

Malware Quiz 7 Answers

Adam Loveless

adam.loveless@gmail.com

Question & Answer

1. Is the malware packed? If so, with which packer?

The malware file is packed. The packer used was Themida which is developed by Oreans Technology.

2. What is the purpose of the malware?

I believe the purpose of this malware to be a trojan horse that will turn the computer into a bot in a botnet controlled by a botherder.

3. Does it connect to a remote server? With which purpose?

Yes it does connect to a remote server. The remote server is london.uk.eu.undernet.org at an IP address of 195.68.221.221 on TCP port 6667, which is a common IRC port. The purpose of this connection is for the infected host to take commands from a botherder.

4. Which channels does it connect to?

The malware only connects to one channel on the london.uk.eu.undernet.org IRC server. The channel is #secretcow and it joins the #secretcow channel with a key (password) of werule.

5. Can you get any passwords related to this malware?

The only password that I can see this malware uses is the key (password) werule to join the channel of secretcow on the london.uk.eu.undernet.org IRC server.

6. Which capabilities does this malware have?

The full capabilities of this malware are unknown to me due to my inexperience at unpacking Themida packed programs. I would then have to generalize and say that once this bot connects up to a botnet, it can be used for various purposes, including denial-of-service attacks, creation of SMTP mail relays for spam, click fraud, and the theft of application serial numbers, login IDs, and financial information such as credit card numbers.

7. Bonus Question: What is the hidden message (if there is any...)?

I could not find any hidden message. I tried googling "secret cow" and "secret cow we rule" but nothing really stood out. The only mentioning of a "secret cow" was a hidden secret cow level to the video game Diablo 2.

Process

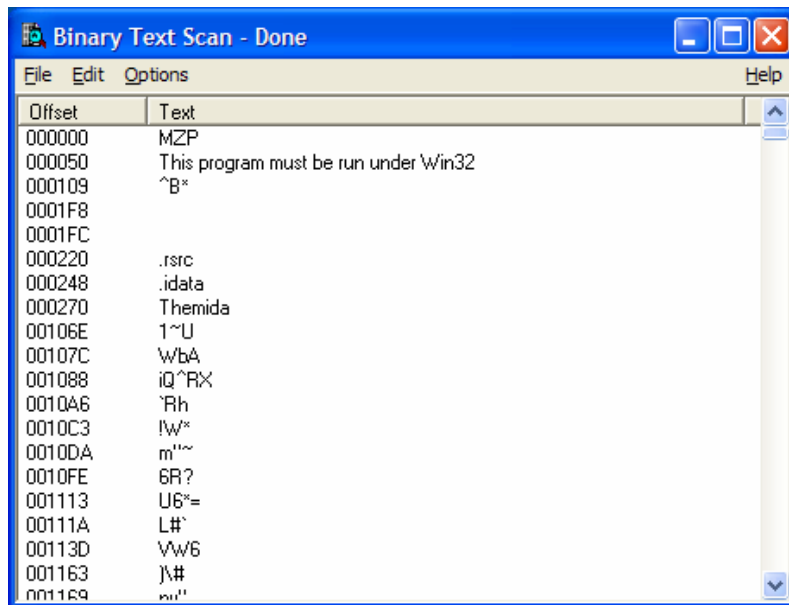
I ran the linux command “md5sum quizmal.zip” to verify that file had not been tampered with and was the actual file that I should have.

```
[root@localhost ~]# md5sum quizmal.zip
baf2c080af23a34ead140d3c891e3be5  quizmal.zip
[root@localhost ~]#
```

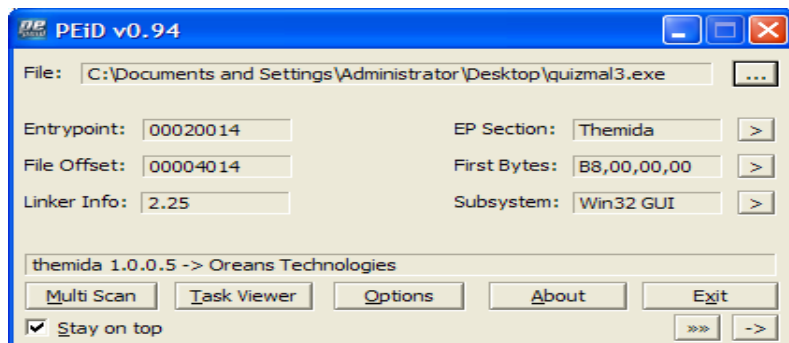
I attempted to identify the file type and packer that was used. I ran the linux command “file quizmal3.exe” to find out it was a regular 32-bit Windows PE file.

```
[root@localhost ~]# file quizmal3.exe
quizmal3.exe: PE executable for MS Windows (GUI) Intel 80386 32-bit
[root@localhost ~]# █
```

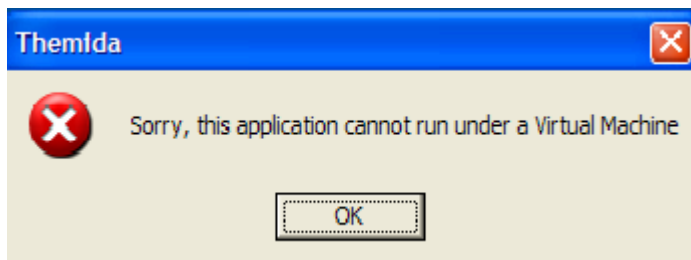
I opened the quizmal3.exe program in BinaryTextScan (<http://www.usa-pass.net/files/BinTxtScan.zip>) to see if the malware was packed and if so what software may have been used to pack it. The only string that stuck out was the Themida, so I googled it and find my way to the Oreans Technologies website (<http://www.oreans.com/themida.php>) and a product description of the Themida software.



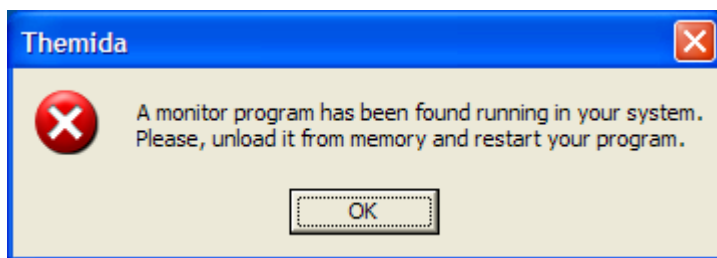
I later found the program PEiD 0.94 (<http://www.secretashell.com/codomain/peid/files/PEiD-0.94-20060510.zip>) which simplified this process immensely.



I fired up VMWare to test out the malware on a completely fresh install of Windows XP Pro and got a nice little message from the Themida software that the malware would not run in a virtual environment. I later found out there are ways to attempt to hide the virtual environment from Themida, but I did not take time to research and implement this (<http://isc.sans.org/diary.php?storyid=1871&rss>).



I had an older laptop laying around that I wiped and put a fresh install of Windows XP Pro on. I then fired up Filemon and Regmon from Sysinternals (These two tools have now been combined into a great utility called Process Monitor and I highly recommend it <http://www.microsoft.com/technet/sysinternals/processesandthreads/processmonitor.mspx>) and Wireshark (<http://www.wireshark.org/>) to monitor what the malware did when it was ran. I came up against another hurdle when I ran the malware. The Themida software detected that I had a monitoring software running and it gave me an error message.



It was detecting the Sysinternal tools and would not load if they were running, so I sat back for a few minutes and pondered what I could do. I then came to the realization of using malware against the malware. I downloaded the FU rootkit(https://www.rootkit.com/vault/fuzen_op/FU_Rootkit.zip) to hide both the Filemon and Regmon. I ran the FU rootkit with the following command line “fu -ph <process id #>” and then ran the malware. It worked this time and the malware went on its happy way doing its thing. At this point I have Filemon monitoring all the file access, Regmon to monitor the registry access, and Wireshark to monitor the network access. I ran TCPView to see what ports the malware had opened and found it had connected to london.uk.eu.undernet.org (195.68.221.221) on TCP port 6667 and was listening on TCP port 3812.

quizmal3.exe:3176	TCP	172.164:3812	195.68.221.221:6667	ESTABLISHED
quizmal3.exe:3176	TCP	0.0.0.0:3812	0.0.0.0	LISTENING

I let the malware run for a couple of hours before finally shutting it down. I took a look at the Filemon and Regmon logs and did not see anything that would really help with what the program was really doing while it was running. I jumped over to Wireshark and took a look. I found a wealth of information at this point. It starts with the malware doing a DNS request for london.uk.eu.undernet.org which comes back with an answer of 195.68.221.221. It then performs a logon process with the following IRC commands:

```
USER Hello3577161 Hello3577161@foo.bar Hello3577161 Hello3577161
NICK Hello3577161
PING :1257453883
PONG :1257453883
```

I looked up the IRC RFC to find out all the goodies about these commands. It is an interesting read and I recommend it (<ftp://ftp.rfc-editor.org/in-notes/pdf/rfc1459.txt.pdf>). The meanings of the commands are:

Command: USER

Parameters: <username> <hostname> <servername> <realname>

The USER message is used at the beginning of connection to specify the username, hostname, servername and realname of s new user.

Command: NICK

Parameters: <nickname> [<hopcount>]

NICK message is used to give user a nickname or change the previous one.

Command: PING

Parameters: <server1> [<server2>]

The PING message is used to test the presence of an active client at the other end of the connection.

Command: PONG

Parameters: <daemon> [<daemon2>]

PONG message is a reply to ping message.

It appeared to me that the malware creates the username with Hello always at the beginning and then a random 7 digit number. After these 4 previous commands are done the logon process is complete. The malware will then issue this command:

```
JOIN #secretcow werule
```

The meaning of this command is:

Command: JOIN

Parameters: <channel>{,<channel>} [<key>{,<key>}]

The JOIN command is used by client to start listening a specific channel.

With IRC a channel name must always have a prefix of # and then the channel name. I thought at first that the malware might be joining two channels, but upon further reading in the RFC, if it was to join two channels then the command would have looked like this:

```
JOIN #secretcow,#werule
```

Therefore the werule part has to be a key, which is basically a password that is needed to join the specified channel. After it has joined the channel it does nothing. For the multiple hours of Wireshark packet captures I had only two commands that kept going after the channel join and this was an exchange of PING/PONG commands that I believe was used to keep the connection alive.

Next, I went to the VirusTotal website and had it analyze the malware.

Antivirus	Version	Update	Result
AntiVir	7.2.0.46	11.30.2006	Worm/IRCBot.1167360
Authentium	4.93.8	11.30.2006	W32/Backdoor.RSS
Avast	4.7.892.0	11.30.2006	Win32/Ircbot-ADY
AVG	386	11.30.2006	BackDoor.Generic3.SXH
BitDefender	7.2	11.30.2006	Backdoor.IRCBot.XS
CAT-QuickHeal	8.00	11.30.2006	Backdoor.IRCBot.xs
ClamAV	devel-20060426	11.30.2006	no virus found
DrWeb	4.33	11.30.2006	no virus found
eSafe	7.0.14.0	11.30.2006	no virus found
eTrust-InoculateIT	23.73.72	11.29.2006	Win32/SdBot.1ny!Trojan
eTrust-Vet	30.3.3223	11.30.2006	Win32/IRCBot.AO
Ewido	4.0	11.30.2006	Backdoor.IRCBot.xs
Fortinet	2.82.0.0	11.30.2006	W32/IRCBot.XS!tr.bdr
F-Prot	3.16f	11.30.2006	security risk named W32/Backdoor.RSS
F-Prot4	4.2.1.29	11.30.2006	W32/Backdoor.RSS
Ikarus	0.2.65.0	11.30.2006	no virus found
Kaspersky	4.0.2.24	11.30.2006	Backdoor.Win32.IRCBot.xs
McAfee	4908	11.30.2006	Generic.IRC.b
Microsoft	1.1804	11.30.2006	no virus found
NOD32v2	1892	11.30.2006	no virus found
Norman	5.80.02	11.30.2006	W32/Ircbot.CXA
Panda	9.0.0.4	11.30.2006	Bck/IRCBot.AHM
Prevx1	V2	11.30.2006	no virus found
Sophos	4.11.0	11.16.2006	Troj/IRCBot-SN
TheHacker	6.0.3.126	11.29.2006	Backdoor/IRCBot.xs
UNA	1.83	11.30.2006	Backdoor.IRCBot.13D0
VBA32	3.11.1	11.30.2006	Backdoor.Win32.IRCBot.xs
VirusBuster	4.3.15.9	11.30.2006	Backdoor.IRCBot.AIN

Additional Information
File size: 1167360 bytes
MD5: 0005802d5a3c20262249b802a3c0aeda
SHA1: 97293be82f783e001ba85b992b1531bd98d86520

These results just verify what I was already thinking before I ran it. This malware is a trojan horse software that will turn your computer into a bot, which will be part of a botnet, and will be controlled by a botherder. The IRC connection will allow the botherder to do almost anything with your machine and the whole botnet. They can send/receive files, create/delete files, execute programs, steal your personal information, use your machine as part of a denial-of-service attack, turn your machine into a SMTP server and have it pump out spam emails, steal your userids and passwords, and many other things.

This has been an extremely fun and I enjoyed learning as much as I did. I would like to thank Pedro Bueno for the great idea of having this malware quizzes.