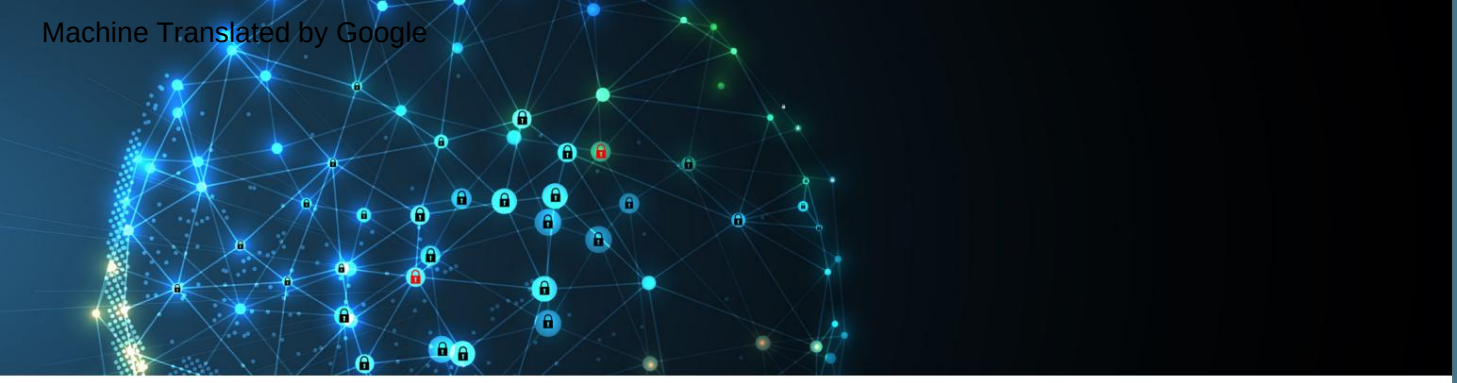
Table of Contents



Summary

In May 2023, the Danish critical infrastructure was exposed to the largest cyber-related attack we have experienced in Denmark to date.
22 companies that operate parts of the Danish energy infrastructure were compromised in a coordinated attack. The result was that the attackers gained access to some of the companies' industrial control systems and several companies had to go into island operation.

The biggest attack
As far as we know, such a large cyber attack against the Danish critical infrastructure has not previously been carried out.
The attackers gained access to the infrastructure of 22 companies in a few days.

Attackers with thorough preparation
These were attackers who knew in advance who they were going to hit. Not once was there a "shot from the side".

Coordinated, successful attacks against Danish critical infrastructure
Denmark is constantly under attack. But it is not normal that we see so many simultaneous, successful attacks against the critical infrastructure.

Possible involvement of state actors
There are indications that a state actor may have been involved in one or more attacks.

SektorCERT's sensor network and strong cooperation Without SektorCERT's sensor network to detect the attacks, our skilled analysts and close cooperation with our members, their suppliers and authorities, the attack could have had operational consequences for the Danes' infrastructure.

The 25 recommendations
Based on the attack, we have highlighted those of our 25 recommendations which are relevant in connection with the concrete attack techniques.
We continue to recommend everyone who operates Danish critical infrastructure to implement all SektorCERT's 25 recommendations.

About SectorCERT

SektorCERT is the cyber security center for the critical sectors.

SektorCERT is an essential part of the sectors' defense against cyber threats. We're in to detect and handle when the critical infrastructure is exposed to cyber attacks, and it is with us that the crucial knowledge that can prevent the next attack is built up and shared.

Among other things, we handle the monitoring of the companies in the sectors that are connected to our extensive sensor network. Via the sensor network, we monitor internet traffic with a view to detecting cyber attacks against Danish critical infrastructure.

SektorCERT is a non-profit association owned and financed by Danish companies within critical infrastructure. We cooperate with Europe's other CERTs, and are part of a number of cyber security organisations, which means that we have extensive knowledge of attacks against critical infrastructure.

Classification

SektorCERT uses the Traffic Light Protocol (TLP) version 2 when sharing information to indicate how the information can be shared further.

The TLP scale is divided into four levels as shown in the picture. The individual level indicates whether, and to what extent, the information may be shared further. The restrictions on sharing apply both when sharing the current document and in other oral and written mention of the content.

This document is classified as **TLP:CLEAR.**

Read more about the Traffic Light Protocol at FIRST: www.first.org/tlp/.

TLP:RED
The information is only intended for the recipient as a person.

TLP:AMBER
The information may be shared internally within the recipient's own organization as well as with companies or individuals who receive cyber security services from the recipient's organization. When **TLP:AMBER+STRICT** is used , this means that the information may only be shared internally within the recipient's organization.

TLP:GREEN
The information can be shared freely within the relevant community. A community can for example be "Danish energy companies".

TLP:CLEAR
The information can be shared without restriction.

About the report

The report describes the most extensive, cyber-related attack against Danish critical infrastructure that we know of so far.

The purpose of the report is to ensure that we learn from the attacks, so that we are collectively better equipped against the next attacks to come.

The description of the attack is structurally divided into two

- The analysis
  In the analysis, SektorCERT has taken the facts about the attack and compared them with the information we have about threat actors, geopolitics, knowledge of attack methods and techniques as well as our knowledge of previous attacks. This part of the report is subjective.

- The timeline
  In the timeline, only the facts are reviewed. What exactly happened and when did it happen. This section is objective.

The analysis can be read independently of the timeline if you do not need all the technical participants.

Facts vs. analysis It
is important to note the difference between facts and analysis.

The timeline for the attacks goes through minute by minute the actual attack against the Danish critical infrastructure.
Only the facts are described here: the things we are aware of that happened based on direct observations. These are things we know.

The analysis is subjective and is our assessment. It has been prepared on the basis of actual observations, visits to the affected members, cooperation with the authorities and review of large amounts of information on threat actors.

Based on the same facts, different analyzes can be prepared.
Our analysis is therefore a description of what we believe and mean.

In the section after the analysis, SektorCERT draws a number of conclusions based on the analysis, as well as describing the recommendations we have in relation to preventing future attacks.

SektorCERT's sensor network

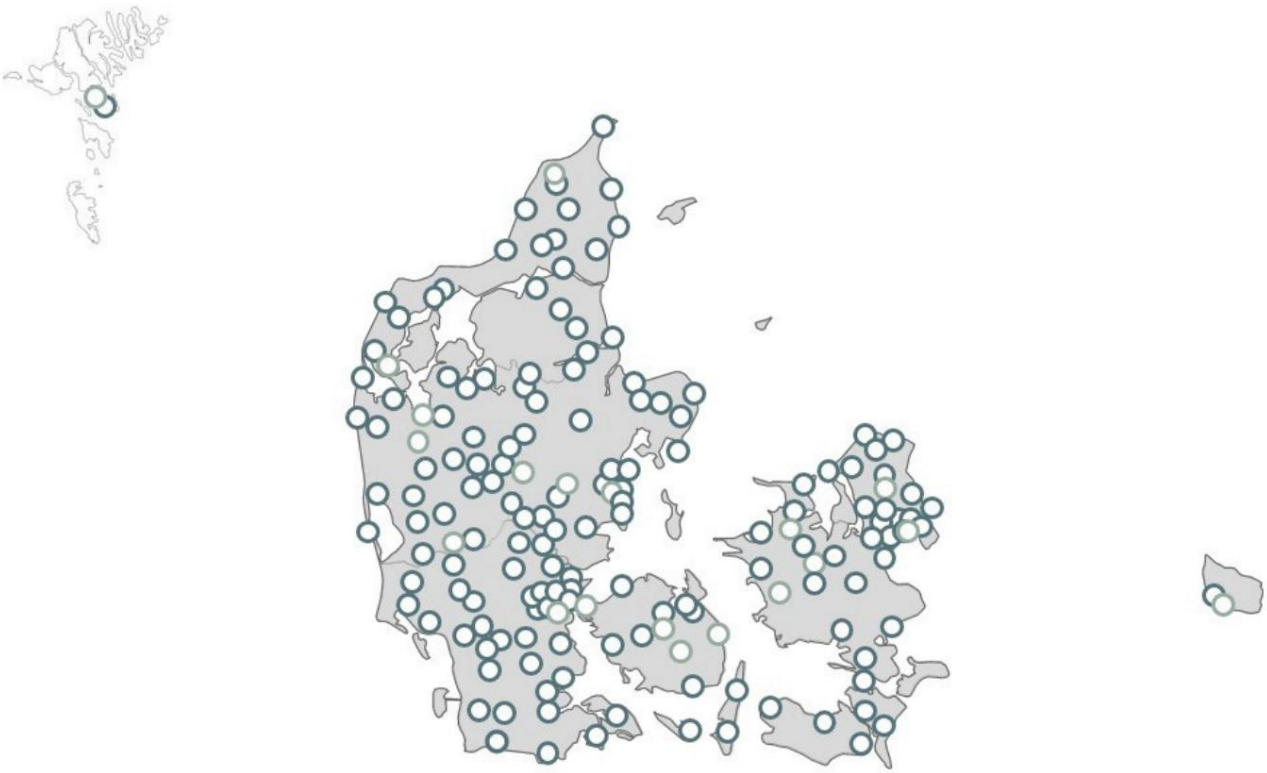
SektorCERT runs a sensor network that we use to create a picture of the threats to the Danish critical infrastructure. It is of course also used to detect attacks against the companies that are part of the sensor network.

In relation to the attacks described in this report, the sensor network has been essential in terms of discovering the patterns of the attacks across the companies and being able to respond quickly.

In cases where the individual attack could have gone unnoticed, the sensor network has ensured that by looking at data across companies we have been able to identify the attackers and their methods.

270
SENSORS

in total implemented in Danish critical infrastructure (May 2023)



ANALYSE

Based on the actual observations, visits to the affected members, cooperation with suppliers and the authorities and review of large amounts of information about threat actors, SektorCERT has prepared an analysis of the attack.

The timeline with the technical details surrounding the attack can be found from page 21 onwards.

Detailed analysis of the case

In the following, the case is reviewed analytically. This means that SektorCERT takes the facts (see the timeline from page 21) about the attack and compares it with the information we have about threat actors, geopolitics, knowledge of attack methods and techniques as well as our knowledge of previous attacks.
This part of the report is subjective and we may be wrong in our assessments.

Before the attack

25/4

On April 25, 2023, Zyxel, which produces firewalls used by many of SektorCERT's members, announced that there was a critical vulnerability in a number of their products.
The vulnerability received a score of 9.8 on a scale of 1-10, which means that the vulnerability was both relatively easy to exploit and that it could have major consequences. The reference for the vulnerability was CVE-2023-28771.

In this particular case, there was a vulnerability which allowed an attacker to send network packets to a Zyxel firewall and gain complete control of the firewall without knowing either usernames or passwords for the device.

What made the situation extra serious was that it is precisely the firewall that must protect the equipment behind it that was vulnerable.

At the same time, we knew that many of our members used these firewalls to protect the industrial control systems.
Thus, these units were often all that stood between the attackers and the control of Danish critical infrastructure.

Zyxel

Zyxel is a large manufacturer of, among other things, firewalls which are often used in slightly smaller companies or in network segments where there is less traffic.

In Denmark, we have experience that Zyxel is used to a large extent to protect the critical infrastructure and we know that many OT environments in smaller, Danish companies within critical infrastructure use Zyxel firewalls.

Shadowserver, a non profit organization that monitors threats on the Internet, stated: *"At this stage if you have a vulnerable device exposed, assume compromise."*

We were therefore in a situation where the attack groups had a publicly known vulnerability they could use to penetrate the industrial control systems. And the primary defense against that happening was precisely the equipment that was vulnerable.
It was a so-called *worst case scenario* – the worst imaginable scenario.

1/5

SektorCERT had previously warned the members about the importance of patching Zyxel firewalls in particular, but on May 1 issued an extraordinary warning to install the latest update. At this time, no attacks had been observed in Denmark, but it was clear from our partners in other countries that it was only a matter of time before the attackers would turn their spotlight on Denmark.

Updates (patches)

Most of the attacks described here in the report were possible because the devices that were attacked had not had the latest updates installed.

For many of our members this was a surprise. Many believed that because the firewall was relatively new, it must be assumed to have the latest software, while others mistakenly assumed that their vendor was responsible for the updates. Other members had deliberately opted out of the updates as there was a cost from the supplier to install them (the software itself is free).

Still others simply did not know they had the devices in question in their network. Either because a supplier had installed them without telling you about it or because you didn't have an overview of the devices that were connected to your network.

This benefited the attackers and gave them weeks to carry out the attacks - even after SektorCERT via SektorForum had alerted all members and encouraged them to install the updates.

First wave

11/5

It happened on May 11.
In a coordinated attack against 16 carefully selected targets among Danish energy companies, an attack group attempted to exploit the vulnerability CVE-2023-28771.

The attackers knew in advance who they wanted to hit. Not once was a shot missed the target. All attacks hit exactly where the vulnerabilities were.
Our assessment was that it was an attacker who didn't want to make too much noise, but wanted to 'fly under the radar' and avoid being detected if someone was watching in traffic.

The vulnerability itself was exploited by sending a single specially crafted data packet to port 500 over the protocol UDP towards a vulnerable Zyxel device.
The packet was received by the Internet Key Exchange (IKE) packet decoder on the Zyxel device. Precisely in this decoder was the said vulnerability. The result was that the attacker could execute commands with root privileges directly on the device without authentication.
An attack that could be performed by sending a single packet towards the device.

11 companies were compromised immediately. This means that the attackers gained control over the firewall of these companies and thus had access to the critical infrastructure behind it.

The other 5 did not end up completing the commands. Possibly because the packets sent were incorrectly formatted, resulting in the attacks failing.

For the 11 that were compromised, the attackers executed code on the firewall that caused it to hand their configuration and current usernames back to the attackers.
SektorCERT estimated that the attackers used this command as reconnaissance to see how the respective firewalls were configured and then choose how the further attack should proceed.

Time was of the essence. It was now a battle between attackers and defenders: could SektorCERT, together with our members, manage to act quickly enough to stop the attacks before the attackers could cause damage to the critical infrastructure we collectively protect.

An incident team was quickly formed in SektorCERT.
Over the next few hours, a series of parallel tracks ran:

- In one track, it was for the analysts to ensure that all the companies that were under attack had been identified and that new attacks would be detected immediately.
- In another track, the focus was to get in touch with the members who had already been affected and ensure that we managed the situation together with the members.
- In the third track, the suppliers were in focus. In cooperation with the suppliers of these firewalls, we wanted to identify any other companies that had not yet installed the updates and to ensure that this happened before the attackers also found them.
- In the last track, the authorities were contacted and the information shared. Both national and international partners were involved, and the authorities were briefed.
  At the same time, we again sent out a notice to the members to immediately install the updates as Danish critical infrastructure was now under active attack.

Several things about the attack were notable:
Firstly, as mentioned, the attackers knew exactly who to attack. At this time, information about who had vulnerable devices was not available on public services such as Shodan. Therefore, the attackers had to have obtained information about who had vulnerable firewalls in some other way.

SektorCERT cannot identify in our data scans prior to the attacks, which could have provided the attackers with the necessary information. To this day, there is no clear explanation of how the attackers had the necessary information, but we can state that among the 300 members, they did not miss a single shot.

The other remarkable thing was that so many companies were attacked at the same time. This kind of coordination requires planning and resources.
The advantage of attacking simultaneously is that the information about one attack cannot spread to the other targets before it is too late. This puts the power of information sharing out of play because no one can be warned in advance about the ongoing attack as everyone is attacked at the same time.
It is unusual – and extremely effective.

Unauthorized scans

SektorCERT analyzes data from the sensor network and compiles a list of observed unauthorized scans that members can use to block these scans.

The aim is to ensure that you appear on as few of the attackers' lists of possible targets as possible.

It also had another consequence: that SektorCERT had to handle 16 simultaneous cases. It was a task that demanded something extraordinary from the incident team.

On 11 May, there was no doubt that work had to be done around the clock to ensure that the attackers did not gain access to the critical infrastructure that supplies the Danes with electricity and heat.

24x7

SektorCERT currently does not have the staff to respond to attacks outside normal working hours.

Therefore, the team made a decision that would later prove decisive: to continue handling the incidents outside working hours, even though there was actually no staffing in SektorCERT to handle this.

Because of this, through the afternoon, evening and night, it was possible to secure each and every one of the 11 compromised energy companies via a very large effort from the team as well as from benevolent suppliers and quickly responding members.

A huge victory for the protection of the critical infrastructure. And a big defeat for the attackers. And at the same time a completely invisible incident for the Danes, who still had electricity and heat in their homes. Quite unaware of the battles that had been fought in cyberspace to protect the infrastructure we all depend on.

Despite good preparatory work, the attackers had to see their first attack wave fail. Fortunately, they managed to gain a foothold and gain control of the energy companies' firewalls, but before they could exploit access to the critical infrastructure, they were discovered and stopped.

For the next 10 days there was silence from the attackers.

Second wave

22/5

On May 22, the second wave began. With a strike group possibly armed with new, never-before-seen cyber weapons.

Whether the same attack group during this period was preparing for the second wave or other groups came into play, we do not know.
We are most inclined to believe that there were two different attack groups based on the 'style' of the attacks. But whether the groups worked together, worked for the same employer or were completely unaware of each other's existence, we do not yet know.

22/5 at 2:44 p.m

On 22 May at At 14:44, another alarm went off at SektorCERT. We could see that a member was downloading new software for their firewall over an insecure connection.
Such an alarm is not in itself necessarily proof that the member is under attack. But with the experience of the previous weeks fresh in the memory, it was a clear sign that something was up.

It was remarkable that the alarm only went off when the member's firewall had started downloading new software. Prior to this, there must have been an attack that enabled the attackers to get the firewall to download this new software. We did not yet have insight into this attack.

SektorCERT monitored the traffic and observed that the firewall in question subsequently began to behave as if it were part of the known Mirai botnet. It was a positive sign as it could mean that the attackers only wanted to use the access to the firewall to carry out DDoS attacks with and not to affect the critical infrastructure they had at the same time (perhaps unknowingly) gained access to.

There was also Command & Control traffic. However, due to encryption, it was not possible to see what commands the Command & Control server sent back. But we could see the consequence. It was that the member subsequently participated in DDoS attacks with two targets in the USA and Hong Kong and thus - without knowing it - became part of a cyber attack against other companies.

Following the recommendation of SektorCERT, the member closed just before 15 their internet connection completely and went into island mode.
This bought some time to get help from their vendor to reset the firewall, install updates and ensure that the attackers had not used the access for anything other than the DDoS attack.

At the same time, we in SektorCERT began to investigate whether the attackers had other goals than this one, as well as which attack method had been used.

At this time, it was not yet clear which vulnerability had been exploited in connection with these attacks. Zyxel had not yet announced any new vulnerabilities, and SektorCERT's analysis of the attacks led it to believe it was a different type of attack than those observed on May 11.

A few days later (on May 24), Zyxel announced two new vulnerabilities: CVE-2023-33009 and CVE-2023-33010.
However, these were unknown vulnerabilities at the time of the attack (May 22) and it is SektorCERT's assessment that the attackers possibly knew about the vulnerabilities before they were announced by Zyxel and chose to use this knowledge of them to attack Danish critical infrastructure, among other things .

On 22 May, SektorCERT could only ascertain that Danish critical infrastructure was still under attack and that Zyxel firewalls appeared to be vulnerable.

However, it wasn't long before the next attack demanded the team's focus.

22/5 at 18:13

As early as 18:13, the next attack started with the same modus operandi as earlier in the day. Again, the team worked long after normal working hours to help the member out with the attackers and cut off the internet connection to go into island operation around 20.

It later proved necessary to completely replace the firewall to get the attackers out, and the old one thus never came into operation again.
In approx. for a day there was silence from the attackers.

23/5 at 18:43

But on 23 May at At 18:43 came the next attack where a new member was compromised.
Here the attackers managed to exploit the member's infrastructure to participate in a brute force attack via SSH against a company in Canada before SektorCERT together with the member stopped the attack.

24/5

On May 24th came the announcement from Zyxel that the two new vulnerabilities had been identified (CVE-2023-33009 and CVE-2023-33010). It also meant that this knowledge was now available to all the world's hackers, who, however, still had to develop the attacks themselves - the so-called exploits.

24/5 at 10:27 a.m

When the next member was attacked on May 24 at At 10:27 we could see that the member's Zyxel firewall picked up 4 different payloads.
It is SektorCERT's assessment that the attackers tried different payloads to see what would work best, which is why several different ones were downloaded. They subsequently used, among other things, the access to carry out DDoS attacks from the member against various targets before SektorCERT could manage to stop the attack in cooperation with the member.

24/5 at 10:31 - 10:58

Over a period of 17 minutes, 3 more members were compromised and a payload named MIPSkiller was used in all cases, and all three members' firewalls were then used to participate in attacks against other targets.

In one case, in such volume that the firewall became overloaded and could no longer function, causing both attacks – and the member's network – to stop working.

For the next five hours, there was a lull in the attacks, giving SektorCERT time to establish new rules to ensure that future attacks could be better identified before another member was compromised in the afternoon.

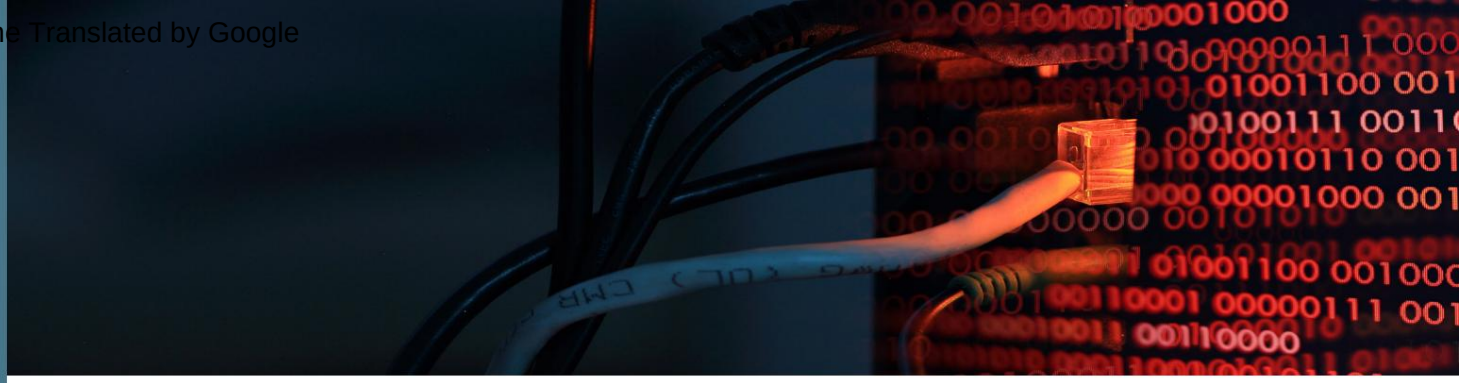
24/5 at 15:59

At 15:59 came the next attack, this time using different payloads than before and the member was then included in the well-known Mirai Moobot network.

What was a bit special about this attack was that the member didn't think they had a Zyxel firewall.
But after a thorough investigation after SektorCERT's call, it turned out that a supplier had used a Zyxel firewall in connection with the installation of cameras and that it was this firewall that had now been attacked.

It was notable for these second-wave attacks that the attackers may have had knowledge of vulnerabilities that Zyxel had not yet disclosed. It could indicate that one or more attackers these days were in possession of cyber weapons that few others knew about and which were therefore very difficult to detect.

Often an attacker will be very careful about where these weapons are used. Because once the weapon is discovered, defenses against them can quickly be developed.



The unthinkable

24/5 at 19:02

On 24 May at At 19:02 one of the alarms that we at SektorCERT never expected to see went off.
It is an alarm that notifies us if we see traffic to or from one of the known APT groups.

One of the best and most well-known APT group is Sandworm. A group which, under the Russian GRU unit, has carried out some of the most sophisticated attacks against industrial control systems ever seen. Among other things, Sandworm was behind the destructive attack against Ukraine in 2015 and 2016, where hundreds of thousands of citizens were left without power as a consequence of the cyber attack.

In SektorCERT's three years of operation, we have never seen signs that these APT groups have attacked Danish critical infrastructure. Their activities tend to be reserved for goals that the states they work for want to disrupt due to various political or military considerations.

APT

Attack groups, which with almost infinite resources and often with a state behind them, take their time, are careful and are very skilled.

These groups are called APT groups – Advanced, Persistent Threat – or advanced, persistent threats.

When an alarm goes off, it is not necessarily because something is wrong. It is a so-called *indicator.* A sign that something is worth investigating further.
Fortunately, at SektorCERT, we have a solid data base to do just that – to investigate what is at the basis of alarms. Not just at the individual company – but across a sector or even several sectors.

This work is time-consuming, but necessary, in order to create an overview of what the attackers have done prior to an attack, as well as who the targets have been and how the attack was carried out. As well as – most importantly – whether the attack has been successful.

Usually there are large amounts of data to work with. An attack requires preparation, reconnaissance, execution, pursuit and more (see Cyber Kill Chain on page 27).

But not this time.
Tucked away among the billions of other network packets SektorCERT received from the sensor network that day, the attackers sent only a single packet back after the compromise.
'One ping only' as one of the analysts observed, with reference to the film The Hunt for Red October.

It was highly unusual and was in all likelihood a maneuver designed for one thing: to avoid detection.

It is roughly equivalent to hiding a grain of sugar in a sandbag. A grain of sugar that we had found and now had to find out why – and how – had been hidden there.

What the analysts at SektorCERT had specifically observed was that there was traffic to 217.57.80[.]18 on port 10049 over the protocol TCP. And that that traffic consisted of one network packet of 1340 bytes and that no response was returned. 'One ping only'.
We had reliable information that this IP address belonged to the Sandworm group, which had been using it actively for approx. a year earlier. From other sources, it was validated that the IP address had continued to be used by the group just a few months earlier.
It is therefore possible that this was communication back to Sandworm.

25/5 at 01:22

The situation repeated itself at 01:22 in the night between May 24 and 25 when a new member was attacked. And this time, too, the attackers sent a single packet to another suspected Sandworm server: 70.62.153[.]174 on port 20600 over protocol TCP.

Again, it was a single packet of 1340 bytes. In contrast to the attack at However, at 19:02 this attack had major, visible consequences for the member. It was only something we became aware of at 11:45 when the member reported that they had lost all visibility to three remote locations and that the firewall was subsequently completely out of order.
They started manually driving out to all remote locations to handle the manual operation. A situation that was handled both professionally and with a bit of good, Jutland humor ("It's good weather to drive in", as the operations manager stated).
Since this firewall also functioned as an internal router for the OT network, this meant that all internal traffic in the production network also stopped working at the member.

25/5 at 7:55 - 8:22

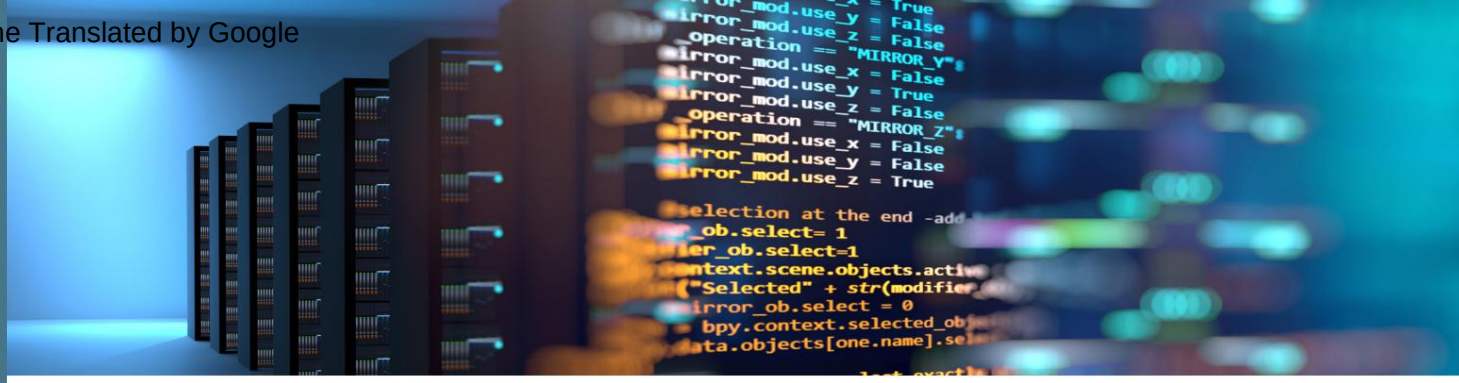
Before the morning was over, there were two more attacks which did not follow the "recipe" from the previous two. In these new attacks, which came at 7:55 and 8:22, many different payloads were used which were attempted to be retrieved several times. That gave us an indication that it might be another attacker.
In the attack, there was no communication back to infrastructure that could be related to Sandworm, which again suggests that it was a different attacker or a different grouping from the same attacker.

The attacks were similar, but the last attack at 8:22 had the complexity that the member chose not to patch his firewall afterwards. This resulted in repeated compromises of the member by several different attackers in the following days.

25/5 at 12:00

Based on the possible involvement of Sandworm and the concrete consequences for the operation of Danish critical infrastructure, SektorCERT took 12 contact both the police's National Center for Cybercrime (NC3) and the Center for Cyber Security. At the same time, SektorCERT sent out analysts to the member to collect as much information as possible.
It was agreed with the member that all connections to the Internet were shut down, but that the firewall continued to run to ensure that any malware in memory was not deleted when it was turned off.

Due to the seriousness of the attack, the member chose to order a new firewall from the supplier and therefore ended up running in island operation for 6 days as a consequence.



In the coming days, SektorCERT worked closely with the police to collect malware code and create an overview of the attack. NC3's analysts subsequently began an in-depth analysis of the malware collected by SektorCERT.

At the same time, information about the new attacks was shared on SektorForum where SektorCERT again called for patching firewalls.

30/5

After the exploit code for some of the vulnerabilities became publicly known around 30/5, attack attempts against the Danish critical infrastructure exploded - especially from IP addresses in Poland and Ukraine.
Where previously individual, selected companies were targeted, now everyone was shot with a scattergun - even firewalls which were not vulnerable.
However, it had no consequences for SektorCERT's members, who by this time had taken the necessary measures to protect themselves and were therefore no longer vulnerable to these attack attempts.

31/5

The recommendations were repeated at SektorCERT's monthly call with our members on 31/5, where more than 100 members participated.

Reflection

Whether Sandworm was involved in the attack cannot be said with certainty. Individual indicators of this have been observed, but we have no opportunity to either confirm or deny it.

A situation that as such is not unusual. Cyber attacks are notoriously difficult to attribute to a specific attacker and often it is small, almost insignificant mistakes on the part of the attacker that can indicate who the attacker may be.
There is therefore no evidence to accuse Russia of being involved in the attack. The only thing we can ascertain is that Danish critical infrastructure is in the spotlight and that cyber weapons are being used against our infrastructure, which require careful monitoring and advanced analysis to detect.
And that the only thing that saved the infrastructure in this case was that SektorCERT, in cooperation with the members and suppliers, managed to react quickly so that the attackers could be stopped before their access could be used to damage the critical infrastructure.

CONCLUSION AND RECOMMENDATIONS

Based on our analysis of the case, SektorCERT has drawn up a conclusion and a number of recommendations.

The purpose of the conclusion is to highlight both what has worked well, as well as the areas where there is room for improvement.

The recommendations are made to help prevent future attacks from having major consequences for the Danish critical infrastructure.

Conclusion

SektorCERT's conclusion on the attack is the following:

Systemic vulnerabilities

Denmark has a highly decentralized energy system with many, smaller operators. Often an attack against one of these operators will therefore not be critical for society.

We have long been concerned about "systemic vulnerabilities". In other words, a situation where the same vulnerability exists in many companies and thus creates a potentially critical situation for society if the vulnerability is exploited across companies.

That's exactly what we saw happening here. And it is something that we as a society should probably focus more on as the consequences can be great.

Across-the-board

visibility Some attacks - such as the one we describe here in the report - can be carried out in such a way that they are very difficult to detect. In SektorCERT, we do not look at one company's data, but across hundreds of companies' data. In this way, we can - as here - detect when someone tries to attack several companies at the same time and we can thus create an insight that is not possible when the companies are monitored individually.

This monitoring across a sector - and across sectors - helps to ensure that we can also detect and respond to attacks with many, simultaneous targets in the future.

Constant attacks

Danish, critical infrastructure is under constant cyber attack from foreign actors. Therefore, everyone who runs critical infrastructure should pay extra attention and ensure that the right measures are taken to be able to prevent, detect and deal with these attacks.

Possible consequences

Had SektorCERT not been there to detect the attacks and quickly shut down the attackers' access, the consequences of these attacks could have been far more serious.
Had the attackers been allowed to maintain their access, they could have taken control of the operation of large parts of Danish critical infrastructure, which could have had major consequences for society.

Cooperation

The cooperation between SektorCERT and our members and their suppliers as well as with the police department NC3 has worked excellently and contributed to the fact that the attacks have had minimal consequences for the critical infrastructure

State actor

There are indications that state actors may have been involved in attacks against Denmark. However, it is outside SektorCERT's area of responsibility to consider any geopolitical issues consequences of this.

Recommendations

Based on SektorCERT's above analysis of the waves of attacks against 22 Danish energy companies, we have the following recommendations for all companies that operate critical infrastructure:

General: Implement SektorCERT's 25 recommendations

Based on our knowledge of both actors and our knowledge of cyber security within critical infrastructure, SektorCERT has made 25 general recommendations for technical and organizational measures that all companies should implement.

Specifically for the attacks mentioned in this report, the focus should be on the following. The figures refer to SektorCERT's recommendation from the "Handbook on SektorCERT's Threat Assessments".

2 **Exposure of services**
Since the vulnerabilities concerned specific services (including VPN), it is important to ensure that only the services that are needed are exposed to the Internet

10 **Update**
In relation to the first attack wave, Zyxel had warned in advance about the vulnerabilities and delivered patches. It is therefore important to ensure that the internal processes for receiving information about vulnerabilities and ensuring that the systems are patched are in place

12 **Contingency plan**
Once the damage has occurred and the systems have been compromised, it is important to have a plan in place for how it will be handled. In the specific cases, several members had to go into island operation. A well-described and rehearsed contingency plan can ensure that the right decisions are made quickly and efficiently and that damage is thus limited.

13 **Logopsamling**
In order to detect attacks, it is important to collect and analyze logs. In some cases, however, it is not enough to look at your own logs. Certain attacks are best detected by looking across an entire sector. SektorCERT provides services for this on both networks and systems.

15 **Map network inputs**
Several of the members we spoke to in connection with these attacks did not know about the networks that were attacked. It is therefore important to ensure that all network inputs to the OT systems have been mapped.

16 **Segmentation**
Sometimes it is not possible to protect all systems - for example against vulnerabilities that are not yet known about. Therefore, it is important to have divided the network so that you can "seize" the attacks behind the systems that are exposed to the Internet.

17 **Identify devices**
Individual members were unaware of the devices that were attacked (often because a vendor had set up the devices). Thus they were not patched either. It is important to identify all devices on the network, otherwise the attackers will find ways in that you are not aware of.

22 **Supplier management**

Several of the mentioned attacks could be done because there was lack of clarity between the members and the suppliers regarding agreements on, for example, updating firewalls.
Close cooperation - and good agreements - with the suppliers is important to ensure a secure infrastructure.

24 **Emergency procedures**

A single member they were in island operation for 6 days. It requires good emergency procedures for the business-critical processes to maintain operations under such conditions.
At the same time, it requires good, well-integrated procedures to handle the transition to island operation.

25 **Vulnerability scans**

When vulnerabilities become publicly known, they can often be identified via vulnerability scans.
Some of the members who were attacked thought their firewalls had been patched when they were not.
A vulnerability scan would have revealed this and can therefore act as an additional validation of whether things are as they should be and whether any agreements with suppliers about updates are being respected.

Follow up on SektorForum If

you are a member of SektorCERT, make sure you follow up on SektorForum every day, so that you are constantly aware of new threats and recommendations.

TIMELINE

The timeline for the attacks goes through minute by minute the actual attack against the Danish critical infrastructure.

Only the facts are described here: the things we know happened based on direct observations. The timeline therefore contains no analyzes or assessments of the attack.

Timeline of the attacks

In what follows, a chronological review of the attacks is given, where only the actual attacks are described. This part of the report is objective.

The timeline covers from 25/4-2023 to 2/6-2023.
Prior to this, SektorCERT called on members several times in 2022 to ensure that Zyxel firewalls in particular were continuously patched due to previous vulnerabilities in these devices and because SektorCERT is aware that these types of devices are widely used in the sectors.

25/4

Zyxel announced that a critical vulnerability had been found in a number of their products.

1/5

SektorCERT issued an additional warning to install the latest update.

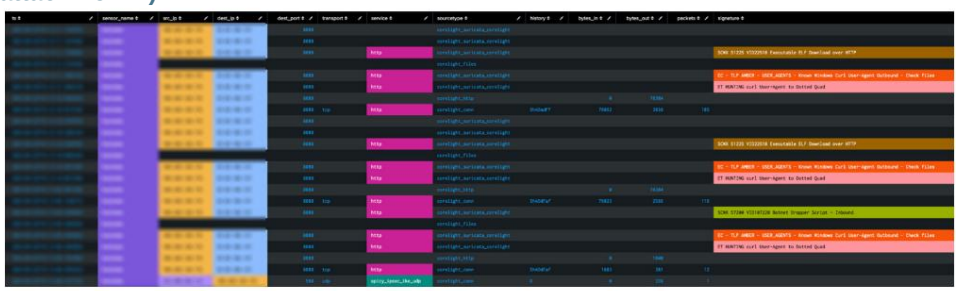
11/5 (the first 11 attacks)

16 companies were attempted to be attacked by one or more attackers using CVE-2023-28771.
A specially formatted network packet was used on port 500 against the firewall's VPN service.
11 of the companies were successfully compromised. The other 5 did not end up completing the commands.

For the 11 that were compromised, the firewalls in question contacted the IP address 46.8.198.196 on port 8080/8081. From here they received the following command: zysh -p 100 -e 'show username';zysh -p 100 -e 'show running-config'
This command was intended to retrieve the firewall's configuration and current usernames.
Information about the attacks was shared on SektorForum.

22/5 at 14:44 (attack no. 12)

SektorCERT observed that a member was downloading new software for their firewall over an insecure connection.



The handling of the alarms on 22/5

Our data showed that 2 different files were downloaded:

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

URL = http://45.89.106[.]147:8080/mips
MD5 = 9a7823686738571abf19707613155012

These files were new software for Zyxel firewalls that changed how the member's firewalls worked. A few minutes later, SektorCERT could observe that the firewall in question began to behave as if it were part of the known Mirai botnet.

This was confirmed when the firewall started communicating with a server named joshan[.]pro" www. which had the IP address 185.44.81[.]147.
This address belongs to Panama and had been created only 3 weeks before. The IP address belongs to France.

The communication took place on port 56999 over the protocol TCP. An address and a port combination known to handle so-called "Command & Control" traffic in relation to the variant of Mirai called MooBot.

SektorCERT could observe that immediately afterwards the member participated in DDoS attacks with two

targets: The first target in Hong Kong: 156.241.86[.]2
The second target in the USA: 63.79.171[.]112

22/5 at 15

Following the recommendation of SektorCERT, the member shut down their internet connection completely and went into island operation.

22/5 at 18:13 (attack no. 13)

Another member was attacked with the same modus operandi as earlier in the day. This member also went into island operation.

22/5 at 20:01

Information about the attacks was shared on SektorForum.

23/5 at 18:43 (attack no. 14)

A new member was attacked. The attackers exploited the member's infrastructure to engage in a brute force attack via SSH against a company in Canada.

24/5 at 9

SektorCERT, together with the member, stopped the attack that started at 18:43 the day before.

24/5 at 10

Zyxel announced two new vulnerabilities (CVE-2023-33009 and CVE-2023-33010).

24/5 at 10:27 (attack no. 15)

The next member was attacked. This time, SektorCERT could observe that the member's Zyxel firewall retrieved 4 different 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 at 10:31 (attack no. 16)
Another member was attacked.
This time the following payload was used:
• http://176.124.32[.]84/mipskiller

Again, the attackers used their access to the infrastructure to allow the member to participate in a DDoS attack.

24/5 at 10:33 (attack no. 17)
A new member was attacked using exactly the same recipe and using the same payload. And again, the attackers used their access to allow the member to participate in DDoS attacks.

24/5 at 10:58 (attack no. 18)
Another attack on a member. Here, the attackers downloaded the same payload three times in 30 minutes:

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

Again, the attackers used their access to make the member part of a DDoS attack against other companies.

24/5 at 15:59 (report no. 19)
Another member was attacked. A number of new payloads were tried here:

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

This time there was communication with a Command and Control server at the address 185.44.81[.]147 on port 56999 over the protocol TCP. A server we know, as part of the Mirai Moobot network.

24/5 at 19:02
SektorCERT observed traffic to 217.57.80[.]18 on port 10049 over protocol TCP.
The traffic consisted of one network packet of 1340 bytes and no response was returned. This IP address previously belonged to the Sandworm group.

24/5 at 01:22 (attack no. 20)
A new member attacked. And this time, too, the attackers sent a single packet to another suspected Sandworm server:
70.62.153[.]174 on port 20600 over protocol TCP.

Again, it was a single packet of 1340 bytes.

25/5 at 7:55 (Attack No. 21)

Another member was attacked.
Many payloads were used here, and many of these payloads were attempted to be retrieved several times.
The different payloads were:

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

Again, Command and Control communication was established with 185.44.81[.]147 on port 56999 over protocol TCP, and again the attackers used the member's infrastructure to engage in attacks against others.

25/5 at 8:22 (Attack No. 22)

Another attack against a member that was compromised and a single payload was used: http://91.235.234[.]251/proxy1

Otherwise, the attack was very similar to the attack at 7:55 the same day.

25/5 at 11:45 a.m

The member who was hit on 24/5 at 01:22 reported that they had lost all visibility to three remote locations and that the firewall was subsequently completely out of order.

25/5 at 12:00

Based on the possible involvement of Sandworm and the concrete consequences for the operation of Danish critical infrastructure, SektorCERT took 12 contact both the police's National Center for Cybercrime (NC3) and the Center for Cyber Security.
At the same time, SektorCERT sent out analysts to the member to collect as much information as possible.

25/5 at 4:01 p.m

Information about the new attacks was shared on SektorForum, where SektorCERT again called for patching firewalls.

26/5 at 10:07 a.m

SektorCERT informed on SektorForum as well as to authorities about the attacks and related recommendations.

30/5

The Cybersecurity and Infrastructure Security Agency (CISA) in the United States chose to place these vulnerabilities from Zyxel on the list of vulnerabilities that were actively exploited by attackers. This happened because it had been observed that the attackers had now developed so-called "exploit code" which made it possible to carry out the attack and that several attack groups were in the process of attacking companies which were still vulnerable.
The fact that the exploit code was now publicly available meant that any attacker could now take the code and use it directly.

The result was that the attack attempts against the Danish critical infrastructure exploded - especially from IP addresses in Poland and Ukraine. SektorCERT saw around 200,000 attack attempts per day against CVE-2023-28771 against our members.
Shots were fired here - also against members whose firewalls were not vulnerable.

31/5 at 8:52 am

SektorCERT informed on SektorForum about the attacks.

31/5 at 13:00

SektorCERTs held monthly calls with our members, where the recommendations were repeated.

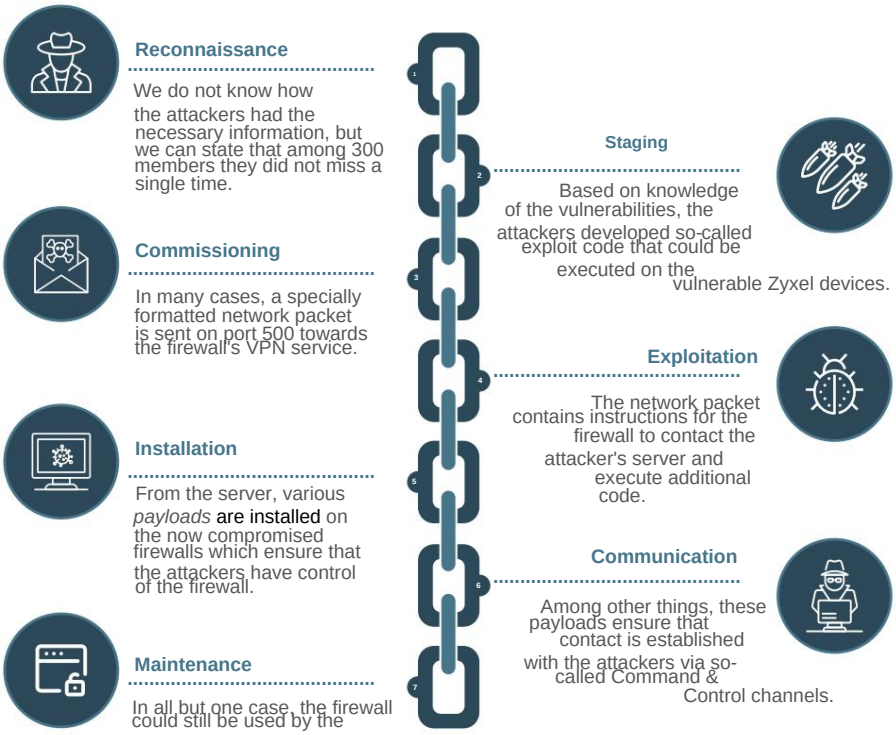
2/6

Zyxel came out with a warning, where they said that there were active attacks in progress against companies with Zyxel firewalls and recommended here, too, to install the latest patches.

Cyber Kill Chain for the overall attack

The Cyber Kill Chain is an international standard for describing the steps necessary to carry out a successful cyber attack.

The Cyber Kill Chain describes the seven stages that a cyber attack can go through.
Below is the Cyber Kill Chain for the overall attack described in this report.



APPENDIX

The observed IOCs, the mentioned CVEs and relevant links are collected here.

IOCs

The following IOCs have been observed (see also the Timeline):

Filer

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

Domains

www.joshan[.]pro

IP addresses

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

CVEs

Description of the CVEs mentioned in the report.

CVE-2023-28771

Zyxel itself describes the vulnerability as follows:
Improper error message handling in some firewall versions could allow an unauthenticated attack-er to execute some OS commands remotely by sending crafted packets to an affected device
The vulnerability received a score of 9.8 out of 10

CVE-2023-33009

Zyxel itself describes the vulnerability as follows:
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 execu-tion on an affected device
The vulnerability received a score of 9.8 out of 10

CVE-2023-33010

Zyxel itself describes the vulnerability as follows:
A buffer overflow vulnerability in the ID processing function in some firewall versions could allow an unau-thenticated attacker to cause DoS conditions and even a remote code execution on an affected device.
The vulnerability received a score of 9.8 out of 10

Links

Links to relevant articles about the Zyxel vulnerabilities:

- 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