Cyberangreb mod europæiske energi- og forsyningsselskaber

September 2022

TLP:CLEAR

Indholdsfortegnelse

Introduktion

Om EnergiCERT

EnergiCERT er energisektorens cybersikkerhedscenter.

EnergiCERT er en væsentlig del af sektorens forsvar mod cybertrusler. Vi er med til at opdage og håndtere, når energisektoren udsættes for cyberangreb, og det er hos os, den afgørende viden som kan forebygge det næste angreb, opbygges og deles.

Vi varetager blandt andet monitoreringen af de virksomheder i sektoren, som er tilsluttet vores omfattende sensornetværk. Via sensornetværket monitorerer vi internettrafikken med henblik på at opdage cyberangreb mod dansk, kritisk infrastruktur.

EnergiCERT er en non-profit forening ejet og finansieret af de danske energiseskaber. Vi samarbejder med Europas andre CERT'er og er med i en række cybersikkerhedsorganisationer som gør, at vi har stor viden om truslerne mod kritisk infrastruktur.

Formål

Formålet med at lave denne rapport har været at sikre, at den debat der foregår i både sektoren, blandt politikere og i pressen, er baseret på fakta.
Vi har derfor forsøgt at skabe et overblik over de succesfulde angreb der har været mod europæiske energi- og forsyningsselskaber, samt i hvor høj grad disse angreb har haft en effekt på de såkaldte OT-netværk - altså de netværk, som indeholder de industrielle kontrolsystemer der driver vores kritiske infrastruktur.

Om rapporten

Rapporten giver et samlet overblik over angreb mod energi- og forsyningsselskaber samt de relaterede organisationer, som har kunnet påvirket leverancen af kritisk infrastruktur i disse sektorer.

Kun succesfulde angreb er medtaget

Meget få angrebsforsøg ender som et succesfuldt angreb, hvor selskabet bliver kompromitteret, fordi selskaberne i de fleste tilfælde har gode forsvarsmekanismer.
I rapporten omtales kun angreb, som succesfuldt er kommet forbi selskabernes forsvarsmekanismer og som har haft betydelig konsekvens for virksomhederne.

Kun kendte angreb er medtaget

Desuden er der kun medtaget angreb som allerede er offentlig. Nogle angreb bliver aldrig rapporteret, da det sker at virksomheder vælger at holde det for sig selv med det resultat, at andre ikke kan lære af angrebene. Heldigvis er denne praksis ved at vige for den langt mere åbne praksis, hvor det ikke er skamfuldt at fortælle, man har været udsat for et cyberangreb. Det ses tværti¬mod som en styrke at man er informativ, åben og ærlig.

Kun angreb mod europæiske selskaber er medtaget

Rapporten omhandler udelukkende angreb mod europæiske energi- og forsyningsselskaber, dog er Rusland ikke medtaget. Det betyder at flere kendte, succesfulde angreb mod energiselskaber udenfor Europa ikke indgår i rapporten. Dette er fx angrebet mod Iran med Stuxnet, Colonial Pipeline i USA, Electrobas i Brasilien, Costa Ricas elforsyning, Triton-angrebet samt angrebet mod Kansas' atomkraftværk.

Klassificering

EnergiCERT benytter sig af Traffic Light Protocol (TLP) version 2 ved deling af information for at angive, hvordan informationerne kan deles videre.
Bemærk at TLP version 2 er ny (august 2022).

TLP-skalaen er opdelt i fire niveauer som vist på billedet. Det enkelte niveau angiver om og i hvilket omfang informationen må deles videre. Restriktionerne for deling gælder både ved deling af det akuelle dokument og i anden mundtlig og skriftlig omtale af indholdet.

Dette dokument er klassificeret som TLP:CLEAR, hvilket betyder at informationerne kan deles frit.

Læs mere om Traffic Light Protocol hos FIRST: www.first.org/tlp/.

TLP:**RED**
Informationen er alene tiltænkt modtageren som person.

TLP:**AMBER**
Informationen kan deles internt i modtagerens egen organisation samt med virksomheder eller personer, som får cybersikkerhedsydelser fra modtagerens organisation. Når der bruges **TLP:AMBER+STRICT** betyder det, at informationen alene må deles internt i modtagerens organisation.

TLP:**GREEN**
Informationen kan deles frit indenfor det relevante fællesskab. Et fællesskab kan fx være "danske energiselskaber".

TLP:**CLEAR**
Informationen kan deles ubegrænset.

Kun åbne kilder

Da vi har valgt, at rapporten skal være offentligt tilgængelig, er der alene brugt offentlige kilder til indhentning af informationer.
Det betyder, at vi er afhængige af kilder, hvor vi ikke altid har garanti for nøjagtigheden af data.

Vi har naturligvis gjort alt hvad vi kan for at sikre, at de data vi rapporterer afspejler de faktiske angreb, men vi kan ikke garantere, at der ikke er fejl eller mangler i det rapporterede.

Det betyder desuden, at eventuelle angreb, som vi kender til, men som ikke er offentligt kendte, ikke fremgår af denne rapport.

KORT OPSUMMERING

Baseret på indsamlet data har vi i EnergiCERT givet vores vurdering af situationen.

Opsummering og vurdering

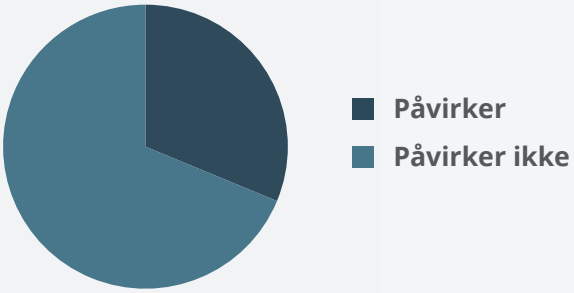
Formål
Formålet med at lave denne rapport har været at sikre, at den debat der foregår i både sektoren, blandt politikere og i pressen er baseret på fakta.
Vi har derfor forsøgt at skabe et overblik over de succesfulde angreb der har været mod europæiske energi- og forsyningsselskaber, samt i hvor høj grad disse angreb har haft en effekt på de såkaldte OT-netværk - altså de netværk, som indeholder de industrielle kontrolsystemer der driver vores kritiske infrastruktur.

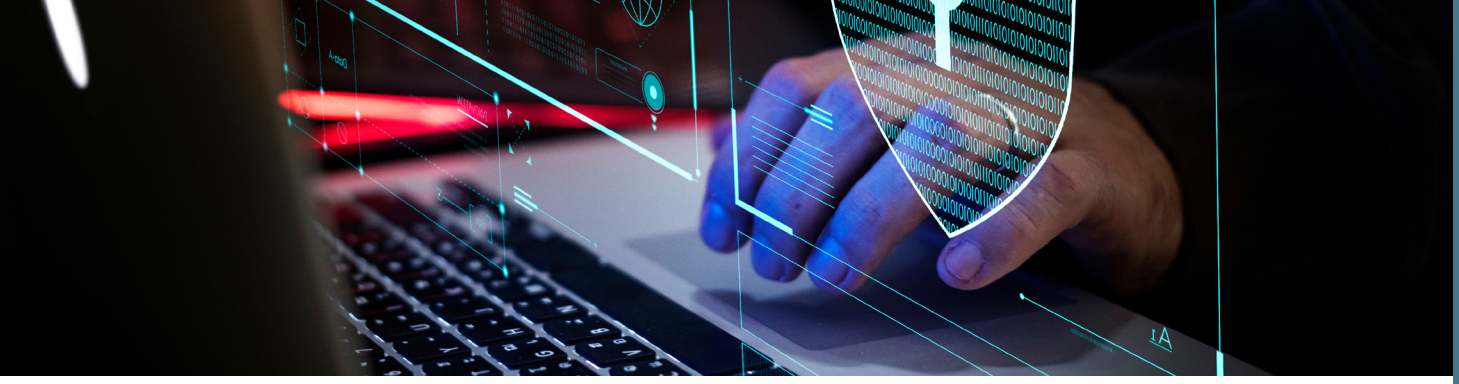
Forbehold og begrænsninger
Da vi har valgt, at rapporten skal være offentligt tilgængelig, er der alene brugt offentlige kilder til indhentning af informationer.
Det betyder, at vi er afhængige af kilder, hvor vi ikke altid har garanti for nøjagtigheden af data. Vi har naturligvis gjort alt hvad vi kan for at sikre, at de data vi rapporterer afspejler de faktiske angreb, men vi kan ikke garantere, at der ikke er fejl eller mangler i det rapporterede.

Vi har desuden begrænset rapporten til at indeholde information om europæiske energi- og forsyningsselskaber (dog undtaget Rusland) samt selskaber, der har en direkte indflydelse på den kritiske infrastruktur i energiselskaberne (fx leverandører som driver dele af infrastrukturen).

Hvad viser data?
Vores data viser, at der har været 48 succesfulde angreb siden 2015 hvor vi så det første.
De fleste angreb har været ransomware-angreb (65%), mens meget få har været angreb, som målrettet er gået efter at påvirke den kritiske infrastruktur (10%).
I alt har der været 15 angreb, som har påvirket den kritiske infrastruktur, hvilket vi definerer som at angrebet har haft indvirkning på de industrielle kontrolsystemer. Heraf har 3 været i Danmark.

Angreb, som påvirker de industrielle kontrolsystemer (OT-netværk)





EnergiCERTs vurdering

Det er bemærkelsesværdigt at så mange angreb, som rammer kritisk infrastruktur, er "almindelige" IT-angreb som fx Ransomware. Det tyder på, at opdelingen mellem de administrative netværk og OT-netværkene, hvor de industrielle kontrolsystemer styres fra, ikke er god nok.

Da der samtidig sker en udvikling hvor flere og flere af de industrielle kontrolsystemer som SRO og SCADA systemer kører på Windows-platformen ser vi ind i en fremtid, hvor ransomware vil være en endnu større trussel mod disse sektorer.

Vi ser det også som tankevækkende, at den samme type af Ransomware kan ramme fem energiselskaber over en periode på fem måneder. Det taler for, at vi i sektoren skal blive endnu bedre til at dele informationer og indarbejde den viden vi har om angreb i beskyttelsen af vores kritiske infrastruktur.

Etableringen af CERT'er - som EnergiCERT - har netop det formål at sikre, at informationer deles på tværs af selskaber i en sektor. Jo bedre vi bliver til at dele med hinanden - og indarbejde de informationer vi får i egne organisationer - jo bedre rustet er vi mod cyberangreb, som kan ramme vores kritiske infrastruktur og dermed vores samfund.

OVERBLIK

EnergiCERT har udarbejdet et overblik over de succesfulde cyberangreb der har været mod europæiske energi- og forsyningsselskaber - herunder selskaber, som har en direkte indflydelse på den europæiske energiforsyning.
Overblikket viser angrebene distribueret over tid og geografi.

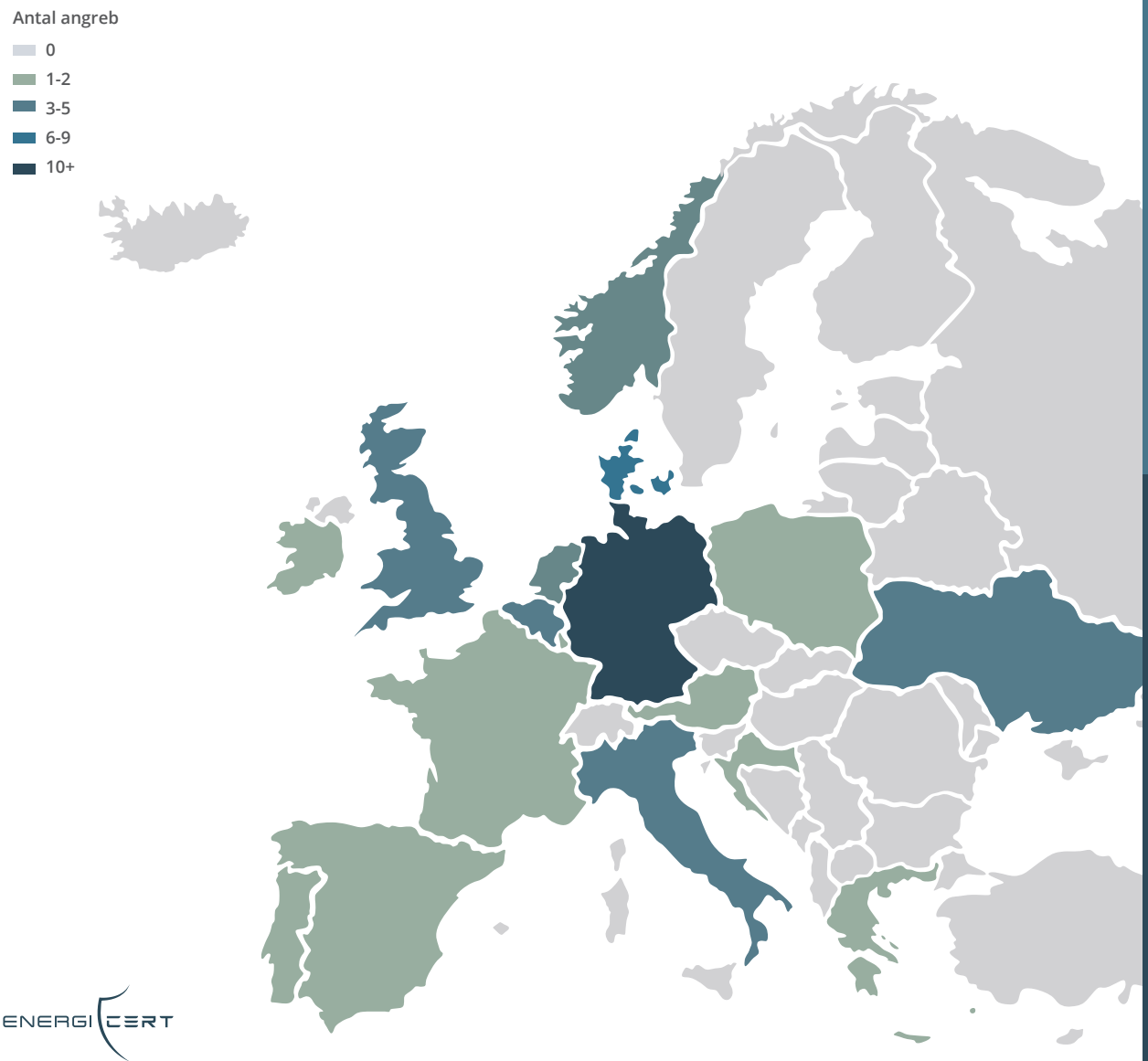
Alle angrebene er vist på side 15-19.

Geografisk fordeling af angreb

Ud fra de angreb, vi har med i rapporten, er der 48 succesfulde cyberangreb mod europæiske energi- og forsyningsvirksomheder der fordeler sig som vist nedenfor.
Kortet viser hvor angrebene har fundet sted og hvor mange angreb, der har været i hvert land.
Lande med flest angreb er Tyskland (12), Danmark (6) og Ukraine (5).
Det er værd at bemærke, at det høje antal for Danmark kan skyldes, at vi i EnergiCERT har lettere ved at tilgå informationer om angreb her end i andre lande. Det er dermed ikke nødvendigvis et udtryk for, at Danmark er et af de lande, som har flest cyberangreb.

Angreb mod Rusland er som nævnt ikke medtaget i denne rapport.

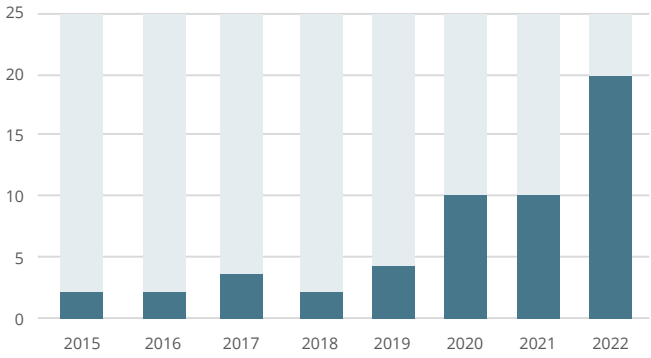
Den fulde liste af angreb er vist i afsnittet “Angreb” længere nede i rapporten.



ENERGI CERT

Tidsmæssig fordeling af angreb

Siden 2015, hvor vi så det første angreb mod et europæisk energiselskab i Ukraine, har der været succesfulde cyberangreb hvert år mod et europæisk energi- eller forsyningsselskab.
I 2022 er det toppet med indtil videre 20 angreb.



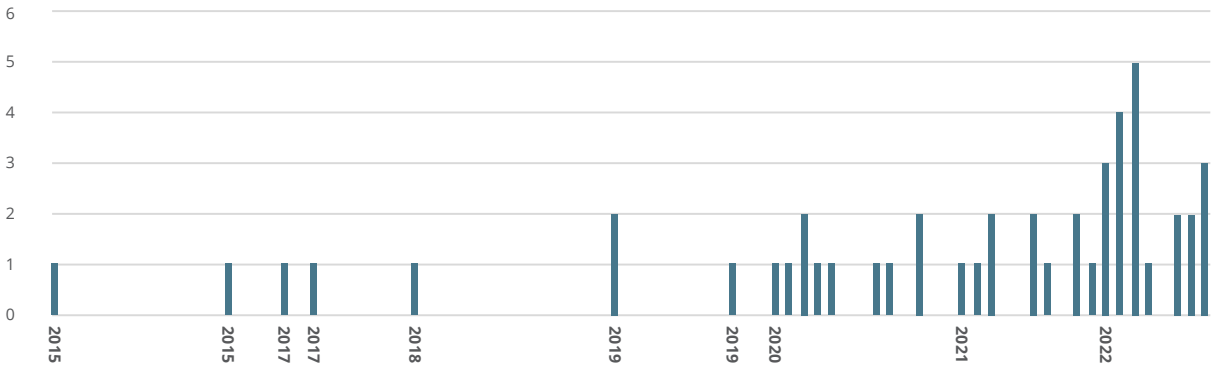
Antal succesfulde angreb pr. år

Som tidligere nævnt i denne rapport kan denne stigning også skyldes, at det er blevet mere acceptabelt (og endda forventeligt) at dele information om angreb nu end det var for blot få år siden.

Samtidig har vi lettere ved at finde oplysninger om nylige angreb end om angreb der er sket for længe siden.

Disse observationer bør medtages i vurderingen, når man vurderer graferne

Succesfuldt angreb
Et cyberangreb, som succesfuldt er kommet forbi virksomhedens forsvarsmekanismer og som har haft betydelig konsekvens for denne.



Antal succesfulde angreb pr. måned

Angrebenes karakteristika

De første succesfulde angreb mod et energiselskab i Europa i 2015 og 2016 var målrettede, statssponsorerede og meget avancerede angreb rettet direkte mod den kritiske infrastruktur i Ukraine. Siden har det vist sig, at den type angreb hører til sjældenhederne.
Risikoen for at blive ramt af et cyberangreb som påvirker den kritiske infrastruktur er langt større ved de angreb, som forsøger at ramme IT-systemerne og som så spreder sig til den kritiske infrastruktur.

48 Angreb mod europæiske energi- og forsyningsselskaber

31 Ransomware-angreb

15 Angreb der påvirkede OT-netværket

Når vi ser på de angreb, der har været mod virksomhederne, er der en klar tendens til, at angreb mod OT starter i IT.
Ud af de 48 angreb, vi har dokumenteret her, er der som nævnt 15 som påvirkede OT. Ifølge vores oplysninger er de alle begyndt i IT.

En anden tendens vi har set generelt - og også her mod energiselskaberne - er, at datatyveri bliver en del af ransomwareangrebene. Det er sket i 10 af ransomwareangrebene vi har registreret.
Derudover har der været 2 tilfælde af spionage og 3 tilfælde af datatyveri hvor angriberne stjæler data af andre årsager end de direkte økonomiske.

13 Ransomware-angreb der også omfatter datatyveri

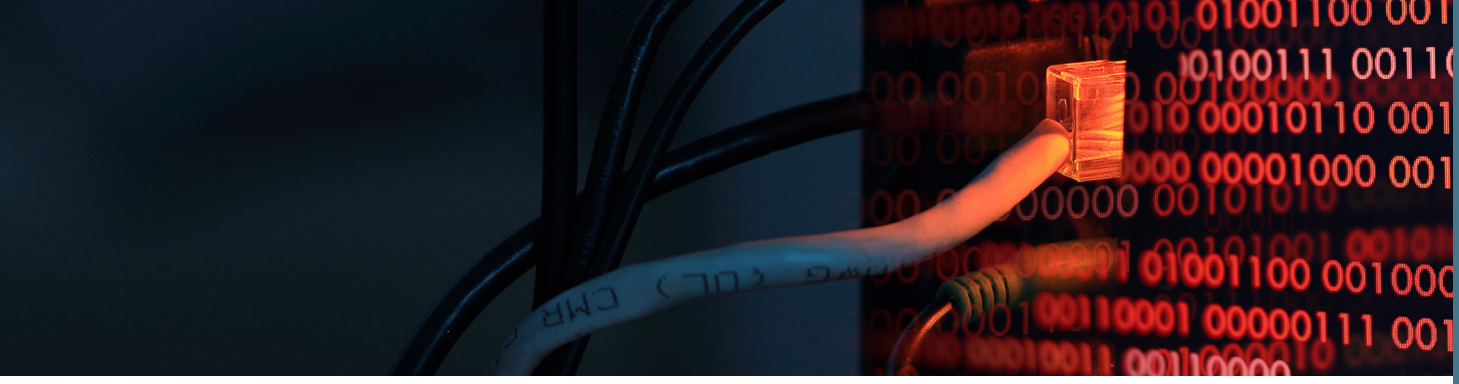
2 Angreb med spionage som fokus

3 Angreb med datatyveri som fokus

Hvis man har sikret sig godt mod ransomwareangreb og i øvrigt følger de anbefalinger, vi giver her i rapporten, er sandsynligheden for at blive udsat for et angreb, som påvirker den kritiske infrastruktur, lille.

ANBEFALINGER

Baseret på historikken af angreb, har EnergiCERT udarbejdet en række anbefalinger som vi vurderer kan styrke vores medlemmers modstandsdygtighed overfor fremtidige angreb mod den kritiske infrastruktur.



IT- og OT-anbefalinger

Listen af anbefalinger kan være lang, men vi har her valgt at udvælge fem anbefalinger til energi- og forsyningsselskaberne som kan hjælpe til at forhindre cyberangreb der påvirker den kritiske infrastruktur.
Generelt skal der arbejdes med sikkerhed i dybden så man undgår, at virksomhedens cyber-forsvar hviler på en enkelt komponent eller proces.

IT-sikkerhed

Da størstedelen af de angreb vi har beskrevet her i rapporten er angreb, som starter i IT, har vi udvalgt fem anbefalinger til energiselskabernes IT-sikkerhed som kan hjælpe til at forhindre, at fx ransomware-angreb får succes.

1 Awareness-træning

Mange ransomware-angreb starter med phishing.

2 Hold systemerne opdaterede

De seneste år er vi gået fra mange dage til få minutter fra vi ser en sårbarhed til det bliver udnyttet af angriberne. Konstante opdateringer - specielt for systemer, som taler med internettet - er vigtigt.

3 Brug multi-faktor godkendelse

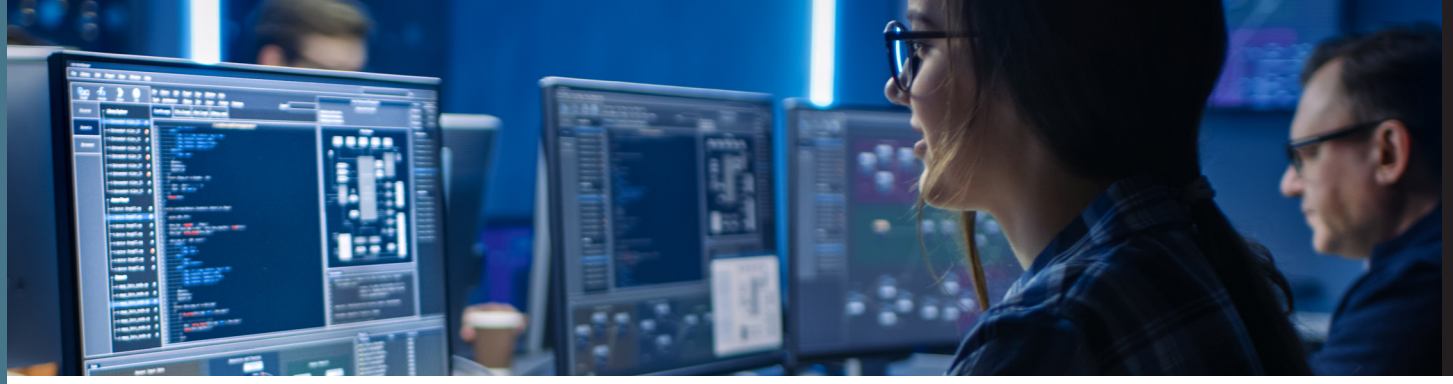
For alle systemer, der er vendt mod internettet, samt alle kritiske systemer, bør der være et ekstra lag af sikkerhed ud over brugernavne og passwords.

4 Begræns administrativ adgang for brugerne

I mange tilfælde har brugerne administrative adgange til deres arbejdsstationer. Dette giver angriberne en stor fordel og bør begrænses til så få brugere som muligt.

5 Opdag og reager på angreb

Sørg for at du kan opdage og reagere på angreb når de sker, fx via netværksmonitore-ring og anden logning.
Sørg derudover for at have tilhørende processer til at håndtere angrebene effektivt så skaden begrænses.



IT- og OT-anbefalinger

OT-sikkerhed

Som vi har set fra mange af angrebene beskrevet her, er der selv i store virksomheder en væsentlig risiko for, at et angreb der starter i IT kan sprede sig til OT.
For at forhindre, at et succesfuldt angreb i de administrative IT-systemer kan påvirke den kritiske infrastruktur, har vi fem udvalgte anbefalinger til OT-sikkerheden i energiselskaberne.

1 Netværkssegmentering
Dette skal sikre at adgangen fra det administrative netværk til OT-netværket begrænses. Brug Purdue-modellen som reference og pas på enheder, der er på både IT- og OT-netværket og dermed kan fungere som bro imellem dem (fx AD).

2 Kend dine enheder
Via processer og værktøjer bør det sikres, at alle enheder i OT-netværket er registreret. Blandt andet så nye enheder kan opdages.

3 Begræns fjernadgang
Undgå direkte fjernadgang til systemer i OT-netværket og sørg for, at der er multi-faktor godkendelse på alle fjernadgange fra IT mod OT.

4 Honeypots og netværksmonitorering
Overvej at implementere såkaldte honeypots i OT-netværket så du vil opdage, hvis en angriber er aktiv i den kritiske infrastruktur - eventuelt kombineret med monitorering af OT-netværkstrafikken. Husk processer til at opdage og reagere på angrebene.

5 Backup
Backup af SCADA systemer, PLC/RTU projektfiler og konfigurationer m.m.

ANGREB

I dette afsnit listes de 48 angreb, EnergiCERT har kunnet identificere.
Listen indeholder information om hvem der er blevet angrebet, på hvilken måde samt hvorvidt angrebet har påvirket OT-netværket hos selskabet.

Angreb mod europæiske energi- og forsynings-selskaber

Listen af angreb nedenfor repræsenterer den viden, EnergiCERT har omkring succesfulde angreb mod europæiske energi- og forsyningsselskaber.
Listen er formentligt ikke komplet da der både vil være angreb, som ikke er offentligt kendt, samt angreb, som vi i EnergiCERT ikke er bekendte med.
Vi modtager meget gerne information om yderligere angreb.
I Appendiks findes en beskrivelse af udvalgte ransomwaretyper.

Virksomhed	Land	Type	Dato	Angreb	Konsekvens	OT påvirket
Prykarpattyaoblenergo, Chernivtsioblenergo, Kyivoblenergo	Ukraine	Energiselskab	23/12-2015	**BlackEnergy** Aktøren Sandworm lavede et manuelt angreb mod 30 substations (7x110kV og 23x35kV) i flere trin (phishing, BlackEnergy malware, manuel kontrol med SCADA, destruktion af data via KillDisk, DoS mod callcentre og nødstrøm til selskaberne blev slået fra).	230.000 mennesker uden strøm i 1-6 timer. I alt blev 73MWh elektricitet fjernet fra nettet (udgjorde ca. 0,015% af strømmen i Ukraine)	Ja
Ukrenergo	Ukraine	Energiselskab	17/12-2016	**Industroyer** Aktøren Sandworm lavede et automatiseret angreb via malwaren Industroyer, som var specifikt lavet til at angribe el-net. Angriberne fjernede muligheden for at tilgå relæer efter de lukkede for strømmen.	1/5 af strømmen til Kyiv blev afbrudt i en time.	Ja
EirGrid	Irland	Energiselskab	20/4-2017	Skjult bag IP adresser i Ghana og Bulgarien fik angriberne adgang til Vodaphone netværket som energiselskabet brugte. Først til deres operationer i Irland og efterfølgende i Wales or Nordirland. Angrebet blev foretaget ved at installere en virtuel aflytningsenhed (GRE tunnel), så al ukrypteret information kunne aflyttes og herefter benyttes til at få adgang til de interne systemer.	Kompromittering af netværk i både DSO og TSO infrastrukturen. Det er ukendt om adgangen blev benyttet til at placere malware. Ingen afbrydelser af forsyningen af el forekom under angrebet.	Nej
Næstved Fjernvarme	Danmark	Fjernvarme	Midt 2017	**Ransomware** Typen Hakunamatata (variant af NMoreira) blev anvendt.	En række filer i SRO-anlægget var blevet låst og kontornetværket var påvirket.	Ja
Isoplus Fjernvarmeteknik	Danmark	Producent og leverandør af fjernvarmesystemer	26/1-2018	**Ransomware** Typen er ukendt.	Låst ude af mailsystemer, ordresystemer og regnskabssytemer.	Nej

Virksomhed	Land	Type	Dato	Angreb	Konsekvens	OT påvirket
British Nuclear	UK	Energiselskab (atomkraft)	13/3-2019	Der er meget begrænsede oplysninger om angrebet da det omhandler atomkraft. Det formodes at være det første, succesfulde cyberangreb mod et atomkraftværk.	Den eneste viden vi har om omfanget af angrebet er dette citat fra dokumenter fra Nuclear Decommissioning Authority: "[we are] aware that an important business in the Nuclear Power Generating Sector has been negatively impacted by a cyber attack"	Ukendt
Hydro	Norge	Hydro-elektrisk energiselskab samt producent af aluminium	18/3-2019	**Ransomware** Typen LockerGoga blev anvendt.	Den globale organisation på tværs af 40 lande mistede al IT-infrastruktur. Energi-delen af selskabet var i stand til at opretholde forsyningen via manuelle processer.	Ja
ENTSO-E	Belgien	TSO koordinering	November 2019	**Remote Access Trojan** Typen PupyRAT blev anvendt til at kompromittere mailserveren	ENTSO-E's mailserver blev kompromitteret og dermed adgangen til emails.	Nej
INA Group	Kroatien	Benzin-stationer	14/2-2020	**Ransomware** Typen CLOP blev anvendt.	En del af virksomhedens servere blev krypteret.	Nej
ENTSO-E	Belgien	TSO koordinering	9/3-2020	Meget lidt information er offentlig, men vores vurdering er, at ENTSO-E's netværk blev kompromitteret, hvilket gav angriberne adgang til interne IT systemer og data.	ENTSO-E har kontaktinformationer og data om de europæiske TSO'er (transmissions-selskaber).	Nej
Energias de Portugal (EDP)	Portugal	Portugals største energiselskab og en af de største operatører af vindmøller i verden	6/4-2020	**Ransomware** Typen RagnarLocker blev anvendt.	Angriberne stjal 10TB data og bad om $10 mio i løsesum. Angrebet ramte ikke OT-netværket.	Nej
Fortum	Polen	Energiselskab der leverer gas og elektricitet	16/4-2020	**Datatyveri** En database med kundeoplysninger blev stjålet.	Virksomheden fik ca. 1 mio. Euro i bøde for tab af persondata.	Nej
Elexon	UK	Balanceansvarlig	11/5-2020	**Ransomware** Typen REvil blev anvendt.	Interne IT-systemer og laptops blev krypteret. Sensitive data blev stjålet.	Nej
Enel Group	Italien	En af europas største energiselskaber med >60 mio kunder	7/6-2020	**Ransomware** Typen Snake (også kendt som EKANS) blev anvendt.	Angrebet blev opdaget inden det kunne sprede sig til hele virksomheden. Dele af det administrative net blev lukket ned.	Nej
Brugg Group / Rittmeyer AG	Tyskland	Leverandør af hydro-elektriske løsninger	10/9-2020	**Ransomware** Typen GUIBrothers blev brugt.	Alle IT-services blev lukket ned.	Nej
Enel Group	Italien	En af europas største energiselskaber med >60 mio kunder	19/10-2020	**Ransomware** Typen Netwalker blev brugt.	Ca. 5TB data blev stjålet og interne systemer blev krypteret. Angriberne bad om $14 mio i løsesum.	Nej
Tønder Forsyning	Danmark	Forsyningsselskab	December 2020	**Ransomware** Angrebet startede med telefonsystemet Lync Edge og herfra til terminal-servere på SRO-anlægget, videre til management-serveren og derfra til it-administrationssystemet.	IT systemer og SRO anlæg var nede i ca. 2 måneder. Personalet på forsyningens renseanlæg måtte klare sig uden SRO-anlæg i et par måneder. Uden it-systemer, overvågning eller alarmer at støtte sig til, har der været behov for manual rundering på anlæggene.	Ja
People's Energy	Skotland	Energiselskab	16/12-2020	**Datatyveri** En database med kundeoplysninger blev stjålet.	En database med sensitive personoplysninger på 270.000 kunder blev stjålet.	Nej
Royal Dutch Shell	Holland	Energiselskab	16/3-2021	**Ransomware** Typen CLOP blev benyttet. Angrebet var rettet mod fildelings-systemet Accellion File Transfer Appliance.	Data blev stjålet - herunder data fra flere af Shells energiselskaber. Ingen af Shells centrale IT systemer blev påvirket.	Nej
Stadtwerke Köflach	Østrig	Energi- og forsyningsselskab	8/4-2021	**Ransomware** Ud fra de sparsomme oplysninger der findes om angrebet tyder det på, at der er tale om ransomware. Typen er ukendt.	Kundeservice og IT-systemer var påvirket. Energi- og drikkevandsforsyningen blev ikke påvirket.	Nej

Virksomhed	Land	Type	Dato	Angreb	Konsekvens	OT påvirket
Albioma	Frankrig	Energiselskab	4/5-2021	**Ransomware** Typen er ukendt.	Interne IT systemer blev påvirket og data blev stjålet. Produktionen af energi blev ikke påvirket.	Nej
Volue	Norge	Leverandør af kritiske infrastruktur services til energisektoren	5/5-2021	**Ransomware** Typen Ryuk blev anvendt.	Angrebet gjorde, at både data i administrative og R&D systemer blev låst. Fjernadgange til energiselskaber blev lukket ned.	Nej
ERG	Italien	Energiselskab	4/8-2021	**Ransomware** Typen Lockbit 2.0 blev anvendt.	Mindre forstyrrelser til de administrative IT-systemer. Angrebet bredte sig ikke til OT-miljøet.	Nej
Kalundborg Forsyning	Danmark	Fjernvameselskab	26/8-2021	**Ransomware** Typen Lockbit 2.0 blev anvendt.	En stor del af IT-systemerne blev krypteret. SRO anlægget holdt op med at virke. Forsyningen kunne fortsætte, men med begrænset visibilitet.	Ja
Stadtwerke Wismar	Tyskland	Energi- og forsyningsselskab (elektricitet, gas, vand og varme)	28/9-2021	**Destruktivt angreb** En trojan blev benyttet til at kryptere data. Ingen løsesum blev forelagt og der blev ikke stjålet data. Angrebet havde alene destruktive egenskaber.	Alle netværksforbindelser blev afbrudt. Systemer blev afbrudt (inkl. email) og data blev krypteret. Det tog 4 måneder at få 85% af systemerne tilbage til normal drift.	Nej
Vestas	Danmark	Vindmølle-producent og operatør	19/11-2021	**Ransomware** Typen Lockbit 2.0 blev anvendt.	Angrebet ramte de administrative systemer og data blev stjålet. OT-systemerne blev ikke ramt.	Nej
Kisters AG	Tyskland	Kritisk infrastruktur leverandør til energiselskaber	30/11-2021	**Ransomware** Typen Conti blev anvendt.	Angrebet ramte de administrative systemer, men nåede ikke at brede sig til OT-systemerne.	Nej
Stadtwerke Pirna	Tyskland	Energi- og forsyningsselskab (strøm, gas, vand, varme)	3/12-2021	**Ransomware** Ud fra de sparsomme tekniske oplysninger om angrebet tyder det på, at der er tale om ransomware.	Mange interne IT-systemer blev berørt, inkl. email. OT-systemerne blev ikke berørt.	Nej
Evos	Holland	Oile og gas opbevaring	29/1-2022	**Ransomware** Typen Conti blev anvendt.	Angrebet påvirkede alle havne i Europa og Afrika som køres af selskabet.	Ja
Oiltanking + Mabanaft	Tyskland	Oile og gas opbevaring og levering	29/1-2022	**Ransomware** Typen BlackCat (også kendt som ALPHV) blev anvendt. Adgangen ind i virksomheden skete via sårbarheder i Microsoft Exchange hvorefter remote access trojanen HYPERBRO blev anvendt.	Angrebet påvirkede evnen til at laste ved havne og tvang Shell til at omdirigere forsyninger til andre depoter. Forsyningsskibe kunne ikke lastes med olie og gas, hvilket påvirkede Aral-benzinstationer i hele Tyskland hvor anden brændstof måtte indkøbes.	Ja
Sea-Invest	Belgien	Oile og gas opbevaring og levering	30/1-2022	**Ransomware** Typen Conti blev anvendt.	Underdivisionen Sea-Tank måtte stoppe alle operationer i 2 dage. Aktiviteter ved havne blev stoppet.	Ja
Regionalt energiselskab	Ukraine	Energiselskab	Februar 2022	**Industroyer2** Gruppen Sandworm angreb energiselskabet med avanceret, destruktiv malware målrettet til at tage energiforsyningen ud.	Den 8/4 skulle substationer og anden kritisk infrastruktur være udkoblet, men angrebet blev opdaget kort inden. Systemerne var dog kompromitterede og malwaren placeret i OT-miljøerne.	Ja
Gruppo Dolomiti Energia	Italien	Energi- og forsyningsselskab (el, vand, gas, varme)	8/2-2022	Der er meget lidt offentlig viden om hvordan angrebet blev udført.	Interne IT-systemer blev påvirket. Der var ikke indikationer på tab af data	Nej
Viasat	Virksomheden hører hjemme i USA, men angrebet var mod den ukrainske del af infrastrukturen.	Kommunikations-leverandør til kritisk infrastruktur	24/2-2022	**Destruktivt angreb** Brugte blandt andet AcidRain malware - en wiper designet til at destruere modems og routere. Efter infiltrering af netværket bevægede angriberen sig via et sikkert management netværk til det OT-net, som driver satellitnetværket.	Viasat bruges som kommunikations-leverandør til meget kritisk infrastruktur både i Ukraine og andre lande. Angrebet havde den effekt, at en lang række modems i Ukraine blev gjort ubrugelige. Angrebet påvirkede samtidig 5.800 Enercon vindmøller i Tyskland samt tusindvis af organisationer på tværs af hele Europa.	Ja

Virksomhed	Land	Type	Dato	Angreb	Konsekvens	OT påvirket
LIFA A/S	Danmark	Leverandør til danske energiselskaber	27/2-2022	**Ransomware** Typen Conti blev anvendt.	Store dele af virksomheden blev påvirket.	Nej
General Directorate of Civil Protection and Emergencies (DGPCE)	Spanien	Strålings-sensor netværk	Marts 2022	**Insider** To interne medarbejdere stod bag angrebet.	Mere end 300 ud af 800 sensorer blev sat ud af drift i mere end to måneder, hvilket nedsatte evnen til at opdage radiaktiv stråling fra atomkraftanlæg.	Ja
Rosneft Deutschland	Tyskland	Petroleums-raffinaderi	11/3-2022	**Spionage** Anonymous-gruppen fik adgang til interne systemer og data.	Omkring 20TB data blev stjålet, inkl. alle emails med mere. OT-netværket blev ikke berørt.	Nej
Atomar sikkerheds-organisation	Ukraine	Sikkerheds-organisation for atomkraft i Ukraine	13/3-2022	**Spionage** Aktøren Bromine (også kendt som EnergeticBear) benyttede en adgang fra december 2021 hvor organisationen blev kompromitteret	Data blev stjålet	Nej
Iberdrola	Spanien	Energiselskab	15/3-2022	**Datatyveri** En ukendt hackergruppe fik adgang til persondata om energikunderne.	Data om 1,3 mio. kunder blev lækket.	Nej
Nordex	Tyskland (samt Kina, Mexico, USA, Brasilien, Spanien og Indien)	Vindmølle-producent og operatør	31/3-2022	**Ransomware** Typen Conti blev anvendt.	Alle IT-systemer blev lukket ned og fjernadgangen til alle turbiner blev afbrudt.	Ja
Deutsche Windtechnik	Tyskland	Vindmølle-producent og operatør	11/4-2022	**Ransomware** Typen BlackBasta blev anvendt.	Fjernmonitorering af alle turbiner var nede i 2 dage.	Ja
Mainzer Stadtwerke	Tyskland	Energiselskab	11/6-2022	**Ransomware** Typen BlackCat blev formentligt anvendt.	Angrebet ramte administrative systemer og medførte tab af persondata.	Nej
Entage	Tyskland	Energiselskab	11/6-2022	**Ransomware** Typen BlackCat blev formentligt anvendt.	Angrebet ramte administrative systemer og medførte tab af persondata	Nej
Enovos og Creos (begge del af Encevo)	Luxembourg	Energiselskab	22/7-2022	**Ransomware** Typen BlackCat (også kendt som ALPHV) blev anvendt.	Angrebet ramte administrative systemer hos begge selskaber og medførte tab af ca. 180.000 filer.	Nej
iSTA	Tyskland (og mange andre lande inkl. Danmark)	Leverandør og operatør af fjernaflæst målerudstyr til fjernvarme, drikkevand m.m. Mere end 25 mio forbundne enheder.	29/7-2022	**Ransomware** Typen Daixin Team blev anvendt. Angrebet startede via kompromittering af en af de 400.000 gateways, som forbinder de 25 mio forbundne IIoT-enheder.	Angrebet har krypteret tusindvis af servere og har derigennem ramt en række forsyningsselskaber i Europa - fx Marymont Potok i Polen som ikke kan afregne vandforbruget hos forbrugerne. 370GB data er blevet stjålet.	Ja
Semikron	Tyskland	Producent af udstyr til energi (vind, sol, energiopbevaring)	6/8-2022	**Ransomware** Typen LV (også kendt som Gold Northfield, baseret på REvil) blev anvendt.	Data krypteret og systemer låst ligesom data er blevet stjålet.	Nej
South Staffs Water	UK	Vandforsyning	15/8-2022	**Ransomware** Typen Cl0p blev anvendt.	Data blev stjålet, men ingen systemer blev lukket ned da gruppen har annonceret, de ikke vil påvirke kritisk infrastruktur.	Nej
DESFA	Grækenland	Grækenlands største gasdistributør	21/8-2022	**Ransomware** Typen Ragnar Locker blev anvendt.	Interne systemer blev lukket ned og data blev stjålet.	Nej

APPENDIKS - ANGREBSTYPER

Da mange af angrebene har været ransomware, vil vi i dette kapitel beskrive to udvalgte ransomware-typer i yderligere detaljer.

Ransomware

Fra oversigten over succesfulde angreb ser vi, at det for størstepartens vedkommende (65%) er ransomware som benyttes.

Vi har derfor i de følgende sider beskrevet to meget udbredte typer af ransomware, BlackBasta og Conti.

Beskrivelserne skal ses som en uddybende forklaring til, hvordan disse typer af ransomware benyttes og kan bruges til at skabe bedre forståelse for, hvordan man som virksomhed beskytter sig mod dem.

Beskrivelserne stammer fra EnergiCERTs trusselsrapporter.

BlackBasta ransomware

BlackBasta gruppes historie

Ransomwaren, BlackBasta, menes at være forbundet med Conti ransomware på grund af flere operationelle ligheder. Conti-gruppen påstod dog den 12. maj, at de ikke havde nogen tilknytning til BlackBasta ransomware-gruppen.

BlackBasta er en relativt ny ransomware-gruppe, der først dukkede op i april 2022, hvilket betyder, at medlemmets leverandør blev ramt kort efter, at gruppen begyndte at være aktiv.

Indtil nu har denne gruppe ramt mere end 30 forskellige ofre på tværs af flere brancher. Gruppen bruger en dobbelt afpresningsstrategi, hvor angriberne ikke kun udfører ransomware, men også stjæler data og truer med at frigive det offentligt, hvis løsepengekravene ikke bliver opfyldt. Data-afsløringsstadiet for disse angreb finder sted på en webservice, der er tilgængeligt via TOR-browseren. Som en mekanisme til at lægge pres for at tvinge offeret til at betale løsesummen, vil operatørerne af BlackBasta gradvist offentliggøre de stjålne data.

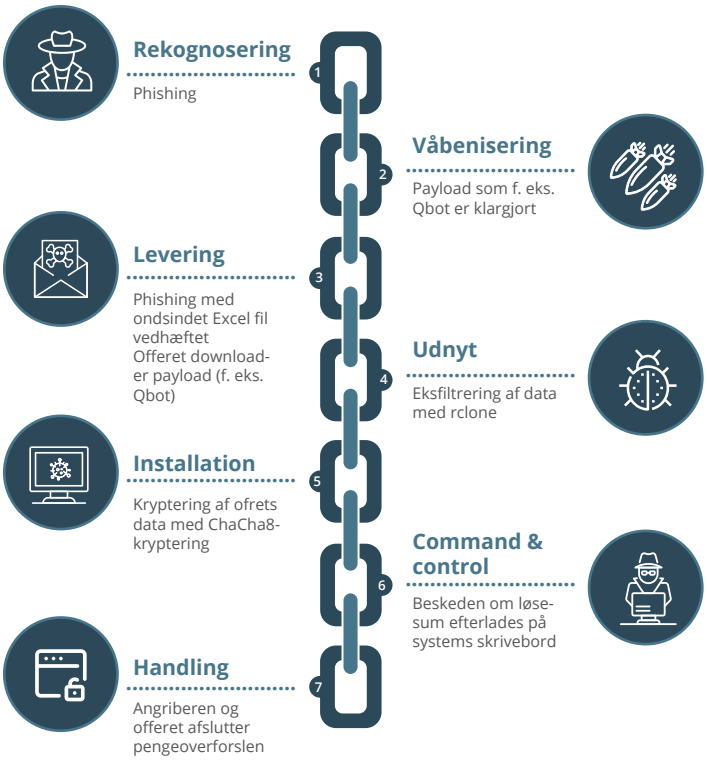
I lighed med Conti ransomware er BlackBasta meget farlig på grund af den høje hastighed, som den bliver implementeret med. Det er derfor udfordrende at opdage symptomer på en infektion, før ransomwaren er blevet implementeret.

BlackBasta Cyber Kill Chain

Datakrypteringen, der bruges af Black-Basta, virker kun med administrator-rettigheder. Dette betyder, at trussels-aktøren skal få privilegeret adgang eller bruge stjålne legitimationsoplysninger for at kunne køre ransomwaren.

Ligesom med Conti ransomware, er den mest almindelige metode til rekognoscering phishing. Offeret får en phishing-e-mail, der indeholder en ondsindet Excel-fil med en payload. I flere tilfælde blev payloaden identificeret som Qbot.

I udnyttelsesfasen downloades og installeres Qbot. Angriberen har nu fuld kontrol over systemet, og starter dataeksfiltreringen af ofrenes data til en af gruppens private servere ved hjælp af softwaren rclone. Desuden deaktiveres Windows Defender for at undgå, at angrebet opdages eller stoppes.



Derefter begynder BlackBasta installationsfasen. En legitim Windows-tjeneste udnyttes til at starte krypteringsprocessen. De anvendte krypteringsteknikker ligner dem, som Conti ransomware benytter: filer på systemet krypteres ved hjælp af ChaCha20-algoritmen. Den nødvendige nøgle til at dekryptere filerne, krypteres derefter med RSA-4096. I modsætning til Conti ransomware, tilføjes filerne .basta suffiks, når de er krypteret.
På dette tidspunkt er alle vigtige filer krypteret. Skrivebordsbaggrunden ændres derefter til at vise en løsesums-notifikationen.

Teksten på baggrunden lyder således:

> Your network is encrypted by the BlackBasta group.
> Instructions in the file readme.txt

BlackBasta efterlader også løsesums notifikationen, readme.txt, som indeholder et unikt ID for organisationen og en URL til en chatside til at forhandle med angriberne. Chatsiden kan kun tilgås via TOR-browser.

Bemærk

BlackBasta er også i stand til at kryptere VMware ESXi-servere. BlackBasta-gruppen har inkorporeret denne Linux-version af ransomwaren, da flere og flere organisationer bruger virtuelle maskiner til omkostningseffektivitet og nemmere administration af enheder. Denne variant bruger også ChaCha20-algoritmen til kryptering.

Conti ransomware

Conti gruppens historie

I slutning af februar 2022 blev LIFA A/S, en leverandør til mange danske energivirksomheder, ramt af Conti ransomware (som nævnt i Afsnit 1). Hændelsen fik, selvom den ikke ramte vores medlemmer direkte, indflydelse på den danske energisektor. Nogle af EnergiCERTs medlemmer, som samarbejder med LIFA A/S, besluttede sig for at isolere deres systemer fra leverandørens for at undgå, at ransomwaren kunne sprede sig til deres systemer. Conti er en gruppe af cyberkriminelle og deres forretning er Ransomware-as-a-Service. De blev første gang blev observeret i oktober 2019.

Hvad er Ransomware-as-a-Service (RaaS)?

RaaS betyder at udviklerne af ransomware sælger eller leaser deres ransomware teknologi til andre selskaber, som derefter bruger denne teknologi til at udføre angreb.

Conti ransomware er ekstremt skadelig på grund af den hastighed, hvormed data krypteres og spredes til andre systemer. Conti gruppen menes at komme fra Rusland og er blevet beskyldt for ransomwareangreb rettet mod mange virksomheder, herunder kritisk infrastruktur. I maj sidste år kompromitterede Conti det irske sundhedsvæsens netværk, hvilket tvang en landsdækkende nedlukning af it-systemer og kostede regeringen mere end 100 millioner dollars.

I slutningen af februar 2022 har Conti hackergruppen truet med at bruge deres fulde kapacitet til "gengældelse". Det vil ifølge gruppen ske, såfremt Vesten angriber kritisk infrastruktur i Rusland eller russisktalende regioner. Ifølge Center for Cybersikkerhed skal udtalelserne tages alvorligt, da gruppen har en meget væsentlig kapacitet til at lave målrettede ransomwareangreb. I øvrigt står udtalelserne i modsætning til en ellers øget tilbageholdenhed med at angribe kritisk infrastruktur i visse kriminelle netværk siden 2021.

Som et resultat af denne modsætning, lækkede ukrainske medlemmer af Conti-trusselsgruppen interne chats og logdata. De lækkede samtaler i Conti-lækagen er dateret mellem januar 2021 og februar 2022 og indeholder information og TTP'er (Tactics, Techniques, and Procedures) om Conti-gruppens seneste aktiviteter.

Sammenhæng mellem Ryuk og Conti grupperne

Baseret på en analyse af ransomware og sammenligning af bitcoin-wallets, er der en forbindelse mellem ransomware grupperne Conti og Ryuk. De kan være det samme hold, eller to hold, der deler deres ressourcer. De første eksempler på Ryuk blev udgivet under navnet Hermes ransomware af en russisktalende trusselsaktør navngivet CryptoTech i februar 2017.
Conti kan ses som en videreudvikling af Ryuk ransomware. De deler en række ligheder såsom brug af Trickbot, Emotet (som vi har skrevet om i Q4 2021 Trusselsrapporten) og BazarLocker som deres payload distributors.

MITRE ATT&CK® gruppens ID: G0102

Tilknyttede grupper:
Hermes, Ryuk, Wizar Spider, UNC1878, TEMP.MixMaster, Grim Spider

Conti's brug af legitime værktøjer og programmer

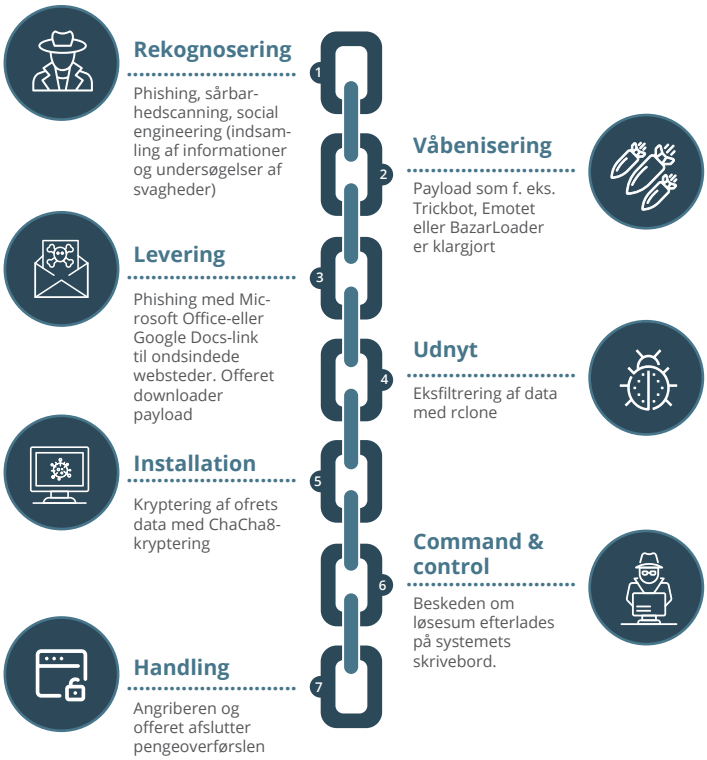
Ovenstående softwarepakker (Trickbot, Emotet og BazarLocker) udfører arbejdet med at levere ransomwaren til offerets system.
Conti ransomware misbruger også flere teknologier, der ellers har lovlig kommerciel brug:

- Cobalt Strike, som er et kommercielt remote access tool, der ofte bruges i simuleringer af cybersikkerhedshændelser
- rclone - kommandolinjeprogram til styring af cloud data storage
- AnyDesk og Atera programmer, der giver fjernadgang til computere og andre enheder[4]
- Ngrok der genererer et interface, hvor brugere kan inspicere al HTTP-trafik, der kører over specificerede tunneler i realtid
- TOR, open-source web browser designet til sikker, anonym kommunikation

Conti Cyber Kill Chain

Conti ændrer konstant deres angrebsmetoder. De udnytter nye exploits og det faktum, at mange brugere sjældent opdaterer deres enheder. Conti ransomwares operationsmodel er stærkt automatiseret, hvilket gør det muligt for dem at udnytte nye sårbarheder inden for få timer efter, at de er blevet offentliggjort.

Den mest almindelige metode til rekognosering er phishing. Den næstmest almindelige metode, sårbarhedsscanning, bruger automatiserede bots, der tjekker for offentligt eksponerede og kendte sårbarheder. På denne måde, indhenter angriberne information og finder svagheder.



Phishingkampagner indeholder ofte Microsoft Office- eller Google Docs-links. Angriberne bruger så disse links til levering af payload, hvor de omdirigerer ofrene til ondsindede websteder. Det vil sige, at ofrene downloader payload med f.eks. Trickbot, Emotet eller BazarLoader backdoor. Når offeret har installeret denne payload, kan angriberne påbegynde undersøgelsen af virksomhedens netværk. Ransomwaren vil forsøge at finde alle mapper og netværksshares på det kompromitterede system med specielt fokus på kritiske systemer (domænecontrollere eller backupservere).
Angriberne vurderer så, om ofrenes data er vigtige nok for virksomheden. Hvis de konkluderer, at de er vigtige nok, så begynder de udnyttelsesfasen. De eksfiltrerer dataene til en anonym konto på den anonyme cloud-baserede tjeneste kaldet MEGA. Værktøjet der bruges til eksfiltration kaldes "rclone".
Derefter begynder Conti installationsfasen. Data krypteres ved hjælp af ChaCha8-kryptering med tilfældigt generede nøgler for hver fil inde i det system, der angribes. Hver genereret nøgle er krypteret med en RSA-4096 offentlig nøgle og gemt på et bestemt sted for hver fil. Disse nøgler bruges til at identificere offeret, administrere forhandlinger og til sidst (i nogle tilfælde) generere dekrypteringskoder efter betalingen.
På dette tidspunkt er alle vigtige filer krypteret, og sikkerhedskopier slettet. En readme.txt-fil, der indeholder løsesums notifikation efterlades på skrivebordet på offerets system.
Løsesums notifikationen indeholder instruktioner om installation af TOR-browseren for at få adgang til Conti gruppens skjulte webservice, som foregår i handlingsfasen. Ved at bruge en unik ID fra løsesums notifikationen, kan offeret derefter få adgang til en chatside til at forhandle med angriberne.

Kontakt os

Kontakt EnergiCERT på følgende nummer:

+45 88327140

Hvis du har spørgsmål om eller til EnergiCERT er du også velkommen til at sende en email:

info@energicert.dk

PGP nøgle:

86B4 C9C8 5C53 513C 1D8F 6F14 B877 3115 64F5 AE13

Besøgs- og postadresse:

Sommerfuglevej 2A
6000 Kolding

CVR nummer:

41369841

Satellittelefon:

+88 1622456029