kraftCERT infraCERT

Threat Assessment 2024

Contents

Summary of InfraCERT's threat assessment . . . **3**

1 Introduction . . . **4**

2 About this report . . . **6**
2.1 Description . . . 6
2.2 Traffic light protocol . . . 6

3 Overall threat assessments . . . **7**
3.1 National assessments . . . 7
3.2 InfraCERT's own assessments . . . 7
3.2.1 Cyber threats to organisations in Norway and Iceland . . . 7
3.2.2 State and state-sponsored actors . . . 7
3.2.3 Attacks and incidents in InfraCERT's member sectors . . . 8

4 Exploiting personnel . . . **9**
4.1 Exploiting insiders . . . 9
4.2 Exploiting variations in human behaviour . . . 9

5 Forms of attack . . . **11**
5.1 Ransomware . . . 11
5.2 Hacktivism . . . 11
5.3 Artificial intelligence and phishing . . . 11
5.4 Other forms of attack . . . 12

6 Actor development . . . **13**

7 Threats to control systems . . . **14**
7.1 Operational disruption . . . 14
7.2 Destructive attacks . . . 16

8 The threat picture is both local and common . . . **20**

Appendices . . . **23**

A About KraftCERT/InfraCERT . . . **23**

B Glossary . . . **24**

Summary of InfraCERT's threat assessment

It is likely that organisations in our sector are exposed to disruptive attacks. It is also highly unlikely that there will be successful destructive attacks in the short term. Even so, it's highly likely that states and mission driven actors continually try to develop the capability for such destructive attacks. Inadequate information control in organisations will make this job easier for them.

Going forwards, there will be attacks on suppliers. The question is what consequences this will have for the individual organisation. Extortion attacks will still be the most widely discussed form of attack, as well as having the biggest consequences, and LotL (Living off the Land) will remain a preferred technique. Hacktivists' potential for achieving serious consequences is low, even if denial-of-service attacks in InfraCERT sectors are likely to occur.

1 Introduction

Welcome to InfraCERT's Threat Assessment 2024. Before we present our analysis, we'd like to offer a few opinions.

The world is becoming more dangerous, but not as dangerous as it sometimes appears. There are many who have an interest in telling you that "Everything is dangerous". InfraCERT's ambition is for our threat assessment to be a sober analysis of the threat picture for our members, without commercial or political ties, and based on a large number of sources and observations.

The line of sources making some claim or other about the cyber threat picture is long, including statements about both observed and expected development. Many private companies issue threat reports, using a variety of methods, terms, categorizations, event selections etc to describe the threat picture. It is often unclear what data any given statement is based on, as well as how plausible and representative the data is. Sometimes there are contradicting statements in different sources, including government assessments. In sum, these factors present a significant challenge for the analysis process.

At times, InfraCERT disagrees with authorities' statements. The Norwegian National Security Authority (NSM) write in their report *Risiko 2024* [1] that a cyber operation against energy systems in Ukraine led to a power failure in large areas in February 2023. In InfraCERT's opinion, this is not the case. It's unfortunate when such statements are presented with no basis, as it challenges our shared situational understanding.

The insider threat is highly topical, but it's easy to get terms mixed up; accidental errors are not the same as espionage. By confusing these terms, organisations risk not being able to handle neither regular mishaps nor actual insider threats, because the tools needed to deal with each issue aren't the same.

Individual threat actors are rarely relevant as a basis for assessment. Both commercial and other threat picture assessors often describe individual actors, but this information is rarely valuable. The latest news about different actors has little value if we don't discuss how threat actors overall are developing future attack methods.

Finally, a request: Let us know if you suspect attacks, attempted attacks and other relevant incidents. Through sharing information with InfraCERT, members can contribute to developing and maintaining a shared sectoral threat picture.

Enjoy the read!

Figure 1: Realationship between assessments

2 About this report

2.1 Description

This document is a report from KraftCERT/InfraCERT, and is shared with select partners.

The report will give KraftCERT's members and sectors an assessment and understanding of relevant threats and their development, and describes what KraftCERT thinks about the threat picture now and in the future. We believe this provides a basis for making local assessments (see figure 1 on the preceding page).

Questions or comments can be sent to `cert@kraftcert.no`.

Change log:

Date	Version	Description
2023-06-17	1.0.0	Initial version

Cover picture: Ryssdalsnebba seen from Trolltinden. © 2024 Ketil Elgethun

2.2 Traffic light protocol

KraftCERT/InfraCERT uses the traffic light protocol (TLP version 2.0) when sharing information to indicate how the information may or may not be shared.

Read more about the traffic light protocol at FIRST[1] and NCSC[2].

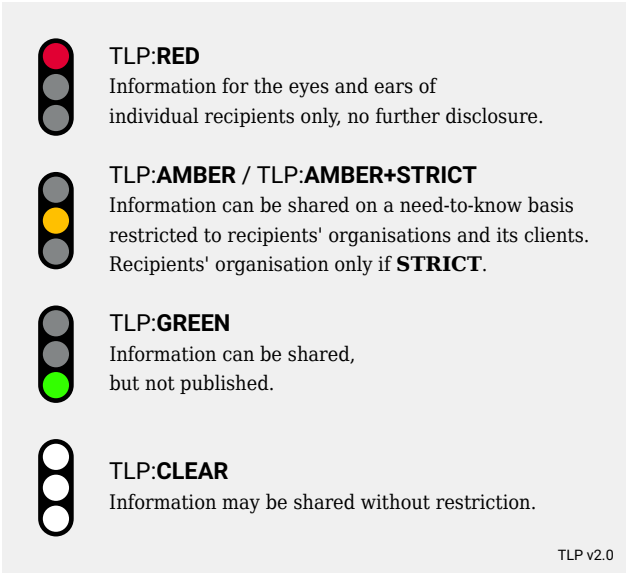

Figure 2: The traffic light protocol

[1] https://www.first.org/tlp
[2] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/kontakt-ncsc/retningslinjer-distribution-of-information/

3 Overall threat assessments

3.1 National assessments

Service [2] says denial-of-service attacks from pro-Russian actors are likely, and that Russian actors are seeking information about the energy sector. The Norwegian Police Security Service (PST) [3] mentions energy as one of several sectors targeted for cyber operations by foreign government actors. NSM [1] states that cyber security is challenged by "ever more advanced cyber operations", and that "Critical infrastructure must be shielded from insight and influence". The National Criminal Investigation Service (Kripos) [4] notes "an increase in all [cybercrime] fields, except for digital vandalism which remains stable", but point out that there's "greater risk associated with the amount of cyber directed crime". The police [5] reports that "technological development contributes to creating an expanded field of action for cybercriminal actors".

3.2 InfraCERT's own assessments

3.2.1 Cyber threats to organisations in Norway and Iceland

It is unlikely that Norwegian and Icelandic[3] organisations are high priority targets for threat actors and cyber-attacks as of today. Norway and Iceland aren't highlighted in analyses of which countries threat actors target. On the contrary, Norway and Iceland are far down on the list of countries experiencing cyber attacks (see e.g. [6], [7], [8]). USA's annual threat assessment [9] suggests that low-income countries are more attractive targets for cybercrime due to ongoing digitalization combined with inadequate security measures. The exception to this is denial-of-service attacks. Several Norwegian and Icelandic organisations experienced denial-of-service attacks in 2023, and InfraCERT believes such attacks will happen in the coming year as well.

Changes may happen that influence the threat picture for Norway and Iceland, such as changes in international politics (like the northern regions), the war in Ukraine or other conflicts. What changes might influence the cyber sphere in the short term are difficult to identify today.

3.2.2 State and state-sponsored actors

It is highly likely that China and China-sponsored actors have a considerable intent and ability to conduct industrial espionage, and to avoid detection. For InfraCERT's members, this primarily means industrial espionage against exposed areas like research and development. The China-affiliated actor Volt Typhoon has received a lot of attention in 2023 and 2024. This threat actor illustrates challenges regarding detection, and the fact that the actor operates with a long-time horizon. To InfraCERT's knowledge, the Volt Typhoon case has not had any consequences in Norway or Iceland (more about actors in chapter 6 on page 13).

Russia and Russia-sponsored threat actors are unlikely to carry out cyber attacks with destructive consequences. The actors pose a threat to critical infrastructure. Both PST and the Intelligence Service say that Russian threats to Norwegian gas- and petroleum export infrastructure persists, but to InfraCERT's understanding of these reports this is mainly in regard to physical attacks and sabotage. Many actors are occupied with the war in Ukraine, and focus their attention on systems that are important to, or aid efforts towards, Ukraine (more about destructive attacks in chapter 7 on page 14).

[3] KraftCERT has members in Norway and Iceland

3.2.3 Attacks and incidents in InfraCERT's member sectors

It is highly likely that the power and petroleum sectors will be indirectly affected by supply chain attacks in the short and intermediate term (1-3 years). The power and petroleum sectors are made up of many suppliers and long supply chains. Attacks on supply chains has been a topic for several years (ref. [10]). Supply chain attacks include both suppliers of equipment and suppliers of digital services and systems (i.e cloud services). Cyber incident overviews show that production companies often are vulnerable targets, topping the incident lists[4]. Many suppliers fall into this category. All kinds of suppliers can be hit by cyber-attacks. It's crucial for organisations to be familiar with and understand supply chains for both digital and non-digital deliveries, and knowing what suppliers are critical for their own operation.

It is unlikely that the power and petroleum sectors will be directly affected by large cyber incidents. NSM [1] points to the potential for cyber operations to "At worst lead to serious physical damage to critical infrastructure and personnel", and specifically mentions "guidance and control of power production, power distribution and production and delivery of oil and gas". Power and petroleum, or "energy", often appears in the lower ranges in overviews of sectors experiencing incidents, typically with 4-12% of total incidents. This can be seen in NSM's overview of incidents in Norway [1], ENISA's overview of incidents in Europe [17], and similar overviews from private companies[5]. Even if national authorities over time have pointed to the power and petroleum sectors as targets for cyber-attacks, this is not reflected in statistics or incident overviews.

InfraCERT members come from a range of critical infrastructure sectors. In USA, there's recently been a lot of focus on escalating cyberattacks on drinking water systems, for instance from the Environmental Protection Agency (see e.g. [18]). InfraCERT does not have sufficient information to speak to the number of incidents or development of attacks on water and sewage systems in Norway or Iceland.

[4] many companies present overviews of sectors and attackks, see e.g. Dragos - *OT Cybersecurity The 2023 Year in review* [11], Microsoft - *Digital Defence Report 2023* [7], Palo Alto - *Incident Response Report 2024* [12], Artic Wolf - *2024 Threat Report* [13], GRF - *Semi annual Ransomware Report H2 2023* [8], Waterfall - *2024 Threat Report* [14], Crowdstrike - *2024 Global Threat Report* [15], IBM Security - *Threat Intelligence Index 2024* [16]

[5] See footnode 4

4 Exploiting personnel

4.1 Exploiting insiders

Insiders refers to a person who exploits legitimate access to company assets for malicious purposes, on behalf of themselves or others.

In the short term, it's unlikely that the insider threat is increasing for our members. National authorities have for several years warned about the insider threat (or insider risk). Russia and China in particular are held up as states that attempt to recruit insiders in Norwegian organisations, including digitally. PST reports that foreign intelligence services' use of social media and chat applications is a developing trend. NSM's *Risiko 2024* [1] and *Nasjonalt digital risikobilde 2023* [19] state that the insider threat is increasingly important, and that improved cyber security increases the significance of having people on the inside of Norwegian organisations.

In InfraCERT's opinion, the basis for claiming an increased insider threat is weak. ENISA's threat report does not include insiders as a threat, due to an "exceptionally small number of publicly reported incidents" [17]. Similarly, there are few known insider incidents and criminal cases in Norway. The insider threat and what factors that drive insiders is also very complex, and an area where knowledge and information is scarce (see e.g. [20]).

The actual ability of foreign powers to recruit and exploit insiders might be lower than before, due to high levels of attention and vigilance. InfraCERT has received several questions regarding the insider threat, and observes that member vigilance is high where the insider threat is most relevant. At the same time this is a difficult topic to gain insight to, and clear answers and advice from authorities are rare. Often different considerations must be weighed against each other, for instance in hiring processes. Organisations have to assess the risks and navigate their need for competence as well as various legal requirements.

It is highly likely that foreign powers' desire to exploit insiders will increase when political conflict and economical competition intensifies. A threat assessment is a snapshot, and changes could influence the insider threat situation for InfraCERT members. An organisation in defence technology or an organisation that delivers equipment to Ukraine has a different threat picture from most InfraCERT members. At the time being it's difficult to see ongoing or potential conflicts or increased economical competition that would significantly affect the desire of foreign powers to exploit InfraCERT member insiders.

Insiders can provide threat actors with opportunities, but so can variations in human behaviour.

4.2 Exploiting variations in human behaviour

It's likely that threat actors increasingly will seek to exploit variations in human behaviour, meaning variations in behaviour and performance, including making mistakes. In InfraCERT's *Threat assessment 2023* we wrote that cybersecurity deals with more than malicious acts. This year, PST says that several cyber actors "exploit the human aspect more" [3]. NSM writes that "unconscious insiders" are employees that open attachments with malware, mistakenly forward data or "carelessly neglect security requirements and updates" [19], and that these account for more than half of insider incidents against digital assets. In InfraCERT's opinion, NSM is conflating different phenomena.

Insiders carrying out intentional actions and variations in human behaviour (with unintended consequences) are two different phenomena. The insider threat could for instance be reduced through security clearance of personnel, but this is not a measure for reducing the likelihood of errors and mishaps. There's also gross negligent behaviour. Figure 3 on the following page on next page illustrates differences between the three:

Insider, variations in human behaviour, gross negligence and grey areas between them. What they all have in common is that they all can provide threat actors with opportunities for attack, and that threat actors continually develop ways to exploit people. Gray areas make this extra challenging. Having employees means variation and that mistakes can happen. Humans can't simply be patched like digital systems.

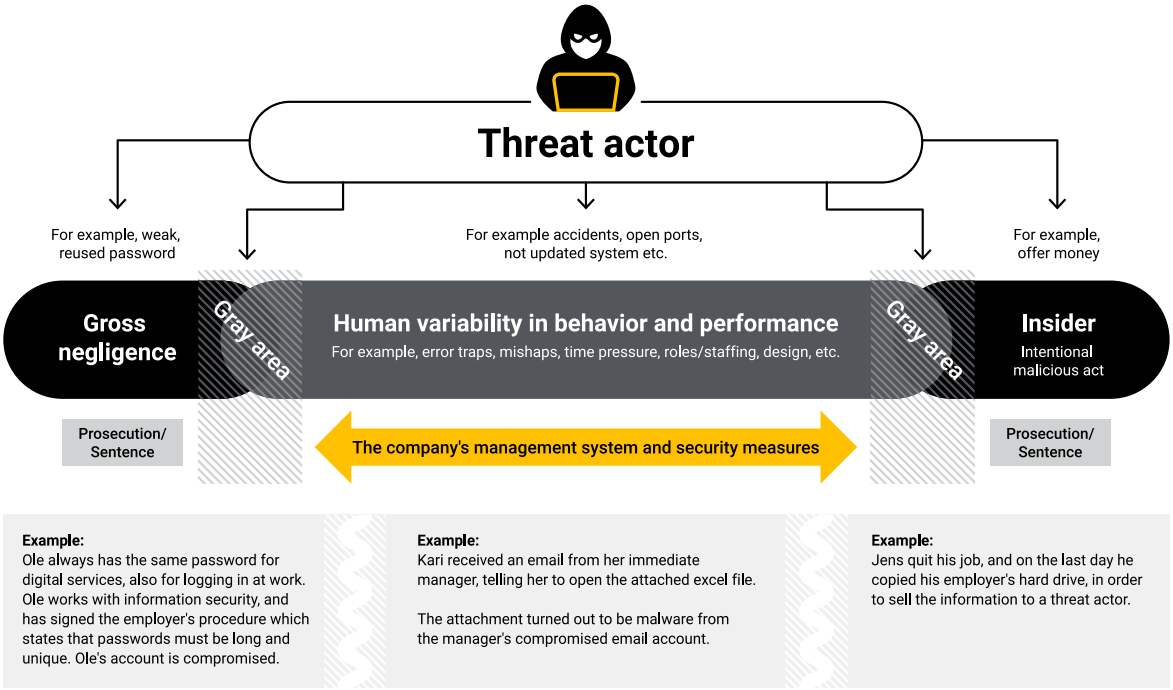

Figure 3: Threat actor's exploitation of insiders

5 Forms of attack

5.1 Ransomware

Ransomware attacks are the most globally widespread form of attack, and it's highly likely that they will increase in volume.

Ransomware attacks have been a top tier threat for several years, for instance in ENISA's annual assessments[17]. In *Cyberkriminalitet 2024* [4, p.12] , Kripos points to a slight decline in the number of reported ransomware cases in Norway. Although Norwegian statistics on cybercrime otherwise is lacking, it is InfraCERT's view that ransomware attacks are the most likely form of attack a business could be subject to, including in Norway.

Ransomware attacks without encryption – where the threat of publication of sensitive data is the basis for the extortion – is highly likely to increase, but not make up the majority of attacks. Palo Alto Unit42 writes about BianLian [21] , which exemplifies this form of extortion.

Even if these attacks more or less always are directed towards IT systems, they can in turn have an effect on production and delivery. For example, if logistics or ordering systems (which tend to be part of the IT system) are affected, production and delivery of goods and services can be difficult, or even impossible. InfraCERT considers this to be the main threat to control systems. Also see chapter 7 on page 14.

Most ransomware attacks are attacks of opportunity; the attacker discovers a way in and exploits this if it seems likely to be worth it.

It's likely that smaller businesses will be significantly more prone to successful encryption attacks than larger ones, as larger businesses have more resources to spend improving their defensive measures. This trend has been observed by Microsoft, among others [7, p.18].

5.2 Hacktivism

It is likely that InfraCERT members will be subject to hacktivism, but this unlikely to cause significant damage in most cases. Hacktivism often manifests in denial-of-service attacks and defacing of websites, which in most cases is inconvenient but not critical. An exception would be businesses where availability online is vital for operations.

It is unlikely that Norwegian and Icelandic businesses will be primary targets for hacktivist actions.

However, InfraCERT considers it likely that hacktivists will attempt to execute attacks on suppliers of services, technology and products, which could also have an impact on InfraCERT members. One example of this is the attacks on Unitronics guidance systems that were carried out in the fall ot 2023 – these attacks were widely reported on, but caused no serious damage.[6].

5.3 Artificial intelligence and phishing

Since *Threat assessment 2023*[10] , artificial intelligence has become a big topic, not least in the field of cyber security.

[6] See for example CISAs report on these attacks [22].

InfraCERT considers it highly likely that AI will make phishing more sophisticated, that phishing to a greater degree will be assisted by AI, and that it will be harder for the user to detect.

NCSC UK [23] believes reconnaissance and social engineering is likely to be influenced by AI the next two years, and that several kinds of actors will adopt the use of it. Especially "less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists" [24] will increase their capacity in phishing and similar activities. Microsoft/OpenAI have identified several threat actors' use of AI to improve spear-phishing, for example.

Social engineering and phishing will remain preferred methods of access for threat actors. They require relatively little effort, and AI assistance will increase their capacity. It's worth quoting NSM: "Anyone can be fooled in a moment of weakness, even the most vigilant". Surveys suggest that it's getting difficult to distinguish between AI generated and human made communication (i.e survey by IBM X-force [25]). Use of AI for phishing is identified as a trend by several security companies.

It is highly likely that the use of QR-codes in phishing is increasing. QR codes are increasingly used in many aspects of society, from ordering food to authentication, and often on mobile devices. There are few ways to verify QR codes, and it's impossible for humans to distinguish between harmful QR-codes from malicious actors and harmless QR codes from legitimate sources. Cofense [26] describes a campaign where QR codes were used against a bigger energy company. InfraCERT has seen phishing with QR codes utilized against Norwegian petroleum sector businesses in 2023.

It is likely that AI will be used in development and adaptation of malware, and that AI generally will increase threat actors' capacity. Google/Mandiant [27] says AI will scale the operations of both attackers and defenders of digital systems. Authorities pay close attention to AI, and all national assessments mention AI. Kripos [4] says AI has "potential for cybercrime in its speed, memory and almost unlimited stamina." On the other hand, they also point to AI as something that can provide the capacity for dynamic security measures and early detection of threats.

5.4 Other forms of attack

It is likely that Living off the Land (LotL) will be a preferred technique for advanced threat actors going forwards. It's harder to detect unwanted behaviour when it's executed through legitimate and already installed tools. The Chinese threat actor Volt Typhoon is an example of a group that uses this technique. CISA [28] has written extensively about them.

Abuse of suppliers' communication platforms (like file transfer, VPN and remote access) as a springboard for attacks, is likely to increase. This is described by Group-IB (among others) in their *Hi-Tech crime trends report 2023/2024* [29, p.13].

6 Actor development

Many analyses and reports put too much emphasis on individual actors. Reports about individual actors can provide fragments of understanding, and at best indicators to look for in one's own security systems. The value increases when this information is assessed and compiled with knowledge of attack techniques. InfraCERT analyses threat actors along several axes, like size, motivation, goals and consequences of attacks. We don't present a full picture of this ecosystem, but focus on what we consider to be our most important conclusions.

Larger threat actors are highly likely to continue using specialized sub- contractors like access brokers to achieve their goals. ENISA believes the Initial Access Broker (IAB) market is booming [17], and Palo Alto / Unit 42 says that stolen identities were one of the main reasons threat actors were successful in their attacks in 2023 [12]. Group-IB points to the fact that in 2023 there was a significant decline in average prices for purchasing access to businesses compared to in 2022, and believe that is because there are more sellers on the market [29]. The ecosystem is dynamic and is also influenced by other factors.

Government actions and sanctions against threat actors may lead to fragmentation of kill chains (methods) and thereby lower predictability in the ecosystem. Authorities have in 2023 carried out actions against several threat actors, including LockBit. [30]

Economically motivated threat actors are very likely to avoid attacks on targets they believe will provoke a strong government reaction. The Colonial Pipeline incident is one example of a cyber-attack that has led to governmental action. Norwegian police also supported the action against the threat actor Hive in early 2023 [4]. In other sectors, willingness to pay attracts economically motivated threat actors. One example of this is in the US, where there is a significant increase in health sector blackmail attacks.

It is highly likely that mission driven threat actors will try to camouflage their activities as that of others. In this way they will portray themselves as true to their words and hide activities they don't want to be known. This could occur in hacktivism, where so called faketivism[7] appears to be a phenomenon worth taking note of. This is described in CrowdStrike's *2024 Global Threat report* [15], among others.

It is highly likely that threat actors publish incorrect claims of leaked data to leak sites. The number of businesses getting their data published on leak sites is growing (see reports from Group-IB[29] and Crowdstrike[15], for example). InfraCERT has observed fake and exaggerated claims of leaked data: attempts at blackmail where no actual leak or publication has taken place. This means it's important to thoroughly investigate claims of leaked data before reacting to them.

[7] Faketivism: term used to describe actions done under the pretext of ideological motivation, but in reality done by governmental or other "professional" organizations.

7 Threats to control systems

Secondary damage from opportunistic attacks is the most likely threat for control systems, while disruption is the most likely consequence of an attack. The most serious in the long term threat is attacks by resourceful state actors aiming to weaken the public's defensive will. Such attacks could have both destructive and disruptive consequences.

7.1 Operational disruption

> A disruption or disruptive effect means a complete or partial temporary stop in delivery. This can be a power outage, a halt in production or supply, or faulty product. Reduced water quality in water works is one example of the latter.

It is likely that organisations in our sectors will see attacks with a disruptive effect. In disruptive attacks, threat actors are highly likely to exploit functional dependencies between the control system zones and the IT zones, or cloud and other external services. Such dependencies are becoming more numerous and important to operations and supply. External connections cause the attack surface to expand beyond the traditional control system zone. It must be possible to segregate the control system and operate it autonomously. Maintaining this integrity requires independence from other functions. A targeted attacker can exploit the fact that operational functions are spread beyond the control system zone, in order to carry out disruptive attacks.

External connections and functional dependencies

Due to a need for exchange of data, the number of connections between control systems and external systems are increasing, and company operations grow more dependent on these connections. Functions that were previously placed within the control system zone, or previously weren't neccessary for operations, are placed in zones with varying criticality or security levels.[a].

For example, the emergence of the Nordic power market has led to a demand for shorter delays in the regulation of production/consumption balance – faster than manual regulation is capable of. This forces new connections between what's traditionally been separate organizations and control systems. This is also done over the internet, which forces dependence on internet facing infrastructure, which presents a larger surface of attack. In total, this amounts to an operational dependency with high risk of being exploited by attackers wishing to disrupt power supply.

In effect, the connection between control and external systems means that the systems outside the control system zone have the same criticality, so that traditional island mode operation becomes an insufficient approach for maintaining normal operations in extraordinary situations. This presents a challenge for that are currently organizations required to carry out island mode drills and maintain knowledge of which functions would shut down and how long the system would be capable of production or service delivery.

[a] https://en.wikipedia.org/wiki/IEC_62443#Security_Level

In direct attacks on control system perimeters, threat actors are likely to exploit remote access and IT system integrations. Attackers will exploit vulnerable equipment or use stolen credentials against internet facing services when directly attacking control systems. Along with missing authentication of traffic inside the control system zone, these vulnerabilities can increase the likelihood of successful attacks.

This also applies to internal IT networks. Systems that exchange information with the control system are often more subject to compromise than the control system itself and can be used as a stepping stone if the connection isn't sufficiently secured, or there are vulnerabilities in the control system.

The use of remote access is increasing due to streamlining of operations and lack of personnel, and because ofmore comprehensive operations agreements where suppliers take a larger share of responsibility for the equipment. This means that the interest in stolen login credentials is increasing, and InfraCERT considers it likely that such remote access information for industrial control systems will be used in attacks.

Disruptive effects can also happen as a consequence of other types of attack. Lacking understanding of functional dependencies can cause an organisation to preventatively shut down a function others depend on, for example in the case of an opportunistic ransomware attack. An attack disrupting IT can cause the business to shut down functions in the OT-zone[8] as a precaution[14, s.9].

For control systems, secondary damage from ransomware attacks is the most likely threat. Control systems are rarely attacked by economically motivated criminals. Compromising control systems would normally require extra effort, since control systems as a rule are better protected than IT services. In addition, it might require a special set of skills that aren't normally needed for attacks on IT support systems[9].

[8] Operational technology (OT)
[9] Systems required for operations, but aren't located in the contrl system zone

Attacks aiming to take control of an ICS system require specialised knowledge about control systems. Combined, these elements make it more likely that opportunist attackers will choose easier targets within the organisation.

InfraCERT is aware of the existence of code that can install ransomware that encrypts controllers. In addition, operations planning systems, supervisory control and data acquisition[10], and internal support systems can all be exposed to generic ransomware. At the same time, Operations[11] often have better routines for restoring operations, which can influence their willingness to pay the ransom.

If an attacker, during an attack, finds the control system without understanding its function, this can lead to the attack having bigger consequences than intended. If the control system is insufficiently separated from the IT networks, an attacker could spread malware from the IT network without realising they're attacking the control system.

Any attack the target becomes aware of, is also likely to trigger actions and reactions that will have a negative effect on control systems. An incident could spread uncertainty causing the victim to shut down or separate networks, which could have consequences for functions depending on communication with other zones.

Ransomware attacks are the most likely form of attack that InfraCERT members might be directly exposed to. There's no difference between IT systems in businesses with or without control systems. They're equally dependent on office applications, Customer relationship management (CRM) systems, inventory systems and so on. Consequently, they're exposed to the same threats as everyone else. Trends show that ransomware attacks are the most common form of attack.

In InfraCERT's opinion, inadequate basic security measures in IT infrastructure creates opportunities for successful attacks that affect control systems. Opportunist attackers go for the most profitable targets. Like other criminals, they want the biggest possible payoff, not unlike legitimate businesses. If businesses have known vulnerabilities or opportunities for attack that don't require specialised knowledge, criminal actors will choose to target these rather than those with better defensive capabilities. Many criminals will also conduct broad but blind attacks, which are stopped by surveillance and defensive capabilities.

At the same time, new malware is continually in development, and these are utilised by several actors for attacks of opportunity. This means basic security measures are essential for businesses to protect themselves against new attacks.

7.2 Destructive attacks

It is highly unlikely that we'll see successful destructive attacks against InfraCERT sectors in the short term. This has not changed since *Threat assessment 2023*[10]. Attacks with the intention of harming people or facilities are very resource-intensive to carry out and require simultaneously attacking both control and safety systems. In attacks on Ukrainian energy companies, threat actors have achieved disruptive, but not destructive effects. Granted, Ukraine has had the opportunity to prepare for such attacks for several years (since before 2014) and has handled several control system attacks in the past decade.

It is highly likely that state and mission driven actors continuously work to develop destructive attacks. InfraCERT presupposes that several threat actors intend to build destructive attack capabilities, and it's likely that an organisations vulnerabilities provide opportunities for execution. This means that it comes down to planning, capacity, timing and not least information about the target.

Disruptive attacks are easier to pull off, since they only require an attack on a function needed for operation.

[10] Supervisory Control And Data Acquisition (SCADA)
[11] By this we mean the operations of the physical and OT processes, i.e. production

Mere suspicion that a system is compromised can be enough to shut it down, just in case. If an actor wants to signal that it's possible to paralyse the power, oil or gas supply, disruption is a possible objective.

Goals and objectives in attacks on control systems
This lists different types of attacks against ICS with an increasing level of difficulty.

Access
Access attacks are when threat actors intend to gain access to an organization's network, either for the purpose of sale through an IAB or to gain a foothold for future attacks.

Data theft
Attacks with the goal of extracting information about a company's products, deliveries, strategies, systems and networks, and/or control systems. This can also be done in preparation for a later attack.

Disruption
Attacks with the goal of disrupting a company's supply. This can be done directly through attacks on control systems, or indirectly by attacking support systems operations depend on. "Disruptive angrep".

Destruction
Attacks aiming to destroy equipment, cause external (environmental) destruction or take lives. They are difficult and resource intensive to carry out, because it's often necessary to access control systems while simultaneously shutting down functions in the safety system.

Control
Attacks with the goal of taking control of control system processes are the hardest. Even though one doesn't have to attack both control and safety systems, this sort of attack requires good domain and local knowledge of the system and its underlying infrastructure to succeed, and be able to control the process. Through full control of a control system, an attacker could be able to create situations that circumvent the safety system.

Disruptive attacks are far more likely to succeed than destructive ones, even in war. The war in Ukraine is a good example of this. The war has lasted more than ten years, and there's only been one known attack that actually had destructive effect: the attacks on the Viasat/KA-SAT modems[31] that put them out of commission. Other attacks have had disruptive effects, including the attacks in 2015 and 2016 that led to power failures in large areas in Ukrainian cities. The malware used in these direct control system attacks has varied over time, from malware with standard IT functionality to malware designed to attack using the control system protocols.

Malware in control systems is continually evolving, but control system malware utilised in attacks have become less complex over time, most likely due to the resource constraints of war[32].

It is likely that target focused, mission driven threat actors will continue to develop malware for the purpose of attacking control systems. In later years, more new malware has appeared (Industroyer2, PIPEDREAM/ INCONTROLLER). Two additional examples of malware with control system functionality were used in Ukraine in 2022 and 2023, where Russian state actors have used new malware on a MicroSCADA[33] system in their attack on the power system. CosmicEnergy[34] was observed being uploaded to an open

malware scanner and is designed to disrupt devices in the power grid using IEC-104[12]. This shows that threat actors are capable of developing malware even when time and resources are scarce.

InfraCERT also believe it's likely that state-sponsored, mission driven threat actors will buy or outsource the development of malware for control systems. For instance, Mandiant suspects that the malware CosmicEnergy is developed by penetration testers at Rostelecom-Solar[34].

In the war in Ukraine, it appears that Russian threat actors have made a shift in the ICS[13] malware they've used: From large, complex and modular systems with several integrated functions and protocols, to smaller, simpler tools with specific functions and hard coded configuration. It's likely that this is because the attackers no longer have time to develop modular, multifunctional malware due to the war.

It is highly likely that mission driven threat actors will gather and organise topological data and addressing information, to be able to build malware and attack techniques. Many types of data, for instance from open sources, professional systems, project plans and IoT[14] devices, would be useful to an attacker in long term preparations of an attack. Data can be acquired through theft or purchase from other actors. Such data would help to simplify the attacks, since they make it possible to build ttacks that are more specifically directed against the control system in question. Without these data, the attacker would have to reconnoitre to get this information or have recon functionality in the malware they intend to use. This is why it's important to prevent threat actors from gaining access to such data, especially if it's located outside of the control system zone.

> **Addressing information: Why is this so important for the threat picture?**
> Addressing information enables communication with addressed devices once the control system perimeter is compromised. Addressing information also provides opportunity for control and disruption. For an attacker, addressing information simplifies communication with control system units, in that it eliminates the need for potentially noisy reconnaissance. Control system reconnaissance is reduced to simple data base theft, which can be done in an earlier phase, or by others.
> Control system addressing information can be found in several locations with highly varying levels of security:
> - Redundant systems
> - Emergency systems
> - Test and development systems
> - Digital twins
> - Supplier support systems
> - Security backups
> - Configuration and security documentation
> - Cloud based operational data systems

It is highly likely that AI will be used to simplify the work of compiling addressing information and topological data with other information to build attack techniques. This will still require human knowledge of the control system both generally and specifically. On it's own, AI isn't capable of understanding what information is useful or critical for building attacks, but in combination with skilled personnel it will be able to gather information and discover weaknesses faster than traditional intelligence and analysis.

In attacks on control systems, it's highly likely that a threat actor will exploit missing authentication of control traffic to SCADA or controllers. Most control systems today do not support authentication

12 IEC-61850-5-104
13 Industrial Control Systems (ICS)
14 Internet of Things (IoT)

of external traffic to the control system, or between SCADA[15]/DCS[16]-system and PLC[17]/RTU[18]. This makes it possible for attackers to falsify sender information so that the traffic originates from a legitimate system, for instance a redundant system. Simple and common countermeasures on controllers or network equipment, like access lists or basic firewall functions, can be circumvented.

15 SCADA
16 Distributed Control System (DCS)
17 Programmable Logic Controller (PLC)
18 Remote Terminal Unit (RTU)

8 The threat picture is both local and common

There are actors in the world who wish to attack our sectors, many for economic reasons, but some also for security political ones. InfraCERT believes that good threat awareness and understanding requires nuance.

Disruptive attacks with brief interruptions of production are likely. This should not be confused with destructive attacks causing injury to humans or lasting damage to equipment, which is highly unlikely. The difference should be communicated to all stakeholders.

InfraCERT encourages members to make their own assessments, and not uncritically accept information or claims from commercial companies nor authorities. The threat picture must be seen in relation to assets and vulnerabilities of the individual business.

It's important that members share information with InfraCERT, so that we can contribute to a common threat picture that is as correct and up to date as possible.

References

[1] Nasjonal sikkerhetsmyndighet. *Risiko 2024*. Feb. 12, 2024. URL: https://nsm.no/getfile.php/1313477-1707733210/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf.

[2] Etteretningstjenesten. *Fokus 2024*. Feb. 9, 2024. URL: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus2024%20-%20NO%20-%20Weboppslag%20v2.pdf.

[3] PST. *Nasjonal trusselvurdering 2024*. Feb. 12, 2024. URL: https://pst.no/globalassets/2024/ntv2024/nasjonal-trusselvurdering-2024_uuweb.pdf.

[4] Kripos. *Cyberkriminalitet 2024*. Apr. 24, 2024. URL: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf.

[5] Politiet. *Politiets trusselvurdering 2024*. Mar. 4, 2024. URL: https://www.politiet.no/globalassets/tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2024.pdf.

[6] Orange Cyberdefense. *Security Navigator 2024*. Jan. 11, 2024. URL: https://www4.orangecyberdefense.com/security-navigator-2024.

[7] Microsoft Security. *Microsoft Digital Defense Report 2023*. Oct. 6, 2023. URL: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[8] Global Resilience Federation. *Semi annual Ransomware Report H2 2023*. Feb. 28, 2024. URL: https://static1.squarespace.com/static/60ccb2c6d4292542967cece7/t/65df77b189e978590077e1cd/1709143989084/Semiannual+Ransomware+Report+-+H2+2023+Final.pdf.

[9] ODNI. *Annual Threat Assessment of the U.S. Intelligence Community*. Mar. 8, 2024. URL: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[10] KraftCERT/InfraCERT. *Threat Assessment 2023*. July 6, 2023.

[11] Inc Dragos. *OT CYBERSECURITY THE 2023 YEAR IN REVIEW FEBRUARY 2024*. Feb. 19, 2024. URL: https://hub.dragos.com/hubfs/312-Year-in-Review/2023/Dragos-2023-Year-in-Review-Full-Report.pdf.

[12] Palo Alto. *Incident Response Report 2024*. Feb. 16, 2024. URL: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf.

[13] Artic Wolf. *2024 Threat Report*. Feb. 20, 2024. URL: https://arcticwolf.com/resource/2024-threat-report-lp/arctic-wolf-labs-2024-threat-report.

[14] Waterfall. *2024 Threat Report: OT cyberattacks with Physical Consequences*. Apr. 1, 2024. URL: https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2024-threat-report-ot-cyberattacks-with-physical-consequences/.

[15] Crowdstrike. *2024 Global Threat Report*. Mar. 6, 2024. URL: https://go.crowdstrike.com/global-threat-report-2024.html.

[16] IBM Security. *Threat Intelligence Index 2024*. May 13, 2024. URL: https://www.ibm.com/downloads/cas/L0GKXDWJ.

[17] ENISA. *ENISA THREAT LANDSCAPE 2023*. Oct. 19, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport.

[18] Environmental Protection Agency. *EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation's Drinking Water*. May 20, 2024. URL: https://www.epa.gov/newsreleases/epa-outlines-enforcement-measures-help-prevent-cybersecurity-attacks-and-protect.

[19] Nasjonal sikkerhetsmyndighet. *Nasjonalt digitalt risikobilde 2023*. Oct. 19, 2023. URL: https://nsm.no/getfile.php/1313382-1697777843/NSM/Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf.

[20] Betina Slagnes. *FFI-RAPPORT 23/00546 Hva vet vi om innsiderisiko?* Mar. 6, 2023. URL: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3155/23-00546.pdf.

[21] Daniel Frank. *Threat Assessment: BianLian*. Jan. 19, 2024. URL: https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment.

[22] CISA. *Exploitation of Unitronics PLCs used in Water and Wastewater Systems*. Nov. 28, 2023. URL: https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems.

[23] National Cyber Security Centre. *The near-term impact of AI on the cyber threat*. Jan. 24, 2024. URL: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.

[24] Microsoft Threat Intelligence. *Staying ahead of threat actors in the age of AI*. Feb. 14, 2024. URL: https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai.

[25] Security Intelligence. *AI vs. human deceit: Unravelling the new age of phishing tactics*. Oct. 24, 2023. URL: https://securityintelligence.com/x-force/ai-vs-human-deceit-unravelling-new-age-phishing-tactics.

[26] Nathaniel Raymond. *Major Energy Company Targeted in Large QR Code Campaign*. Sept. 20, 2023. URL: https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign.

[27] Google Cloud. *Insights for future planningCybersecurity Forecast 2024*. Nov. 9, 2023. URL: https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf.

[28] CISA. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Feb. 7, 2024. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[29] Group-IB. *HI-TECH CRIME TRENDS REPORT 2023/2024 - EUROPEAN CYBER THREAT LANDSCAPE*. Feb. 28, 2024. URL: https://www.group-ib.com/landing/hi-tech-crime-trends-2023-2024/.

[30] Trend Micro. *LockBit Attempts to Stay Afloat with a New Version*. Feb. 22, 2024. URL: https://www.trendmicro.com/en_us/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version.html.

[31] Viasat. *KA-SAT Network cyber attack overview*. Mar. 31, 2022. URL: https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview.

[32] Mandiant. *APT44: Unearthing Sandworm*. Apr. 17, 2024. URL: https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf.

[33] Mandiant. *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*. Nov. 10, 2023. URL: https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.

[34] Mandiant. *COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises*. May 25, 2023. URL: https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response.

Appendices

A About KraftCERT/InfraCERT

InfraCERT optimizes securing of process control systems for the power industry. We update our members about relevant vulnerabilities and threats, so that they will be able to detect and defer digital attacks.

InfraCERT is an ISAC (Information Sharing and Analysis Center) and an IRT (Incident Response Team) for its constituency, and InfraCERT aims at ensuring good, secure and efficient incident management and information sharing between relevant companies nationally and internationally.

InfraCERT is a sector CERT for the electric power and petroleum sectors. The InfraCERT constituency also includes process control industry, water & wastewater, and energy recovery. InfraCERT is part of the Norwegian national response organization.

InfraCERT is an independent non-profit corporation, but has alerting responsibilities for the power and petroleum sectors in Norway in the event of serious cyber incidents. InfraCERT also does threat assessments, and gives input to national threat assessments.

InfraCERT is part of the Norwegian Sector Response Network, is a full member of Forum of Incident Response and Security Teams (FIRST) and is a certified incident response team in Trusted Introducer. InfraCERT has members both in Norway and Iceland.

Read more about our services on https://www.kraftcert.no/en/

Notify KraftCERT about an incident: https://varsling.infracert.no/

Contact info:

- cert@kraftcert.no (Incidents)
- postmottak@kraftcert.no (Administrative requests)
- Phone: +47 940 32 443 (service 08-16 on weekdays, Oslo-time)

B Glossary

Access Broker Actor reselling stolen access to systems. Page 13.

CRM *Customer relationship management*. Systems used for managing customer relations. Page 16.

DCS *Distributed Control System*. Control system with a large degree of site autonomy. A central monitoring system is often used in combination. Page 19.

HMI *Human-Machine Interface*. Interface between human and machine, typically in the form of a screen and buttons / keys. Page 24.

IAB Initial Access Broker. Page 13, 17, *see also* Access Broker.

ICS *Industrial Control Systems*. Systems for management and control of industrial processes. Includes terms likeHMI,PLC,PLS. Page 18.

IoT *Internet of Things*. Internet of Things Equipment (Sensors, Switches, etc.) Networked. Page 18.

OT *Operational technology*. Process technology. Page 15.

PLC *Programmable Logic Controller*. Specialized computer capable of controlling industrial processes. Page 19, 24.

PLS Programmable Logic Control. Page 24, *see also* PLC.

RTU *Remote Terminal Unit*. Terminal unit for converting digital and analog signals between sensors and actuators and control system (SCADA, DCS). Page 19.

SCADA *Supervisory Control And Data Acquisition*. Control and monitoring systems. Page 16, 19.