CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Gamle hackere på nye platforme

Ransomware-miljøet omorganiserer sig efter pres udefra

1. udgave september 2021

Formål
Trusselsvurderingen sætter fokus på det kriminelle miljø, der understøtter og udfører ransomware-angreb. Dele af det kriminelle miljø har været under omorganisering, bl.a. efter pres fra de amerikanske myndigheder. Formålet med trusselsvurderingen er derfor at give beslutningstagere i virksomheder og myndigheder en opdateret forståelse af truslen fra ransomware-angreb.

Hovedvurdering

- Den overordnede trussel fra cyberkriminalitet er fortsat **MEGET HØJ**. Det er fortsat meget sandsynligt, at danske organisationer vil blive ramt af målrettede ransomware-angreb inden for de næste år.

- Det kriminelle miljø, der står bag Ransomware-as-a-Service (RaaS), er under omorganisering efter ransomware-angrebet på det amerikanske olieselskab Colonial Pipeline i maj 2021.

- Flere RaaS-bagmænd har enten permanent eller kortvarigt lukket deres platforme, og flere førende hacker-fora har indført forbud mod rekruttering på deres platforme.

- Forandringerne betød, at antallet RaaS-angreb faldt en kort periode henover sommeren 2021. Dette hul er dog siden blevet fyldt ud af andre RaaS-udbydere.

- Flere af de erfarne kriminelle er sandsynligvis ikke stoppet med at hacke men har bare skiftet platform, hvilket betyder, at antallet af RaaS-angreb igen nærmer sig niveauet fra før angrebet på Colonial Pipeline.

- Det har understreget robustheden i de kriminelle netværks forsyningskæder, hvor dele af kæden kan udskiftes, uden det for alvor forstyrrer eller skader de kriminelle aktiviteter.

- Reaktionen fra de amerikanske myndigheder efter angrebet på bl.a. Colonial Pipeline har sandsynligvis afskrækket nogle af de kriminelle fra på kort sigt at gå målrettet efter kritisk infrastruktur, særligt i USA. Det er dog ikke nogen garanti for, at angreb ikke vil ske.

USA har øget presset på ransomware-hackere
Truslen fra cyberkriminalitet er fortsat **MEGET HØJ**. Det er fortsat meget sandsynligt, at danske organisationer vil blive ramt af målrettede ransomware-angreb inden for de næste år.

Det kriminelle miljø, der står bag RaaS-angreb, er imidlertid under omorganisering efter ransomware-angrebet mod det amerikanske olieselskab Colonial Pipeline i maj 2021.

Angrebet var den første i en række af begivenheder i midten af 2021, som har bidraget til at skabe flere ændringer i RaaS-miljøet og føjet nye nuancer til trusselsbilledet.

Angrebet, som blev udført af hackere med tilknytning til RaaS-platformen Darkside, påvirkede store dele af den amerikanske østkysts brændstofforsyning. Det tydeliggjorde, hvordan cyberkriminelle angreb også kan få konsekvenser, der rækker ud over de økonomiske tab, som den ramte organisation lider.

Efterfølgende blev den amerikanske afdeling af fødevaregiganten JBS samt it-virksomheden Kaseya udsat for meget omfattende ransomware-angreb. Disse angreb blev udført af hackere bag RaaS-platformen REvil.

De amerikanske myndigheder har siden reageret kraftigt på disse angreb. Indsatsen mod truslen fra ransomware-angreb er kommet i indenrigspolitisk fokus og opprioriteret, så den nu kan efterforskes som en trussel mod den nationale sikkerhed, på samme måde som det er tilfældet med terrortruslen. Det betyder blandt andet, at indsatsen vil blive genstand for en whole-of-government tilgang, hvor alle myndigheder skal bistå hinanden og koordinere indsatsen.

Ransomware-angreb kom samtidig på den udenrigs- og sikkerhedspolitiske dagsorden. Her kritiserede USA Rusland på præsidentniveau for ikke at gøre nok mod de kriminelle hackere, som amerikanerne mener opholder sig i Rusland. Amerikanske myndigheder meldte også ud, at selvom de kriminelle opholder sig på russisk jord, vil de amerikanske myndigheder sætte ind over for dem, hvis Rusland ikke selv gør det. USA har i den forbindelse udpeget ransomware-angreb mod 16 navngivne samfundskritiske sektorer som værende særligt alvorlige, og hvor man fra amerikansk side forbeholder sig retten til at svare igen med midler og på et tidspunkt, man fra amerikansk side finder passende.

Som et direkte virkemiddel over for hackerne forsøger de amerikanske myndigheder at ramme dem økonomisk. Kort efter angrebet mod Colonial Pipeline beslaglagde de bitcoins svarende til over 2 mio. dollars fra bagmændene bag angrebet. I slutningen af september 2021 har det amerikanske finansministerium for første gang nogensinde indført sanktioner mod at handle på en specifik kryptobørs, som myndighederne bl.a. beskylder for at blive brugt til at håndtere løsesummer i forbindelse med ransomware-angreb. Sanktionerne vil blokere for al handel mellem den russiske kryptobørs Suex og amerikanske selskaber. Formålet med dette indgreb er at gøre det sværere for hackerne at modtage betaling for deres angreb og tjenester, og skal ses som et led i den nye prioriterede tilgang mod ransomware-angreb.

Ransomware-angreb som platformsøkonomi
Både Darkside og REvil er eksempler på ransomware, der er blevet udbudt som 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 det mørke net (dark web).

Ændringer i RaaS-miljøet efter Colonial Pipeline-angrebet
I løbet af sensommeren 2021 er der sket flere væsentlige ændringer i RaaS-miljøet.

Mest markant lukkede bagmændene bag flere dominerende RaaS-platforme, herunder REvil, Avaddon og Darkside, sine platforme ned. Mens Avaddon og Darkside fortsat er lukket ned, blev REvil reaktiveret i midten af september 2021 efter omkring to måneders pause.

Samtidigt forbød to centrale russisksprogede dark web hackerfora, Exploit og XSS, RaaS-bagmændene at rekruttere hackere på deres fora. Disse fora har tidligere spillet en central rolle i rekrutteringen af hackere til RaaS-platformene samt til udvekslingen af tjenester, adgange og værktøjer, der bliver brugt i målrettede ransomware-angreb.

Der er også tidligere eksempler på, at dele af det kriminelle miljø udvider eller udskifter deres malware-arsenal. Det skete eksempelvis i foråret og sommeren 2020 under Covid-19 pandemien, hvor flere kriminelle hackergrupper fornyede deres værktøjer, samarbejdsrelationer og aktiviteter.

De relativt samtidige og pludselige ændringer i RaaS-miljøet skyldes i denne omgang sandsynligvis især det øgede pres, som de amerikanske myndigheder har lagt på flere kriminelle grupper efter ransomware-angrebet mod Colonial Pipeline, og risikoen for et indgreb fra russiske myndigheder mod hackermiljøet i Rusland.

Hackerne samarbejder og hacker videre fra andre platforme
Nedlukningen af flere RaaS-platforme og forbuddet mod at rekruttere hackere på førende hackerfora førte til et fald i antallet af nye ofre for ransomware-angreb i løbet af sommeren 2021.

CFCS har før rapporteret om, at kriminelle hackere generelt er gode til at omstille sig og tænke nyt, når de bliver presset udefra eller ser nye muligheder for at tjene penge. Det tomrum, som fraværet af de tidligere meget brugte platforme skabte, er hurtigt blevet udfyldt af andre grupper, der har været interesserede i at udbygge deres RaaS-platform.

Det gælder især for RaaS-platformen LockBit. LockBit har været brugt i flere medieomtalte angreb sommeren over. Det er sandsynligt, at flere af de erfarne kriminelle, der tidligere har været hackere for bl.a. Darkside, Avaddon og REvil, er skiftet til at hacke for LockBit. Det har været medvirkende til, at antallet af angreb med LockBit er steget kraftigt de seneste måneder.

Niveauet for angreb med RaaS nærmer sig nu niveauet fra før Colonial Pipeline-angrebet. Det har understreget robustheden i de kriminelle netværks forsyningskæder, hvor dele af kæden kan udskiftes, uden det for alvor forstyrrer eller skader de kriminelle aktiviteter.

Bagmændene går i charmeoffensiven for at lokke hackere til

Bagmændene bag LockBit har været særligt udadvendte og offentligt synlige under reorganiseringen denne sommer. Gruppen bag RaaS-platformen har deltaget i interviews i flere medier. Her har de reklameret for deres platform, deres arbejdsdeling, og hvem de angriber.

LockBit har bl.a. været i stand til at rekruttere hackere via forummet Russian Anonymous Marketplace (RAMP), der sandsynligvis er etableret af tidligere RaaS-bagmænd. RAMP rekrutterer aktuelt medlemmer fra Exploit og XSS og skaber således et ideelt mødested for RaaS-hackere og -bagmænd.

I nylige interviews i medierne hævdede en bagmand for LockBit, at de ikke vil angribe organisationer, der arbejder inden for uddannelses- eller sundhedssektoren, ligesom de har hævdet, at de ikke vil ramme organisationer, der arbejder med velgørenhed.

Der har været lignende udmeldinger i 2020, hvor flere RaaS-grupper eksempelvis under Covid-19 pandemien udtalte, at de ikke ville angribe mål i sundhedssektoren. I løbet af pandemien var der dog flere eksempler på målrettede ransomware-angreb mod sundhedssektoren i udlandet.

Kriminelle, der udfører ransomware-angreb, laver konstant afvejninger af risiko og fortjeneste. Det illustreres bl.a. af, at langt størstedelen af grupperne eksempelvis ikke angriber mål i Rusland og lande, der tidligere var en del af Sovjetunionen, hvor flere af bagmændene og deres hackere sandsynligvis opholder sig.

Det er sandsynligt, at udmeldingen fra LockBit-bagmændene både skal ses som et udtryk for risikohåndtering og som et reklamefremstød for at rekruttere nye hackere og samarbejdspartnere snarere end samfundssind.

Reaktionen fra de amerikanske myndigheder efter angrebet på bl.a. Colonial Pipeline har sandsynligvis afskrækket nogle af de kriminelle fra på kort sigt at gå målrettet efter kritisk infrastruktur, særligt i USA.

Ligesom der var angreb mod sundhedssektoren under Covid-19 pandemien, så vurderer CFCS, at de kriminelle sandsynligvis kun vil holde sig fra at angribe de pågældende sektorer, så længe de mener, at risikoen vejer tungere end fortjenesten.

Det er derfor ikke nogen garanti mod angreb i de samfundsvigtige sektorer, at en kriminel aktør lige nu har udtalt, at de ikke vil forsøge at ramme mål i bestemte sektorer. Andre kriminelle hackere kan være villige til i stedet at gøre det, eller de kriminelle kan ombestemme sig, hvis de vurderer, at fortjenesten overstiger risikoen.

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 planlægning. 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
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/

CENTER FOR CYBERSIKKERHED

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

1. udgave september 2021