



# Angrebet mod dansk, kritisk infrastruktur

---

Udgivet: november 2023



## Indholdsfortegnelse

**SIDE-3** Opsummering

**SIDE-4** Om SektorCERT

**SIDE-5** Om rapporten

**SIDE-6** SektorCERTs sensornettværk

**SIDE-7** Analyse

**SIDE-8** Detaljeret analyse af sagen

**SIDE-17** Konklusion og anbefalinger

**SIDE-18** Konklusion

**SIDE-19** Anbefalinger

**SIDE-21** Tidslinje

**SIDE-22** Tidslinje for angrebene

**SIDE-27** Cyber kill chain for det samlede angreb

**SIDE-28** Appendix

**SIDE-29** IOC'er

**SIDE-30** CVE'er

**SIDE-31** Links



## Opsummering

I maj måned 2023 blev den danske, kritiske infrastruktur utsat for det hidtil mest omfangsrike, cyberrelaterede angreb vi har oplevet i Danmark.

22 selskaber, som driver dele af den danske energiinfrastruktur, blev kompromitteret i et koordineret angreb. Resultatet var, at angriberne opnåede adgang til nogle af selskabernes industrielle kontrolsystemer og flere selskaber måtte gå i ø-drift.

### Det største angreb

Så vidt vi ved, er der ikke tidligere blevet gennemført så stort et cyberangreb mod den danske, kritiske infrastruktur.

Angriberne opnåede på få dage adgang til 22 selskabers infrastruktur.

### Angrebsaktører med grundigt forarbejde

Der var tale om angribere, som på forhånd vidste, hvem de skulle ramme. Ikke en eneste gang blev der "skudt ved siden af".

### Koordinerede, succesfulde angreb mod dansk kritiske infrastruktur

Danmark er konstant under angreb. Men det er ikke normalt, at vi ser så mange samtidige, succesfulde angreb mod den kritiske infrastruktur.

### Mulig involvering af statslige aktører

Der er tegn på, at en statslig aktør kan have været involveret i et eller flere angreb.

### SektorCERTs sensornettværk og et stærkt samarbejde

Uden SektorCERTs sensornettværk til at opdage angrebene, vores dygtige analytikere samt et tæt samarbejde med vores medlemmer, deres leverandører og myndigheder kunne angrebet have medført driftmæssige konsekvenser for danskernes infrastruktur.

### De 25 anbefalinger

På baggrund af angrebet har vi fremhævet de af vores 25 anbefalinger, som er relevante i forbindelse med de konkrete angrebsteknikker.

Vi anbefaler fortsat alle, som driver dansk, kritisk infrastruktur, at implementere alle SektorCERTs 25 anbefalinger.



## Om SektorCERT

SektorCERT er de kritiske sektorer cybersikkerhedscenter.

SektorCERT er en væsentlig del af sektorernes forsvar mod cybertrusler. Vi er med til at opdage og håndtere, når den kritiske infrastruktur 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 sektorerne, som er tilsluttet vores omfattende sensornetværk. Via sensornetværket monitorerer vi internettrafikken med henblik på at opdage cyberangreb mod dansk, kritisk infrastruktur.

SektorCERT er en nonprofit forening ejet og finansieret af danske selskaber indenfor kritisk infrastruktur. Vi samarbejder med Europas andre CERT'er, og er med i en række cybersikkerhedsorganisationer, som gør, at vi har stor viden om angreb mod kritisk infrastruktur.

## Klassificering

SektorCERT benytter sig af Traffic Light Protocol (TLP) version 2 ved deling af information for at ange, hvordan informationerne kan deles videre.

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 aktuelle dokument og i anden mundtlig og skriftlig omtale af indholdet.

Dette dokument er klassificeret som TLP:CLEAR.

Læs mere om Traffic Light Protocol hos FIRST:  
[www.first.org/tlp/](http://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 cybersikkerhedsydeler 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.



## Om rapporten

Rapporten beskriver det hidtil mest omfangsrige, cyberrelaterede angreb mod dansk kritisk infrastruktur vi kender til.

Formålet med rapporten er at sikre, at vi lærer af angrebene, således at vi samlet står stærkere rustet mod de næste angreb, der kommer.

### Beskrivelsen af angrebet er strukturelt opdelt i to

- **Analysen**  
I analysen har SektorCERT taget fakta om angrebet og sammenholdt med de oplysninger, vi har om trusselsaktører, geopolitik, viden om angrebsmetoder og teknikker samt vores kendskab til tidligere angreb. Denne del af rapporten er subjektiv.
- **Tidslinjen**  
I tidslinjen gennemgås alene fakta. Hvad skete der helt præcist og hvornår skete det. Dette afsnit er objektivt.

Analysen kan læses uafhængigt af tidslinjen, hvis man ikke har behov for alle tekniske deltager.

#### Fakta vs. analyse

Det er vigtigt at bemærke forskellen mellem fakta og analyse.

Tidslinjen for angrebene gennemgår minut for minut selve angrebet mod den danske, kritiske infrastruktur.

Her beskrives alene fakta: de ting, vi har kendskab til, der skete ud fra direkte observationer. Det er ting, vi ved.

Analysen er subjektiv og er vores vurdering. Den er udarbejdet ud fra de faktiske observationer, besøg hos de berørte medlemmer, samarbejde med myndighederne og gennemgang af store mængder information om trusselsaktører.

Ud fra samme fakta kan der udarbejdes forskellige analyser. Vores analyse er altså en beskrivelse af det, vi tror og mener.

I afsnittet efter analysen drager SektorCERT en række konklusioner på baggrund af analysen, ligesom vi beskriver de anbefalinger, vi har i forhold til at forhindre fremtidige angreb.

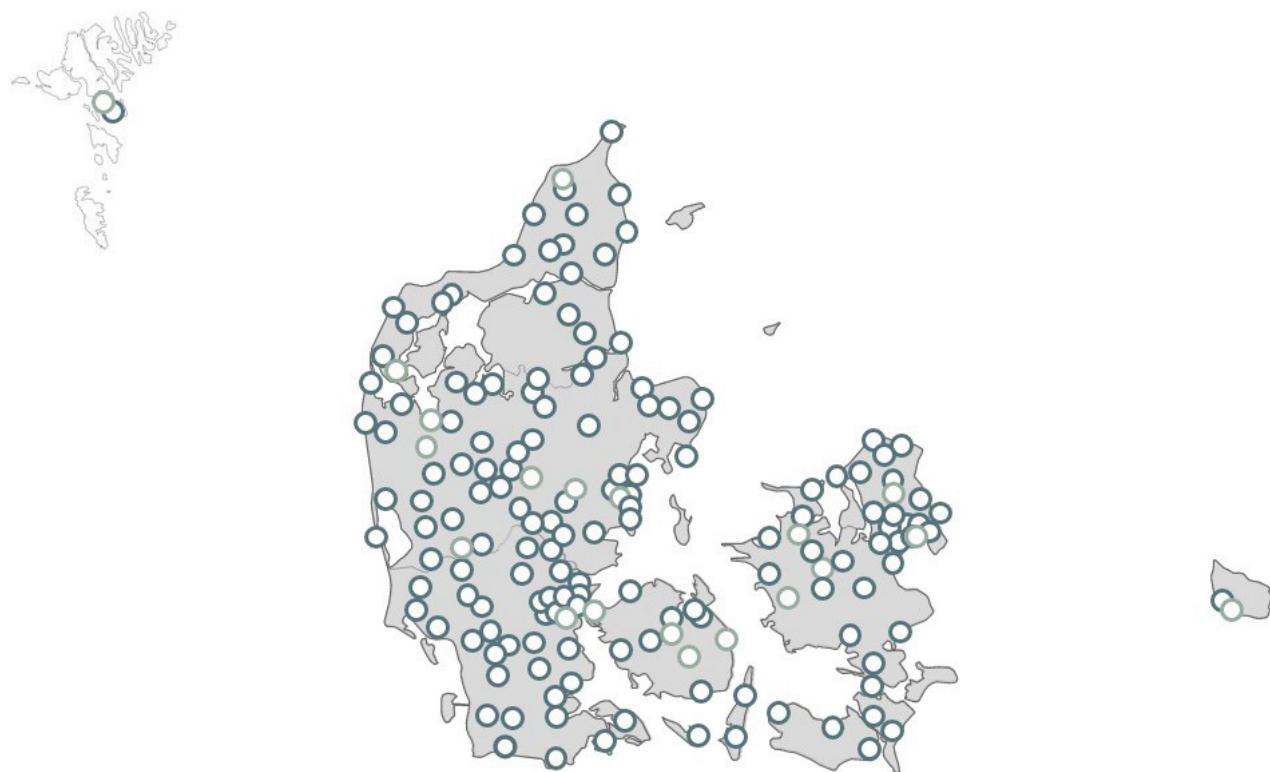


## SektorCERTs sensornetværk

SektorCERT driver et sensornetværk, som vi bruger til at skabe et billede af truslerne mod den danske, kritiske infrastruktur. Det bruges selvfølgelig også til at opdage angreb mod de virksomheder, der er en del af sensornetværket.

I relation til angrebene beskrevet i denne rapport, har sensornetværket været essentielt i forhold til at opdage mønstrene for angrebene på tværs af virksomhederne samt hurtigt at kunne reagere.

I de tilfælde, hvor det enkelte angreb kunne være gået ubemærket hen, har sensornetværket sikret, at vi ved at kigge på data på tværs af selskaber har kunne identificere angriberne og deres metoder.



## A N A L Y S E

Ud fra de faktiske observationer, besøg hos de berørte medlemmer, samarbejde med leverandører og myndighederne og gennemgang af store mængder information om trusselsaktører, har SektorCERT udarbejdet en analyse af angrebet.

Tidslinjen med de tekniske detaljer omkring angrebet er at finde fra side 21 og frem.



## Detaljeret analyse af sagen

I det følgende gennemgås sagen analytisk. Det vil sige, at SektorCERT tager fakta (se tidslinjen fra side 21) om angrebet og sammenholder med de oplysninger, vi har om trusselsaktører, geopolitik, viden om angrebsmetoder og teknikker samt vores kendskab til tidligere angreb. Denne del af rapporten er subjektiv og vi kan tage fejl i vores vurderinger.

### Før angrebet



#### 25/4

Den 25. april 2023 annoncerede Zyxel, som producerer firewalls som bruges hos mange af SektorCERTs medlemmer, at der var en kritisk sårbarhed i en række af deres produkter. Sårbarheden fik en score på 9.8 på en skala fra 1-10, hvilket betyder, at sårbarheden både var relativt nem at udnytte og at den kunne få store konsekvenser. Referencen for sårbarheden var CVE-2023-28771.

I dette konkrete tilfælde var der tale om en sårbarhed, som gjorde, at en angriber kunne sende netværkspakker til en Zyxel firewall og få komplet kontrol med firewallen uden at kende hverken brugernavne eller passwords til enheden.

Det der gjorde situationen ekstra alvorlig var, at det netop er den firewall, som skal beskytte det udstyr som står bagved den, som var sårbar.

Samtidig vidste vi, at mange af vores medlemmer benyttede disse firewalls til at beskytte de industrielle kontrollsystemer. Dermed var disse enheder ofte alt der stod mellem angriberne og kontrollen med dansk, kritisk infrastruktur.

Shadowserver, en non profit organization som overvåger trusler på internettet, udtalte: *"At this stage if you have a vulnerable device exposed, assume compromise."*

Vi var altså i en situation, hvor angrebsgrupperne havde en offentligt kendt sårbarhed de kunne bruge til at trænge ind i de industrielle kontrollsystemer. Og det primære forsvar mod at det skulle kunne ske var præcist det udstyr, som var sårbart.

Det var et såkaldt *worst case scenario* – det værste, tænkelige scenarie.

#### Zyxel

Zyxel er en stor producent af blandt andet firewalls som ofte benyttes i lidt mindre virksomheder eller i netværkssegmenter, hvor der er mindre trafik.

I Danmark har vi erfaring med, at Zyxel i høj grad benyttes til at beskytte den kritiske infrastruktur og vi ved, at mange OT-miljøer i mindre, danske selskaber indenfor kritisk infrastruktur, benytter Zyxel firewalls.





## 1/5

SektorCERT havde tidligere advaret medlemmerne om vigtigheden af at patche netop Zyxel firewalls, men udsendte den 1. maj ekstraordinært en advarsel om at få installeret den seneste opdatering. På dette tidspunkt var der ikke observeret angreb i Danmark, men fra vores samarbejdspartnere i andre lande stod det klart, at det kun var et spørgsmål om tid før angriberne ville rette deres søgelys mod Danmark.

## Første bølge

### 11/5

Det skete den 11. maj. I et koordineret angreb mod 16 nøje udvalgte mål blandt danske energiselskaber, forsøgte en angrebsgruppe at udnytte sårbarheden CVE-2023-28771.

Angriberne vidste på forhånd, hvem de ville ramme. Ikke en eneste gang blev der skudt forbi målet. Alle angreb ramte præcist der, hvor sårbarhederne var. Vores vurdering var, at det var en angriber, som ikke ønskede at skabe for meget støj, men ønskede at 'flyve under radaren' og undgå at blive opdaget, hvis nogen sad og kiggede med i trafikken.

Selve sårbarheden blev udnyttet ved at sende en enkelt specielt konstrueret datapakke til port 500 over protokollen UDP mod en sårbar Zyxel-enhed. Pakken blev modtaget af Internet Key Exchange (IKE) packet decoderen på Zyxel-enheten. Netop i denne dekoder var den nævnte sårbarhed. Resultatet var, at angriberen kunne afvikle kommandoer med root-privilegier direkte på enheden uden autentificering. Et angreb, som kunne udføres ved at sende en enkelt pakke afsted mod enheden.

11 selskaber blev kompromitteret med det samme. Det vil sige, at angriberne opnåede kontrol over firewallen hos disse selskaber og havde dermed adgang til den kritiske infrastruktur som stod bagved.

De øvrige 5 endte ikke med at afvikle kommandoerne. Muligvis fordi de pakker der blev sendt, var forkert formateret med det resultat, at angrebene fejlede.

For de 11 der blev kompromitteret afviklede angriberne kode på firewallen som gjorde, at den afleverede deres konfiguration og nuværende brugernavne tilbage til angriberne. SektorCERT vurderede, at angriberne brugte denne kommando som rekognoscering for at se hvordan de pågældende firewalls var konfigureret for derefter at vælge, hvordan det videre angreb skulle foregå.

### Opdateringer (patches)

De fleste af de angreb, der beskrives her i rapporten, var mulige fordi de enheder der blev angrebet, ikke havde fået installeret de nyeste opdateringer.

For mange af vores medlemmer var dette en overraskelse. Mange troede, at fordi firewallen var relativt ny, måtte den antages at have nyeste software, mens andre fejlagtigt antog, at deres leverandør stod for opdateringerne. Andre medlemmer havde bevidst fravalgt opdateringerne da det havde en omkostning fra leverandørens side at installere dem (selve softwaren er gratis).

Igen andre vidste ganske enkelt ikke, at de havde de pågældende enheder i deres netværk. Enten fordi en leverandør havde installeret dem uden at fortælle om det eller fordi man ikke havde et overblik over de enheder, der var forbundet til ens netværk. Dette kom angriberne til gode og gav dem ugevis at udføre angrebene i - selv efter SektorCERT via SektorForum havde alarmeret alle medlemmer og opfordret til at få installeret opdateringerne.



Tiden var afgørende. Det var nu en kamp mellem angribere og forsvarere: kunne SektorCERT sammen med vores medlemmer nå at handle hurtigt nok til at få stoppet angrebene, før angriberne kunne forvolde skade på den kritiske infrastruktur, vi i fællesskab beskytter.

Der blev i SektorCERT lynhurtigt dannet et incident team.

I løbet af de næste timer kørte en række parallelle spor:

- I et spor handlede det for analytikerne om at sikre, at alle de selskaber, som var under angreb, var blevet identificeret samt at nye angreb ville blive opdaget med det samme.
- I et andet spor var fokus at få kontakt til de medlemmer, som allerede var ramt og sikre, at vi sammen med medlemmerne fik håndteret situationen.
- I det tredje spor var leverandørerne i fokus. Vi ønskede i samarbejde med leverandørerne af disse firewalls at identificere eventuelle andre selskaber, som endnu ikke havde installeret opdateringerne og få sikret, at det skete før angriberne også fandt frem til dem.
- I det sidste spor blev myndighederne kontaktet og informationerne delt. Både nationale og internationale samarbejdspartnere blev involveret, og myndighederne blev briefet. Samtidig sendte vi igen et varsel ud til medlemmerne om øjeblikkeligt at installere opdateringerne da dansk, kritisk infrastruktur nu var under aktivt angreb.

Flere ting omkring angrebet var bemærkelsesværdige:

For det første vidste angriberne som nævnt præcist hvem de skulle angribe. På dette tidspunkt var information om, hvem der havde sårbare enheder ikke tilgængeligt på offentlige tjenester som Shodan. Derfor måtte angriberne på anden vis have skaffet sig informationer om, hvem der havde sårbare firewalls.

SektorCERT kan ikke i vores data identificere scanninger forud for angrebene, som kunne have givet angriberne den nødvendige information. Der er den dag i dag ikke en entydig forklaring på, hvordan angriberne havde den nødvendige information, men vi kan konstatere, at de blandt 300 medlemmer ikke ramte ved siden af én eneste gang.

Den anden bemærkelsesværdige ting var, at så mange selskaber blev angrebet samtidig. Den slags koordinering kræver planlægning og ressourcer.

Fordelen ved at angribe samtidigt er, at informationerne om ét angreb ikke kan nå at sprede sig til de øvrige mål før det er for sent. Man sætter dermed informationsdelingens styrke ud af spil fordi ingen kan nå at blive advaret på forhånd om det igangværende angreb da alle angribes samtidig. Det er usædvanligt – og særdeles effektivt.

### **Uautoriserede scanninger**

SektorCERT analyserer data fra sensornetværket og udarbejder en liste over observerede uautoriserede scanninger som medlemmerne kan anvende til at blokere for disse scanninger.

Formålet er at sikre, at man fremstår på så få af angribernes lister over mulige mål som muligt.





Det havde også en anden konsekvens: at SektorCERT skulle håndtere 16 samtidige sager. Der var tale om en opgave, som kærvede noget ekstraordinært fra incidentteamet.

Der var den 11. maj ingen tvivl om, at der måtte arbejdes i døgndrift for at sikre, at angriberne ikke fik adgang til den kritiske infrastruktur, som forsyner danskerne med el og varme.

#### 24x7

SektorCERT har i dag ikke bemanding til at reagere på angreb udenfor almindelige arbejdstid.

Derfor tog teamet en beslutning, som senere skulle vise sig afgørende: at fortsætte håndteringen af hændelserne udenfor arbejdstid selvom der egentlig ikke var bemanding i SektorCERT til at håndtere dette.

På grund af dette lykkedes det gennem eftermiddagen, aftenen og natten at få sikret hver eneste af de 11 kompromitterede energiselskaber via en meget stor indsats fra teamet samt fra velvillige leverandører og hurtigt reagerende medlemmer.

En kæmpe sejr for beskyttelsen af den kritiske infrastruktur. Og et stort nederlag for angriberne. Og samtidig en fuldstændig usynlig hændelse for danskerne, som fortsat havde el og varme i hjemmene. Ganske uvidende om de kampe der var blevet kæmpet i cyberspace for at beskytte den infrastruktur, vi alle afhænger af.

På trods af godt forarbejde, måtte angriberne se deres første angrebsbølge slå fejl. Godt nok lykkedes det at få fodfæste og opnå kontrol med energiselskabernes firewalls, men før de kunne nå at udnytte adgangen til at komme ind til den kritiske infrastruktur, var de blevet opdaget og stoppet.

De næste 10 dage var der stilhed fra angriberne.

## Anden bølge

### 22/5

Den 22. maj begyndte anden bølge. Med en angrebsgruppe, der muligvis var bevæbnet med nye, hidtil usete cybervåben.

Om den samme angrebsgruppe i denne periode gjorde sig klar til anden bølge eller andre grupper kom i spil, ved vi ikke.

Vi hælder mest til, at der var tale om to forskellige angrebsgrupper baseret på 'stilen' i angrebene. Men om grupperne arbejdede sammen, arbejdede for samme arbejdsgiver eller var helt uvidende om hinandens eksistens, ved vi endnu ikke.

### 22/5 kl. 14:44

Den 22. maj kl. 14:44 gik endnu en alarm hos SektorCERT. Vi kunne se, at et medlem var i gang med at hente ny software til deres firewall over en usikker forbindelse.

En sådan alarm er ikke i sig selv nødvendigvis bevis på, at medlemmet er under angreb. Men med de tidligere ugers erfaring frisk i hukommelsen, var det et klart tegn på, at noget var på færde.



Det var bemærkelsesværdigt, at alarmen først gik da medlemmets firewall var begyndt at hente ny software. Forud for dette måtte der have været et angreb, som gjorde angriberne i stand til at få firewallen til at hente denne nye software. Dette angreb havde vi endnu ikke indsigt i.

SektorCERT fulgte med i trafikken og observerede, at den pågældende firewall efterfølgende begyndte at opføre sig som om, den var en del af det kendte Mirai-botnet. Det var sådan set et positivt tegn da det kunne betyde, at angriberne alene ønskede at bruge adgangen til firewallen til at foretage DDoS-angreb med og ikke til at påvirke den kritiske infrastruktur, de samtidig (måske uvidende) havde fået adgang til.

Der var også Command & Control trafik. Men på grund af kryptering var det ikke muligt at se, hvilke kommandoer Command & Control-serveren sendte tilbage. Men konsekvensen kunne vi se. Det var, at medlemmet efterfølgende deltog i DDoS-angreb med to mål i USA og Hong Kong og altså dermed – uden at vide det - blev en del af et cyberangreb mod andre selskaber.

Efter anbefaling fra SektorCERT lukkede medlemmet lige før kl. 15 deres internetforbindelse helt og gik i ø-drift.

Dermed kunne der købes lidt tid for at få hjælp fra deres leverandør til at nulstille firewallen, installere opdateringer og sikre, at angriberne ikke havde brugt adgangen til andet end DDoS-angrebet.

Samtidig gik vi i SektorCERT i gang med at undersøge, om angriberne havde haft andre mål end dette ene, samt hvilken angrebsmetode der var blevet brugt.

På dette tidspunkt var der endnu ikke klarhed over, hvilken sårbarhed der var blevet udnyttet i forbindelse med disse angreb. Zyxel havde endnu ikke annonceret nogen nye sårbarheder og SektorCERTs analyse af angrebene gav anledning til at tro, der var tale om en anden type af angreb end de, der var observeret den 11. maj.

Få dage senere (den 24. maj) annoncerede Zyxel to nye sårbarheder: CVE-2023-33009 og CVE-2023-33010.

Disse var dog ukendte sårbarheder på tidspunktet for angrebet (den 22. maj) og det er SektorCERTs vurdering, at angriberne muligvis kendte til sårbarhederne før de blev annonceret af Zyxel og valgte at bruge denne viden om dem til blandt andet at angripe dansk, kritisk infrastruktur.

Den 22. maj kunne SektorCERT alene konstatere, at dansk, kritisk infrastruktur fortsat var under angreb og at Zyxel firewalls så ud til at være sårbare.

Der gik dog ikke lang tid før det næste angreb krævede teamets fokus.

### 22/5 kl. 18:13

Allerede klokken 18:13 startede det næste angreb med samme modus operandi som tidligere på dagen. Igen arbejdede teamet længe efter normal arbejdstid for at få hjulpet medlemmet af med angriberne og afbrudt internetforbindelsen for dermed at gå i ø-drift omkring kl. 20.



Det viste sig senere nødvendigt helt at udskifte firewallen for at få angriberne ud og den gamle kom dermed aldrig i drift igen.  
I ca. et døgn var der stilhed fra angriberne.

#### 23/5 kl. 18:43

Men den 23. maj kl. 18:43 kom det næste angreb hvor et nyt medlem blev kompromitteret. Her nåede angriberne at udnytte medlemmets infrastruktur til at deltage i et brute force angreb via SSH mod et selskab i Canada før SektorCERT sammen med medlemmet fik stoppet angrebet.

#### 24/5

Den 24. maj kom annonceringen fra Zyxel om, at de to nye sårbarheder var identificeret (CVE-2023-33009 og CVE-2023-33010). Det betød også, at denne viden nu var tilgængelig for alle verdens hackere, som dog stadig skulle udvikle selve angrebene – de såkaldte exploits.

#### 24/5 kl. 10:27

Da det næste medlem blev angrebet den 24. maj kl. 10:27 kunne vi se, at medlemmets Zyxel firewall hentede 4 forskellige payloads. Det er SektorCERTs vurdering, at angriberne forsøgte sig med forskellige payloads for at se, hvad der ville virke bedst hvilket er grunden til, at flere forskellige blev hentet. De brugte efterfølgende blandt andet adgangen til at foretage DDoS-angreb fra medlemmet mod forskellige mål før SektorCERT kunne nå at stoppe angrebet i samarbejde med medlemmet.

#### 24/5 kl. 10:31 - 10:58

Over en periode på 17 minutter blev yderligere 3 medlemmer kompromitteret og en payload ved navn MIPSkiller blev i alle tilfælde brugt ligesom alle tre medlemmers firewalls herefter blev brugt til at deltage i angreb mod andre mål. I et enkelt tilfælde i en sådan volumen, at firewallen bliver overbelastet og ikke længere kunne fungere, hvilket fik både angreb – og medlemmets netværk – til at holde op med at fungere.

I de næste fem timer var der et ophør i angrebene, hvilket gav SektorCERT luft til at få etableret nye regler for at sikre, at fremtidige angreb bedre kunne identificeres inden endnu et medlem blev kompromitteret om eftermiddagen.

#### 24/5 kl. 15:59

Kl. 15:59 kom næste angreb, Denne gang med brug af andre payloads end tidligere og medlemmet indgik herefter i det kendte Mirai Moobot netværk.

Det lidt specielle ved dette angreb var, at medlemmet ikke mente, de havde en Zyxel firewall. Men efter en grundig undersøgelse efter SektorCERTs opkald, viste det sig, at en leverandør havde brugt en Zyxel firewall i forbindelse med installationen af kameraer og at det var denne firewall, som nu var blevet angrebet.

Det var bemærkelsesværdigt for disse angreb i anden bølge, at angriberne muligvis har været i besiddelse af viden om sårbarheder som Zyxel endnu ikke havde offentliggjort. Det kunne tyde på en eller flere angribere i disse dage var i besiddelse af cybervåben, som få andre kendte til og som derfor var meget svære at opdage.

Ofte vil en angriber være meget forsiktig med, hvor disse våben bliver brugt. For når først våbenet bliver opdaget, kan der hurtigt udvikles forsvar mod dem.



## Det utænkelige



### 24/5 kl. 19:02

Den 24. maj kl. 19:02 gik en af de alarmer, som vi i SektorCERT aldrig havde forventet at se. Det er en alarm, som giver os besked, hvis vi ser trafik til eller fra en af de kendte APT-grupper.

En af de bedste og mest kendte APT-gruppe er Sandworm. En gruppe, som under den russiske GRU-enhed har udført nogle af de mest sofistikerede angreb mod industrielle kontrolsystemer, der nogensinde er set. Det var blandt andet Sandworm som stod bag det destruktive angreb mod Ukraine i 2015 og 2016 hvor hundredtusindvis af borgere stod uden strøm som konsekvens af cyberangrebet.

I SektorCERTs tre års virke har vi aldrig set tegn på, at disse APT-grupper har angrebet dansk, kritisk infrastruktur. Deres aktiviteter plejer at være reserveret til mål, som de stater de arbejder for, ønsker at forstyrre på grund af diverse politiske eller militære overvejelser.

#### APT

Angrebsgrupper, som med næsten uendelige ressourcer og ofte med en stat i ryggen, tager sig god tid, er forsigtige og er meget dygtige.

Disse grupper kaldes for APT-grupper – Advanced, Persistent Threat – eller avancerede, vedholdende trusler.

Når en alarm går, er det ikke nødvendigvis fordi noget er galt. Det er en såkaldt *indikator*. Et tegn på, at noget er værd at undersøge nærmere.

Heldigvis har vi hos SektorCERT et solidt datagrundlag til at gøre netop det – at undersøge, hvad der ligger til grund for alarmene. Ikke blot hos det enkelte selskab – men på tværs af en sektor eller endda flere sektorer.

Det arbejde er tidskrævende, men nødvendigt, for at skabe overblik over, hvad angriberne har foretaget sig forud for et angreb samt hvem målene har været og hvordan angrebet er udført. Samt – vigtigst af alt – om angrebet er lykkedes.

Normalt er der store mængder af data at arbejde med. Et angreb kræver forberedelse, rekognoscering, eksekvering, forfølgelse og meget mere (se Cyber Kill Chain på side 27).

Men ikke denne gang.

Gemt mellem milliarder af andre netværkspakker SektorCERT modtog fra sensornettværket den dag, sendte angriberne efter kompromitteringen kun en enkelt pakke tilbage.

'One ping only' som en af analytikerne observerede, med reference til filmen The Hunt for Red October.

Det var stærkt usædvanligt og var med al sandsynlighed en manøvre, som var designet til én ting: at undgå at blive opdaget.

Det svarer nogenlunde til at gemme et sukkerkorn i en sandsæk. Et sukkerkorn, som vi havde fundet og nu skulle finde ud af, hvorfor – og hvordan – var blevet gemt der.



Det som analytikkerne hos SektorCERT konkret havde observeret var, at der var trafik til 217.57.80[.]18 på port 10049 over protokollen TCP. Og at den trafik bestod af én netværkspakke på 1340 bytes og at der ikke blev leveret et svar tilbage. 'One ping only'. Denne IP-adresse havde vi troværdige informationer om tilhørte Sandworm-gruppen som havde brugt den aktivt ca. et år tidligere. Fra andre kilder blev det valideret, at IP-adressen fortsat var blevet brugt af gruppen blot få måneder tidligere. Det er derfor muligt, at der her var tale om kommunikation tilbage til Sandworm.

#### 25/5 kl. 01:22

Situationen gentog sig kl. 01:22 om natten mellem den 24. og 25. maj hvor et nyt medlem blev angrebet. Og også denne gang sendte angriberne en enkelt pakke til en anden formodet Sandworm-server: 70.62.153[.]174 på port 20600 over protokollen TCP.

Igen var der tale om en enkelt pakke på 1340 bytes. I modsætning til angrebet kl. 19:02 havde dette angreb dog store, synlige konsekvenser for medlemmet. Det var først noget, vi blev bekendt med klokken 11:45 da medlemmet rapporterede, at de havde mistet al visibilitet til tre fjernlokationer og at firewallen efterfølgende var helt ude af drift.

De begyndte at køre manuelt ud til alle fjernlokationer for at håndtere den manuelle drift. En situation, der blev håndteret både professionelt og med lidt god, jysk humor ("Det er jo godt vejr at køre i", som driftschefen udtalte).

Da denne firewall samtidig fungerede som intern router for OT-netværket betød det, at al intern trafik i produktionsnettet også holdt op med at fungere hos medlemmet.

#### 25/5 kl. 7:55 - 8:22

Inden morgenen var omme, kom endnu to angreb som ikke fulgte "opskriften" fra de to foregående. I disse nye angreb, som kom kl. 7:55 og 8:22, blev der brugt mange forskellige payloads som blev forsøgt hentet flere gange. Det gav os en indikation af, at der muligvis var tale om en anden angriber.

I angrebet blev der ikke kommunikeret tilbage til infrastruktur, som kunne relateres til Sandworm, hvilket igen taler for, at der var tale om en anden angriber eller en anden gruppering fra samme angriber.

Angrebene lignede hinanden, men det sidste angreb kl. 8:22 havde den kompleksitet, at medlemmet valgte ikke at patche sin firewall efterfølgende. Dette resulterede i gentagne kompromitteringer af medlemmet fra flere forskellige angribere i de efterfølgende dage.

#### 25/5 kl. 12:00

På baggrund af den mulige involvering af Sandworm og de konkrete konsekvenser for driften af dansk, kritisk infrastruktur, tog SektorCERT kl. 12 kontakt til både politiets nationale center for cyberkriminalitet (NC3) samt Center for Cybersikkerhed. Samtidig sendte SektorCERT analytikere ud til medlemmet for at indsamle så meget information som muligt.

Det blev aftalt med medlemmet, at alle forbindelser til internettet blev lukket ned, men at firewallen kørte videre for at sikre, at eventuel malware i hukommelsen ikke blev slettet når den blev slukket.

Grundet seriøsitet af angrebet, valgte medlemmet at bestille en ny firewall fra leverandøren og endte derfor som konsekvens af dette at køre i ø-drift i 6 dage.



SektorCERT arbejdede i de kommende dage tæt sammen med politiet om at indsamle malware-kode og skabe et overblik over angrebet. NC3's analytikere gik efterfølgende i gang med en dybdegående analyse af den malware, som SektorCERT havde indsamlet.

Samtidig blev information om de nye angreb delt på SektorForum hvor SektorCERT igen opfordrede til at patche firewalls.

### 30/5

Efter exploit-koden til nogle af sårbarhederne blev offentligt kendte omkring den 30/5 eksploderede angrebsforsøgene mod den danske, kritiske infrastruktur – specielt fra IP-adresser i Polen og Ukraine.

Hvor der før blev gået målrettet efter enkelte, udvalgte selskaber, blev der nu skudt med spredehagl mod alle - også firewalls som ikke var sårbare.

Det havde dog ingen konsekvenser for SektorCERTs medlemmer, som på dette tidspunkt havde fået lavet de nødvendige tiltag for at beskytte sig og derfor ikke længere var sårbar overfor disse angrebsforsøg.

### 31/5

Anbefalingerne blev gentaget på SektorCERTs månedskald med vores medlemmer den 31/5, hvor mere end 100 medlemmer deltog.

## Refleksion

Hvorvidt Sandworm var involveret i angrebet kan ikke siges med sikkerhed. Der er observeret enkelte indikatorer på dette, men vi har ikke mulighed for hverken at be- eller afkræfte det.

En situation, der som sådan ikke er usædvanlig. Cyberangreb er notorisk svære at attribuere til en bestemt angriber og ofte er det små, næsten ubetydelige fejl fra angriberens side, der kan indikere, hvem angriberen kan være.

Der er derfor ikke belæg for at anklage Rusland for at være involveret i angrebet. Det eneste vi kan konstatere er, at dansk, kritisk infrastruktur er i søgelyset og at der bruges cybervåben mod vores infrastruktur, som kræver nøje monitorering og avanceret analyse at opdage.

Og at det eneste, der i denne sag har reddet infrastrukturen har været, at SektorCERT i samarbejde med medlemmerne og leverandører formåede at reagere lynhurtigt så angriberne kunne stoppes før deres adgange kunne udnyttes til at skade den kritiske infrastruktur.

## KONKLUSION OG ANBEFALINGER

På baggrund af vores analyse af sagen, har SektorCERT udarbejdet en konklusion samt en række anbefalinger.

Konklusionen har til formål at fremhæve både det, som har fungeret godt, samt de områder, hvor der er plads til forbedring.

Anbefalingerne er lavet for at hjælpe til at forhindre fremtidige angreb i at have store konsekvenser for den danske, kritiske infrastruktur.



# Konklusion

SektorCERTs konklusion på angrebet er følgende:

## Systemiske sårbarheder

Danmark har et meget decentraliseret energisystem med mange, mindre operatører. Ofte vil et angreb mod én af disse operatører derfor ikke være kritisk for samfundet.

Vi har længe været bekymret for "systemiske sårbarheder". Altså en situation, hvor samme sårbarhed eksisterer hos rigtig mange selskaber og dermed skaber en potentiel kritisk situation for samfundet, hvis sårbarheden udnyttes på tværs af selskaber.

Det var præcist det, vi så ske her. Og det er noget, vi som samfund muligvis bør fokusere mere på da konsekvenserne kan være store.

## Visibilitet på tværs

Nogle angreb - som det vi beskriver her i rapporten - kan udføres så de er meget svære at opdage. I SektorCERT ser vi ikke på ét selskabs data, men på tværs af hundredevis af selskabers data. Dermed kan vi - som her - opdage, når nogen forsøger at angribe flere selskaber samtidig og vi kan dermed skabe en indsigt, som ikke er mulig når selskaberne monitoreres individuelt.

Denne monitorering på tværs af en sektor - og på tværs af sektorer - er med til at sikre, at vi også i fremtiden kan opdage og reagere på angreb med mange, samtidige mål.

## Konstante angreb

Dansk, kritisk infrastruktur er under konstant cyberangreb fra fremmede aktører. Derfor bør alle, som driver kritisk infrastruktur, være ekstra opmærksom og sikre, at de rette tiltag bliver gjort for at kunne hindre, opdage og håndtere disse angreb.

## Mulige konsekvenser

Havde SektorCERT ikke været der til at opdage angrebene og lynhurtigt få lukket for angribernes adgange, kunne konsekvensen af disse angreb have været langt mere alvorlig.

Havde angriberne fået lov til at opretholde deres adgange, kunne de have taget kontrol med driften af store dele af dansk, kritisk infrastruktur, hvilket kunne have haft store konsekvenser for samfundet.

## Samarbejde

Samarbejdet mellem SektorCERT og vores medlemmer og deres leverandører samt med politiets afdeling NC3 har fungeret glimrende og bidraget til, at angrebene har haft minimale konsekvenser for den kritiske infrastruktur.

## Statslig aktør

Der er indikationer på, at en statslig aktører kan have været involveret i angreb mod Danmark. Det er dog udenfor SektorCERTs ansvarsområde at overveje eventuelle geopolitiske konsekvenser af dette.

# Anbefalinger

Baseret på SektorCERTs ovenstående analyse af angrebsbølgerne mod 22 danske energiselskaber, har vi følgende anbefalinger til alle selskaber, som driver kritisk infrastruktur:

## **Generelt: Implementer SektorCERTs 25 anbefalinger**

SektorCERT har ud fra vores viden om både aktører og vores kendskab til cybersikkerhed indenfor kritisk infrastruktur lavet 25 generelle anbefalinger til tekniske og organisatoriske foranstaltninger som alle selskaber bør implementere.

Specifikt for angrebene nævnt i denne rapport bør der være fokus på nedenstående. Tallene henviser til SektorCERTs anbefaling fra "Håndbog om SektorCERTs Trusselsvurderinger".

### **2 Ekspesponering af services**

Da sårbarhederne omhandlede bestemte services (blandt andet VPN) er det vigtigt at sikre, at kun de services, der er brug for, er eksponerede mod internettet

### **10 Opdatering**

I forhold til første angrebsbølge havde Zyxel på forhånd advaret om sårbarhederne samt leveret patches. Det er derfor vigtigt at sikre, at de interne processer for at modtage informationer om sårbarheder samt sikre, at systemerne patches, er på plads

### **12 Beredskabsplan**

Når først skaden er sket og systemerne er blevet kompromitteret er det vigtigt at have en plan på plads for, hvordan det skal håndteres. I de konkrete tilfælde måtte flere medlemmer gå i ø-drift. En velbeskrevet og indøvet beredskabsplan kan sikre, at de rigtige beslutninger træffes hurtigt og effektivt og at skaderne dermed begrænses.

### **13 Logopsamling**

For at kunne opdage angreb, er det vigtigt at logs opsamles og analyseres. I nogle tilfælde er det dog ikke nok at se på egne logs. Visse angreb opdages bedst ved at se på tværs af en hel sektor. SektorCERT leverer ydelser til dette på både netværk og systemer.

### **15 Kortlægge netværksindgange**

Flere af de medlemmer vi talte med i forbindelse med disse angreb kendte ikke til de netværk, som blev angrebet. Det er derfor vigtigt at sikre, at alle netværksindgange til OT-systemerne er blevet kortlagt.

### **16 Segmentering**

Nogle gange er det ikke muligt at beskytte alle systemer - fx mod sårbarheder, man endnu ikke kender til. Derfor er det vigtigt at have opdelt netværket så man kan "gibe" angrebene bag de systemer, der eksponeres med internettet.

### **17 Identificer enheder**

Enkelte medlemmer kendte ikke til de enheder, som blev angrebet (ofte fordi en leverandør havde opsat enhederne). Dermed blev de heller ikke patchet. Det er vigtigt at identificere alle enheder på netværket da angriberne ellers finder veje ind, man ikke kend er til.



## 22 Leverandørstyring

Flere af de omtalte angreb kunne lade sig gøre, fordi der var uklarhed mellem medlemmerne og leverandørerne omkring aftaler om fx opdatering af firewalls.

Et tæt samarbejde - og gode aftaler - med leverandørerne er vigtig for at sikre en sikker infrastruktur.

## 24 Nødprocedurer

Et enkelt medlem var de i ø-drift i 6 dage. Det kræver gode nødprocedurer for de forretningskritiske processer at opretholde driften under sådanne forhold.

Samtidig kræver det gode, velintegrerede procedurer at håndtere overgangen til ø-drift.

## 25 Sårbarhedsscanninger

Når sårbarheder bliver offentligt kendt, kan de ofte identificeres via sårbarhedsscanninger. Nogle af de medlemmer som blev angrebet troede, at deres firewalls var blevet patchet selvom de ikke var. En sårbarhedsscanning ville have afsløret dette og kan derfor fungere som en ekstra validering af, om tingene er som de bør være samt om eventuelle aftaler med leverandører om opdateringer bliver overholdt.

## Følg med på SektorForum

Er du medlem af SektorCERT, så sorg for at følge med på SektorForum hver dag, så I løbende bliver bekendt med nye trusler og anbefalinger.

## T I D S L I N J E

Tidslinjen for angrebene gennemgår minut for minut selve angrebet mod den danske, kritiske infrastruktur.

Her beskrives alene fakta: de ting, vi ved, der skete ud fra direkte observationer. Tidslinjen indeholder derfor ingen analyser eller vurderinger af angrebet.



# Tidslinje for angrebene

I det følgende gives en kronologisk gennemgang af angrebene, hvor alene de faktiske angreb beskrives. Denne del af rapporten er objektiv.

Tidslinjen dækker fra 25/4-2023 til 2/6-2023.

Forud for dette opfordrede SektorCERT flere gange i 2022 medlemmerne til at sikre, at specielt Zyxel firewalls løbende blev patchet grundet tidligere sårbarheder i disse enheder og fordi SektorCERT er bekendt med, at disse typer enheder bruges bredt i sektorerne.

- 25/4**  
Zyxel annoncerede, at der var fundet en kritisk sårbarhed i en række af deres produkter.
  - 1/5**  
SektorCERT udsendte en ekstra advarsel om at få installeret den seneste opdatering.
  - 11/5 (de første 11 angreb)**  
16 selskaber blev forsøgt angrebet af en eller flere angribere som brugte CVE-2023-28771. Der blev brugt en specielt formatteret netværkspakke på port 500 mod firewallens VPN-service. 11 af selskaberne blev succesfuldt kompromitteret. De øvrige 5 endte ikke med at afvike kommandoerne.

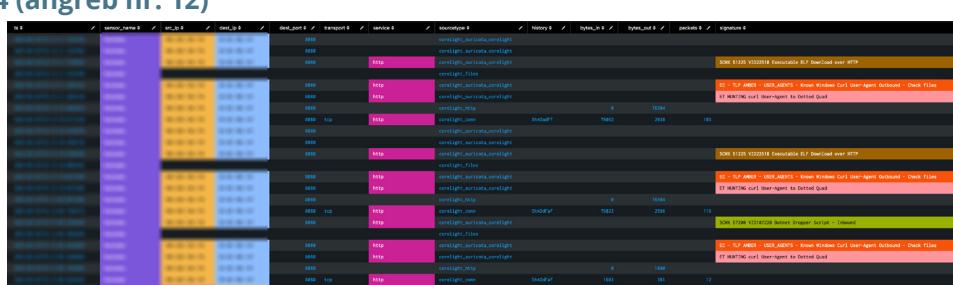
For de 11 der blev kompromitteret, kontaktede de pågældende firewalls IP-adressen 46.8.198.196 på port 8080/8081. Herfra modtog de følgende kommando:

```
zysh -p 100 -e 'show username';zysh -p 100 -e 'show running-configuration'
```

Denne kommando havde til formål at hente firewallens konfiguration og nuværende brugernavne. Information om angrebene blev delt på SektorForum.

22/5 kl. 14:44 (angreb nr. 12)

SektorCERT observerede, at et medlem var i gang med at hente ny software til deres firewall over en usikker forbindelse.



Håndteringen af alarmerne den 22/5

Vores data viste, at der blev hentet 2 forskellige filer:

URL = http://45.89.106[.]147:8080/mpsl  
MD5 = 5b0f10b36a240311305f7ef2bd19c810

URL = http://45.89.106[.]147:8080/mips  
MD5 = 9a7823686738571ahf19707613155012



Disse filer var ny software til Zyxel firewalls som ændrede på, hvordan medlemmets firewalls fungerede. Få minutter herefter kunne SektorCERT observere, at den pågældende firewall begyndte at opføre sig som om, den var en del af det kendte Mirai-botnet.

Det blev bekræftet da firewallen begyndte at kommunikere med en server ved navn "www.joshan[.]pro" som havde IP-adressen 185.44.81[.]147.

Denne adresse hører hjemme i Panama og var blevet oprettet kun 3 uger forinden. IP-adressen hører hjemme i Frankrig.

Kommunikationen foregik på port 56999 over protokollen TCP. En adresse og en port-kombination, der er kendt for at håndtere såkaldt "Command & Control"-trafik i relation til den variant af Mirai som kaldes MooBot.

SektorCERT kunne observere, at medlemmet straks herefter deltog i DDoS-angreb med to mål:

Det første mål i Hong Kong: 156.241.86[.]2

Det andet mål i USA: 63.79.171[.]112

#### 22/5 kl. 15

Efter anbefaling fra SektorCERT lukkede medlemmet deres internetforbindelse helt og gik i ø-drift.

#### 22/5 kl. 18:13 (angreb nr. 13)

Et andet medlem blev angrebet med samme modus operandi som tidligere på dagen. Dette medlem gik også i ø-drift.

#### 22/5 kl. 20:01

Information om angrebene blev delt på SektorForum.

#### 23/5 kl. 18:43 (angreb nr. 14)

Et nyt medlem blev angrebet. Angriberne udnyttede medlemmets infrastruktur til at deltage i et brute force angreb via SSH mod et selskab i Canada.

#### 24/5 kl. 9

SektorCERT fik sammen med medlemmet stoppet angrebet der startede kl. 18:43 dagen før.

#### 24/5 kl. 10

Zyxel annoncerede to nye sårbarheder (CVE-2023-33009 og CVE-2023-33010).

#### 24/5 kl. 10:27 (angreb nr. 15)

Det næste medlem blev angrebet. Denne gang kunne SektorCERT observere, at medlemmets Zyxel firewall hentede 4 forskellige payloads:

- http://145.239.54[.]169/mipskiller
- http://176.124.32[.]84/mipskiller
- http://185.180.223[.]48/mipskiller
- http://91.235.234[.]81/proxy2

**24/5 kl. 10:31 (angreb nr. 16)**

Endnu et medlem blev angrebet.

Denne gang blev følgende payload benyttet:

- [http://176.124.32\[.\]84/mipskiller](http://176.124.32[.]84/mipskiller)

Også denne gang brugte angriberne deres adgang til infrastrukturen til at lade medlemmet deltage i et DDoS-angreb.

**24/5 kl. 10:33 (angreb nr. 17)**

Et nyt medlem blev angrebet efter helt samme opskrift og med brug af samme payload. Og igen brugte angriberne deres adgang til at lade medlemmet deltage i DDoS-angreb.

**24/5 kl. 10:58 (angreb nr. 18)**

Endnu et angreb mod et medlem. Her hentede angriberne den samme payload tre gange i løbet af 30 minutter:

- [http://176.124.32\[.\]84/mipskiller](http://176.124.32[.]84/mipskiller)
- [http://145.239.54\[.\]169/mipskiller](http://145.239.54[.]169/mipskiller)
- [http://185.180.223\[.\]48/mipskiller](http://185.180.223[.]48/mipskiller)

Igen brugte angriberne deres adgang til at gøre medlemmet til en del af et DDoS-angreb mod andre selskaber.

**24/5 kl. 15:59 (angeb nr. 19)**

Endnu et medlem blev angrebet. Her blev en række nye payloads forsøgt brugt:

- [http://205.147.101\[.\]170:82/fuckjewishpeople.mips](http://205.147.101[.]170:82/fuckjewishpeople.mips)
- [http://45.89.106\[.\]147:8080/mips](http://45.89.106[.]147:8080/mips)
- [http://45.89.106\[.\]147:8080/mpsl](http://45.89.106[.]147:8080/mpsl)
- [http://45.128.232\[.\]143/bins/paraiso.mips](http://45.128.232[.]143/bins/paraiso.mips)
- [http://45.128.232\[.\]143/bins/libcurl1337.mips](http://45.128.232[.]143/bins/libcurl1337.mips)

Denne gang blev der kommunikeret med en Command and Control server på adressen 185.44.81[.]147 på port 56999 over protokollen TCP. En server vi kender, som en del af Mirai Moobot netværket.

**24/5 kl. 19:02**

SektorCERT observerede trafik til 217.57.80[.]18 på port 10049 over protokollen TCP.

Trafikken bestod af én netværkspakke på 1340 bytes og der blev ikke blev leveret et svar tilbage. Denne IP-adresse havde tidligere tilhørt Sandworm-gruppen.

**24/5 kl. 01:22 (angreb nr. 20)**

Et nyt medlem angrebet. Og også denne gang sendte angriberne en enkelt pakke til en anden formodet Sandworm-server:

70.62.153[.]174 på port 20600 over protokollen TCP.

Igen var der tale om en enkelt pakke på 1340 bytes.



### 25/5 kl. 7:55 (angreb nr. 21)

Endnu et medlem blev angrebet.

Her blev der brugt mange payloads, og mange af disse payloads blev forsøgt hentet flere gange. De forskellige payloads var:

- [http://145.239.54\[.\]169/mipskiller](http://145.239.54[.]169/mipskiller)
- [http://205.147.101\[.\]170:82/fuckjewishpeople.mips](http://205.147.101[.]170:82/fuckjewishpeople.mips)
- [http://45.128.232\[.\]143/bins/libcurl1337.mips](http://45.128.232[.]143/bins/libcurl1337.mips)
- [http://45.128.232\[.\]143/bins/paraiso.mips](http://45.128.232[.]143/bins/paraiso.mips)
- [http://45.89.106\[.\]147:8080/mips](http://45.89.106[.]147:8080/mips)
- [http://45.89.106\[.\]147:8080/mpsl](http://45.89.106[.]147:8080/mpsl)

Igen blev der etableret Command and Control kommunikation med 185.44.81[.]147 på port 56999 over protokollen TCP, og igen brugte angriberne medlemmets infrastruktur til at deltage i angreb mod andre.



### 25/5 kl. 8:22 (angreb nr. 22)

Endnu et angreb mod et medlem som blev kompromitteret og en enkelt payload blev brugt:  
[http://91.235.234\[.\]251/proxy1](http://91.235.234[.]251/proxy1)

Ellers lignede angrebet meget angrebet kl. 7:55 samme dag.



### 25/5 kl. 11:45

Medlemmet der blev ramt den 24/5 kl. 01:22 rapporterede, at de havde mistet al visibilitet til tre fjernlokationer og at firewallen efterfølgende var helt ude af drift.



### 25/5 kl. 12:00

På baggrund af den mulige involvering af Sandworm og de konkrete konsekvenser for driften af dansk, kritisk infrastruktur, tog SektorCERT kl. 12 kontakt til både politiets nationale center for cyberkriminalitet (NC3) samt Center for Cybersikkerhed.

Samtidig sendte SektorCERT analytikere ud til medlemmet for at indsamle så meget information som muligt.



### 25/5 kl. 16:01

Information om de nye angreb blev delt på SektorForum, hvor SektorCERT igen opfordrede til at patche firewalls.



### 26/5 kl. 10:07

SektorCERT informerede på SektorForum samt til myndigheder om angrebene og relaterede anbefalinger.



### 30/5

Cybersecurity and Infrastructure Security Agency (CISA) i USA valgte at placere disse sårbarheder fra Zyxel på listen over sårbarheder, som aktivt blev udnyttet af angribere. Det skete fordi man havde observeret, at angriberne nu havde udviklet såkaldt "exploit-kode" som gjorde det muligt at afvike angrebet og at flere angrebsgrupper var i gang med at angribe virksomheder, som stadig var sårbare.

Det at exploit-koden nu var offentligt tilgængelig betød, at enhver angriber nu kunne tage koden og bruge den direkte.



Resultatet var, at angrebsforsøgene mod den danske, kritiske infrastruktur eksploderede – specielt fra IP-adresser i Polen og Ukraine. SektorCERT så omkring 200.000 angrebsforsøg om dagen mod CVE-2023-28771 mod vores medlemmer.

Her blev skudt med spredhagl - også mod medlemmer, hvis firewalls ikke var sårbare.



**31/5 kl. 8:52**

SektorCERT informerede på SektorForum om angrebene.



**31/5 kl. 13:00**

SektorCERTs afholdte månedskald med vores medlemmer, hvor anbefalingerne blev gentaget.



**2/6**

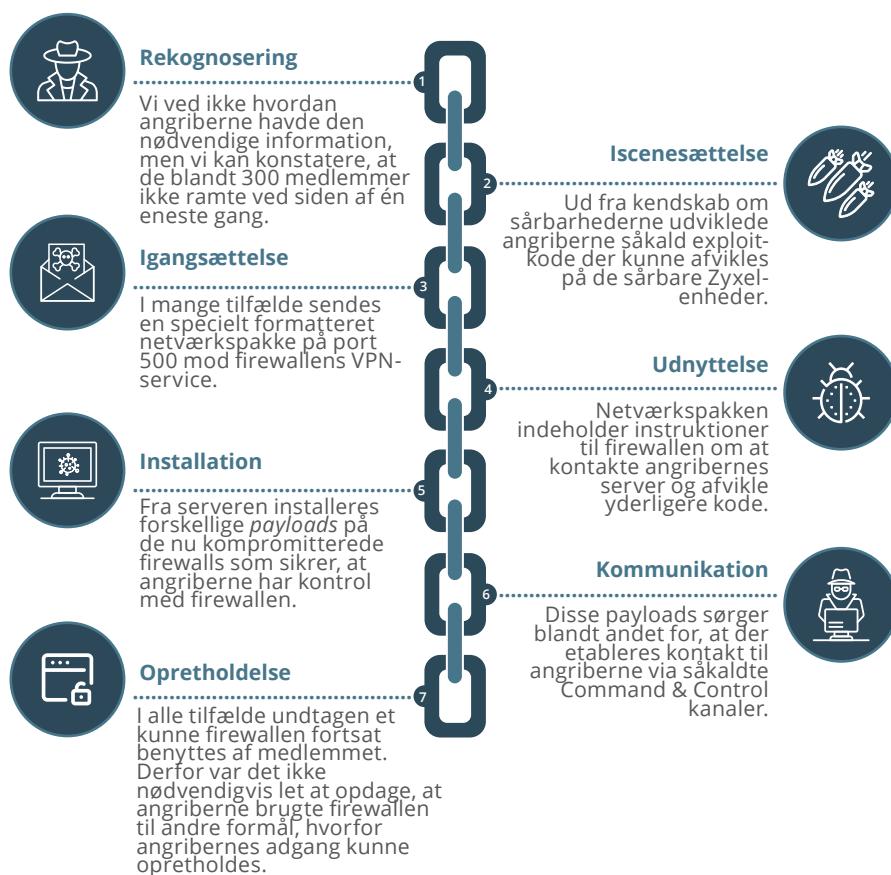
Zyxel udkom med et varsel, hvor de fortalte, at der var aktive angreb i gang mod selskaber med Zyxel firewalls og anbefalede også her, at installere de seneste patches.



## Cyber Kill Chain for det samlede angreb

Cyber Kill Chain er en international standard for beskrivelse af de nødvendige skridt for at kunne udføre et succesfuldt cyberangreb.

Cyber Kill Chain beskriver de syv faser, som et cyberangreb kan gennemgå. Nedenfor vises Cyber Kill Chain for det samlede angreb, som er beskrevet i denne rapport.



## A P P E N D I X

De observerede IOC'er, de omtalte CVE'er samt relevante links er samlet her.



## IOC'er

Følgende IOC'er er observeret (se også Tidslinjen):

### Filer

[http://45.89.106\[.\]147:8080/mpsl](http://45.89.106[.]147:8080/mpsl) (MD5 = 5b0f10b36a240311305f7ef2bd19c810)  
[http://45.89.106\[.\]147:8080/mips](http://45.89.106[.]147:8080/mips) (MD5 = 9a7823686738571abf19707613155012)  
[http://145.239.54\[.\]169/mipskiller](http://145.239.54[.]169/mipskiller)  
[http://176.124.32\[.\]84/mipskiller](http://176.124.32[.]84/mipskiller)  
[http://185.180.223\[.\]48/mipskiller](http://185.180.223[.]48/mipskiller)  
[http://91.235.234\[.\]81/proxy2](http://91.235.234[.]81/proxy2)  
[http://205.147.101\[.\]170:82/fuckjewishpeople.mips](http://205.147.101[.]170:82/fuckjewishpeople.mips)  
[http://45.128.232\[.\]143/bins/paraiso.mips](http://45.128.232[.]143/bins/paraiso.mips)  
[http://45.128.232\[.\]143/bins/libcurl1337.mips](http://45.128.232[.]143/bins/libcurl1337.mips)  
[http://91.235.234\[.\]251/proxy1](http://91.235.234[.]251/proxy1)

### Domains

[www.joshan\[.\]pro](http://www.joshan[.]pro)

### IP-adresser

45.89.106[.]147  
145.239.54[.]169  
176.124.32[.]84  
185.180.223[.]48  
91.235.234[.]81  
205.147.101[.]170  
45.128.232[.]143  
91.235.234[.]251  
46.8.198[.]196  
156.241.86[.]2  
185.44.81[.]147  
63.79.171[.]112  
217.57.80[.]18  
70.62.153[.]174



## CVE'er

Beskrivelse af CVE'erne som omtales i rapporten.

### CVE-2023-28771

Zyxel beskriver selv sårbarheden således:

*Improper error message handling in some firewall versions could allow an unauthenticated attacker to execute some OS commands remotely by sending crafted packets to an affected device*

Sårbarheden fik en score på 9.8 ud af 10

### CVE-2023-33009

Zyxel beskriver selv sårbarheden således:

*A buffer overflow vulnerability in the notification function in some firewall versions could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and even a remote code execution on an affected device*

Sårbarheden fik en score på 9.8 ud af 10

### CVE-2023-33010

Zyxel beskriver selv sårbarheden således:

*A buffer overflow vulnerability in the ID processing function in some firewall versions could allow an unauthenticated attacker to cause DoS conditions and even a remote code execution on an affected device.*

Sårbarheden fik en score på 9.8 ud af 10



## Links

---

Links til relevante artikler omkring Zyxel-sårbarhederne:

- <https://arstechnica.com/information-technology/2023/05/researchers-tell-owners-to-assume-compromise-of-unpatched-zyxel-firewalls/>
- <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls>
- <https://www.zyxel.com/global/en/support/security-advisories/zyxels-guidance-for-the-recent-attacks-on-the-zywall-devices>



## Kontakt os

**Kontakt SektorCERT  
på følgende nummer:**

+45 88327140

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

[info@SektorCERT.dk](mailto:info@SektorCERT.dk)

**PGP nøgle:**

C2EF 6314 7860 2B1E 2341 ACF4 DBC3 511D 3D06 BB3A

**Besøgs- og postadresser:**

Sommerfuglevej 2A 6000 Kolding	Bredgade 45 1260 København K
-----------------------------------	---------------------------------

**CVR nummer:**

41369841

**Satellittelefon:**

+88 1622456029