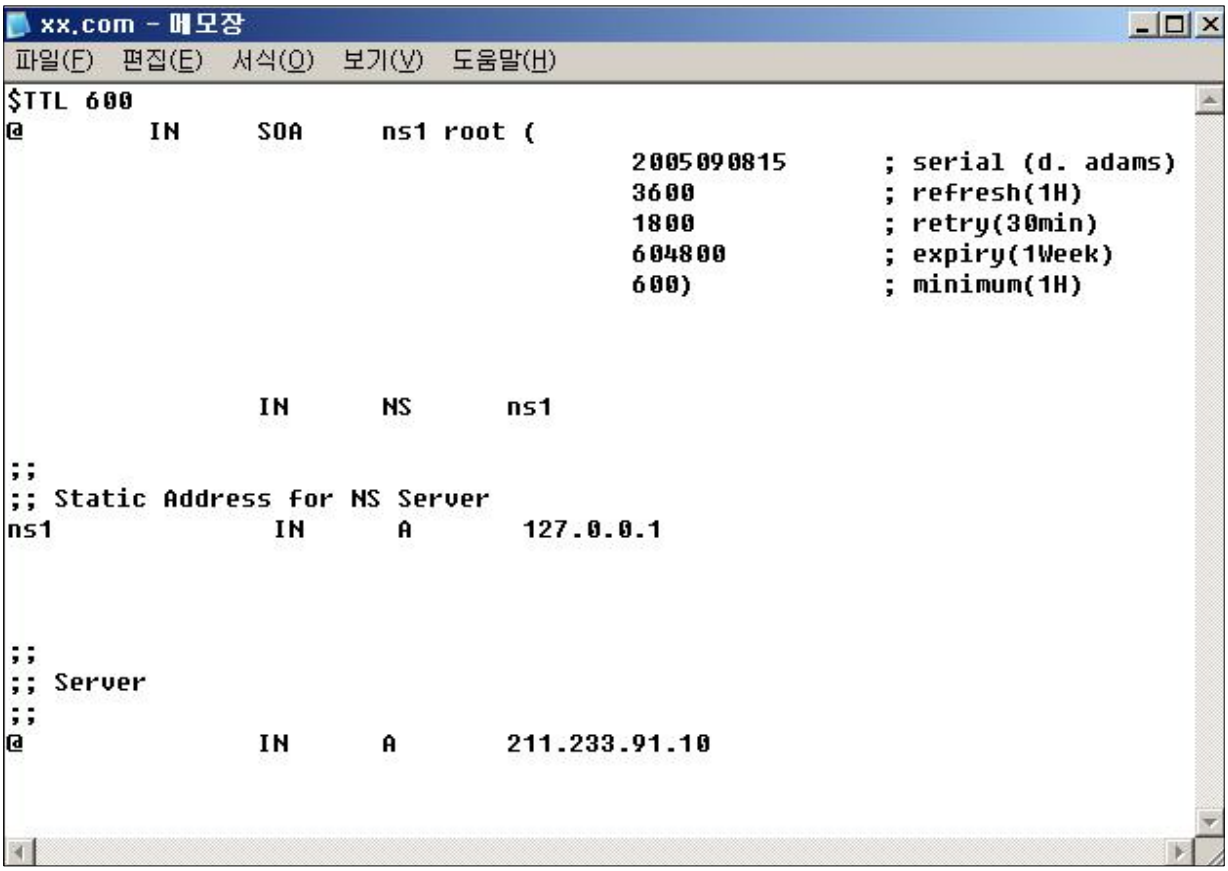
o DNS 서버 설치 디렉토리로 이동

- 설정 작업을 위하여 DNS 관련 파일이 저장된 폴더로 이동한다.



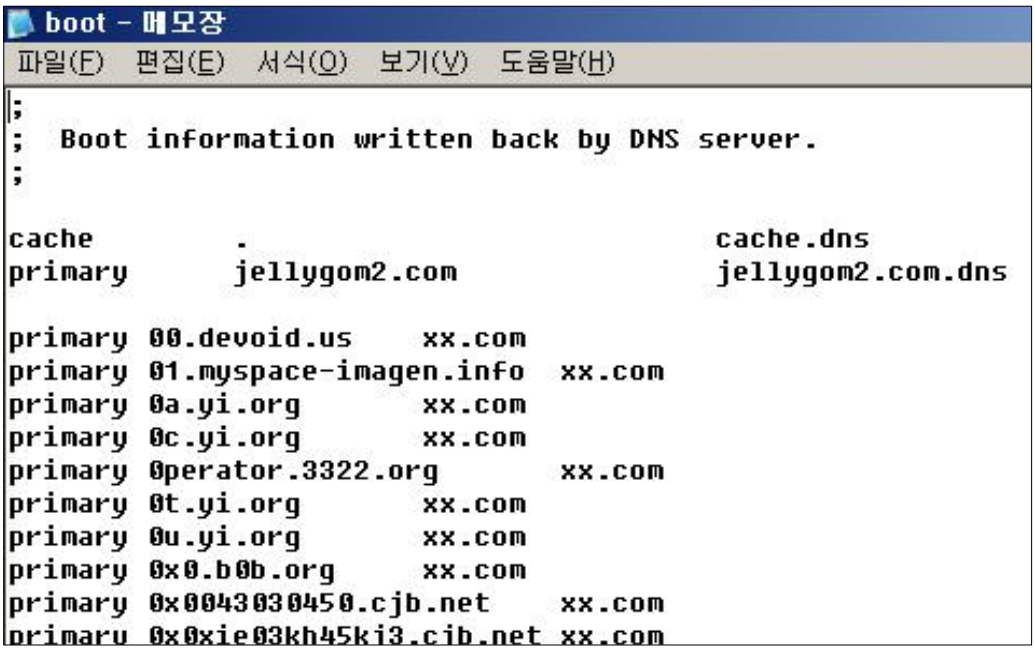
o 싱크홀 적용 zone 파일 생성

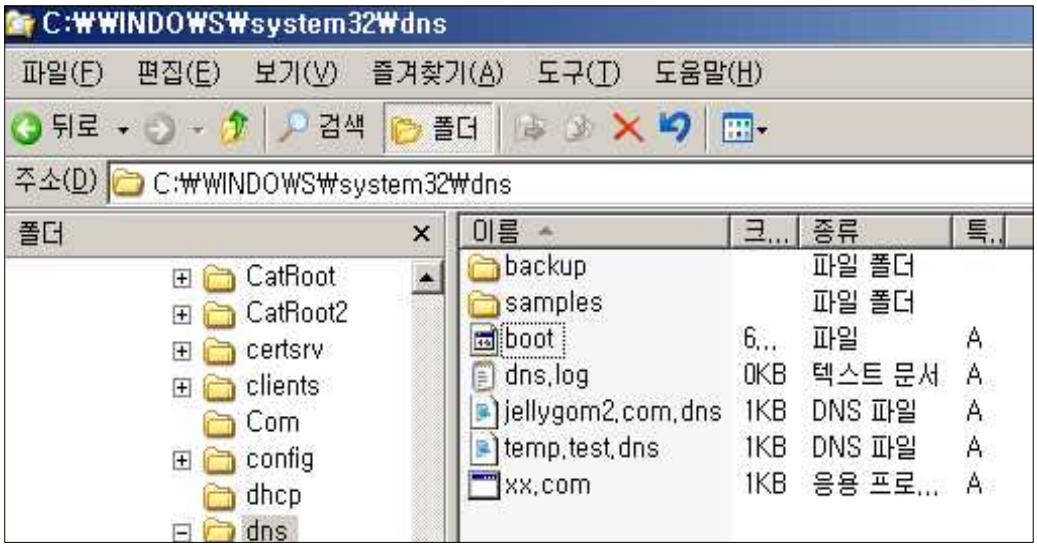
- KISA에서 제공하는 “xx.com” 파일을 해당 디렉토리(%SystemRoot%\System32\DNS)로 복사한다.



o DNS 서버 설정파일(boot) 변경

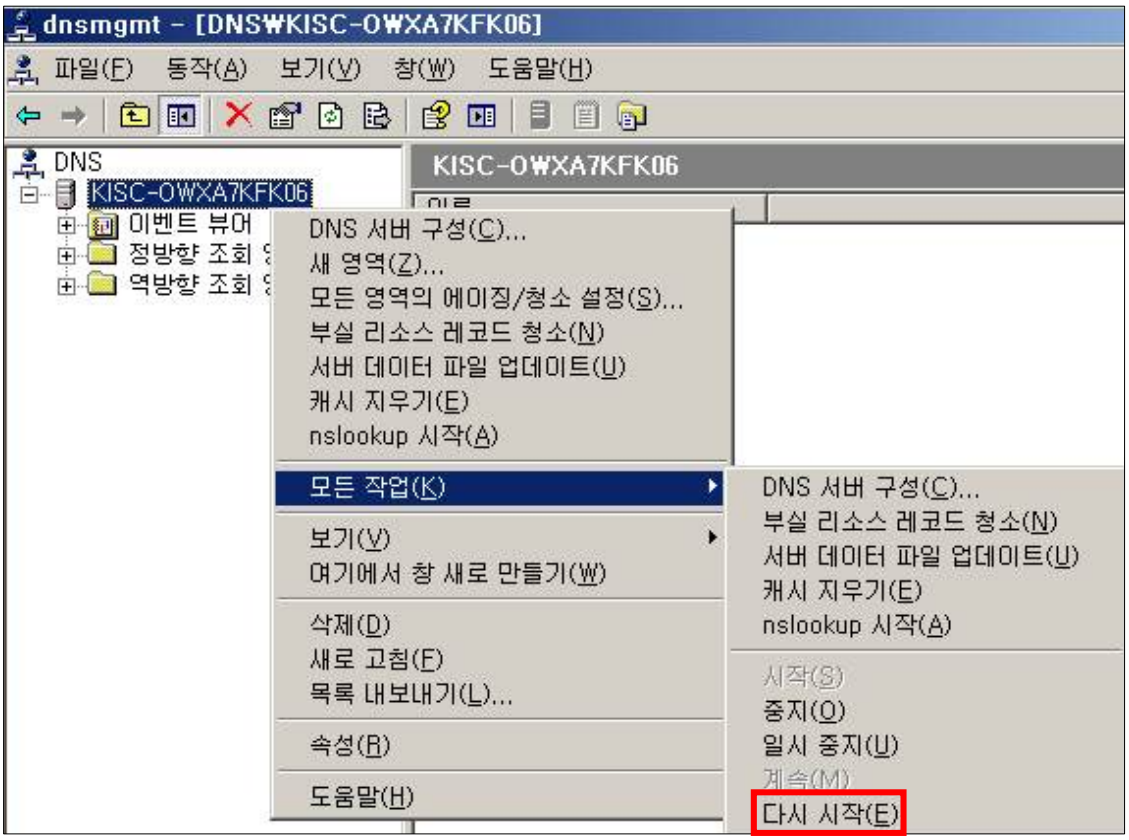
- KISA에서 제공하는 boot 파일의 내용을 기존의 "%SystemRoot%\System32\DNS\"에 존재하는 boot 파일에 추가한다.





o 서버 재시작

- DNS 서버를 선택한 뒤 “우측버튼 → 모든 작업 → 다시 시작”을 선택한다.



- 모든 적용이 완료되면 DNS 서버의 정방향 조회 영역에 싱크홀 적용이 완료된 도메인 목록이 나타남을 확인 할 수 있다.

3) 적용 확인

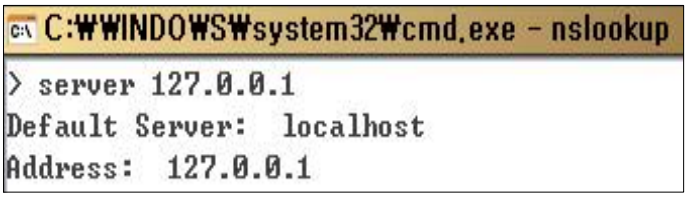
o boot 파일에 포함된 도메인 중 하나를 nslookup 명령어를 사용하여 응답이 싱크홀 서버 주소로 오는지 확인한다.

o nslookup 시작

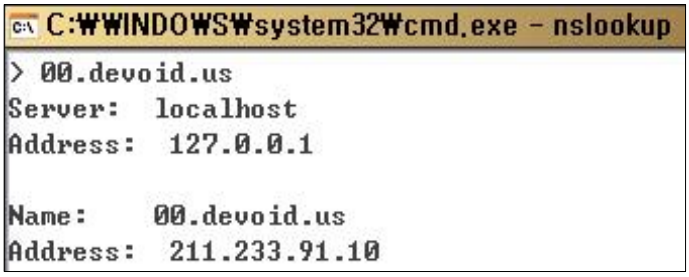
- 윈도우 커멘드 창에서 nslookup을 입력한다.

o DNS 서버 지정

- 싱크홀을 적용한 DNS 서버를 nslookup 질의를 보낼 서버로 설정한다. 아래 그림에서는 DNS 서버가 설치된 서버에서 테스트 중이므로 localhost 주소를 DNS 서버로 설정했다.



- boot 파일에 저장된 악성 도메인 주소를 입력하면 응답이 211.233.91.10 (싱크홀 서버 IP주소)로 오는 것을 확인 할 수 있다.



4.2 Unix 계열

싱크홀 시스템의 동작 원리는 좀비 PC가 C&C에 대한 질의 요청 시 해당 DNS 서버에서 C&C에 대한 IP주소 대신 싱크홀 서버 IP주소를 매핑 함으로써 C&C를 차단한다.

본 절은 유닉스 계열의 DNS 서버인 BIND(8.x, 9.x) 환경에서 DNS 싱크홀 적용을 위한 설명이며, 설명의 용이성을 위해 아래 구성 파일과 같은 사항을 가정한다.

1) 구성 파일

o 싱크홀 적용을 위한 DNS 서버 설정 파일

- DNS가 설치된 디렉토리 : /var/named
- 싱크홀 적용 zone 파일 이름 : xx.com

※ C&C 질의에 대해 싱크홀 IP로 우회시키기 위한 설정 파일로 싱크홀 이용자 포탈사이트 Home에서 다운로드 가능

- 악성 도메인 설정 파일 : forward_black.php

※ C&C 목록이 저장된 파일로 wget 명령으로 다운로드 가능

o 운영 시스템별로 DNS 설치 디렉토리를 반드시 확인 후 적용 할 것

2) 적용 방법

o DNS 서버 설치 디렉토리로 이동

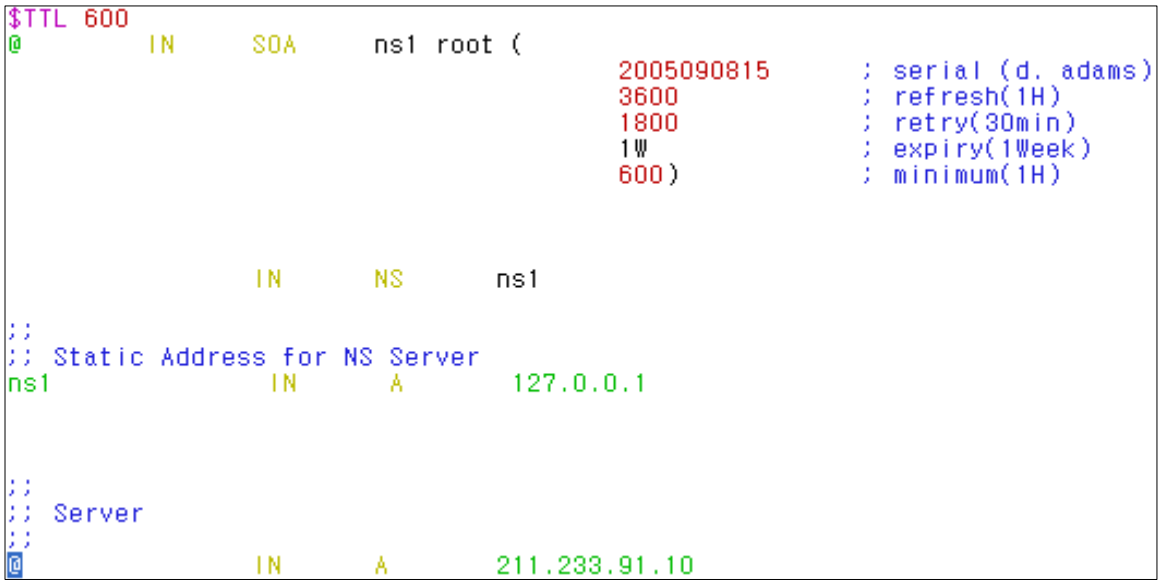
- Linux 계열에서는 보통 "/var/named" 아래 관련 파일이 저장되어 있다.

```
[root@localhost root]# cd /var/named
[root@localhost named]# pwd
/var/named
```

o 싱크홀 적용 zone 파일 생성

- 악성 도메인에 대한 접속을 싱크홀 서버로 연결시키기 위한 zone 파일 생성이 필요하며 이를 위해 "/var/named/forward/black" 위치에 "xx.com" 파일을 생성한다.

```
[root@localhost named]# cd /forward/black
[root@localhost black]# pwd
/var/named/forward/black
[root@localhost black]# vi xx.com
```



```
$TTL 600
@       IN      SOA     ns1 root (
                                        2005090815      ; serial (d. adams)
                                        3600            ; refresh(1H)
                                        1800            ; retry(30min)
                                        1W              ; expiry(1Week)
                                        600)            ; minimum(1H)


                IN      NS      ns1

;;
;; Static Address for NS Server
ns1             IN      A       127.0.0.1


;;
;; Server
;;
@               IN      A       211.233.91.10
```

o DNS 서버 설정파일에 악성 도메인이 등록된 파일 추가

- zone 파일 생성 후 악성 도메인을 “xx.com”으로 연결시키기 위한 설정이 필요하다.
- 이를 위해 악성 도메인 목록인 “forward_black.php”를 생성하고 DNS 설정 파일에 include 하도록 설정한다. DNS 서버 설정파일은 주로 “etc/” 아래 위치하고 있으며 이를 수정하여 “forward_black.php”를 추가하도록 설정한다.

```
[root@localhost etc]# pwd
/etc
[root@localhost etc]# vi named.conf
```

```
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
zone "jellygom.com" IN {
        type master;
        file "jellygom.zone";
        allow-update { none; };
};
zone "23.168.192.in-addr.arpa" IN {
        type master;
        file "jellygom.rev";
        allow-update { none; };
};

include "/etc/rndc.key";
include "/var/named/forward_black.php";
```

o 악성 도메인 목록 파일 다운로드

- KISA에서 제공하는 "forward_black.php" 파일을 해당 디렉토리(/var/named)로 복사하여 사용하며 아래와 같이 wget 명령어를 사용하면 간단하게 다운로드 가능하다.

```
[root@localhost named]# wget http://s4.knsp.org/sink_dns/forward_black.php
--2010-06-23 20:36:04--  http://s4.knsp.org/sink_dns/forward_black.php
Resolving s4.knsp.org... [redacted]
Connecting to s4.knsp.org[redacted]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `forward_black.php'

    [ <=>

2010-06-23 20:36:04 (2.04 MB/s) - `forward_black.php' saved [243995]

[root@localhost named]# ll
합계 260
drwxr-xr-x. 4 root root    4096 2010-06-23 20:30 forward
-rw-r--r--. 1 root root  243995 2010-06-23 20:36 forward_black.php
-rw-r--r--. 1 root root       2 2010-06-23 20:29 jellygom.zone
-rw-r--r--. 1 root root       2 2010-06-23 20:29 localhost.zone
-rw-r-----. 1 root named   1892 2008-02-18 21:29 named.ca
-rw-r-----. 1 root named    152 2007-06-21 19:09 named.localhost
[root@localhost named]#
```

o DNS 서버 설정 업데이트

- BIND 8.x : rdc reconfig
- BIND 9.x : rndc reconfig

```
[root@localhost named]# rndc reconfig
[root@localhost named]# tail /var/log/messages
Apr 18 06:43:08 localhost named[2522]: zone irc.lebobot.tk/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: zone richard-server.us.to/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: zone www.finelife.com.tw/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: zone irc.1-2-1tarot.co.uk/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: zone b.bakigjk.co.uk/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: zone bader.dirty-site.us/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: zone r0ma.dirty-site.us/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: zone tanak.dirty-site.us/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: zone next.hi5photos.us/IN: loaded serial 2005090815
Apr 18 06:43:08 localhost named[2522]: any newly configured zones are now loaded
[root@localhost named]#
```

3) 적용 확인

o “forward_black.php” 파일에 포함된 도메인 중 하나를 nslookup 명령어를 사용하여 싱크홀 서버 주소로 응답이 오는지 확인한다.

o nslookup 시작

- 쉘 커멘트 창에서 nslookup을 입력한다.

o DNS 서버 지정

- 싱크홀을 적용한 DNS 서버를 nslookup 질의를 보낼 서버로 한다.

※ 질의할 DNS 서버는 자신의 DNS 서버 IP를 사용한다.

```
> server 127.0.0.1
Default server: 127.0.0.1
Address: 127.0.0.1#53
```

o 응답 확인

- “forward_black.php” 파일에 저장된 악성 도메인 주소를 입력하면 응답이 211.233.91.10(싱크홀 서버 IP 주소)로 오는 것을 확인 할 수 있다.

※ 아래에서는 00.devoid.us를 이용하여 테스트 함

```
> 00.devoid.us
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   00.devoid.us
Address: 211.233.91.10
>
```

4) 자동업데이트

o 싱크홀 목록 자동 업데이트를 위한 cron 적용

- 아래와 같이 crontab 명령을 사용하여 자동 업데이트 설정을 적용한다.

```
crontab -e

0 0,12 * * * wget -P /etc/named http://s4.knsp.org/sink_dns/forward_black.php
0 12 30 * * rndc reconfig
# BIND 8.x : rdc reconfig
# BIND 9.x : rndc reconfig
```

[부록] 용어정리

o **(도메인)** 숫자로 이루어진 인터넷상의 컴퓨터 주소를 알기 쉬운 영문으로 표현한 것을 말하며 서비스, 조직, 조직의 종류, 국가의 이름순으로 구분되어 있다.

※ 예 : www.kisa.or.kr

o **(호스트)** 인터넷에 연결된 컴퓨터 시스템으로 다른 컴퓨터들과 통신이 가능한 컴퓨터를 말한다.

o **(IP주소)** Internet Protocol address는 컴퓨터 네트워크에서 장치들이 서로를 인식하고 통신하기 위해 사용하는 고유 식별번호이다.

o **(ISP)** Internet Service Provider는 개인이나 기업체에게 인터넷 접속 서비스, 웹사이트 구축 및 웹호스팅 서비스 등을 제공하는 회사를 말하며 국내의 경우 KT, SK브로드밴드, LG U+ 등이 있다.

o **(악성봇)** 로봇과 같이 스스로 움직이지 못하지만 명령자의 명령에 의해 원격에서 실행이 가능한 프로그램 또는 코드로 스팸 메일 발송이나 DDoS 공격에 악용된다.

o **(C&C 서버)** Command and Control 서버는 악성코드에 감염된 PC에 스팸메일 발송, DDoS 공격을 수행하도록 명령을 내리는 서버로 주로 해커가 운영한다.

o **(DDoS 공격, Distributed Denial of Service 공격)** 해커가 감염시킨 대량의 좀비 PC를 이용해 특정 시스템으로 과다한 트래픽을 무차별적으로 보내 서비스를 마비시키는 공격이다.

o **(좀비 PC)** 악성코드에 감염된 후 해커의 원격 조종에 의해 스팸 메일을 발송하거나 DDoS 공격에 이용되는 PC이다.