CENTER FOR CYBERSIKKERHED

Trusselsvurdering:

Fjern adgangen

Hackere kompromitterer sårbare fjernadgange og sælger dem videre til andre kriminelle, som udnytter dem til målrettede ransomware-angreb

1. udgave december 2021

Trusselsvurdering: Fjern adgangen

Formål
Formålet med trusselsvurderingen er at give læseren en forståelse af det cyberkriminelle økosystem og en indsigt i en af de indledende faser i et målrettet ransomware-angreb. Vurderingen er målrettet personer med ansvar for cybersikkerhed i danske myndigheder og virksomheder.

Hovedvurdering

- Truslen fra cyberkriminalitet er **MEGET HØJ.** Hackere specialiseret i at kompromittere og videresælge fjernadgange hos myndigheder og virksomheder understøtter truslen fra cyberkriminalitet generelt og ransomware-truslen i særdeleshed.

- CFCS vurderer, at nogle af de mest aktive kriminelle hackergrupper i øjeblikket bruger fjernadgange som udgangspunkt for deres ransomware-angreb.

- Det er især de hackere, som bruger Ransomware-as-a-Service (RaaS)-platforme til at udføre deres målrettede ransomware-angreb, der er med til at drive efterspørgslen efter kompromitterede fjernadgange.

- Online hackerfora fungerer som centrale markedspladser, hvor kriminelle kan videresælge bl.a. kompromitterede fjernadgange.

- Salget af kompromitterede fjernadgange er en del af en bevægelse, hvor dele af det cyberkriminelle miljø udvikler sig fra fortrinsvis at basere sig på relationer til i højere grad at basere sig på udbud og efterspørgsel.

- Muligheden for at købe services som ransomware og kompromitterede fjernadgange bidrager til en arbejdsdeling i det kriminelle miljø, der understøtter truslen fra cyberkriminalitet mod Danmark. Samtidigt gør den dog de cyberkriminelle aktører mere afhængige af centrale, online markedspladser.

- Nedlukning og distancearbejde i forlængelse af COVID19-pandemien har øget hackernes muligheder for at angribe via kompromitterede fjernadgange. Når arbejdspladserne flytter hjem i stuen, kan det skabe sårbarheder, som de kriminelle hackere kan misbruge til bl.a. ransomware-angreb.

Analyse

Målrettede ransomware-angreb er en alvorlig trussel mod danske virksomheder og myndigheder. Den generelle trussel fra cyberkriminalitet er **MEGET HØJ.**

Hackere, der udfører målrettede ransomware-angreb, misbruger bl.a. kompromitterede fjernadgange i deres angreb. I løbet af 2021 har hackere, der bruger Ransomware-as-a-Service (RaaS)-platforme som Darkside, Egregor, LockBit og REvil, eksempelvis udnyttet kompromitterede fjernadgange i flere af deres angreb.

CFCS vurderer, at der er flere underliggende faktorer, som har bidraget til, at nogle af de mest aktive kriminelle hackergrupper i øjeblikket bruger fjernadgange i deres ransomware-angreb.

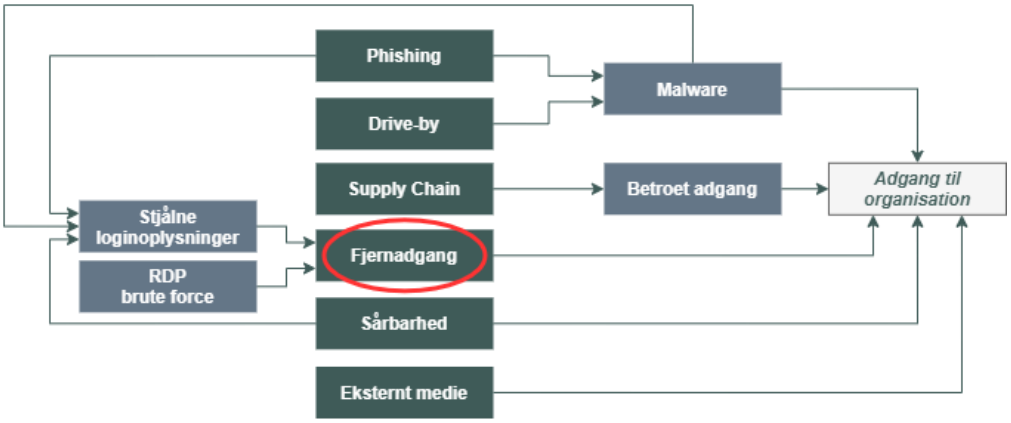
I 2021 er der dukket flere mindre servicerede RaaS-platforme op. De hackere, der gør brug af disse mindre servicerede RaaS-platforme, vil oftest selv skulle finde og skaffe adgange til ofre. Det driver efterspørgslen efter kompromitterede fjernadgange.

Samtidigt fungerer hackerfora på dark web (det mørke net) som centrale markedspladser. I flere år har de faciliteret en udveksling af ydelser og tjenester online. Disse fora gør det muligt for hackere, der er specialiseret i at kompromittere fjernadgange, at videresælge deres adgange. Det har skabt et stabilt udbud af kompromitterede fjernadgange.

Den tredje faktor, som har bidraget til den hyppige brug af kompromitterede fjernadgange i ransomware-angreb, er COVID19-pandemien. Pandemien skabte et akut behov for at opretholde produktion og serviceniveau hjemmefra i de fleste myndigheder og virksomheder. Brugen af fjernadgange er siden blevet en integreret del af mange organisationers hverdag. Det har været med til at øge angrebsfladen for de hackere, der kompromitterer fjernadgange.

De hackere, der videresælger loginoplysninger til fjernadgange eller på anden vis etablerer adgang på vegne af andre hackere, bliver i it-sikkerhedskredse kaldt for *Initial Access Brokers*. De arbejder konstant med at finde huller og forsøger så at komme ind via usikre adgangskoder, såkaldte information-stealers, der stjæler loginoplysninger, eller kendte sårbarheder i fjernadgangsopsætningerne.

Kriminelle arbejder specialiseret med at hacke og videresælge fjernadgange
Hacking og videresalg af kompromitterede fjernadgange til netværk hos myndigheder og virksomheder udgør i dag en vigtig del af det cyberkriminelle økosystem. De kompromitterede adgange bliver bl.a. udnyttet af kriminelle hackere til at begå målrettede ransomware-angreb.



Figur 1: *Typiske metoder hackerne opnår indledende adgang på med fokus på fjernadgange. (Kilde: Anatomien af målrettede ransomware-angreb).*

I et målrettet ransomware-angreb er hackernes første mål at opnå indledende adgang til deres offer og misbruge adgangen som et brohoved i det videre angreb. CFCS har tidligere beskrevet, hvordan hackere kan udnytte bestemte typer malware til at installere ransomware på ofres systemer. Alternativt kan hackerne udnytte mulighederne for at få adgang til organisationers interne netværk via eksterne fjernadgangssystemer såsom Remote Desktop Protocol (RDP) eller Virtual Private Network (VPN).

Fire måder fjernadgange bliver misbrugt på
Hackerne udnytter overordnet fjernadgangssystemerne på fire forskellige måder.

I den første metode franarrer hackerne loginoplysninger til fjernadgangssystemer gennem phishingangreb.

Den anden metode involverer udnyttelse af sårbarheder i selve fjernadgangsløsningernes software til at fremskaffe loginoplysninger på organisationens brugere.

I den tredje metode bruger hackerne brute force for at udnytte, at nogle RDP-opsætninger ikke er sat op med tilstrækkelig sikkerhed. Hackerne udnytter, at nogle RDP-fjernadgangsforbindelser ikke gemmes bag en RDP-Gateway eller ikke tilgås gennem en VPN-forbindelse. Uden ekstra sikkerhedsforanstaltninger er det eneste, der holder hackerne tilbage ved disse opsætninger, typisk kun ét kodeord.

Den sidste metode er de såkaldte information-stealers, der er en malware, som eksempelvis er blevet spredt via phishing, og som kan bruges til at stjæle login-oplysninger.

Ofte vil Inital Access Brokers, der kompromitterer de indledende fjernadgange, ikke selv udføre ransomware-angreb men i stedet sælge fjernadgangen videre til andre hackere, der udfører det egentlige ransomware-angreb.

Ved at understøtte og muliggøre andre hackeres angreb indtager Initial Access Brokers således en vigtig rolle i det cyberkriminelle økosystem. En rolle som ikke er blevet mindre aktuel af, at flere hackere er begyndt at bruge RaaS-platforme til at udføre målrettede ransomware-angreb de seneste par år.

RaaS: Ransomware-angreb som platformsøkonomi
Både Egregor, LockBit og REvil er eksempler på ransomware, der er blevet udbudt som såkaldt Ransomware-as-a-Service (RaaS).

RaaS er et underkoncept af Crime-as-a-Service (CaaS), der 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. RaaS har introduceret en form for platformsøkonomi til cyberkriminalitet, hvor hackerne gennem ransomware-angreb samtidigt tjener penge til sig selv og til de bagmænd, der ejer platformen.

Rekruttering til platformene og samarbejdet mellem hackerne sker bl.a. gennem hackerfora på dark web.

Mindre servicerede RaaS-platforme driver efterspørgslen
CFCS vurderer, at der er forskel på, hvor servicerede de forskellige RaaS-platforme er. Nogle RaaS-platforme forsøger at stille så mange ressourcer til rådighed for deres partnere som muligt. Andre tilbyder færre services, men er typisk nemmere og billigere for hackerne at få adgang til. I 2021 er flere mindre servicerede RaaS-platforme dukket op og er blevet populære. De hackere, der gør brug af mindre servicerede RaaS-platforme, vil f.eks. oftest selv skulle finde og skaffe adgange til ofre. Det driver efterspørgslen efter kompromitterede fjernadgange.

Én af disse mindre servicerede RaaS er Lockbit. Her betaler de kriminelle for retten til at bruge LockBit-ransomwaren, men hackerne skal selv skaffe sig adgang til potentielle ofre og afpresse disse. Denne type af "gør-det-selv-ransomware" er på denne måde med til at drive efterspørgslen efter afgrænsede ydelser som kompromitterede fjernadgange, der kan give de kriminelle adgang til de potentielle ofre.

I modsætning hertil er der andre RaaS-platforme, hvor de kriminelle ikke bare køber retten til at bruge en ransomware, men også får andre tjenester med i købet. De kan eksempelvis få adgang til bl.a. andre typer malware eller et stort antal ofre, som bagmændene allerede har kompromitteret. Denne type RaaS-platforme er som udgangspunkt dyrere og sværere at få adgang til.

CFCS vurderer, at de hackere, der benytter sig af mindre servicerede RaaS-platforme, ofte agerer uden faste samarbejdsaftaler. De hackere, der benytter sig af de mere servicerede RaaS-platforme er ofte en del af mere komplekse operationer, der afføder

længere samarbejder mellem hackere specialiseret i online infrastrukturer, udviklingen og spredningen af malware og andre værktøjer.

Det er et udtryk for den bevægelse, hvor dele af det cyberkriminelle miljø udvikler sig fra fortrinsvis at basere sig på relationer til i højere grad at basere sig på udbud og efterspørgsel.

Mulighederne for at købe kompromitterede fjernadgange fra Initial Access Brokers og udbuddet af forskellige typer RaaS-platforme bidrager generelt til at sænke barren for, hvem der kan udføre ransomware-angreb. Kravene til den enkelte kriminelles it-kompetencer bliver mindre, når de kan købe sig til den malware eller de tjenester, som de ikke selv har mulighed for eller evner til at udføre.

Initial Access Brokers styrker det cyberkriminelle miljø
Initial Access Brokers er finansielt motiverede og sælger som udgangspunkt de kompromitterede fjernadgange til den højeste byder.

Initial Access Brokers bidrager til en arbejdsdeling i det kriminelle miljø. Arbejdsdelingen gør det muligt for den enkelte hacker at specialisere sig inden for et afgrænset felt. Det kan derfor sammenlignes med klassiske produktionsvirksomheder, der udnytter specialiserede leverandører til at arbejde mere effektivt.

Selvom Initial Access Brokers udgør en vigtig del af andre hackeres angreb, så indtager de generelt en af de nederste pladser i det kriminelle økosystems fødekæde.

Initial Access Brokers er første led i en værdikæde, hvor udbyttet fra ransomware-angreb i første omgang bliver delt mellem de hackere, der udfører selve ransomware-angrebet, og de bagmænd, der driver ransomware-platformen. Ofte anvender Initial Access Brokers ikke avancerede teknikker eller værktøjer. I stedet udnytter de kommercielle værktøjer, relativt simple angrebsteknikker og allerede kendte sårbarheder, når de skaffer adgange.

Denne forretningsmodel indebærer, at Initial Access Brokers er afhængige af, at der er nogle, som er villige til at købe adgangene. De er derfor grundlæggende afhængige af en udveksling med andre cyberkriminelle aktører.

Markedspladser er en forudsætning for køb og salg af adgange
Køb og salg af kompromitterede fjernadgange forudsætter markedspladser, hvor eksempelvis hackerforaene XSS og Exploit har været populære. Flere ændringer i miljøet i 2021 har dog tvunget noget af den aktivitet over på andre fora. Her har især forummet RAMP rekrutteret medlemmer fra Exploit og XSS, der forbød ransomware-relateret indhold på deres fora. Det er muligt at læse mere om disse ændringer i CFCS' trusselsvurdering "Gamle hackere på nye platforme".

Denne migration afslørede en gensidig afhængighed, som sandsynligvis forstærkes af det cyberkriminelle miljøs bevægelse mod en højere grad af specialisering. Således har Initial Access Brokers brug for en markedsplads, hvor de kan videresælge de kompromitterede adgange, mens de aktører, der udfører ransomware-angreb med disse adgange, har behov for markedspladsen til at erhverve fremtidige adgange.

Hackerfora, som XSS og Exploit, har indtil nu fungeret som en formidler, der varetog denne gensidige afhængighed. Da XSS og Exploit i sommer forbød ransomware-relateret indhold på deres platforme, og antallet af nye ofre for ransomware-angreb simultant hermed faldt i en periode, afdækkede det sandsynligvis en grundlæggende sårbarhed i de kriminelles afhængighed af centrale, online markedspladser.

Den gensidige afhængighed mellem Initial Access Brokers og hackere, der laver ransomware-angreb, bliver også synliggjort af, at nogle bagmænd og hackere bag RaaS-platforme åbent efterspørger bestemte typer adgange. Bagmændene bag ransomwaren LockBit har eksempelvis efterspurgt adgang til amerikanske virksomheder med en omsætning på minimum 100 mio. USD.

Nedlukning og distancearbejde har øget angrebsfladen for hackerne
Nedlukningen af det danske samfund i foråret og vinteren 2020 skabte et akut behov for at opretholde produktion og serviceniveau hjemmefra i de fleste myndigheder og virksomheder. Dén omstilling krævede for mange organisationer hurtige beslutninger om etablering eller udvidelse af fjernadgange og digitale løsninger til online samarbejde.

Når arbejdspladserne flytter hjem i stuen, kan det skabe udfordringer for it-sikkerheden. Når computere uden for organisationens digitale perimeter får adgang til dens it-netværk, kan de blive en genvej ind for hackere og øger derved organisationens angrebsflade. Det kan for eksempel ske, hvis fjernadgange ikke opdateres eller er sat op uden tilstrækkeligt hensyn til sikkerhed eller monitering.

Det har givet nye muligheder for de hackere, der arbejder som Initial Access Brokers. De arbejder fokuseret med at finde huller og forsøger så at komme ind via kendte sårbarheder, malware, der stjæler loginoplysninger, eller usikre adgangskoder, for som beskrevet i sidste ende at tjene penge på at sælge den videre til andre hackergrupper.

En utilstrækkelig sikring af hjemmearbejdspladser og fjernadgange kan således blive et udgangspunkt for et målrettet ransomware-angreb mod organisationen.

Råd til sikring af fjernadgange i organisationen
CFCS anbefaler, at myndigheder og virksomheder tager nedenstående råd med i deres overvejelser om anvendelsen af fjernadgange:

- Organisationen bør gennem en segmentering af organisationens infrastruktur sikre, at fjernadgang kun sker til de dele af infrastrukturen, som en risikovurdering har afdækket er acceptabel.
- Organisationen bør sikre, at medarbejderes og leverandørers fjernadgang til organisationens interne systemer sker over krypterede forbindelser og ved anvendelse af fler-faktor-autentifikation.
- RDP-servere bør ikke være direkte tilgængelige fra internettet. De bør kun kunne tilgås via en fler-faktor beskyttet VPN-løsning, eller via en anden gateway, der sikrer fler-faktor autentifikation, inden adgang gives.

- Organisationer bør sikre, at anvendt software holdes opdateret til nyeste versioner. Dette gælder i denne sammenhæng specielt software relateret til brugen af VPN, RDP, samt gateways og understøttende systemer.
- Adgang til organisationens systemer bør altid baseres på stærke passwords. Ofte-anvendte eller tidligere lækkede passwords bør ikke tillades. Se i den forbindelse evt. CFCS' passwordvejledning.
- Brugerkonti bør låses ude ved gentagen indtastning af forkert password.
- Organisationer bør sikre tilstrækkelig og anvendelig logning. Det gælder i denne sammenhæng specielt de systemer, der er tilgængelige via fjernadgang, samt de understøttende systemer som eksempelvis gateways og autentifikationsservere mv. Loggene bør aktivt monitoreres, så en eventuel kompromittering kan opdages hurtigt.
- Organisationen bør løbende sikre, at brugerkonti lukkes, når en medarbejders ansættelsesforhold ophører. Brugerkonti relateret til leverandører og samarbejdspartnere bør kun tildeles personligt, og kun holdes åbne, så længe den konkrete opgave kræver adgang.
- Organisationen bør sikre, at muligheden for fjernadgang kun tillades for brugere, der har et reelt behov herfor.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og plan-lægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynligheder i analyser

Usandsynligt | **Mindre sandsynligt** | **Muligt** | **Sandsynligt** | **Meget sandsynligt**

"FE vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.

Andre relevante publikationer

Center for Cybersikkerhed (CFCS) udgiver løbende vejledninger og trusselsvurderinger. Nedenfor er fremhævet en række produkter af særlig relevans for truslen fra cyberkriminalitet. Alle produkterne er tilgængelige på CFCS' hjemmeside.

Samarbejdet mellem cyberkriminelle
Trusselsvurderingen "Drømmer cyberkriminelle om tillidsfulde relationer?" beskriver, hvordan veletablerede samarbejdsrelationer, arbejdsdeling og udveksling af tjenester i det kriminelle miljø bidrager til den meget høje trussel fra cyberkriminalitet i almindelighed og målrettede ransomware-angreb i særdeleshed. Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/organiseret-cyberkriminalitet/

Oprustningen i det cyberkriminelle miljø
Trusselsvurderingen "Gamle hackere på nye platforme" giver en opdateret forståelse af truslen fra ransomware-angreb efter det meget medieomtalte angreb mod det amerikanske olieselskab Colonial Pipeline i maj, og det efterfølgende øgede pres fra USA mod hackere, der udfører ransomware-angreb. Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/trusselsvurdering-cyberkriminelle-gamle-hackere-på-nye-platforme/

Kriminelle opruster i pandemiens skygge
I trusselsvurderingen "Kriminelle opruster i pandemiens skygge" kan du læse mere om, hvordan de cyberkriminelle tidligere har fornyet deres værktøjer, samarbejdsrelationer og aktiviteter. Læs vurderingen her
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/trusselsvurdering-cyberkriminelle-opruster-i-pandemiens-skygge/

Truslen fra målrettede ransomware-angreb
Trusselsvurderingen "Digitale gidseltagere på storvildtjagt" beskriver truslen fra målrettede ransomware-angreb, der kan have alvorlige konsekvenser for en organisation. Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/malrettet-ransomware/

Anatomien af målrettede ransomware-angreb
Undersøgelsesrapporten "Anatomien af målrettede ransomware-angreb" beskriver, hvordan ransomware-angreb typisk forløber, og hvordan organisationer kan beskytte sig imod dem. Læs rapporten her:
https://cfcs.dk/da/cybertruslen/rapporter/anatomien-i-ransomware-angreb/

Reducér risikoen for ransomware
I vejledningen "Reducér risikoen for ransomware" kan du læse mere om en række anbefalinger, som organisationer bør overveje for at reducere risikoen for at blive ramt af et ransomware-angreb samt mindske konsekvenserne ved et evt. angreb. Læs vejledningen her: https://cfcs.dk/da/forebyggelse/vejledninger/ransomware/

Password-sikkerhed
Vejledningen Password-sikkerhed giver en række anbefalinger og tips til, hvordan sikkerheden i og omkring passwords kan højnes og derved øge organisationens sikkerhedsniveau.
Den omhandler blandt andet emner som passwordstyrke, passwordpolitik, flerfaktorautentifikation, password managers og awareness.
Læs vejledningen her: https://www.cfcs.dk/da/forebyggelse/vejledninger/passwords/

CENTER FOR CYBERSIKKERHED

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