10th February 2013

MFT vs Super Timeline: Part 1

Now, Tom requested some posting about Super Timeline as he learned about it in FOR508. Well I actually covered Super Timeline back in 2011, but while I read my old posts a new idea came to me.

The last time I did full on disk acquisition was maybe 6 months ago. Its an issue now with disk sizes becoming quite massive in size. Obviously though, having a disk image has its advantages. You can extract any and all files, and of course... timeline analysis.

That being said, you can get a lot of information from the Master File Table (MFT). The MFT is a file on your Windows OS which pretty much is a listing of all files created on the machine. From Microsoft:

> *" There is at least one entry in the MFT for every file on an NTFS file system volume, including the MFT itself. All information about a file, including its size, time and date stamps, permissions, and data content, is stored either in MFT entries, or in space outside the MFT that is described by MFT entries. As files are added to an NTFS file system volume, more entries are added to the MFT and the MFT increases in size. When files are deleted from an NTFS file system volume, their MFT entries are marked as free and may be reused. However, disk space that has been allocated for these entries is not reallocated, and the size of the MFT does not decrease."*
> (http://msdn.microsoft.com/en-gb/library/windows/desktop/aa365230%28v=vs.85%29.aspx)

So this got me thinking, besides for some obvious differences, would the MFT from a disk suffice for a quick and dirty investigation? It would obviously be much faster than a disk acquisition and parsing the entire contents for a drive, but obviously timeline analysis would give you much more information... but enough to justify the time? I think this all depends on what a person is up against, but let's do an example and see....

Setup

For this I will go for a Windows 7 VM. For the malware I want something that has been used before (sadly I have no APTs up my sleeve to work with), but again 'estalished malware' which has been analysed before so it is easier to see the variances between MFT and Super Timeline. So I decided to use a sample from Contagio.

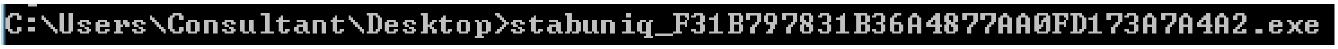
Contagio Link: Trojan.Stabuniq [http://contagiodump.blogspot.co.uk/2012/12/dec-2012-trojanstabuniq-samples.html]

MD5: F31B797831B36A4877AA0FD173A7A4A2
Virus Total Information: 37/46 detection rate [https://www.virustotal.com/file/5a0d64cc41bb8455f38b4b31c6e69af9e7fd022b0ea9ea0c32c371def24d67fb/analysis/]
Malwr.com: Link to Report [http://malwr.com/analysis/f31b797831b36a4877aa0fd173a7a4a2/]
Anubis: Link to Report [http://anubis.iseclab.org/?action=result&task_id=1ec7eb47ca6359024f9f78a4cf72d7f81&format=html]

I also put on the machine FTK_Imager_Lite [http://www.accessdata.com/support/product-downloads] , which I will use to image the VM and also extract the MFT. To be on the safe side, I also setup INetSim on my Remnux [http://zeltser.com/remnux/] image so I can log any callout to the Internet from the malware. I also start to downloaded the latest SIFT VM image [http://computer-forensics.sans.org/community/downloads] from SANS (2.14

right now)

I unpack the exe on the VM at 1510 GMT time. At 1512 I run via the command line and let it fester for about 10 minutes or so so more badness can be done.

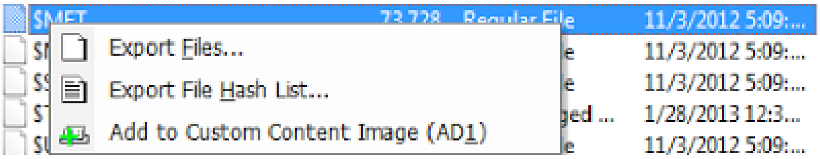


```
C:\Users\Consultant\Desktop>stabuniq_F31B797831B36A4877AA0FD173A7A4A2.exe
```

[http://2.bp.blogspot.com/-oJK2lWUOAG0/URe5wJUDpOI/AAAAAAAACa0/Lual5o5_AB4/s1600/Screen+Shot+2013-02-10+at+15.12.14.png]

1525GMT - FTK Imager

MFT: This is quite simple to extract, simply navigated to the $MFT file located at the root of the drive and extracted it. ***Duration: 1 minute***



[http://2.bp.blogspot.com/-SzVTUS39eAE/URfAz7_zSYI/AAAAAAAACbM/THlvUCfCgpE/s1600/FTK_Imager_MFT.png]

What took longer was trying to figure out how enable a Mac to view hidden files (as when I copied and pasted the MFT to my host machine, it disappeared on me, but I could see it from the terminal). Anyways I found the how-to here [http://www.brooksandrus.com/blog/2007/03/23/mac-os-x-show-hide-hidden-files-in-finder/] . Hoorah!

1541GMT

Timeline Analysis: Begin to grab the HD image using FTK imager. I am putting it on a USB drive. This will take a bit more time of course... I also decided to compress the drive to save on space. This is roughly a 60GB drive.

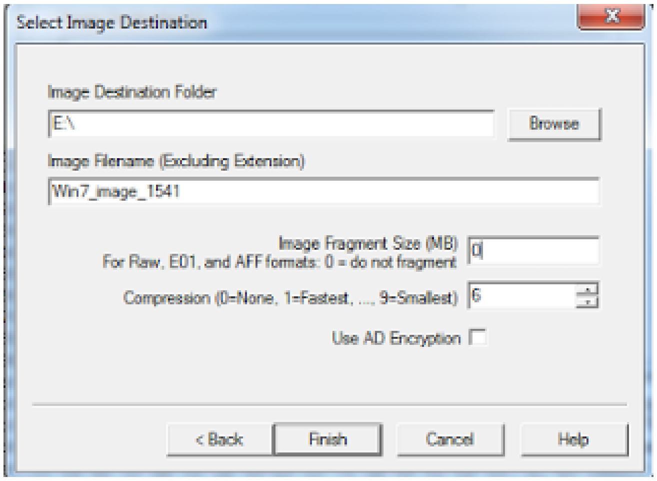


Image Destination Folder
E:\

Image Filename (Excluding Extension)
Win7_image_1541

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
0

Compression (0=None, 1=Fastest, ..., 9=Smallest)
6

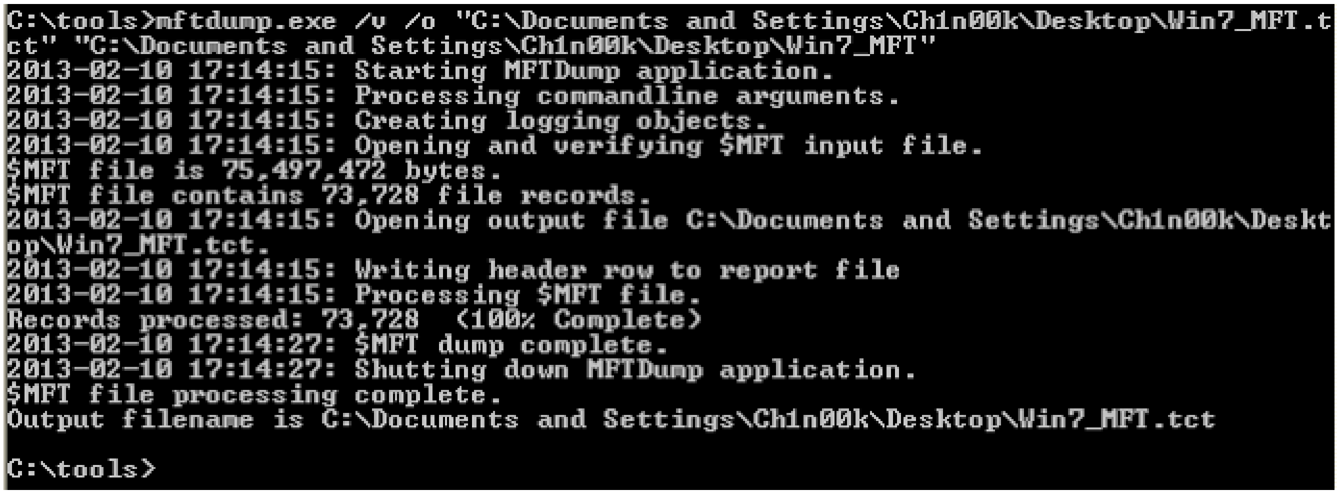
Use AD Encryption □

[http://1.bp.blogspot.com/-NzfxSoWzXs0/URfAz2iy8-I/AAAAAAAACbQ/se5KCuRZYIc/s1600/FTK_Imager_Drive.png]

Elapsed Time(imaging): 16 minutes 12 seconds
Elapsed Time(verification): 34 minutes

MFT Analysis

I will be using Mike Spohn's MFTDump [http://malware-hunters.net/wp-content/downloads/MFTDump_V.1.3.0.zip] tool. It's simple and quick. VERY quick... it took less than a minute to parse through the MFT! Now its time to use every analysts favourite tool - Excel :)



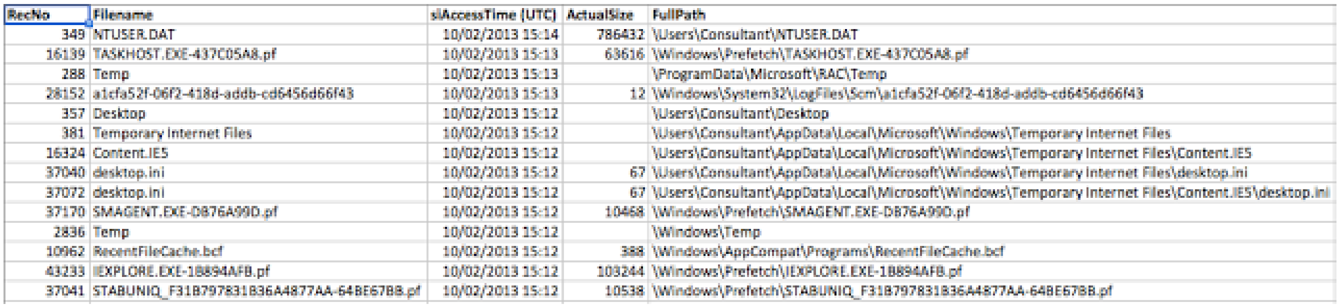
```
C:\tools>mftdump.exe /v /o "C:\Documents and Settings\Ch1n00k\Desktop\Win7_MFT.t
ct" "C:\Documents and Settings\Ch1n00k\Desktop\Win7_MFT"
2013-02-10 17:14:15: Starting MFTDump application.
2013-02-10 17:14:15: Processing commandline arguments.
2013-02-10 17:14:15: Creating logging objects.
2013-02-10 17:14:15: Opening and verifying $MFT input file.
$MFT file is 75,497,472 bytes.
$MFT file contains 73,728 file records.
2013-02-10 17:14:15: Opening output file C:\Documents and Settings\Ch1n00k\Deskt
op\Win7_MFT.tct.
2013-02-10 17:14:15: Writing header row to report file
2013-02-10 17:14:15: Processing $MFT file.
Records processed: 73,728  (100% Complete)
2013-02-10 17:14:27: $MFT dump complete.
2013-02-10 17:14:27: Shutting down MFTDump application.
$MFT file processing complete.
Output filename is C:\Documents and Settings\Ch1n00k\Desktop\Win7_MFT.tct

C:\tools>
```

[http://3.bp.blogspot.com/-2wx0Wsa-728/URfH1aRrMSI/AAAAAAAACbs/O7Ayz7RO7yI/s1600/Screen+Shot+2013-02-10+at+16.14.42.png]

Sorting by Last Accessed Time

Ok so this will probably be a bit hard to show here, but lets give it a try. First thing is I want to see what was last accessed around 1512GMT.



RecNo	Filename	siAccessTime (UTC)	ActualSize	FullPath
349	NTUSER.DAT	10/02/2013 15:14	786432	\Users\Consultant\NTUSER.DAT
16139	TASKHOST.EXE-437C05A8.pf	10/02/2013 15:13	63616	\Windows\Prefetch\TASKHOST.EXE-437C05A8.pf
288	Temp	10/02/2013 15:13		\ProgramData\Microsoft\RAC\Temp
28152	a1cfa52f-06f2-418d-addb-cd6456d66f43	10/02/2013 15:13	12	\Windows\System32\LogFiles\Scm\a1cfa52f-06f2-418d-addb-cd6456d66f43
357	Desktop	10/02/2013 15:12		\Users\Consultant\Desktop
381	Temporary Internet Files	10/02/2013 15:12		\Users\Consultant\AppData\Local\Microsoft\Windows\Temporary Internet Files
16324	Content.IE5	10/02/2013 15:12		\Users\Consultant\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
37040	desktop.ini	10/02/2013 15:12	67	\Users\Consultant\AppData\Local\Microsoft\Windows\Temporary Internet Files\desktop.ini
37072	desktop.ini	10/02/2013 15:12	67	\Users\Consultant\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\desktop.ini
37170	SMAGENT.EXE-DB76A99D.pf	10/02/2013 15:12	10468	\Windows\Prefetch\SMAGENT.EXE-DB76A99D.pf
2836	Temp	10/02/2013 15:12		\Windows\Temp
10962	RecentFileCache.bcf	10/02/2013 15:12	388	\Windows\AppCompat\Programs\RecentFileCache.bcf
43233	IEXPLORE.EXE-1B894AFB.pf	10/02/2013 15:12	103244	\Windows\Prefetch\IEXPLORE.EXE-1B894AFB.pf
37041	STABUNIQ_F31B797831B36A4877AA-64BE67BB.pf	10/02/2013 15:12	10538	\Windows\Prefetch\STABUNIQ_F31B797831B36A4877AA-64BE67BB.pf

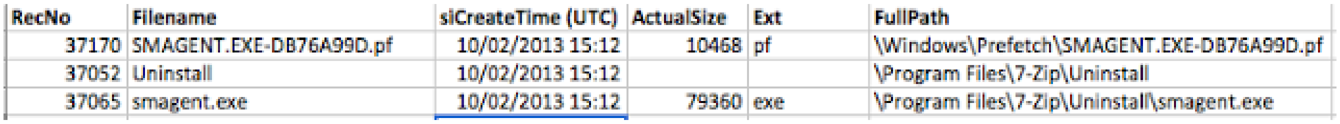
[http://3.bp.blogspot.com/-34j4F1nCuMA/URfOxwTe7UI/AAAAAAAACcM/pXRVtDSG1nc/s1600/Screen+Shot+2013-02-10+at+16.45.22.png]

A bit hard to see, apologies. So from this starting point I make the following assumptions:

- I see the Prefetch file starting at 1512GMT (of course it would not be this obvious in real-life, the filename screams out sketchy)
- The malware starts Internet Explorer (IExplorer.pf is started one second after the suspicious executable)
- Something is accessed/modified in the Temp folder (I don't see anything being created there...)
- A process called SMAGENT is run
- The users registry is accessed (NTUSER.DAT)
- Taskhost is started (I can't tell if this is relevant from this data). What is taskhost? From ghacks.net:

> *"Taskhost.exe is a generic process that acts as a host for processes that run from dynamic link libraries (dll) instead of exe"*

Sorting by Created Time nabs us the creation of smagent.exe in the \Program Files\7-Zip\Uninstall



RecNo	Filename	siCreateTime (UTC)	ActualSize	Ext	FullPath
37170	SMAGENT.EXE-DB76A99D.pf	10/02/2013 15:12	10468	pf	\Windows\Prefetch\SMAGENT.EXE-DB76A99D.pf
37052	Uninstall	10/02/2013 15:12			\Program Files\7-Zip\Uninstall
37065	smagent.exe	10/02/2013 15:12	79360	exe	\Program Files\7-Zip\Uninstall\smagent.exe

[http://3.bp.blogspot.com/-poEORbNFkP0/URfTPGAG3gI/AAAAAAAACcU/UpQYBq_mWbw/s1600/MFT_CreateTime.png]

Elapsed Time (from importing into Excel): 25 minutes

So, with this sample at least we have some decent indicators of what potentially happened. The originally offending process looks to create a new malicious file (smagent), and does something wit iexplore.exe. We see at least one persistence mechanism potential with the NTUSER.dat entry. Looking at Anubis we see the SOFTWARE hive also gets an entry created, but of course, registry hives are being accesses by the OS all the time, so sorting on Create/Access/Modified time may not be the best option for that. Still, good indicators in roughly 30 minutes.

Initial Thoughts

Well from start to finish using the **MFT totalled 26 minutes** of quick and dirty analysis. That's pretty darn good. Of course not all malware is created equal. This analysis missed some things as well, however, it does lead the analysts to a dropped file which could break the analysis wide open. The timeline analysis is already at 45 minutes (with verification).. will it provide enough clues to justify the additional time needed?

Posted 10th February 2013 by -Sketchymoose

Labels: DFIR, FTK, master file table, MFT, MFTDump

5 View comments

David Cowen 12:02 AM

Hello Sketchymoose,
Did you re-enable access times? In my testing/experience they are disabled by default in win 7. It would be interesting to see if you sorted the MFT by MFT Entry modification date which is the best reflection of the last record change.

Also it sounds like what you did could also be called Triaging which is a good way to figure out which systems are deserving of further analysis.

Otherwise interesting write up, I'll be watching for mre.

Reply

Erik Loman 1:39 AM

HitmanPro 3.7.2 constructs NTFS timeline and clusters related files to detect zero-day malware: screenshot

Reply

-Sketchymoose 5:25 AM

One of the things I love most about blogging is learning about yet more tools which can be used! Thanks Erik!

David-- yes, I completely forgot about the access time thing in Windows 7 (my sunday was too lazy !) but when I went back to double check the registry setting, it was still disabled. But then re-checking the MFT dump results shows a difference between CreateTime and AccessTime (for both fn and SI attributes) So I am in contacts with the FMTDump developer to figure out what is happening... good catch!

Reply

-Sketchymoose 8:03 AM

Think I figured it out... I was using an out of date tool version. Lesson learned: ALWAYS CHECK TOOLSETS

FOR UPDATES!

Reply

Anonymous 10:11 PM

thanks for share...

Reply

Enter your comment...

Comment as: Google Accou ▼

Publish Preview