

MRUPrac.exe

Chandra Kant Bauri

Static Analysis Findings

- SHA256 Hash

07f9bb352f46a7b0b99a3768f0ec4518a5d3627862215c1a1a40ab9ce655b1ac

- Interesting Strings

```
DecodePointer
InternetConnection
https://www.byp4ssm3.lol/haha/
Error
Failed to create file.
THALA FOR A REASON
Software\Microsoft\Windows\CurrentVersion\Run
M-a-l-w-a-r-e
Error
Failed Registry.
magic Started
Error
Failed to download image.
Error
Failed wallpaper.
Error
No Internet Found. Exiting.
Error
Anti-VM Triggered. Exiting.
d21pYyBvcyBnZXQgY2FwdGlvg==
Error
Failed to decode command.
https://pbs.twimg.com/media/F1FbAD9XoAAxLkM.jpg
C:\Public
C:\Public\wallpaper.jpg
QGVjaG8gIkhlbGxvLCB3b3JsZCEi
C:\CheemTapakDumDum.bat
Error
Failed to decode script.
Operations completed successfully!
```

- Packed/Unpacked

c:\users\kant\Desktop\mruprac.exe		property	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	.reloc	
name	.text	.rdata	.data			
footprint > sha256	530CEFC691DB961D867EF53...	1EF8D696BB8E7326BF700AA...	D31E2348416408EE9BBE9233...	AEDEB50A2D6510C1BD1C30...		
entropy	6.558	4.820	3.159	6.197		
file-ratio (98.91%)	64.13 %	26.63 %	3.26 %	4.89 %		
raw-address (begin)	0x00000400	0x0000F000	0x00015200	0x00015E00	0x00015E00	
raw-address (end)	0x0000F000	0x00015200	0x00015E00	0x00017000	0x00017000	
raw-size (93184 bytes)	0x0000E000 (60416 bytes)	0x00006200 (25088 bytes)	0x0000C000 (3072 bytes)	0x0001200 (4608 bytes)		
virtual-address	0x00001000	0x00010000	0x00017000	0x00019000		
virtual-size (94960 bytes)	0x0000EB4E (60238 bytes)	0x0000618E (24974 bytes)	0x00001610 (5648 bytes)	0x00001004 (4100 bytes)		
characteristics	0x60000020	0x40000040	0xC0000040	0x42000040		
write	-	-	x	-		
execute	x	-	-	-		
share	-	-	-	-		
self-modifying	-	-	-	-		
virtual	-	-	-	-		

Entropy is 6.5 and the .text section is present so the malware is not likely packed.

- Any other finding

No Internet Found. Exiting.

Anti-VM Triggered. Exiting.

d21pYyBvcyBnZXQgY2FwdGlvbg==

Failed to decode command.

<https://pbs.twimg.com/media/F1FbAD9XoAAxLkM.jpg>

C:\Public

C:\Public\wallpaper.jpg

QGVjaG8glkhlbGxvLCB3b3JsZCEi

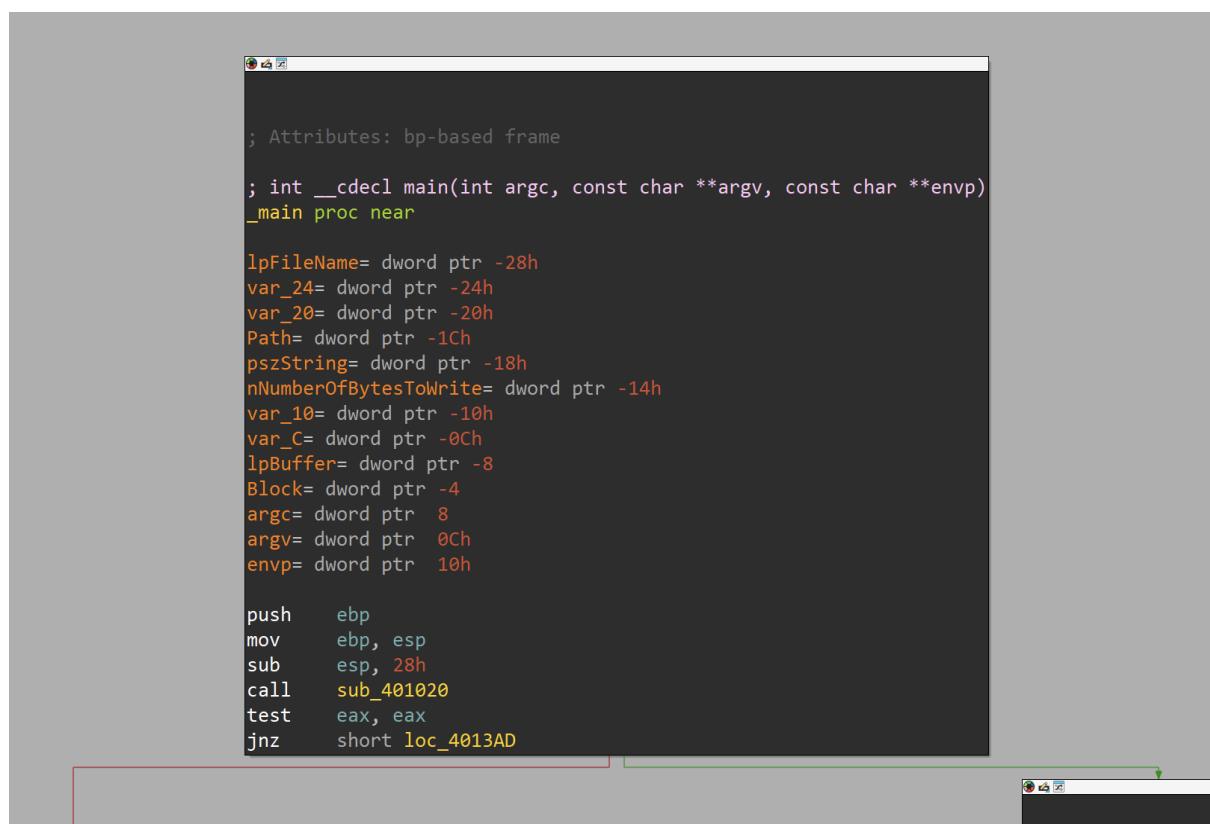
C:\CheemTapakDumDum.bat

Failed to decode script.

Operations completed successfully!

Dynamic Analysis Findings

Main Function



The screenshot shows a debugger window displaying assembly code for the main function. The code is annotated with variable names and their memory addresses:

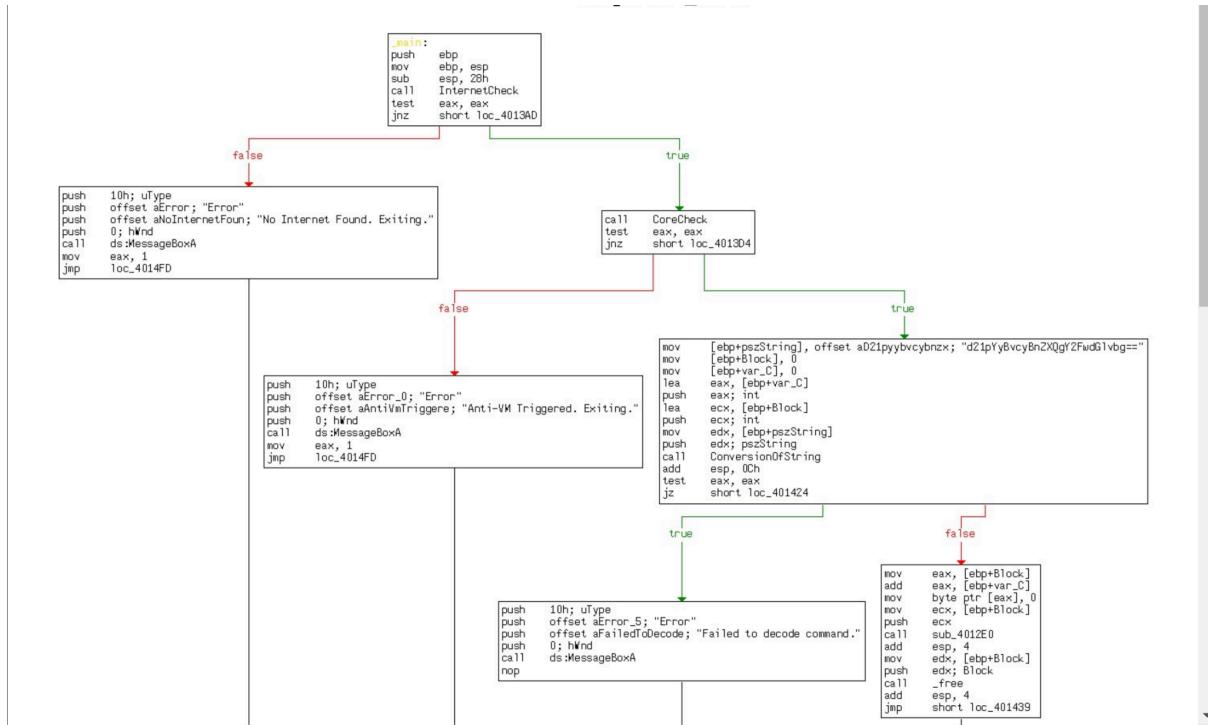
```
; Attributes: bp-based frame
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

lpFileName= dword ptr -28h
var_24= dword ptr -24h
var_20= dword ptr -20h
Path= dword ptr -1Ch
pszString= dword ptr -18h
nNumberOfBytesToWrite= dword ptr -14h
var_10= dword ptr -10h
var_C= dword ptr -0Ch
lpBuffer= dword ptr -8
Block= dword ptr -4
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h

push    ebp
mov     ebp, esp
sub     esp, 28h
call    sub_401020
test   eax, eax
jnz    short loc_4013AD
```

Code Analysis Findings

Execution flow



Anti vm techniques

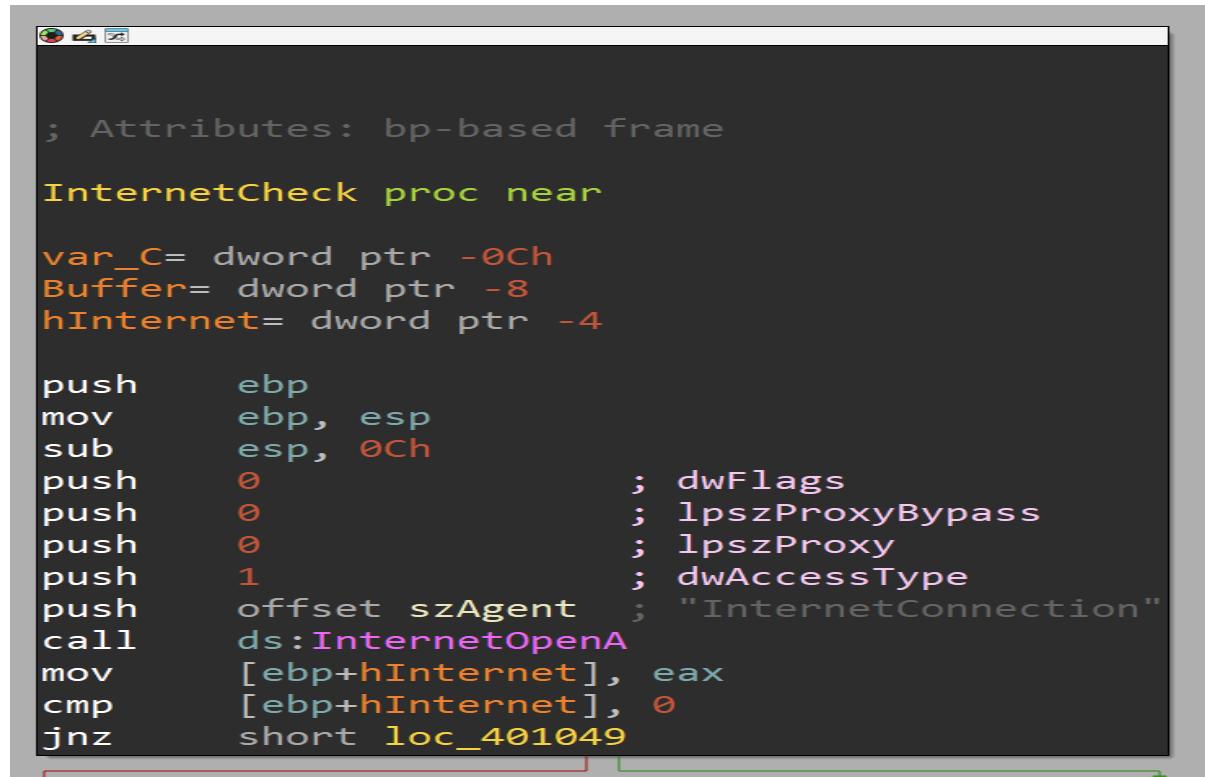
```

loc_4014D2: ; uType
push 10h
push offset aError_6 : "Err"
push offset aFailedToDecode
push 0 ; hWnd
call ds:MessageBoxA
nop

loc_4014E7: ; uType
push 40h ; '@'
push offset aInfo ; "Info"
push offset aOperationsComp ; "Operations completed successfully!"
push 0 ; hWnd
call ds:MessageBoxA
xor eax, eax

```

Sample is checking no. of cores, internet connection



The screenshot shows a debugger window displaying assembly code. The code is annotated with comments explaining the parameters and purpose of each instruction. A red rectangle highlights the 'call' instruction, and a green rectangle highlights the 'cmp' instruction.

```
; Attributes: bp-based frame

InternetCheck proc near

var_C= dword ptr -0Ch
Buffer= dword ptr -8
hInternet= dword ptr -4

push    ebp
mov     ebp, esp
sub    esp, 0Ch
push    0          ; dwFlags
push    0          ; lpszProxyBypass
push    0          ; lpszProxy
push    1          ; dwAccessType
push    offset szAgent ; "InternetConnection"
call    ds:InternetOpenA
mov     [ebp+hInternet], eax
cmp     [ebp+hInternet], 0
jnz    short loc_401049
```

Core check

```
; Attributes: bp-based frame

CoreCheck proc near

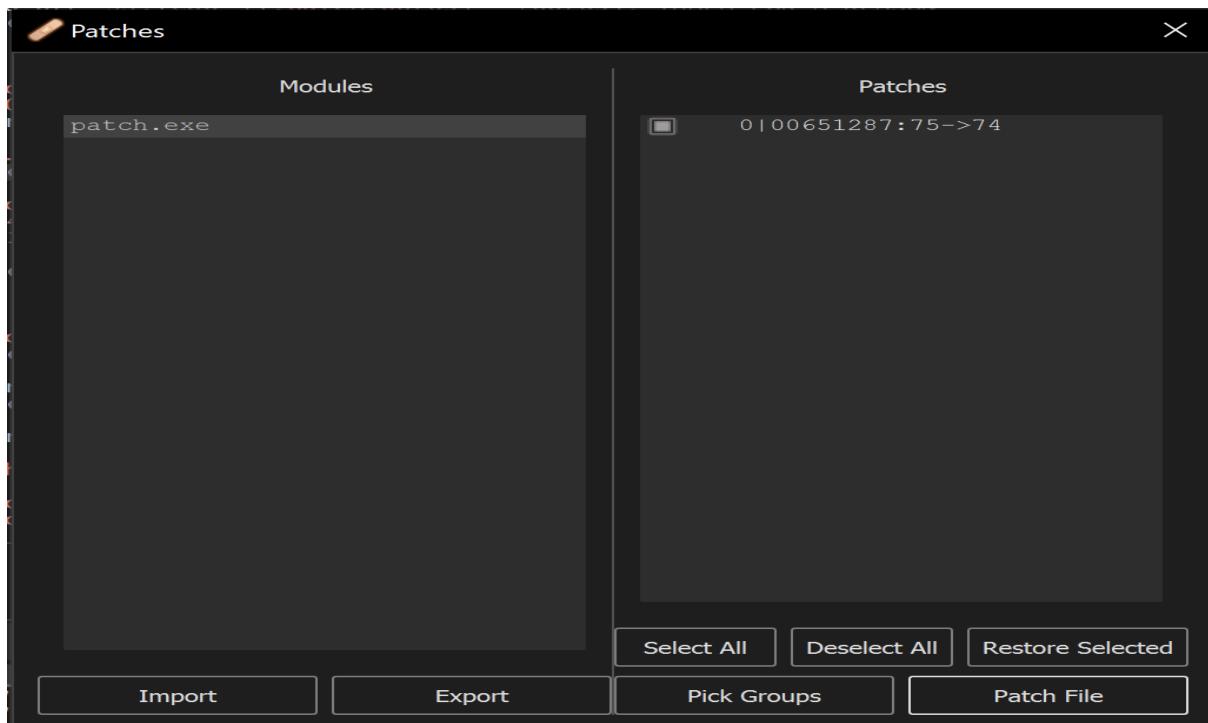
SystemInfo= _SYSTEM_INFO ptr -74h
var_50= dword ptr -50h
var_4C= dword ptr -4Ch
var_48= dword ptr -48h
Buffer= _MEMORYSTATUSEX ptr -44h
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub    esp, 74h
mov     eax, __security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
mov     [ebp+Buffer.dwLength], 40h ; '@'
lea     eax, [ebp+Buffer]
push    eax           ; lpBuffer
call    ds:GlobalMemoryStatusEx
push    0
push    1000000h
mov     ecx, dword ptr [ebp+Buffer.ulTotalPhys+4]
push    ecx
mov     edx, dword ptr [ebp+Buffer.ulTotalPhys]
push    edx
call    __au1ldiv
mov     [ebp+var_50], eax
mov     [ebp+var_4C], edx
lea     eax, [ebp+SystemInfo]
push    eax           ; lpSystemInfo
call    ds:GetSystemInfo
mov     ecx, [ebp+SystemInfo.dwNumberOfProcessors]
mov     [ebp+var_48], ecx
cmp     [ebp+var_4C], 0
ja     short loc_40113A
```

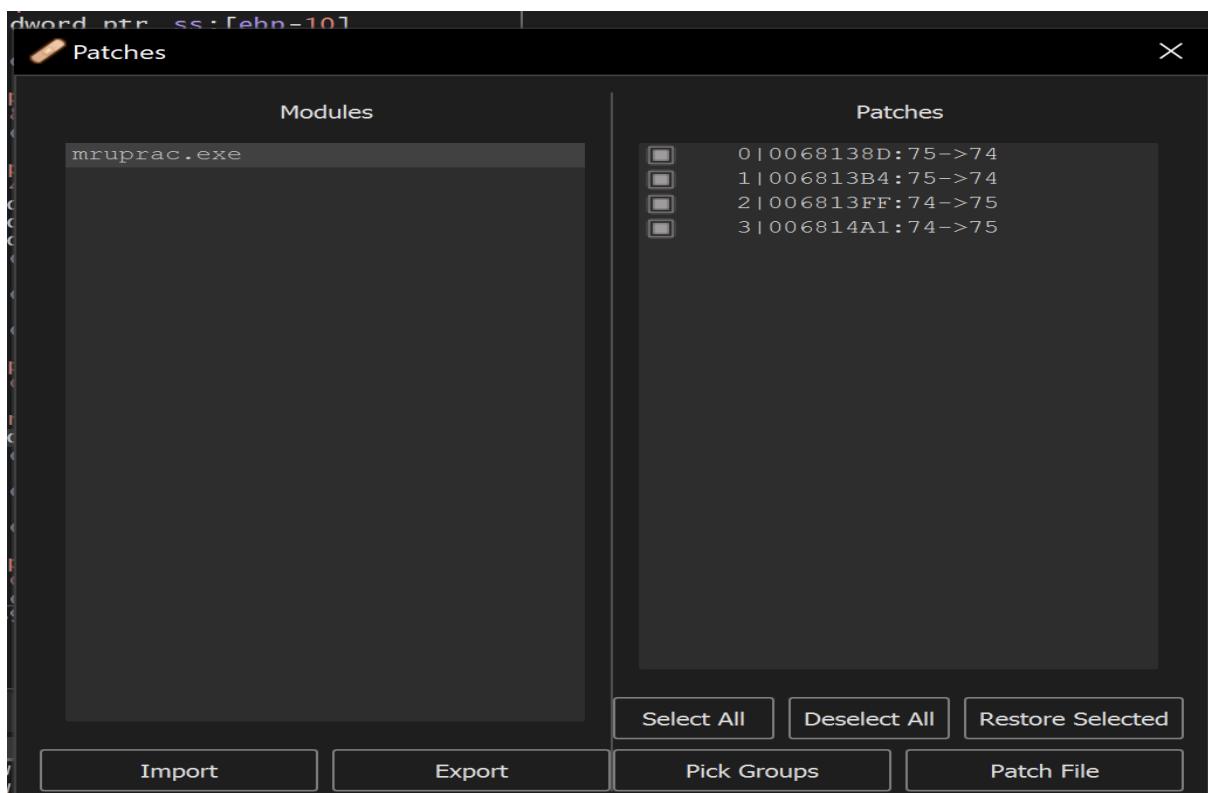
Debugging and Patching

Patches applied.

Internet Patch



Anti VM Patch



The screenshot shows the x32dbg debugger interface. The assembly window displays the following code:

```

006817CF E8 C6030000          call mruprac.681B9A
006817D4 55                   push ebp
006817D9 55                   push esp
006817DA 88EC                mov ebp,esp
006817DC 6A00                push 0
006817DE FF15 4C006900        call dword ptr ds:[<SetUnhandledException>]
006817E4 FF75 08              push dword ptr ss:[ebp+8]
006817E7 FF15 48006900        call dword ptr ds:[<UnhandledExceptionFilter>]
006817ED 68 090400C0          push c0000409
006817F2 FF15 50006900        call dword ptr ds:[<GetCurrentProcess>]
006817F8 50                   push eax
006817F9 FF15 54006900        call dword ptr ds:[<TerminateProcess>]
006817FF 5D                   pop ebp
00681800 C3                   ret
00681801 55                   push ebp
00681802 88EC                mov ebp,esp
00681804 81EC 24030000        sub esp,324
0068180A 6A17                push 1
0068180C FF15 58006900        call dword ptr ds:[<IsProcessInJob>]
00681812 85C0                test eax,eax
00681814 7405                je mruprac.68181B
00681816 6A02                push 2
00681818 59                   pop ecx

```

A tooltip message "Operations completed successfully!" is displayed over the assembly window.

The memory dump window shows the following hex dump:

Address	Hex	ASCII
774B1000	16 00 18 00 80 7D 4B 77 14 00 00 10 7C 4B 77Kw.....
774B1010	00 00 02 00 05 5F 4B 77 08 00 10 00 08 7F 4B 77x.Kw.....
774B1020	00 00 00 00 7F 4B 77 08 00 0A 00 48 7B 4B 77x.Kw.....H
774B1030	06 00 08 00 58 7F 4B 77 06 00 08 00 68 7F 4B 77x.Kw.....h
774B1040	06 00 08 00 60 7F 4B 77 06 00 08 00 60 7F 4B 77Kw.....P
774B1050	1C 00 1E 00 44 7C 4B 77 20 00 22 00 00 82 4B 77D!Kw.....
774B1060	84 00 86 00 78 81 4B 77 00 6C 4E 77 20 48 5B 77x.Kw.inw H

Dynamic Analysis Findings (Part 2)

Findings

Initial Execution: The sample Changes the wallpaper



Sample is downloading image from this url:

<https://pbs.twimg.com/media/F1FbAD9XoAAxLkM.jpg>

Process Tree

Description: Console Window Host
 Company: Microsoft Corporation
 Path: C:\Windows\System32\Conhost.exe
 Command: \?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
 User: DESKTOP-BI93CH6\kant
 PID: 3332 Started: 11/29/2024 11:39:51 AM
 Exited: 11/29/2024 11:40:09 AM

[Go To Event](#) [Include Process](#) [Include Subtree](#)

Sample saves the wallpaper in location: C:\Public\wallpaper.jpg

11:39:56.41134...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 10,968, Length: 1,371
11:39:56.42098...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 12,339, Length: 1,371
11:39:56.42555...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 13,710, Length: 4,113 ...
11:39:56.43093...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 17,823, Length: 1,371
11:39:56.45534...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 19,194, Length: 2,742
11:39:56.47053...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 21,936, Length: 2,742
11:39:56.49041...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 24,678, Length: 1,371
11:39:56.49489...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 26,049, Length: 1,371
11:39:56.50571...	patch.exe	5004	WriteFile	C:\Public\wallpaper.jpg	SUCCESS	Offset: 27,420, Length: 1,371

File Summary:

File Summary										
Files accessed during trace:										
0.0148204	777	230	203	10	1	91,410	45,675	142	0	0
0.0002124	3	1	0	0	1	0	45,675	0	0	0
0.0016111	22	5	5	0	0	0	0	4	0	8 C:\Users\kant\Desktop\patch.exe
0.0001230	18	3	3	9	0	91,350	0	0	0	0 C:\Users\kant\AppData\Local\Microsoft\Windows\INetC...
0.0000968	18	5	5	0	0	0	0	2	0	6 C:\Windows\SysWOW64\CoreMessaging.dll
0.0000836	17	5	5	0	0	0	0	2	0	5 C:\Windows\SysWOW64\WinTypes.dll
0.0001327	16	8	4	0	0	0	0	0	0	4 C:\Users\kant
0.0001118	16	8	4	0	0	0	0	0	0	4 C:\Users\kant\AppData\Local
0.0001564	14	6	4	0	0	0	0	0	0	4 C:\Users\kant\AppData\Local\Microsoft\Windows\INetC...
0.0002308	14	4	4	0	0	0	0	2	0	4 C:\Windows\SysWOW64\winmmbase.dll
0.0000553	12	3	3	0	0	0	0	2	0	4 C:\Windows\SysWOW64\imm32.dll
0.0000655	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\CoreUIComponents.dll
0.0000694	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\PHLAPI.DLL
0.0000585	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\OnDemandConnRouteHelper.dll
0.0000613	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\TextInputFramework.dll
0.0001282	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\TextShaping.dll
0.0000575	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\cryptbase.dll
0.0000746	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\cryptsp.dll
0.0000743	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\ncapi.dll
0.0000641	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\dapi.dll
0.0002043	11	3	3	0	0	0	0	2	0	3 C:\Windows\SysWOW64\dhmap.dll