Dag:
4

Kategori:
Forensics

Opgavebeskrivelse:
I Brun Bjørns forsøg på at lave spionage, har de som det dræn han nu engang er, eksekveret sine ondsindede filer på sin egen pc.

I denne opgave får du derfor et image af hans pc, hvor du her skal grave dybere for at finde det ondsindede aktivitet filen har generet.

Windows password er "123".

Writeup
Efter en mindre evighed har jeg downloadet zip filen ned og extracted den.

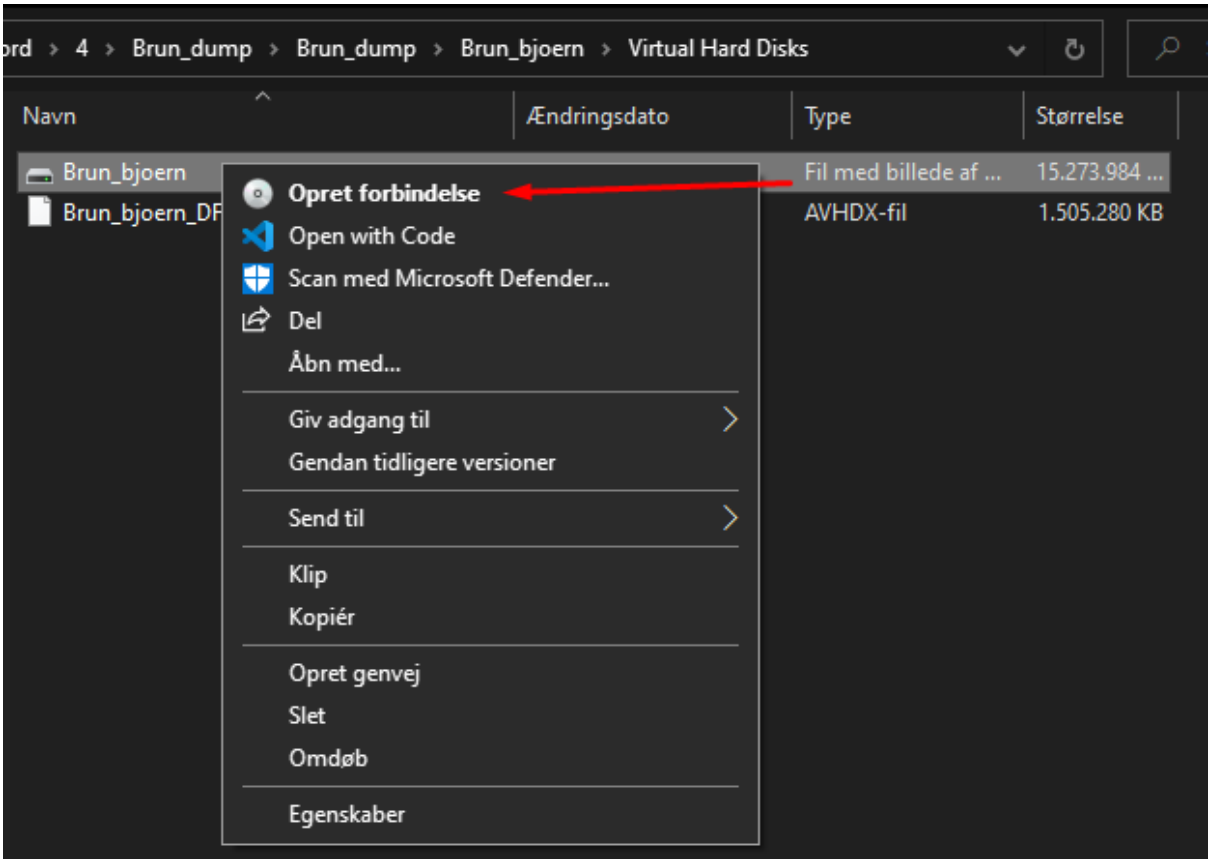
```
C:.
└───Brun_bjoern
    ├───Snapshots
        8A9FADFE-10FA-43E6-A3B6-9E0F8A692552.vmcx
        8A9FADFE-10FA-43E6-A3B6-9E0F8A692552.vmgs
        8A9FADFE-10FA-43E6-A3B6-9E0F8A692552.VMRS

    ├───Virtual Hard Disks
        Brun_bjoern.vhdx
        Brun_bjoern_DF841218-8811-4ACD-A62C-1380FE0AC2D5.avhdx

    └───Virtual Machines
        EA5CC8A1-1C1D-424B-BB33-46278EB1E47D.vmcx
        EA5CC8A1-1C1D-424B-BB33-46278EB1E47D.vmgs
        EA5CC8A1-1C1D-424B-BB33-46278EB1E47D.VMRS
```

1. Min første tanke er at det må være muligt at boote imaget i en Hypervisor. Det var sværere end først antaget da det iflg. min research ikke er muligt at boote **.VHDX** images direkte i Virtualbox/VMWare.
   For at kunne boote vil det først være nødvendigt at konvertere filen til **.VHD** så jeg valgte at gå videre med en lidt nemmere løsning

2. Jeg mounter disken fra **Brun_dump\Brun_bjoern\Virtual Hard Disks\Brun_bjoern.vhdx** på min egen maskine.

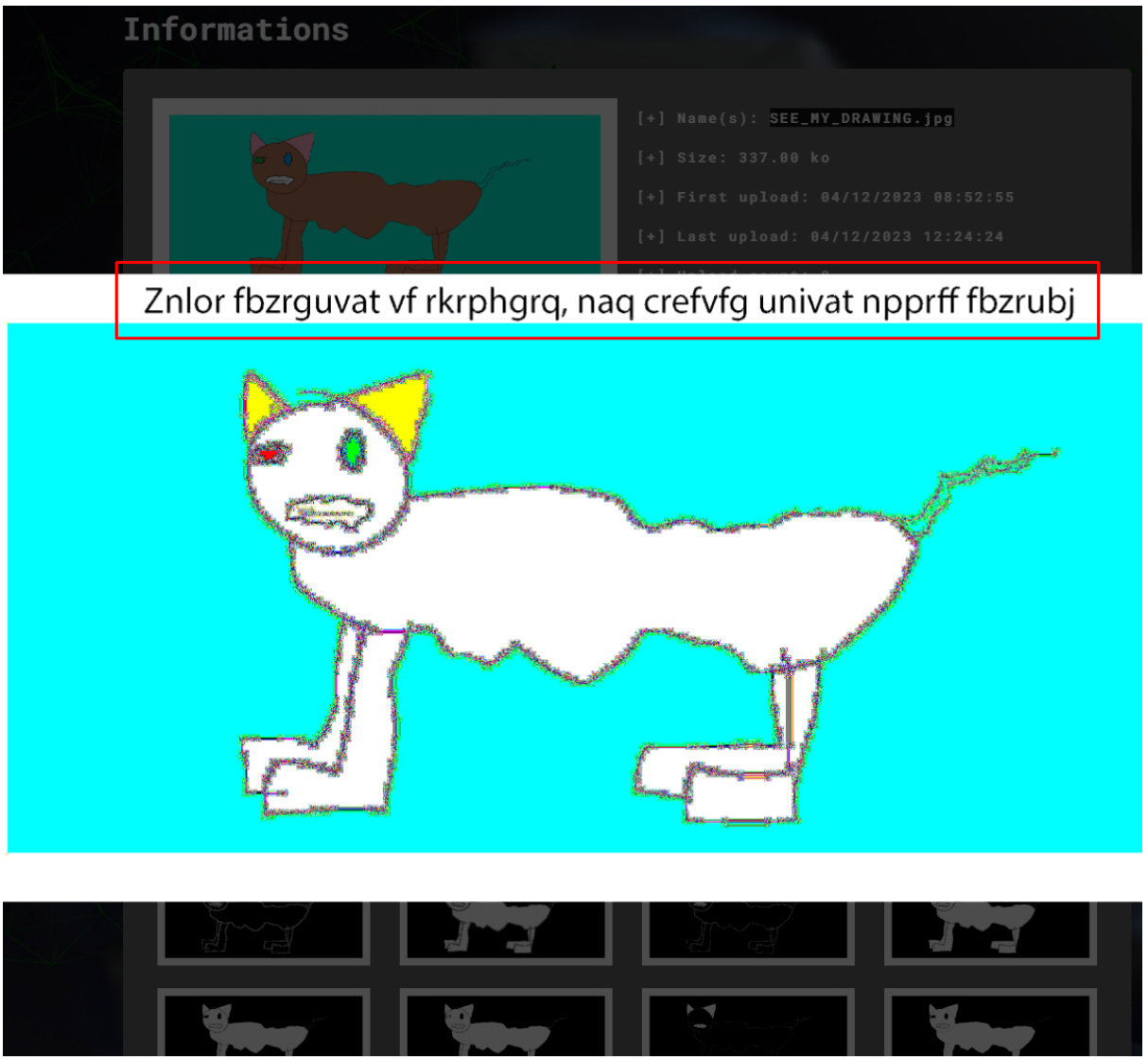


3. Jeg kigger kort igennem filerne, primært under **E:\Users\Brunbjoern** og finder nogle filer på hans Desktop. Det meste af det ser ret useless ud men en fil skiller sig ud **\Users\Brunbjoern\Desktop\Saved Pictures\SEE_MY_DRAWING.jpg** Jeg spotter den primært pga dens navn som er det samme som opgavenavnet.

   Når man zoomer ind på billedet ser man dette

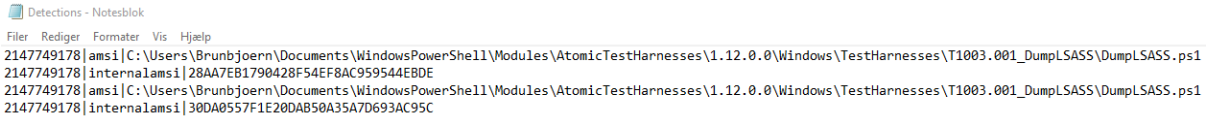
   Det er sgu nok et hint.
   Jeg uploader billedfilen til https://www.aperisolve.com/ hvor jeg ser en ulæselig tekststreng. Jeg formoder det er encoded med ROT13.



Efter tekststrengen er decoded givet det følgende hint

→13 (←13)	maybe something is executed, and persist having access somehow

4. Da jeg kiggede systemet hurtigt igennem kontrollorede jeg også lige Windows Defender scan history (**E:\ProgramData\Microsoft\Windows Defender\Scans\History\Service\Detections.log**) og fandt ud af at der har været eksekveret et DumpLSASS.ps1 powershell script



5. Jeg har fundet hvad der muligvis er dele af "den ondsindede aktivitet" men stadig ingen tegn på Persistence.

   Jeg beslutter mig for at tage et kig i de Registry Hives som ligger på maskinen. Til dette anvender jeg **Registry Explorer** (https://ericzimmerman.github.io/#!index.md:~:text=plugins%2C%20and%20more-,Registry%20Explorer,-1.6.0.0%20%7C%202.0.0.0)

   Det første Hive jeg kigger i er Amcache.hve og det var bare fordi det var det første jeg lokaliserede. Efter at have kigget på hvilke drivere og printer der var installeret tog jeg mig sammen og lavede lidt research på hvor det ville være oplagt at lave persistence.

   Jeg finder frem til at jeg skal kigge i Registry Hivet **NTUSER.DAT (for brugeren "Brunbjoern")**

   I **E:\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run** ligger der en shortcut fil til et powershell script. Det betyder altså at hver gang Brunbjoern logger på så eksekverer scriptet.

	Value Name	Value Type	Data	Value Slack	Is De
	abc	abc	abc	abc	
▶	OneDrive	RegSz	"C:\Users\Brunbjoern\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background	00-00-00-00	
	Ps	RegSz	"C:\Users\Brunbjoern\Documents\WindowsPowerShell\powershell.exe.lnk" /background	69-00-6C-00-65-00-20-0...	

   Jeg inspicerer shortcut-filen og den referer til **C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -File "C:\Users\Brunbjoern\AppData\Local\Temp\b85rN6T.ps1"**