CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cyberkriminelle opruster i pandemiens skygge

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave november 2020.

Cyberkriminelle opruster i pandemiens skygge

Formål
Trusselsvurderingen har til formål at orientere beslutningstagere i virksomheder og myndigheder om ændringer i flere kriminelle hackergruppers aktiviteter i 2020. Ændringerne stiller virksomheder og myndigheder overfor fornyede, alvorlige trusler fra kriminelle hackere.

Hovedvurdering

- Flere kriminelle hackergrupper har fornyet deres værktøjer, samarbejdsrelationer og aktiviteter i 2020. Sådanne ændringer er normale for cybertruslen, men i 2020 er de sket mere omfattende og mere samtidigt end normalt.

- Ændringerne betyder, at danske virksomheder og myndigheder står over for kriminelle netværk med nye værktøjer og måder at angribe på.

- For nogle af grupperne har ændringerne medført pauser i deres normale aktiviteter over foråret 2020. Grupperne er nu igen aktive.

- COVID-19-pandemien, pres fra myndigheder og sikkerhedsfirmaer samt kriminelles interesse i målrettede ransomware-angreb har på hver sin vis været medvirkende til forandringerne.

Analyse

Flere cyberkriminelle hackergrupper har over foråret og sommeren 2020 fornyet deres værktøjer, samarbejdsrelationer og aktiviteter.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) vurderer, at selvom sådanne ændringer er normale for cybertruslen, så er ændringerne i 2020 mere omfattende og sker mere samtidigt end normalt.

Ændringerne er sket på flere områder. Nogle grupper har spredt deres cyberangreb mod nye typer ofre, eller øget deres fokus på udbyttet ved målrettede ransomware-angreb gennem trusler om læk af stjålne data.

Andre grupper har udskiftet deres vigtigste malware med ny malware. Det er en betydelig ændring, da malwaren for disse grupper normalt er deres mest centrale værktøj i deres daglige aktiviteter. For flere af grupperne har malwaren også en værdi for kriminelle samarbejdspartnere.

Med nye værktøjer og måder at angribe på står flere hackergrupper stærkere end ved begyndelsen af 2020. Danske virksomheder og myndigheder står derfor overfor fornyede, alvorlige trusler fra kriminelle hackere.

CFCS vurderer, at der er flere årsager til forandringerne. COVID-19-pandemien og pres fra myndigheder og sikkerhedsfirmaer har på hver sin vis haft væsentlig betydning. Kriminelle hackeres interesse i at tjene penge på målrettede ransomware-angreb og trusler om læk af stjålne data har også medvirket til forandringer i trusselsbilledet i år.

Forandringerne bekræfter CFCS's tidligere vurdering af, 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.

Fremtrædende grupper har holdt pause i foråret
Nogle fremtrædende kriminelle hackergrupper har holdt pause i deres cyberangreb i foråret 2020. Det gælder bl.a. hackere, der normalt stod bag angreb med Emotet, GetAndGo Loader, Ryuk og BitPaymer. Grupperne genoptog deres angreb over forsommeren og sommeren 2020.

Pauserne falder i nogen grad sammen med nedlukninger af samfundet i bl.a. Rusland, hvor CFCS vurderer, at flere kriminelle hackergrupper opholder sig. Hackernes evne til at udføre angreb har sandsynligvis ikke i væsentligt omfang været påvirket af nedlukningerne. Det understreges af, at nogle af hackerne igen var aktive i maj inden genåbningen af samfundet i Rusland i juni.

CFCS vurderer, at pauserne hovedsageligt skyldes, at grupperne har lukket deres normale aktivitet ned. Det har de sandsynligvis gjort for at få tid til at lave de væsentlige ændringer af deres aktiviteter, der er beskrevet i denne vurdering.

Pandemien tvinger kriminelle til at tænke nyt

COVID-19-pandemien har verden rundt medført store ændringer af vores samfund og vores vaner. Disse ændringer har også en betydning for de kriminelles indtægtsmuligheder.

Hackergrupper, der tidligere er gået målrettet efter betalingssystemer i restaurations- og hotelbranchen, har bl.a. spredt deres aktiviteter mod andre sektorer og nye angrebsmåder. Netop restaurations- og hotelbranchen har været hårdt ramt af nedlukninger og restriktioner som følge af COVID-19-pandemien, og det har sandsynligvis skadet de kriminelle hackeres indtjeningsgrundlag. Det har tvunget dem til at tænke nyt.

Det gælder f.eks. for en ældre, veletableret hackergruppe kaldet bl.a. Carbanak. Gruppen har over en årrække specialiseret sig i at kompromittere betalingssystemer i restaurations- og hotelbranchen samt detailhandel verden over for at stjæle kreditkortoplysninger.

Efter pandemiens udbrud har hackerne bag Carbanak spredt deres normale cyberangreb til også at være rettet mod andre dele af samfundet. Medlemmer af gruppen har sandsynligvis også stået bag målrettede ransomware-angreb, bl.a. i samarbejde med andre hackergrupper.

Det er nyt for hackerne bag Carbanak at udføre ransomware-angreb og samarbejde med disse grupper, men disse ændringer i deres cyberangreb giver hackerne nye indtjeningsmuligheder.

Sanktioner medvirker til forandringer

Pres fra myndigheder har også haft en betydning for cyberkriminelle aktiviteter i 2020.

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 har bl.a. været brugt i målrettede ransomware-angreb til spredningen af ransomwaren Bitpaymer.

Fra midten af marts 2020 holdt hackergruppen pause i deres målrettede ransomware-angreb. Da gruppen vendte tilbage med nye ransomware-angreb i maj 2020, havde de skiftet deres normale ransomware BitPaymer ud med en ny ransomware kaldet WastedLocker. Det mest medieomtalte angreb skete mod fitnessmærket Garmin i juli 2020. Garmin valgte ifølge flere medier at betale en løsesum for at få deres systemer tilgængelige igen.

Sanktionerne mod Evil Corp og den negative medieomtale i forbindelse med sanktionerne kan virke afskrækkende på ofre, der er fristet til at få adgang til deres ramte it-systemer igen ved at betale løsesum.

CFCS vurderer, at sanktionerne og den negative medieomtale i forbindelse med sanktionerne har været medvirkende til, at gruppen har valgt at skifte deres kendte ransomware ud med en ny og ukendt type.

Amerikanske myndigheder advarede i oktober 2020 virksomheder mod at udbetale løsesum til Evil Corp med henvisning til sanktionerne, dog uden at nævne den nye ransomware. Udmeldingen har sandsynligvis haft til formål at lægge pres på organisationer, der fristes til at betale løsesum.

Angreb på malware påvirkede kriminelt økosystem

Et angreb på verdens mest spredte malware har også haft en direkte betydning for dele af det cyberkriminelle økosystem i 2020.

I februar 2020 udsendte hackere fra et it-sikkerhedsfirma et såkaldt script, der ødelagde brugen af malwaren Emotet, der over en årrække var blevet spredt til mange tusinde computere og it-systemer verden over. Angrebet på Emotet fremtvang en pause i brugen af malwaren på fem måneder. Efter pausen er Emotet dog vendt stærkt tilbage. Emotet er nu igen den mest spredte malware i verden.

Angrebet på Emotet havde en betydning for det kriminelle økosystem, da Emotet bruges til spredning af andres gruppers malware. En kernekunde for Emotet har i de seneste år været hackerne bag malwaren Trickbot, der igen er blevet brugt i målrettede ransomware-angreb med ransomwaren Ryuk.

Hackerne bag Trickbot forsøgte i april 2020 forgæves at genetablere deres leverandørs netværk ved at sprede Emotet gennem deres eget netværk af it-systemer inficeret med Trickbot. Rollerne blev således kortvarigt byttet om mellem de to samarbejdspartnere som følge af angrebet.

Trickbot blev også udsat for et angreb i september 2020. Angrebet havde kun en kortvarig effekt, da hackerne bag Trickbot bl.a. har brugt Emotet til at styrke Trickbots ramte botnet. Det viser endnu engang Emotets centrale rolle som distributør af andre gruppers malware.

U.S. Cyber Command stod sammen med flere private virksomheder bag angrebet mod Trickbot. Angrebet mod det kriminelle netværk er et udtryk for de amerikanske myndigheders strategi, der på mere offensiv vis forsøger at bekæmpe cybertruslen. Et af formålene med angrebet var bl.a. at svække mulighederne for at påvirke det amerikanske valg gennem denne malware.

Hackere indstiller angreb for at udvikle ny ransomware

I marts 2020 stoppede hackergruppen bag Trickbot og Ryuk deres målrettede ransomware-angreb. Ryuk har været brugt i angreb mod især sundhedssektoren, offentlige skoler og lokale myndigheder i USA.

I maj 2020 vendte gruppen igen tilbage, men denne gang med en ny ransomware, Conti. Gruppen har sandsynligvis været i besiddelse af Conti siden 2019 og færdigudviklet denne under pausen i foråret. Tidligere på året havde gruppen også introduceret et værktøj, der automatisk stjæler dokumenter om følsom eller hemmeligstemplet information i forbindelse med ransomware-angreb. Hackerne kan

derefter true med at lække eller videresælge dokumenterne, hvis offeret ikke betaler løsesummen.

Pausen i angrebene viser, at udviklingen af Conti har været en stor investering for gruppen. Der var i 2019 sager i medierne om, at ofre for Ryuk havde svært ved at få adgang til deres systemer, selvom de havde betalt løsesum. Da motivet for at betale løsesum netop er at få adgang til systemerne igen, kan det havde skadet Ryuks omdømme. Det kan være en væsentlig årsag til, at hackerne valgte at udvikle en ny ransomware.

Udvikling af Conti har dog endnu ikke sat et punktum for Ryuk. Efter et halvt års pause blev Ryuk i september 2020 brugt i et ransomware-angreb på en amerikansk sundhedsvirksomhed, United Health Services.

Kriminelle øger afpresningen med trusler om læk

Målrettede ransomware-angreb er siden 2019 blevet en del af normalbilledet. Denne udvikling er fortsat i 2020, hvor nye hackergrupper og ransomware er dukket op.

I 2019 startede hackerne bag ransomwaren Maze en ny trend kendt som dobbelt afpresning. Gruppen nøjedes nu ikke kun med at ramme virksomheder og myndigheder med ransomware men truede også med at lække information, som hackerne havde stjålet fra offeret i forbindelse med ransomware-angrebet.

Den angrebsmetode er blevet efterlignet af flere hackergrupper i 2020 og blevet en del af normalbilledet ved målrettede ransomware-angreb. Fra foråret 2020 sker denne dobbelte afpresning eksempelvis for alle ofre for Maze, REvil og DoppelPaymer. Ofre for mindst fjorten andre typer ransomware bliver også udsat for dobbelt afpresning.

Dobbelt afpresning kræver ressourcer i form af etablering af hjemmesider til posteringer af trusler om læk samt markedsføring og salg af data, der ikke bliver frikøbt af offeret. I juni 2020 lancerede hackerne bag Maze, Ragnar Locker og Lockbit derfor et samarbejde om læk kaldet Maze Cartel. Det viser endnu engang, at kriminelle hackere er villige til at tænke nyt, også i deres måde at samarbejde på.

FE bruger denne skala for sandsynligheder i analyser

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