**Analyse av binære filer – del (file på ubuntu gir hvilke type fil det er )**

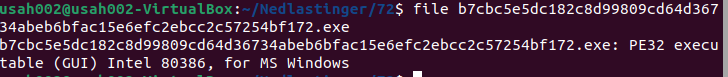
Oppgave 1: pakker ut filen i ubuntu pass:infected

Et bilde som inneholder tekst

Automatisk generert beskrivelseDette er en exe- fil eller med andre ord en programfil (husk å pakke ut zip filen i nedlastinger , ikke flytt på den)

Oppgave 2:

Kjører filen med kommandoen file <filnavnet> og finner ut av at dette er en gui



Oppgave 3

Et bilde som inneholder tekst

Automatisk generert beskrivelse

**Finner du noen strenger du tenker er unike for denne skadevaren?**

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Oppgave 4 : lager en yara regel for å detektere filen:

Et bilde som inneholder tekst

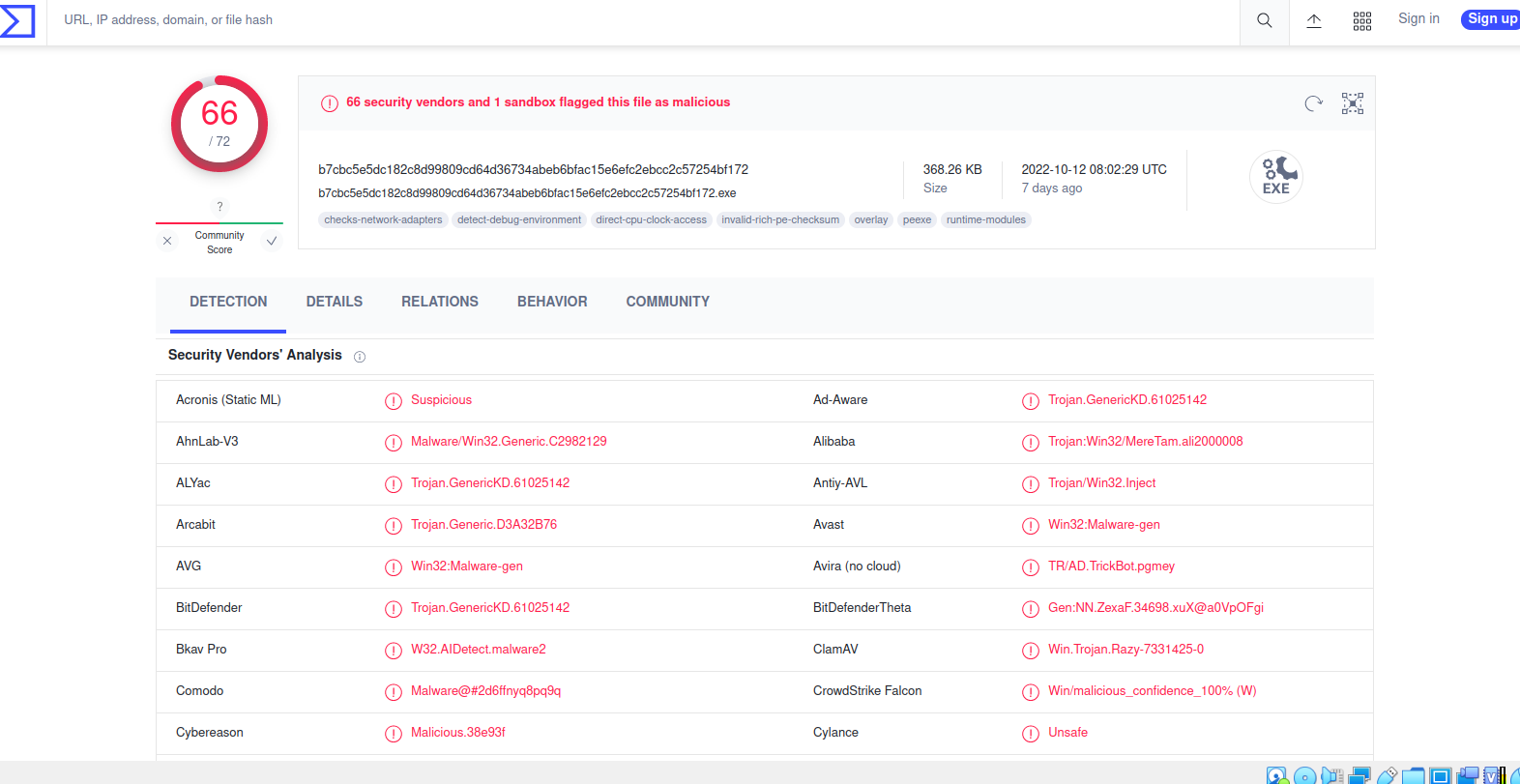
Automatisk generert beskrivelse

Oppgave 5 : kjører md5sum på filen:



8402ab33eafb84178069f8f490ca604d

Limer inn md5-summen i virustotal.com:



**Hvor mange leverandører detekterer dette malwaret?**

66 leverandører (står under security vendors) detekterte denne skadevaren eller filen

**Når ble det først sett på Virustotal?**

**Et bilde som inneholder tekst

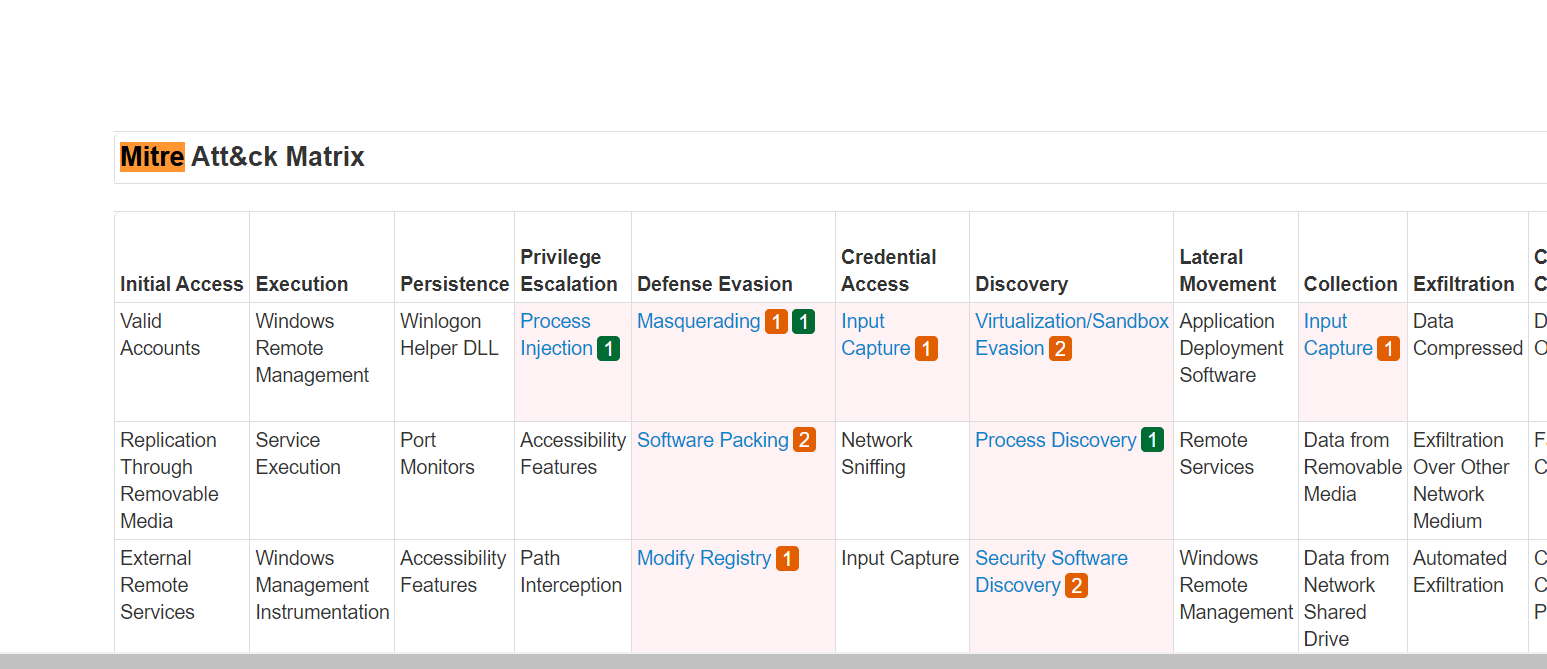
Automatisk generert beskrivelse**

**Hvorfor tror du enkelte leverandører ikke har deteksjon?**

Fordi de ikke har benyttet seg av riktige verktøy for å analysere malwaren , derfor klarer de ikke å detektere den

Kan du se referanser til Mitre?

Se på Mitre dataene og hendelser med malwaret. Hvem brukte det, og hvordan fungerte angrepene i følge Mitre? Er det samsvar mellom det Mitre oppgir og de sakene du kan finne på nett?



Angripere brukte denne skadevaren for å insfisere maskinen slik at de kunne hente ut sensitive data

Slik fungerte det:

Et bilde som inneholder bord

Automatisk generert beskrivelse

**PDF -del**

1. **I en terminal kjører du pdf-parser på filen. Ser du noe mistenkelig? (bruker kali)**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

1. **Ekstraher de mistenkelige elementene med verktøyet**

Ser at det ligger en skjult javascript kode , antar at dette er en skadelig kode som vil kjøre når du trykker på filen som kan infisere maskinen

Et bilde som inneholder tekst

Automatisk generert beskrivelse

1. **Kjør md5sum på elementene som ble dumpet**

****

1. **Sjekk md5 med Virustotal. Hvilken fil var gjemt i PDFen?**

Under ser man filene som gjemmer seg i pdf en:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

**Analyse av office dokumenter del med oledump.py (sudo apt install python3)**

**Gå inn i oledump mappen og kjør python oledump.py <<filnavn>>**

Et bilde som inneholder tekst

Automatisk generert beskrivelse