

Malware Challenge Submission
Dan Kieta 10/26/2008
daniel.m.kieta@sherwin.com

Question 1

Describe your malware lab.

My lab consists of an installation of VMWare Workstation 6 on a Lenovo P61 laptop. I have two VM's that are restricted to a private VNET.

- A Windows SP2 PC with no patches beyond the default SP2 installation, with the windows firewall disabled. No security software is installed. I have various monitoring, debugging, and disassembly tools installed (sysinternals suite, regshot, lord pe, ollydbg, ida pro freeware, bintext, etc).
- A Redhat Linux VM, that is stripped down with monitoring tools installed (ircd, honeyd, snort, tcpdump, netcat, etc).

The windows VM has the default route pointed to the linux VM so that all ip traffic will be forwarded to the linux VM for monitoring.

Question 2

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

I uploaded the sample to virustotal, which identified the executable against 35 of the leading AV engines. It also determined that the file has been packed with UPX, a common and reversible packing routine. Although likely in a zero day scenario, this output from virustotal would be much less valuable.

I used the bintext utility to look for useful strings in the binary. I did not see any that were interesting, suggesting that the file was likely packed. When analyzing the code statically with IDA pro freeware, it seems to confirm that it may be packed with something similar to UPX, as you do see a POPAD instruction, followed by a jump into the likely original entry point (OEP). It appears that I should be able to dump the unpacked executable with ollydump.

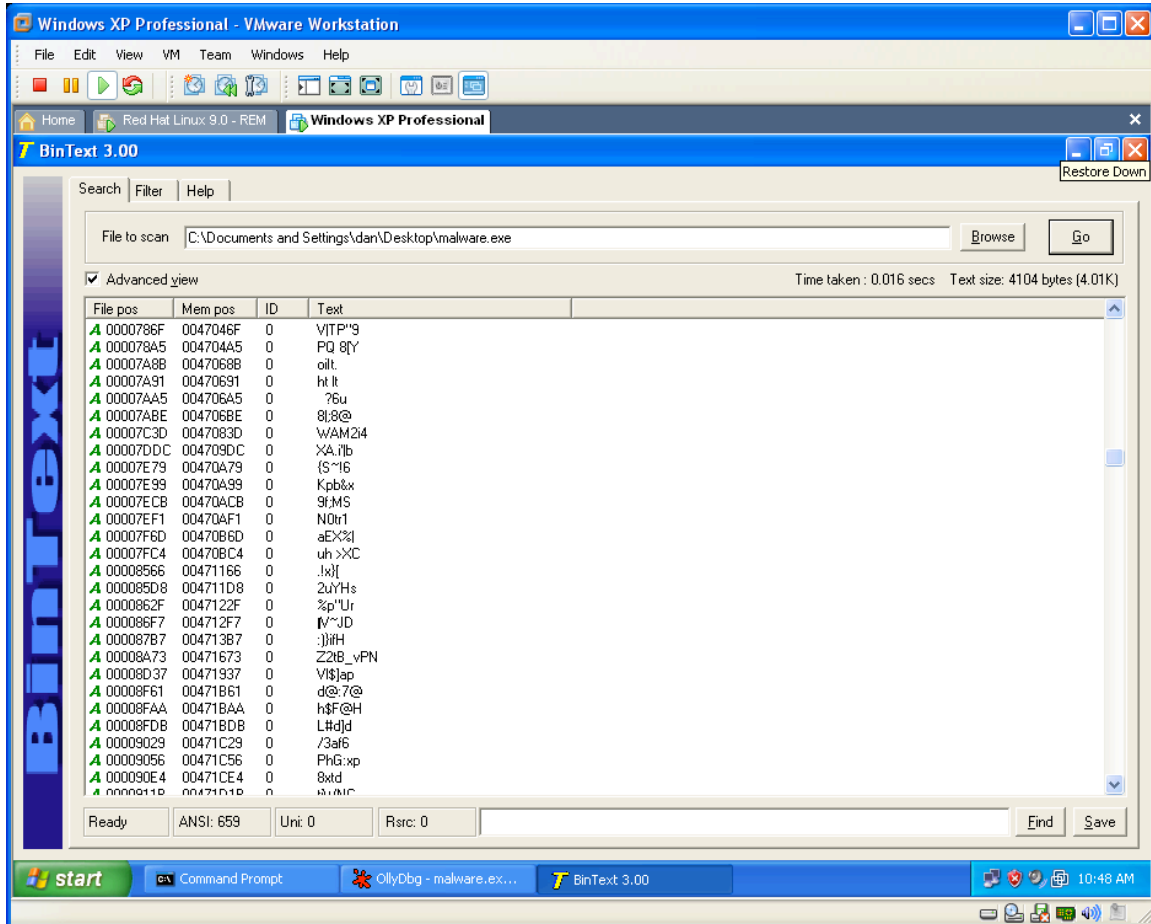
Question 3

Is the malware packed? If so, how did you determine what it was?

The file is definitely packed as mentioned in the answer to question 2.

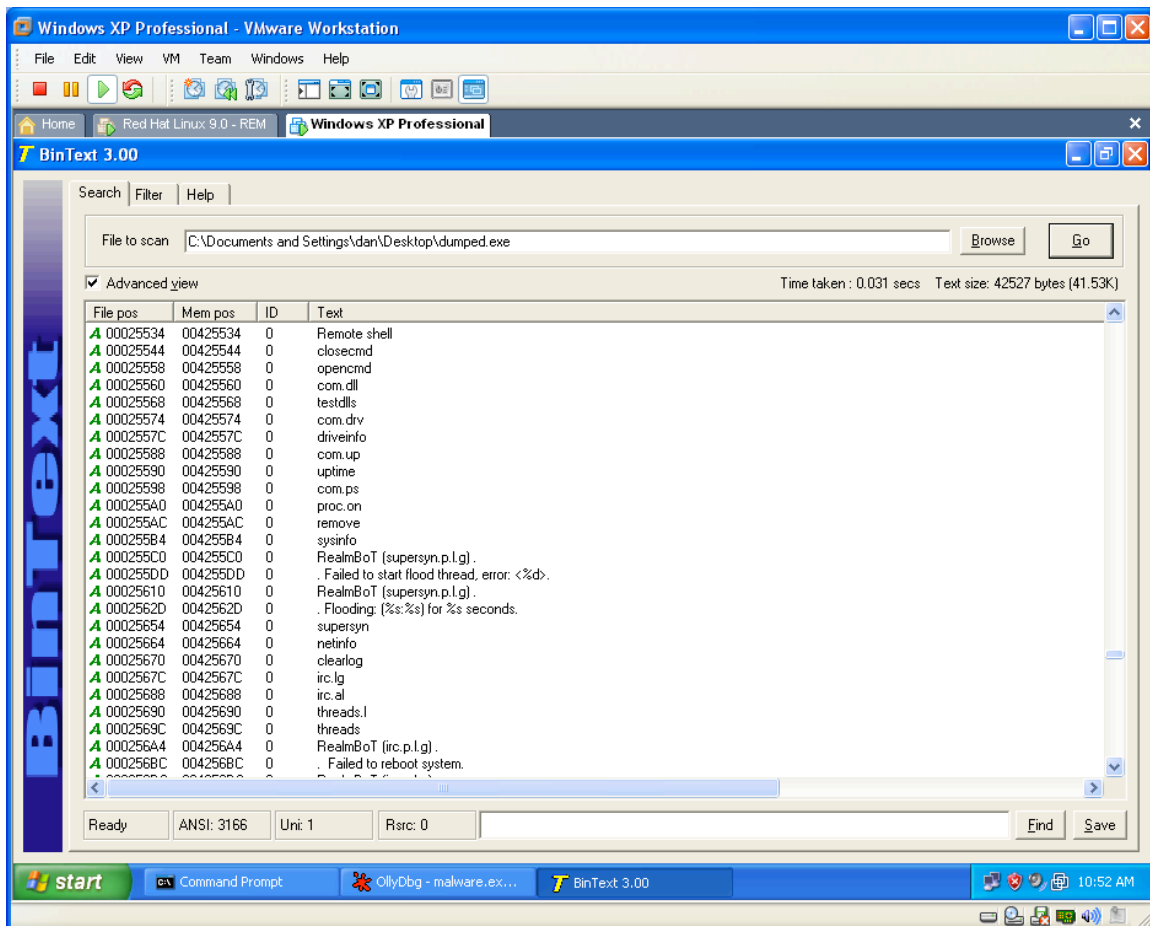
Virustotal.com indicated that it was probably UPX packed. I attempted to unpack the file with a UPX unpacker, but was unsuccessful. I received an error that indicated that the file was modified/hacked/protected.

Packed Executable, no interesting strings.



As mentioned in question 2, my static code analysis seemed to indicate that it either was UPX packed, or was something similar. I was able to determine what I thought was the OEP at 004109cc. I dumped the file with ollydump and rebuilt the PE headers with Lord PE. This produced a functioning executable. I ran the file through bintext, which revealed a lot of interesting strings that reveal the function of the malware as a bot.

Unpacked executable, showing possible bot command structure



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?

Before first executing the malware, I did two things. I started regshot so that I can determine what files and reg keys had changed after running the executable. I also started procmon to monitor the activity.

I launched the executable and waited a minute or two. I then ran a second shot with regshot and determine that the following file was dropped (and was executed and left running):

C:\windows\Winsec32.exe

The following registry keys were added:

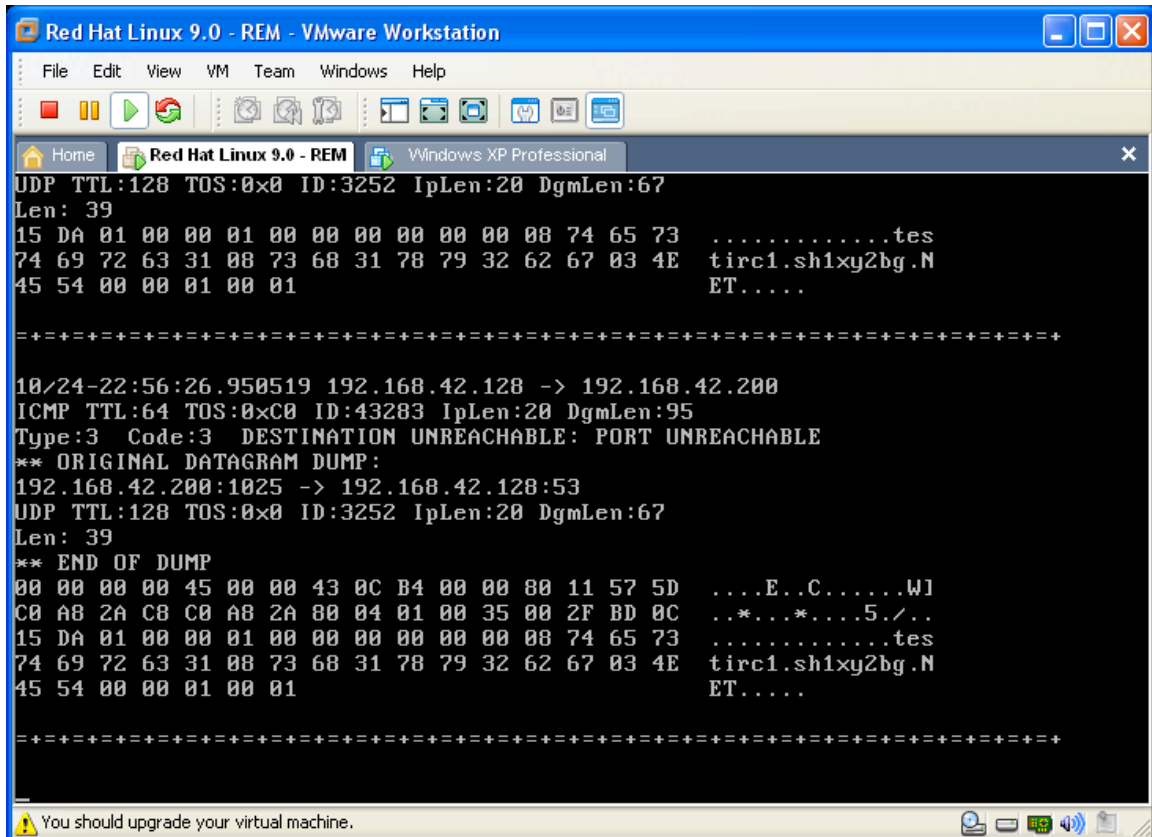
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Svchost local services: "Winsec32.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Svchost local services: "Winsec32.exe"

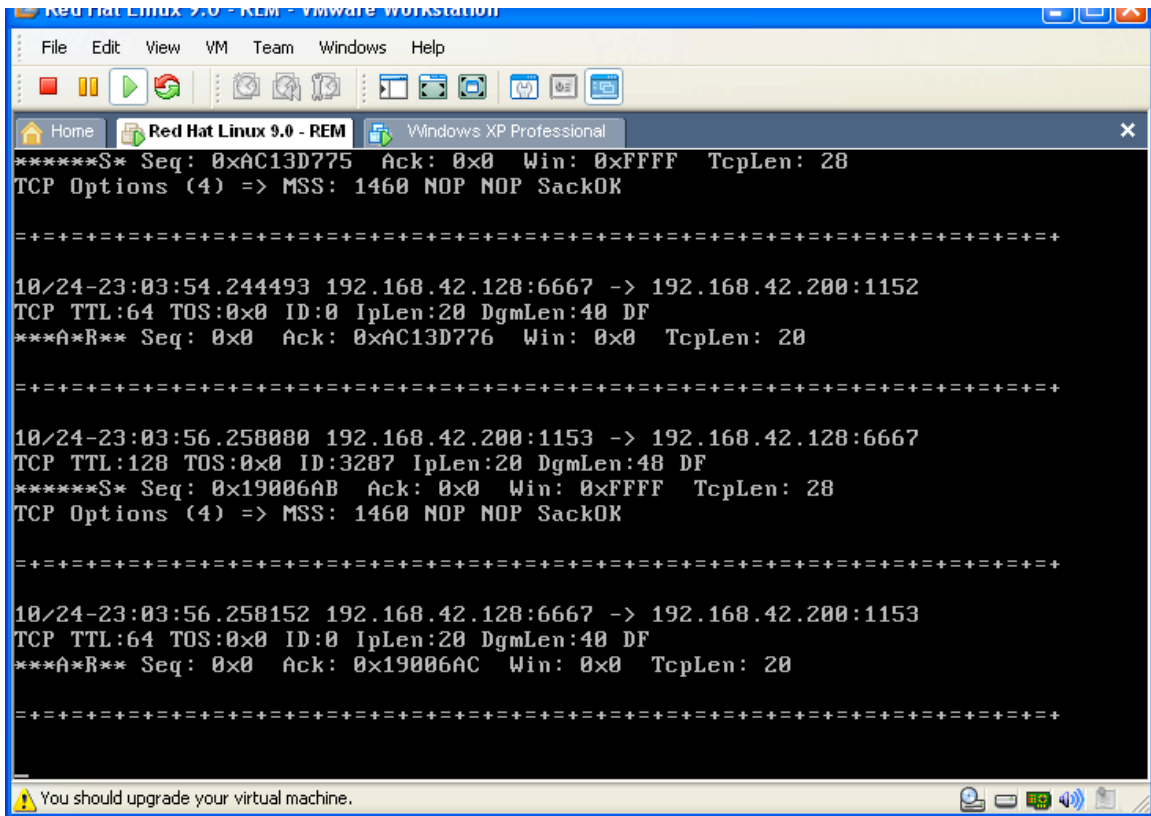
HKEY_USERS\S-1-5-21-1993962763-287218729-725345543-1003\Software\Microsoft\OLE\Microsoft Svchost local services: "Winsec32.exe"

The combination of the file and reg keys would cause the malware to be persistent if the machine is restarted as the malicious executable would be launched at start time.

To monitor the network traffic possibly generated by the malware. I used snort on the linux VM to look for interesting traffic. The first thing I looked for was DNS queries, which were revealed. The malware was trying to lookup testirc.sh1xy2bg.net.



I edited the hosts file on the PC to point the desired hostname to the linux box and relaunched the exe. This now showed that it was attempting to connect to TCP/6667, IRC traffic.



I gave the malware what it wanted and launched IRCD on the linux server and launched the malware again. This time it connected to the IRC server and joined a channel #challenge and set its NICK to USA[XP]57. This appears to be obvious bot activity connecting to a command and control server.

I decided to connect to the IRC channel and determine if I could interact with it. I joined the channel #challenge and noticed that it was in moderated mode. This did not allow me to interact with the bot. I killed the malware and joined the channel and then relaunched it. At this point, I was an op in the channel and could send messages. I decided to attempt some of the commands I had seen in the unpacked binary file, specifically "login". I found that I needed a period before the login command for it to be understood, but seemed to get a reaction from the bot:

```
Red Hat Linux 9.0 - REM - VMware Workstation
File Edit View VM Team Windows Help
Home Red Hat Linux 9.0 - REM Windows XP Professional
*** WALLCHOPS PREFIX=(ov)@+ CHANTYPES=#& MAXCHANNELS=20 MAXBANS=25 NICKLEN=9
+TOPICLEN=120 KICKLEN=90 NETWORK=EFnet CHANMODES=b,k,l,impst MODES=4 are
+supported by this server
*** There are 0 users and 1 invisible on 1 servers
*** This server has 1 clients and 0 servers connected
*** Current local users: 1 Max: 1
*** Current global users: 1 Max: 1
*** Highest connection count: 1 (1 clients) (3 since server was (re)started)
*** - localhost.localdomain Message of the Day -
*** - This is an IRC server. Authorized users only.
*** Mode change "+i" for user ircd by ircd
*** Channel Users Topic
*** ircd (~ircd@127.0.0.1) has joined channel #challenge
*** Mode change "+nt" on channel #challenge by localhost.localdomain
*** #challenge 1224910446
*** Mode change "+nt" on channel #challenge by ircd
*** No argument specified
#challenge ircd HQ ~ircd@127.0.0.1 (*Unknown*)
*** USA[XP]83 (~ppbszhcp@192.168.42.200) has joined channel #challenge
> .login
> .login test
-USA[XP]83- Are you a Fucker?. (ircd!ircd@127.0.0.1).
-USA[XP]83- No pass for you.
[11 00:56 @ircd (+i) on #challenge (+nt) * type /help for help
-
You should upgrade your virtual machine.
```

I found what could be the password by looking for strings of the unpacked file in ollydbg "gemp123". Trying this with .login, it appeared I got another reaction.

Although, I did not have time to further analyze this, I feel confident that full access could be gained into this botnet app. It appears that I am failing some sort of host authentication. It may be expecting my hostname to be in the w32.gen.us domain. One could probably build a local DNS server on the linux server to trick it into thinking that was the source domain via reverse lookup.

The code appeared to also attempt to access a website at ahleinaks.ru.

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 question was covered in the previous answer.

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 appear to be quite a few commands available in the code, I will not create an exhaustive list here, but many are shown in the previous bintext

screenshot from question 3.

The bot does seem to have the ability to both harvest information (keystrokes, payment site info, etc) from the local host, as well as DDOS and reconnaissance capabilities.

I was not able to successfully log into the botnet, and seem to be failing authentication with my hostname. A little more time with it would likely be enough to figure out what else is needed to do so.

I did also notice that the bot seems to have http capabilities. I did not investigate this, but it may have a HTTP server that allows it to accept commands outside of the IRC command and control.

Question 7

How would you classify this malware? Why?

I would classify this malware as a Trojan/Bot. The code does not appear to have a method to self replicate, which would require some sort of social engineering to allow it to be installed. This would likely classify it as a Trojan.

The malware also uses a command and control structure via IRC that would classify it as a bot. An infected PC would be under the control of the master, in which any one of many commands could be issued to the "bot".

Question 8

What do you think the purpose of this malware is?

I think that this software is designed for financial gain, as most bot code is. It appears that sensitive information can be gathered by the software, as well as DDOS attacks, etc could also be launched. These type of actions are all financially motivated and the master/controller would likely be quite profitable.

Bonus questions

Is it possible to find the malware's source code? If so, how did you do it?

I was able to find the sourcecode quite easily. After inspecting the strings in the unpacked file, I noticed that the malware was called "Crx Alias REalmbot – by Lindem" (possible author?)

A quick google search and I found the source at:

<http://rapidshare.com/files/101359254/BotNets.part1.rar>

I was able to download the code, and it appeared to be a similar version.