Uge 2 opgave – Cyber Security.

Delopgave 1

1. **Forskellen på virus, trojanske heste, spyware og ransomware.**

* **Virus:** En computervirus, kan sammenlignes med en biologisk virus som man kender, hvis man bliver syg. Fordi, en virus er en inficering af et system som spreder sig selv ved at angribe ”sunde” systemer på andre enheder.

En virus er en type af malware, som tit ligger gemt i en anden fil og som først går til angreb på det infiltreret system, hvis og når den får adgang til dit computersystem.

En virus på en PC kan eksempel vis, være det som man kalder for en keylogger, hvis design er at få alt den information som der bliver givet via de tastetryk man som bruger laver på computeren. På den måde kan virussen afkode de loginoplysninger og adgangskoder til forskellige sider, som for eksemplet netbank og lign.

**Trojanske heste:** Inden jeg forklarer hvad det er for en type malware, vil jeg kort dykke ned i hvor navnet stammer fra. Navnet stammer fra den græske myte, som siger at for snart 3000 år siden.

Hvor grækerne kæmpede imod trojanerne. Grækerne lavet en kæmpe træ hest som trojanerne troede var en gave. Men så viste det sig, at det var en fælde hvilke førte til at Troja faldt.

En trojansk hest, som også bliver kaldet for trojaner.

Er et fænomen, der udgiver sig for at være et andet program, som man som bruger kan tro er det program man skal bruge. Men kun for at finde ud af, at man har fået en trojaner ind på system som ender med at helt at ødelægge eller forvolde skade på systemet.

Det er netop på samme måde, som Trojanske hest virker idag, hvilket ikke overrasker hvorfor den type af malware har fået det navn.

* **Spyware:** Spyware er en form for malware, der indsamler data på enheden for at videregive den indsamlet data til en tredjepart, uden at offeret har kendskab eller har give samtykke til det.

Cyberkriminelle bruger det til at indsamle data og oplysninger fra deres ofre, statslige instanser bruger det til at opspore kriminelle eller borgere, og større virksomheder og organisationer bruger sommetider spyware til at overvåge sine ansatte.

Ordet Spyware, er en overordnet betegnelse for den type af software som har inficeret ens enhed. Hvis man undersøger det nærmere, så findes der flere forskellige typer af spyware. Følgende er de mest almindelige:

**Adware:** en softwareapplikation med reklamer på din enhed, som kan gemme på et spyware program.

**Cookies:** spyware via såkaldte ‘sporingscookies’ som sporer din online færden.

**Systemovervågning:** spyware, der overvåger dit system og din internetadfærd, mailsystem og hjemmesider, som du besøger.

* **Ransomware:** Navnet ransomware, dækker over et særligt specifikt stykke malware, som går ind og låser det indhold man har på sin maskine, hvor efter at de kræver en løsesum for at få det oplåst igen.

Nu ved vi kort, hvad ransomware er, lad os kigge på hvordan man kan blive ramt af et ransomware angreb.

Man kan blive ramt af ransomware på flere forskellige måder, og er uheldet ude, kan selv et glimrende stykke antivirus-software ikke stoppe det. Den vej, man oftest ser ind, er ved hjælp af et link, en besked eller en fil, der sendes via sociale medier eller e-mail, som giver sig ud for at være noget andet, og hvor man f.eks. giver tilladelse til at installere en fil eller på anden måde giver adgang til sin enhed.

1. **Hvordan kan malware spredes til computere og netværk, nævn 3 metoder.**

* **E-mail vedhæftede filer:**

En af de mest almindelige måder malware spreder sig på er gennem e-mails, der indeholder inficerede vedhæftede filer eller links til ondsindede websteder. Angriberen sender en e-mail, der ser ud til at være fra en legitim kilde, og opfordrer modtageren til at åbne en vedhæftet fil eller klikke på et link.

* **Sårbarheder i software:**

Malware kan udnytte sikkerhedshuller i software og operativsystemer for at få adgang til en enhed. Hvis et system ikke er opdateret med de nyeste sikkerhedsopdateringer, kan ondsindede aktører udnytte disse sårbarheder til at installere malware.

* **Infektion gemmen eksterne enheder:**

Malware kan også spredes via eksterne enheder som USB-drev, eksterne harddiske eller andre lagermedier. Når en inficeret enhed tilsluttes en computer, kan malware automatisk blive overført og køre på systemet.

1. **Hvad er et ’zero-day’ angreb og hvorfor er det særligt farligt i forhold til malware?**

Helt grundlæggende er et ’zero-day’ angreb, en type cyberangreb, som udnytter en sårbarhed i et stykke software eller system, som endnu ikke er opdaget af udviklerne af programmet/systemet. ’zero-day’ angreb er særligt farlige fordi, de kan udnytte en sårbarhed før der er et forsvar på plads og de kan have meget alvorlige konsekvenser for både den individuelle bruger, men også organisationer.

1. **Hvordan identificerer man en malware inficering?**

At identificere en malwareinfektion kan være svært, men der nogen ”almindelige” symptomer som man kan kigge efter, hvis man tror at man har en malware infektion:

Langsommere performance – Er din computer blevet langsommere?

Uventede pop-up vinduer – Et klart tegn på at man er inficeret.

Uventede systemnedbrud eller fejl – mistænkelige crashes eller fejlmeddeleser.

Ukendte netværksforbindelser – Malware prøver at kommunikere med fjernservere.

Opretter din PC til ukendte netværk, kan det være tegn på infektion.

1. **Hvordan påvirker og hvordan håndtere en organisation et ransomware angreb?**

Et ransomware-angreb kræver en effektiv og hurtig reaktion for at minimere skaderne. Forberedelse i form af træning, sikre backup-systemer og robuste sikkerhedspolitikker er afgørende for at beskytte organisationen mod angreb. I tilfælde af et angreb bør organisationen reagere hurtigt, isolere inficerede systemer, kommunikere effektivt og gendanne data. Efter angrebet bør der gennemføres en grundig analyse for at forbedre cybersikkerheden og forhindre fremtidige angreb.

1. **Hvad er phising og hvordan kan det bruges til at sprede malware**

**Phising:** Phising er et begreb, der dækker over flere metoder hvor man lokker offeret til at afgive personlige oplysninger. Dette ses oftest ved at udgive sig for at være en velkendt hjemmeside, eller endda en person, som man normalt har stor tiltro til, og det ses oftest i form af phishing-mails. På sociale medier finder man også ofte phishing – Facebook og Messenger er især meget brugt.

Når det kommer til Phising og Malware, så kan malwaret være inde i en fil som offeret har fået i e-mail og lign. Den vil så installere sig selv på PC’en. Hvor den kan give angriberen fjernadgang, hente og sende filer til angriberen, kryptere filer via ransomware og installere yderligere malware for at gøre skaden endnu værre.

1. **Hvordan kan man sikre sig at malware er væk?**

Der findes mange forskellige måder som man kan sikre sig at malwaren er væk, følgende er en liste over de forskellige måder:

**Kør en komplet systemscanning.**

**Kør en scanning i sikker tilstand.**

**Find og stop mistænkelige processer i joblisten.**

**Kig på opstartslisten efter mistænkelige programmer.**

**Aktiver firewall**

**Skift adgangskoder.**

**Sikkerhedskopier**

1. **Hvad er de kendte typer af malware familier?**

Her er en kort liste over de mest kendte malware-familier, samt en samling af eksempler til hver malware familie:

**Ransomware**

WannaCry, NotPetya, Ryuk

**Trojanere**

Emotet, Zeus, TrickBot

**Adware**

Fireball, Gator

**Rootkits**

TDSS/TDL-4, Stuxnet

**Worms**

Conficker, Sasser

**Spyware**

CoolWebSearch, Keyloggers

**Botnets**

Mirai, Necurs

**Fileless Malware**

PowerShell Backdoor, Cerber

**Banking Malware**

Banload, Dridex

**Keyloggers**

Spyrix, Perfect Keylogger

**File Encrypter Malware**

Locky, CryptoLocker

**Backdoors**

Sub7, NetBus

Delopgave 2

1. Hvilke metoder kan man bruge til at undersøge software hvis man er i tvivl om det er sikkert?

Der er mange forskellige måder hvor man kan tjekke om et program eller fil er sikker at bruge. Men jeg har fundet følgende metoder som man kan bruge:

**VirusTotal**: Upload en fil eller en URL til [VirusTotal](https://www.virustotal.com/) for at scanne den med flere

Antivirus motorer.

**Dynamisk analyse (sandboxing)**: Brug en sandkasse (f.eks. Any.Run eller Cuckoo Sandbox) til at køre mistænkelig software i et isoleret miljø og observere dens adfærd.

**Statisk analyse**: Undersøg filens kode, hvis den er tilgængelig, eller brug reverse engineering-værktøjer (f.eks. Ghidra eller IDA Pro).

**Digitale signaturer**: Kontroller, om programmet er signeret af en legitim udvikler.

**Netværksaktivitet**: Brug værktøjer som Wireshark eller TCPView til at overvåge, om programmet sender data til ukendte servere.

**Tilladelser og systemændringer**: Overvåg, hvilke ændringer softwaren foretager i registreringsdatabasen eller filsystemet.

1. Hvad skal man gøre for at håndtere en fil eller et program der er mistænkeligt på sikker vis?

For at håndtere potentielt skadelig software sikkert:

* **Brug en sandbox eller virtuel maskine**: Kør mistænkelige filer i et isoleret miljø som VirtualBox eller Windows Sandbox.
* **Upload til en analyseplatform**: Scan filen på VirusTotal, Hybrid Analysis eller andre tjenester.
* **Undgå at åbne filen direkte**: Åbn den ikke på din primære enhed, før du er sikker på, at den er sikker.
* **Scan med opdateret antivirus**: Brug en velrenommeret antivirus- eller antimalwareløsning (f.eks. Windows Defender, Malwarebytes).
* **Tjek hash-værdier**: Brug en checksum-generator til at verificere filens hash (SHA-256, MD5) mod officielle kilder.
* **Kontakt IT-sikkerhedseksperter**: Hvis du er på en virksomhed eller institution, bør du rapportere mistænkelig software til IT-afdelingen.

1. Er der nogle offentlige instanser eller mellemstatslige instanser der overvåger det aktuelle trusselsbillede – hvordan foregår det, og hvordan kan de være til gavn?

Der findes flere organisationer, som overvåger cybertrusler og offentliggør advarsler samt vejledning:

**Europol (EC3 – European Cybercrime Centre)**

* + Efterforsker cyberkriminalitet på tværs af EU-medlemslande.
  + Koordinerer aktioner mod hackinggrupper og organiseret cyberkriminalitet.
  + Arbejder tæt sammen med nationale politimyndigheder.

**ENISA (European Union Angency for Cybersecurity):**

* + Analyserer og rapporterer om cybertrusler i Europa.
  + Udarbejder vejledninger og strategier for cybersikkerhed i EU.
  + Støtter medlemsstaternes CERT-teams med teknisk assistance.

**CERT (Computer Emergency Response Teams):** Nationale CERT’er som DK-CERT I Danmark overvåger og rapporterer cybersikkerhedstrusler.

**CISA (Cybersecurity and Infrastructure Security Agency, USA):**

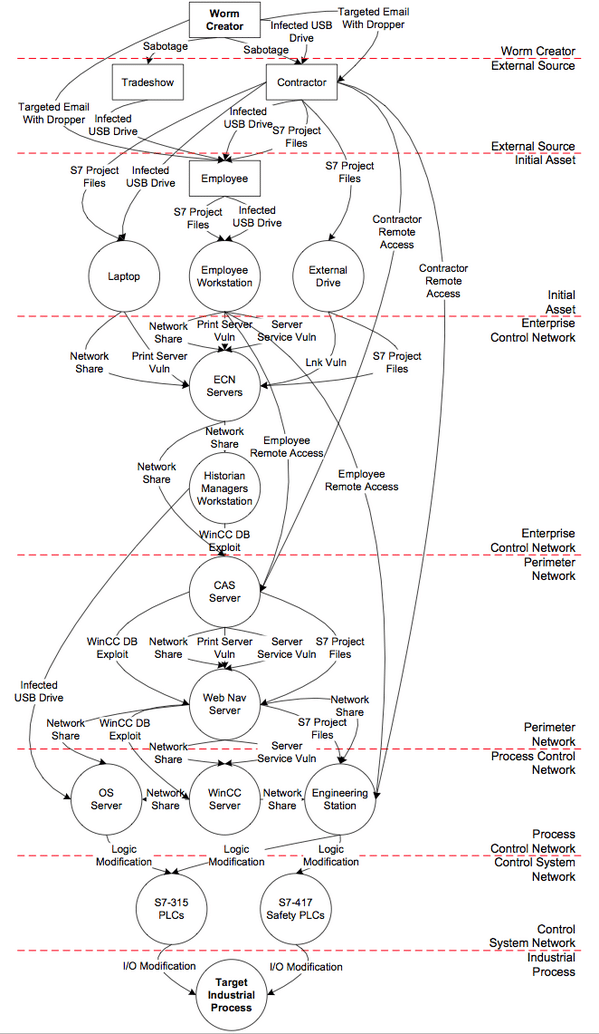
* + Overvåger cybertrusler i Danmark.
  + Informerer virksomheder og borgere om cybersikkerhedsrisici.
  + Håndterer IT-sikkerhedshændelser for danske universiteter og forskning.

**Hvordan kan de være til gavn?**

* De udgiver **trusselsvurderinger**, der hjælper virksomheder og borgere med at beskytte sig.
* De advarer om **nye malwareangreb, phishing-kampagner og sårbarheder**.
* De hjælper med at koordinere **reaktioner på cyberangreb**, både nationalt og internationalt.
* De tilbyder **vejledning og best practices** for cybersikkerhed.

Delopgave 4

**Hvad gør Stuxnet?:**

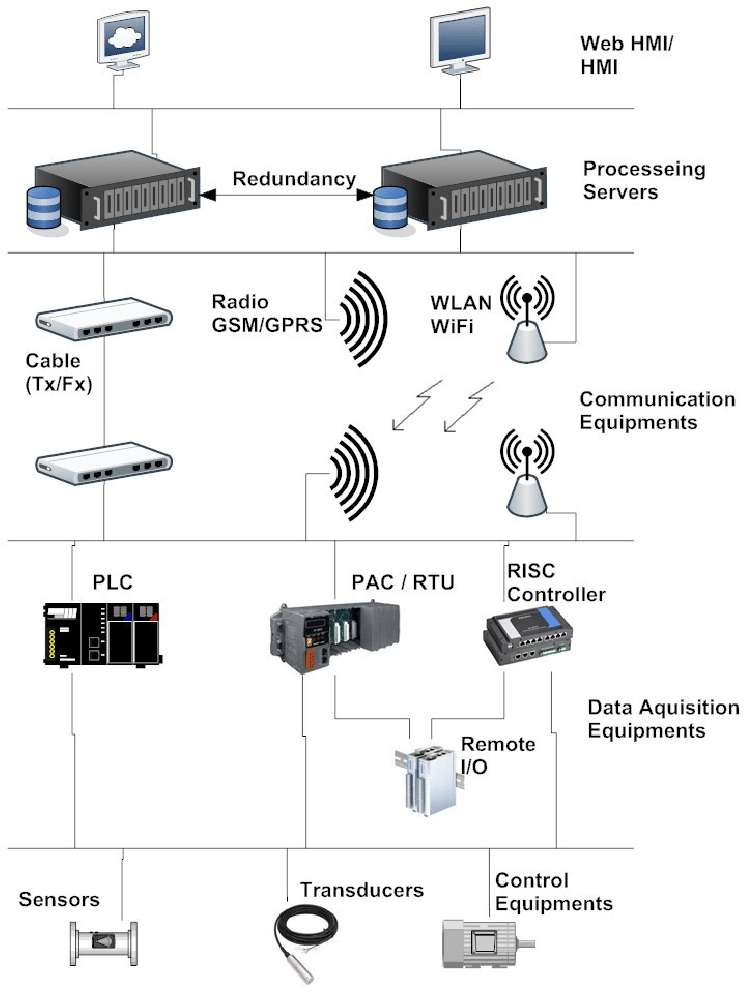


Figur Et diagram, der illustrerer, hvordan Stuxnet blev spredt via USB-drev, udnyttede Windows-sårbarheder og infiltrerede SCADA-systemerne.

Stuxnet er en avanceret og målrettet computermalware, der blev opdaget i 2010. Den klassificeres som en computerorm og er specielt designet til at angribe industrielle kontrolsystemer (ICS), især Siemens PLC'er (Programmable Logic Controllers), der anvendes i kritisk infrastruktur.

Stuxnet infiltrerer systemer, manipulerer styringsparametre og forårsager uopdaget skade på industrielle processer. Dens kompleksitet og præcision gør den unik blandt kendte cyberangreb, da den specifikt var udviklet til at ramme et snævert udvalg af systemer.

**Mål for angrebet:**



Figur Et diagram over en typisk SCADA-systemarkitektur, som viser, hvordan industrielle kontrolsystemer er opbygget, og hvor Stuxnet kunne have påvirket.

Stuxnet var primært designet til at angribe SCADA-systemer (Supervisory Control and Data Acquistion), især dem der blev brugt i Irans uranberigelses faciliteter ved Natanz.

Målet var at forstyrre landets atomprogram ved at manipulere centrifugernes rotationshastigheder, hvilket førte til deres fysiske nedbrydning.

Ved at ændre hastighederne på centrifugerne uden at operatørene opdagede det, blev systemerne gradvist ødelagt, hvilket forsinkede Irans atomprogram betydeligt.

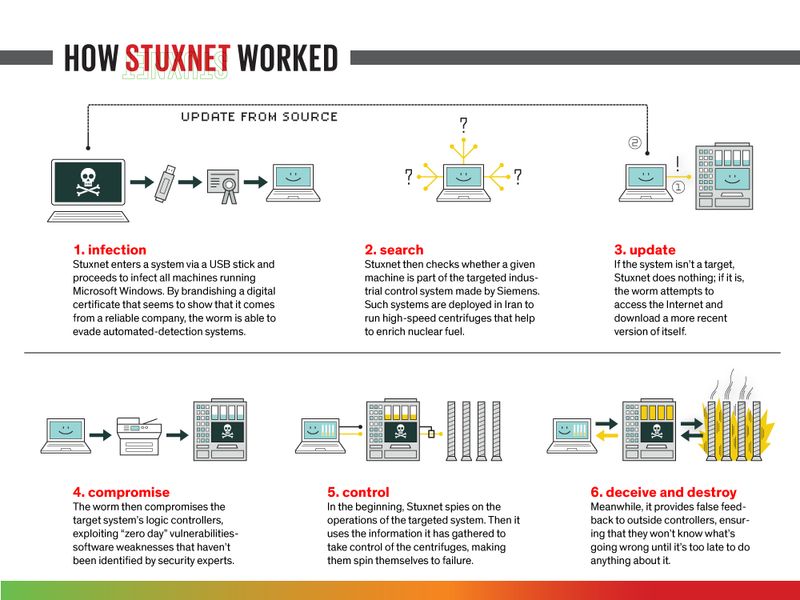
**Geografisk spredning:**

Stuxnet blev først opdaget i Iran, men den spredte sig også til andre lande som Indien, Indonesien og USA.

Selvom den var målrettet mod specifikke systemer i Iran, blev den utilsigtet spredt globalt gennem inficerede USB-drev og netværk.

Dens evne til at sprede sig bredt og infektere computere uden for de opfrindelige målområder var en af de mest bemærkelsesværdige egenskaber ved angrebet.

**Infektionsveje:**



Figur En visuel tidslinje, der viser opdagelsen af Stuxnet i 2010 og de efterfølgende konsekvenser for cybersikkerhed.

Stuxnet blev primært installeret via inficerede USB-drev, hvilket gjorde det muligt at omgå air-gappede systemer (systemer, der ikke er forbundet til internettet).

Derudover brugte den netværksudnyttelser og Windows-sårbarheder til at sprede sig yderligere i lokale netværk og inficere andre systemer.

Den benyttede sig også af stjålne digitale certifikater fra betroede virksomheder for at undgå detektering af sikkerhedssoftware.

**Bagmænd:**

Det antages bredt, at Stuxnet blev udviklet af USA og Israel under en hemmelig cyberoperation kaldet ”Operation Olympic Games”.

Beviser inkluderer sofistikerede angrebsmekanismer, involvering af nationale sikkerheds mydigheder og koden, der var specifikt retttet mod iranske atomfaciliteter.

Lækager fra tidligere embedsmænd samt analyser fra cybersikkerhedsfirmaer peger på statsstøttet udvikling.

**Udnyttede sårbarheder:**

Stuxnet udnyttede mindst fire nul-dags sårbarheder i Windows-operativsystemet samt sårbarheder is Siemens’ PCS 7, WinCC og Step7 software, der blev brugt til industriel processtyring.

Disse sårbarheder gjorde det muligt for Stuxnet at installere sig selv, sprede sig og manipulere styringssystemerne uden at blive opdaget af almindelige sikkerhedsforanstaltninger.

**Efterfølgerne af Stuxnet:**

Angrebet førte til øget opmærksomhed omkring cyberkrigsførelse og industrielt cybersikkerhedsforsvar.

Efterfølgende har lignende malware som Duqu, Flame og Triton viste sig, der også sigter mod kritisk infrastruktur.

Duqu fokuserede på spionage, men Triton var designet til at deaktivere sikkerhedsystemer i industrielle miljøer, hvilket potentielt kunne føre til katastrofale fysiske konsekvenser.

**Trusselsniveauet på tidspunktet:**

Sikkerhedseksperter, herunder SANS Stormcenter, vurderede Stuxnet som et af de mest sofistkerede cyberangreb nogensinde. Dets evne til at manipulere fysiske processer uden at blive opdaget var hidtil uset.

Det skabte en ny forståelse af, hvor effektive cybervåben kan være, og hvordan de kan bruges til at opnå strategiske mål uden brug af koventionelle militære midler.

**Eksisterende varianter i dag:**

Selvom den oprindelige Stuxnet-malware ikke længere er en direkte trussel, er varianter og relateret malware stadig i omløb. Flere efterfølgende cyberangreb har været inspireret af Stuxnet og anvendt lignende teknikker.

Malware som Duqu, en trojaner baseret på Stuxnets kode, blev opdaget kort efter og bruges til spionage og informationsindsamling. Derudover er Trition/Trisis et nyere angreb, der målrettet rammer industrielle sikkerhedssystemer, potentielt med henblik på fysisk sabotage.

Der er også eksempler på Stuxnet-lignende angreb, der forsøger at inficere industrielle kontrolsystemer i energisektoren og andre kritiske infrastrukturer.

**Kan du identificere paralleller mellem Stuxnet og nyere cyberangreb:**

Lignende angreb inkluderer NotPetya, som ramte globale virksomheder og statsinfrastrukturer, og Triton, der forsøgte at sabotere industrielle sikkerhedssystemer.

Disse angreb demonstrerer, hvordan cyberkrigsførelse er blevet en integreret del af moderne konflikter

Både statslige aktører og cyberkriminelle har udviklet avancerede værktøjer inspireret af Stuxnet, hvilket har øget trusselsniveauet globalt.

**Beskyttelse mod lignende angreb:**

For at beskytte sig mod lignende angreb kan organisationer implementere følgende foranstaltninger:

* Opdatering og patching af software regelmæssigt for at lukke kendte sårbarheder.
* Segmentering af netværk for at minimere spredning af malware.
* Strenge adgangskontroller og overvågning for at reducere insidertrusler.
* Implementering af Intrusion Detection Systems (IDS) og Intrusion Prevention Systems (IPS) for at opdage og blokere mistænkelig aktivitet.
* Øget medarbejderuddannelse om cybersikkerhed for at minimere risikoen for social engineering og phishing-angreb.

Stuxnet markerede begyndelsen på en ny ære inden for cyberkrigsførelse, og dets arv fortsætter med at påvirke moderne sikkerhedsstrategier. Cyberangreb på kritisk infrastuktur er nu en reel trussel, og virksomheder samt regeringer må konstant opdatere deres sikkerhedsforanstaltninger for at beskytte sig mod nye trusler.

**Kildeliste:**

* Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown, 2014.
* Symantec Security Response. "W32.Stuxnet Dossier." Symantec, 2011.
* Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security & Privacy, 2011.
* Sanger, David E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. Crown, 2012.
* ICS-CERT. "ICS-CERT Alert (IR-ALERT-H-16-056-01) - Stuxnet Malware Analysis." U.S. Department of Homeland Security, 2016.
* <https://www.researchgate.net/figure/Stuxnet-partial-attack-graph-figure-adopted-from-5_fig1_316939466?utm_source=chatgpt.com>
* <https://nordvpn.com/da/blog/hvad-er-computer-virus/>
* <https://nordvpn.com/da/blog/hvad-er-ransomware/>
* <https://nordvpn.com/da/blog/hvad-er-spyware/>
* <https://nordvpn.com/da/blog/trojan/>