Portfolios

Memory Analysis Ransomware

DIGITAL FORENSIC

2024

Prepared by :

Arya Widyanto Utomo

+6285865492276

www.reallygreatsite.com

Utomoa448@gmail.com

DAFTAR ISI

Deskripsi Kasus

Eksekutif Akun menelepon SOC sebelumnya dan terdengar sangat frustrasi dan marah. Ia menyatakan tidak dapat mengakses file apa pun di komputernya dan terus menerima pop-up yang menyatakan bahwa file-filenya telah dienkripsi. Saya memutus sambungan komputer dari jaringan dan mengekstrak dump memori mesinnya dan mulai menganalisisnya dengan Volatility. Saya melanjutkan penyelidikan untuk mengungkap cara kerja ransomware dan cara menghentikannya!

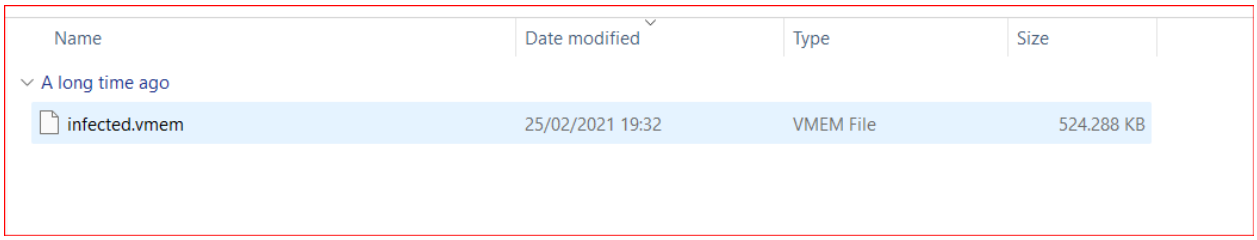
Pembukaan : Sifat Laporan

Pro Justitia.

Demi hukum dan undang-undang yang berlaku saya akan memberikan laporan hasil investigasi dan keterangan ahli ini dengan sebenar-benarnya dan seadil-adilnya.

Barang Bukti

bukti tersebut berupa memory dari sebuah komputer,lalu saya lakukan dump pada memory dengan FTK Imager untuk melakukan analisis lebih lanjut.



Img 1. Bukti digital

Maksud Pemeriksaan

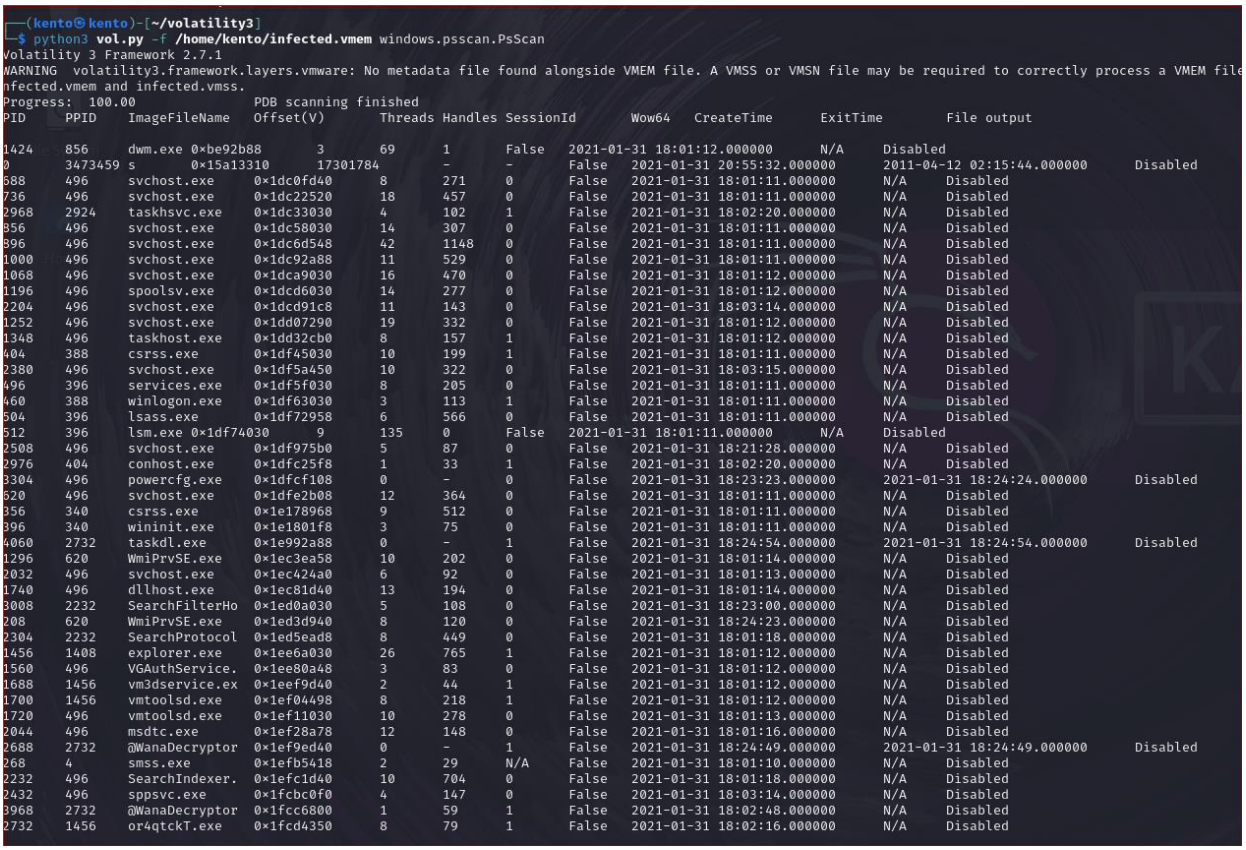
Maksud pemeriksaan adalah untuk mengetahui :

1. Mencari nama proses yang mencurigakan
2. Mencari tahu ID Proses yang mencurigakan.
3. Mencari tahu file yang melakukan eksekusi terjadinya proses mencurigakan tersebut.
4. Mencari tahu proses yang digunakan untuk menghapus file
5. Temukan jalur tempat file berbahaya pertama kali dieksekusi
6. Melakukan investigasi tentang jenis Ransomware tersebut
7. Apa nama file untuk file dengan ransomware public key yang digunakan untuk mengenkripsi private key?

Hasil Pemeriksaan

Adapun berdasarkan Maksud pemeriksaan diatas, maka dilakukan pemeriksaan lebih lanjut dan kemudian menemukan hasil sebagai berikut.

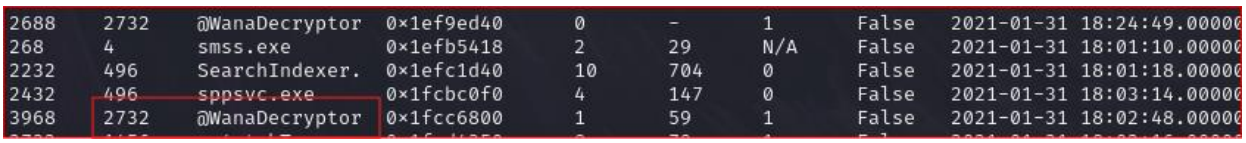
Yang pertama,file snapshot memory tadi (infected.vmem) kami lakukan analisis menggunakan ***volatility3*** untuk mencari proses yang berjalan pada memory komputer yang terdampak dengan command berikut : python3 vol.py /home/kento/infected.vmem windows.psscan.PsScan



```
┌──(kento㉿kento)-[~/volatility3]
└─$ python3 vol.py -f /home/kento/infected.vmem windows.psscan.PsScan
Volatility 3 Framework 2.7.1
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file
nfected.vmem and infected.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

1424    856     dwm.exe 0×be92b88       3       69      1       False   2021-01-31 18:01:12.000000      N/A     Disabled
0       3473459 s       0×15a13310      17301784        -       -       False   2021-01-31 20:55:32.000000      2011-04-12 02:15:44.000000      Disabled
688     496     svchost.exe     0×1dc0fd40      8       271     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
736     496     svchost.exe     0×1dc22520      18      457     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
2968    2924    taskhsvc.exe    0×1dc33030      4       102     1       False   2021-01-31 18:02:20.000000      N/A     Disabled
856     496     svchost.exe     0×1dc58030      14      307     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
896     496     svchost.exe     0×1dc6d548      42      1148    0       False   2021-01-31 18:01:11.000000      N/A     Disabled
1000    496     svchost.exe     0×1dc92a88      11      529     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
1068    496     svchost.exe     0×1dca9030      16      470     0       False   2021-01-31 18:01:12.000000      N/A     Disabled
1196    496     spoolsv.exe     0×1dcd6030      14      277     0       False   2021-01-31 18:01:12.000000      N/A     Disabled
2204    496     svchost.exe     0×1dcd91c8      11      143     0       False   2021-01-31 18:03:14.000000      N/A     Disabled
1252    496     svchost.exe     0×1dd07290      19      332     0       False   2021-01-31 18:01:12.000000      N/A     Disabled
1348    496     taskhost.exe    0×1dd32cb0      8       157     1       False   2021-01-31 18:01:12.000000      N/A     Disabled
404     388     csrss.exe       0×1df45030      10      199     1       False   2021-01-31 18:01:11.000000      N/A     Disabled
2380    496     svchost.exe     0×1df5a450      10      322     0       False   2021-01-31 18:03:15.000000      N/A     Disabled
496     396     services.exe    0×1df5f030      8       205     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
460     388     winlogon.exe    0×1df63030      3       113     1       False   2021-01-31 18:01:11.000000      N/A     Disabled
504     396     lsass.exe       0×1df72958      6       566     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
512     396     lsm.exe 0×1df74030      9       135     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
2508    496     svchost.exe     0×1df975b0      5       87      0       False   2021-01-31 18:21:28.000000      N/A     Disabled
2976    404     conhost.exe     0×1dfc25f8      1       33      1       False   2021-01-31 18:02:20.000000      N/A     Disabled
3304    496     powercfg.exe    0×1dfcf108      0       -       0       False   2021-01-31 18:23:23.000000      2021-01-31 18:24:24.000000      Disabled
620     496     svchost.exe     0×1dfe2b08      12      364     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
356     340     csrss.exe       0×1e178968      9       512     0       False   2021-01-31 18:01:11.000000      N/A     Disabled
396     340     wininit.exe     0×1e1801f8      3       75      0       False   2021-01-31 18:01:11.000000      N/A     Disabled
4060    2732    taskdl.exe      0×1e992a88      0       -       1       False   2021-01-31 18:24:54.000000      2021-01-31 18:24:54.000000      Disabled
1296    620     WmiPrvSE.exe    0×1ec3ea58      10      202     0       False   2021-01-31 18:01:14.000000      N/A     Disabled
2032    496     svchost.exe     0×1ec424a0      6       92      0       False   2021-01-31 18:01:13.000000      N/A     Disabled
1740    496     dllhost.exe     0×1ec81d40      13      194     0       False   2021-01-31 18:01:14.000000      N/A     Disabled
3008    2232    SearchFilterHo  0×1ed0a030      5       108     0       False   2021-01-31 18:23:00.000000      N/A     Disabled
208     620     WmiPrvSE.exe    0×1ed3d940      8       120     0       False   2021-01-31 18:24:23.000000      N/A     Disabled
2304    2232    SearchProtocol  0×1ed5ead8      8       449     0       False   2021-01-31 18:01:18.000000      N/A     Disabled
1456    1408    explorer.exe    0×1ee6a030      26      765     1       False   2021-01-31 18:01:12.000000      N/A     Disabled
1560    496     VGAuthService.  0×1ee80a48      3       83      0       False   2021-01-31 18:01:12.000000      N/A     Disabled
1688    1456    vm3dservice.ex  0×1eef9d40      2       44      1       False   2021-01-31 18:01:12.000000      N/A     Disabled
1700    1456    vmtoolsd.exe    0×1ef04498      8       218     1       False   2021-01-31 18:01:12.000000      N/A     Disabled
1720    496     vmtoolsd.exe    0×1ef11030      10      278     0       False   2021-01-31 18:01:13.000000      N/A     Disabled
2044    496     msdtc.exe       0×1ef28a78      12      148     0       False   2021-01-31 18:01:16.000000      N/A     Disabled
2688    2732    @WanaDecryptor  0×1ef9ed40      0       -       1       False   2021-01-31 18:24:49.000000      2021-01-31 18:24:49.000000      Disabled
268     4       smss.exe        0×1efb5418      2       29      N/A     False   2021-01-31 18:01:10.000000      N/A     Disabled
2232    496     SearchIndexer.  0×1efc1d40      10      704     0       False   2021-01-31 18:01:18.000000      N/A     Disabled
2432    496     sppsvc.exe      0×1fcbc0f0      4       147     0       False   2021-01-31 18:03:14.000000      N/A     Disabled
3968    2732    @WanaDecryptor  0×1fcc6800      1       59      1       False   2021-01-31 18:02:48.000000      N/A     Disabled
2732    1456    or4qtckT.exe    0×1fcd4350      8       79      1       False   2021-01-31 18:02:16.000000      N/A     Disabled
```

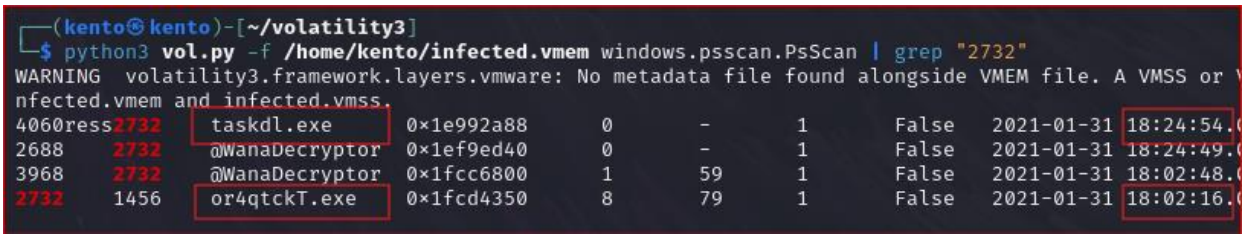
Gulir ke bawah..... Anda akan melihat proses abnormal dengan ID induk yang tidak biasa seperti yang ditunjukkan pada gambar di bawah.



```
2688    2732    @WanaDecryptor  0×1ef9ed40      0       -       1       False   2021-01-31 18:24:49.00000
268     4       smss.exe        0×1efb5418      2       29      N/A     False   2021-01-31 18:01:10.00000
2232    496     SearchIndexer.  0×1efc1d40      10      704     0       False   2021-01-31 18:01:18.00000
2432    496     sppsvc.exe      0×1fcbc0f0      4       147     0       False   2021-01-31 18:03:14.00000
3968    2732    @WanaDecryptor  0×1fcc6800      1       59      1       False   2021-01-31 18:02:48.00000
```

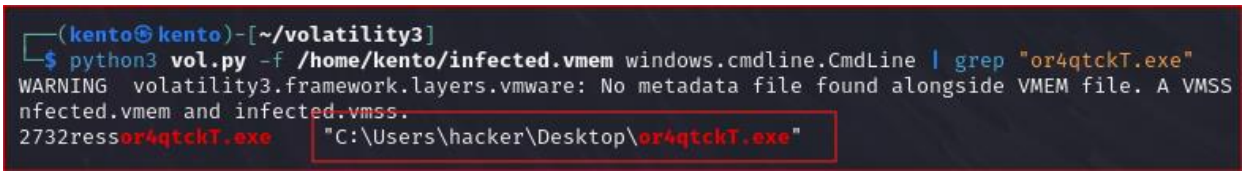
Dari gambar diatas kita dapat mengetahui proses dan PPID yang mencurigakan, yaitu untuk prosesnya @Wannacry dan PPID nya adalah 2732 .

Karena telah mengetahui PPID nya,selanjutnya saya akan mencari tahu file yang melakukan eksekusi proses mencurigakan dan menghapus file tersebut menggunakan PPID dengan command berikut : python3 vol.py /home/kento/infected.vmem windows.psscan.PsScan | grep “2732”



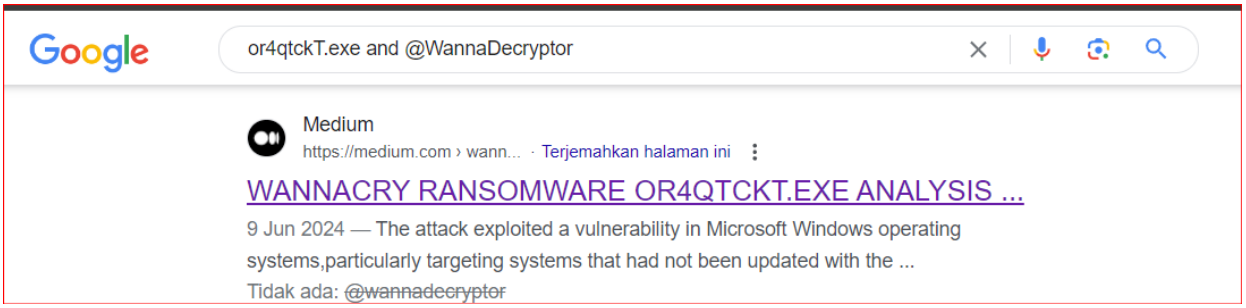
Dari gambar screenshoot an diatas, dilihat dari jam eksekusinya,sebelum proses @Wannacry terjadi,terdapat sebuah aksi eksekusi sebuah file exe (or4qtckT.exe) yang berarti file tersebut adalah file yang mengeksekusi proses tersebut terjadi. Lalu setelah proses tersebut dijalankan,ada sebuah file exe yang mengakhiri proses tersebut (taskdl.exe),yang berarti merupakan proses yang digunakan untuk menghapus file.

Setelah itu,saya akan mencari tahu dimana letak pertama kali file tersebut dieksekusi dengan command berikut : python3 vol.py /home/kento/infected.vmem windows.cmdline.CmdLine | grep “or4qtckT.exe”



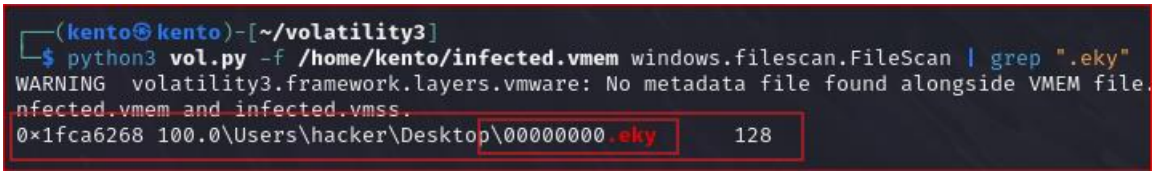
Dari gambar screenshoot an diatas,dapat ditemukan bahwa file pertama dieksekusi pada “C:\Users\hacker\Dekstop\or4qtckT.exe”.

Selanjutnya saya akan mencari tahu informasi tentang jenis Ransomware tersebut menggunakan media search engine dengan mencari dua keyword berikut : or4qtckT.exe and @WannaDecryptor.



Dari gambar tersebut dan pencarian dengan search engine,dapat ditemukan bahwa ransomware tersebut adalah Wannacry.

Setelah mengetahui informasi-informasi mengenai ransomware tersebut,selanjutnya saya akan mencari tahu file public key ransomware yang mengenkripsi private key nya.Biasanya file yang menyimpan kunci enkripsi menggunakan ektension .eky , jadi saya akan mencoba mencarinya dengan command berikut : python3 vol.py /home/kento/infected.vmem filescan.FileScan | grep “.eky”



Dari gambar screenshoot an diatas berhasil ditemukan sebuah file dengan ektension .eky (00000000.eky) yang berfungsi untuk menyimpan kunci enkripsi.

Kesimpulan

Telah dilakukan pemeriksaan dan analisis terhadap barang bukti berupa memory komputer berikut. Pemeriksaan dan analisis dilakukan dengan menggunakan sistem operasi kali linux. Hasil analisis berhasil menemukan semua informasi yang diminta.

Penutup

Demikian laporan hasil investigasi dan keterangan ini dibuat dengan sebenarnya dengan menjunjung tinggi nilai keadilan berdasarkan keahlian dan kompetensi yang dimiliki sesuai dengan peraturan dan perundang-undangan yang berlaku.