Oppgave 2 a)

Email til amber i splunk :

**index= “botsv2” sourcetype= “stream:smtp” {“Domain of the company found in answer 1”} amber**

Eksamen blob:

Pakker ut og ekstraherer i ubuntu

Finner filtype:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Virustotal



Finner md5sum og søker den med virustotal:

68013de4691a963a96d9432d4d60be51

Virustotal har definert pdfen som et virus/ramsonware

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Finner en javascript kode: og det ble detektert en word (doc )fil i pdf-en : eicar-dropper.doc (de fleste leverandørene detekterte pdf-en som en trojaner

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Python-parser.py ubuntu installasjon: (ekstraherer ut elementer /objekter med dette verktøyet eller strings «filplassering» er også et alternativ)

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Pdfid er en annen verktøy vi ikke har lært om, men greit å vite: (dette er et verktøy som gir antall objekter på pdf-filer se under)

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Malware kode kan gjemme seg i pdf-er det var vanlig før at angripere benyttet seg av pdf for spredning av malware ved å legge til en link for eksempel for å manipulere brukere til å trykke på det.

Koden er executable