Malware Analysis
Homework 4

Raghu Pusapati

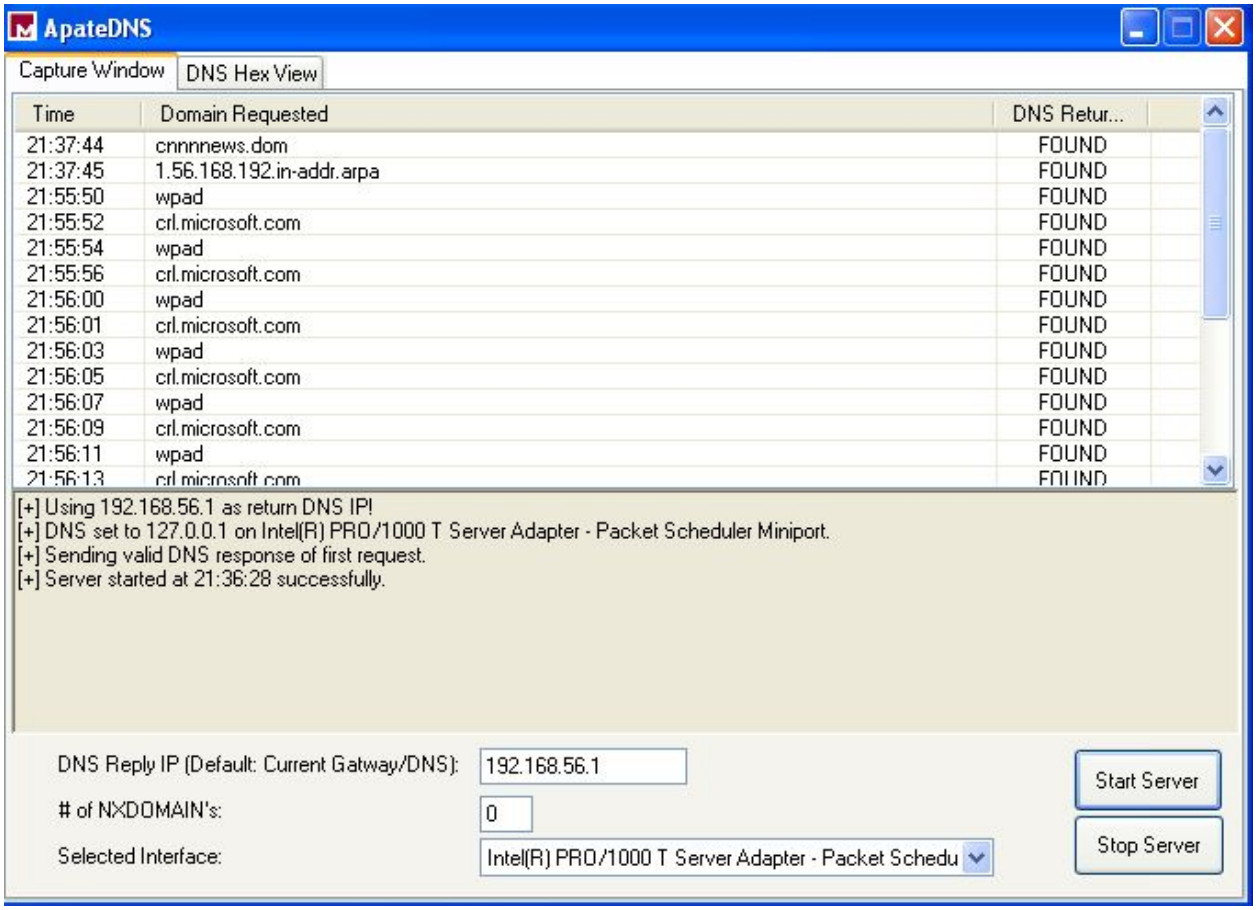
pusaparv@mail.uc.edu

Environment setup:
Host machine - Arch Linux
Guest machine - Windows XP mode
Tools used - Procmon, Procexp, Regshot, ApateDNS, Wireshark

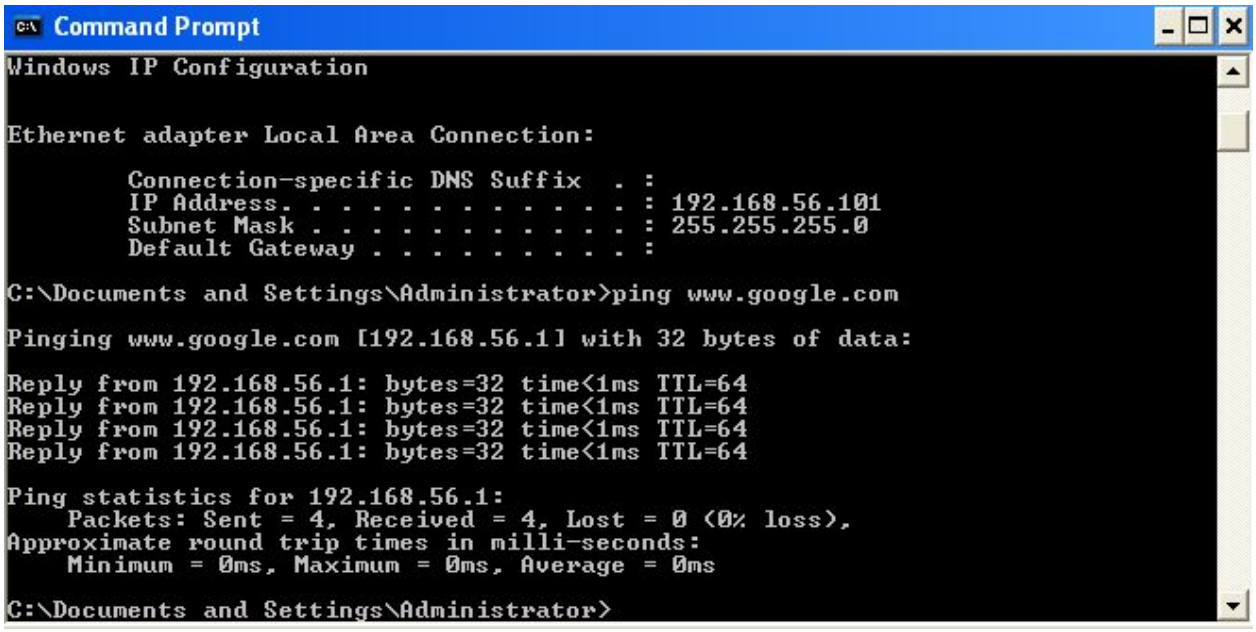
IP addresses:
Arch Linux - 192.168.56.1
Windows - 192.168.56.101

Steps taken before running the malware:

1. Started up ApateDNS and configured the DNS reply IP to 192.168.56.1



All the DNS requests will be redirected and replied with IP 192.168.56.1, tricking the malware into thinking there is internet connection.

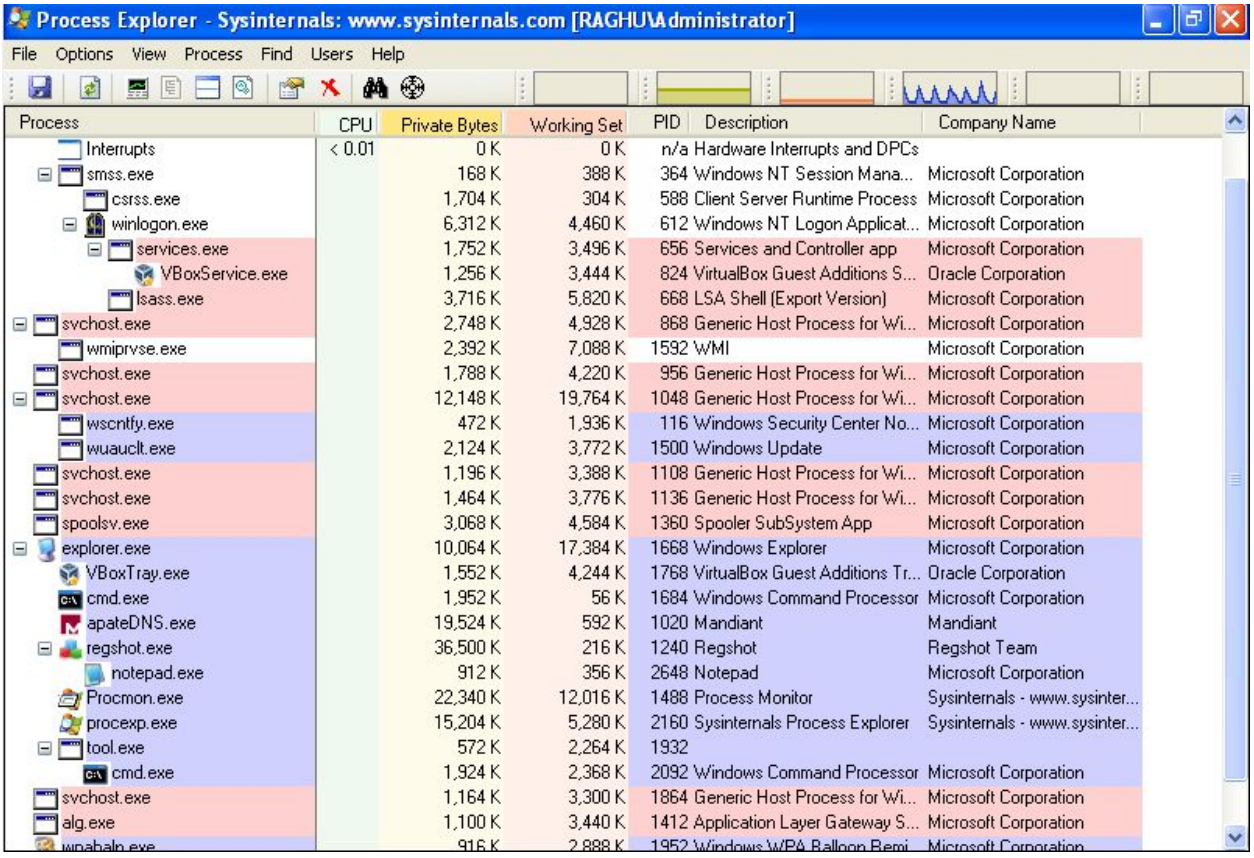


2. Start procmon with filter, process name is tool.exe
3. Start procexp

4. Start wireshark on Arch Linux and capture virtualbox network
5. Start the bdconsole.py on Arch Linux
6. Take a snapshot registry using regshot

Running and analysing the malware:

The malware is now ready to be run. The process was started and I could see it in the procexp.

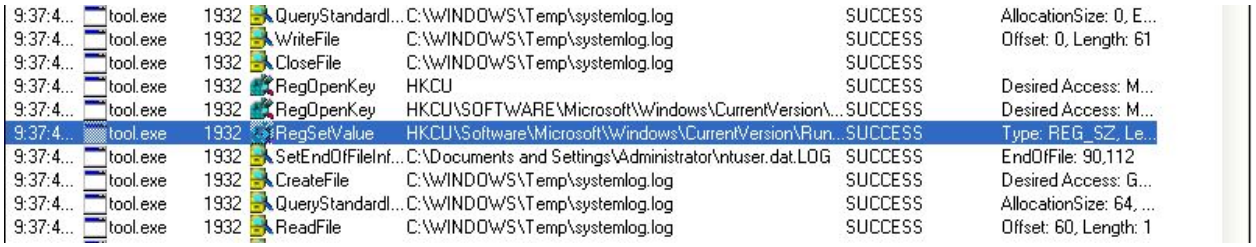


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		168 K	388 K	364	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,704 K	304 K	588	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,312 K	4,460 K	612	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,752 K	3,496 K	656	Services and Controller app	Microsoft Corporation
VBoxService.exe		1,256 K	3,444 K	824	VirtualBox Guest Additions S...	Oracle Corporation
lsass.exe		3,716 K	5,820 K	668	LSA Shell (Export Version)	Microsoft Corporation
svchost.exe		2,748 K	4,928 K	868	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe		2,392 K	7,088 K	1592	WMI	Microsoft Corporation
svchost.exe		1,788 K	4,220 K	956	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		12,148 K	19,764 K	1048	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		472 K	1,936 K	116	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		2,124 K	3,772 K	1500	Windows Update	Microsoft Corporation
svchost.exe		1,196 K	3,388 K	1108	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,464 K	3,776 K	1136	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		3,068 K	4,584 K	1360	Spooler SubSystem App	Microsoft Corporation
explorer.exe		10,064 K	17,384 K	1668	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,552 K	4,244 K	1768	VirtualBox Guest Additions Tr...	Oracle Corporation
cmd.exe		1,952 K	56 K	1684	Windows Command Processor	Microsoft Corporation
apateDNS.exe		19,524 K	592 K	1020	Mandiant	Mandiant
regshot.exe		36,500 K	216 K	1240	Regshot	Regshot Team
notepad.exe		912 K	356 K	2648	Notepad	Microsoft Corporation
Procmon.exe		22,340 K	12,016 K	1488	Process Monitor	Sysinternals - www.sysinter...
procexp.exe		15,204 K	5,280 K	2160	Sysinternals Process Explorer	Sysinternals - www.sysinter...
tool.exe		572 K	2,264 K	1932		
cmd.exe		1,924 K	2,368 K	2092	Windows Command Processor	Microsoft Corporation
svchost.exe		1,164 K	3,300 K	1864	Generic Host Process for Wi...	Microsoft Corporation
alg.exe		1,100 K	3,440 K	1412	Application Layer Gateway S...	Microsoft Corporation
wpabaln.exe		916 K	2,888 K	1952	Windows WPA Balloon Remi...	Microsoft Corporation

Behavior:

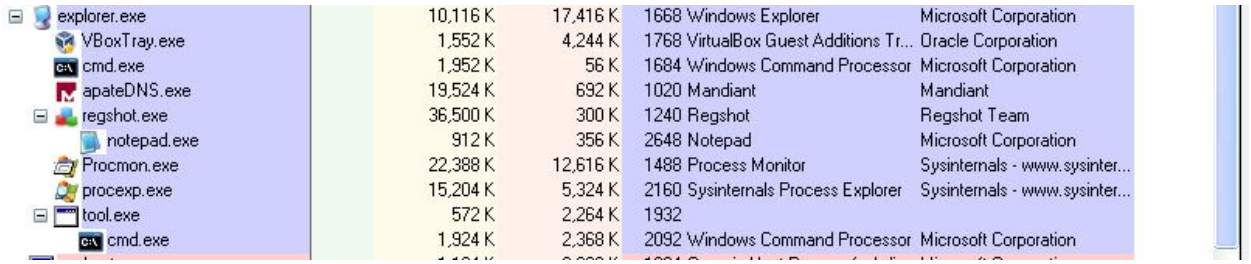
1. Modify startup registry

The malware has modified startup registry to make sure it get executed every time a user logs in or when the system boots up.



9:37:4...	tool.exe	1932	QueryStandardI...	C:\WINDOWS\Temp\systemlog.log	SUCCESS	AllocationSize: 0, E...
9:37:4...	tool.exe	1932	WriteFile	C:\WINDOWS\Temp\systemlog.log	SUCCESS	Offset: 0, Length: 61
9:37:4...	tool.exe	1932	CloseFile	C:\WINDOWS\Temp\systemlog.log	SUCCESS	
9:37:4...	tool.exe	1932	RegOpenKey	HKCU	SUCCESS	Desired Access: M...
9:37:4...	tool.exe	1932	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\...	SUCCESS	Desired Access: M...
9:37:4...	tool.exe	1932	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run...	SUCCESS	Type: REG_SZ, Le...
9:37:4...	tool.exe	1932	SetEndOfFileInf...	C:\Documents and Settings\Administrator\ntuser.dat.LOG	SUCCESS	EndOfFile: 90,112
9:37:4...	tool.exe	1932	CreateFile	C:\WINDOWS\Temp\systemlog.log	SUCCESS	Desired Access: G...
9:37:4...	tool.exe	1932	QueryStandardI...	C:\WINDOWS\Temp\systemlog.log	SUCCESS	AllocationSize: 64, ...
9:37:4...	tool.exe	1932	ReadFile	C:\WINDOWS\Temp\systemlog.log	SUCCESS	Offset: 60, Length: 1

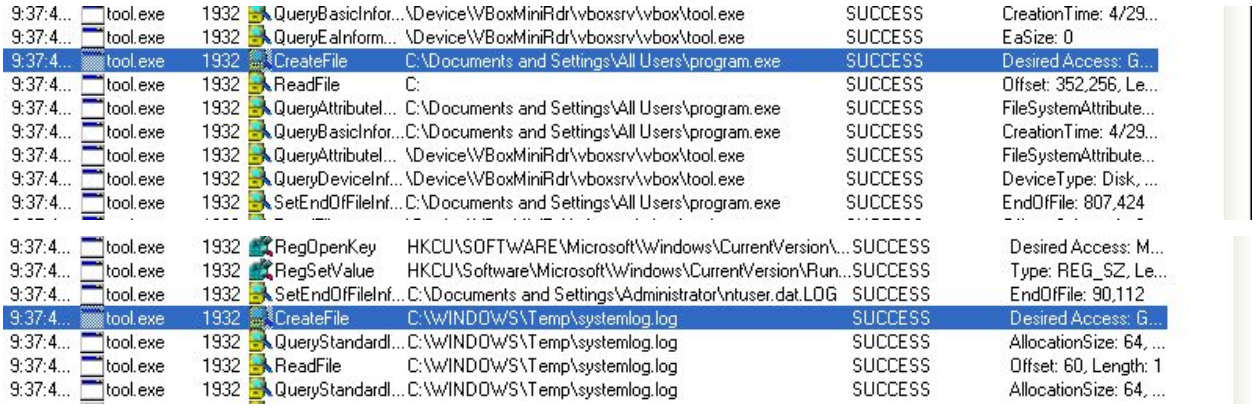
2. Spawn a cmd.exe process



explorer.exe	10,116 K	17,416 K	1668 Windows Explorer	Microsoft Corporation
VBoxTray.exe	1,552 K	4,244 K	1768 VirtualBox Guest Additions Tr...	Oracle Corporation
cmd.exe	1,952 K	56 K	1684 Windows Command Processor	Microsoft Corporation
apateDNS.exe	19,524 K	692 K	1020 Mandiant	Mandiant
regshot.exe	36,500 K	300 K	1240 Regshot	Regshot Team
notepad.exe	912 K	356 K	2648 Notepad	Microsoft Corporation
Procmon.exe	22,388 K	12,616 K	1488 Process Monitor	Sysinternals - www.sysinter...
procexp.exe	15,204 K	5,324 K	2160 Sysinternals Process Explorer	Sysinternals - www.sysinter...
tool.exe	572 K	2,264 K	1932	
cmd.exe	1,924 K	2,368 K	2092 Windows Command Processor	Microsoft Corporation

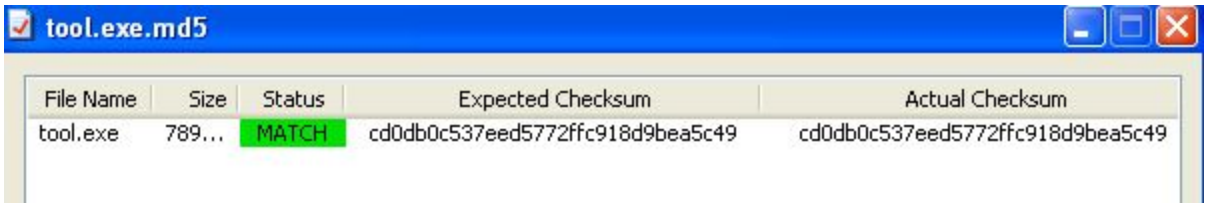
We can see under tool.exe, there is a cmd.exe process. This terminal is however not visible to us.

3. Created files - program.exe and systemlog.log



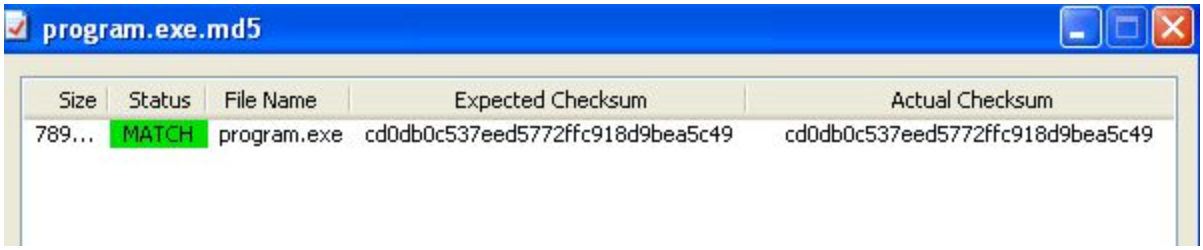
9:37:4...	tool.exe	1932	QueryBasicInfor...	\Device\VBoxMiniRdr\vboxsrv\vbox\tool.exe	SUCCESS	CreationTime: 4/29...
9:37:4...	tool.exe	1932	QueryEaInform...	\Device\VBoxMiniRdr\vboxsrv\vbox\tool.exe	SUCCESS	EaSize: 0
9:37:4...	tool.exe	1932	CreateFile	C:\Documents and Settings\All Users\program.exe	SUCCESS	Desired Access: G...
9:37:4...	tool.exe	1932	ReadFile	C:	SUCCESS	Offset: 352,256, Le...
9:37:4...	tool.exe	1932	QueryAttributeI...	C:\Documents and Settings\All Users\program.exe	SUCCESS	FileSystemAttribute...
9:37:4...	tool.exe	1932	QueryBasicInfor...	C:\Documents and Settings\All Users\program.exe	SUCCESS	CreationTime: 4/29...
9:37:4...	tool.exe	1932	QueryAttributeI...	\Device\VBoxMiniRdr\vboxsrv\vbox\tool.exe	SUCCESS	FileSystemAttribute...
9:37:4...	tool.exe	1932	QueryDeviceInf...	\Device\VBoxMiniRdr\vboxsrv\vbox\tool.exe	SUCCESS	DeviceType: Disk, ...
9:37:4...	tool.exe	1932	SetEndOfFileInf...	C:\Documents and Settings\All Users\program.exe	SUCCESS	EndOfFile: 807,424
9:37:4...	tool.exe	1932	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\...	SUCCESS	Desired Access: M...
9:37:4...	tool.exe	1932	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run...	SUCCESS	Type: REG_SZ, Le...
9:37:4...	tool.exe	1932	SetEndOfFileInf...	C:\Documents and Settings\Administrator\ntuser.dat.LOG	SUCCESS	EndOfFile: 90,112
9:37:4...	tool.exe	1932	CreateFile	C:\WINDOWS\Temp\systemlog.log	SUCCESS	Desired Access: G...
9:37:4...	tool.exe	1932	QueryStandardI...	C:\WINDOWS\Temp\systemlog.log	SUCCESS	AllocationSize: 64, ...
9:37:4...	tool.exe	1932	ReadFile	C:\WINDOWS\Temp\systemlog.log	SUCCESS	Offset: 60, Length: 1
9:37:4...	tool.exe	1932	QueryStandardI...	C:\WINDOWS\Temp\systemlog.log	SUCCESS	AllocationSize: 64, ...

I have checked the md5 sum of both the tool.exe and program.exe files and they turn out to be the same files.



tool.exe.md5

File Name	Size	Status	Expected Checksum	Actual Checksum
tool.exe	789...	MATCH	cd0db0c537eed5772ffc918d9bea5c49	cd0db0c537eed5772ffc918d9bea5c49

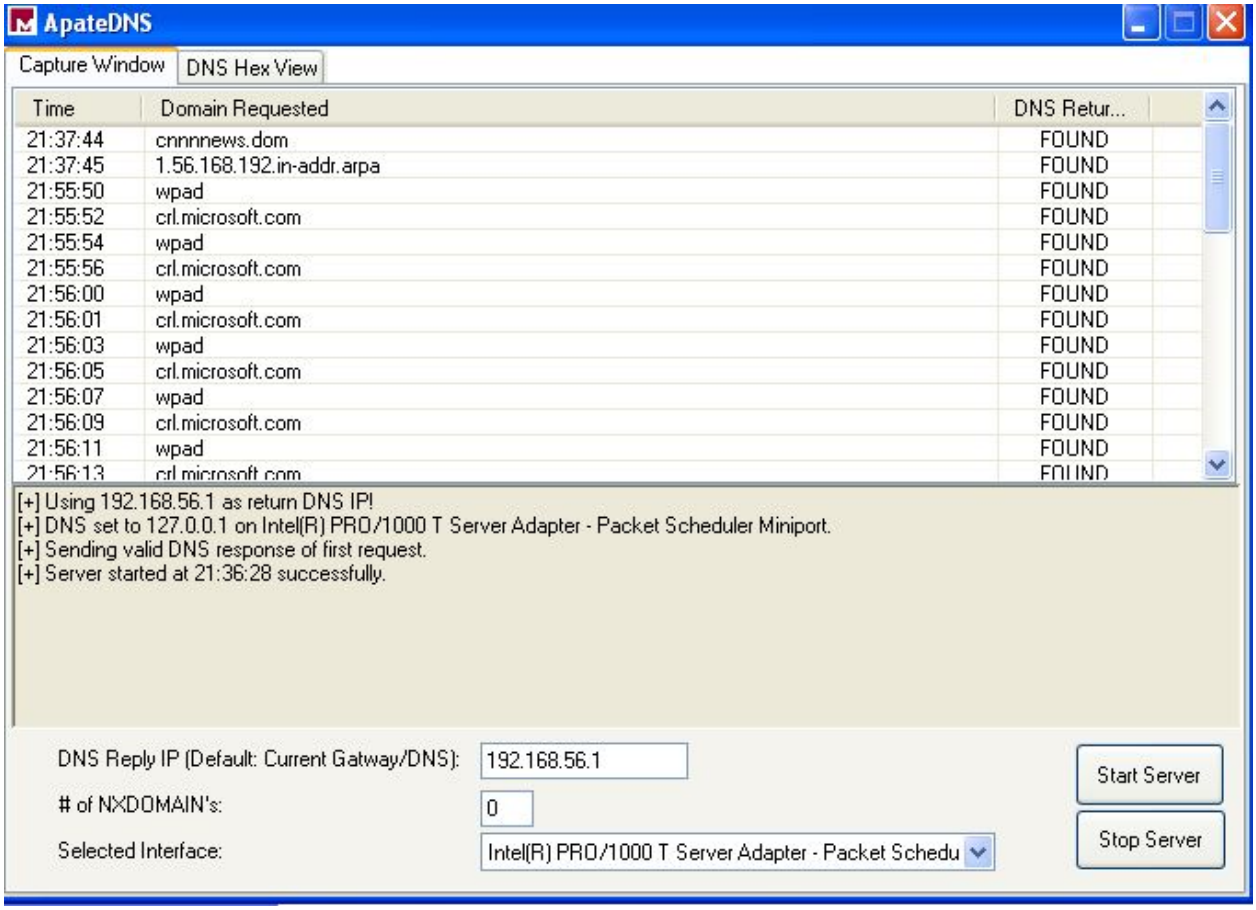


program.exe.md5

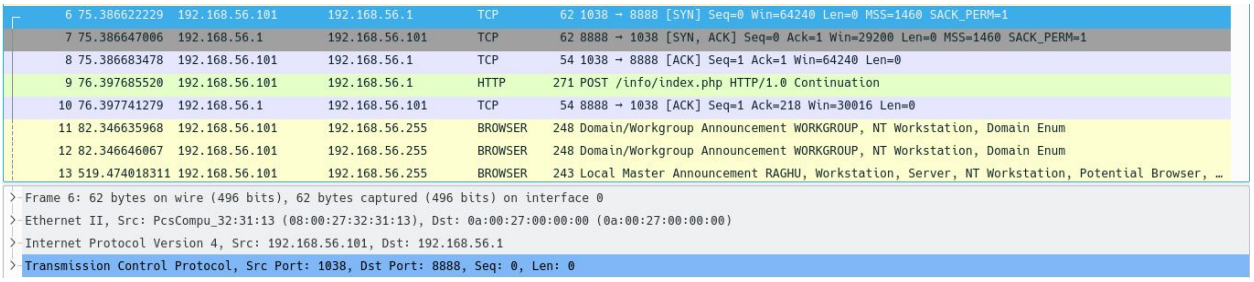
Size	Status	File Name	Expected Checksum	Actual Checksum
789...	MATCH	program.exe	cd0db0c537eed5772ffc918d9bea5c49	cd0db0c537eed5772ffc918d9bea5c49

4. Network usage

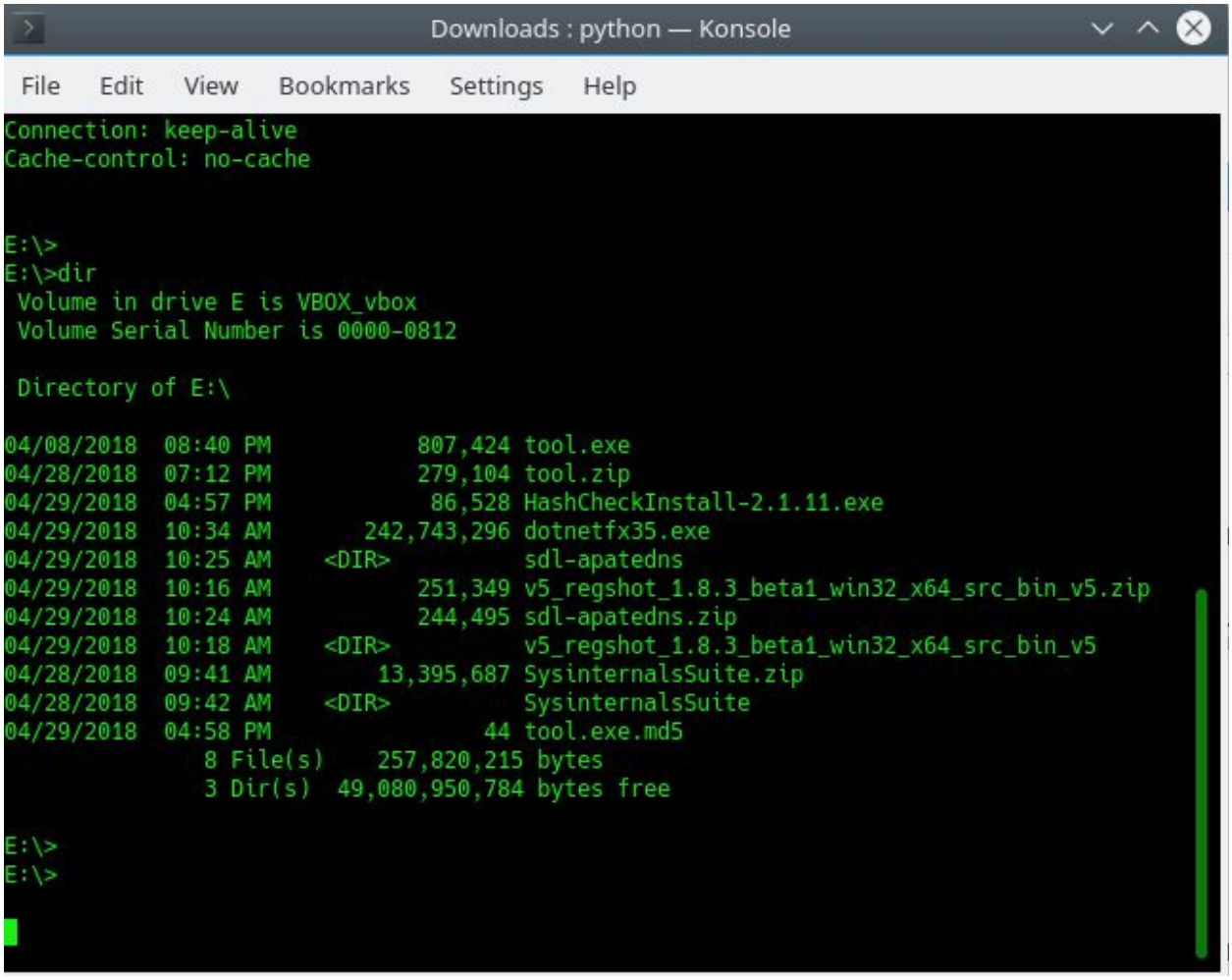
The malware tried to connect to cnnnnews.dom ApateDNS redirected the traffic to 192.168.56.1



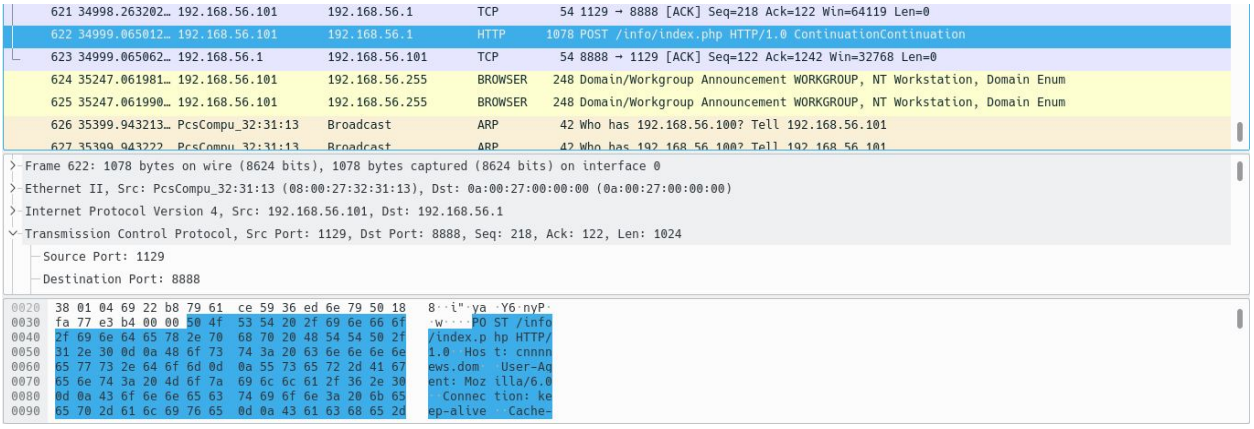
The malware has used port number 1038 to communicate with the c2 server.



The cmd.exe that the malware spawned isn't visible but the session that it opened is accessible through bdconsole.py program. The malware has given access to the folder in which it resides.



The protocol it used to communicate is HTTP. I restarted tool.exe and found that it has changed the source port from 1038 to 1129. Malware is using different source port everytime.



The network traffic looks like a series of HTTP requests and responses.
When I terminated bdconsole, an error popped up in the windows machine.

This could raise suspicion to users.