CENTER FOR CYBERSIKKERHED

Undersøgelsesrapport

Anatomien af målrettede ransomware-angreb

Hvordan målrettede ransomware-angreb foregår, og hvordan du forsvarer dig mod dem.

Indhold

Resumé **3**

Indledning **3**

Et typisk målrettet ransomware-angreb **4**

1. Indledende adgang 6
   a. Phishing 7
   b. Drive-by 8
   c. Supply Chain 9
   d. Fjernadgang 10
   e. Eksternt medie 11
   f. Sårbarhed 11
2. Konfigurering af værktøjer 12
3. Netværksrekognoscering 13
4. Lateral bevægelse 14
5. Persistens i netværket 15
6. Domæneadministratorrettigheder 15
7. Destruering af backup 16
8. Mulig eksfiltrering af følsom data 17
9. Deaktivering af sikkerhedssystemer 17
10. Deployering af ransomware og afpresning 18

Sådan forsvarer du dig mod et målrettet ransomware-angreb **20**

CENTER FOR CYBERSIKKERHED

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

1. udgave oktober 2020.

Formål
Denne undersøgelsesrapport beskriver, hvordan et typisk målrettet ransomware-angreb forløber, og giver forslag til tiltag, som kan hjælpe myndigheder og virksomheder med at beskytte sig endnu bedre. Forløbet er generaliseret, men baserer sig på indsigt fra virkelige hændelser. Målgruppen for denne rapport er primært it-ledelse og it-teknikere.

Resumé

- Adskillige danske virksomheder er blevet ramt af målrettede ransomware-angreb det seneste år. Angrebene har betydet meget store økonomiske tab på flere hundrede millioner kroner i nogle tilfælde.
- Ransomware-angreb kan ramme alle, men nogle hackere målretter deres angreb mod store eller samfundsvigtige virksomheder og myndigheder, som de forventer både kan og vil betale en stor løsesum.
- Rapporten kortlægger, hvordan disse særligt målrettede ransomware-angreb forløber, og giver konkrete anbefalinger til, hvordan myndigheder og virksomheder kan beskytte sig endnu bedre.
- Hackerne opnår ofte deres indledende adgang via phishing-angreb, kompromitterede fjernadgangssystemer eller sårbarheder i internetvendte enheder. Hackerne kan dog også opnå indledende adgang via drive-by angreb, supply chain angreb eller potentielt gennem levering af inficerede eksterne medier.
- Med adgang til organisationen vil hackerne typisk starte med at konfigurere deres værktøjer, foretage netværksrekognoscering, sprede sig i netværket og etablere persistens. Herefter vil de forsøge at skaffe domæneadministratorrettigheder, stoppe backupsystemer og i nogle tilfælde eksfiltrere følsom data, før de deaktiverer sikkerhedssystemer og deployerer ransomware.
- Viden om hackeres ageren giver myndigheder og virksomheder mulighed for at opdage og stoppe målrettede ransomware-angreb, før hackerne formår at kryptere deres systemer. Rapporten præsenterer konkrete forsvarsinitiativer, som modvirker effekterne af de angrebsteknikker, som hackerne anvender undervejs.

Indledning

Der er en vedvarende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder. Modsat cyberspionage, hvor hackere opererer i det skjulte, udspiller ransomware-angreb sig særdeles direkte, når systemer pludselig krypteres, og en besked om løsesum toner frem på skærmen.

Ransomware-angreb kan ramme alle, men nogle hackere udvælger mål, som de forventer både kan og vil betale en stor løsesum. Derfor er der en tendens til, at hackerne målretter angreb mod store eller samfundsvigtige myndigheder og virksomheder.

Mens nogle typer ransomware spreder sig automatisk, så kræver målrettede ransomware-angreb en manuel udførelse og en betydelig indsats fra hackerne på deres ofres interne netværk. Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) kalder disse ransomware-angreb for ”målrettede ransomware-angreb”, hvor hackerne over længere tid og med betydelig manuel udførelse forsøger at kryptere dele af it-infrastrukturen i store eller samfundsvigtige

myndigheder og virksomheder med henblik på at afpresse dem. "Målrettet" betyder ikke, at hackerne nødvendigvis på forhånd udvælger konkrete organisationer og aktivt går efter dem. Det betyder derimod, at hackerne målretter deres tid og indsats mod de organisationer, som de forventer vil betale en meget stor løsesum på baggrund af bredere og mere opportunistiske indledende kompromitteringer. Det er særligt målrettede ransomware-angreb, som har været i vækst de seneste par år, og som derfor danner fokus i denne rapport.

Målrettede ransomware-angreb er oftest ikke lette at gennemføre for hackerne. Et målrettet ransomware-angreb kan derfor være undervejs på organisationens indre netværk i flere dage, uger eller endda måneder, før systemerne rent faktisk krypteres. I dén periode kan organisationer nå at reagere og afværge angreb, før systemerne endeligt krypteres.

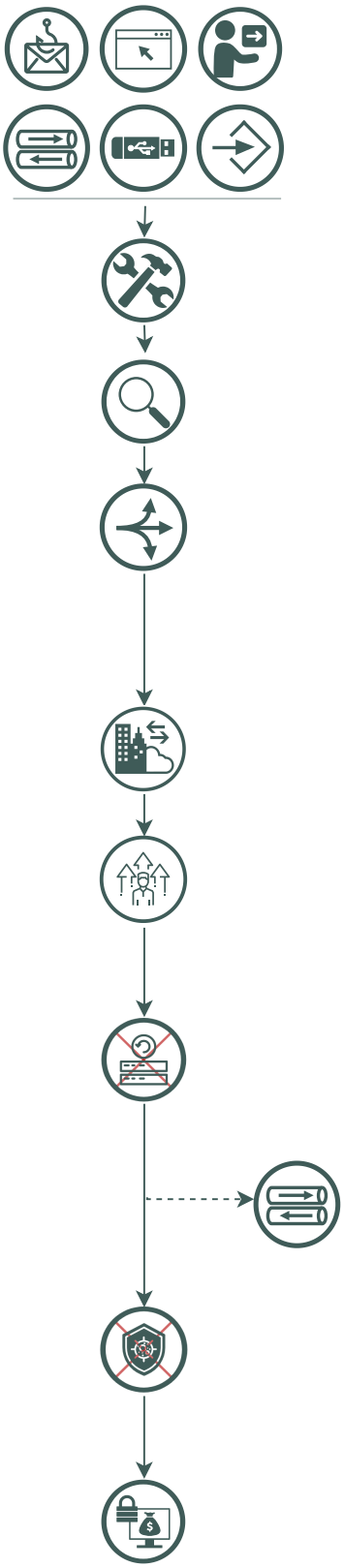
Denne rapport kortlægger angrebsforløbet i et typisk målrettet ransomware-angreb, og giver konkrete anbefalinger til, hvordan myndigheder og virksomheder kan beskytte sig mod dem. Selvom beskrivelsen er generaliseret, er rapporten baseret på indsigt fra rigtige målrettede ransomware-angreb mod danske organisationer suppleret med rapporter fra industripartnere og enkelte åbne kilder.

Rapporten er todelt. I første del kortlægges hver angrebsfase i et typisk målrettet ransomware-angreb. I anden del præsenteres konkrete forsvarsinitiativer, som myndigheder og virksomheder kan implementere for at beskytte sig bedre. Her bliver hver angrebsteknik, som hackerne ofte anvender, koblet med specifikke forsvarsinitiativer, der modvirker deres effekt.

Et typisk målrettet ransomware-angreb

I dette afsnit kortlægges forløbet i et typisk målrettet ransomware-angreb. Beskrivelsen er inddelt i en række faser, der tilsammen danner det samlede angrebsforløb. Den opdeling kaldes for en Cyber Kill Chain, som betyder, at hver enkelt fase ofte er nødvendig for den næste. Derfor vil angrebet potentielt kunne afværges, hvis hackerne blot stoppes under én fase i angrebet. Rapporten refererer til specifikke ID-numre fra MITREs ATT&CK® terminologi over angrebs- og forsvarsteknikker. MITRE er en nonprofitorganisation, der bl.a. arbejder med cybersikkerhed, og som har udviklet et analyseframework kaldet ATT&CK®. Henvisningerne giver en fælles referenceramme, og organisationer kan søge yderligere information om hver angrebs- og forsvarsteknik bl.a. på MITREs hjemmeside. Figur 1 illustrerer, hvordan et typisk målrettet ransomware-angreb forløber suppleret med ID'er på de angrebsteknikker, som hackerne særligt ofte anvender i hver fase.

ANGREBSFORLØB: MÅLRETTET RANSOMWARE



1. **Indledende adgang**
   - Phishing
   - Drive-by
   - Supply Chain
   - Fjernadgang
   - Eksternt medie
   - Sårbarhed
2. **Konfigurering af værktøjer**
   - Eksisterende malware
   - Nyt malware eller pen-tester værktøj
   - Legitime programmer på offerets computer
3. **Netværksrekognoscering**
   - Skanner netværk
4. **Lateral bevægelse**
   - Stjæler legitime loginoplysninger
   - Gætter usikre kodeord
   - Bevæger sig lateralt bl.a. via RDP
5. **Persistens i netværket**
   - Legitime fjernadgangssystemer
   - Malware Remote Access Tools (RATs)
   - Pen-test Remote Access Tools (RATs)
6. **Domæneadministratorrettigheder**
   - Stjæler loginoplysninger
   - Gætter kodeord
7. **Destruering af backup**
   - Shadow copies
   - Centraliserede backupløsninger
8. **Mulig eksfiltrering af følsom data**
   - Finder følsom data
   - Eksfiltrerer data
9. **Deaktivering af sikkerhedssystemer**
   - Stopper endpointsikkerhedsløsninger
   - Afbryder andre systemer, som muligvis kan forhindre kryptering
10. **Deploying af ransomware og afpresning**
    - Krypterer systemer med ransomware
    - Afpresser offer for løsesum for dekryptering
    - Truer muligvis med offentliggørelse af følsom data

MITRE ATT&CK®

TA0001 I Initial Access
- T1566 I Phishing
- T1189 I Drive-by Compromise
- T1199 I Trusted Relationship
- T1133 I External Remote Services
- T1091 I Replication Through Removable Media
- T1190 I Exploit Public-Facing Application
- T1078 I Valid Accounts

TA0026 I Stage Capabilities
- T1362 I Upload, install, and configure software/tools

TA0007 I Discovery
- T1046 I Network Service Scanning
- T1135 I Network Share Discovery

TA0006 I Credential Access
- T1003 I OS Credential Dumping
- T1552 I Unsecured Credentials
- T1110 I Brute Force

TA0008 I Lateral Movement
- T1021 I Remote Services
- T1070 I Lateral Tool Transfer

TA0003 I Persistence
- T1033 I External Remote Services
- T1505 I Server Software Component
- T1053 I Scheduled Task/Job
- T1197 I BITS Jobs

TA0006 I Credential Access
- T1003 I OS Credential Dumping
- T1552 I Unsecured Credentials

TA0004 I Privilege Escalation
- T1078 I Valid Accounts

TA0040 I Impact
- T1490 I Inhibit System Recovery
- T1485 I Data Destruction
- T1486 I Data Encrypted for Impact

TA0010 I Exfiltration
- T1041 I Exfiltration Over C2 Channel
- T1048 I Exfiltration Over Alternative Protocol

TA0005 I Defense Evasion
- T1562 I Impair Defenses

TA0002 I Execution
- T1059 I Command and Scripting Interpreter
- T1053 I Scheduled Task/Job
- T1072 I Software Deployment Tools
- T1047 I Windows Management Instrumentation

TA0040 I Impact
- T1486 I Data Encrypted for Impact

Figur 1: Forløbet i et typisk målrettet ransomware-angreb. Hver fase henviser til et selvstændigt afsnit i rapporten.

Først vil hackerne forsøge at bryde organisationens ydre forsvar og etablere en adgang ind i organisationens indre netværk. Det gør de via forskellige teknikker, som beskrives nedenfor. Disse indledende angrebsveje anvendes også i andre typer cyberangreb, og gennemgangen er derfor også relevant for at kunne forstå og modvirke andre typer cyberangreb.

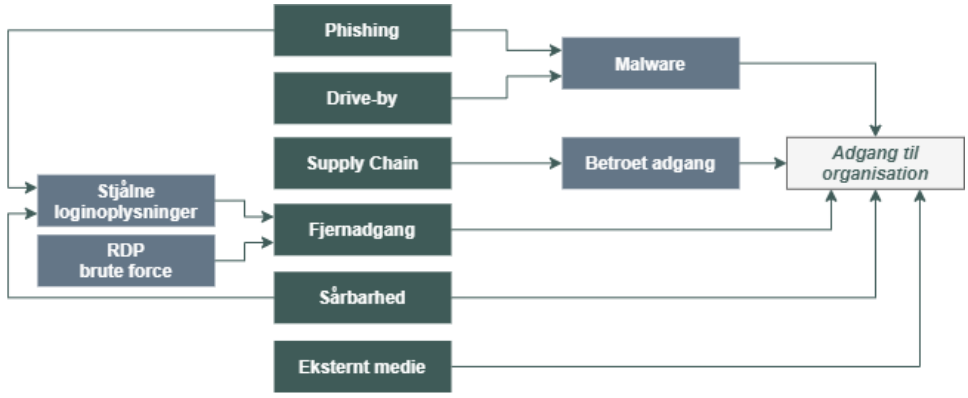
Cyberkriminalitet er en industri
Den indledende kompromittering udføres ikke nødvendigvis af de samme aktører, som gennemfører resten af ransomware-angrebet. Der eksisterer et kriminelt undergrundsmarked, hvor cyberkriminelle bl.a. videresælger adgange til hinanden og på anden vis understøtter hinandens virke. Det er med andre ord sjældent én aktør, men nærmere et netværk af specialiserede hackere, som står bag et målrettet ransomware-angreb.

Med adgang til organisationen vil hackerne udføre en række handlinger frem mod deployering af ransomwaren og afpresning af deres offer. Selvom de værktøjer, som hackerne anvender undervejs i angrebet, varierer og løbende bliver udviklet, så følger de fleste målrettede ransomware-angreb det samme overordnede forløb.

I det følgende præsenteres de ti faser, som hackerne typisk gennemgår under et målrettet ransomware-angreb.

1 Indledende adgang

Hackernes første mål er at opnå indledende adgang til deres offer. De mest almindelige metoder, hackerne opnår denne adgang på, er gennem phishing-angreb, drive-by angreb, kompromitterede fjernadgangssystemer, udnyttelse af sårbarheder i internetvendte systemer, supply chain angreb eller potentielt gennem inficerede eksterne medier. Nogle metoder giver hackerne direkte adgang til offerets systemer, eksempelvis via stjålne loginoplysninger, mens andre forudsætter, at ofrene først får leveret malware til deres systemer, som herefter åbner op for hackerne. Hackerne udnytter enten de indledende adgange selv eller sælger dem videre til andre kriminelle. Figur 2 illustrerer de mest almindelige indledende kompromitteringsveje anvendt i målrettede ransomware-angreb.



Figur 2: Typiske metoder hackerne opnår indledende adgang på.

Phishing

I phishing-angreb forsøger hackerne at manipulere en person til at videregive personlige oplysninger, åbne inficerede filer eller klikke på links til falske hjemmesider. Phishing distribueres ofte gennem e-mails, der sendes ud til tusindvis af modtagere, men sker også via SMS'er, sociale medier eller andre kommunikationsplatforme.

Når phishing er målrettet enkeltpersoner eller organisationer, kaldes det for spear-phishing. Her har afsenderen gjort sig særligt umage for at tilpasse indholdet til den specifikke modtager.

Hvis ofrene klikker på links, vil de enten downloade malware eller blive ledt hen til falske hjemmesider, som vil forsøge at franarre dem personlige oplysninger såsom følsomme loginoplysninger. Disse loginoplysninger kan eksempelvis misbruges til at tilgå organisationers interne netværk via fjernadgangssystemer. Det beskrives nærmere nedenfor.

Hvis ofrene derimod åbner inficerede vedhæftede filer, vil de typisk downloade malware direkte til deres computer og derved åbne en adgang for hackerne. Mange af disse filer forudsætter imidlertid godkendelse, af f.eks. brug af makroer eller at der eksisterer en sårbarhed i systemet.

Mens de fleste banale phishing-forsøg fanges af it-systemer eller årvågne medarbejdere, er hackere imidlertid begyndt at bruge mere sofistikerede teknikker som f.eks. "e-mail thread hijacking". Her kompromitterer hackerne en e-mailkonto på en samarbejdspartner og udsender svar på igangværende e-mailkorrespondancer til offerets kontakter. De inficerede mails kommer derfor fra en troværdig afsender og i naturlig forlængelse af allerede etablerede samtaler. Hackerne forsøger på den måde at misbruge troværdigheden i allerede eksisterende samtaler sendt fra en rigtig samarbejdspartner for at øge chancen for, at deres ofre åbner vedhæftede filer eller klikker på links til falske hjemmesider.

Flere danske ofre for målrettede ransomware-angreb blev kompromitteret via e-mail thread hijacking. I ét tilfælde modtog syv medarbejdere i en dansk organisation en mail fra en kompromitteret samarbejdspartner med et ondsindet link gemt i et svar på en igangværende mailkorrespondance. Da en medarbejder trykkede på linket, blev der downloadet en ondsindet fil. Medarbejderen accepterede brug af makroer og åbnede filen, hvilket startede et PowerShell script, der downloadede en kendt trojaner ved navn QBot. Malwaren gav hackerne adgang til medarbejderens computer, hvorfra de kunne sprede sig.

Ransomware-angrebet mod Danish Agro i april 2020 startede også med e-mail thread hijacking. Som Danish Agros CEO, Henning Haahr, udtalte i et interview med Agriwatch: "*Hackerne overtog leverandørernes it-system og sendte en phishing-mail direkte fra leverandøren ind i en helt konkret mailkorrespondance med os, der kørte i forvejen. På den måde kom de ind i vores system og fik installeret hackersoftware*".

Banktrojanere misbruges i målrettede ransomware-angreb
Det er ofte banktrojanere, som bliver leveret forud for målrettede ransomware-angreb. Banktrojanere er malware, der oprindeligt er udviklet til at stjæle bankoplysninger. Den adgang malwaren giver, bliver dog i stigende grad misbrugt af hackere til at udføre målrettede ransomware-angreb i stedet. Banktrojanere har eksisteret i mange år, og kriminelle bagmænd har etableret store netværk af kompromitterede maskiner. Bagmændene har imidlertid fundet ud af, at de kan tjene penge på at sælge deres adgange til inficerede maskiner videre til andre hackere, der bl.a. anvender dem til at udføre målrettede ransomware-angreb.

Emotet er et eksempel på denne type malware, som oprindeligt var en banktrojaner, men som nu bl.a. fungerer som et globalt distribueringsnetværk, hvor udvalgte kriminelle grupper kan tilkøbe sig adgang til inficerede organisationer ved at få leveret deres egen malware til ofrenes systemer. Flere cyberkriminelle grupper har anvendt Emotet-adgange til at få leveret malware herunder operatørerne bag hhv. TrickBot og Qbot, som senere har deployeret hhv. Ryuk og DoppelPaymer ransomware.

Ét målrettet ransomware-angreb mod en dansk organisation startede netop med leveringen af TrickBot, der gav hackerne adgang til organisationen. Det er uklart præcist, hvordan malwaren blev leveret, men TrickBot er tidligere blevet leveret gennem phishing, drive-by angreb eller downloadet via Emotet malwaren. Angrebet endte med at store dele af organisationens vitale systemer blev krypteret med Ryuk ransomware.

Drive-by
Et drive-by-angreb er, når et offer utilsigtet downloader malware i forbindelse med almindelig websurfing. I denne type angreb gemmer hackerne typisk kode, som udnytter sårbarheder i brugerens webbrowser, eller gemmer links til malware i hjemmesidens indhold. Malware bliver så downloadet, hvis besøgende klikker på det inficerede indhold.

Ofte vil hackerne kompromittere legitime hjemmesider med betydelig trafik eller hjemmesider, som besøges af udvalgte grupper. Et målrettet drive-by angreb mod en udvalgt hjemmeside kaldes også for strategisk webkompromittering eller et vandhulsangreb.

I almindelige drive-by angreb starter hackerne med at identificere én eller flere sårbare hjemmesider, som har besøgende, de ønsker at kompromittere. Hackerne kan eksempelvis bruge frit tilgængelige søgeværktøjer såsom Shodan eller lignende services, som kan skanne internettet for sårbare webservere, der hoster hjemmesider. Ved målrettede kompromitteringer, vil hackerne starte med at finde ud af, hvilke hjemmesider deres mål er tilbøjelige til at besøge, og herefter forsøge at finde sårbarheder i de tilhørende specifikke webservere. En sidste metode er, at hackerne selv opsætter en eller flere hjemmesider, og forsøger at lokke besøgende til disse hjemmesider.

Hvis ofrene downloader malware, åbnes en adgang for hackerne ind i organisationens system. Dridex og lignende banktrojanere er bl.a. blevet distribueret via drive-by angreb.

Supply Chain

Et supply chain angreb er kendetegnet ved kompromittering gennem en leverandør eller betroede samarbejdspartnere. Udlicitering af services og infrastruktur til tredjepartsleverandører giver organisationer mulighed for at fokusere på sine kerneydelser, men gør dem samtidig afhængige af sine leverandørers cybersikkerhed. Det sker, fordi leverandører typisk har brug for en adgang ind i organisationens interne netværk for at kunne levere sine ydelser. Hvis leverandøren kompromitteres, får hackerne imidlertid samme adgang, som leverandøren har ind i organisationen. Hvis nødvendige sikkerhedsforanstaltninger ikke er etableret, reduceres organisationens cybersikkerhedsniveau således til laveste fællesnævner blandt sine leverandører.

Supply chain angreb sker både som brede kampagner, hvor hackerne forsøger at kompromittere samtlige af leverandørernes kunder, men også som mere målrettede angreb, hvor hackerne kun angriber enkelte af leverandørens kunder.

Ved et supply chain angreb starter hackerne med at finde leverandører eller samarbejdspartnere, som enten kan give dem adgang til mange eller særligt interessante mål. For at styrke deres brand reklamerer nogle virksomheder eksempelvis på deres hjemmeside med, hvem deres kunder er. Den information kan hackerne misbruge til at målrette angreb mod dem og deres kunder.

Managed Service Providers (MSP'er), hosting-virksomheder og Cloududbydere er af samme grund særligt attraktive mål for hackere i relation til supply chain angreb. Disse organisationer råder nemlig typisk over et stort antal betroede adgange, og deres adgange er i nogle tilfælde underlagt færre sikkerhedsforanstaltninger end alternative kompromitteringsveje ind i en organisation. Bl.a. er hackerne bag Sodinokibi/REvil kendte for bl.a. at ramme serviceudbydere.

Når hackerne har fundet en leverandør, kompromitterer de ofte leverandørerne eller samarbejdspartnerne med de samme metoder, der er beskrevet her i rapporten.

Kompromitterede samarbejdspartnere misbruges som nævnt bl.a. til at udføre e-mail thread hijacking mod interessante organisationer, de kommunikerer med via email. Hvis der derimod er tale om en leverandør med en direkte betroet adgang kan hackerne finde på at søge efter fjernadministrationsløsninger og konti, som leverandøren bruger til at tilgå deres kunder. Med sådanne adgange kan hackerne tilgå netværket hos leverandørens kunder med samme privilegier, som leverandøren normalt har.

I det målrettede ransomware-angreb mod GlobalConnect i maj 2020 kompromitterede hackerne, foruden GlobalConnect selv, også flere af deres kunder via betroede adgange, herunder den danske medicinal-indkøbsvirksomhed Amgros.

Fjernadgang

Hackerne udnytter også mulighederne for at tilgå organisationens interne netværk via eksterne fjernadgangssystemer såsom Remote Desktop Protocol (RDP) eller Virtual Private Network (VPN). Hackerne udnytter overordnet fjernadgangsløsningerne på tre forskellige måder.

De første to involverer stjålne loginoplysninger, der misbruges til at tilgå organisationen via fjernadgangsløsninger forklædt som en legitim medarbejder.

I den første metode franarrer hackerne loginoplysninger til fjernadgangssystemer gennem phishingkampagner, som hackerne kan tilgå organisationen med.

Den anden metode involverer udnyttelse af sårbarheder i selve fjernadgangsløsningerne til at fremskaffe loginoplysninger på organisationens brugere. I 2019 blev en sårbarhed i VPN-forbindelsesløsningen Pulse Secure Connect eksempelvis opdaget (CVE-2019-11510). Sårbarheden gav hackere mulighed for at downloade brugernavne og kodeord på organisationers VPN-brugere i klartekst.

I et målrettet ransomware-angreb mod en dansk organisation udnyttede hackerne netop denne sårbarhed til at stjæle loginoplysninger på flere af organisationens medarbejderes VPN-konti. Med disse kunne hackerne tilgå organisations indre netværk forklædt som en legitim bruger.

I den tredje og sidste metode udnytter hackerne sårbare RDP-opsætninger. Hackerne udnytter, at nogle RDP-fjernadgangsforbindelser ikke gemmes bag en RDP-Gateway eller ikke tilgås gennem en VPN-forbindelse. Port 3389 efterlades derimod åben mod internettet. I praksis betyder det, at ikke blot de tiltænkte medarbejdere, men alle med internetforbindelse kan tilgå computeren og forsøge at logge ind. Det kræver dog, at de også kender IP-adressen på enheden med den åbne port.

Hackerne starter ofte den sidste type angreb med at skanne internettet for åbne port 3389. Det kan nemt gøres eksempelvis via Masscan.exe, der kan skanne hele internettet for åbne port 3389 på under seks minutter. De anvender alternativt åbne databaser som Shodan, der stiller den slags information frit til rådighed. Resultatet af søgningerne danner herefter listen over potentielle ofre.

Uden ekstra sikkerhedsforanstaltninger er det eneste, der holder hackerne tilbage ved disse opsætninger, typisk kun ét kodeord. Kodeordet kan hackerne sætte en computer til at forsøge at gætte gentagne gange, indtil de finder det rigtige. Den teknik kaldes for brute force. Hvis kodeordet ikke er tilstrækkeligt langt eller kompliceret, kan en computer gætte et kodeord meget hurtigt. Alternativt udfører hackerne såkaldt 'password spraying', hvor hackerne gætter på færre, men særligt populære kodeord mod et stort antal adgange. Sidstnævnte anvendes eksempelvis, hvis organisationer har opsat et maksimalt antal loginforsøg, før kontoen spærres. Når det rigtige kodeord er fundet, kan hackerne logge ind hos organisationen.

Netop fordi RDP-adgange er relativt lette at kompromittere, er disse blandt de billigste og mest tilgængelige adgange, som bliver solgt på det cyberkriminelle marked. CFCS har udsendt flere varsler om brugen af RDP. I Danmark er der per

september 2020 stadig over 4.500 potentielt sårbare enheder med port 3389 åben mod internettet og over fire millioner på verdensplan.

Eksternt medie

Eksterne medier såsom USB-nøgler er nyttige til at flytte filer fra én maskine til en anden. Hackerne kan dog også distribuere inficerede USB-nøgler, der leverer malware, hvis de tages i brug.

CFCS er ikke bekendt med målrettede ransomware-sager, hvor USB-nøgler har været brugt til at skabe indledende kompromittering. Inficerede USB-nøgler bliver dog jævnligt brugt, og det er derfor en metode, som er relevant at være opmærksom på, herunder ift. hvilke politikker man som organisation har for deres anvendelse.

Sårbarhed

Den sidste metode, som ofte ses anvendt til at skaffe adgang til organisationer, involverer udnyttelsen af sårbarheder i internetvendte systemer. Udnyttelse af sårbarheder indgår både som delelement i de andre metoder, men repræsenterer også en selvstændig indledende kompromitteringsvej.

Drive-by angreb kræver eksempelvis nogle gange, at hackerne kan udnytte en sårbarhed i de besøgendes webbrowser. Som beskrevet kan hackerne alternativt også finde sårbarheder i selve fjernadgangsløsningerne, der eksempelvis kan give dem adgang til interne netværk via VPN-fjernadgangsløsninger. Andre sårbarheder virker imidlertid uafhængigt af de andre metoder og repræsenterer derfor en selvstændig kompromitteringsvej.

I 2019 blev en sårbarhed i Citrix netværksudstyr f.eks. offentliggjort (CVE-2019-19781). Sårbarheden gjorde det muligt for hackerne at levere malware til organisationer direkte over internettet. Der gik meget kort tid fra offentliggørelsen af sårbarheden, til der blev set mange forsøg på hacking af Citrix-udstyr.

Hackerne foretager løbende rekognoscering efter sådanne sårbarheder, som de kan udnytte til at kompromittere organisationer med. Sårbarheder publiceres bl.a. på online fora eller på leverandørers hjemmesider, herunder i forbindelse med sikkerhedsopdateringer. Håndteringen af sårbarheder er et tveægget sværd, idet deres offentliggørelse er nødvendig for sikkerhedsansvarlige, så de kan opdatere deres systemer. Offentliggørelsen gør dog samtidig hackerne opmærksomme på, at der eksisterer sårbarheder i systemerne, som de kan forsøge at finde frem til og udnytte. Håndteringen af sårbarheder er derfor et kapløb mellem sikkerhedsansvarlige, der skal nå at implementere sikkerhedsopdateringer, og hackerne som forsøger at finde sårbarhederne og udnytte dem. Hackere er set udnytte sårbarheder blot få dage efter deres offentliggørelse. CFCS ser desværre hyppigt, at sikkerhedsopdateringer overses eller ikke prioriteres. Mange organisationer bliver derfor kompromitteret via kendte sårbarheder, som i nogle tilfælde er flere år gamle, og hvor der eksisterer sikkerhedsopdateringer.

I den tidligere undersøgelsesrapport ”Glemmer du, så husker hackerne” beskrives mere dybdegående, hvordan en dansk organisation blev kompromitteret fem gange på cirka to år med udnyttelse af en ældre, kendt sårbarhed. Rapporten kan læses på CFCS’ hjemmeside.

Med en adgang ind i organisationen vælger nogle hackerne at videresælge deres adgang til andre hackere, som overtager og udfører resten af angrebet. Uanset om det er de oprindelige hackere eller et nyt hold har overtaget, vil de typisk starte med at downloade eller konfigurere det værktøj, som de forventer at benytte undervejs i angrebet på organisationens interne netværk.

2 Konfigurering af værktøjer

Selvom hackernes værktøjskasse ændrer sig konstant, så kan værktøjerne overordnet inddeles i tre forskellige typer, som hackerne typisk anvender undervejs i et målrettet ransomware-angreb:

a. Eksisterende malware på systemet.
b. Nyt malware eller pen-test værktøj.
c. Eksisterende legitime programmer på offerets computer.

a. Hvis hackerne har samarbejdet med andre kriminelle om at få leveret deres egen malware via deres malware, så kan hackerne udnytte de funktioner, som deres indledende malware tilbyder fra start. Emotet har eksempelvis leveret TrickBot, som består af en række selvstændige moduler med et væld af funktioner, som hackerne kan udnytte. Selvom de har adgang til funktioner i sådanne indledende eksisterende malware, vil hackerne dog ofte supplere med yderligere malware eller andre redskaber, som de kan anvende som supplement.

b. Hvis hackerne ikke har adgang til organisationen i kraft af eksisterende malware, må de downloade alle redskaberne selv. Det er eksempelvis tilfældet, hvis hackerne har fået adgang via stjålne loginoplysninger til valide konti med RDP eller VPN fjernadgang.

Download og eksekvering af nyt malware eller pen-test værktøj kræver dog nogle gange lokale administratorrettigheder. Hvis hackerne kun har brugerrettigheder, vil de forsøge at hæve deres privilegier, så de kan downloade og sammensætte deres værktøjskasse. Det hjælper dem også til senere at kunne sprede sig i netværket. Meget af den malware, der leveres som indledende adgang, har indbyggede funktioner til at hæve privilegier og giver dermed hackerne mulighed for at downloade yderligere værktøjer. Hvis hackerne ikke har adgang til disse vil de typisk i stedet forsøge at udnytte sårbarheder eller anvende andre teknikker, som omgår begrænsningerne, således at de alligevel kan få lov til at downloade yderligere værktøj. Dét hackerne vælger at downloade som supplement til evt. eksisterende malware er typisk:

- Flere banktrojanere.
- Rekognosceringsværktøj.
- Credential stealers.

I flere målrettede ransomware-angreb har hackere valgt at downloade flere af de typer banktrojanere, som løbende er blevet udbygget med ekstra funktioner. Aktørerne bag BitPaymer ransomwaren har eksempelvis udnyttet Emotet-adgange til at downloade deres egen banktrojaner, Dridex, som de herefter udførte ransomware-angreb med. Disse supplerende banktrojanere

eller andet malware har typisk forskellige indbyggede funktioner såsom credential stealers eller opsætninger der skaber persistens, som hackerne kan udnytte og som løbende udvikles.

Den anden type værktøj, som hackerne ofte downloader, er rekognosceringsværktøj. Når hackere får adgang til en organisation, ved de ofte ikke, hvor de er i netværket, eller hvad de har adgang til. De har derfor brug for værktøj, som kan skanne netværket. Netværksskannere eller relaterede værktøjer gør dem også i stand til at finde måder, hvorpå de kan sprede sig lateralt i netværket og identificere særligt privilegerede konti, som holder nøglerne til at lægge hele netværk ned på én gang. Netværksskannerne inkluderer kendte legitime netværksskannere, men også pen-test værktøj såsom Nmap, Process Hacker eller BloodHound, som er observeret i flere nylige ransomware-angreb.

Den tredje og sidste type værktøj, som hackerne næsten altid downloader er credential stealers, hvis de ikke allerede har adgang til én indbygget i eksisterende malware. Hvis hackerne vil gøre sig forhåbninger om et succesfuldt målrettet ransomware-angreb, har de brug for at kunne sprede sig i netværket og overtage særligt privilegerede konti. Måden de gør dette på er ofte via credential stealers, som de sammen med netværksskannere anvender til at finde og stjæle loginoplysninger. Mimikatz er en særlig populær credential stealer, der i øjeblikket bliver brugt i mange målrettede ransomware-angreb. Andre udbredte credential stealers og metoder inkluderer LaZagne og ProcDump.

c. Mange af de redskaber, som hackerne anvender, er afhængige af legitime programmer, der allerede er tilstede på computeren. Hackerne udnytter altså, at computere i stigende grad 'fødes' med sofistikerede programmer, som hackerne enten direkte eller indirekte kan udnytte til ondsindede formål. Hackerne misbruger særligt PowerShell, Windows Command Shell, Windows Management Instrumentation (WMI), PsExec og RDP, som ofte allerede er installeret ved levering af computeren, undervejs i målrettede ransomware-angreb.

Den angrebsteknik kaldes også for "Living-off-the-Land", hvor ellers legitime programmer indgår i hackernes værktøjskasse. Teknikken gør det svært at skelne mellem legitim og ondsindet aktivitet. Truslen fra misbrug af legitime programmer er beskrevet mere uddybende i trusselsvurderingen "Hackere misbruger legitime programmer i cyberangreb", som findes på CFCS' hjemmeside.

3 Netværksrekognoscering

Med værktøjerne klar vil hackerne ofte skanne netværket for at finde måder, hvorpå de kan sprede sig til andre klienter eller servere.

Hackerne skanner typisk netværket med legitime netværksskannere eller pentest skannere, som de i nogle tilfælde supplerer med mere specialiserede netværksmonitoreringsprogrammer såsom ProcessHacker eller BloodHound. Skanningerne kan bl.a. genere en liste over åbne porte på klienter og servere i netværket. En åben port betyder, at enhederne 'lytter' til kommunikation via denne

port. Fordi specifikke services kommunikerer over specifikke porte, kan hackerne regne ud hvilke services, som kan benyttes til at kommunikere med andre klienter i samme netværk.

En åben port 3389 betyder i udgangspunktet, at man kan kommunikere over Remote Desktop Protocol (RDP). Server Message Block (SMB) er en anden meget udbredt service, der anvendes af mange organisationer til fildeling. SMB kommunikerer over port 445 eller 139 i ældre versioner. Begge porte vil typisk være åbne i de fleste organisationer. Legitime netværksadministratorer anvender bl.a. RDP til at administrere klienter og servere i netværket, og SMB faciliterer filadgang, som de fleste organisationer er afhængige af. Det ved hackerne, og det udnytter de bl.a. til at bevæge sig lateralt rundt i netværket.

4 Lateral bevægelse

Med en oversigt over klienter og servere med åbne porte vil hackerne ofte forsøge at bevæge sig lateralt på tværs i netværket. Det gør de bl.a. ved at forsøge at logge ind på andre klienter eller servere som lokaladministrator via RDP over port 3389. Når en administrator opretter forbindelse til en klient eller en server, skal de validere deres identitet med et kodeord. Det er dog tit en udfordring for administratorer, som skal holde styr på samtlige kodeord for alle enheder i et netværk, hvilket kan dreje sig om hundrede- eller tusindvis af individuelle kodeord afhængigt af netværket. Derfor er der en tendens til, at kodeordene er ens eller meget forudsigelige på tværs af klienter og servere. Det udgør imidlertid en stor sikkerhedsrisiko, hvis hackerne kan gætte eller på anden vis få fat i kodeordene. Hvis dét sker, kan hackerne frit oprette forbindelse til klienterne eller serverne på netværket med administratorrettigheder.

Her kommer credential stealers ofte ind i billedet. Hackerne anvender bl.a. credential stealers til at stjæle kodeordet til lokaladministrator-kontoen på den første kompromitterede maskine, hvis de ikke allerede har den. Hackerne anvende ofte Mimikatz, der kan stjæle kodeord gemt i computerens hukommelse i klartekst. Andre metoder inkluderer LaZagne og ProcDump til at stjæle loginoplysningerne. Med kodeordet på den første klient afprøver de typisk kodeordet på de andre klienter med åben port 3389 i netværket for at tilgå dem via RDP. Der er eksempler på, at hackerne afprøver hundredvis af kombinationer af kodeord, hvis kodeordet eksempelvis ser ud til at variere med en talrække. Hvis kodeordet på den første kompromitterede maskine f.eks. er 'Admin112' vil hackerne med andre ord afprøve samtlige talkombinationer efter 'Admin' indtil de finder den rigtige. Herefter kan de gentage teknikken på andre maskiner i netværket. Hvis det lykkes dem, kan de frit bevæge sig mellem maskinerne med privilegerede rettigheder.

Alle Windows 7 computere hos et dansk offer havde eksempelvis samme lokale administrator-kodeord. Dét udnyttede hackerne til frit at bevæge sig rundt mellem disse computere, bl.a. via RDP.

En anden mulighed for at sprede sig lateralt er at udnytte sårbarheder. Udnyttelse af sårbarheder er særligt blevet anvendt af de såkaldte kryptoorme, som er en særlig type ransomware, der automatisk udnytter sårbarheder til at sprede sig og kryptere systemer på deres vej. I modsætningen til målrettede ransomware-angreb, der kræver manuel deployering af ransomware, opererer kryptoorme med andre ord autonomt, når de først er leveret til klienten. WannaCry

er den mest kendte kryptoorm, der i løbet af få dage i 2017 inficerede tusindvis af computere verden over med ransomware ved at udnytte EthernalBlue/DoublePulsar sårbarhederne til at sprede sig til klienter med åbne SMB-porte.

5 Persistens i netværket

Med kompromitterede brugere på tværs af netværket vil hackerne som regel cementere deres tilstedeværelse ved at etablere flere forskellige adgange ind i organisationens netværk. På den måde forsøger hackerne at sikre deres tilstedeværelse, såfremt én adgang skulle gå tabt. Hvis hackerne f.eks. fik adgang til organisationen via stjålne loginoplysninger, og medarbejderen valgte at skifte kodeord, så ville de miste deres adgang. Hackerne opsætter overordnet tre forskellige typer ekstra adgange ind i organisationens netværk:

- Legitime fjernadgangssystemer.
- Malware Remote Access Tools (RATs).
- Pen-test Remote Access Tools (RATs).

En af de mest udbredte teknikker til at skabe persistens er udnyttelsen af legitime fjernadgangssystemer. Igen bliver RDP nogle gange misbrugt, hvor hackerne bevidst åbner for en ekstern port, som de herefter kan tilgå fra en hvilken som helst computer med internetadgang. Hackere er også set downloade kommercielle fjernadgangssystemer såsom TeamViewer eller lignende, der fungerer som hackernes alternative indgang ind i systemerne.

En anden metode til at skabe persistens er malware-baseret, hvor hackere f.eks. placerer såkaldte webshells, som åbner op for ekstern adgang via internettet. Amerikanske National Security Agency (NSA) og Australske Australian Signals Directorate (ASD) har i april 2020 offentliggjort en dybdegående rapport netop om webshells, som kan læses på deres hjemmesider.

Webshell
En webshell er et lille stykke programkode, der kan gemmes i en fil, og som giver fjernadgang via internettet.

Webshells fungerer derfor som et såkaldt ”remote access tool” (RAT), der giver hackere mulighed for at læse, skrive, ændre, downloade eller slette filer på en server.

En sidste metode involverer misbrug af pen-test værktøjer med indbyggede fjernadgangsfunktioner. Hackere er eksempelvis set gemme pen-test værktøjet Cobalt Strike på mere end ti forskellige computere under samme angreb, der bl.a. fungerede som hackernes bagdøre. Flere pen-test værktøjer, der faciliterer persistens, er desuden indbygget i flere af hackernes malware.

6 Domæneadministratorrettigheder

Med flere adgange spredt i organisationens netværk, går jagten ind på organisationens kronjuveler: Administratoradgang til Active Directory på Domain Controlleren Servere(n). Domain Control Servere er hjertet i de fleste organisationers

netværk. Den giver adgang til hele organisationens domæne, hvorfra de kan styre store dele af organisationens it-infrastruktur. Disse funktioner er guld værd for hackere, der ønsker at udføre et lammende ransomware-angreb. I stedet for at skulle opnå adgang til hver eneste klient og server i netværket giver en administratoradgang til en Domain Controller mulighed for at udrulle ransomware til hele domænet på én gang. Domæneadministratorer med adgang til Domain Controllere er derfor meget attraktive for hackerne, og deres konti bør være særligt beskyttede.

Første udfordring for hackerne er at finde frem til disse særligt privilegerede konti. Ofte bruger hackerne samme redskaber, som de indledningsvist anvendte til at skanne netværket suppleret med specialudviklede værktøjer, herunder særligt open-source værktøjet BloodHound. BloodHound kan hurtigt kortlægge organisationens hierarki af privilegerede konti og har en meget brugervenlig grafisk brugerflade. Hackerne kan herefter planlægge, hvordan de mest effektivt kan kompromittere forskellige brugere med stigende privilegier for gradvist at bevæge sig frem mod en domæneadministrator.

Hvis BloodHound eller et lignende værktøj ikke afslører domæneadministratorerne, lægger hackerne sig typisk i stedet på lur og venter på, at de afslører sig selv. Måden hackerne kan gøre det på er eksempelvis ved at gemme sig på kompromitterede klienter, og løbende tjekke efter aktive RDP-forbindelser. RDP anvendes som sagt ikke blot som ekstern fjernadgang, men også internt af legitime administratorer til at foretage ændringer på brugernes systemer. Ved løbende at holde øje med aktive RDP-forbindelser kan hackerne således identificere, hvilke konti der har administratorprivilegier og herefter målrette deres indsats mod dem.

Når hackerne har identificeret særligt privilegerede konti, opnår de typisk adgang til dem ved at stjæle deres loginoplysninger. Det sker eksempelvis, når administratorerne opretter RDP-forbindelser til klienter, som allerede er kompromitterede af hackerne. Hvis administratorerne tilgår klienter via RDP-forbindelser, kan deres loginoplysninger i nogle tilfælde stjæles. Det kan de fordi forbindelsen autentificeres gennem et login fra administratoren, hvilket eksponerer deres loginoplysninger for hackerne. Hackerne venter altså tålmodigt på, at RDP-forbindelser oprettes, og stjæler løbende loginoplysninger i håbet om, at en domæneadministratorkonto kigger forbi. Mimikatz er en særlig populær credential stealer, der i øjeblikket bliver brugt i mange målrettede ransomware-angreb. Aktører benytter dog også credential dumping såsom LaZagne og ProcDump til at få fat i loginoplysninger.

Hackerne opretter i nogle tilfælde en ny domæneadministratorkonto, når de har adgang til Domain Controlleren. Det gør de dels i forsøget på at omgå logning, men også for at undgå at miste adgangen igen, i tilfælde af at den kompromitterede domæneadministrator skulle ændre kodeord.

7 Destruering af backup

Med nøglerne til kongeriget i form af domæneadministratorrettigheder vil hackerne ofte sikre sig, at deres angreb ikke blot kan tilbagerulles ved at genskabe systemerne fra backups. Hvis hackerne har domæneadministratorrettigheder, er backups typisk det eneste håb, der kan redde organisationen fra et alvorligt ransomware-angreb.

Domæneadministratoradgangen giver adgang til hele netværket, hvorfra hackerne bl.a. hurtigt kan kortlægge og tilgå hele organisationens datainfrastruktur. Den er ofte allerede kortlagt af organisationen selv med henblik på at udrulle opdateringer, men alternativt anvendes ofte PowerShell scripts eller integrerede søgestrenge i Active Directory brugerfladen til at danne sig en komplet liste over alle enheder i domænet.

Backups findes typisk både lokalt på den enkelte klient, det som kaldes shadow copies, men også som centrale backupløsninger for hele organisationen for de fleste organisationers vedkommende. Aktørerne vil enten forsøge at slette eller kryptere disse systemer.

De lokale backupfiler vil hackerne typisk tilgå med legitime programmer såsom PowerShell eller Windows Management Instrumentation (WMI) og herefter slette shadow copies med VSSADMIN.EXE eller WMIC.EXE.

Centrale backupsystemer kommer i mange forskellige varianter, men hackerne vil aktivt forsøge at uskadeliggøre disse. Hvis det ikke lykkes hackerne at tilgå backups direkte, er de set løbende kryptere backups i en længere periode, før de krypterer resten af organisationens systemer. På den måde forsøger de at øge datatabet for at gøre valget om at betale løsesummen mere attraktivt. Nogle hackere har endda timet krypteringen af systemerne til at sættes i gang, mens der foretages backups.

8 Mulig eksfiltrering af følsom data

Ved udgangen til 2019 begyndte man at kunne se en ny trend, hvor hackerne truer med at lække følsom data fra deres ofre, hvis løsesummen ikke bliver betalt. Hackerne er med andre ord i stigende grad begyndt at udnytte den store indsigt, de typisk opnår i ofrenes organisation, til at eksfiltrere data og afpresse dem yderligere. Flere kriminelle grupper truer med at offentliggøre følsom data på offentlige internetsider, hvis ofrene ikke betaler løsesummen. Andre forsøger at sælge informationen til interesserede købere. Senest er aktørerne kendt som Sodinokibi/REvil begyndt at afholde online auktioner, hvor de sælger ofres data til højstbydende. Nogle organisationer er endda blevet afpresset til, at hackerne mod betaling "lover" at slette deres stjålne data, selvom organisationen aldrig kan vide sig sikker på, at det rent faktisk sker.

Eksfiltreringen af data kan ske på mange forskellige måder, f.eks. gennem de ekstra adgange eller malware, som hackerne har gemt i netværket. I 2019 fandt et it-sikkerhedsfirma eksempelvis et nyt værktøj ved navn Sidoh, som er blevet anvendt til eksfiltrering af data i forbindelse med målrettede ransomware-angreb. Værktøjet søger efter specifikke søgeord såsom "Spy", "Government" og "Secret" og eksfiltrerer dokumenter, som indeholder disse eller lignende ord.

9 Deaktivering af sikkerhedssystemer

Umiddelbart før hackerne deployerer ransomware, vil de typisk deaktivere antivirus og andre sikkerhedssystemer på de enkelte klienter for at sikre sig, at ransomwaren ikke stoppes på de enkelte maskiner.

Ofte anvendes Windows' TASKKILL.EXE eller Net Stop kommandoer, mens andre anvender kommercielle løsninger såsom ProcessHacker, PCHunter, PowerTool x64, GMER, Total Uninstall Portable eller Defender Control til formålet. Hackerne kan relativt nemt gøre dette, idet de allerede har de højst mulige privilegier i domænet.

I tillæg til antivirus og andre sikkerhedsforanstaltninger, stopper de også andre processer, som muligvis kunne forhindre krypteringsprocessen, såsom Exchange Servere og SQL Servere.

10 Deployering af ransomware og afpresning

Først nu deployerer hackerne ransomware på tværs af organisationen, som krypterer systemerne. Selve krypteringen tager typisk ikke lang tid og foretages ofte om natten, mens systemadministratorer normalt ikke er opmærksomme. Om morgenen når de ansatte møder på arbejde, vil offeret være låst ude af deres systemer med en besked om løsesum for at få låst dem op igen.

Nogle gange fastsætter hackerne et specifikt tidspunkt ude i fremtiden, hvor krypteringen skal sættes i gang. Det gør de for at forsøge at få det til at ligne, at krypteringen kommer ud af det blå.

Hackerne spreder typisk deres ransomware gennem legitime programmer såsom PsExec i Microsoft SysInternals, et logon-logoff script via Group Policy Object (GPO) eller Windows Management Interface (WMI).

Det er vigtigt at bemærke, at landskabet af ransomware og kriminelle grupper er i konstant udvikling, men fælles for de fleste typer ransomware er, at de misbruger de samme krypteringsalgoritmer, som til hverdag beskytter almindelig kommunikation på internettet til at kryptere ofrenes systemer. Selvom selve krypteringsmekanismerne er meget ens, så kan det hjælpe oprydningsarbejdet af et angreb at vide præcis, hvilken ransomware man er ramt af. Det kan det, fordi de enkelte grupper anvender specifikke ransomware, og deres angrebstaktikker i nogen grad ligner hinanden på tværs af cases.

Selvom den ransomware ofrene rammes af varierer, så efterlader hackerne typisk en meget enslydende note med instruktioner og krav om betaling af en løsesum. Her forsøger hackerne at overbevise organisationen om, at deres filer nu er utilgængelige, men at hackerne kan dekryptere dem igen mod betaling af en løsesum. Nogle efterlader e-mailadresser som kan benyttes til at kommunikere med grupperne direkte. Løsesummen ønsker de typisk udbetalt i kryptovaluta som Bitcoin eller Monero via en TOR-browser i forsøget på at bevare anonymitet. Ofrene sættes nogle gange under tidspres, hvor beløbet stiger over tid i forsøget på at presse ofrene yderligere til at betale løsesummen.

Størrelsen på løsesummen varierer, og er ofte tilpasset organisationens størrelse og natur med henblik på at opnå størst muligt afkast og sandsynlighed for at opnå betaling. Flere hackere afstemmer nøje beløbene efter organisationernes indtjeningsgrundlag og betydning for samfundet. Beløbene varierer fra et par hundrede tusinde til tocifrede millionbeløb ved målrettede ransomware-angreb. Ifølge nogle sikkerhedsfirmaer kan beløbet imidlertid nogle gange kan forhandles ned.

Hackerne anvender som nævnt typisk de samme stærke krypteringsalgoritmer, som beskytter vores kommunikation på internettet til hverdag. Af samme grund er det ofte rigtigt, at det ikke muligt at dekryptere filer uden hackernes dekrypteringsnøgle. Det er på trods af, at der findes services på internettet, som lover, at de kan dekryptere filerne. Nogle gange lykkes det dog for sikkerhedseksperter at finde fejl i hackernes implementering af algoritmerne, som af og til leder til løsninger, der kan hjælpe ofre med at dekryptere filer. Det sker imidlertid relativt sjældent og hackerne opdager hurtigt deres fejl og retter dem løbende. Europol har sammen med en række virksomheder samlet dekrypteringsværktøjer, som rent faktisk kan dekryptere en del særligt ældre ransomwares. Hjemmesiden hedder https://nomoreransom.org.

CFCS anbefaler generelt, at organisationer ikke betaler løsesummen.

Betaling af løsesummen skaber et incitament for videreførelse af det kriminelle virke, og der er ingen garanti for, at hackerne rent faktisk dekrypterer indholdet, selv hvis løsesummen betales. I nogle tilfælde modtager ofrene heller ikke en dekrypteringsnøgle, selvom de har betalt løsesummen. I andre tilfælde er ofrenes data ikke blot krypteret, men blevet slettet og kan derfor slet ikke genskabes. Hackerne er i nogle tilfælde også kommet til at dobbeltkryptere de samme systemer af flere omgange, så selv hvis hackerne udleverede en dekrypteringsnøgle, kunne ofrene kun dekryptere det første krypteringslag og data forblev utilgængelig.

Det er desuden værd at overveje, at selve dekrypteringen med købte dekrypteringsnøgler kan tage mindst lige så lang tid, som at genskabe data fra backups. Herudover skal man huske på, at hackerne sandsynligvis har gemt bagdøre spredt i netværket, som stadig skal fjernes selv, hvis man vælger at betale løsesummen. Hvis man betaler for dekrypteringsnøgler, ligger der med andre ord stadig et stort arbejde forude med at dekryptere hver enkelt maskine samt at finde og fjerne hackernes mulige bagdøre.

Hvis det kan lade sig gøre, vil genskabelse via backups være den foretrukne løsning. Man skal dog være opmærksom på risikoen for, at bagdørene bliver kopieret med over under genskabelsen. Dét sker, hvis hackerne allerede var til stede i systemerne, da backuppen blev foretaget. Derfor er det vigtigt at fastslå, hvornår hackerne første gang fik adgang til systemerne, og herefter genskabe med en backup fra før denne dato.

Det er desuden værd at overveje, hvor vigtig bevarelsen af troværdigheden i data er for organisationen. Med den betydelige adgang hackerne typisk opnår under et målrettet ransomware-angreb, har de ofte mulighed for at tilgå og redigere i følsom data. Hvis organisationen eksempelvis er et hospital, kan det være meget vigtigt at fastslå, hvorvidt troværdigheden i data i f.eks. patientjournaler er bevaret eller ej.

Selvom alle ransomware-angreb er forskellige og hvert trin kan variere i rækkefølge eller gentages af flere omgange, så følger de fleste angreb forløbet beskrevet her. Viden om hackernes ageren er det bedste redskab, når vi skal forsvare os imod dem. I sidste del af rapporten bruger vi vores viden om hackernes ageren til at præsentere forslag, som kan hjælpe myndigheder og virksomheder med at beskytte sig bedre mod målrettede ransomware-angreb.

Sådan forsvarer du dig mod et målrettet ransomware-angreb

De angrebsteknikker, der er anvendt i de konkrete ransomware-angreb denne rapport bygger på, kobles i dette afsnit op mod specifikke forsvarsinitiativer, der kan modvirke dem.

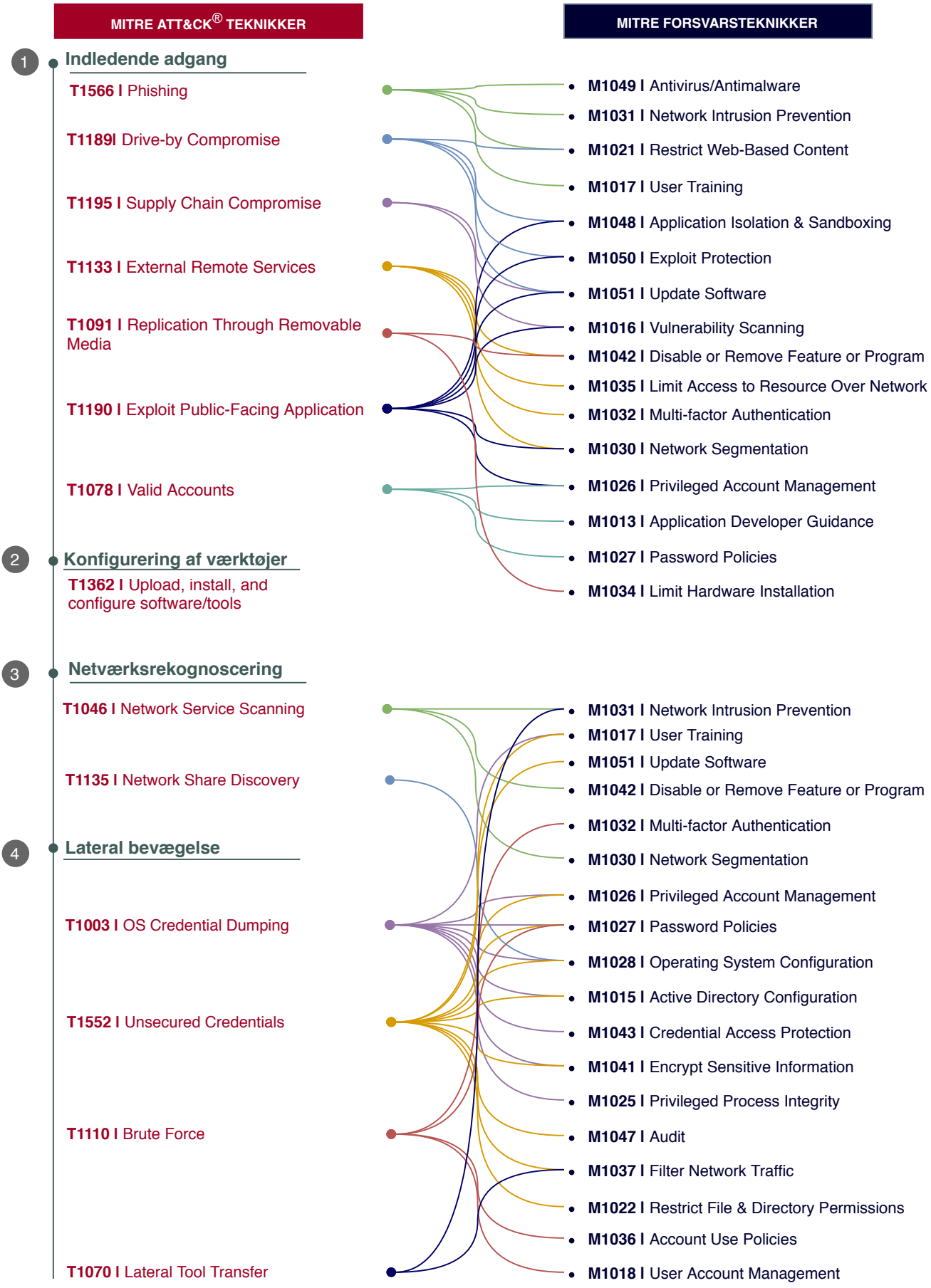
Koblingen er baseret på MITREs ATT&CK® framework. Organisationer kan med fordel anvende illustrationerne i Figur 3-5 aktivt i deres cyberforsvar som guidelines til, hvordan de bedre kan beskytte sig i alle faser af typiske målrettede ransomware-angreb. Da hvert angreb og hver organisation er unik, bør initiativerne dog tilpasses organisationens systemer, politikker og processer og ikke ses som en fuldstændig facitliste. Målgruppen for forsvarsanbefalingerne er særligt større virksomheder og offentlige institutioner.

Initiativerne tager afsæt i princippet om "forsvar i dybden", som betoner, at man ikke bør forlade sig på et enkelt sikringstiltag, men i stedet opbygge et forsvar af sikringstiltag i flere lag, der supplerer hinanden såfremt et enkelt lag bliver omgået. Derved øges sandsynligheden for at opdage, forhindre og begrænse konsekvenserne af et angreb.

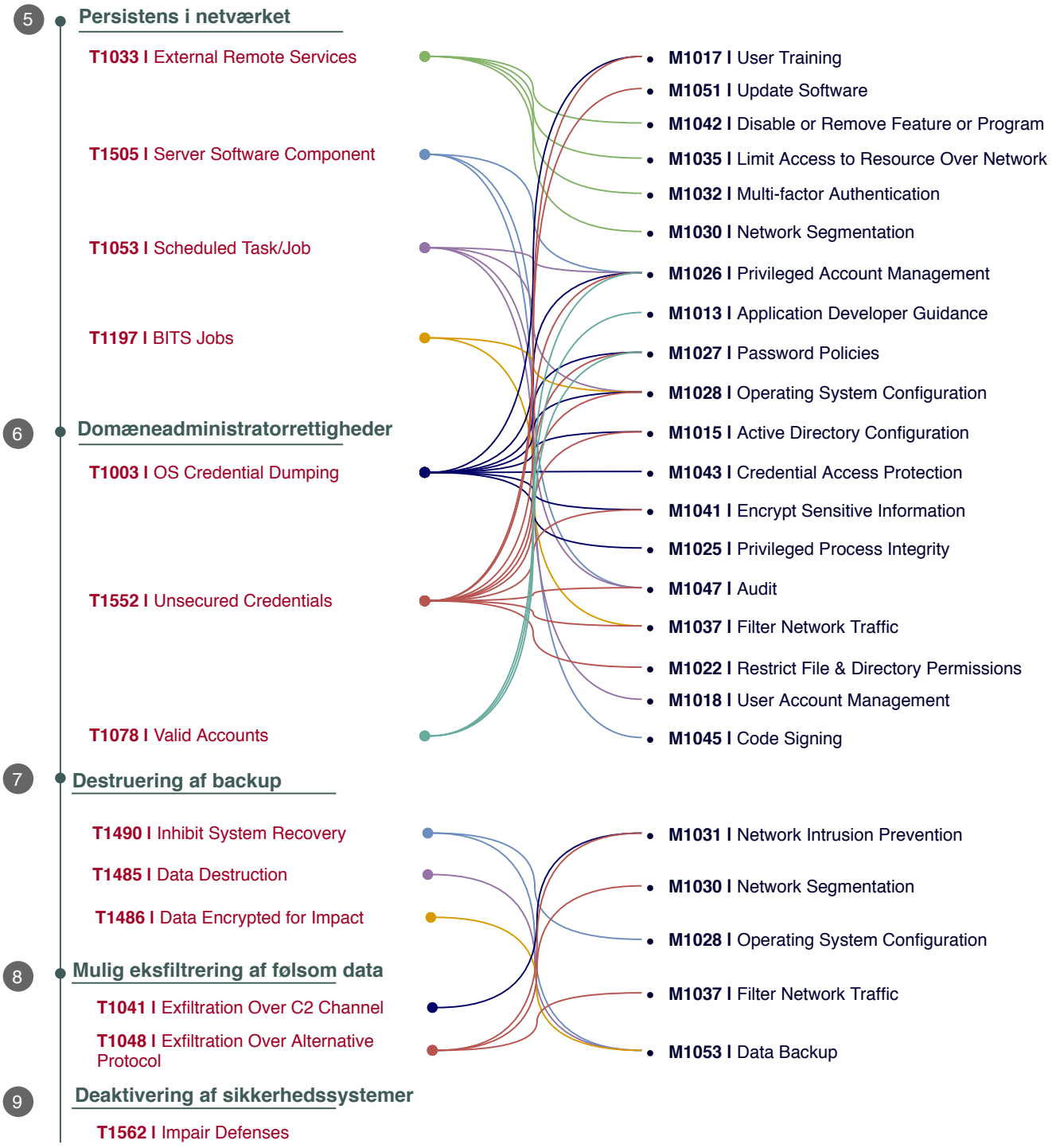
Der er en række grundlæggende sikkerhedstiltag, som det er vigtigt at have styr på. Disse er beskrevet i vejledningen "Cyberforsvar der virker", som kan findes på CFCS' hjemmeside.

Da denne rapport primært er baseret på ransomware-angreb i Microsoft-baserede miljøer, kan de overordnede anbefalinger med fordel suppleres med følgende generelle råd om opsætning af Microsoft miljøer:

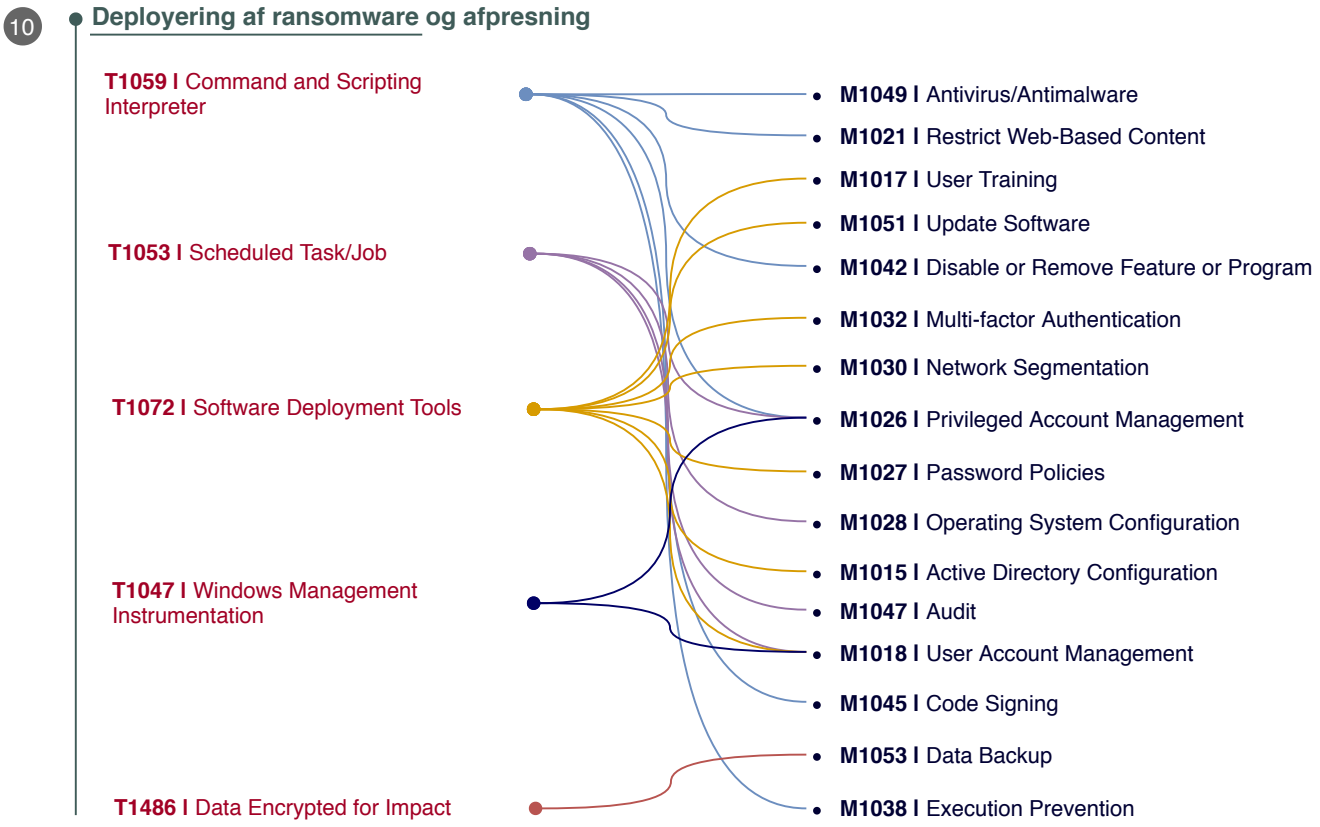
- **Best practices for securing Active Directory**
  Denne guide indeholder Microsofts anbefalinger til at reducere Active Directory-angrebsfladen, håndtere privilegerede konti/grupper og administratormaskiner, sikre Domain Controllers, samt anbefalinger vedrørende logning og monitorering.
- **Windows security baselines**
  Disse baselines indeholder Microsofts anbefalede sikkerhedskonfigurationer og kan bruges som udgangspunkt til at etablere den specifikke opsætning en organisation ønsker. Det medfølgende Policy Analyzer Tool kan bruges til at sammenligne indstillinger i eksisterende Group Policies med Microsofts anbefalede baseline eller med andre Group Policies.



Figur 3: Angrebsteknikker og forsvarsinitiativer - fase 1-4



Figur 4: Angrebsteknikker og forsvarsinitiativer - fase 5-9



Figur 5: Angrebsteknikker og forsvarsinitiativer - fase 10

M1013	Vejledning til applikationsudviklere
Beskrivelse og råd	Ransomware-aktører går efter kontooplysninger, hvor som helst, de kan finde dem. Det er derfor vigtigt, at applikationer ikke gemmer følsomme data eller kontooplysninger usikkert, som eksempelvis kontooplysninger i klar tekst, i kode, i versionsstyrings-/kildekode-værktøjer eller i konfigurationsfiler. Systemadministratorer og applikationsudviklere bør altid sikre, at kontooplysninger opbevares og håndteres på sikker vis.
Evt. anbefalinger	
Læs mere	https://cfcs.dk/da/forebyggelse/vejledninger/passwords/

M1015	Active Directory konfiguration
Beskrivelse og råd	Konfigurér Active Directory til at reducere risikoen for kompromittering af login oplysninger via teknikker, som anvendes i forbindelse med ransomware-angreb. Det bør eksempelvis undgås at gemme loginoplysninger i registreringsdatabasen og logge på klient computere med Domain Administrator konti. Hvis man har ressourcerne hertil, kan Kerberos events overvåges med henblik på at opdage pass-the-hash. Hvis organisationen har adgang til Azure ATP, kan overvågning foretages der. Ved mistanke om AD kompromittering - og med jævnlige mellemrum, f.eks. én gang om året - bør KBRTGT passwordet skiftes. KBRTGT-kontoen anvendes til kryptering og signering af Kerberos tickets. Vær opmærksom på, at passwordet bør skiftes to gange for at nulstille eksisterende Kerberos tickets.
Evt. anbefalinger	• Anvend konti uden overflødige rettigheder til fjernsupport af klienter.
Læs mere	https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/ https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard https://www.microsoft.com/security/blog/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/

M1016	Sårbarhedsskanning
Beskrivelse og råd	Jævnlige sårbarhedsskanninger af både interne og internetvendte systemer kan hjælpe med at identificere sårbarheder. Fundne sårbarheder kan således håndteres, inden de eventuelt udnyttes af ondsindede aktører. Sårbarhedsskanninger kan med fordel suppleres med egentlige penetrationstest, hvor erfarne specialister fra sikkerhedsfirmaer med ekspertise heri aktivt prøver at afdække og udnytte sårbarheder.

	I flere af de analyserede sager i denne rapport, er den indledende kompromittering sket via kendte sårbarheder, som en skanning kunne have identificeret.
Evt. anbefalinger	• Foretag jævnlige skanninger af internetvendte systemer og applikationer. • Foretag jævnlige skanninger af interne netværk og systemer. • Få foretaget penetrationstest af nye og eksisterende systemer og netværk, af erfarne sikkerhedsspecialister. • Monitorer tredje-parts komponenter for offentliggjorte sårbarheder.
Læs mere	https://owasp.org/www-community/Vulnerability_Scanning_Tools https://docs.microsoft.com/en-us/azure/security-center/built-in-vulnerability-assessment https://www.zaproxy.org https://owasp.org/www-project-dependency-check https://cve.mitre.org https://nvd.nist.gov
M1017	**Brugertræning**
Beskrivelse og råd	Udover tekniske sikringstiltag er sikkerhedsbevidste brugere et vigtigt forsvarsværk i kampen mod ransomware. I mange tilfælde af ransomware er den indledende adgang opnået med kontooplysninger fra et succesfuldt phishing-angreb. Brugere bør løbende trænes i at genkende tegn på phishing og på de kneb, der anvendes i social engineering. Alle brugere og administratorer bør være bekendte med organisationens passwordpolitikker og undgå genbrug af passwords.
Evt. anbefalinger	
Læs mere	https://www.ncsc.gov.uk/collection/you-shape-security https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/user-education-and-awareness https://www.social-engineer.org/framework/attack-vectors/phishing-attacks-2/ https://cfcs.dk/da/forebyggelse/vejledninger/passwords/
M1018	**Bruger- og rettighedshåndtering**
Beskrivelse og råd	Håndtering af brugerkonti og deres tildelte rettigheder er vigtige værktøjer i kampen mod ransomware-angreb.

	At have en klar proces og politik for hvordan brugerkonti oprettes, vedligeholdes og nedlægges, kan hjælpe med at reducere angrebsfladen. At processerne og politikken følges, bør sikres gennem egenkontrol. Det er også vigtigt, at konti ikke har unødvendige rettigheder, som kan udnyttes af en hacker, hvis kontoen kompromitteres. Her kan Least-Privilege tilgangen hjælpe ved kun at tildele de rettigheder, der er nødvendige for, at en medarbejder kan udføre sit arbejde. Reagér hurtigt og nulstil proaktivt kodeord på konti, der har været i brug i forbindelse med lækkede legitimationsoplysninger. Gør det så snart lækket - eller forsøget på brute force – opdages.
Evt. anbefalinger	• Hav en klar politik med veldefinerede processer for håndtering af brugerkonti og rettigheder. • Administrative rettigheder for brugere bør kun tildeles undtagelsesvis, tidsbegrænset og baseret på veldokumenterede behov.
Læs mere	https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
M1021	**Adgang til web-baseret indhold**
Beskrivelse og råd	Den indledende infektion med malware i forbindelse med et ransomware-angreb sker ofte ved, at brugeren lokkes til at besøge en ondsindet hjemmeside eller downloade og køre et uønsket script eller applikation (Potentially Unwanted Application). Et effektivt led i forsvarskæden kan derfor være at beskytte mod adgang til kendte malware-hjemmesider, og forhindre download og udførsel af potentielt farlige filer (applikationskontrol). Det kan også ud fra et sikkerhedsmæssigt perspektiv overvejes, om der skal blokeres for reklamer i brugernes browser.
Evt. anbefalinger	• Begræns brugeres mulighed for at køre scripts baseret på filtype eller applikationskontrol. • Overvåg og reagér på alarmer om forsøg på udførsel af blokerede scripts og applikationer. • Anvend en sikker-DNS tjeneste eller implementér anden løsning til beskyttelse mod adgang til skadelige hjemmesider.
Læs mere	https://support.microsoft.com/en-us/help/4562299/protect-your-pc-from-potentially-unwanted-applications https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control
M1022	**Begræns fil og folderrettigheder**
Beskrivelse og råd	I deres forsøg på at undgå opdagelse, vil hackerne ofte prøve at deaktivere sikringstiltag som antivirus og EDR (Endpoint Detection and Response), og at skjule deres spor ved at slette logs. Det bør derfor verificeres, at brugere ikke har adgang til at ændre filer i kritiske applikations- og systemfoldere.

	Brugere bør heller ikke have adgang til at kunne ændre eller slette logs, som kan bruges til at opdage igangværende ondsindede aktiviteter, eller til at undersøge tidligere kompromitteringsaktivitet. Adgang til delte foldere bør ligeledes begrænses til det strengt nødvendige, for at reducere risikoen for, at en kompromitteret konto kan bruges til at finde andre logindetaljer eller private krypteringsnøgler på eksempelvis fællesdrev. Sysinternals-værktøjerne Accesschk og AccessEnum kan eventuelt bruges til at få overblik over brugeradgange til foldere.
Evt. anbefalinger	• Begræns brugeres adgang til at nulstille eller slette logs. • Overvåg og reagér på alarmer om forsøg på skrivning til beskyttede foldere. • Overvåg og reagér på alarmer om forsøg på sletning af logs.
Læs mere	https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/controlled-folders https://docs.microsoft.com/en-us/sharepoint/deploy-file-collaboration https://docs.microsoft.com/en-us/sysinternals/
M1024	**Begræns rettigheder til registreringsdatabasen**
Beskrivelse og råd	Rettigheder til kritiske dele af registreringsdatabasen kan i nogle tilfælde misbruges til at forhindre sikkerhedsværktøjer som antivirus, EDR, firewall eller logløsninger i at starte eller køre.
Evt. anbefalinger	• Begræns brugeres adgang til dele af registreringsdatabasen, der vedrører sikkerhedsværktøjer. • Overvåg og reagér på alarmer om forsøg på ændringer i registreringsdatabasen relateret til sikkerhedsværktøjer.
Læs mere	https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/prevent-changes-to-security-settings-with-tamper-protection
M1025	**Bevár integriteten af privilegerede processer**
Beskrivelse og råd	LSA processen, der validerer brugere og håndhæver sikkerhedspolitikker, kan angribes med henblik på at omgå restriktioner eller udtrække kontooplysninger. LSA Protection eller Windows Defender Credential Guard kan hjælpe til at beskytte mod denne angrebsteknik.
Evt. anbefalinger	
Læs mere	https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard
M1026	**Privilegeret kontoadministration**
Beskrivelse og råd	I flere ransomware-angreb har brugerkonti med lokale administratorrettigheder, eller genbrug af lokale administrator-passwords på tværs af klienter, gjort det nemt for hackerne af få fodfæste og bevæge sig rundt i netværket.

	I Microsoft miljøer kan LAPS anvendes til at sikre unikke passwords på lokale administratorkonti. Ved kun at anvende privilegerede konti på dedikerede administrationsmaskiner, og kun til opgaver der kræver specielle rettigheder, reduceres risikoen for kompromittering.
Evt. anbefalinger	• Brug kun privilegerede konti til aktiviteter, der kræver specielle rettigheder. • Anvend almindelige brugerkonti, uden specielle rettigheder, til almindeligt kontorarbejde. • Administrative rettigheder bør kun tildeles brugere undtagelsesvist, tidsbegrænset og baseret på veldokumenterede behov.
Læs mere	https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-admin-roles-secure https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview https://www.microsoft.com/en-us/download/details.aspx?id=46899
M1027	**Password politikker**
Beskrivelse og råd	Implementering af en passwordpolitik baseret på best practices kan reducere risikoen for kompromittering af konti i et ransomware-angreb. Genbrug aldrig passwords på tværs af konti, heriblandt lokale administratorkonti, og andre privilegerede konti. I Microsoft-miljøer kan LAPS anvendes til at sikre unikke passwords på lokale administratorkonti. Fler-faktor autentifikation kan gøre det svært for hackere at anvende kompromitterede loginoplysninger til at få adgang og fodfæste i en organisations systemer.
Evt. anbefalinger	For anbefalinger vedrørende password- og passwordpolitikker henvises til CFCS' Passwordvejledning.
Læs mere	https://cfcs.dk/da/forebyggelse/vejledninger/passwords/ https://www.microsoft.com/en-us/download/details.aspx?id=46899
M1028	**OS konfiguration**
Beskrivelse og råd	Visse OS-indstillinger kan misbruges af ransomware-aktører til at tilgå cachede kontodetaljer, begrænse organisationens muligheder for hurtig genetablering af krypteret data og til eskalering af privilegier. Da tidligere NTLM versioner er usikre, bør det undersøges om organisationens miljø kan konfigureres til at kræve NTLMv2, hvis Kerberos-baseret autentificering ikke lykkes. Denne konfiguration og stan-

	dardindstillingen for WDigest (UseLogonCredential=0), der deaktiverer caching af kontodetaljer i hukommelsen, kan med fordel påtvinges gennem GPO. Da der findes eksempler på ransomware, som ændrer disse indstillinger, vil overvågning af dem kunne give en indikation på, at et angreb er undervejs. Der er også set eksempler på ransomware, der sletter Volume Shadow Copies ved hjælp at Wmic, Powershell eller Vssadmin, for at gøre det sværere at genskabe data. Det bør derfor sikres, at backup sker til et andet beskyttet system, og at disse aktiviteter monitoreres. Eskalering af privilegier fra en konto med Server Operator privilegier, kan udføres ved at bruge "at" kommandoen til at schedulere et job, der udføres i kontekst af SYSTEM-kontoen på en Domain Controller. Dette kan imødegås med en GPO, der påtvinger at indstillingen: "Domain controller: Allow server operators to schedule tasks" er slået fra.
Evt. anbefalinger	• Påtving OS sikkerhedspolitikker automatisk og begræns antallet af administratorer, der kan foretage ændringer.
Læs mere	https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-controller-allow-server-operators-to-schedule-tasks https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares
M1030	**Netværkssegmentering**
Beskrivelse og råd	Ved netværkssegmentering kan kritiske systemer, funktioner eller ressourcer isoleres, og trafik mellem dem begrænses til det absolut nødvendige. Internettilgængelige tjenester bør som udgangspunkt isoleres (eksempelvis i en DMZ), således at en eventuel kompromittering ikke resulterer i fuld adgang til øvrige netværk eller andre tjenester. Fjernadgang til interne ressourcer bør beskyttes med både kryptering og fler-faktor autentifikation. Fjernadgang fra betroede enheder kan eksempelvis ske via en VPN-løsning. Der er flere eksempler på ransomware-angreb, der er startet med fjernadgang til eksempelvis Remote Desktop Services med brug af kompromitterede eller brute forced kontooplysninger. Remote Desktop servere bør ikke være tilgængelig direkte fra internettet, men i stedet publiceres via en RD Gateway og beskyttes med fler-faktor autentifikation. Løsningen kan med fordel suppleres med en Azure AD Application Proxy, der kan yde ekstra beskyttelse.

	Segmentering af netværket kan besværliggøre en angribers arbejde med at kortlægge og bevæge sig rundt i netværket. Ved udløsning af en krypto-orm, vil segmentering således være med til at begrænse spredningen til de netværkssegmenter, der er adgang til.
Evt. anbefalinger	• Fjernadgang bør ske over en krypteret forbindelse og anvende fler-faktor autentifikation. • Opdel netværket i segmenter således, at enheder (klienter, servere eller netværksudstyr) placeres på segmenter i henhold til deres anvendelse og sensitivitet. • Netværkstrafik mellem enkelte netværkssegmenter bør begrænses og overvåges i henhold til dokumenterede behov.
Læs mere	https://tools.cisco.com/security/center/resources/framework_segmentation https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/network-level-segmentation https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from-anywhere https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-security https://docs.microsoft.com/en-us/azure/virtual-network/ https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares
M1031	**Systemer til forebyggelse af netværksindtrængen**
Beskrivelse og råd	Intrusion Prevention Systems (IPS) har til hensigt til at opdage og fjerne ondsindet trafik mellem netværkssegmenter. I konteksten af ransomware kan IPS blokere for eksempelvis serviceskanninger, ondsindede links og filer i phishingmails, og forsøg på exfiltrering af data. Placeringen i netværket bør besluttes ud fra en risikovurdering, således at systemet opnår størst mulig effekt. Løsning bør aktivt overvåges, og eventuelle alarmer bør håndteres rettidigt.
Evt. anbefalinger	
Læs mere	https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50951
M1032	**Fler-faktor autentifikation**
Beskrivelse og råd	Brug af fler-faktor autentifikation er meget effektivt i kampen mod ransomware. Fler-faktor autentifikation kan reducere risikoen for, at kompromitterede kontooplysninger kan bruges til at opnå adgang til organisationens systemer eller til at udføre kritiske handlinger.

	Der findes flere eksempler på, at fjernadgangstjenester uden fler-faktor autentifikation er blevet tilgået med brute-force eller genbrugte passwords.
Evt. anbefalinger	• Anvend fler-faktor autentifikation hvor muligt og som minimum på al fjernadgang og på alle privilegerede konti. Se i øvrigt CFCS' passwordvejledning for yderligere råd om fler-faktor autentifikation.
Læs mere	https://cfcs.dk/da/forebyggelse/vejledninger/passwords/
M1034	**Begræns hardwareanvendelse**
Beskrivelse og råd	Organisationer bør have en politik for brugen af USB-enheder og flytbare medier. Overvej at blokere for, at brugere eller grupper af brugere kan forbinde ikke-godkendt hardware på systemer, herunder USB-enheder. Sørg for, at alle USB-enheder kontrolleres for malware, før de tilsluttes enheder med forbindelse til netværket. Dette kan eksempelvis ske på en offline men opdateret malware-skanningsstation.
Evt. anbefalinger	• Etablér en politik for anvendelse af flytbare medier.
Læs mere	https://docs.microsoft.com/en-us/windows/security/threat-protection/device-control/control-usb-devices-using-intune
M1035	**Begræns adgang til ressourcer over netværket**
Beskrivelse og råd	Fjernadgangstjenester som Webmail, VPN, Citrix og Remote Desktop Services misbruges ofte til at opnå den indledende adgang til en organisations systemer ved hjælp af kompromitterede loginoplysninger. Adgang til disse tjenester bør derfor kun ske gennem gateways eller proxyer, der sikrer, at brugeren valideres med fler-faktor autentifikation. Gateways og proxyer kan også sikre, at trafikken krypteres, inden adgangen tillades. (se også M1030)
Evt. anbefalinger	• Fjernadgang bør ske over en krypteret forbindelse og anvende fler-faktor autentifikation.
Læs mere	https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from-anywhere https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-security https://docs.citrix.com/en-us/citrix-gateway-service.html
M1036	**Regler for brugerkonti**
Beskrivelse og råd	Loginpolitikker kan bruges til at begrænse det tilladte antal fejlede loginforsøg, hvornår login kan finde sted og hvorfra. Disse sikringstiltag kan bidrage til at reducere risikoen for, at ransomware-aktører kompromitterer loginoplysninger ved hjælp af brute-force angreb, herunder risikoen for password spraying og credential stuffing. Ved anvendelse af meget restriktive politikker er

	der dog en risiko for, at legitime brugere nemt kan lukkes ude af deres konti. Tegn på brute-force angreb kan være et tidligt tegn på forsøg på kompromittering, der kan lede til udløsning af ransomware og bør derfor behandles rettidigt.
Evt. anbefalinger	Se CFCS' passwordvejledning for yderligere råd om konto og password politikker.
Læs mere	https://cfcs.dk/da/forebyggelse/vejledninger/passwords/
M1037	**Filtrér netværkstrafik**
Beskrivelse og råd	Ransomware-aktører exfiltrerer i nogle tilfælde data med henblik på at afpresse den kompromitterede organisation. Dataexfiltreringen kan finde sted over en eksisterende C2-kanal eller gennem hvilken som helst anden tilladt kommunikationskanal. Ved kun at tillade relevante servere at kommunikere ud mod internettet på nødvendige porte, kan man besværliggøre exfiltreringen. Blokerede forsøg på udgående kommunikation fra servere, eller unormale datatransmissionsmønstre kan være en indikation på et dataexfiltreringforsøg.
Evt. anbefalinger	• Tillad kun den nødvendige udgående trafik fra servere til internettet. • Anvend en sikker-DNS tjeneste.
Læs mere	https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-exfiltration-alerts
M1038	**Script- og Applikationskontrol**
Beskrivelse og råd	I de fleste faser af et ransomware-angreb, anvendes scripts og eksekverbare programmer til at opnå hackerens mål. Disse kan være lavet af andre, være egenudviklede eller følge med operativsystemet (eksempelvis Powershell). Applikationskontrol kan være et effektivt værktøj til at begrænse anvendelsen og opdage uautoriserede handlinger, der kan være en del af et aktivt ransomware-angreb. Windows Defender Application Control og Applocker kan eksempelvis bruges til at styre hvilke programmer og scripts, der må køre på en standard arbejdsplads, og er et stærkt supplement til Antivirus og EDR platforme. (Se også M1045)
Evt. anbefalinger	• Begræns brugeres mulighed for at køre scripts baseret på filtype eller applikationskontrol. • Begræns brugeres mulighed for at køre ikke-godkendte applikationer. • Overvåg og reagér på alarmer om forsøg på udførsel af blokerede scripts og applikationer.
Læs mere	https://support.microsoft.com/en-us/help/4562299/protect-your-pc-from-potentially-unwanted-applications

	https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control
M1041	**Kryptér sensitive informationer**
Beskrivelse og råd	Hvis en organisations Windows-miljø stadig tillader RC4-kryptering af Kerberos tickets, kan en servicekontos NTLM password hash findes via Kerberoasting. Opdaterede Windows-miljøer kan anvende AES-kryptering i stedet, og Azure Security Center kan bruges til at opdage forsøg på Kerberoasting. En ukrypteret backup af Domain Controllere kan også være et interessant mål. Ligeså krypteringsnøgler som ikke er opbevaret sikkert.
Evt. anbefalinger	
Læs mere	https://adsecurity.org/?p=3458 https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group https://docs.microsoft.com/en-us/archive/blogs/motiba/detecting-kerberoasting-activity-using-azure-security-center
M1042	**Deaktiver eller fjern funktionalitet / program**
Beskrivelse og råd	Hver tilgængelig tjeneste kan angribes af hackere og eventuelle indbyggede sårbarheder udnyttes. Derfor bør angrebsfladen reduceres, og servere kun tilbyde de nødvendige tjenester. Øvrige tjenester bør afinstalleres, deaktiveres eller blokeres. Ransomware-aktører bruger ofte standardscripting og administrationsværktøjer fra operativsystemet til at foretage rekognoscering, lateral bevægelse og eskalering af privilegier. Hvis disse ikke anvendes til administration af organisationens miljø, kan de fjernes fra klienter og servere, og blokeres ved hjælp af eksempelvis Windows Defender Application Control og/eller Applocker. Execution Policies kan desuden bruges til at begrænse, hvilke Powershell scripts der kan afvikles. Alternativt bør adgang til disse værktøjer begrænses til relevante it-administratorer, og reduceres til de nødvendige funktioner, eksempelvis med Just Enough Administration (JEA).
Evt. anbefalinger	• Deaktiver unødvendige tjenester på systemer for at reducere angrebsfladen. • Tillad kun de nyeste udgaver af nødvendige scriptfortolkere og administrationsværktøjer. • Begræns adgangen til at afvikle scripts og anvende administrationsværktøjer, og overvåg logs om deres anvendelse.
Læs mere	https://docs.microsoft.com/en-us/windows-server/security/windows-services/security-guidelines-for-disabling-system-services-in-windows-server https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

	https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/winrmsecurity
M1043	**Beskyttelse af kontooplysninger**
Beskrivelse og råd	Ransomware-aktører vil ofte forsøge at tilgå cachede konto-oplysninger eller angribe autentificeringsprocessen for at kompromittere konti. For at begrænse caching af konto-oplysninger lokalt på stationære klienter og på servere, kan det overvejes at slå caching fra med en GPO, baseret på et relevant WMI-filter. Laptops kan dog have behov for at cache kontooplysninger for at tillade login, når brugere ikke er direkte forbundet til organisationens netværk. Windows Defender Credential Guard kan yderligere reducere risikoen for, at konto-oplysninger kan tilgås af hackere.
Evt. anbefalinger	
Læs mere	https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication
M1045	**Signering af kode**
Beskrivelse og råd	Ved kun at tillade kryptografisk signeret kode med godkendte signaturer, kan man begrænse, hvilke scripts der kan køres, og dermed gøre hackerens arbejde sværere. Powershell Execution policies kan kontrollere Powershell scripts, men ikke forhindre at Powershell kommandoer udføres manuelt. (Se også M1038)
Evt. anbefalinger	
Læs mere	https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies
M1047	**Audit**
Beskrivelse og råd	Kontooplysninger gemt i registreringsdatabasen, scheduled tasks eller i scripts og andre filer, kan være yderst værdifulde for ransomware-aktører. Det er derfor vigtigt at reducere tilfælde af kontooplysninger gemt i tilgængelige lokationer. De konti, der anvendes bør have begrænsede rettigheder. Det er også vigtigt, med jævne mellemrum, at skanne efter tilfælde af gemte kontooplysninger med henblik på at finde følsomme kontooplysninger, inden en ransomware-aktør gør det.
Evt. anbefalinger	• Søg jævnligt efter gemte kontooplysninger på systemer og i filer.
Læs mere	https://adsecurity.org/?p=2288
M1048	**Applikationsisolering**

Beskrivelse og råd	Ved at begrænse eksekvering af applikationer til et virtuelt sandkasse-miljø, kan muligheden for at skadelig kode breder sig til systemer uden for sandkassen reduceres. Ved isoleret afvikling af programmet, begrænses hvilke data og hvilke processer og systemfunktioner, den ondsindede kode kan få adgang til.
Evt. anbefalinger	
Læs mere	https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-overview https://blogs.windows.com/msedgedev/2017/03/23/strengthening-microsoft-edge-sandbox/
M1049	**Antivirus/antimalware**
Beskrivelse og råd	Et opdateret antivirusprogram kan beskytte imod ondsindet programmel og kode. Det kan automatisk sætte mistænkelige filer i karantæne og alarmere om mistænkelig programadfærd. I flere af de analyserede ransomware-angreb opdagede den installerede antivirus hackernes ondsindede aktivitet flere dage forud for den egentlige deployering af ransomwaren.
Evt. anbefalinger	• Installer og vedligehold et opdateret antivirus/antimalware program. • Monitorer og reager rettidigt på alarmer fra antivirus/antimalware programmer.
Læs mere	https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-microsoft-defender-antivirus-features
M1051	**Software opdatering**
Beskrivelse og råd	Al software, der implementeres bør være omfattet af regelmæssig opdatering, for at sikre, at evt. sårbarheder lukkes hurtigst muligt, så systemet ikke kan udnyttes af offentligt tilgængelige exploits.
Evt. anbefalinger	• Hold al anvendt software opdateret med de seneste sikkerhedsopdateringer
Læs mere	
M1052	**Bruger adgangskontrol**
Beskrivelse og råd	Leverandører og andre partneres betroede adgang kan, hvis de kompromitteres, bruges som trædesten ind i organisationens systemer. Det er derfor vigtigt at sikre sig, at konti til tredjeparter udstedes og administreres i henhold til organisationens politikker. Dette kan blandt andet inkludere, at der kun udstedes personlige konti til identificerbare personer med begrænset gyldighedsperiode, og kun med den nødvendige adgang (principle of least-privilege). Det bør også sikres, at aftalevilkår afspejler tredjepartens ansvar, rapporteringspligt i forbindelse med egen kompromittering, og indeholder relevante sikkerhedskrav til adgangen. Det bør sikres, at anvendelsen af disse konti logges, og at logning eventuelt udvides i forhold til niveauet for egne ikke-priviligerede konti.
Evt. anbefalinger	• Konti udstedt til tredjepart bør følge organisationens sikkerhedspolitikker, og sikkerhedsansvaret afspejles i aftaledokumentet.

Læs mere	https://cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/
M1053	**Backup**
Beskrivelse og råd	For at øge sandsynligheden for at modtage en løsesum, vil angribere ofte forsøge at destruere eventuelle backups inden ransomwaren udløses. Det er derfor vigtigt at opbevare en backup af kritiske data offline, og sikre at kompromitterede administratorkonti ikke har adgang til backupsystemet og dets data. Man kan eksempelvis begrænse administrationen af backupsystemet til konti uden for domænet, og kun tillade adgang fra dedikerede, hærdede og isolerede administrationsmaskiner. Det er desuden vigtigt, jævnligt at sikre sig, at forventede data er inkluderet i backuppen, og teste at det er muligt at genskabe data fra backup.
Evt. anbefalinger	• Tag backup af forretningskritiske data og systemkonfigurationer, og test jævnligt, at backuppen indeholder det forventede. • Opbevar en kopi af kritisk backupdata offline. • Test jævnligt at data kan genskabes fra backup. • Beskyt adgang til backupsystem og backupdata.
Læs mere	

FE bruger denne skala for sandsynligheder i analyser