Øvelse 52 – (Gruppe øvelse)Grundlæggende malwareanalyse med VirusTotal

Formål

Formålet med øvelsen er at give dig en introduktion til **malwareanalyse** ved brug af værktøjet **VirusTotal**. Du lærer at:

- Uploade filer og hashes til analyse
- Tolke resultater fra antivirusmotorer
- Reflektere over begreber som *signaturer*, *heuristik* og *falsk-positiver*
- Vurdere malwarefund uden at afvikle dem

Baggrund

Malware (malicious software) er blot almindelig software. Det består af kode og data og kan kun udføre det, systemet tillader. Analyse handler derfor om at finde tegn på skadelig hensigt.

Antivirusværktøjer – som dem VirusTotal bruger – identificerer malware vha. Bla.:

- **Signaturer**: Kendte mønstre, fx i filens indhold eller hash
- **Heuristik**: Regler, der vurderer om noget *ligner* malware
- **Mønster**: Klassificering baseret på mønstre genereret af applikationen

VirusTotal er en gratis tjeneste, der analyserer filer og URLs med over 70 antivirusmotorer. Det bruges af sikkerhedsteams, udviklere og analytikere til hurtigt at vurdere, om en fil er mistænkelig.

Vigtigt: Du må aldrig afvikle filer, du ikke kender – heller ikke i tests.
I denne øvelse **analyserer du udelukkende uden at køre noget**. Uploads til VirusTotal er sikre og isolerede.

Opgaver

1. Undersøg "Martins very non suspicious app"

1. Hent zip-filen fra *Ressourcer* i dagens lektion på Itslearning.
2. Udpak filen.
3. Upload den til VirusTotal.
4. Besvar:
   - Bliver filen markeret som skadelig?
   - Hvor mange antivirusmotorer reagerer?
   - Er der enighed blandt motorerne – og hvad kunne forklare forskellene?

---

2. Undersøg en EICAR-testfil

EICAR (European Institute for Computer Antivirus Research) er en nonprofit-organisation, der samarbejder med antivirusbranchen om at lave **standarder og testværktøjer**.

EICAR har udviklet en testfil, som indeholder en **helt ufarlig tekststreng**, men som med vilje udløser en advarsel i antivirusprogrammer.

OBS: Brug *aldrig* EICAR-filen på din egen laptop – antivirus vil blokere den.
Brug i stedet en **virtuelt miljø**, fx Kali Linux i VirtualBox eller Proxmox.

1. Gå til EICAR testfil
2. Kopiér tekstindholdet fra *EICAR.txt*
3. Opret en ny fil og gem den som `eicar.txt`
4. Upload filen til VirusTotal
5. Undersøg:
   - Genkender alle antivirusmotorer filen?
   - Hvorfor bliver den markeret som malware, selvom den ikke er det?

EICAR-filen bliver markeret som malware, fordi antivirusmotorer er programmeret til at reagere på enten:

- *En eksakt hashværdi af testfilen*
- *Eller på selve tekststrengen i indholdet, som matcher en kendt test-signatur*
  Strengen udfører ikke noget – den er blot en ufarlig tekstsekvens

---

3. Undersøg en kendt hash

1. Gå til VirusTotal

2. Søg på følgende SHA-256-hash:

```
e9104fcd09a12192bb49579a999db843a86ca2a75d750973daf9e618f829ff40
```

3. Analyser:
   - Hvad viser analysen? Er filen klassificeret som malware?
   - Hvilken type malware er det?

Nyttige links

- VirusTotal
- EICAR testfil

Refleksionsspørgsmål

- Hvad kan vi lære af at sammenligne flere antivirusmotorer?
- Hvad betyder det, når nogle motorer markerer og andre ikke gør?
- Hvordan kan VirusTotal bruges i et incident response-forløb?
- Hvad kan du IKKE konkludere ud fra en VirusTotal-analyse?
- Hvordan kunne du bruge den type data i en større sikkerhedsløsning?
- Hvordan kunne hashbaseret søgning bruges til at identificere kendt malware i systemer?
- Hvad ville du gøre, hvis kun én motor udpegede en fil som skadelig?
- Hvordan kan malware tilpasses for at undgå detektion i VirusTotal?

CIS Controls – Kobling

CIS Control	Titel	Relevans
10 – Malware Defenses	Identifikation uden afvikling	Øvelsen bruger statisk signaturanalyse til vurdering af malware
03 – Data Protection	Håndtering af mistænkelige filer	Testfiler håndteres forsigtigt og aldrig eksekveres

CIS Control	Titel	Relevans
17 – Incident Response Management	Analyse af fund	Øvelsen træner analysemetoder, som kan bruges i IR-forløb

---

Videre perspektiv

I større systemer bruges **SIEM-løsninger** som fx **Wazuh**, som kan:

- Indsamle metadata om filer og hashes fra hele systemet
- Sammenligne mod virusdatabaser og kendte signaturer
- Udløse alarmer baseret på fund som dem, du har analyseret her

Dermed kan du **automatisere malwaredetektion og korrelation** på tværs af logs og systemer.

2025-04-29 07:28:03