

악성프로그램 유포로 이용된 국내 시스템 사고 분석

2005. 4. 1

인터넷침해사고대응지원센터 (KISC)

※ 본 보고서의 전부나 일부를 인용시 반드시 [자료: 한국정보보호진흥원(KISA)]를 명시하여 주시기 바랍니다.

목 차

1. 개 요	1
2. 피해 시스템 분석	2
3. 결 론	9

1. 개 요

- 한국정보보호진흥원은 국내에서 웹 호스팅으로 사용 중인 시스템이 최근 문제가 되고 있는 악성 프로그램 유포 사이트로 사용되고 있다는 연락을 국외 바이러스 업체로부터 연락을 받아 해당 시스템에 대하여 분석을 수행하였다.
- 해당 시스템은 약 200여개의 웹호스팅을 하는 시스템으로서 여러 가지 잠재적인 취약점을 가지고 있었으며, 이미 몇 차례 해킹을 당한 흔적을 발견하였다. 최근 급증하는 국내 웹호스팅 시스템에 대한 웹 변조와 아울러서 국내의 취약한 시스템을 이용하여 제2의 해킹 경유지, 불법 프로그램 유포, Botnet 사용, 서비스 거부 공격 등을 위하여 사용되고 있다.

□ 피해 시스템 서버 정보

- 용도 : 웹 호스팅 시스템
- 호스팅 숫자 : 200 여개
- 위치 : 국내 모 IDC 위치
- 운영체제 : Linux (RedHat 9.0)
- Kernel 버전 : 2.4.20

□ 악성 프로그램 개요

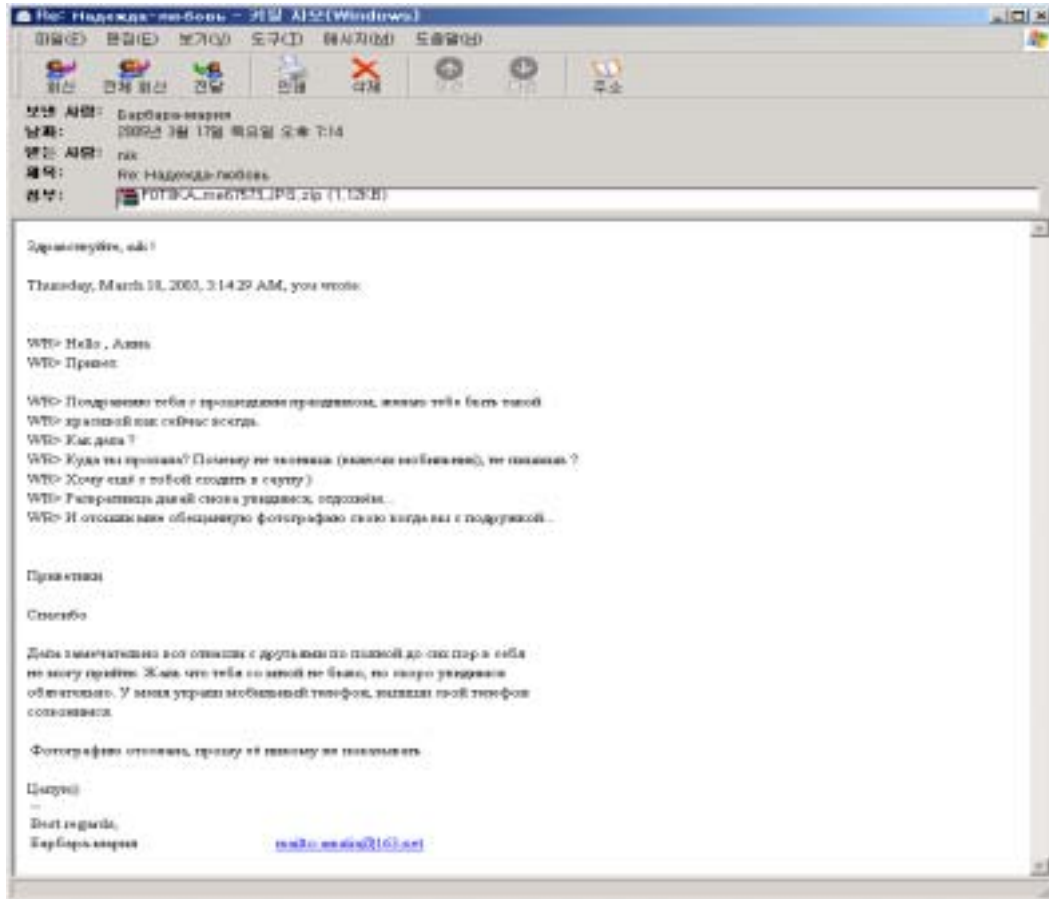
- 바이러스명 : Trojan-Downloader.Win32.Small.aon 등 다수
- 위의 파일은 다른 5개 이상의 Trojan, BackDoor 등을 해당 사이트로부터 다운로드 함
- 참고 사이트 : <http://www.encyclopedia-virus.com/virus/vervirus.php?id=1789>
- 유포자는 E-Mail 첨부 파일을 통하여 일반사용자들에게 전송후, 일반 사용자는 첨부파일 OPEN시 바로 국내 사이트로부터 순차적으로 특정 악성 프로그램을 다운로드 받게 됨

□ 악성 프로그램 유포 방법

- 유포자는 국내 시스템 해킹후 관련 악성 프로그램을 피해 시스템에 upload 후에 악성 프로그램들을 다운로드 하도록 하는 유도 E-Mail을 무작위로 배포
- 유포자는 수차례 관련 악성 프로그램을 피해 시스템을 통하여 배포 하였으며, 악성 프로그램 배포 현황을 파악하기 위하여 상대 파악 프로그램을 통하여 모니터링

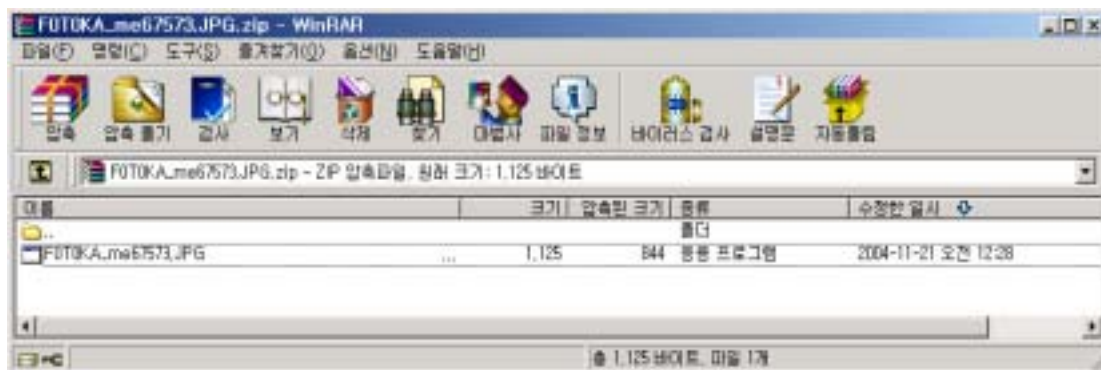
2. 피해 시스템 분석

□ 악성 프로그램 유포 E-Mail 원본 및 내용



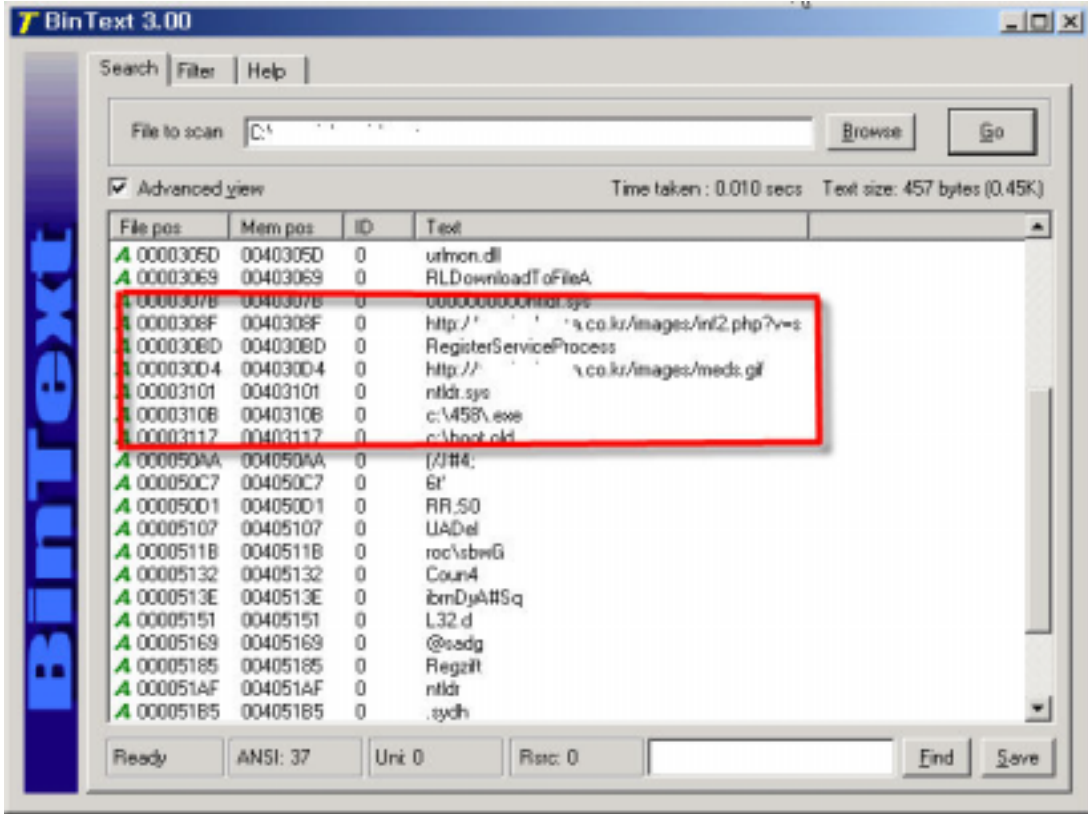
※ 유포자는 러시아 언어로 된 E-Mail을 유포

- 유포자는 악성 프로그램 Downloader 프로그램을 첨부하여 메일 수신자로 하여금 추가적인 악성 프로그램을 피해 시스템으로부터 다운로드 하도록 하였다.



※ 첨부파일 압축 해제 후 화면

- 첨부 파일을 Click에 자동으로 피해 사이트로부터 추가적인 악성 프로그램 다운로드 실행



※ 국내의 웹사이트로부터 악성 프로그램을 다운로드 받도록 설계

□ 피해 시스템 해킹 원인 분석

- 피해 시스템은 최근 국내 웹페이지 변조에 많이 사용되는 Zeroboard 사용하고 있었으며, 몇몇 사용자는 취약성 버전을 사용하고 있었다.
- 또한 피해 시스템에서 운영중인 공개용 데이터베이스 프로그램인 MySQL 프로그램 또한 취약한 버전을 운영하고 있었으며, 관리자 비밀번호 또한 추측하기 쉬운 것을 사용하여 해킹 공격에 매우 취약하였다.
- 마지막으로 피해시스템은 웹 호스팅 사용자들이 원격에서 접속을 하도록 서비스를 허용을 하였는데, 많은 고객들이 숫자로 구성된 비밀번호를 사용하거나, 사용자 ID 와 같은 비밀번호를 사용하여 Brute Force 공격에 취약하였다.

※ 최근 이러한 SSH Brute Force 공격은 일반화되었으며, 흔히 발견된다. 이런 공격으로 국내에도 많은 시스템이 피해를 입은 것으로 파악된다.

```

SecureCRT
File Edit View Options Transfer Script Tools Window Help
sh-2.05b# find /home -name zboard.php -ls
20498540 12 -rw-r--r-- 1 ventura ventura 9493 Jun  8 2002 /home/ventura/public_html/bbs/zboard.php
17875140 12 -rw-r--r-- 1 lynx25 lynx25 9493 May 22 2003 /home/lynx25/public_html/bbs/zboard.php
12173568 12 -rw-r--r-- 1 teaa teaa 9493 Jun  8 2002 /home/teaa/public_html/bbs/zboard.php
20136768 12 -rw-r--r-- 1 deus2925 deus2925 9493 Jun  8 2002 /home/deus2925/public_html/bbs/zboard.php
27525292 12 -rw-r--r-- 1 zboard zboard 9493 Jun  8 2002 /home/zboard/public_html/bbs/zboard.php
23576668 12 -rw-r--r-- 1 cxc cxc 9493 Jun  8 2002 /home/cxc/public_html/bbs/zboard.php
2363666 12 -rw-r--r-- 1 dalvit dalvit 9493 May 17 2004 /home/dalvit/public_html/zboard/zboard.php
27686445 12 -rw-r--r-- 1 silvan silvan 9493 Aug 14 2003 /home/silvan/public_html/bbs/zboard.php
20004998 12 -rw-r--r-- 1 cebukore cebukore 9493 Jun  8 2002 /home/cebukore/public_html/bbs/zboard.php
5488908 12 -rw-r--r-- 1 hansinfo hansinfo 9493 Jul 24 2004 /home/hansinfo/public_html/zero/zboard.php
22741102 12 -rw-r--r-- 1 cebu-bbs cebu-bbs 9493 Jun  8 2002 /home/cebu-bbs/public_html/bbs/zboard.php
sh-2.05b#
Ready [ssh2: AES-128 | 14, 11 | 14 Rows, 132 Cols | VT100]

```

※ Zeroboard를 사용하는 웹 호스팅 고객(사이트) 리스트

- 원격에서 PHP Injeciton 공격이 가능하도록 PHP 설정파일의 보안을 설정 하지 않음

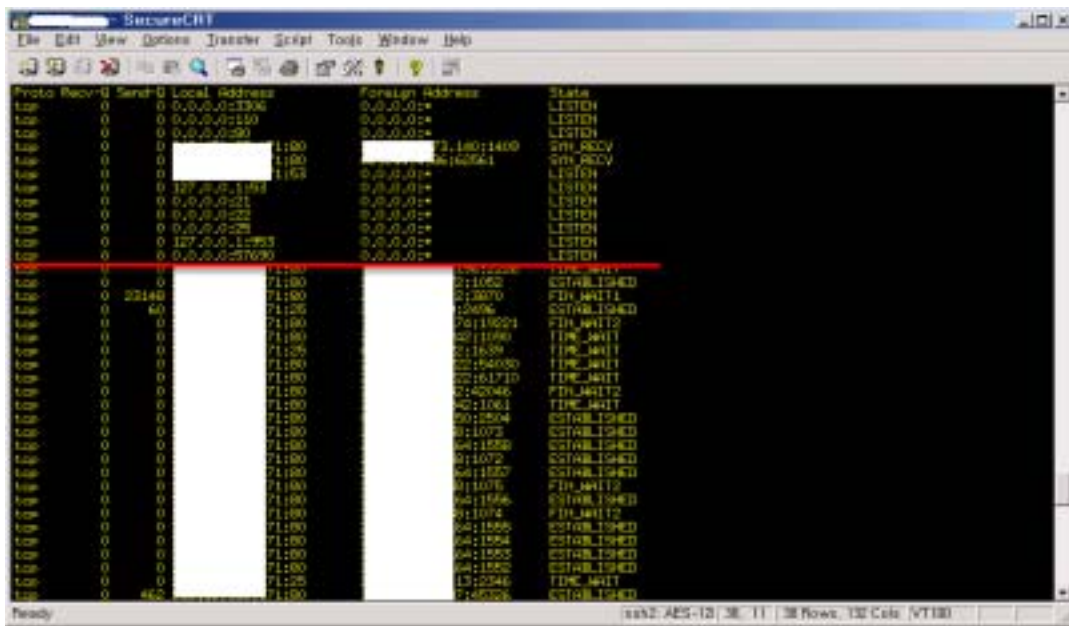
```

SecureCRT
File Edit View Options Transfer Script Tools Window Help
PHP
#####
1 README.txt
#####
2 This is the default settings file for new PHP installations.
3 By default, PHP installs itself with a configuration suitable for
4 development purposes, and safe for production purposes.
5 For several security-oriented considerations that should be taken
6 before going online with your site, please consult php.ini-recommended
7 and http://www.netmeister.org/security.php.
#####
8 About this file
9 #####
10 This file controls many aspects of PHP's behavior. In order for PHP to
11 read it, it must be named 'php.ini', PHP looks for it in the current
12 working directory, in the path designated by the environment variable
13 PHP_INI, and in the path that was defined in configure time (in that order).
14 Under Windows, the compile-time path is the WinPath directory. The
15 path in which the php.ini file is looked for can be overridden using
16 --ini-path
17 #####
18 Whether to allow the treatment of URLs like http:// or ftp:// as files.
19 allow_url_fopen = On
20
21 Define the accurate ftp password (user email address)
22 $ftp_pass="jsh@kore.com"
23
24 Define the User-Agent string
25 user_agent="PHP"
26
27 Default timeout for socket based streams (seconds)
28 default_socket_timeout = 60
29
30 If your scripts have to deal with files from Macintosh systems,
31 or you are running on a Mac and need to deal with files from
32 unix or windows systems, setting this flag will cause PHP to
33 automatically detect the OS character in those files so that
34 fopen() and file() will work regardless of the source of the files.
35 auto_detect_line_endings = Off
#####
Now--(SSH)
Ready [ssh2: AES-128 | 14, 11 | 14 Rows, 132 Cols | VT100]

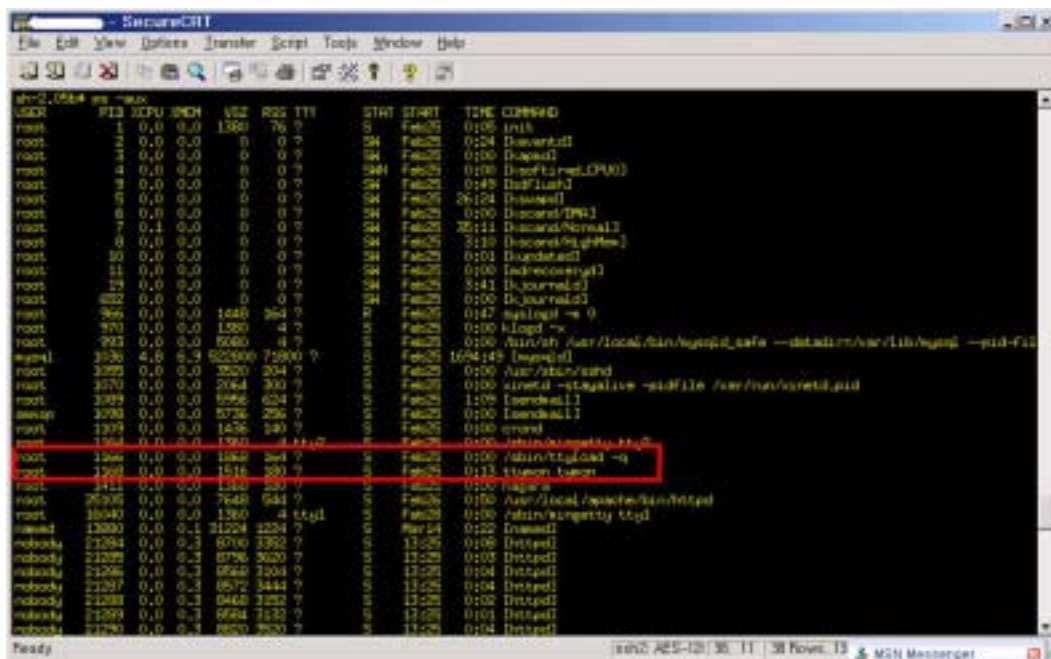
```

※ 원격 PHP Injection을 방어하기 위해서는 `allow_url_fopen=off` 로 설정을 하여야 하나, 시스템 관리자는 "On"을 설정하여 원격에서 PHP Injection 공격이 가능하도록 설정되어 있음

- 피해 시스템을 해킹한 침입자는 해당 시스템을 원격에서 접속하기 위하여 rootkit을 설치하였다.
 - 일반적으로 Linux 피해 시스템에서 가장 많이 사용되고 있는 SSH backdor를 TCP/57690 포트에 설치하였다.



- SSH Backdoor 프로세서 및 관련 파일



※ 피해 시스템의 주요 파일들이 변조되어, 분석을 위하여 일부 분석에 필요한 파일을 훼손되지 않는 시스템에서 가져와 분석함

- 침입자는 피해 시스템에 /sbin/ttyload라는 파일로 SSH Backdoor를 실행하였으며, 변조된 ls 명령어료를 해당 파일이 보이지 않게 해둠
- /sbin/ttyload는 최근 Linux 피해 시스템에서 많이 발견되며, 웹 변조 그룹에서 활발히 사용하는 SH Team Rootkit을 사용하였다.

```

sh-2.05# strings /tmp/0000000000
Linux
Info: This file is the property of SH-Crew team designed for test purposes.
We: SH-April/2003 produced in SH-Linux For LINUX Systems,fun and enjoy.
LINUX
T: 9
H:44
zXC*_]
MVSj
/whf
Filej
SH-1u
j1Rj
/tmp/sh-0000000000
rux,so.2,
0IG4U
r9*4
43*4
23*4
E1P61 MW
*611
DV304
4CD4D
774
1/7443Ub
2041/60
N116
J137
4*44h
_C1d
546,
47'48
T:4:
Ready
ssh@AES-128 3 38 Rows, 132 Cols VT100

```

※ SH-Crew Team Rootkit에 대해서는 향후 다른 기회에 상세 분석 예정

- 침입자는 피해 시스템의 사용자 ID로 기존의 시스템의 파일을 rootkit 파일 및 기타 파일로 변조를 하였다.

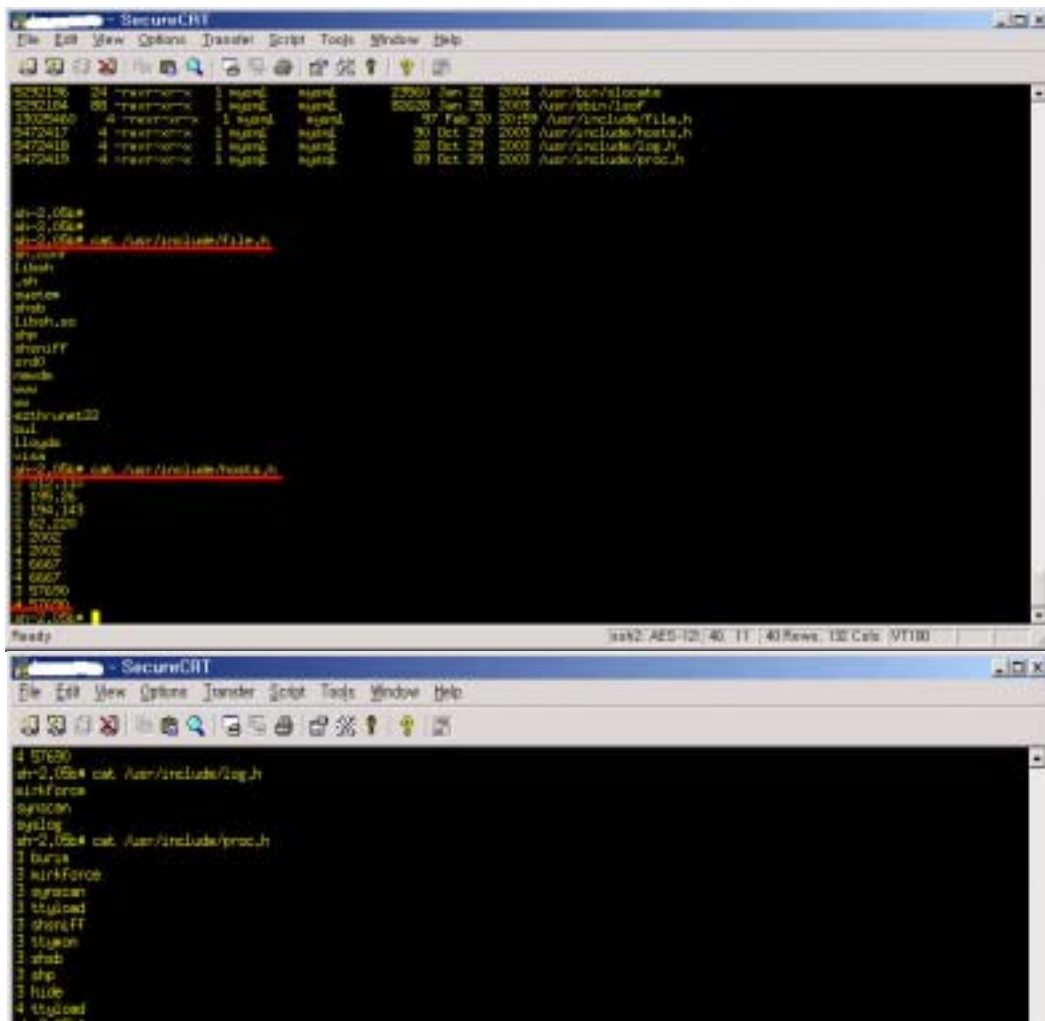
```

sh-2.05# find /usr/user -ls | grep tv apache
5292186 56 root:x86_64 1 sjml sjml 51006 Feb 25 20:10 /usr/bin/Find
5292185 40 root:x86_64 1 sjml sjml 39636 Oct 29 2003 /usr/bin/dtr
5292188 32 root:x86_64 1 sjml sjml 31462 Oct 29 2003 /usr/bin/wdsum
5292190 36 root:x86_64 1 sjml sjml 33992 Feb 20 2003 /usr/bin/top
5292196 24 root:x86_64 1 sjml sjml 23560 Jan 22 2004 /usr/bin/locate
5292184 88 root:x86_64 1 sjml sjml 82628 Jan 25 2003 /usr/bin/lscf
13025460 4 root:x86_64 1 sjml sjml 97 Feb 20 20:59 /usr/include/file.h
5472417 4 root:x86_64 1 sjml sjml 90 Oct 29 2003 /usr/include/hosts.h
5472418 4 root:x86_64 1 sjml sjml 28 Oct 29 2003 /usr/include/lang.h
5472419 4 root:x86_64 1 sjml sjml 89 Oct 29 2003 /usr/include/proc.h
sh-2.05#
Ready
ssh@AES-128 12 11 12 Rows, 132 Cols VT100

```

※ 주요 파일 변조 및 rootkit 설정 파일 생성

- 주요 변조 파일, 침입자 IP 대역 및 관련 포트에 대하여 탐지가 되지 않도록 설정



※ Backdoor 포트, 침입자 접속 IP 대역, 특정 Process 에 대하여 일반적으로 많이 사용하는 명령어인 ps, netstat 등으로 탐지되지 않게 설정

- 마지막으로 해당 시스템은 시스템 설치후 추가적인 보안 패치를 적용하지 않아 일반사용자로 접속후 최근 1-2년 동안 공개된 Linux용 Local 공격 도구를 이용하여 관리자 권한 획득이 가능하였다.

o 또한 다른 침입자에 의하여 피해 시스템에서는 불법 프로그램을 유포 목적으로 운영하는 Bot이 설치되어 있었다.

- 이러한 유형의 Bot은 최근에 유행한 홈페이지 변조 시스템에서도 종종 발견이 되었으며, 주로 해커그룹의 Channel Bot, Shell Bot 및 불법 프로그램 유포 용도로 사용하고 있다.

```
##### CONFIGURACAO #####
my $processo = '[httpd]';      $nome do processo if

$verita o findod i)
my $linhas_max=10; $depois de X ?
my $sleep=7;      $ ele dorme X ?

$ IRC
my $index="[DowDian]"; $path dos administradores
my $canais="[Vomur]";
my $nick="/bot_?";      $ nick do bot,, o o nick ja' estive' em uso,, vai aparece com um numero randomico no final
my $ircname = 'kif';

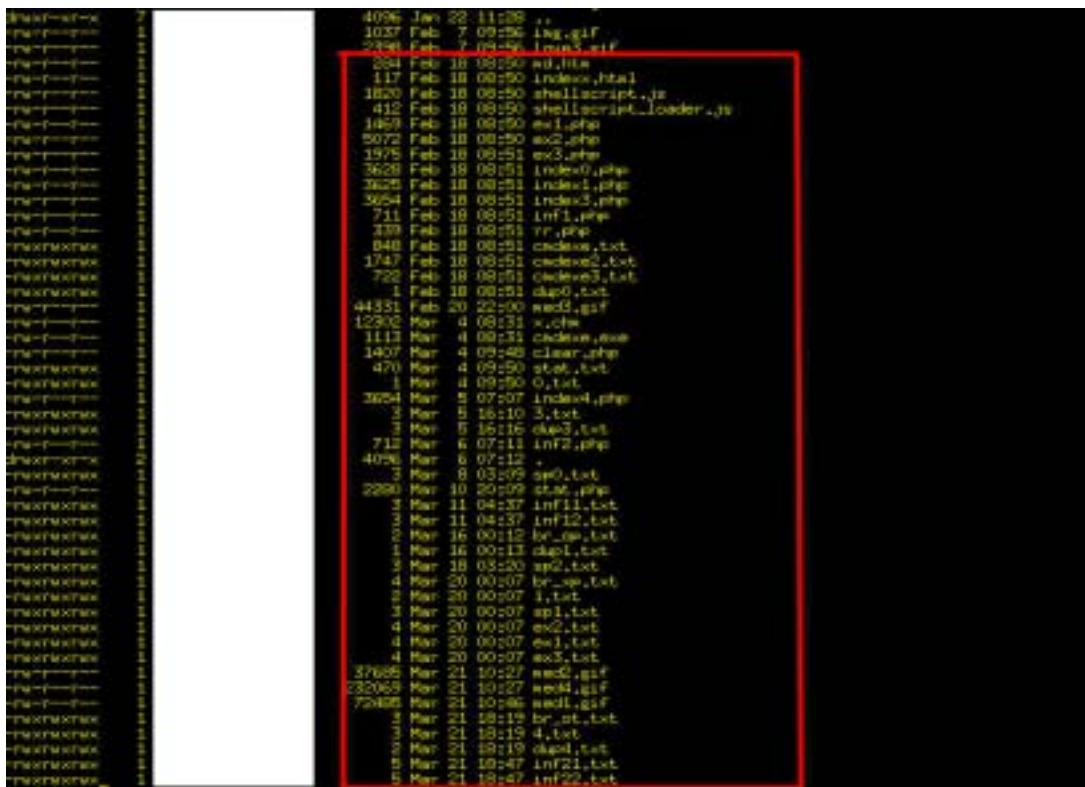
chomp (my $realname = `uname -n`);
$servidor= " " ".100" unless $servidor;      $servidor é irc q vai e usaia e não' foi especificado no argumento
my $porta= "6667";      $porta do servidor é irc

$ACENDO A SPILL
my $seco = 1;      $ 1 para 1 acesso a shell
#####
```

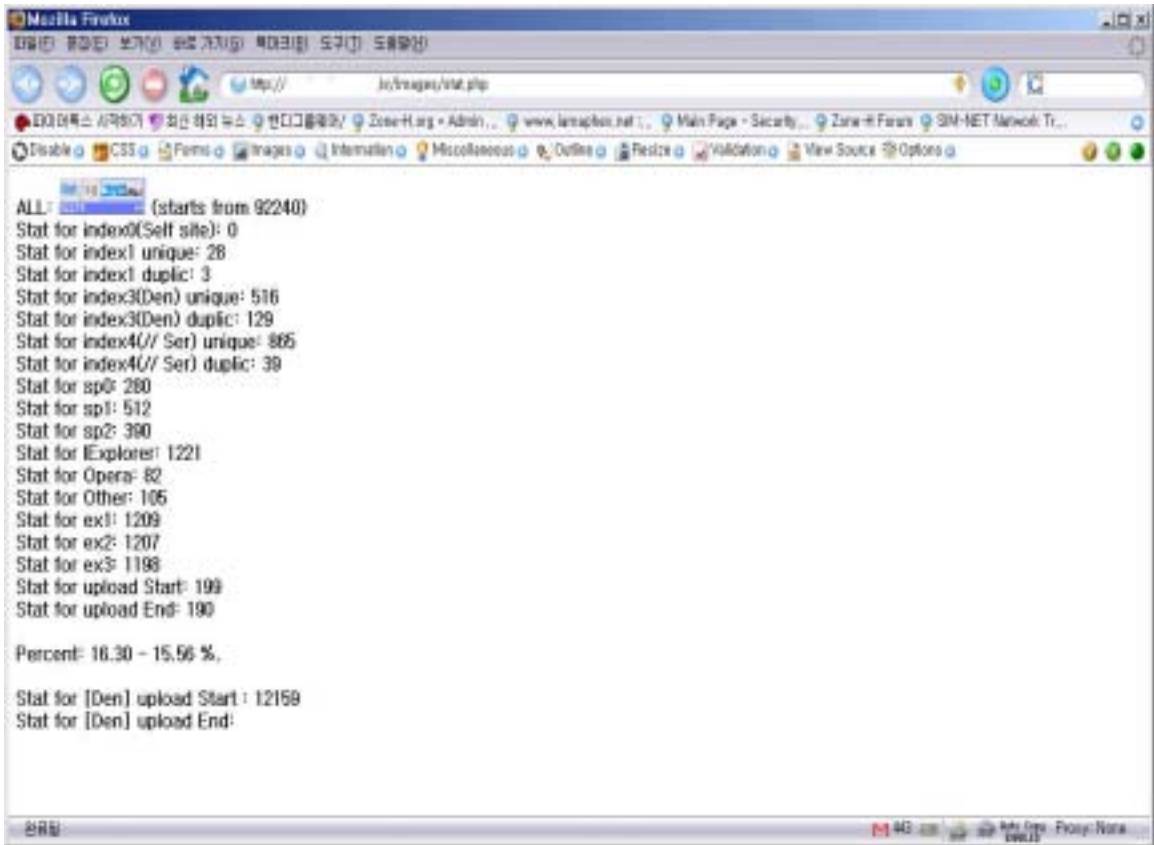
- 피해 시스템이 해킹을 당한지가 오래되어서 침입의 흔적을 발견하기는 쉽지 않아 침입자의 추적은 관련 로그 파일이 존재하지 않아서 이번 분석에서는 수행하지 않았다.

□ 악성 프로그램 유포 관련 분석

- 침입자는 악성 프로그램을 유포하기 위하여 피해시스템에서 웹호스팅하는 특정 사용자의 Directory중 일반적으로 간과하기 쉬운 images Directory를 이용하였다.



- 또한 침입자는 악성 프로그램을 탐지가 되지 않도록 Image 파일과 유사한 파일 형태로 악성 프로그램의 이름을 바꾸어 놓았다.
- 침입자는 악성 프로그램의 유포 현황을 파악하기 위하여 상태를 볼수 있도록 프로그램 만들어 두었는데, 접속하는 사용자의 인터넷 브라우저 형태, 보안 c패치 상태, 배포 현황 등을 원격에서 모니터링 하도록 만들어 놓았다.



- 주요 탐지되는 바이러스 정보는 다음과 같다.

파일명	바이러스명	비고
med1.gif	Trojan-PSW.Win32.Vipgsm.ac	
med2.gif	Trojan-Proxy.Win32.Daemonize.au	
med3.gif	Backdoor.Win32.Haxdoor.bx	
med4.gif	Backdoor.Win32.RA-based.p	
cmdexe.exe	Trojan-Downloader.Win32.Small.aon	
x.chm	Trojan-Downloader.Win32.Small.aon	

※ 침입자는 지속적으로 악성 프로그램을 배포를 위하여 관련 파일들을 변경 하였던 것으로 파악됨

3. 결론

- 국내에는 많은 웹 호스팅 업체들이 존재하고 있으며, 상당수의 시스템들이 보안에 취약한걸 로 파악되고 있다. 이러한 이유는 최근에 급증한 웹페이지 변조, 국내의 많은 시스템들이 Botnet 명령/제어 서버로 이용, 악성 프로그램 유포 사이트로 이용되고 있다.
- 이번 악성 프로그램 유포 사이트의 경우 웹 호스팅 시스템에 대한 주기적인 관리가 이루어 지지 않아서 몇 개월 동안 시스템이 해킹을 당하였어도 시스템 관리자는 이를 탐지 하지 못하고 있었으므로, 시스템 관리자의 주기적인 시스템 모니터링 및 보안 패치 적용이 선행되어야 한다.
- 대부분의 많은 사람들이 눈에 보이는 웹페이지 변조를 위하여 노력을 하고 있지만은 탐지 되지 않은 더욱 많은 해킹 피해 시스템들이 국내에 존재하고 있으며, 이에 대한 탐지 및 대응이 필요하다고 할 수 있다.
- 특히 공개소프트웨어를 많이 사용하는 웹 호스팅 및 국내 .Com 시스템들에 대해서 보다 체계적인 정보보호 접근 및 대책이 필요하다고 할 수 있다.