

# Under the Lens The Energy Sector

PwC Threat Intelligence

Q3 2024



TLP: GREEN

# Contents

<b>Key Findings</b>	<b>2</b>
<b>Threat Trends</b>	<b>4</b>
Espionage	4
Cyber crime	5
Sabotage	6
Hacktivism	7
<b>Sector Trends</b>	<b>7</b>
Operational Technology	7
Energy Sector Regulation	8
Third party and Supply chain risks	8
<b>Timeline of attacks</b>	<b>9</b>
<b>Threat landscape</b>	<b>10</b>
<b>Case study</b>	<b>12</b>
<b>Conclusion</b>	<b>13</b>
Appendix 1: Analysis methodology	15
Appendix 2: PwC Threat Intelligence	16
Appendix 3: Threat Assessment Matrix	17

# Introduction

The energy sector is the foundation of modern society. It encompasses production, transmission, distribution chains and retail and includes various energy forms such as electricity, natural gases, and renewables like wind and solar. A significant shift in the sector has been the digitalization of legacy Operational Technology (OT), which traditionally relied on manual controls and isolated systems. As these legacy systems become integrated with modern digital technology they enhance efficiency but also introduce new vulnerabilities to the sector. The growing digital footprint and diverse motivation of threat actors that target the sector make it crucial for organisations to monitor the threat landscape, create secure environments, and have the capability to detect and respond to cyber incidents to minimise their impact. Cyber security is typically considered a board level risk and organisations should be taking active steps to prioritise it as a result.

This report provides an overview of common cyber threats currently facing the energy sector, to illustrate the motivations behind such attacks, and support intelligence-led decision making in cyber security policies and strategies within organisations. The overall view presented in this report, spans the entire energy sector (as described above), and more granular threat analysis should be done on a per-organisation basis due to the unique risk profile that exists in each organisation.

This report does not cover threats to the Electric Vehicle (EV) sector. Although there are cross overs with the energy sector, technology used in EV production is less reliant on legacy Operational Technology and therefore presents a differing threat landscape than the one described in this report.

Our analysis is informed by our own in-house intelligence on cyber attacks and targeting from a variety of threat actors, intelligence gleaned from our incident response engagements around the world, and publicly available reports on attacks in the sector.



# Key Findings

The overall threat level to the energy sector globally is assessed as **CRITICAL**.<sup>1</sup> The energy sector is a permanently attractive target to multiple threat actors because of the information its constituents hold, the significant and vulnerable attack surface that exists in the sector, and the importance that the sector plays in powering modern societies. In determining threat levels, a threat actors' intent, capability, and opportunity to conduct an attack has been assessed.

- The threat of espionage attacks is assessed as **CRITICAL**. Espionage threat actors have shown they are determined to carry out operations against the energy sector. This intent has been assessed against the current backdrop of geopolitical issues dominating the world and social and government pressure to transition to, and innovate in, alternative sustainable energy sources. Espionage motivated threat actors have demonstrated an advanced capability to exploit and persist in networks for long periods undetected, enabling them to collect against intelligence requirements and observe the activities of their targets.
- The threat of cyber crime attacks is assessed as **HIGH**. While the energy sector, compared to many other sectors, is less likely to be specifically targeted, cyber criminals are opportunistic and, will target vulnerable systems within the energy sector when they get the opportunity. These threat actors are financially motivated and are typically interested in things they can monetise, i.e., payment or identity information. Cyber criminals have a range of technical capabilities, leading to a broad spectrum of attack sophistication. Further elevating this threat level is the expanding attack surface that has been created by the interconnectivity of systems, and a proliferation of legacy systems due to the geographically dispersed and often extremely remote nature of some operational sites, offering increased opportunities for exploitation.
- The threat from sabotage is assessed as **MODERATE**. Threat actors have the capability to launch an attack of this type, however, the decision to do so is often influenced by geopolitical events and the relationships between governments. This threat level can quickly escalate if diplomatic relations deteriorate, or conflicts worsen, as demonstrated by Russia's targeting of Ukraine's energy sector during the war to cause widespread impact.
- The threat of cyber hacktivism is assessed as **MODERATE**. Due to the social and geopolitical issues that are dominating the world stage, patriotic hacktivist attacks are becoming more prolific, often overseen or directed by state sponsored entities, giving hacktivist motivated threat actors an implied intent. Hacktivist threat actors have been assessed as having a medium capability. The ability to initiate a hacktivist-driven attack spans a spectrum of complexity, from basic operations, such as website defacement and DDoS attacks, to slightly more sophisticated operations that involve the theft and subsequent release of sensitive information. This diversity and increased targeting across all sectors, underscores the elevated threat level posed by such activities.

---

<sup>1</sup> Refer to appendix 3 for more information on threat level definitions.

# Threat Trends

The overall threat level to the energy sector is **CRITICAL**. The Critical National Infrastructure (CNI) (also referred to as Critical Infrastructure in Australia and other parts of the world) status of the energy sector combined with geopolitical tensions and conflict across the globe, such as Russia's war in Ukraine or the ongoing war between Israel and Hamas, and the public exposure of Russia, China and Iran's cyber operations within this sector all contribute to the heightened threat level. Compounding the threat is the ever-increasing digitalisation and connectivity of systems used to manage the generation and transmission of energy, as well as the increasing presence and integration of renewable energies into the existing infrastructure and operations. The attack surface of the energy sector is also significantly increased by the use of Operational Technology (OT) systems. These OT systems are often geographically dispersed, meaning they are not typically within corporate buildings or enterprise data centres and therefore more complex to manage during a cyber attack. Adding to the vulnerability of the ever-expanding attack surface is the fact some of the OT systems are unpatchable legacy systems, and therefore difficult to secure without significant network segregation efforts.

## Espionage

The threat of espionage attacks is assessed as **CRITICAL**.

The resilience and reliability of energy sources continue to be a top priority for most governments and the sector in general. The energy sector has heavily invested in Research and Development (R&D) to evolve technologies from renewables to nuclear power. The pressure on R&D has been increasing due to growing demands for green energy and the shift away from fossil fuels. This pressure has been further compounded following Russia's stoppage of gas supply to Europe in 2022, prompting governments around the world, including the United States and multiple European countries, to intensify their support for renewable energy production.<sup>2</sup> This move aimed to fortify domestic energy output and reduce dependence on external exports. The heightened emphasis on seeking alternative energy sources is highly likely to see an increase in cyber espionage attacks from both state-sponsored threat actors and competitors. Intellectual property stolen through espionage intrusions can be used by other countries or competitors looking to cut the high costs and long timescales typically needed in the development of new technology.<sup>3</sup> This was the case that was launched against five agents reportedly working for the People's Liberation Army for hacking computers of multiple targets, including SolarWorld in 2012. It was alleged they stole and shared with Chinese energy companies the Intellectual Property (IP) to produce Passivated Emitter Rear Contact (PERC) solar cells. In 2017 SolarWorld's CEO testified at a special US committee hearing that their Chinese competitors gained advantage through the stolen information in 2012 that ultimately saved them time and money in their own R&D to produce PERC technology.<sup>4</sup>

China based threat actors are involved in extensive and complex cyber espionage operations around the world. The energy sector is a particularly attractive target to them. In March 2021, China released its 14<sup>th</sup> Five-Year Plan (FYP), in which it articulated key sectors that it was going to focus on over the next five years. One of the key areas of interest, and of relevance here, was the energy sector, with a greater emphasis on Research & Development (R&D) and innovation. PwC has previously assessed there is a correlation between strategies set out in China's FYP and China-based threat actors' targeting behaviour.<sup>5</sup> In March 2024, a China-based threat actor conducted espionage targeting critical infrastructure in the US. Using living-off-the-land techniques to stay hidden, the threat actor stole control and monitoring system information, remaining undetected for five years.<sup>6,7</sup> This operation likely aimed to gather intelligence on power generation and infrastructure to be applied in their own energy companies'

---

<sup>2</sup> Analysing the impacts of Russia's invasion of Ukraine on energy markets and energy security – Russia's war on Ukraine, International Energy Agency, <https://www.iea.org/topics/russias-war-on-ukraine>

<sup>3</sup> CTO-UTL-20221010-01A – Energy Sector Report

<sup>4</sup> SolarWorld testifies on Chinese IP theft, Christian Roselund, PV Magazine, <https://pv-magazine-usa.com/2017/10/10/solarworld-testifies-on-chinese-ip-theft/> (10<sup>th</sup> October 2017)

<sup>5</sup> CTO-SIB-20210423-01A China's 14<sup>th</sup> Five-Year Plan

<sup>6</sup> US, UK accuse China of cyberespionage that hit millions of people, Reuters, <https://www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25/> (26<sup>th</sup> March, 2024)

<sup>7</sup> FBI calls out China for making critical infrastructure 'fair game' for cyber operations, VOA, <https://www.voanews.com/a/fbi-calls-out-china-for-making-critical-infrastructure-fair-game-for-cyber-operations-/7576013.html> (18<sup>th</sup> April, 2024)

R&D programs and enable them to find vulnerabilities in the system, and steal information that can be used to enhance any future sabotage strategies. Information such as business continuity plans can arm threat actors with the knowledge to develop tactics to undermine or neutralise a business' response strategy and increasing the effectiveness and severity of their overall attack.

## Cyber crime

The threat of cyber crime attacks is assessed as **HIGH**.

The energy sector is an attractive target for multiple reasons, including its critical infrastructure status, and the distorted perception that the entire sector is highly profitable, which doesn't take into consideration the high number of smaller organisations in the sector. According to data analysed by PwC, the energy sector was ranked 19th out of 25 sectors in terms of actual victims of ransomware attacks in 2023. This ranking only includes successful attacks and does not consider the number of companies that were targeted but where the attempts failed. Data since 2022 to the time of writing indicates a steady upward trend in ransomware attacks on the energy sector, highlighting an increase in the number of targeted energy sector companies.<sup>8</sup> This is ransomware data and does not account for other forms of cyber crime, for example, Business Email Compromise (BEC) or data theft of credentials or other forms of personal information that can be on sold, which account for greater levels of revenue loss.

Due to their critical infrastructure status and the broad societal impacts of disruptions, cyber criminals likely perceive the energy sector as more likely to pay ransoms to minimise disruptions. While outwardly facing, the energy sector appears to have a high profitability, this is only true for some of the companies operating within the sector, with many small to medium sized businesses that are not as profitable as their more prominent counter-parts within the sector. Media reporting however, does not reflect this and largely focuses on the industry as a whole or the larger energy companies. This leads to distorted opinions on the true profitability of the sector. For instance, McKinsey & Company reported that investment in the energy sector is to grow from USD 1.5 trillion in 2024 to USD 2.0 - 3.2 trillion by 2040.<sup>9</sup> This reported financial strength would lead threat actors to the belief that companies can meet their demands, despite there being many companies not able to do so.

Many larger energy companies operate globally, owning generation or retail arms in multiple countries, meaning their systems are likely connected in some way, and cyber attacks can have global impact. Within each of these companies there are also suppliers and vendors who often have software or technology integrated with that of the energy company. This interconnectedness has created a much larger attack surface that is harder to protect, given that companies rarely have complete visibility of every single technological asset they have. This has created more possible vulnerabilities for opportunistic cyber criminals to exploit and infiltrate systems to steal or ransom valuable information or affect availability of critical business systems. This was the case for EnergyOne, a global supplier of software products and outsourced operations for companies within the energy sector. When the Australian branch of EnergyOne was targeted by a cyber attack, its corporate systems in both Australia and the UK were impacted.<sup>10</sup> In the case of EnergyOne, information suggested only their corporate systems were compromised, and the company had disconnected its corporate systems from customer-facing systems to prevent the attack spreading downstream.<sup>11</sup> However, had EnergyOne not disconnected the systems, this attack could have played out differently and had adverse flow on impacts on energy companies using their software.

Stolen information can also lead to further revenue loss by way of BEC and Vendor Email Compromise (VEC) for energy sector companies. BEC and VEC are effective tools that cyber criminals have increasingly used, with stolen information making it harder to identify impersonations and fraudulent invoices. A study by security researchers, identified that there had been a 65% increase in VEC targeting to the energy and infrastructure sector while there was an 18% rise in BEC attacks in a six month period from July to December 2023.<sup>12</sup> Lastly, parts of the sector

---

<sup>8</sup> PwC GTI Ransomware data

<sup>9</sup> Global Energy Perspective 2023: Energy value pools outlook, McKinsey & Company, <https://www.mckinsey.com/industries/oil-and-gas/our-insights/global-energy-perspective-2023-energy-value-pools-outlook> (16th January, 2024)

<sup>10</sup> Energy One systems hit by cyber attack, Information Age <https://ia.acs.org.au/article/2023/energy-one-systems-hit-by-cyber-attack.html> (22nd Aug, 2023)

<sup>11</sup> Cyber attack on Aussie energy services firm may hit UK CNI, ComputerWeekly, <https://www.computerweekly.com/news/366549074/Cyber-attack-on-Aussie-energy-services-firm-may-hit-UK-CNI> (21st August 2023)

<sup>12</sup> Energy and Infrastructure Industry Sees Steady Growth in Cyberattacks, Mike Britton, Abnormal, <https://abnormalsecurity.com/blog/energy-infrastructure-email-attacks-2023> (27th February 2024)

involved in retail aspects of energy distribution hold a lot of valuable information, such as customer data, including credit card and bank account details, and other personally identifiable information that can be on-sold later the black market.

## Sabotage

The threat from sabotage is assessed as **MODERATE**.

Attacks designed to destroy or disrupt data and networks have increased in recent years, especially as they have become very prevalent in conflicts such as the Israel-Hamas conflict, where small to medium enterprises in Israel are frequently being targeted with destructive attacks by both Iran and its proxies, and the Russian war in Ukraine, where the energy sector has been targeted to cause widespread blackouts. This underscores Russia's intent and capability to launch such attacks during times of conflict.<sup>13,14</sup>

State-based threat actors almost certainly have cyber sabotage capability, however their intent to use it is largely dependent on geopolitical events and strategic goals. Factors such as deterioration in diplomatic relationships could quickly escalate this threat level, highlighting the importance of companies within the energy sector maintaining a current understanding of geopolitical issues around the world and how it can impact them.

In mid-2021 a China-based threat actor compromised a single computer and made their way through a series of networks that were a part of critical infrastructure, including the energy sector in Guam.<sup>15</sup> Guam is a strategic country for the US as they house military assets there and would underpin any US military response in the event there was an escalation in conflict between China and Taiwan. Using living-off-the-land techniques the threat actor remained undetected for a long period of time.<sup>16</sup> The US government has since identified that the same China-based threat actor has also infiltrated and hidden malicious code across the US and its critical infrastructure, including the energy sector.<sup>17</sup> While the threat actor has not been reported to have triggered a sabotage attack, reports from US authorities and cyber security experts, including Microsoft, warn this act of espionage, in certain narratives, could be interpreted as a potential pre-positioning to escalate to sabotage in the future.<sup>18</sup> This could serve dual purposes: providing China with a tactical edge if they escalate their military operations in Taiwan, or disrupting US critical infrastructure to affect civilians should relationships between the two nations deteriorate.<sup>19</sup> While the above reporting is focused on attacks in the US,<sup>20</sup> similar reports have also surfaced in Australia stating China-based threat actors had targeted Australian networks in an effort to pre-position for future attacks<sup>21</sup> and the UK has also assessed similar attacks from China-based threat actors to be likely.<sup>22</sup>

---

<sup>13</sup> Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology, Mandiant,

<https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/> (9<sup>th</sup> Nov 2023)

<sup>14</sup> Russian Hackers target 20 energy facilities in Ukraine amid intense missile strikes, The Record, <https://therecord.media/russian-hackers-target-energy-facilities-ukraine> (24<sup>th</sup> April 2024)

<sup>15</sup> Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?, The New York Times,

<https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html> (24<sup>th</sup> May 2023)

<sup>16</sup> Microsoft: Chinese hackers hit key US bases on Guam, BBC, <https://www.bbc.com/news/world-asia-65705198> (25 May 2023)

<sup>17</sup> Chinese hackers have lurked in some US infrastructure systems for 'at least five years' CNN,

<https://edition.cnn.com/2024/02/07/politics/china-hacking-us-agencies-report/index.html> (7<sup>th</sup> February 2024)

<sup>18</sup> Volt Typhoon targets US critical infrastructure with living-off-the-land techniques, Microsoft, <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/> (24<sup>th</sup> May 2023)

<sup>19</sup> Americans should prepare for cyber sabotage from Chinese hackers, Us official warns, Reuter,

<https://www.reuters.com/world/americans-should-prepare-cyber-sabotage-chinese-hackers-us-official-warns-2023-06-12/> (13<sup>th</sup> June, 2023)

<sup>20</sup> People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection, Joint Cybersecurity Advisory,

[https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA\\_Living\\_off\\_the\\_Land.PDF](https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF) (24<sup>th</sup> May 2023)

<sup>21</sup> China domestic interference, cyber attacks 'never been more prolific': Coalition, The Sydney Morning Herald,

<https://www.smh.com.au/politics/federal/china-domestic-interference-cyberattacks-never-been-more-prolific-coalition-20240616-p5jm5r.html> (17<sup>th</sup> June 2024)

<sup>22</sup> NCSC and partners issue warning about state-sponsored cyber attackers hiding on critical infrastructure, National Cyber Security Centre, <https://www.ncsc.gov.uk/news/ncsc-and-partners-issue-warning-about-state-sponsored-cyber-attackers-hiding-on-critical-infrastructure-networks> (7<sup>th</sup> February 2024)

## Hactivism

The threat of cyber hactivism is assessed as **MODERATE**.

Hactivism in the energy sector has traditionally focused on social issues like climate change and energy demand. However, with events such as Russia's invasion of Ukraine and the conflict between Israel and Hamas, hactivist groups are increasingly active. Their targets extend beyond direct conflict participants to countries and companies supporting either side. For instance, Anonymous, targeted an Israeli nuclear facility in retaliation for the deaths of Palestinian children.<sup>23</sup> Energy companies are also becoming collateral damage in hactivist campaigns motivated by issues unrelated to the energy sector. This was demonstrated in October 2022, when the Iranian Atomic Energy Organization (AEIO) was hacked, and documents were stolen in retaliation for the death of Mahsa Amini while in the custody of the Islamic Republic's morality police.<sup>24</sup>

Hactivist motivated attacks have previously been limited to superficial attacks such as website defacement or DDoS attacks that are aimed at disrupting digital services and websites. However, in early 2024 it was reported that hactivist groups have shown their intent to move into more destructive attacks.<sup>25</sup> In early 2024, a pro-Russian hactivist group sympathetic to Russia's invasion of Ukraine targeted vulnerable and small-scale Industrial Control Systems (ICS) in North America and Europe. According to the UK's National Cyber Security Centre (NCSC), these groups expressed an intent to escalate from DDoS and website defacement to more disruptive and destructive attacks on western CNI.<sup>26</sup>

# Sector Trends

Beyond the threats posed by different threat actors, the energy sector is faced with challenges caused by the significant Operational Technology (OT) footprint within energy organisations, as well as increasing numbers of regulations and third party/supply chains.

## Operational Technology

The OT environments within the energy sector are highly specialised and complex. Traditionally OT systems were intended to be standalone, and not connected to the internet or other systems. However, through the digitalisation and integration of OT with IT systems, remote access and monitoring by businesses has become possible. In some circumstances it is also a contractual requirement that vendors have remote access to OT systems. This interconnectivity has expanded the attack surface that threat actors could potentially exploit. Compounding this issue is the challenge of legacy systems in OT that cannot be easily updated or replaced without disrupting operations or done in an efficient way, making it vulnerable to attack by threat actors.<sup>27, 28</sup> In early 2024 malware designed specifically to target OT systems was observed to have been used in an attack that cut off heating to 600 apartments in Ukraine. This malware, which was assessed as being the first of its kind in the sense that it used Modbus TCP communication, highlights the evolving capabilities being observed amongst threat actors and the cascading impact that an attack on OT can have.<sup>29</sup>

---

<sup>23</sup> Anonymous claims hack on Israeli nuclear facility, Cyber Daily, <https://www.cyberdaily.au/security/10356-anonymous-claims-hack-on-israeli-nuclear-facility?highlight=WyJpc3JhZWxpIiwibnVjbGVhciJd> (22<sup>nd</sup> March 2024)

<sup>24</sup> Iran says 'specific foreign country' behind hactivist leak of atomic energy emails, The Record, <https://therecord.media/iran-says-specific-foreign-country-behind-hactivist-leak-of-atomic-energy-emails> (24th October 2022)

<sup>25</sup> Pro-Russia hactivist attacking vital tech in water and other sectors, agency says, CyberScoop, <https://cyberscoop.com/pro-russia-hactivists-attacking-vital-tech-in-water-and-other-sectors-agencies-say/> (1<sup>st</sup> May 2024)

<sup>26</sup> Heightened threat of state-aligned groups against western critical national infrastructure, National Cyber Security Centre, 01-May-2024, <https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups> (1st May 2024)

<sup>27</sup> The UK energy sector faces an expanding OT threat landscape, Security Intelligence, <https://securityintelligence.com/articles/uk-energy-expanding-of-threat-landscape/> (20<sup>th</sup> March, 2024)

<sup>28</sup> National Cyber Security Centre – Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, <https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices> (16 April 2018)

<sup>29</sup> Impact of Frostygoop ICS Malware on connected OT Systems, Dragos (July 2024)



State based-threat actors aiming to hinder military mobilisation could use attacking energy sector OT as a vector to shut off power in an area. For hackers, an attack on OT would send stronger messaging or provide them with greater leverage for their demands to be met.

## Energy Sector Regulation

Many regulators have sought to create minimum standards of cyber security for the energy sector within their countries or, in the case of Europe, cross border regulations for the electricity companies with cross-border flows. This includes mandatory reporting of cyber breaches, standardised risk assessments and monitoring.<sup>30,31,32,33</sup> Despite these laws, many energy sector companies still have a way to go to achieve cyber security maturity. For instance, the European Union Agency for Cyber Security reported that 32% of energy sector operators do not have a single critical IT process monitored by a Security Operations Centre.<sup>34</sup> This highlights that while legislation has been designed to improve cyber security standards, the sector is still in the process of growing their cyber security maturity.

## Third party and Supply chain risks

The energy sector supply chain is complex, involving multiple interdependent companies. It begins with the extraction of natural resources from the mining sector, followed by their refining and processing for energy production, and includes transportation, storage, and distribution. Each of these sub-sectors operates within its own supply chain, adding to the layers of complexity across the whole energy sector supply chain. For instance, the software supply chain involves the development, deployment integration and maintenance of software applications for both IT and OT across all segments of the energy sector. This interconnectedness and reliance on each other increases vulnerabilities across the energy supply chain. A company does not need to be in the same supply chain that an initial attack occurs in to be impacted.

North Korea-based threat actors attacked X\_Trader, a financial trading software company, by trojanizing some of their software leading to a supply chain attack.<sup>35</sup> Further research by security organisations later determined that the X\_Trader compromise also directly led to two other organisations, both energy companies, getting compromised as well.<sup>36</sup> Attackers, driven by motives such as financial gain or espionage, need only identify a company within a supply chain that provides a service they can exploit to achieve their desired outcome, leading to a cascading effect on other companies using that service. This highlights the flow-on effect that a supply-chain attack can have and an attacker's ability to create new opportunities to attack companies they would not have otherwise had the chance to attack.

The MoveIt File Transfer system hack in May 2023 is another prime example of the far-reaching impacts of a third-party/supply chain breach. It is estimated that over 2,500 companies, including companies within the energy sector, had been impacted, and over 90 million people had their personal information compromised.<sup>37</sup> PwC's data suggests at least 18 energy companies have been impacted by this hack. However, this number is likely higher as it does not account for companies that paid the ransom before listing.

While the regulations mentioned above could lead to improvements to cyber security practices in the energy sector,

---

<sup>30</sup> 2023-2030 Australian Cyber Security Strategy, Home Affairs, <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy> (22nd November 2023)

<sup>31</sup> National Cybersecurity Strategy", White House, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> (March 2023)

<sup>32</sup> Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L\\_202401366](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401366) (24<sup>th</sup> May 2024)

<sup>33</sup> Cyber security in the UK, House of Commons Library: Adam Clark, April 2024, <https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf>

<sup>34</sup> Cyber Europe tests EU Cyber Preparedness in the Energy Sector, ENISA – European Union Agency for Cybersecurity, <https://www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector> (20th June 2024)

<sup>35</sup> 3CX Software Supply Chain Compromise initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible, Mandiant, <https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise/> (20rd April 2023)

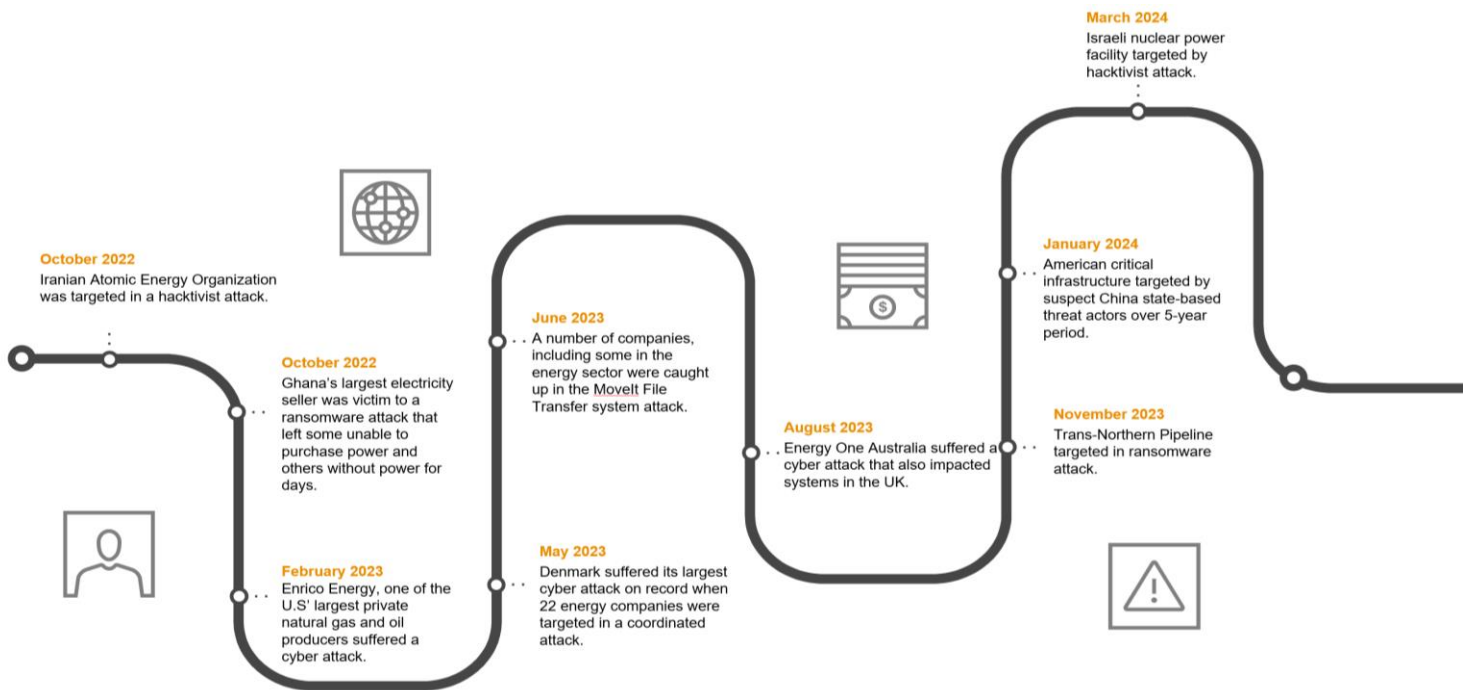
<sup>36</sup> X\_Trader Supply Chain Attack Affects Critical Infrastructure Organizations in U.S. and Europe, Symantec <https://symantec-enterprise-blogs.security.com/threat-intelligence/xtrader-3cx-supply-chain> (22<sup>nd</sup> April 2023)

<sup>37</sup> MoveIt hack victim list, Kon Briefing, <https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html> (20th December 2023)

they do not always place the same level of responsibility for cyber security on third parties and their supply chains. As highlighted in the Cyber Security in the UK Report, there are few mandatory cyber security requirements on third parties.<sup>38</sup> While there is a proposal to bring those services within scope of the Network and Information System (NIS) regulation under the NIS 2 directive in Europe, these changes have not yet been made.<sup>39</sup> Part of this proposal is to require in-scope entities to engage with third party suppliers who have demonstrated adherence to the Cybersecurity Certification Framework.<sup>40,41</sup> This means that any third party engaged with by a company that is considered in-scope by NIS 2 may also need to adhere to the Cybersecurity Certification Framework.

# Timeline of attacks

Across 2023, there were over 200 known cyber security incidents that targeted the energy sector, with more than half of them targeting countries in Europe.<sup>42</sup> PwC has observed a steady upward trend in ransomware attacks on the sector. The below timeline highlights some key incidents since October 2022.



<sup>38</sup> Cyber security in the UK, House of Commons Library: Adam Clark, April 2024, <https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf>

<sup>39</sup> Cyber security in the UK, House of Commons Library: Adam Clark, April 2024, <https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf>

<sup>40</sup> Article 24, Use of European cybersecurity certification schemes, The NIS 2 Directive, Final Text, [https://www.nis-2-directive.com/NIS\\_2\\_Directive\\_Article\\_24.html](https://www.nis-2-directive.com/NIS_2_Directive_Article_24.html)

<sup>41</sup> Cybersecurity Certification Framework, European Union Agency for Cybersecurity, <https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework>

<sup>42</sup> Cyber Europe tests EU Cyber Preparedness in the Energy Sector, ENISA – European Union Agency for Cybersecurity, <https://www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector> (20th June 2024)

# Threat landscape

The below threat actors have been observed by PwC to target the energy sector. These threat actors have different targets according to regions, organisation types, motivations, and intentions. The energy sector's threat landscape can be used to help determine and prioritise coverage of threat actors targeting specific organisations.

## Espionage



Threat Actor	Aliases	Country of Origin
Black Artemis	Lazarus Group, Hidden Cobra, APT38	North Korea
Black Banshee	Kimsuky, Velvet Chollima	North Korea
Blue Athena	APT28, Fancy Bear	Russia
Blue Echidna	Sandworm, Voodoo Bear, Iron Viking	Russia
Blue Kraken	Energetic Bear, Dragonfly, Berserk Bear	Russia
Orange Athos	China Strat, APT-C-09, Patchwork	India
Red Apollo	APT10, Stone Panda, Menupass Team	China
Red Dev 49	Volt Typoom, Bronze Silhouette	China
Red Dev 61	UTA0178, UNC5221	China
Red Ladon	APT40, TEMP.Periscope	China
Red Phoenix	APT27, Emissary Panda,	China
Red Scylla	Chromium, Red Dev 10, Aquatic Panda, Charcoal Typhoon	China
Yellow Dev 29	TA457	Iran
Yellow Liderc	Yellow Dev 11, Imperial Kitten, Totoiseshell, Crimson Sandstorm	Iran
Yellow Maero	OilRig, APT34, Helix Kitten	Iran
Yellow Nix	MuddyWater, TEMP.zagros, Static Kitten	Iran

## Criminal



Blue Cronos	Conti, Emotet, Trickbot, Bumblebee, Lockbit	Russia
Blue Lelantos	Dridex, Evil Corp.	Russia
White Janus	Lockbit, White Dev 66	Under Assessment
White Dev 101	Alphv-NG, Blackcat	Under Assessment
White Dev 15	Blackbasta	Under Assessment
White Austaras	TA505, CL0P ransomware	Under Assessment
White Mjolnir	Ragnarlocker	Under Assessment
White Dev 81	Ozie Team	Under Assessment

	White Veles	DEV-0504	Under Assessment
<b>Sabotage</b> 	Black Artemis	Lazarus Group, Hidden Cobra, APT38	North Korea
	Blue Echidna	Sandworm, Voodoo Bear	Russia
	Yellow Dev 15	Fox Kitten, Parasite, Pioneer Kitten	Iran
	Yellow Dev 19	DEV-0198, Vice Leaker, Emennet Pasargad	Iran
	Yellow Dev 24	Nemesis Kitten, Dev-0270	Iran
	Yellow Dev 35	Soldiers of Solomon, Cyber Av3ngers, White Dev 167	Iran
<b>Hacktivism</b> 	White Dev 149	NoNAME057(16), NoNAME05716, NNM05716	Under Assessment
	Yellow Dev 33	Moses Staff, Abraham's Ax, Marigold Sandstorm	Iran

# Case study

The below case study provides an overview of the publicly reported attacks on 22 Danish energy companies that took place in May 2023.<sup>43</sup>

Threat Actor Motivation	Target	Date
Unknown	Energy Companies	May 2023

## Executive Summary

On 25<sup>th</sup> April 2023, firewall device producer, Zyxel, publicly announced CVE-2023-28771 in several of its devices. This vulnerability was rated as 9.8, indicating the vulnerability was both easy to exploit and the impact of any exploitation would have major consequences. Following this announcement, on 1<sup>st</sup> May 2023, SektorCERT reiterated and emphasised to its members the importance of patching the Zyxel firewalls.

## Tools, Techniques, and Procedures (TTPs)

On 11<sup>th</sup> May 2023, the first wave of two attacks started, with 16 energy companies being targeted in a coordinated attack exploiting CVE-2023-28771. Of these 16, 11 were successful. The threat actors used a specifically designed data packet to port 500 over the protocol UDP to the vulnerable Zyxel devices. The packet was sent to the Internet Key Exchange (IKE) packet decoder on the vulnerable Zyxel devices. This allowed the attacker to execute commands with root privileges on the device without the need for authentication. SektorCERT assessed this allowed them to commence the reconnaissance phase of the attack and gain control of configurations and current usernames. They were then able to see how respective firewalls were configured and decide how to proceed with their attack. SektorCERT in conjunction with the impacted clients was able to stop the attack and prevent damage being caused to the critical infrastructure. SektorCERT later reported that these threat actors had clearly planned the operation extensively, as shown by their precise targeting of companies using vulnerable devices and the resources needed for such a large-scale attack.

There were 10 days between this attack and the next wave of attacks occurring. Between the 22<sup>nd</sup> and 30<sup>th</sup> May 2023 there was at least 11 more attacks on Danish energy companies:

- Six companies were used to participate in attacks against other companies across Hong Kong, the U.S, and Canada. These attacks consisted of DDoS attacks, a brute force attack via a SSH and attacking other companies' firewalls; and.
- Two other companies were attacked by a threat actor using an IP that had links to a Russia-based threat actor, Sandworm (tracked as Blue Echidna by PwC). This caused them to lose visibility of three remote sites and staff needing to physically attend. Since the compromised firewall also functioned as an internal router for the OT network, it meant all internal traffic in the production network had stopped working.

## Key findings from SektorCERT retrospective report:

Most of the attacks were possible because the vulnerable devices did not have the latest updates installed. Many of the companies believed their devices were up to date because they were new and assumed they must have had the latest updates. Some companies had deliberately not updated them because there was a cost from the supplier to install them. Other companies did not know they had the devices connected to their networks, either because they did not have a complete overview of their assets, or suppliers had not informed the companies they were installed.

<sup>43</sup> The attack against Danish, critical infrastructure, SektorCERT, November 2023, <https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf>

# Conclusion

Many threat actors have targeted energy sector organisations in the last few years. Based on incident trends, case studies of attacks and our own-in house analysis, espionage threat actors pose the largest threat to the energy sector. While threat actor objectives may differ, Russia- and China-based threat actors have been the most active in their targeting of energy sector companies. More recently, espionage attacks are suspected to be dual purpose, in that they allow both the theft of sensitive information or research and offer an opportunity for pre-positioning or to collect information for future sabotage attacks.





Looking ahead we assess there will be an increased impact on the energy sector threat levels in the coming years. This will be influenced by the continued growth, investment and innovation in renewable energy solutions and technology advancements, such as increased use and integration of Artificial Intelligence (AI). These advancements will impact the way threat actors target the sector in the future. Decision makers should consider their application within a business in conjunction with a corresponding cyber security strategy as these tools and changes are integrated into the sector.



# Appendix 1: Analysis methodology

Most cyber-attacks have an underlying and ultimate motivation. Although attacks by separate threat actors might share objectives, separate threat actors do not always share the same motivation. Examining the motivation of an attack can enable the identification of the category of attacker.

PwC divides the threat landscape according to the motivation of those behind cyber-attacks. For each, some common tactics, techniques, and procedures (TTPs) observed by PwC’s Threat Intelligence team are included. The divisions are as follows.

Motivation	Description
 <p><b>Espionage</b> For the information</p>	<p>Espionage threat actors (often referred to as “Advanced Persistent Threats”, or APTs) typically seek to steal information which will provide an economic or political advantage to their benefactor. Attacks motivated by espionage usually originate from either industry competitors or state-sponsored threat actors. Often the benefactor is a nation state, and espionage activity aligned to state objectives will reflect geopolitics and real-world events.</p> <p>Usually, the information sought out by espionage attackers is only found at specific organisations, meaning they repeatedly target the same organisation and their suppliers until they have completed their mission.</p>
 <p><b>Criminal</b> For the money</p>	<p>Cyber criminals can be indiscriminate in who they attack as they simply seek to monetise their activities. The range in sophistication of cyber criminals is vast, and displays a widely different set of Tactics, Techniques and Procedures (TTPs).</p> <p>Cyber crime includes both direct ‘cash out’ schemes where an immediate financial gain is made, such as business email compromise, ATM hijacking or the theft of cryptocurrency wallets, as well as activity that seeks to monetise stolen data such as harvesting payment card details or other personal information. Many cyber criminals are merely consumers of stolen data compromised by more sophisticated actors; this data is typically used to commit fraud or identity theft.</p> <p>Ransomware has become a particularly prevalent cause for concern, affecting major private sector corporations through to charities and local government, and everything in-between.</p>
 <p><b>Hactivist</b> For the cause</p>	<p>Hactivists conduct attacks to increase their public profile and raise awareness of their cause. This is typically done through the disruption of services such as denial of service (DoS) attacks, and website defacements. In many cases such attacks are random; they care little how this is done or who is affected, so long as their message is promoted.</p> <p>In some cases, however, their victims are targeted, due to an organisation or individual’s perceived actions or support of an issue. As with espionage, attacks from hactivists are sometimes influenced by real-world events, meaning the risk of such attacks is subject to change.</p>
 <p><b>Sabotage</b> For the impact</p>	<p>Saboteurs seek to damage, destroy or otherwise subvert the integrity of data and systems. Sabotage attacks are not always deliberate and have been used to mask other malicious activity. Sabotage operations designed to be a diversion can still result in significant collateral damage.</p> <p>Examples of attacks include wiping hard drives, causing SCADA systems to malfunction or altering trade data. As with espionage attacks, attacks from saboteurs tend to be influenced by real-world events, making the risk of attacks specific to geography and company actions in relation to political events/issues.</p>



# Appendix 2: PwC Threat Intelligence

## About Us

PwC is globally recognised as a leader in cyber security; as a firm with strong global delivery capabilities, and the ability to address the security and risk challenges our clients face. We underpin our board-level security strategy and advisory consulting services with expertise gleaned from the front lines of cyber defence across our niche technical expertise in services such as Managed Cyber Defence, red teaming, incident response and threat intelligence.

Our threat intelligence team specialises in providing the services which help clients resist, detect, and respond to advanced cyber-attacks. This includes crisis events such as data breaches, economic espionage, and targeted intrusions, including those commonly referred to as APTs.

We differentiate ourselves with our ability to combine strong technical capabilities with strategic thinking, with our research conducted by our in-house experts recruited primarily from governments, the military, and the security services - giving us a unique perspective and a vast array of contacts. Our unique research and security intelligence, technical expertise, and understanding of cyber risk helps clients get the clarity they need to confidently adapt to new challenges and opportunities.

Our threat intelligence research underpins all our security services and is used by public and private sector organisations around the world to protect networks, provide situational awareness, and inform strategy.





<b>Cyber threat intelligence subscription</b> Access to PwC's targeted attack indicator feeds, network and endpoint signatures and tactical and strategic reporting.	<b>Directed research and assessments.</b> Direct access to PwC's threat research team for tasks relating to ad-hoc or long-term enquiries – both tactical and strategic research into malicious samples, threat actors or analysis support.	<b>Cyber threat intelligence monitoring</b> Continuous, bespoke, and focused research which would augment our subscription services.	<b>Consulting and advisory</b> Advisory services to help organisations define requirements, consume, apply, and produce threat intelligence in a way which best suits their organisation.
---	--	---	--

If you would like more information on our services, or to discuss any of the threats contained in this report please feel free to get in touch at [threatintelligence@pwc.com](mailto:threatintelligence@pwc.com).

# Appendix 3: Threat Assessment Matrix

Threat is determined by intent + capability + opportunity. This matrix has been designed to assess the intent and capability of threat actors to provide an overall threat rating they pose to the sector as a whole. Intent talks to the motives that a threat actor possess for targeting a victim. The capability speaks to the technological know-how of a threat actor to act on its assessed intent. The intent and capability are then assessed against the backdrop of what opportunities and vulnerabilities exist that would enable them to carry out an attack.

Knowing which threats are relevant to a given sector is an important step toward strategically directing investment in appropriate defences. The overall view presented in this report, however, spans the entire energy sector, and more granular threat analysis should be done on a per-organisation basis.

<b>INTENT</b>	<b>Persistent</b>	Moderate	High	Critical	Critical	Critical Espionage 
	<b>Attempted</b>	Moderate	Moderate Sabotage 	High Cyber Crime 	Critical	Critical
	<b>Implied</b>	Low	Moderate Hactivism 	Moderate	High	Critical
	<b>Consistent</b>	Very Low	Low	Moderate	Moderate	High
	<b>Not Demonstrated</b>	Very Low	Very Low	Low	Moderate	Moderate
	<b>Little</b>	<b>Medium</b>	<b>Substantial</b>	<b>Severe</b>	<b>Advanced</b>	
<b>CAPABILITY</b>						

Overall Threat Level	Description
<b>Critical</b>	Threat actor targeting is highly likely
<b>High</b>	Threat actor targeting is likely
<b>Moderate</b>	There is a roughly even chance of threat actor targeting
<b>Low</b>	Threat actor targeting is possible but not likely
<b>Very Low</b>	Threat actor targeting is highly unlikely



This content is for general information purposes only and should not be used as a substitute for consultation with professional advisors.

© 2024 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom), which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.

This document may only be distributed according to the TLP classification where one is provided, and otherwise it may not be provided to anyone else. If you believe you are not the intended recipient of this document please do not forward or disclose its contents or existence to others. Please email a copy to [threatintelligence@pwc.com](mailto:threatintelligence@pwc.com) and remove it from your systems.

1407577428331769379.1719551001.