CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Kriminelle spænder den digitale tommelskrue

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave december 2020

Kriminelle spænder den digitale tommelskrue

Trusselsvurderingen informerer beslutningstagere i danske myndigheder og virksomheder om truslen fra såkaldt dobbelt afpresning, hvor hackere truer med at lække stjålet information i forbindelse med ransomware-angreb.

Hovedvurdering

- Målrettede ransomware-angreb, hvor kriminelle afpresser myndigheder og virksomheder for store pengebeløb ved at kryptere data på centrale it-systemer, er en del af trusselsbilledet, også for danske myndigheder og virksomheder.

- Kriminelle hackere har siden efteråret 2019 udvidet afpresningen ved også at true med at lække eller sælge følsom information stjålet i forbindelse med angrebet. Kombinationen af ransomware-angreb og trusler om læk kaldes for dobbelt afpresning.

- Dobbelt afpresning blev først brugt mod ofre i USA, men afpresning mod en dansk virksomhed i september 2020 viser, at danske myndigheder og virksomheder også kan blive ramt.

- Dobbelt afpresning udgør ikke kun en meget væsentlig trussel mod de myndigheder og virksomheder, der udsættes for ransomware-angreb, men også for de kunder, samarbejdspartnere og borgere, der risikerer at få følsomme oplysninger lækket eller solgt.

Analyse: Dobbelt afpresning er en ny normal

Målrettede ransomware-angreb, hvor kriminelle afpresser myndigheder og virksomheder for store pengebeløb ved at kryptere data på centrale it-systemer, har i de seneste år været et globalt fænomen. Der har siden 2019 været flere ofre for målrettede ransomware-angreb i Danmark.

Truslen fra målrettede ransomware-angreb har i det seneste år udviklet sig i en ny retning. Kriminelle hackere har siden efteråret 2019 udvidet afpresningen i forbindelse med målrettede ransomware-angreb ved også at true med at lække eller sælge følsom information stjålet i forbindelse med ransomware-angrebet. Angrebsmetoden omtales i it-sikkerhedskredse som dobbelt afpresning.

Hackere bag ransomwaren Maze igangsatte en trend med den nye afpresningsmetode i 2019, og andre kriminelle hackere har siden efterlignet metoden. I dag udfører hackere bag de fleste målrettede ransomware-angreb denne type afpresning.

Dobbelt afpresning var i starten rettet mod myndigheder og virksomheder i USA, og er i dag et globalt fænomen. Afpresning mod en dansk virksomhed i september 2020 viser, at danske myndigheder og virksomheder også kan blive ramt.

Den dobbelte afpresning styrker de kriminelles indtjeningsmuligheder ved målrettede ransomware-angreb. Det stiller nye krav til beredskabet hos danske myndigheder og virksomheder.

Mange myndigheder og virksomheder har i dag procedurer for genoprettelse af systemer fra backup, hvis de skulle blive ramt af ransomware-angreb. Det betyder, at de som udgangspunkt er mindre villige til at betale løsesum for igen at få adgang til deres it-systemer.

De kriminelle kan dog stadig tjene penge på information stjålet i forbindelse med ransomware-angrebet. Det kan de enten ved at få penge fra offeret mod ikke at lække informationen, eller ved at sælge den til andre kriminelle eller interesserede.

Læk af information giver i sig selv ikke et udbytte for de kriminelle, men det synliggør truslen for andre ofre for deres afpresning og medvirker til at lægge pres på fremtidige ofre.

Hackerne øger presset med trusler om skadelige læk

Ved denne type afpresning truer hackerne med at sælge eller lække stjålne data på særlige hjemmesider, såkaldte dedikerede læksider. Hjemmesiderne er generelt tilgængelige for offentligheden, men kræver ofte, at besøgende tilgår siden via anonymiseringstjenesten TOR.

På hjemmesiderne skriver hackerne om deres ofre og viser eksempler på stjålne dokumenter mv. På nogle af siderne er det muligt at byde på data, som de har sat til salg. Prisen på de stjålne data varierer markant. Den højeste pris CFCS har set er 42 mio. USD for information fra et advokatfirma med bl.a. kendte musikere som klienter.

Hackerne udnytter, at læk af fortrolige oplysninger kan gøre stor skade på offeret, og det forsøger de at udnytte til deres fordel.

Data på hackernes læksider indeholder derfor typisk person- og kundefølsomme data såsom mails og oplysninger om medarbejdere og kunder. Læk af sådanne oplysninger kan skade både virksomheden, medarbejdere og kunder. Udover tab af omdømme kan læk også føre til, at offeret får en bødestraf på grund af brud på beskyttelsen af persondata. Nogle hackere omtaler endda brud på GDPR i deres afpresning.

Der er også eksempler på læk af intellektuel ejendom, eksempelvis kildekode fra softwarevirksomheder og tekniske beskrivelser af produkter lavet af

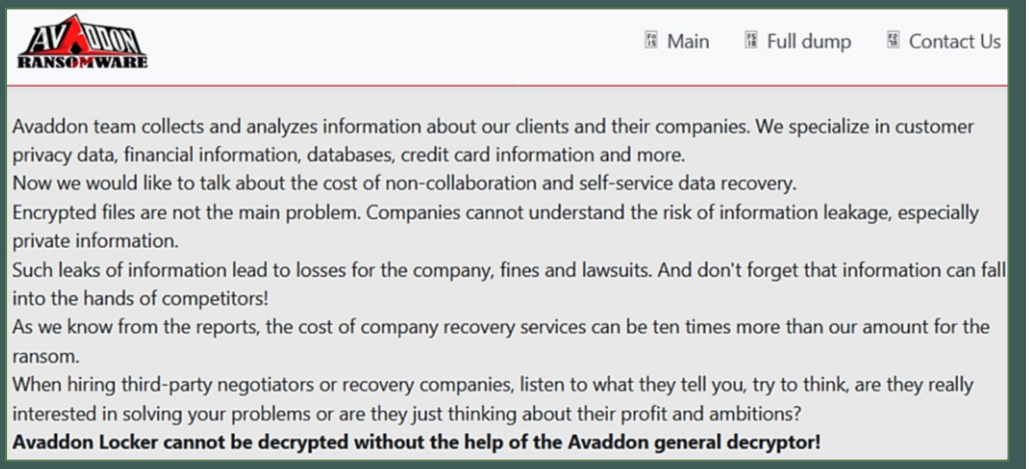
produktionsvirksomheder. Læk af den type oplysninger kan skade virksomhedernes konkurrenceevne og forretningsgrundlag.

Den offentlige eksponering flytter afpresningen fra ofte diskrete forhandlinger om løsesummer mellem offer og gerningsmænd til det offentlige rum. Med eksponeringen forsøger de kriminelle hackere at opretholde et negativt fokus på offeret for at vedligeholde presset.

Hackerne: Vi er de ansvarlige
Der er flere eksempler på, at hackerne bag ransomware-angrebene omtaler sig selv som ansvarlige hackere eller it-specialister, der blot ønsker en afgift for at have fundet sikkerhedsbrister i offerets systemer. Ofrene omtales ofte ikke som ofre, men som klienter eller partnere.

Ofrene, der ikke ønsker at betale løsesum, omtales som ansvarsløse og pengegriske. Tonen er omvendt positiv mod ofre, der ønsker at drøfte en betaling. Nogle hackere indleder endda forhandlingerne med nedslag i afpresningsbeløb, bl.a. i form af "Corona-rabat".

Den fortælling har sandsynligvis til formål at overbevise deres ofre om, at de på den ene side er professionelle nok til at give adgang til de krypterede it-systemer, hvis offeret betaler. På den anden side er de også parate til at gøre virkelighed af deres trusler om læk, hvis offeret ikke betaler, og lægge ansvaret herfor over på offeret.



Billede 1. Hackerne bag ransomwaren Avaddon beskriver her sig selv og truer deres ofre på siden "Avaddon Info" (skærmbillede).

For at styrke fortællingen om, at de er ansvarlige og professionelle, forsøger nogle grupper endda at modvirke negativ medieomtale af deres angreb. Hackerne bag Maze har eksempelvis lovet ikke at angribe hospitaler under COVID-19-pandemien, og andre grupper har efterfølgende stillet lignende garantier. Der har dog siden pandemiens udbrud været flere eksempler på målrettede ransomware-angreb mod sundhedssektoren i udlandet.

En ny og væsentlig trussel, der også er rettet mod Danmark

Dobbelt afpresning udgør ikke kun en meget væsentlig trussel mod de myndigheder og virksomheder, der bliver udsat for angrebene. Det er også en trussel mod kunder, samarbejdspartnere og borgere, der risikerer, at forretnings- eller personfølsomme oplysninger bliver eksponeret i offentligheden eller solgt videre til kriminelle netværk.

Det er vigtigt, at danske myndigheder og virksomheder tænker truslen fra læk og videresalg af fortrolige oplysninger ind i beredskabet mod ransomware-angreb. Det gælder både, hvis angrebet rammer ens egen organisation, eller hvis organisationens følsomme oplysninger hos en ramt leverandør, samarbejdspartner eller myndighed bliver lækket.

Hackerne bag læksiden "Happy Blog" hævdede i september 2020 at have ramt den nordiske brillekæde Synsam Group, hvori danske Profil Optik indgår. Sagen viser, at danske myndigheder og virksomheder også kan blive ofre for denne type afpresning.

Billede 2. Udstilling af Synsam Group på læksiden "Happy Blog" (skærmbillede, CFCS har fjernet kontakt- og personoplysninger).

Man kan læse mere om truslen fra målrettede ransomware-angreb og anbefalinger til at modgå ransomware-angreb på CFCS' hjemmeside.

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.