CENTER FOR CYBERSIKKERHED

TRUSSELSVURDERING

Drømmer cyberkriminelle om tillidsfulde relationer?

Stadig mere professionaliserede kriminelle aktører samarbejder om at udføre omfattende og avancerede angreb på nettet

Formål
Trusselsvurderingen har til formål at give beslutningstagere et indblik i, hvordan det organiserede samarbejde mellem kriminelle på nettet har udviklet sig, og hvad det betyder for truslen fra cyberkriminalitet.

Hovedvurdering

- CFCS vurderer, at truslen fra cyberkriminalitet er MEGET HØJ. Truslen underbygges af cyberkriminelle, der samarbejder og udveksler tjenester indbyrdes under markedslignende vilkår kaldet Crime-as-a-Service.

- Crime-as-a-Service gør det muligt for kriminelle mod betaling at anskaffe sig adgange, værktøjer og infrastruktur, som de bruger i cyberangreb, frem for at udvikle det selv.

- Samarbejdet øger specialiseringen og effektiviteten i det cyberkriminelle miljø, hvilket skaber robuste og organiserede forsyningskæder, der bl.a. understøtter målrettede ransomware-angreb.

- Brugen af kryptovaluta bidrager til udviklingen mod et mere kommercialiseret og specialiseret cyberkriminelt miljø.

- Ransomware-as-a-Service har introduceret en form for platformsøkonomi til cyberkriminalitet, hvor hackerne gennem ransomware-angreb tjener penge til sig selv og til de bagmænd, der ejer platformen.

- Nogle kriminelle grupper kan som følge af udviklingen arbejde mere målrettet og professionaliseret. Det har bl.a. bidraget til den stigende trussel fra målrettede ransomware-angreb.

Center for Cybersikkerhed
Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave. Oktober 2020

Analyse

CFCS vurderer, at truslen fra cyberkriminalitet er MEGET HØJ. Truslen underbygges af, at kriminelle hackere sælger og køber tjenester af hinanden på internettet. Denne indbyrdes udveksling af tjenester, der i it-sikkerhedskredse kaldes Crime-as-a-Service (CaaS), er ikke et nyt fænomen. De seneste par år har dette samarbejde dog udviklet og ændret sig, hvilket har påvirket trusselsbilledet.

Udvekslingen af varer og tjenester foregår på lukkede internetfora og gennem etablerede, personlige samarbejdsrelationer. Her sælges og udveksles en bred palet af værktøjer som malware, infrastruktur som botnets, kompromitterede adgange og distribution gennem phishing og downloadere. CaaS gør det således muligt for hackere at anskaffe sig de tjenester og adgange, de skal bruge i deres cyberangreb, frem for selv at udvikle dem.

Det skaber værdikæder mellem de kriminelle hackere, der på forskellig vis bidrager til at øge muligheden for udbytte af cyberkriminalitet.

Handlen med kriminelle tjenester kan begrænse sig til specifikke ydelser med en fastsat pris. I disse tilfælde minder udvekslingen af kriminelle tjenester om den udveksling af varer, der foregår på et traditionelt marked med veldefinerede roller for køber og sælger. Et typisk eksempel på denne form for handel er online markedspladser, hvor kriminelle bl.a. sælger varer som stjålne personlige og finansielle oplysninger, eksempelvis credentials i form af brugernavne og adgangskoder.

RDP-adgange sælges på nettet
Cyberkriminelle misbruger ofte sårbare Remote Desktop Protocol-adgange (RDP) i cyberangreb, for eksempel i forbindelse med målrettede ransomware-angreb. Videregivelse og salg af kompromitterede RDP-adgange er derfor udbredt i kriminelle kredse.

Ofte kompromitterer kriminelle aktører et stort antal RDP-adgange gennem f.eks. brute force-angreb. Herefter sælger de specifikke adgange videre til andre hackere, der bruger dem som udgangspunkt for mere målrettede cyberangreb.

I 2018 identificerede et sikkerhedsfirma en værdikæde, hvor bagmændene bag den cyberkriminelle gruppe SamSam for 10 amerikanske dollars købte stjålne RDP-adgange til it-systemer. Herefter brugte gruppen adgangen til at kryptere systemerne og krævede i visse tilfælde op mod 40.000 amerikanske dollars i løsesum for at dekryptere.

Faste samarbejdsrelationer strømliner produktionen

CaaS antager også form af længerevarende samarbejdsrelationer mellem kriminelle. Det skyldes bl.a., at udvekslingen af tjenester i sin natur foregår ureguleret uden for lovens rammer. Risikoen for at blive snydt vil således næsten altid være til stede, når kriminelle udveksler tjenester, og der findes flere eksempler på, at kriminelle har brugt forskellige internetfora til at snyde andre kriminelle. CaaS bygger derfor – som andre samarbejdsrelationer – på tillid blandt de kriminelle. En tillid, der tager lang tid at opbygge, men som hurtigt kan forsvinde.

Samtidig er der en risiko for, at inkompetente hackere, der anvender andres tjenester, eksponerer både sig selv og de mere erfarne dele af det cyberkriminelle miljø.

Flere kriminelle netværk søger derfor længerevarende samarbejdsrelationer med andre aktører, som de har opbygget tillid til.

Samarbejdet har en pris
I december 2019 indførte amerikanske myndigheder i koordination med britiske myndigheder økonomiske sanktioner mod flere navngivne personer og virksomheder i Rusland, der menes at stå i ledtog med et cyberkriminelt netværk kaldet Evil Corp.

Netværket har ifølge sanktionerne stået bag spredningen af malwaren Dridex. Dridex, der i tidligere varianter blev kaldt Bugat og Cridex, er siden 2012 blevet spredt gennem massive phishing-angreb med et udbytte svarende til mere end en halv milliard danske kroner. Spredningen er bl.a. sket i et samarbejde med de netværk, der står bag kendte botnet som Crap2P og Cutwail, der bruges som infrastruktur i phishing-angrebene. Dridex har også været brugt i målrettede angreb med ransomwaren BitPaymer.

Anklageskriftet illustrerede samtidig, hvordan kriminelle, der er villige til at betale, kan få adgang til infrastruktur og malware, drevet af netværk som Evil Corp. En person bosat i Storbritannien skulle ifølge anklageskriftet have betalt en indledende sum på 100.000 amerikanske dollars og herefter minimum 50.000 amerikanske dollars om ugen for at få adgang til Dridex og Evil Corps tjenester.

De kriminelle, der udfører målrettede angreb, samarbejder eksempelvis med de kriminelle, der rammer tusindvis af ofre gennem bl.a. phishing. Målrettede ransomware-angreb sker således ofte efter en indledende kompromittering af offeret med malware spredt bredt gennem phishing.

I disse tilfælde bliver det indledende og oftest automatiserede forsøg på kompromittering, der gennem f.eks. botnets sendes ud til mange modtagere, efterfulgt af mere målrettede og manuelle angreb foretaget af andre aktører mod udvalgte ofre.

Den form for samarbejde er typisk mere organiseret og etableret end handlen med specifikke tjenester på bl.a. online markeder.

I de tilfælde, hvor samarbejdet antager en mere organiseret form, vil hackergrupper eller netværk ofte specialisere sig i at udføre afgrænsede dele af et angreb eller levere afgrænsede tjenester. Det bidrager til at skabe en arbejdsdeling internt i det kriminelle miljø.

Arbejdsdelingen gør det muligt for den enkelte hacker eller hackergruppe at specialisere sig inden for et afgrænset felt. Det kan derfor på flere måder sammenlignes med klassiske produktionsvirksomheder, der udnytter specialiserede leverandører til at arbejde mere effektivt.

Samarbejdet mellem Emotet, Trickbot og Ryuk viser, hvordan cyberkriminelle udvikler organiserede forsyningskæder
Emotet og Trickbot er to kendte såkaldte trojanere, der oprindeligt er udviklet og brugt uafhængigt af hinanden. De senere år har der dog været flere eksempler på, at de to malware bliver brugt sammen med ransomwaren Ryuk som en slags tre-trins-raket.

Hvor Emotet tidligere blev brugt til at stjæle finansielle oplysninger fra netbankkunder, bruges malwaren nu hovedsageligt som et værktøj, andre kriminelle kan købe sig adgang til. Emotet benyttes således eksempelvis til at distribuere Trickbot, der bl.a. kan bruges som brohoved i målrettede ransomware-angreb begået med Ryuk.

I juli 2019 kostede et ransomware-angreb eksempelvis bystyret i Lake City i Florida 460.000 amerikanske dollars i løsesum. En analyse af angrebet viste, at Emotet havde fungeret som den indledende angrebsvektor. Efter denne indledende kompromittering blev Emotet brugt til at distribuere Trickbot, der efterfølgende downloadede ransomwaren Ryuk. Herefter har bagmændene bag Ryuk sandsynligvis haft ansvaret for selve krypteringen og den efterfølgende forhandling omkring løsesum med offeret.

Det understøtter et generelt kompetenceløft i det cyberkriminelle miljø, hvor det i højere grad end før bliver specialister fremfor generalister, der udfører kriminelle cyberangreb.

Kompetenceløftet er med til at øge både omfanget og udbyttet af de cyberkriminelle angreb. Det afspejler sig bl.a. i det stigende udbytte fra målrettede ransomware-angreb, der kan indbringe millioner af kroner i løsesum til de kriminelle bagmænd.

Hvor den tidligere omtalte handel med specifikke ydelser bl.a. bidrager til at sænke barren for, hvem der kan begå cyberkriminalitet, da øger professionaliseringen og specialiseringen også produktiviteten blandt de aktører, der allerede udfører cyberkriminalitet.

Specialiseringen kan også øge robustheden i de kriminelle netværk. Når f.eks. myndighederne slår ned på en leverandør, vil det ofte kun ramme en del af forsyningskæden, som kan udskiftes, og ikke hele angrebskæden.

Cyberkriminelle kan skade den demokratiske proces
Amerikanske myndigheder har advaret om, at ransomware-angreb udgør en af de væsentligste trusler mod det amerikanske præsidentvalg i november 2020. Angreb mod myndigheder og software-udbydere, der eksempelvis administrerer vælgerdata, kan potentielt skabe kaos og mistillid til den demokratiske proces.

Selvom cyberkriminelle som udgangspunkt ikke har en selvstændig interesse i at påvirke det amerikanske valg, kan de alligevel skade tilliden til demokratiet og valgprocessen. Det kan ske, hvis de videresælger adgange til statsstøttede hackergrupper, der ønsker at påvirke valget, eller tilfældigt krypterer systemer hos myndigheder, der varetager centrale roller under valget.

Cyberkriminalitet herunder Crime-as-a-Service kan således indirekte udgøre en trussel mod den nationale sikkerhed. Derfor angreb U.S. Cyber Command (USCC) og efterfølgende Microsoft i samarbejde med en række internationale aktører i slutningen af september 2020 infrastrukturen omkring TrickBot malwaren. Selvom forstyrrelserne som følge af angrebene sandsynligvis kun er midlertidige, så er et af formålene bl.a. at svække mulighederne for at påvirke det amerikanske valg gennem denne malware.

Angrebet mod det kriminelle netværk er et udtryk for, hvad U.S. Cyber Command kalder ”persistent engagement”, der er en del af de amerikanske myndigheders strategi mod cybertruslen. Strategien forsøger på mere offensiv vis at bekæmpe cybertruslen – også fra kriminelle grupper.

Kryptovaluta bidrager til kommercialiseringen af den cyberkriminelle industri

Teknologier som kryptovaluta og værktøjer til anonymisering har givet profitable rammer for et mere udviklet kriminelt miljø med bedre muligheder for samarbejde.

De muligheder for at anonymisere finansielle transaktioner, som kryptovaluta giver, gør det sværere for myndigheder og it-sikkerhedsfolk at opspore hackerne via deres finansielle transaktioner.

Fælles valutaenheder på tværs af markeder og lande gør det også lettere at sammenligne priser og handle indbyrdes. Derfor bidrager brugen af kryptovaluta også til, at det bliver nemmere for kriminelle aktører at udveksle tjenester.

Når ofrene for ransomware og andre former for digital afpresning betaler, foregår det også typisk i form af kryptovaluta. Det betyder, at

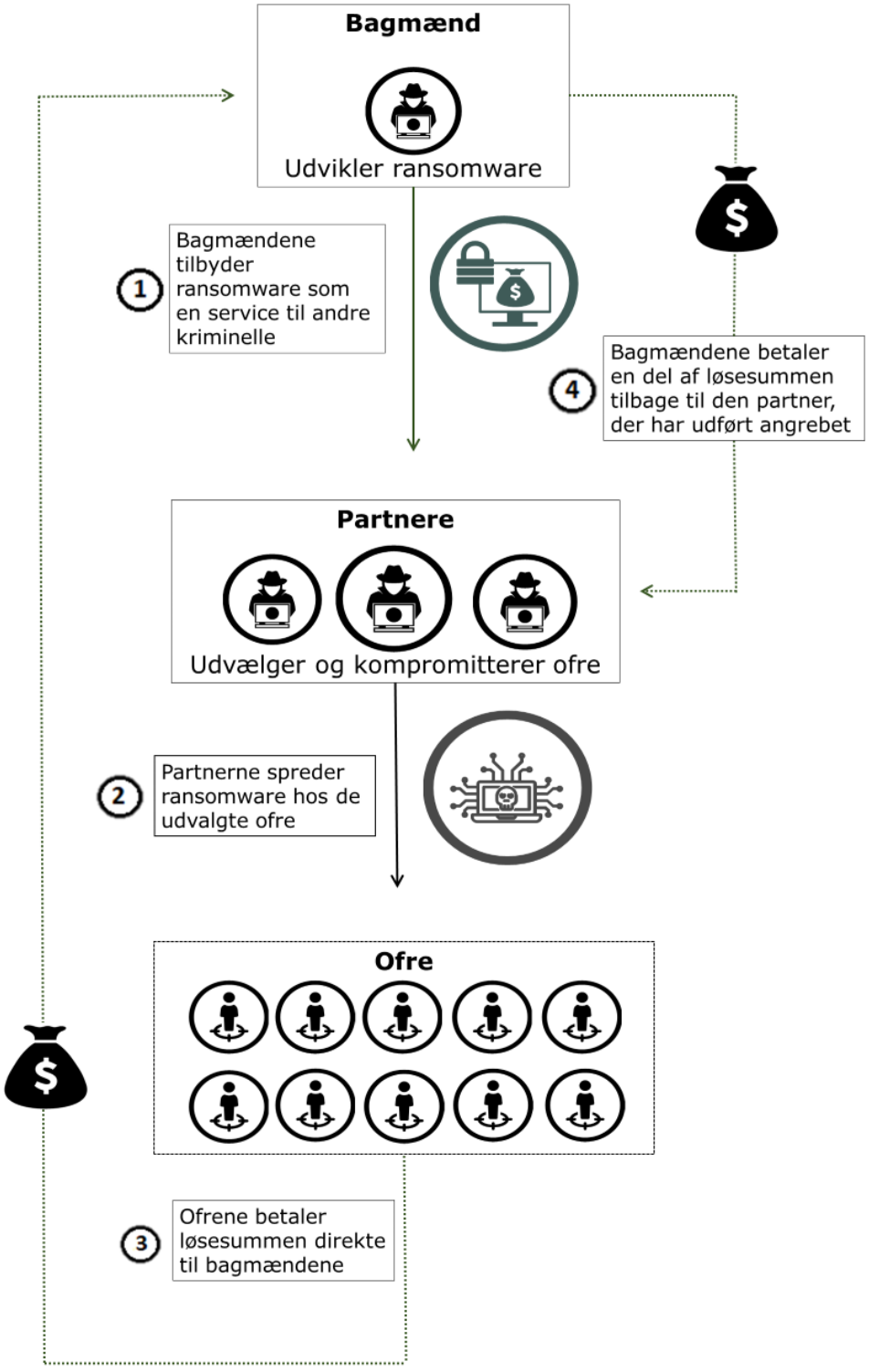
pengestrømmen gennem hele den cyberkriminelle værdikæde kan holdes anonym og digital.

Da de enkelte aktører i forsyningskæden således får nemmere ved at modtage betaling for deres specifikke bidrag til cyberkriminaliteten, understøtter brugen af kryptovaluta udviklingen mod et mere kommercialiseret og specialiseret cyberkriminelt miljø.

Ransomware-angreb som platformsøkonomi

Ransomware-as-a-Service (RaaS) er et andet eksempel på, at hackerne samarbejder mere organiseret og længerevarende. Forretningsmodellen bag RaaS efterligner på nogle punkter den platformsøkonomi, der findes på legale markeder. Transportvirksomheden Uber er et eksempel på en virksomhed, der specialiserer sig i at stille en platform til rådighed for udvalgte partnere, mod at platformsejeren selv modtager en procentdel af indtjeningen. I tilfældet RaaS er det løsesummen fra vellykkede angreb.

RaaS baserer sig på, at nogle bagmænd ejer en platform – oftest i form af malware eller infrastruktur. Hertil knytter de et netværk af partnere, der bruger platformen til ransomware-angreb. Løsesummerne fra de vellykkede angreb går oftest direkte til bagmændene, der efterfølgende sender en del af fortjenesten fra de vellykkede angreb tilbage til disse partnere. Det varierer fra netværk til netværk, hvor tæt knyttede partnere og bagmænd er, samt hvem der har det specifikke ansvar for f.eks. kontakt med ofrene. I de fleste tilfælde vil forretningsmodellen dog ligne illustrationen nedenfor.



Figur: Illustration af en typisk Ransomware-as-a-Service-forretningsmodel

Det er en forretningsmodel, der har fordele for både bagmændene og de kriminelle partnere. For bagmændene, der udvikler malware, er der en mindre risiko og en lavere arbejdsbyrde forbundet med dette, fordi det er partnerne, der har ansvaret for spredningen. RaaS kan derved give bagmændene en stabil indkomst med en relativt lav risiko.

Der er ransomware, som er programmeret sådan, at de ikke fungerer i en række lande, hvor bagmændene sandsynligvis opholder sig, herunder de tidligere Sovjetlande. Det er sandsynligvis for at beskytte bagmændene mod retsforfølgelse. Amerikanske myndigheder har i 2019 og 2020 beskyldt Rusland og Kina for at samarbejde med lokale cyberkriminelle.

For den kriminelle partner, der bruger malwaren, er der også flere fordele. Først og fremmest skal vedkommende ikke selv udvikle den malware, der bliver brugt i angrebet. Det medvirker bl.a. til at sænke tærsklen for, hvem der kan udføre cyberangreb.

GandCrab-netværket stjal platformsmodellen
Et af de første eksempler på RaaS som platformsmodel var GandCrab. Før GandCrab havde ransomware-grupper som udgangspunkt arbejdet i det skjulte og generelt forsøgt at undgå opmærksomhed. Da bagmændene bag GandCrab lancerede deres RaaS-program i starten af 2018, ændrede det sig.

Det er en forudsætning for forretningsmodellen bag RaaS, at der er rekrutterede partnere, der bruger platformen, som bagmændene stiller til rådighed. GandCrab-ransomware blev derfor lanceret med branding, marketing og personer, der stod for kommunikationen med partnere og ofre.

GandCrab blev derved et af de første offentligt kendte eksempler på, at kriminelle bagmænd kunne tjene penge på at tilbyde en platform til partnere for herefter at lade disse udføre det manuelle og risikable arbejde med at kompromittere ofre.

Tendensen mod et mere professionaliseret og organiseret samarbejde har de senere år også spredt sig til de dele af det kriminelle miljø, der udbyder RaaS. Det har medført, at bagmændene bag nogle RaaS-operationer opstiller skrappere kriterier for, hvem der kan bruge deres malware.

Det er f.eks. tilfældet med ransomwaren REvil, der er blevet brugt i flere profilerede angreb det sidste år. REvil viderefører konceptet fra GandCrab, og meget peger på, at der er flere sammenfald mellem bagmænd og partnere i de to RaaS-platforme. REvil adskiller sig dog fra GandCrab ved, at der bl.a. er et mere udtalt fokus på, hvem de vælger at indgå i samarbejde med. REvil baserer sig således på et netværk af nøje udvalgte, kvalificerede samarbejdspartnere.

En medvirkende årsag til denne udvikling er sandsynligvis den store usikkerhed, der kan være forbundet med CaaS og RaaS. Udvekslingen af tjenester internt i det kriminelle miljø indebærer – som tidligere beskrevet – en risiko for at blive snydt eller eksponeret.

REvil bruges hovedsageligt til målrettede ransomware angreb, hvor de kriminelle afpresser myndigheder og virksomheder for store pengebeløb ved at kryptere data på centrale it-systemer. Det stiller højere krav til de kriminelle partneres evner og håndtering af ofrene i forbindelse med f.eks. afpresning.

De skrappere udvælgelseskriterier er sandsynligvis derfor både et spørgsmål om tillid og kompetencebehov.

Internationalt samarbejde bekæmper ransomware
Det Nationale Cyber Crime Center (NC3), der er Rigspolitiets center for cyberkriminalitet, samarbejder med flere internationale partnere for at modarbejde kriminelle, der bruger ransomware.

NC3 deltager bl.a. i projektet No More Ransom. Projektet har et mål om at hjælpe ofre for ransomware med at få deres krypterede data tilbage uden at blive nødt til at betale de kriminelle. No More Ransom-projektet arbejder også for at udbrede den generelle viden om ransomware.

I sommeren 2019 beskrev Europol, hvordan No More Ransom-projektet havde hjulpet mere end 200.000 ofre for ransomware og sikret, at mere end 100 millioner amerikanske dollars ikke er havnet i de kriminelles lommer.

Du kan læse mere om projektet her: www.nomoreransom.org

Udviklingen øger truslen fra målrettede ransomware-angreb

CFCS har i tidligere vurderinger advaret mod en stigende trussel fra målrettede ransomware-angreb. Angrebene er bl.a. målrettede i den forstand, at hackerne angriber store eller samfundsvigtige myndigheder og virksomheder. Hackerne forventer, at sådanne myndigheder og virksomheder er villige til at betale en meget stor løsesum.

Udviklingen indenfor CaaS og RaaS har bidraget til den stigende trussel fra målrettede ransomware-angreb.

RaaS-platforme som REvil har specialiseret sig i målrettede ransomware-angreb, der kan give store afkast. Løsesummen for ransomware-angreb begået med REvil er betydeligt højere end de operationer, der benyttede sig af GandCrab. Der har været løsesumskrav på op imod 42 millioner amerikanske dollars for et enkelt angreb begået med REvil.

Det afspejler en generel tendens. I oktober sidste år rapporterede Europol om et fald i det samlede antal af ransomware-angreb. Sideløbende er der dog sket en stigning i den gennemsnitlige løsesum, som ofrene for cyberangreb har betalt for at få data dekrypteret.

Disse tal er dog behæftet med en vis usikkerhed, da ofre for ransomware sjældent melder betalte løsesummer ud til offentligheden. CFCS vurderer dog, at udviklingen er sandsynlig, da flere offentligt kendte sager afspejler den udvikling.

Truslen underbygges af, at den kriminelle industri kontinuerligt opruster og udvikler produkter og metoder. Kriminelle netværk opdaterer således krypteringsværktøjer og malware løbende, så de er i stand til at omgå sikkerhedsforanstaltninger, som deres ofre har taget for at imødegå disse typer angreb.

Den kriminelle industri vil grundet arbejdsdelingen fortsat opretholde evnen til i fremtiden at udføre brede angreb mod alle brugere af internettet i form af f.eks. organiserede phishingkampagner. På samme tid medfører udviklingen sandsynligvis, at visse typer af kriminelle cyberangreb bliver yderligere målrettede. De succesfulde angreb vil derfor sandsynligvis være mere profitable for de kriminelle og skabe større økonomisk skade hos ofrene.

Vil du vide mere?
Du kan læse mere om den generelle trussel fra cyberkriminalitet i udgivelsen *Cybertruslen mod Danmark 2020*.

Du kan læse mere om truslen fra målrettet ransomware i udgivelserne *Anatomien af målrettede ransomware-angreb* og *Digitale gidseltagere på storvildtjagt.*

Publikationerne kan findes på CFCS's hjemmeside.