악성프로그램 유포로 이용된 국내 시스템 사고 분석

2005. 4. 1

인터넷침해사고대응지원센터 (KISC)

목 차

1. 개 요

o 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.

o 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

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

□ 악성 프로그램 개요

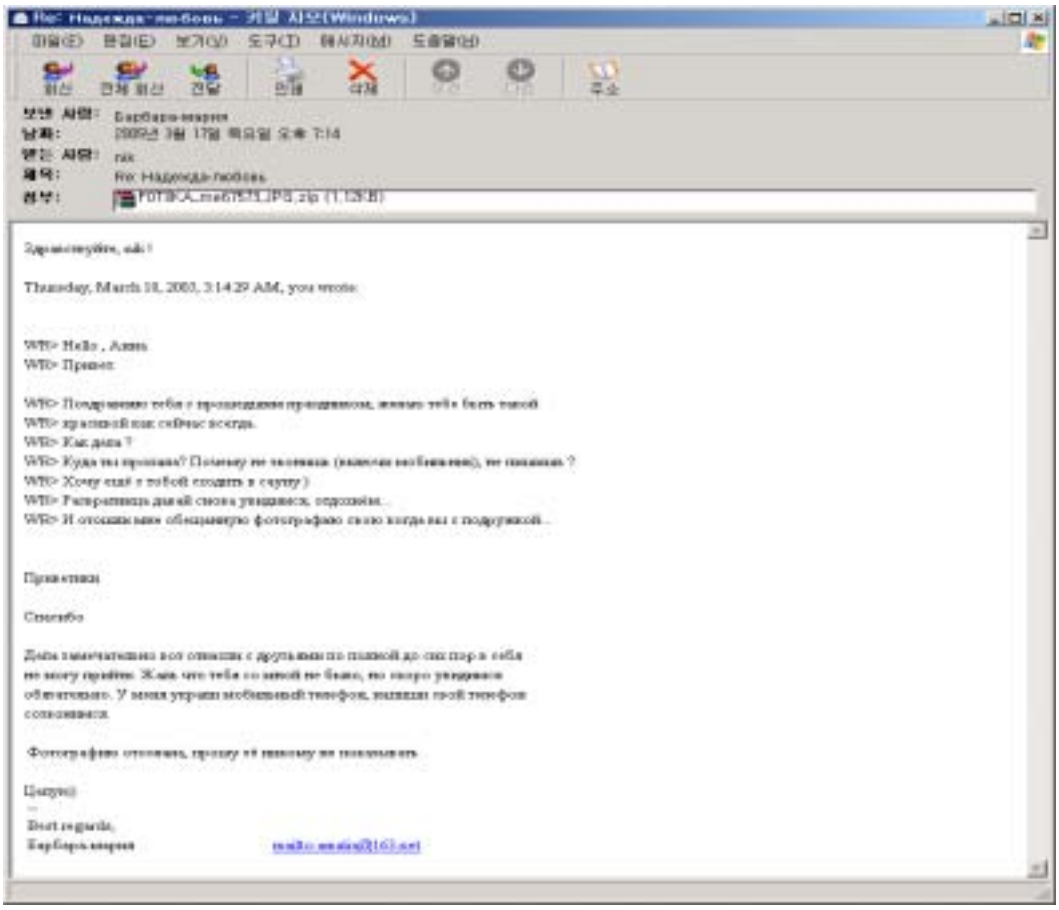
o 바이러스명 : Trojan-Downloader.Win32.Small.aon 등 다수
o 위의 파일은 다른 5개 이상의 Trojan, BackDoor 등을 해당 사이트로부터 다운로드 함
o 참고 사이트 : http://www.enciclopedia-virus.com/virus/vervirus.php?id=1789
o 유포자는 E-Mail 첨부 파일을 통하여 일반사용자들에게 전송후, 일반 사용자는 첨부파일 OPEN시 바로 국내 사이트로부터 순차적으로 특정 악성 프로그램을 다운로드 받게 됨

□ 악성 프로그램 유포 방법

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

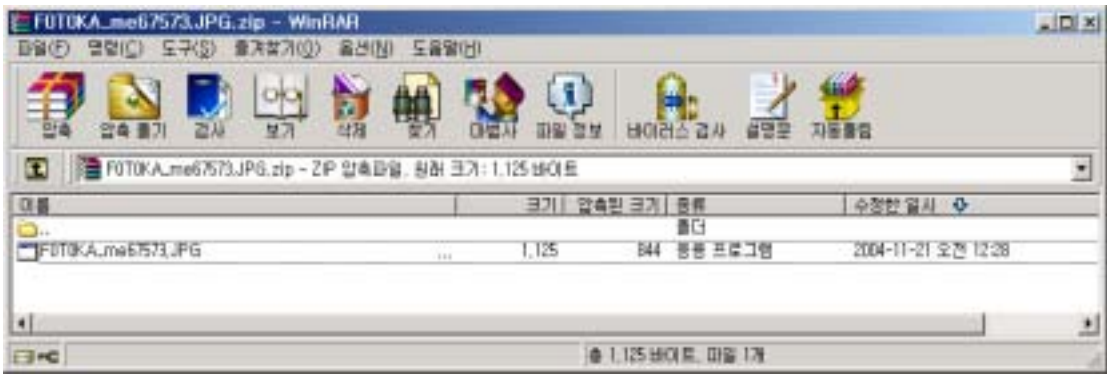
2. 피해 시스템 분석

□ 악성 프로그램 유포 E-Mail 원본 및 내용



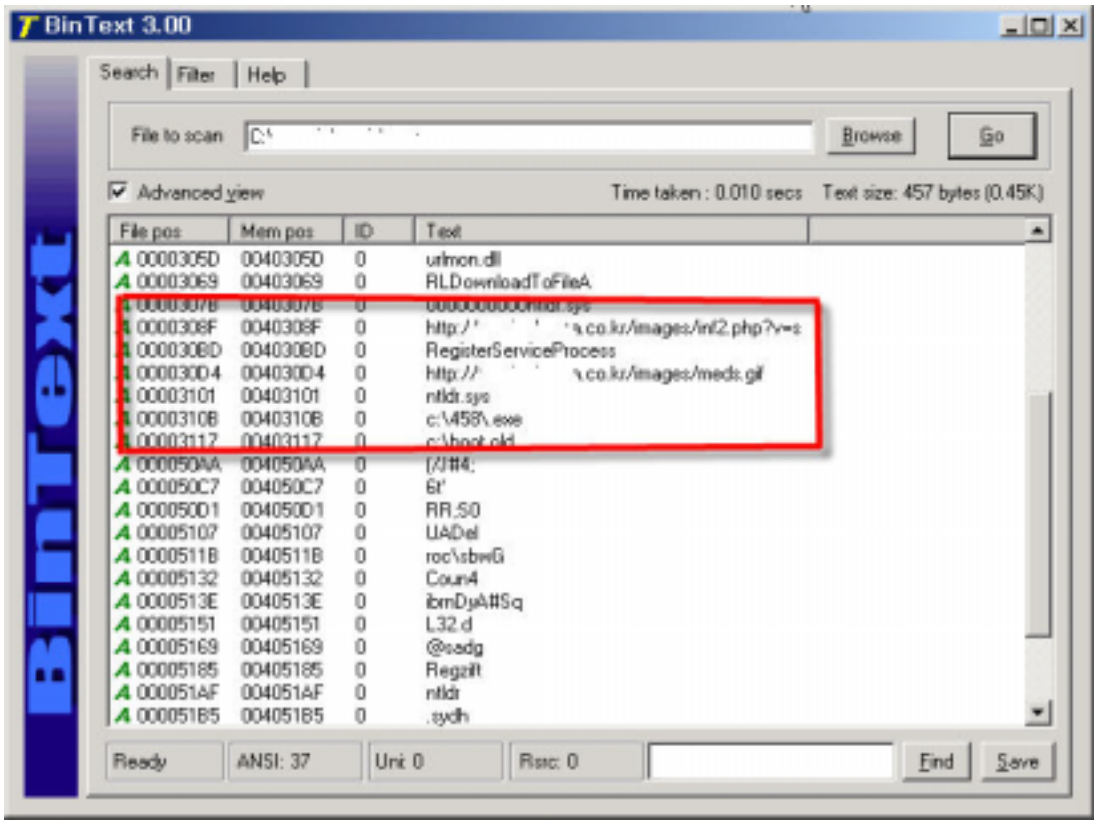
※ 유포자는 러시아 언어로 된 E-Mail을 유포

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



※ 첨부파일 압축 해제 후 화면

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



※국내의 웹사이트로부터 악성 프로그램을 다운로드 받도록 설계

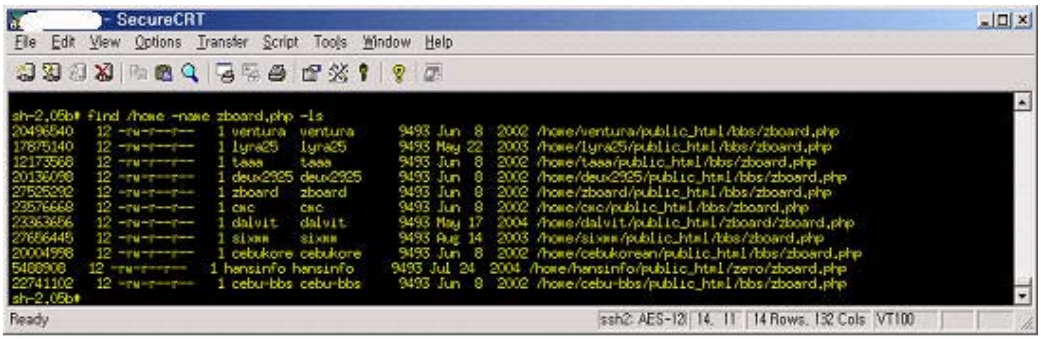
□ 피해 시스템 해킹 원인 분석

o 피해 시스템은 최근 국내 웹페이지 변조에 많이 사용되는 Zeroboard 사용하고 있었으며, 몇몇 사용자는 취약성 버전을 사용하고 있었다.

o 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.

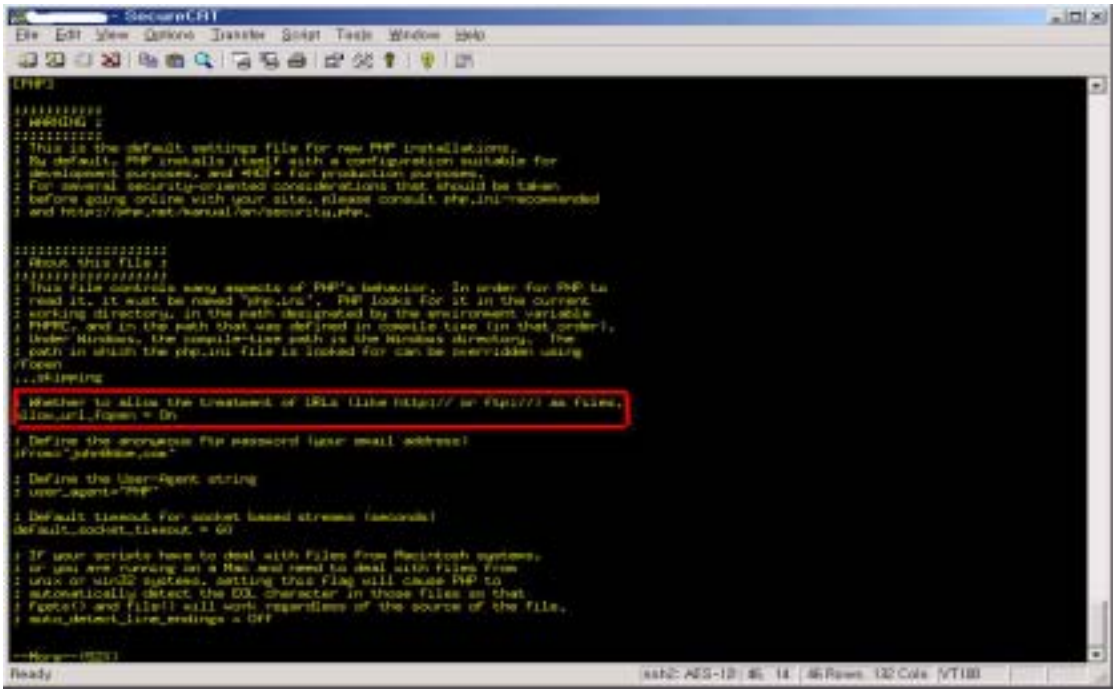
o 마지막으로 피해시스템은 웹 호스팅 사용자들이 원격에서 접속을 하도록 서비스를 허용을 하였는데, 많은 고객들이 숫자로 구성된 비밀번호를 사용하거나, 사용자 ID 와 같은 비밀번호를 사용하여 Brute Force 공격에 취약하였다.

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



※ Zeroboard를 사용하는 웹 호스팅 고객(사이트) 리스트

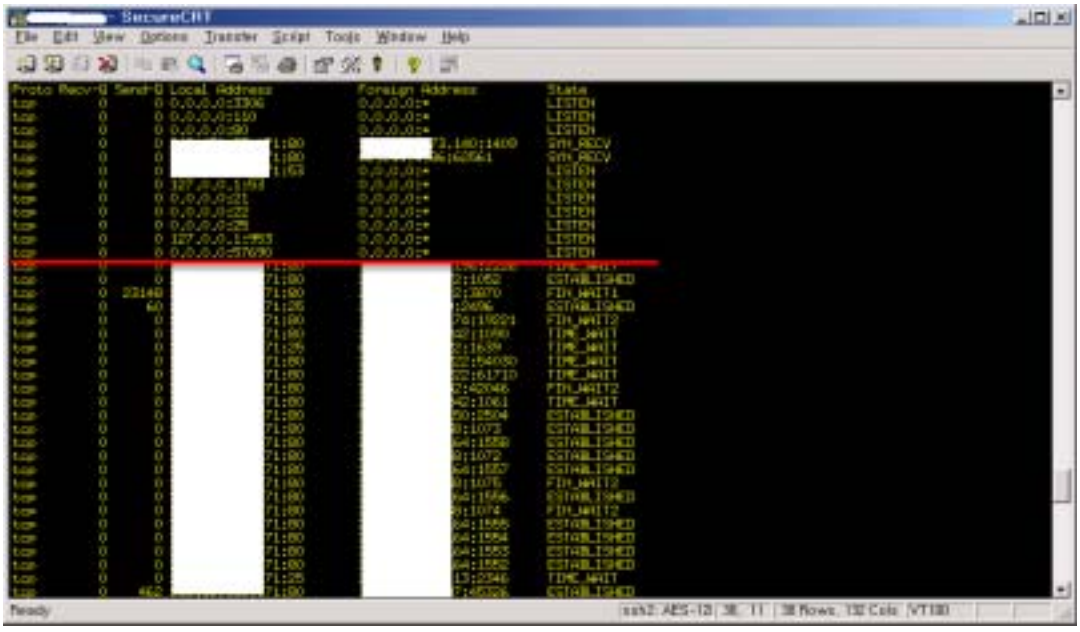
o 원격에서 PHP Injeciton 공격이 가능하도록 PHP 설정파일의 보안을 설정 하지 않음



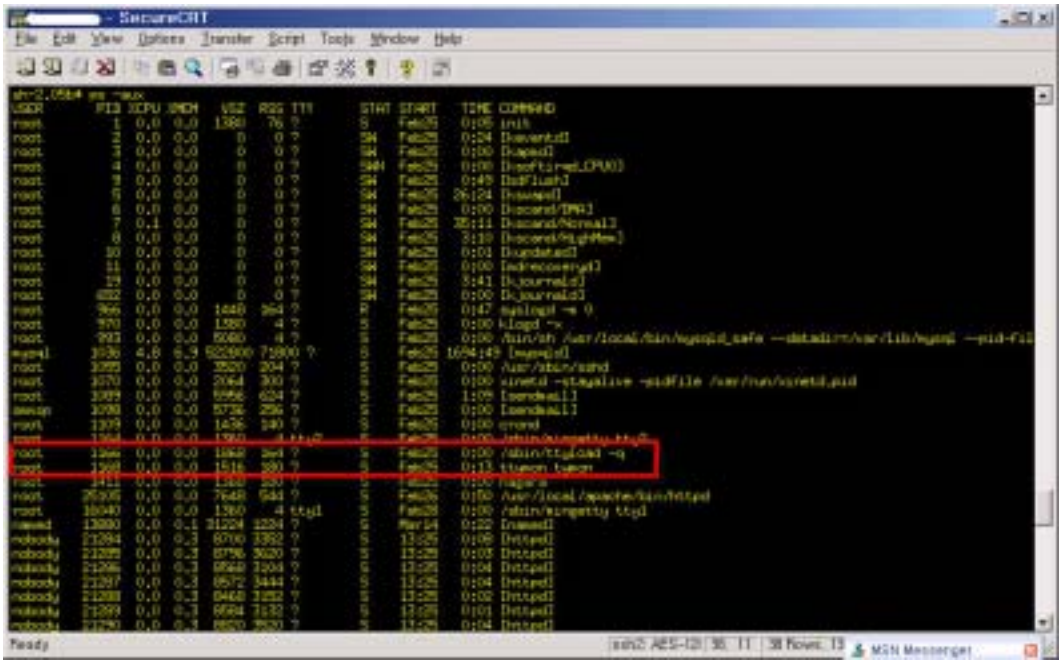
※원격 PHP Injection을 방어하기 위해서는 allow_url_fopen=off 로 설정을 하여야 하나, 시스템 관리자는 "On"을 설정하여 원격에서 PHP Injection 공격이 가능하도록 설정되어 있음

o 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.



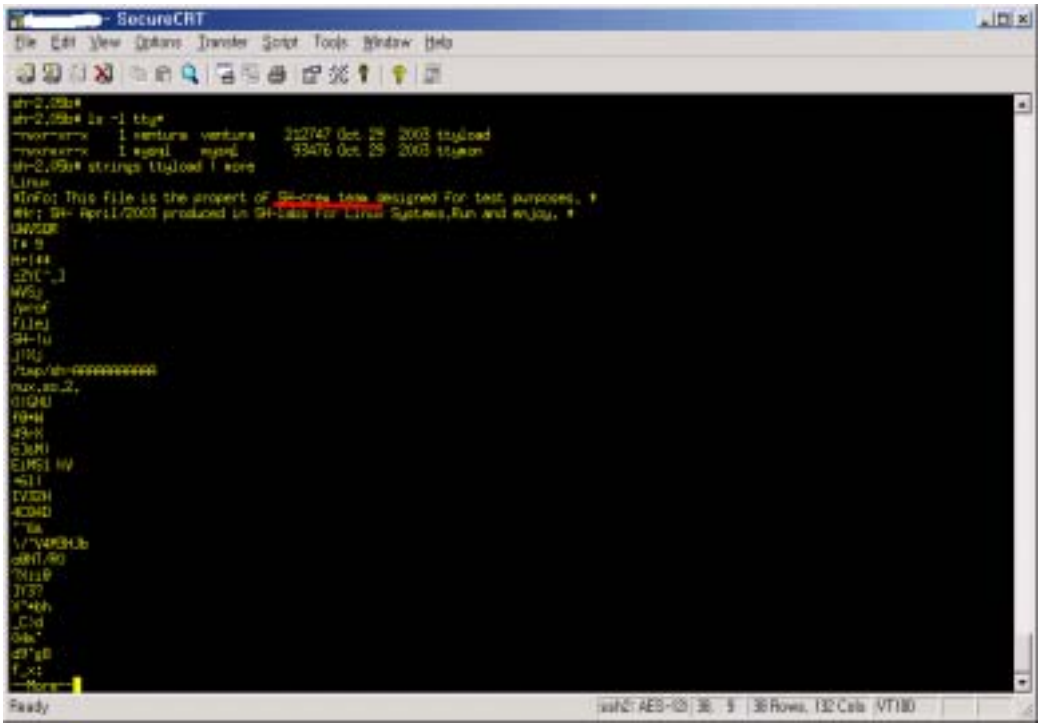
- SSH Backdoor 프로세서 및 관련 파일



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

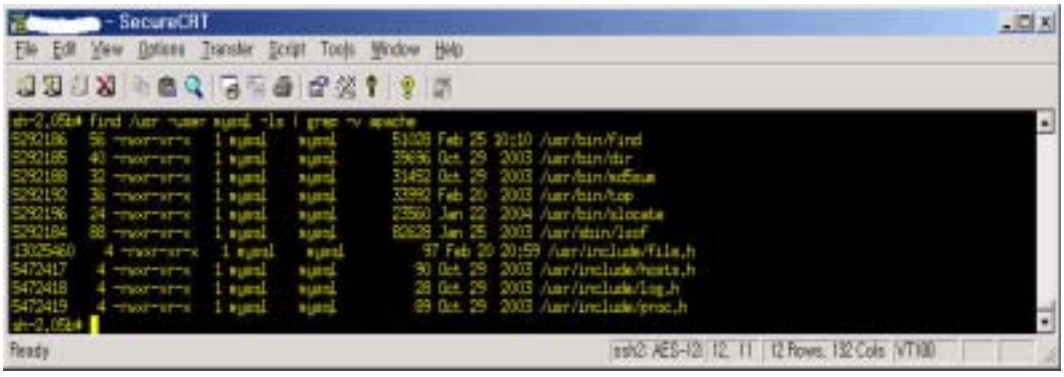
- 침입자는 피해 시스템에 /sbin/ttyload라는 파일로 SSH Backdoor를 실행하였으며, 변조된 ls 명령어로를 해당 파일이 보이지 않게 해둠

- /sbin/ttyload는 최근 Linux 피해 시스템에서 많이 발견되며, 웹 변조 그룹에서 활발히 사용하는 SH Team Rootkit을 사용하였다.



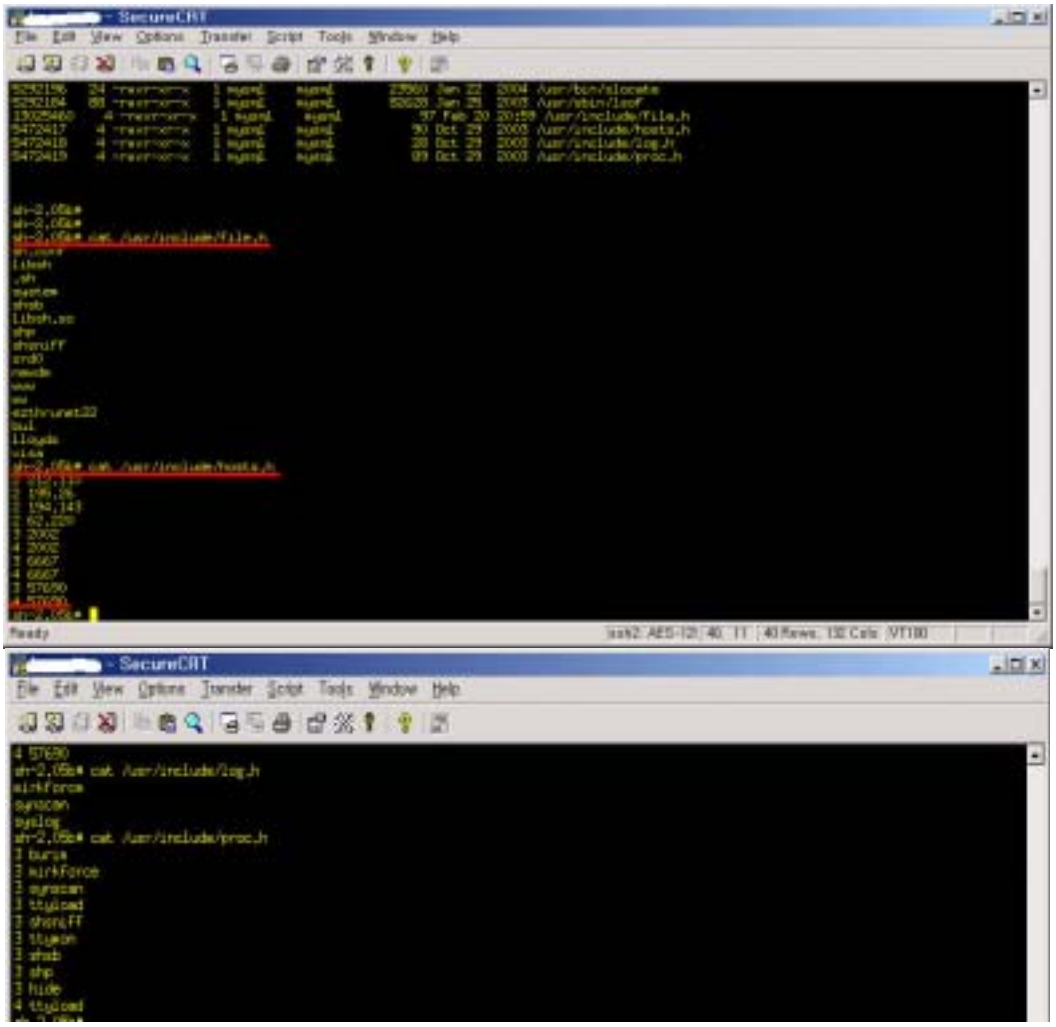
※ SH-Crew Team Rootkit에 대해서는 향후 다른 기회에 상세 분석 예정

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



※ 주요 파일 변조 및 rootkit 설정 파일 생성

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

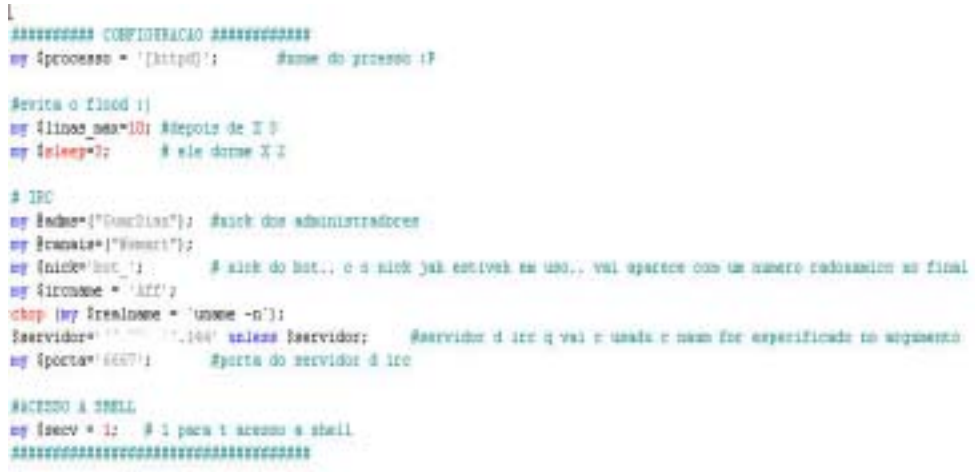


※ Backdoor 포트, 침입자 접속 IP 대역, 특정 Process 에 대하여 일반적으로 많이 사용하는 명령어인 ps, netstat 등으로 탐지되지 않게 설정

- 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.

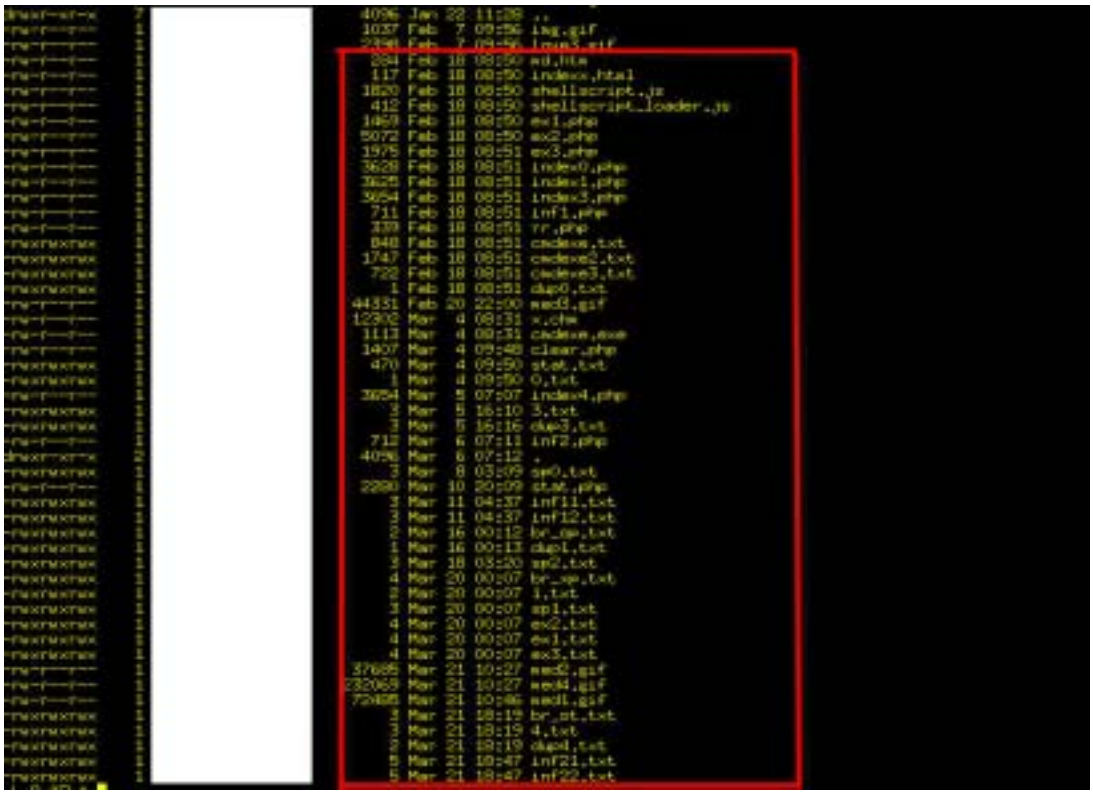
- 이러한 유형의 Bot은 최근에 유행한 홈페이지 변조 시스템에서도 종종 발견이 되었으며, 주로 해커그룹의 Channel Bot, Shell Bot 및 불법 프로그램 유포 용도로 사용하고 있다.



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

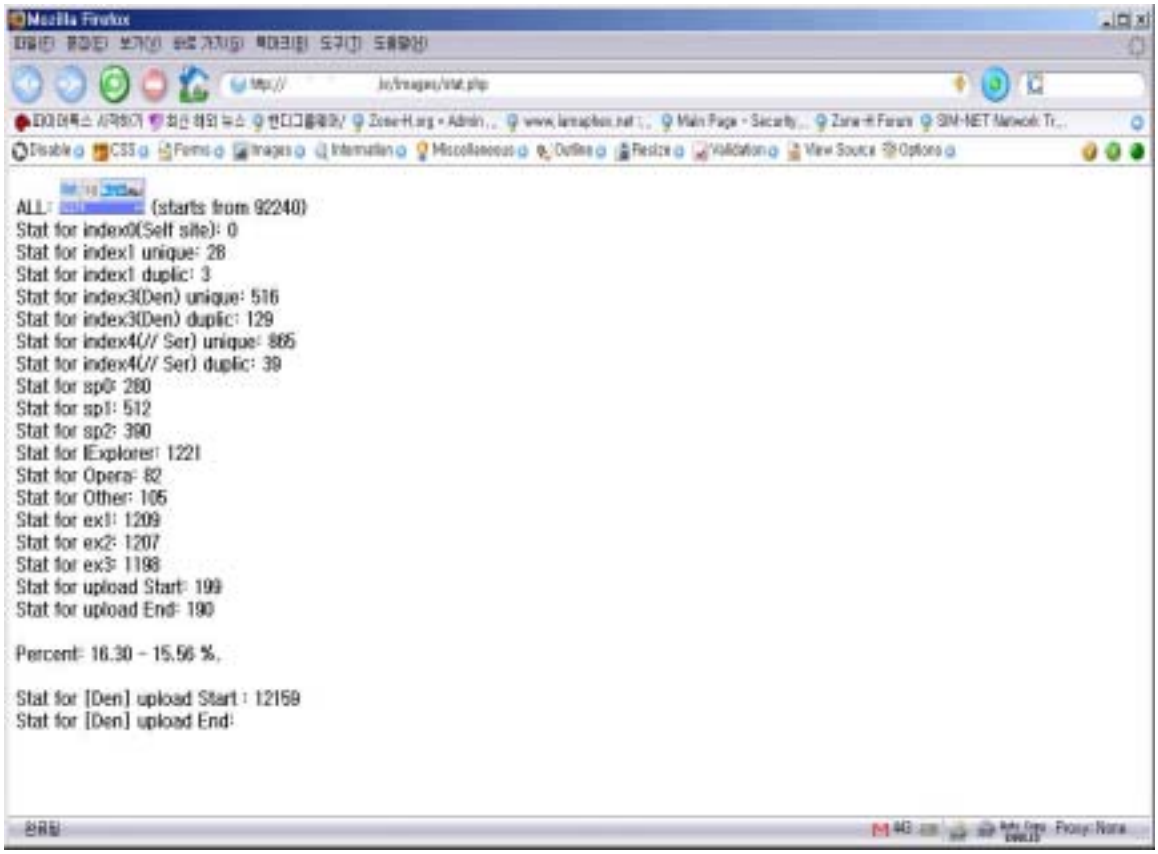
□ 악성 프로그램 유포 관련 분석

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



o 또한 침입자는 악성 프로그램을 탐지가 되지 않도록 Image 파일과 유사한 파일 형태로 악성 프로그램의 이름을 바꾸어 놓았다.

o 침입자는 악성 프로그램의 유포 현황을 파악하기 위하여 상태를 볼수 있도록 프로그램 만들어 두었는데, 접속하는 사용자의 인터넷 브라우저 형태, 보안 c 패치 상태, 배포 현황 등을 원격에서 모니터링 하도록 만들어 놓았다.



o 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 변경하였던 것으로 파악됨

3. 결론

o 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.

o 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.

o 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.

o 특히 공개소프트웨어를 많이 사용하는 웹 호스팅 및 국내 .Com 시스템들에 대해서 보다 체계적인 정보보호 접근 및 대책이 필요하다고 할 수 있다.