

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

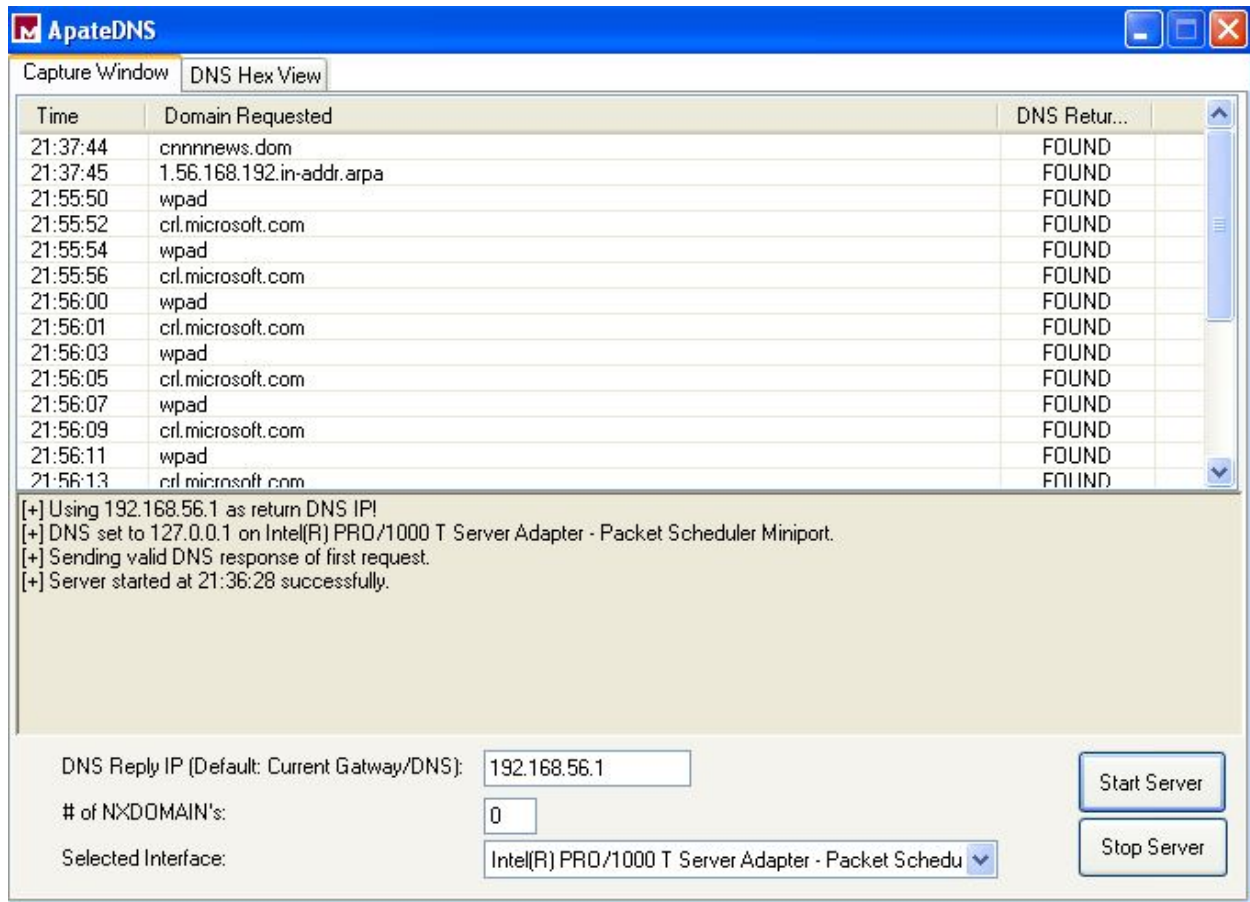
IP addresses:

Arch Linux - 192.168.56.1

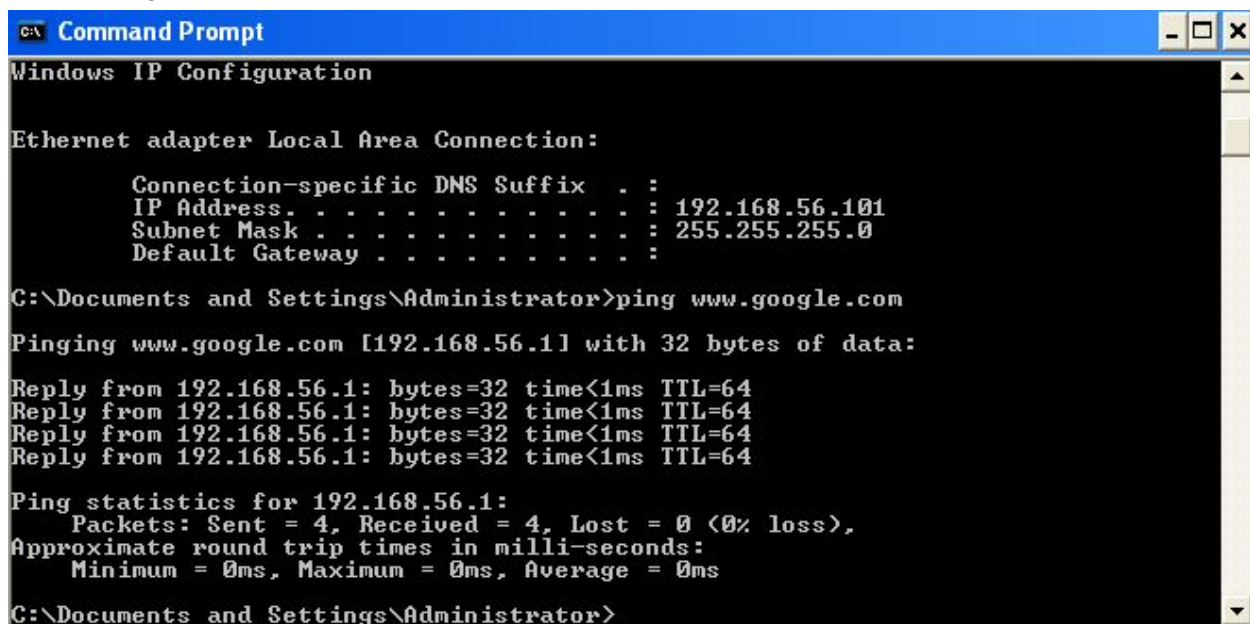
Windows - 192.168.56.101

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
mspateDNS.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
wpaabalp.exe		916 K	2,888 K	1952	Windows WPA Balloon Bemi...	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	QueryStandardl...	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	QueryStandardl...	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\WBoxMiniRd\vbosrv\vbos\tool.exe	SUCCESS	CreationTime: 4/29...
9:37:4...	tool.exe	1932	QueryEaInfor...	\Device\WBoxMiniRd\vbosrv\vbos\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	QueryAttribut...	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	QueryAttribut...	\Device\WBoxMiniRd\vbosrv\vbos\tool.exe	SUCCESS	FileSystemAttribute...
9:37:4...	tool.exe	1932	QueryDeviceInf...	\Device\WBoxMiniRd\vbosrv\vbos\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	QueryStandardl...	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	QueryStandardl...	C:\WINDOWS\Temp\systemlog.log	SUCCESS	AllocationSize: 64, ...

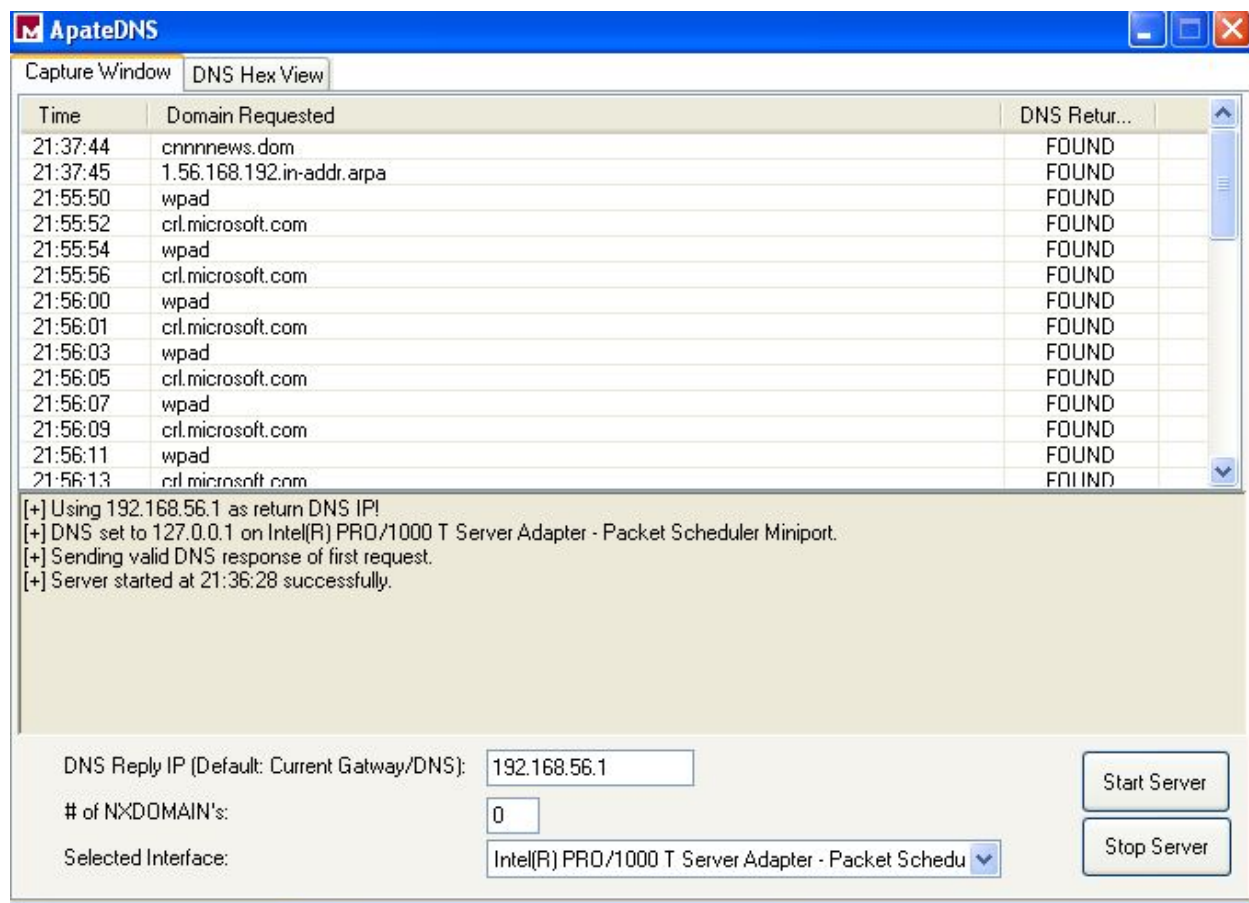
I have checked the md5 sum of both the tool.exe and program.exe files and they turn out to be the same files.

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 cnnnnnews.dom ApateDNS redirected the traffic to 192.168.56.1



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

6	75.386622229	192.168.56.101	192.168.56.1	TCP	62	1038 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
7	75.386647006	192.168.56.1	192.168.56.101	TCP	62	8888 → 1038 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
8	75.386683478	192.168.56.101	192.168.56.1	TCP	54	1038 → 8888 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9	76.397685520	192.168.56.101	192.168.56.1	HTTP	271	POST /info/index.php HTTP/1.0 Continuation
10	76.397741279	192.168.56.1	192.168.56.101	TCP	54	8888 → 1038 [ACK] Seq=1 Ack=218 Win=30016 Len=0
11	82.346635968	192.168.56.101	192.168.56.255	BROWSER	248	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
12	82.346646067	192.168.56.101	192.168.56.255	BROWSER	248	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
13	519.474018311	192.168.56.101	192.168.56.255	BROWSER	243	Local Master Announcement RAGHU, Workstation, Server, NT Workstation, Potential Browser, ...

> Frame 6: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
 > Ethernet II, Src: PcsCompu_32:31:13 (08:00:27:32:31:13), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
 > Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.1
 > Transmission Control Protocol, Src Port: 1038, Dst Port: 8888, Seq: 0, Len: 0

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.

```
Downloads : python — Konsole
File Edit View Bookmarks Settings Help

Connection: keep-alive
Cache-control: no-cache

E:\>
E:\>dir
Volume in drive E is VBOX_vbox
Volume Serial Number is 0000-0812

Directory of E:\

04/08/2018  08:40 PM                807,424 tool.exe
04/28/2018  07:12 PM                279,104 tool.zip
04/29/2018  04:57 PM                86,528 HashCheckInstall-2.1.11.exe
04/29/2018  10:34 AM            242,743,296 dotnetfx35.exe
04/29/2018  10:25 AM            <DIR>          sdl-apatedns
04/29/2018  10:16 AM            251,349 v5_regshot_1.8.3_beta1_win32_x64_src_bin_v5.zip
04/29/2018  10:24 AM            244,495 sdl-apatedns.zip
04/29/2018  10:18 AM            <DIR>          v5_regshot_1.8.3_beta1_win32_x64_src_bin_v5
04/28/2018  09:41 AM           13,395,687 SysinternalsSuite.zip
04/28/2018  09:42 AM            <DIR>          SysinternalsSuite
04/29/2018  04:58 PM                44 tool.exe.md5
                8 File(s)  257,820,215 bytes
                3 Dir(s)  49,080,950,784 bytes free

E:\>
E:\>
```

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.

621	34998.263202...	192.168.56.101	192.168.56.1	TCP	54 1129 → 8888 [ACK] Seq=218 Ack=122 Win=64119 Len=0
622	34999.065012...	192.168.56.101	192.168.56.1	HTTP	1078 POST /info/index.php HTTP/1.0 ContinuationContinuation
623	34999.065062...	192.168.56.1	192.168.56.101	TCP	54 8888 → 1129 [ACK] Seq=122 Ack=1242 Win=32768 Len=0
624	35247.061981...	192.168.56.101	192.168.56.255	BROWSER	248 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
625	35247.061990...	192.168.56.101	192.168.56.255	BROWSER	248 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
626	35399.943213...	PcsCompu_32:31:13	Broadcast	ARP	42 Who has 192.168.56.100? Tell 192.168.56.101
627	35399.943222...	PcsCompu_32:31:13	Broadcast	ARP	42 Who has 192.168.56.100? Tell 192.168.56.101

> Frame 622: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits) on interface 0

> Ethernet II, Src: PcsCompu_32:31:13 (08:00:27:00:00:00), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)

> Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 1129, Dst Port: 8888, Seq: 218, Ack: 122, Len: 1024

Source Port: 1129

Destination Port: 8888

0020	38 01 04 69 22 b8 79 61 ce 59 36 ed 6e 79 50 18	8-i*va-Y6 nYP-
0030	fa 77 e3 b4 00 00 60 4f 53 54 20 2f 09 6e 66 6f	w... NO ST /info
0040	2f 69 66 64 65 78 2e 70 68 70 20 48 54 54 50 2f	/index.p hp HTTP/
0050	31 2e 30 0d 0a 48 6f 73 74 3a 20 63 6e 6e 6e 6e	1.0 Hos t: cnnnn
0060	65 77 73 2e 64 6f 6d 0d 0a 55 73 65 72 2d 41 67	ews.dom User-Aq
0070	65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 36 2e 30	ent: Moz illa/6.0
0080	0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65	Connec tion: ke
0090	65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d	ep-alive Cache-

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.