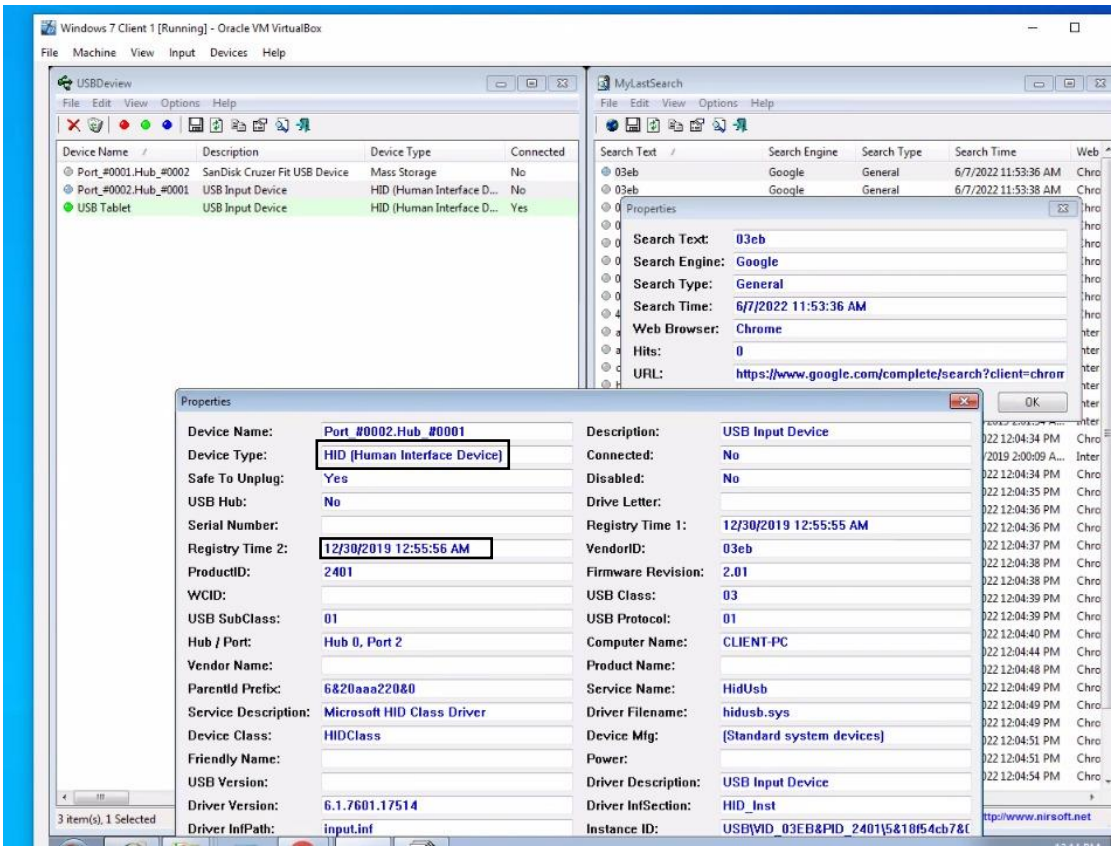
בס"ד

Forensics investigation

By: Tamir Maidani

1.i have installed the VM that needed to be investigated.

2.i began investigating the usb history of the machine by installing and viewing the "USBDeview" program inside the VM.

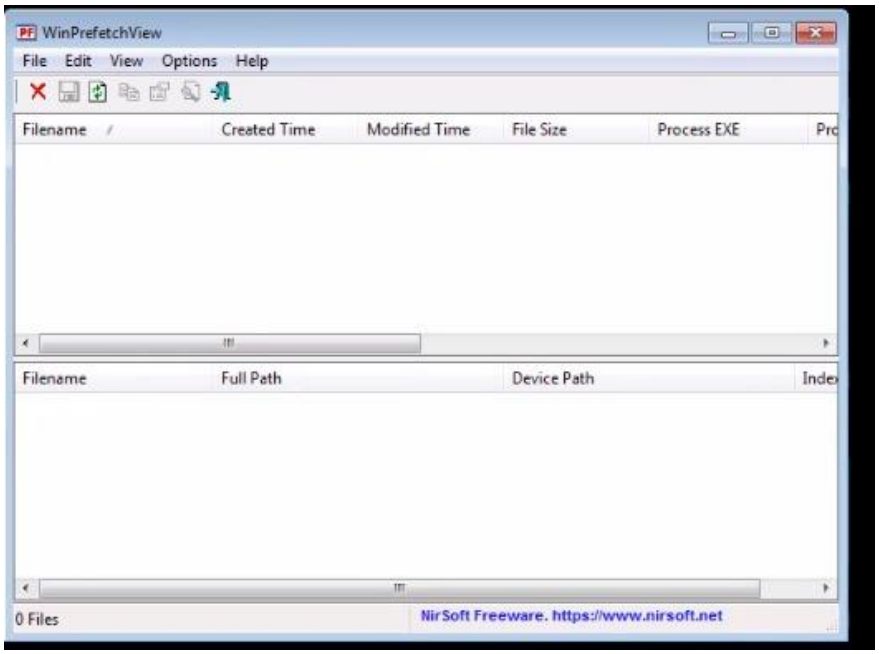


We can see that there is a suspicious entering of a usb and HID device for

Very limited time which can turn a red light!

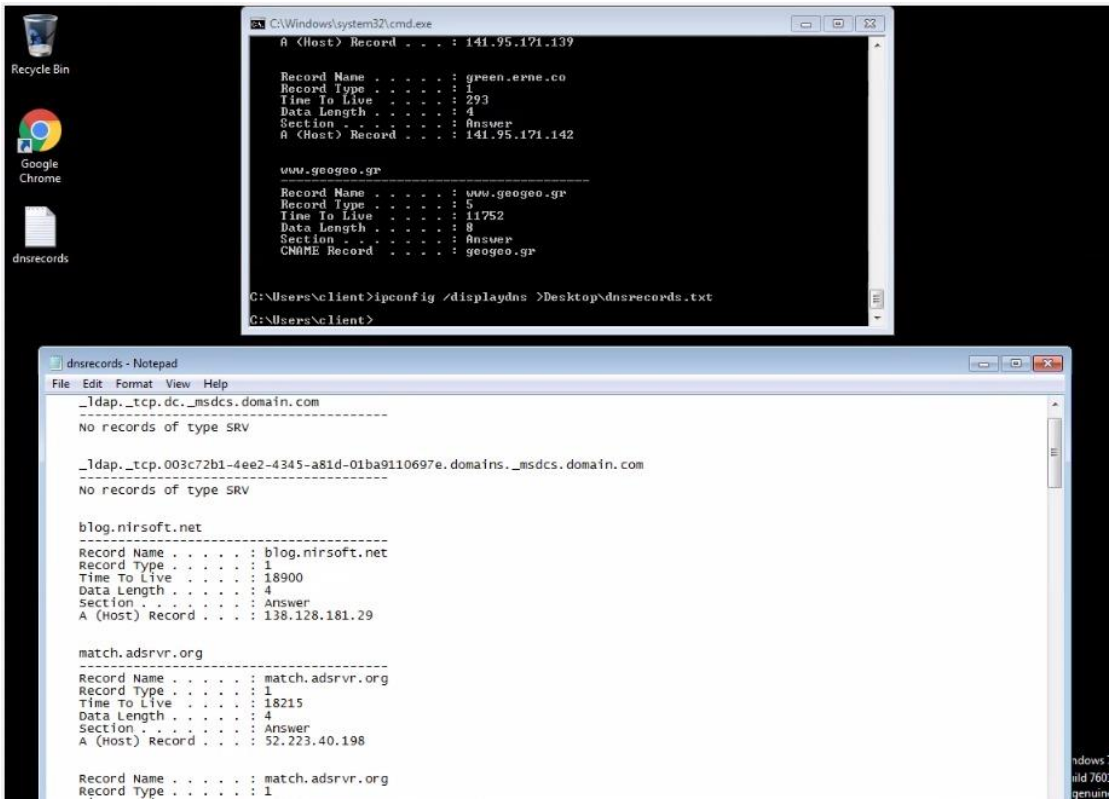
3.i then moved to install and view "WinPrefetchView" inside the VM to check

If there is documented files that where prefetched on the machine.



As the results shows – there is now record of no files that have been opened or engaged with – these results are very unusual because usually there is some record about some files. which we can only assume that someone has deleted the records.

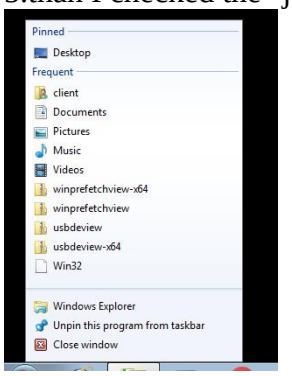
4.then I moved to check the "DNS cache" for seeking some information about my files sources.



Because the machine was turned off, we are only seeing my current web activity

So it is less relevant.

5.than I checked the "jump lists" to see if there is latest files that where mass with.

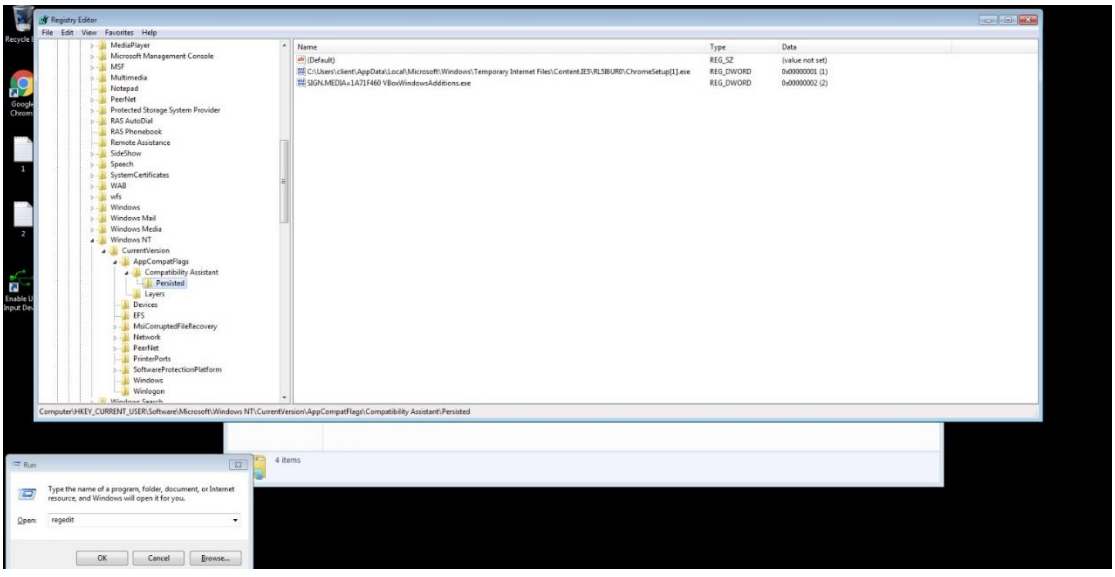


Here we can see that there is a file that called "win32" that has been deleted for some reason.

6.than I want to check the "registry" to see if there has been changes or abnormality.

The first location was:

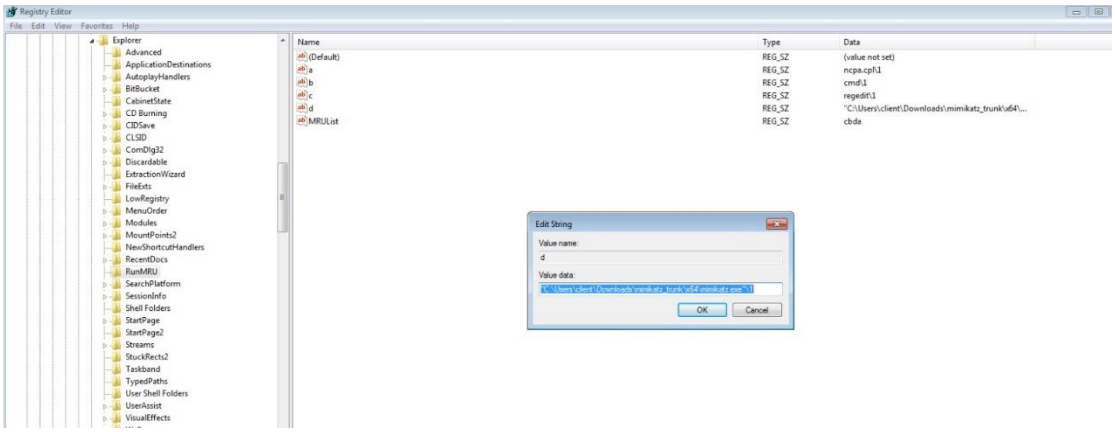
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted



Unfortunately, there were no interesting data there.

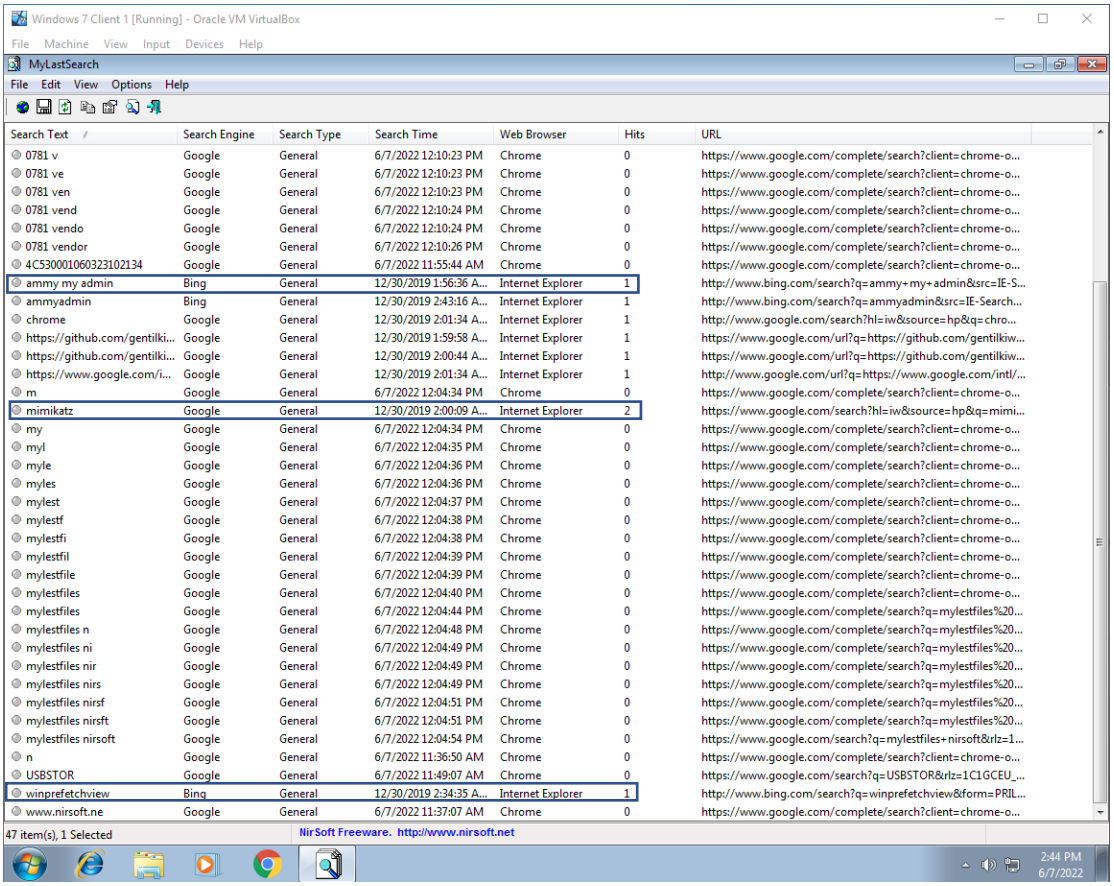
Then I tried another place at the registry which shows what was executed with 'run' :

Navigate to the following path:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Run MRU



Here we have found our first indication of malicious activity – we can see that "Mimikatz.exe" was executed by 'run'.

7. lastly, I tried to check for web history activity with installing and viewing "Mylastsearch" program.



Search Text	Search Engine	Search Type	Search Time	Web Browser	Hits	URL
0781 v	Google	General	6/7/2022 12:10:23 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
0781 ve	Google	General	6/7/2022 12:10:23 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
0781 ven	Google	General	6/7/2022 12:10:23 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
0781 vend	Google	General	6/7/2022 12:10:24 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
0781 vendo	Google	General	6/7/2022 12:10:24 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
0781 vendor	Google	General	6/7/2022 12:10:26 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
4C530001060323102134	Google	General	6/7/2022 11:55:44 AM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
ammy my admin	Bing	General	12/30/2019 1:56:36 A...	Internet Explorer	1	http://www.bing.com/search?q=ammy+my+admin&src=IE-S...
ammyadmin	Bing	General	12/30/2019 2:43:16 A...	Internet Explorer	1	http://www.bing.com/search?q=ammyadmin&src=IE-Search...
chrome	Google	General	12/30/2019 2:01:34 A...	Internet Explorer	1	http://www.google.com/search?hl=iw&source=hp&q=chro...
https://github.com/gentilki...	Google	General	12/30/2019 1:59:58 A...	Internet Explorer	1	https://www.google.com/url?q=https://github.com/gentilkiw...
https://github.com/gentilki...	Google	General	12/30/2019 2:00:44 A...	Internet Explorer	1	https://www.google.com/url?q=https://github.com/gentilkiw...
https://www.google.com/i...	Google	General	12/30/2019 2:01:34 A...	Internet Explorer	1	http://www.google.com/url?q=https://www.google.com/intl/...
m	Google	General	6/7/2022 12:04:34 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
mimikatz	Google	General	12/30/2019 2:00:09 A...	Internet Explorer	2	https://www.google.com/search?hl=iw&source=hp&q=mimi...
my	Google	General	6/7/2022 12:04:34 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
myl	Google	General	6/7/2022 12:04:35 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
myle	Google	General	6/7/2022 12:04:36 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
myles	Google	General	6/7/2022 12:04:36 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
mylest	Google	General	6/7/2022 12:04:37 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
mylestf	Google	General	6/7/2022 12:04:38 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
mylestfi	Google	General	6/7/2022 12:04:38 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
mylestfil	Google	General	6/7/2022 12:04:39 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
mylestfile	Google	General	6/7/2022 12:04:39 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
mylestfiles	Google	General	6/7/2022 12:04:40 PM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
mylestfiles	Google	General	6/7/2022 12:04:44 PM	Chrome	0	https://www.google.com/complete/search?q=mylestfiles%20...
mylestfiles n	Google	General	6/7/2022 12:04:48 PM	Chrome	0	https://www.google.com/complete/search?q=mylestfiles%20...
mylestfiles ni	Google	General	6/7/2022 12:04:49 PM	Chrome	0	https://www.google.com/complete/search?q=mylestfiles%20...
mylestfiles nir	Google	General	6/7/2022 12:04:49 PM	Chrome	0	https://www.google.com/complete/search?q=mylestfiles%20...
mylestfiles nirs	Google	General	6/7/2022 12:04:49 PM	Chrome	0	https://www.google.com/complete/search?q=mylestfiles%20...
mylestfiles nirsf	Google	General	6/7/2022 12:04:51 PM	Chrome	0	https://www.google.com/complete/search?q=mylestfiles%20...
mylestfiles nirsft	Google	General	6/7/2022 12:04:51 PM	Chrome	0	https://www.google.com/complete/search?q=mylestfiles%20...
mylestfiles nirsoft	Google	General	6/7/2022 12:04:54 PM	Chrome	0	https://www.google.com/search?q=mylestfiles+nirsoft&rlz=1...
n	Google	General	6/7/2022 11:36:50 AM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...
USBSTOR	Google	General	6/7/2022 11:49:07 AM	Chrome	0	https://www.google.com/search?q=USBSTOR&rlz=1C1GCEU_...
winprefetchview	Bing	General	12/30/2019 2:34:35 A...	Internet Explorer	1	http://www.bing.com/search?q=winprefetchview&form=PRIL...
www.nirsoft.ne	Google	General	6/7/2022 11:37:07 AM	Chrome	0	https://www.google.com/complete/search?client=chrome-o...

By the results it seems that the files were downloaded from the explorer and they all was downloaded at the same day.

To summarize:

The user used an HID device as "USB rubber ducky" of some kind which can have executed a script that will do the following steps:

1.copy the "win32" folder to the "USB rubber ducky" throw 'run' and then delete the program from the pc.

2.downlowed from the net the "Mimikatz" program throw 'run' to steal the system credentials send it to "USB rubber ducky" and then delete the program.

3.downlowd from the net the program "ammy my admin" throw 'run' and run it in order to create a backdoor.

4.and lastly download from the net the program "WINprefatch" throw 'run', and run it in order to delete all entries and then delete the program.

there is a possibility that "ammy my admin" also been used to create a backdoor but it there is no certain prove to it.