CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Digitale gidseltagere på storvildtjagt

Trusselsvurderingen har til formål at informere myndigheder og virksomheder om truslen fra og modforanstaltninger mod målrettede ransomware-angreb, der kan have alvorlige konsekvenser.

December 2019

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Hovedvurdering

- Der er en stigende trussel fra målrettede ransomware-angreb, hvor kriminelle afpresser myndigheder og virksomheder for store pengebeløb ved at kryptere data på centrale it-systemer.
- Målrettede ransomware-angreb kan ramme alle typer virksomheder og myndigheder.
- I værste fald kan sådanne angreb skade drift og levering af samfundsvigtige ydelser.
- Målrettede ransomware-angreb sker i flere faser. Angriberne inficerer typisk it-systemer med ransomware efter først at have kompromitteret offeret med andre typer malware eller misbrug af Remote Desktop Protocol (RDP).
- Ofte er der en periode mellem den indledende kompromittering og deployeringen af ransomware, hvor det er muligt for offeret at opdage og standse angrebet, inden systemerne bliver krypteret.
- Myndigheder og virksomheder kan generelt modvirke truslen ved at følge Forsvarets Efterretningstjenestes Center for Cybersikkerheds anbefalinger og vejledninger.

Analyse

Der er på globalt plan på ny en stigende trussel fra målrettede ransomware-angreb mod myndigheder og virksomheder. Center for Cybersikkerhed (CFCS) vurderer, at truslen mod danske myndigheder og virksomheder også er stigende. Målrettede ransomware-angreb har i enkelte tilfælde ramt danske virksomheder.

Ved et ransomware-angreb bliver data og systemer på offerets computer holdt som gidsel, da de krypteres og derved bliver utilgængelige for offeret. Aktøren bag angrebet kræver en løsesum for at give offeret adgang til data igen.

Der har i flere lande været sager, hvor målrettede ransomware-angreb medførte, at myndigheder og virksomheder i perioder ikke kunne udføre dele af deres arbejde. Bl.a. lokale myndigheder, skoler, produktionsvirksomheder, hospitaler, it-firmaer, havne og søfart har været ramt.

I værste fald kan sådanne angreb skade drift og levering af samfundsvigtige ydelser. Det har eksempelvis været tilfældet i forbindelse med ransomware-angreb mod sundhedssektoren i USA og Storbritannien, hvor nedetid i administrative systemer medførte, at patientaftaler blev aflyst.

Eksempler på ransomware mod danske virksomheder
Den danske producent af bl.a. høreapparater, Demant, blev i september 2019 udsat for et ransomware-angreb, der medførte, at virksomheden lukkede ned for it-systemer på tværs af virksomheden. Demant vurderer, at angrebet medførte et tab på op mod 650 mio. kr.

Distributionsselskabet NRGi blev i 2015 udsat for et målrettet ransomware-angreb, der påvirkede virksomhedens forretningssystemer i væsentlig grad. Her havde cyberkriminelle ikke adgang til kritiske netværk, men ransomware-angrebet påvirkede deres it-infrastruktur på det administrative netværk.

Hackerne tager sig tid til at tage offerets data som gidsel
I målrettede ransomware-angreb forsøger kriminelle at afpresse myndigheder og virksomheder for store pengebeløb ved at kryptere centrale dele af offerets it-systemer ved hjælp af ransomware. For at svække offerets evne til selv at gendanne sine systemer går angriberne typisk også efter tilgængelige backupsystemer. Løsesummen er nogle gange flere millioner kroner i kryptovaluta.

Angrebene er målrettede i den forstand, at hackerne bruger tid på først at kompromittere offeret for derefter at bevæge sig videre ind i offerets it-systemer, så de kan skabe størst mulig skade. Der kan derfor gå dage mellem hackernes indledende kompromittering af offeret og den endelige deployering af ransomware, hvor hackerne krypterer offerets it-systemer. De kriminelle hackere arbejder i perioden på at kunne kryptere centrale it-systemer og derved lægge et maksimalt pres på det enkelte offer.

Det er sandsynligt, at nogle kriminelle hackere sælger den indledende kompromittering videre til andre kriminelle hackere. Salg af sådanne adgange tager tid. Her kan der derfor gå endnu længere tid mellem den indledende kompromittering og deployeringen af ransomware end normalt.

Angrebene adskiller sig fra generelle ransomware-angreb, der forsøger at ramme mange ofre på én gang ved f.eks. at sende spammails, hvor ransomwaren er vedhæftet. De målrettede angreb er mere tidskræ-

vende for angriberne, men angriberne kan potentielt få de enkelte ofre til at betale en meget højere løsesum ved at ramme centrale it-systemer hos organisationer frem for enkelte computere i organisationer eller hos privatpersoner.

Administrative it-netværk, der er forbundet til internettet, er særligt udsatte over for målrettede cyberangreb. Alvorlige nedbrud i de administrative systemer som følge af målrettede ransomware-angreb kan vanskeliggøre opretholdelsen af en normal drift hos den enkelte virksomhed eller myndighed.

Ransomware kan potentielt også blive spredt af angriberne til it-understøttede produktionssystemer, hvis der er sårbarheder i eksempelvis segmenteringen af administrative og operationelle netværk, eller hvis disse systemer er koblet til internettet. I værste fald kan det medføre, at hele virksomhedens produktion bliver lammet.

Ryuk indtjener millioner til cyberkriminelle
Ryuk-ransomware har siden august 2018 været brugt i flere målrettede ransomware-angreb mod især sundhedssektoren, offentlige myndigheder og skoler samt produktionsvirksomheder i Nordamerika og i Europa. Ofre for Ryuk har i flere tilfælde betalt, hvad der svarer til millioner af kroner i løsesum.

Ryuk er typisk blevet deployeret efter misbrug af Remote Desktop Protocol, inficeringer med TrickBot eller Emotet eller en kombination af disse værktøjer. Ryuk er sandsynligvis opkaldt efter en japansk tegneseriefigur med samme navn. Tegneserie- og spilreferencer er ikke ualmindelige i hackermiljøer.

Virksomheder og myndigheder er mål for digital storvildtjagt
Udover at angriberne bruger tid på at kryptere centrale it-systemer i ramte organisationer, er angrebene også målrettede i den forstand, at hackerne ofte angriber store eller samfundsvigtige myndigheder og virksomheder. Hackerne forventer, at sådanne myndigheder og virksomheder er villige til at betale en meget stor løsesum. Angrebene på større virksomheder og myndigheder bliver i it-sikkerhedskredse ofte omtalt som storvildtjagt (big game hunting).

Angrebene er som udgangspunkt opportunistiske. Målrettede ransomware-angreb kan derfor ramme alle typer virksomheder og myndigheder, og der er ikke en specifik type ofre. Der er dog eksempler på, at nogle typer af virksomheder og myndigheder hyppigere udsættes for denne type angreb inden for et geografisk område eller inden for en bestemt tidsperiode. I efteråret 2019 har der eksempelvis været en bølge af angreb på lokale myndigheder i Spanien.

Mens der indtil videre kun har været enkelte meldte tilfælde i Danmark, er det muligt, at Danmark også kan blive udsat for lignende bølger af

angreb. I efteråret 2019 har to danske virksomheder, Demant og GlobalConnect, været ramt af separate ransomware-angreb.

Ransomware rulles ud efter en indledende kompromittering
Som nævnt inficerer hackerne typisk myndighedernes eller virksomhedernes it-systemer med ransomware efter først at have skabt adgang til offerets it-netværk. Der er nogle typiske metoder, angriberne har brugt til denne indledende kompromittering, herunder adgang via Remote Desktop Protocol (RDP), inficering med malware eller sårbare internetvendte servere.

Adgang via RDP gør det muligt for angriberne at få adgang til individuelle computere (klienter), hvorfra angriberne kan nå videre ind i organisationens netværk. For at få adgang via RDP kan angriberne f.eks. udnytte stjålne brugernavne og kodeord eller forsøge at gætte brugernavne og kodeord gennem såkaldte brute force-angreb. Svage kodeord og manglende brug af to-faktor-godkendelse kan gøre det nemt for angriberne at få adgang på denne måde.

Alternativt kan angriberne få adgang til relevante it-systemer ved at inficere klienter med malware, der ikke er ransomware, og bruge denne adgang i den videre kompromittering og inficering med ransomware. Her har kriminelle bag inficeringer med BitPaymer-ransomware bl.a. brugt Dridex-malware, og kriminelle bag inficeringer med Ryuk-ransomware har bl.a. brugt TrickBot og Emotet-malware. Både Dridex, Emotet og TrickBot bliver normalt spredt via phishing-mails, men de kan også installeres af angriberne via eksempelvis RDP-adgang. REvil ransomware er set spredt med hjælp af Gozi og SmokeBot-malware.

Andre typer malware og software bliver også brugt i den videre kompromittering af relevante it-systemer og deployeringen af ransomware, eksempelvis Metasploit, Cobalt Strike, Meterpreter, ADFIND, PowerShell, PsExec, Empire Framework, BloodHound og Mimikatz.

Det er også muligt for angriberne at sprede ransomware mod servere, der er sårbare over for angreb direkte fra internettet, og som kan identificeres gennem sårbarhedsscanninger.

Når angriberne har kompromitteret offeret ved at stjæle adgangsoplysninger eller installere anden malware end ransomware, så kan de vende tilbage til offeret, også selvom offeret har gendannet eller frikøbt sine krypterede it-systemer. Det kan de, såfremt brugernavne og kodeord ikke nulstilles, eller hvis der stadig er malware på systemerne, som angriberne kan udnytte.

Ransomware, der er blevet brugt i målrettede angreb i det seneste år i udlandet, inkluderer bl.a. Ryuk, REvil, RobbinHood, BitPaymer, DoppelPaymer, LockerGoga, Clop, Dharma og MegaCortex.

Angriberne ønsker typisk at blive kontaktet af offeret via e-mailkommunikation til mail-konti baseret på krypterede mailtjenester såsom Protonmail og Tutanota. Løsesummen ønskes sædvanligvis

modtaget i kryptovaluta, ofte Bitcoin, for at besværliggøre sporingen af udbetalt løsesum.

Anbefalinger
Ransomware udvikler sig hele tiden og ændrer karakter, hvorfor sikkerhedsforanstaltninger også hele tiden bør tilpasses de aktuelle varianter af angreb og ransomware. Det er et kapløb, som kræver konstant fokus. Her er en række anbefalinger, organisationer bør implementere for at imødegå de i trusselsvurderingen omtalte forhold.

Anbefalinger til, hvad der kan gøres for at imødegå målrettede ransomware-angreb.

- Der bør etableres detaljeret overvågning, der sikrer, at organisationen bliver opmærksom på uønsket aktivitet, særlig med henblik på detektering af og reaktion på de i trusselsvurderingen nævnte ransomware (Ryuk, REvil, RobbinHood, BitPaymer, DoppelPaymer, LockerGoga, Clop, Dharma og MegaCortex) og øvrige malware (Trickbot, Emotet, Dridex, Gozi og Smokebot).
- Anvendelsen af privilegerede services, herunder Remote Desktop Protocol (RDP), bør altid ske ved anvendelse af VPN.
- RDP-brugere bør altid autentificere sig ved brug af to-faktor-autentifikation, når brugerne tilgår organisationens it-systemer.
- Der bør altid anvendes to-faktor-autentifikation ved ekstern adgang til organisationens it-systemer.
- Fjern eller bloker unødvendig software på brugeres pc'er f.eks. PowerShell, hvis der ikke er et konkret behov.
- Der bør anvendes individuelle passwords til lokaladministratorkonti på organisationens it-systemer. Brugeres lokaladministratorrettigheder bør begrænses.
- Virksomhederne bør sikre, at afgående medarbejderes konti lukkes ved afgang.

Anbefalinger til hvad der bør være på plads, hvis skaden sker.

- Der bør udarbejdes en forretnings- og ledelsesgodkendt beredskabsplan for, hvordan man vil begrænse konsekvensen af et ransomware-angreb.
- Systematisk backup af alle kritiske informationer, centrale konfigurationsfiler og andre opsætningsdata, herunder AD'et, er absolut påkrævet.
- Backup-rutinen gennemføres med høj frekvens. Der bør altid findes offline kopi af backup.
- Systematisk og løbende kontrol af, at backup fungerer efter hensigten.
- Ved eventuel tilbagerulning af systemer fra backup bør der foretages ændring af passwords for alle brugere og systemer. Nye passwords bør være væsentligt forskellige fra de gamle.
- Plan for dokumentation af hændelseshåndteringen.

Der findes derudover en række tekniske løsninger, hvis funktionalitet varierer fra udbyder til udbyder, som kan bidrage til yderligere sikring af organisationens it-systemer mod ransomware.

Endelig er der grundlæggende sikkerhedsforanstaltninger, der bør være på plads. Der er vejledninger på CFCS's hjemmeside til yderligere inspiration, eksempelvis:

- Cyberforsvar der virker
- Reducer risikoen for ransomware
- Passwordvejledning
- Spear-phishing – et voksende problem
- Reducer risikoen for falske mails

FE bruger denne skala for sandsynligheder i analyser