

# Malware Analysis #6

Anthony Martinez (Pi), pi@pihost.us

February 18, 2006

## 1 Are the files packed?

No. Both files are in cleartext.

## 2 Identify what the malware can do

### 2.1 Static analysis

/usr/bin/strings on shell1 reveals phrases relevant to IRC connections, as well as DDoS attacks. (Reformatted to fit on the page)

```
irc.ircnet.net
NOTICE %s :Unable to comply.
%s : USERID : UNIX : %s
NICK %s
USER %s localhost localhost :%s
ERROR
NOTICE %s :TSUNAMI <target> <secs>
    = Special packeter that wont be blocked by most firewalls
NOTICE %s :PAN <target> <port> <secs>
    = An advanced syn flooder that will kill most network drivers
NOTICE %s :UDP <target> <port> <secs>
    = A udp flooder
NOTICE %s :UNKNOWN <target> <secs>
    = Another non-spoof udp flooder
```

cmd.gif appears to be a PHP-based command execution facility, using one of passthru(), system(), exec(), popen(), shell\_exec(), or proc\_open(), whichever it finds first. It also looks for the existence of xterm, netcat, wget, lynx, and a C compiler. The script also appears to have file editing capability built in.

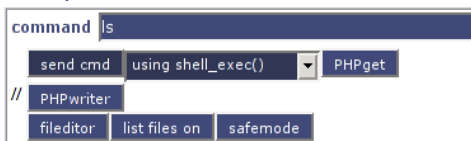
```
//
Warning: main(http://ess.trix.net/therules.dat): failed to open stream: HTTP request failed! HTTP/1.1 403 Forbidden in /var/www/cmd.php on line 13

Warning: main(): Failed opening 'http://ess.trix.net/therules.dat' for inclusion (include_path='.:usr/share/php:usr/share/pear') in /var/www/cmd.php on line 13
//
```

**[ Defacing Tool Pro v ] ?**  
by r3v3ng4ns - revengans@gmail.com

//

```
sysname: Linux
nodename: coffeeshost
release: 2.6.15-plague
version: #1 PREEMPT Wed Jan 11 18:44:19 MST 2006
machine: i686
user: uid(33) euid(33) gid(33)
write permission: no
server info:
pro info: ip 127.0.0.1, wget at /usr/bin/wget, safe_mode: NO, PHP
4.4.2-1
current path: /var/www
```



stdOut from "", using shell\_exec()

```
//Comandos Exclusivos do DTool Pro
chdir <diretorio>; outros; cmds;
//uda o diretorio para aquele especificado e permanece nele. Eh como se fosse o 'cd' numa shell,
mas precisa ser o primeiro da linha. Os arquivos listados pelo filelist sao o do diretorio
especificado ex: chdir /diretorio/sub;/pwd;ls
PHPget, PHPwriter, Fileditor, File List e Overwrite
fale com o r3v3ng4ns :P
```

## 2.2 Running it

Running shell1 under strace revealed that it forked immediately, tried to connect to IRCnet and found itself klined: :irc1.us.open-ircnet.net 465 KCGGPDPI :You (\*@63.xxx.xxx.xxx) are banned from this server: Random drone-like nicks are prohibited. ERROR :Closing Link: KCGGPDPI[unknown@63.xxx.xxx.xxx] (K-lined: Random drone-like nicks are prohibited.)

## 3 What changes will the malware make?

Neither file makes any immediate change to the system, but *do* provide ways to run arbitrary shell commands.

## 4 What is the purpose of the malware? Are they related?

cmd.gif may be used to remotely launch shell1, edit files, and run any shell command, including wget, and xterm. shell1 is an irc drone, providing the ability to DDOS machines. They are not immediately related in function, but were probably uploaded by the same attacker.

## 5 Why didn't they show in ps aux?

cmd.gif runs under apache. It's not going to show up as a separate process, since it is part of the http server.

shell1, on the other hand, overwrites ARGV[0] with the string -bash, to make it appear that it is legit. Any of these processes could be shell1:

```
root      29578  73.6  0.3  1820   640 pts/0    R   14:39   5:48 -bash
root      29638   0.0  0.2   1680   468 pts/0    S   14:42   0:00 -bash
root      29695   0.0  0.2   1680   468 pts/0    S   14:44   0:00 -bash
root      29720   0.0  0.2   1680   500 pts/0    S   14:44   0:00 -bash
```

## 6 How was the machine compromised?

A (disturbingly) quick session with John the Ripper revealed the password of the user `backup` as `backup`. `/var/log/secure` shows that the machine was ssh scanned and the `backup` account was broken into.

## 7 What useful information in in the files?

`cmd.gif` was originally called "Defacing Tool," and was written by `r3v3ng4ns`, `revengans@gmail.com`.

## 8 Possible attack scenario

In addition to compromising the `backup` user, the attacker seems to have broken root: `shell1` is running as the superuser. The method of root compromise is not immediately obvious. Perhaps it is due to the fact that they are running their GUI environments (`gnome`, `dbus`, `esd`, and `aRts`) as the superuser.

## 9 Security measures

1. Don't run GUI environments as root. The risk of possible compromise is too high.
2. Set a password policy that outlaws at least setting password equal to username.
3. Firewall outgoing IRC connections if you do not use IRC.