DARKTRACE

AI & Cybersecurity: The state of cyber in UK and US energy sectors

Disclaimer

This report is for informational purposes only.

While every effort has been made to ensure the accuracy and completeness of the findings, the conclusions are based on available data, which may change over time. The information does not constitute legal, financial, or professional advice, and readers should consult relevant experts for specific guidance.

The views expressed in this report are those of the authors and do not necessarily reflect the views of any specific organization or governmental entity. The report does not guarantee the security of any systems, and ongoing vigilance and adaptive strategies are required to address emerging threats.

This report is provided “as is,” without warranties or representations, express or implied, regarding accuracy or completeness. No liability is accepted for any damages or losses arising from the use or reliance on the content.

Acknowledgements

This report is intended to highlight the current challenges the energy sector face, particularly in the United States and the United Kingdom.

The energy sector, which includes electricity generation plants, oil and gas companies, nuclear power facilities, and renewable energy sources, is a critical part of any nation's infrastructure. A cyber-attack on these systems could disrupt the supply of energy, which could have serious consequences for society and the economy.

Cyber threats to the energy sector come in many forms, from state-sponsored attackers looking to disrupt a country's infrastructure, to cybercriminals trying to make a profit, to insiders causing damage. The systems used in the energy sector, such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, can be vulnerable to these threat actors.

Historically, the energy sector has been a major target for numerous cyber attacks across the world for well over a decade. The attacks range from the targeting of the US oil and natural gas firms, Ukraine's power grid, to Saudi Arabia's primary oil manufacturer and distributor, Saudi Aramco.

Therefore, it is crucial that energy companies take cybersecurity seriously.

This involves not just deploying technical measures, but also ensuring they have policies in place to manage cyber risk, training staff to recognize and respond to cyber threats, and planning for how to respond to a cyber incident.

We would like to thank the various energy sector organizations and cybersecurity professionals who took the time to discuss their valuable experiences and knowledge with us. Their willingness to share crucial information has contributed significantly to our research. Thank you also to the Darktrace Analyst and Incident Management teams for their help with this research.

A special thank you to the following:

Siobhan Waldron
EDF UK, Senior Manager,
Cyber Threat Intelligence

James Sutton
EDF UK, Manager,
Cyber Defense & Response

Reyam Enad
EDF UK, Lead Data Scientist,
AI& Automation

Dan Marks
Royal United Services Institute,
Energy Research Fellow

Pia Hüsch
Royal United Services Institute, Cyber,
Technology and National Security Fellow

Mark Bristow
MITRE, Director, Cyber Infrastructure
Protection Innovation Center (CIPIC)

Jeffrey Macre
Darktrace, OT SME

David Masson
Darktrace, Energy SME

Authors: Zoe Tilsiter, Harriet Rayner, Dylan Hinz, Chloe Phillips, Steven Sosa, and Nathaniel Jones

Contents

03	**Executive Summary**	19	Hypotheses
03	Rationale	21	**Threat Hunt Findings**
03	Research Objectives	21	Hypothesis 1
03	How	21	Hypothesis 2
04	Threat Hunts	22	Hypothesis 3
04	Key Findings	22	Hypothesis 4
05	**Definitions**	22	Finding Focus
05	**Introduction**	23	**Discussion and Implications**
06	**UK and US Energy Sectors**	23	Interviews
06	UK	23	AI adoption in energy sector
08	US	23	Risks of tech transformation and AI in the energy sector
09	Increased Cyber Risk	24	Future Threat Landscape
10	**Research Methodology**	27	AI and Cyber Defense
11	**Darktrace Customer Incident Observations**	27	Policy implications
11	General Findings	27	UK Policy Landscape
11	Observed Attack Vectors	29	US Policy Landscape
13	**OSINT Analysis**	30	Gaps and considerations for regulation and policy
13	LLM Literature Review Findings	31	Future Considerations
13	Attack Vectors	32	**Conclusion**
16	UK Findings	33	**References**
16	US Findings	35	**Appendices**
17	**Threat Profile Spotlight**	35	Appendix A: APT28 TTPs
17	APT28	36	Appendix B: Volt Typhoon TTPs
18	Volt Typhoon	37	Appendix C: Experimental Model IoCs
19	**Threat Hunts**	37	Appendix D: Reading UpSet Plots

Executive Summary

Rationale

The energy sector is critical, powering every part of the economy, and has undergone vast technological transformation. Such transformation has increased the sector's cyber-attack surface and risk. External research on Operational Technology (OT) security incidents found that threat actors are intensely focused on the energy sector, over three times more than the next most frequently attacked sectors (critical manufacturing and transportation) [1].

Research Objectives

This research seeks to understand the historical and current threat landscape for the energy sector across the US and UK. It does this by exploring:

- The main advanced persistent threats (APTs) and attack vectors targeting the sector
- Whether technology, including Artificial Intelligence (AI), has and is transforming the energy sector threat landscape
- Whether AI has changed the nature of cyber defense within the sector
- The insights of key stakeholders
- Whether the changing threat landscape is reflected within policy, and the key considerations for businesses and governments

How

Research focused on the UK and US energy sector over a three-year period (November 2021- Dec 2024). Open-source intelligence and customer incidents were analyzed to identify tactics, techniques, and procedures (TTPs). Based on these, hypothesis-driven threats hunts were run, and predictions tested against large language models (LLMs). AI-driven experimental anomaly detection models were created to test the hypotheses across the energy customer base. Findings from these were then posited to key US and UK energy sector stakeholders, to gain critical insights.

Threat Hunts

The hypotheses tested:

- Exploitation of internet facing Human-Machine Interfaces (HMIs) and Programmable Logic Controllers (PLCs) to command-and-control (C2) externally and establish persistence
- Utilization of PerfectData software and multi-factor authentication (MFA) bypass to compromise user accounts and destruct data
- APT28 will target the energy sector, via spear-phishing campaigns and abuse Ivanti Connect Secure virtual private networks (VPN) to perform remote arbitrary code and malware execution
- Volt Typhoon will target energy sector providers, using their KV-Botnet to compromise Small Office/Home Office (SOHO) router devices, and move laterally to achieve their end goal of accessing OT environments

Key Findings

Tech transformation

- Technological advancement in the sector brings cyber risks; Internet of Things (IoT) adoption and control automation in non-dispatchable solar and wind sectors increases attack surface, whilst IT/OT convergence makes islanding during cyber incidents more difficult
- Over dependency on few vendors and systems and a movement towards cloud operations creates further single points of failure, whilst tangled supply chains reduce visibility and management of assets
- The energy sector has long been using AI in sector, although not yet adopted sector-wide due to lack of data quality readiness, data risks, and heavy sector regulation
- Stakeholders are facing challenges in becoming data-driven to develop in-house AI systems

Threat Hunts

- PerfectData experimental model hits were found in the energy sector, including a Saudi Arabian oil and gas investor. PerfectData software and MFA bypass were observed being used to compromise user accounts and destruct data, and in one case facilitated exfiltration of sensitive industrial machine data, demonstrating intent to conduct an OT attack.
- Internet-facing OT devices such as PLCs and HMIs are particularly prevalent in the energy sector. Little evidence was found that this risk is being exploited to C2 externally
- Energy sector devices had connected to low fidelity APT28 indicators of compromise (IoCs), specifically Tor exit nodes, as historically observed by this APT. No further signs of compromise via email or Ivanti Secure Connect VPN vulnerability were observed. The history of APT28 suggests they adapt to evade detection and are likely using new zero-day vulnerabilities
- Low fidelity Volt Typhoon IoCs were observed across energy sector base, including KV-Botnet IoCs on ASUS devices, file hashes and user agents, but no further evidence to confirm definite presence

Attacks and Threat Landscape

- Across the energy customer base, analysis of Darktrace metadata alone was not able to qualify with certainty whether AI was used in the observed attacks, although AI could've been utilized to enhance the speed or scale of attacks
- OT specific attacks were observed. For a Canadian energy provider, unauthorized remote access to the site was exploited to start up a PLC motor at a field substation in the SCADA environment, and request write commands from the PLC to multiple coils
- Geopolitical events have caused an uptick in Nation-state attacks on the sector
- Supply chain attacks via third-party data stores occur across the sector, as evidenced by Clop ransomware group exploiting the MOVEit Vulnerability
- Phishing is still a prolific attack vector across the sector
- Renewable energy producers were increasingly targeted
- Vulnerabilities are commonly exploited in the sector, including common vulnerabilities and exposures (CVEs), lack of MFA on devices, and internet-exposed assets

Implications

Businesses need to ensure asset management across their supply chain, and regular risk assessments and response plans/scenarios are practiced. Efforts must not be siloed across the sector, and increased collaboration is needed. Email security is still integral to reduce initial access, and vulnerabilities need to be addressed; enforcing MFA policies and securing internet-facing devices.

Such findings stress the need for governments to increase preparedness and response to Nation-state attacks, to mitigate critical dependencies through supply chain management and to facilitate intelligence sharing across the sector. They need to also ensure innovation and frameworks keep pace to defend against AI-powered threats in the energy sector.

These findings arise amidst changes within the energy and wider critical national infrastructure (CNI) regulatory landscape across both the UK and US, as The White House Office of the National Cyber Director (ONCD) adopts its Energy Modernization Cybersecurity Implementation Plan, and the UK implements the upcoming Cyber Security and Resilience Bill.

Definitions

Critical National Infrastructure (CNI) is defined by UK National Cyber Security Centre as national assets that are essential for the functioning of society, such as those associated with energy supply, water supply, transportation, health and telecommunications [2].

In the US, 16 sectors are currently designated as CNI. In the UK, there are 14, and in September 2024, Data Centers were newly designated as UK CNI, marking the first CNI designation in a decade following Space and Defense in 2015 [3].

For the purpose of this report, the term "energy sector" refers to any company, public or private, that contributes to the production, distribution or consumption of energy resources [4]. Energy resources are broad and include nuclear, oil, coal and gas, electric, and renewable sources such as hydro, solar and wind.

The roles energy companies play within the sector can be broken into 3 categories. Companies can operate one, or more than one role [5]:

01 **Producer:** the production or generation of the energy source, varying from extraction of oil and gas to electricity generation

02 **Provider:** infrastructure and platforms responsible for transporting and delivering energy, such as transmission or distribution networks

03 **Supplier:** retail suppliers buying energy from wholesale market and supplying electricity and gas to homes and businesses

Darktrace models leverage anomaly detection and integrate outputs from Darktrace Deep Packet Inspection, telemetry inputs, and additional modules, creating tailored activity detection. Darktrace applies Self-Learning AI to an organization's data to understand and identify anomalies specific to them. The research in this report leveraged Darktrace's approach and models.

For the purpose of this report, custom experimental models were developed and tested as part of hypothesis-driven threat hunts.

Introduction

The energy sector is critical, powering every part of the economy. Over the past ten years, there have been important technological changes transforming this critical sector. Most notably, observed IT/OT convergence with the rise of smart grids, signalling a transformation to cyber-physical systems. Many companies in the energy sector have also adopted AI for various uses, such as forecasting supply and demand.

With technological transformation comes greater cyber risk. External research on Operational Technology (OT) security incidents showed that threat actors are intensely focused on the energy sector [1]. The report found that 39 percent of all attacks on critical infrastructure target the energy sector--over three times more than the next most frequently attacked sectors (critical manufacturing and transportation).

This research focuses on understanding how the UK and US energy sector threat landscapes have changed over a three-year period (November 2021-December 2024). Open-source intelligence (OSINT) and customer incidents were analyzed to identify TTPs.

Based on these, hypothesis-driven threats hunts were run, and predictions tested against LLMs. AI-driven experimental anomaly detection models were created to test the hypotheses across the energy customer base. Findings from these were then posited to key US and UK energy sector stakeholders to gain critical insights.

It also explores how AI is reshaping cyber defense in this sector, as well as its implications for national governments, policymakers, and industry innovators. This echoes Department of Homeland Security's emphasis on managing both the evolving risks and opportunities presented by AI as a priority risk area for US critical infrastructure security and resilience [6].

At a time when AI is booming, and when energy sectors globally continue to adapt through technological transformation, understanding how the downstream effects of these changes impact the threat landscape is imperative.

This report provides insight into the current and future AI threat landscape in this sector, and how AI can be used to defend it.

UK and US Energy Sectors

UK

UK Energy Sector

As part of the UK's Energy Delivery System (EDS), energy is first generated or produced. In the UK in 2023, the top domestically produced energy sources were primary oil (crude oil and natural gas liquids) and natural gas [7]. Nuclear output fell by 15 per cent, to levels last seen in the 1960s.

The UK is a net importer, importing 40.8% of energy used, mainly from Norway and US. The UK banned Russian coal imports in August 2022, reflecting a decrease in reliance on Russian energy in an effort to drive energy security [7] [8]. Energy is carried across the country from power plants to substations via transmission network operators (TNOs).

There are three TNOs in the UK:

- National Grid
- SP Energy Networks
- Scottish & Southern Electricity Networks

Distribution network operators (DNOs) move energy from substations towards consumers via powerlines and interconnectors.

In the UK, there are six DNOs:

- Electricity Northwest
- Northern Powergrid
- SP Energy Networks
- Scottish & Southern Electricity Networks
- UK Power Networks
- Western Power Distribution

In 2023, the UK formed the National Energy System Operator, an independent system planner and operator to balance energy supply and demand 24/7 [5,7,8]. The sector is regulated by Ofgem. Domestic energy suppliers then provide energy to homes and business. The main UK energy suppliers are:

- EDF Energy
- British Gas
- E.ON, Scottish Power
- SSE

Energy is also consumed by other sectors, including industry, transport, and services such as agriculture. The UK has set a legally binding target to achieve net-zero (decarbonize all sectors of UK economy) by 2050 [9], and to deliver clean power by 2030. Key to this is growth in the renewable energy sector and reduction in coal production. The share of renewable electricity generation in 2023 was 46.4 per cent, a new record. Both wind and solar generation have increased rapidly in recent years [8, 10].

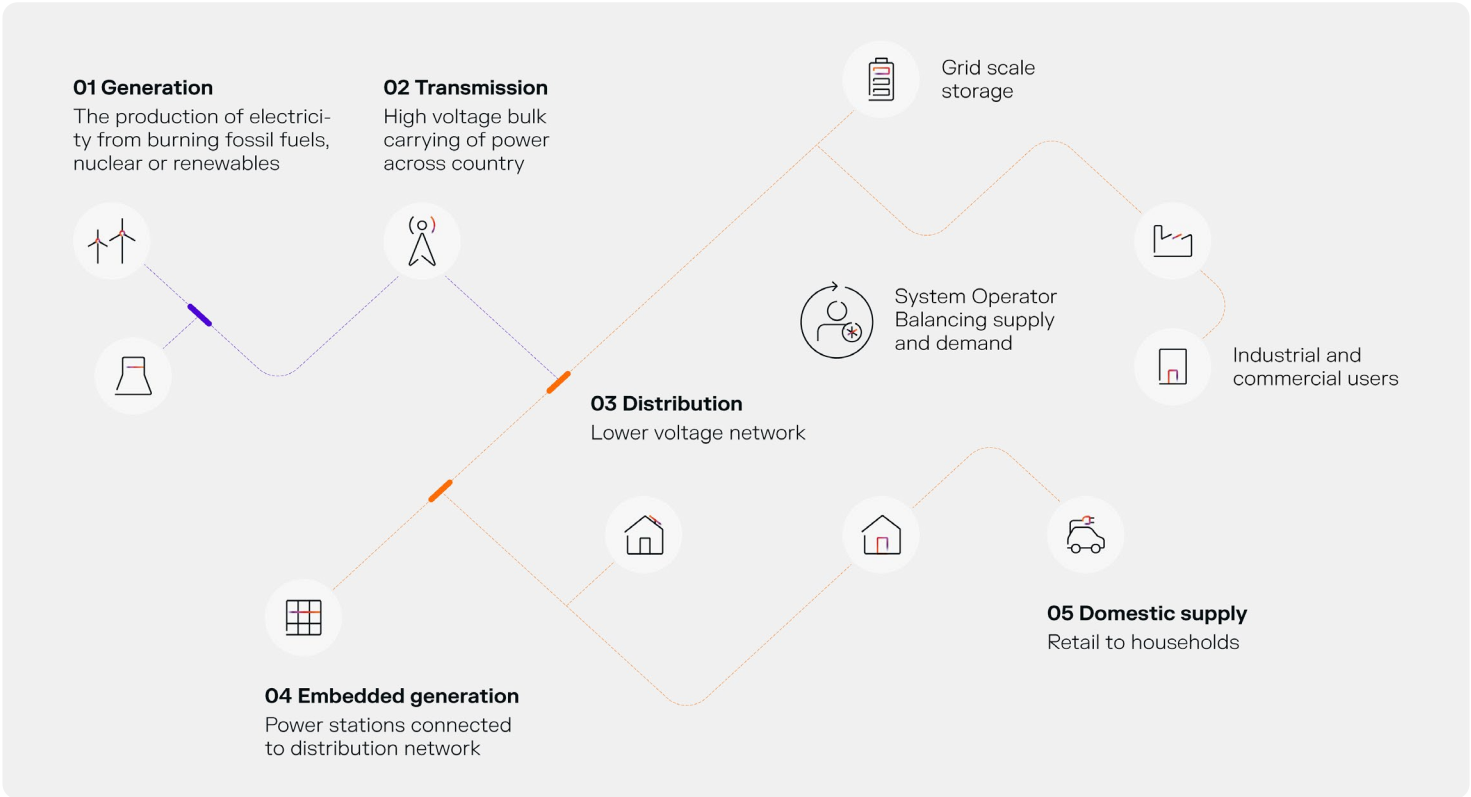


Figure 01: UK Energy structure [5].

Tech transformation in UK Energy Sector

The UK energy sector has adopted multiple technologies throughout the supply chain, from production, transmission, and consumption.

In production, AI is used for wind turbine optimization, calculating wind turbine operations in response to other turbines and variable weather conditions. Vind AI is a company developing this software, supporting various windfarms in Europe, including some based in the UK [12].

At the energy transmission level, sensors are now placed across the UK grid, monitoring the health of components, flagging faults and inefficiencies, and predicting issues prior to becoming real-world issues, such as an outage [13].

At the interface between production and wholesale purchasing, the UK is using AI-driven trading platforms to predict and control the buying and selling of energy stored in batteries across markets in real-time. This AI accesses vast data and manages customer energy storage systems. This method has now become a standard practice in the UK energy market [14].

At the supplier level, technology has transformed domestic energy consumption. Adoption of smart meters has been rapidly rising since 2012. In 2023, 61% of all meters were smart and advanced [15]. Smart meters are an IoT technology, allowing users to track energy consumption in real time, often from an app.

Cybersecurity in UK Energy Sector

In 2018, Ofgem and DESNZ were jointly named as Competent Authority (CA) in the NIS Regulations. As CA, Ofgem imposes duties on Operators of Essential Services (OES) to ensure that UK downstream gas and electricity is meeting network cyber security standards [16], namely through self-assessments based on NCSC's CAF, improvement plans, and incident reporting.

However, across the UK EDS, organizations face challenges in implementing cybersecurity best practices. Information sharing within the UK EDS model is limited. Barriers include trust; reputation; competition; and technical/financial constraints.

Additionally, there is no Information Sharing and Analysis Center (ISAC), or Malware Information Sharing Platform (MISP) within the UK energy sector to facilitate CTI sharing across the sector. Broader information sharing network exist and can help, such as the UK's Cyber Security Information Sharing Partnership (CiSP) and the European Network and Information Security Agency (ENISA) [17].

Operators have varying maturity levels and approaches to cyber security risks management and procurement. This creates inconsistencies along the supply chain and management of risks across the sector. Operators can therefore procure compromised or risky equipment or services within the network and OT, that can put the EDS at risk [18]. Additionally, legacy technology, particularly OT, within the UK EDS, is difficult and expensive to update. This leaves infrastructure and networks vulnerable to cyber-attacks and unable to manage against sophisticated threats.

Additionally, historically, little attention has been given to cybersecurity within the sector. In renewable energy production, a 2024 assessment found that only 1% of UK wind energy firms have capable cyber protection [19]. The need for such protection had not been considered before, but is increasingly coming into focus as renewables increasingly contribute to electricity generation, and are being targeted by attackers [19].

More broadly, historically, little has been spent on energy cyber controls in the UK. In the first RIIO price control review issued by Ofgem for electricity distribution, transmissions and gas distribution, cybersecurity was referred to as "enhanced security costs (IT systems)" and companies were not requesting allowances for cyber [20].

This has changed, and now in RIIO-3, companies need to submit a NIS-R Cyber Resilience Business Plan ('CRBP') as part of their price controls, that aligns with NIS requirements and includes both IT and OT environments [21].

US

US Energy Sector

In the US in 2023, petroleum, natural gas, and coal accounted for 84% of total primary energy production, 8% renewables and 8% nuclear. It has been an annual net total energy exporter since 2019, and in 2023, total US energy exports reached a record high [23]. The general energy structure is similar to the UK; energy is generated at centralized power plants and is transmitted via the grid through electricity substations, transformers, and power lines that then distribute energy to consumers. US Energy consumption in 2023 saw 37% consumed by transport, 35% by industry, 15% residential and 13% commercial [23].

However, the ownership and structure of generation through to distribution depends on whether a state is regulated or unregulated [24]. Three interconnected grid system utilities operate in the US and deliver power to the lower 48 states:

- The Eastern Interconnection
- The Western Interconnection
- The Texas Interconnection

The Eastern and Western Interconnections in the United States are also linked with Canada's power grid.

For regulated parts of wholesale market, these utilities own and are responsible for the entire flow of energy from generation and transmission to distribution to customers. This also includes being a balancing authority to manage supply and demand [24].

However, for unregulated parts of the market, transmission also works on a regional level via independent regional transmission organizations (RTOs) [24]. RTOs purchase wholesale power from these utilities and sell to traders before it reaches consumers. They will also work as balancing authorities on a regional level. There are nine RTOs in North America [25].

The US had been progressing towards decarbonization and net-zero goals.

The Biden Administration committed to net-emissions by 2050 [104]. Both the US and UK have joined the Global Renewable and Energy Efficiency pledge with 130 other countries, committing to triple the world's installed renewable energy generation capacity to 11,000 GW by 2030 [26]. This has increased investments in renewable energy. In 2023, USD 34 billion of US federal government money was spent on clean energy incentives, mostly tax credits, while USD 239 billion was invested in clean energy overall [11].

Tech transformation in US Energy Sector

In terms of production, AI is being used in the US to analyze geographical data to identify possible oil and gas reserves and to optimize drilling processes. [27] AI is being used in nuclear power plants to constantly monitor data from sensors and can detect anomalies to ensure safety [28]. AI is also being increasingly applied for energy trading, predicting energy demands, and predicting when equipment may need maintenance.

AI is used in the grid to detect and isolate faults; ensure voltage levels remain at an optimal level and distribute the energy across the grid evenly to prevent overloading certain areas. It is also used to reconfigure following an issue to reduce disruption [28].

The public sector in the US has adopted optical core arresting wire capable of high-speed transmission of data and is being used in some cases as a secure way to connect the SCADA network or connect the IoT devices across the grid. [29] The grid, as well as industry, homes and workplaces, are using smart meters, sensors, and automated controls to more effectively manage the power distribution, automate energy usage and run certain devices at times when energy prices are lower. Connecting smart devices to apps allows for convenience but does introduce a level of risk when the vulnerabilities of those apps are beyond the organization's control [30].

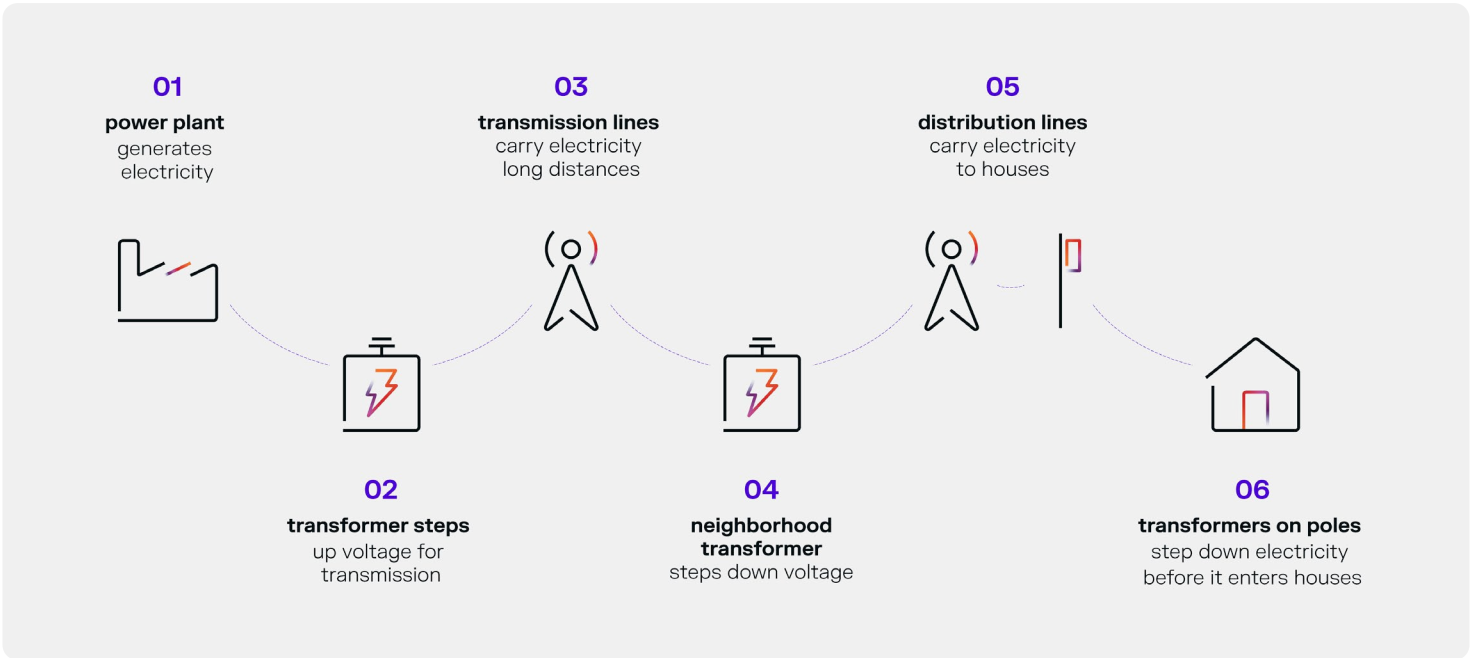


Figure 02: Figure 2: US Energy structure [22].

Cybersecurity in US Energy Sector

The US Department of Energy and CESER recognises the need for the US EDS to be cyber resilient [31]. However, not all actors in the US EDS are subject to the same regulatory authority and differ between whether they have federal or state oversight, which makes it difficult to ensure the same standard of cyber security [32].

Some RTOs for example CAISO and NYISO operate under state regulations, while others like MISO and PJM are subject to federal oversight by the Federal Energy Regulatory Commission (FERC) [33]. The Federal Energy Regulatory Commission (FERC) regulates interstate transmission of electricity, natural gas, and oil, and also regulates hydropower projects and natural gas terminals [34]. However, some government-owned balancing area authorities have limited FERC jurisdiction, such as the Bonneville Power Administration (BPA) and Tennessee Valley Authority [35].

Additionally, the 3 grid interconnection networks are instead overseen by the federal North American Electric Reliability Corporation (NERC). NERC provides an Electricity Information Sharing and Analysis Center (E-ISAC) [36]. However, although NERC provides regulatory requirements for cyber security, some utilities require financial assistance to create cyber strategies and feel like they lack guidance to achieve cyber security outcomes and defences [37].

Such a range of oversight can lead to confusion in jurisdictional applicability, and their different regulatory guidelines regarding cyber security practices results in different levels of adoption. This results in utilities adopting different standards within the US, making it hard to manage from an EDS perspective [38].

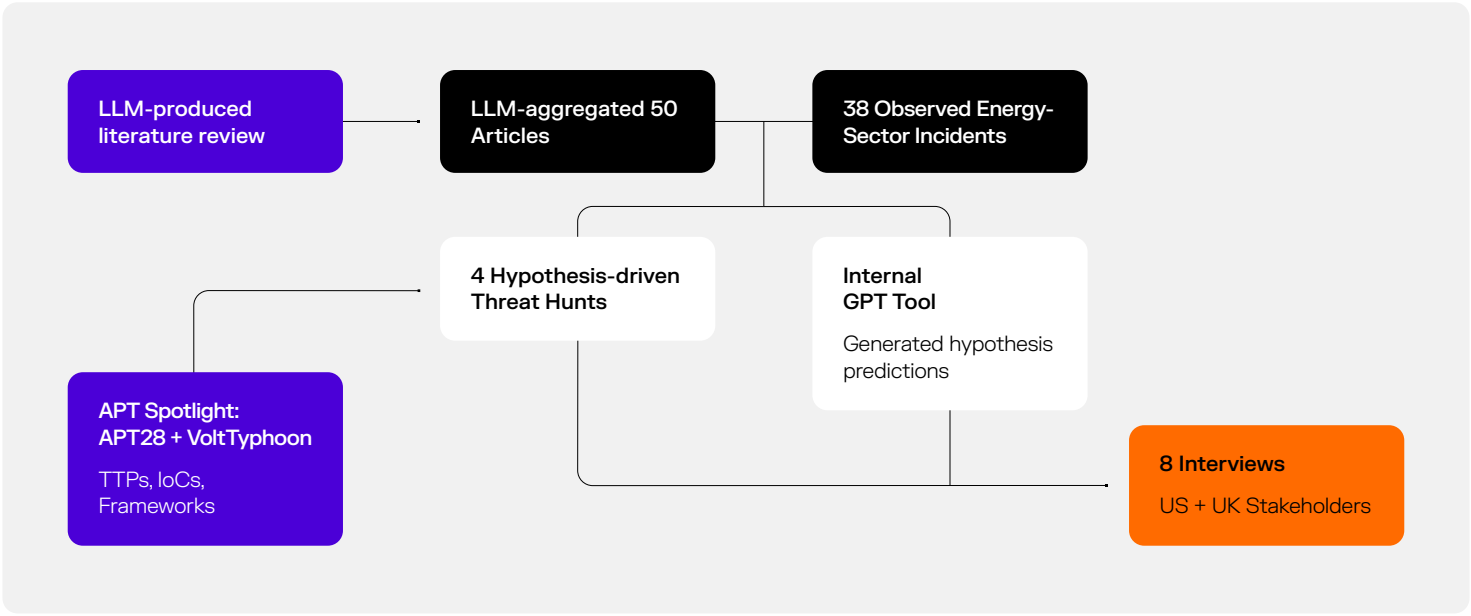
Increased Cyber Risk

Such technological transformation in both UK and US energy sectors increases their cyber risks. Technological adoption increases the attack surface along the supply chain, whilst the increased interconnectivity creates critical dependencies within the sector, making the sector a more high-impact and attractive target to attackers.

The adoption of AI, both within and outside the energy sector, increases the risk of AI being utilized in cyber-attacks.

AI-powered cyber-attacks can identify targets quicker and collect more accurate reconnaissance through customized approaches like social engineering, whilst also automating the execution of the attacks themselves [39]. AI-driven attacks include AI phishing campaigns, AI enabled ransomware, utilizing AI to penetrate CNI attack pathways [40], and attackers poisoning datasets feeding into AI models to interrupt correct functioning [41].

Research Methodology



To address the outlined research objectives, Darktrace undertook research using a range of methods, starting with collection and analysis of open-source and Darktrace customer data pertaining to energy sector attacks from November 2021 to December 2024. To analyze energy sector cyber incidents and evaluate threat vectors, threat actor techniques, sector resilience and policies, Darktrace research implemented a structured approach, leveraging a LLM and its advanced tools and integrations.

During research, a content aggregation platform was used to source and categorize open-source articles into four distinct buckets based on geographic regions: Global, UK, Europe, Middle East and Africa (EMEA), and the US.

Regional buckets provided insights into region-specific threats and trends, while the "Global" bucket allowed detection of broader patterns and benchmark regional resilience. Darktrace researchers used these findings to identify specific cyber incidents, attack vectors employed by threat actors, and TTPs used in cyberattacks targeting energy infrastructure.

Researchers selected a total of 50 articles based on their relevance to these criteria. Researchers used the LLM to generate literature reviews of the articles it found, to provide a structured overview of the threat and attack landscape for each energy sector region, and how policy makers were reacting to them. Researchers compared these findings against incidents observed across the Darktrace customer base. Researchers queried Darktrace metadata and analyzed relevant incidents from November 2021 to December 2024. In total, 38 incidents were analyzed.

This initial analysis informed understanding of the threat landscape, and key Nation-states or state-affiliated threat actors and TTPs targeting the sector.

This was used to inform an Advanced Persistent Threat (APT) spotlight analysis on two groups: Volt Typhoon and APT28, deep diving into the groups' motivations, structures and TTPs. The findings were applied to threat hunting frameworks, namely the Diamond Model of Intrusion Analysis [42] and Mandiant's A4 Framework [43], to craft four hypotheses for hypotheses-driven threat hunts. An LLM was used to query the hypotheses as to whether similar attacks within the energy sector threat landscape had been observed in open-source data. Experimental anomaly detection models were then built and tested across Darktrace environments to search for TTPs or IoCs aligning with the hypotheses. Model outputs were analyzed, in combination with existing Darktrace stock model hits and metadata queries across the energy customer base, to determine whether findings aligned with the sector specific hypotheses.

Findings from these outputs were then posited to key UK and US energy sector stakeholders in eight interviews.

Interview Number	Interviewee
1	Dan Marks and Pia Hüsch, RUSI
2	Siobhan Waldron and James Sutton, EDF UK
3	Reyam Enad, EDF UK
4	Mark Bristow, MITRE
5	US threat intelligence cyber security company
6 + 7	Darktrace OT Subject Matter Experts (SMEs)
8	Cybersecurity vendor roundtable

Darktrace Customer Incident Observations

General Findings

Repeat attacks: A small proportion of incidents were cases of customers being repeatedly targeted by attackers. One such customer was a large energy supplier and the research team investigated them several times over the past year. The investigations were for possible compromises related to Microsoft 365 user accounts and email phishing.

Geography: The majority of cases were US-based, partially accounted for by the respective weighting of regional customer bases. In addition, observed incidents affected energy sector customers in Africa (South Africa, Nigeria and Ghana), Europe (Germany, Denmark, Italy and Spain), and Asia-Pacific (APAC) (Australia, Singapore).

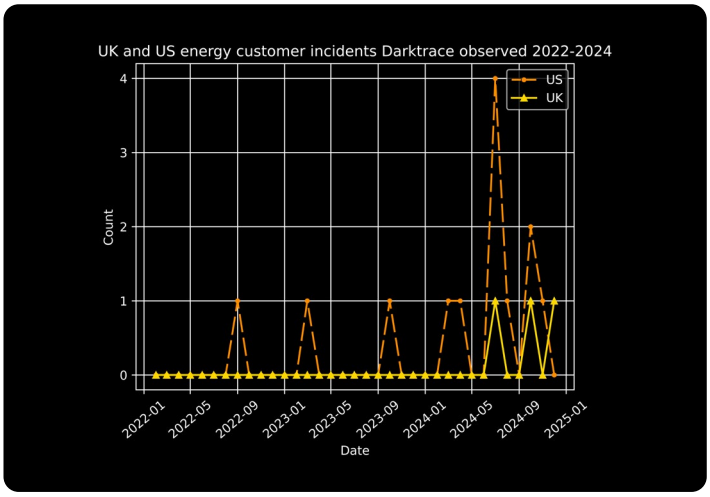


Figure 03: Observed incidents across UK and US energy customer base (2022-2024).

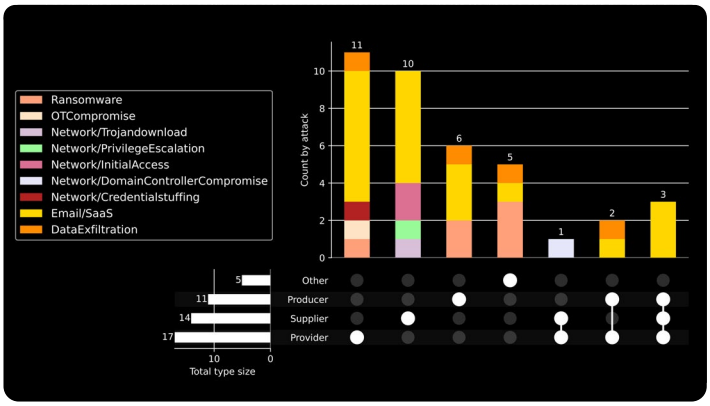


Figure 04: Observed incidents across UK and US energy customer base November 2021- December 2024, according to function and attack vector.

Function: Most of the energy customers affected operate multiple functions, but the majority had provider capabilities (17), followed by supplier (14), and then producers (11). Five of those affected were tangential to the energy sector, operating in energy research or governmental capabilities. There did not appear to be a trend in the types of attack targeting energy functions.

Observed Attack Vectors

Across the customer base, analysis of Darktrace metadata alone was not able to qualify with certainty whether AI was used in the observed attacks. However, AI could've been used utilized to enhance the speed or scale of attacks [44]. Commonly observed attack vectors included:

Email/Software-as-a-Service (SaaS)

As observed in both US and UK cases, and across energy customers of all functions, 55% of cases involved Email/SaaS, making it the most common attack vector. The inbox still represents the most utilized vector for payload delivery, followed by the propagation of SaaS compromises across a deployment. In observed cases, notable trends were:

- **Email as initial attack vector:** Phishing campaign techniques were utilized and varied, including more bespoke attacks via thread hacking, safe-link smuggling and free content sending. More basic methods included malicious file storage links, known adversary-in-the-middle (AiTM) phishing kits, impersonating domains, and hijacking personal email accounts.
  - **AI:** Generative AI can be used in phishing attacks to create realistic and personalised messages to victims at scale. It can also be used, via chatbots, to automate the replies within a phishing attack, building a victim's perception of the correspondence's legitimacy. The customization and scale of these AI phishing campaigns increase the likelihood of an attack [44].
  - **Metadata analysis:** Darktrace / EMAIL alert metadata was analyzed by the team to identify email attack trends across energy customer base. From a sample of data over an 11-month period, a strong correlation was found between the number of active mailboxes and the number of inbound emails detected as phishing. Disseminating phishing emails at this scale could've been assisted by AI. Additionally, it was found that roughly 1/5 of all inbound emails detected as phishing, targeted VIP users within organizations. As discussed, AI is increasingly being used to create sophisticated and customized impersonations to increase the likelihood of a successful phishing attempt.

- **SaaS account spread:** In most cases, the phishing emails were used to harvest credentials, leading to compromise of (often) Microsoft 365 accounts.
  - Once compromised, persistence was established through different means; stealing valid MFA tokens, editing authentication methods or granting OAuth permissions for software. This included abusing PerfectData software, to allow a threat actor to exfiltrate whole mailboxes as a PST file [105].
  - In a few cases, attacks were then seen further propagating, creating new email rules to send outbound phishing emails to compromise further users.
- **Aims:** Motivations of the observed incidents appeared to vary, including accessing sensitive files, destroying data, and financial motivations as some phishing emails led to fraudulent payments being made.

Ransomware and Ransomware-as-a-Service (RaaS)

18% of cases utilized and deployed ransomware. Common threat actors included ALPHV/BlackCat and Fog with others including Sodinokibi, Hunters International, and KOK08. Some of these ransomware groups such as Sodinokibi operate as a RaaS model [45].

- **Initial attack vectors:** Initial entry points varied; cases of Fog appear to use AnyDesk remote access, but other entry points include VPN users or VPN access to steal credentials, VMs to access servers, and AD accounts.
- **Extent:** Ransomware generally resulted in encryption of files, demand of ransom and exfiltration of sensitive data. This led to disruption and impact on services; in one case, multiple oil terminals were forced to operate with limited capacity.
- **Financial motivations:** As a CNI providing essential services, the energy sector is an attractive target for ransomware. As seen with the Colonial Pipeline attack [46], disruptions can have disastrous and very public consequences, lending itself to large ransoms being demanded, and victims quickly making ransomware payments in order to restore operations [47] [48].

OT-specific compromises

In one incident, a Canadian energy provider was attacked via an OT-specific compromise in the SCADA environment.

- **Initial attack vector:** a third party confirmed access via unauthorized remote access.
- **Extent:** A PLC motor was started up at a field substation in the SCADA environment, and write commands were requested by the PLC to multiple coils.

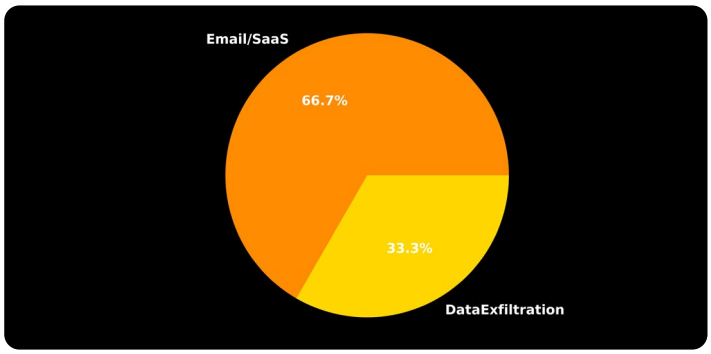


Figure 05: Attack vectors utilized by attackers in Darktrace observed UK customer incidents 2022-2024.

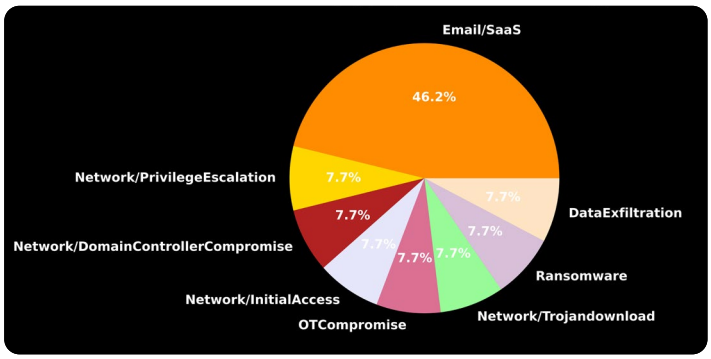


Figure 06: Attack vectors utilized by attackers in US Darktrace observed US customer incidents 2022-2024.

Exploitation of cyber security posture

13% of cases gained initial access due to poor cyber security posture.

- **CVE exploitation:** In one case, CVE-2023-3519 was used to grant initial access by exploiting an internet-facing server hosting Citrix NetScaler. The attack did not progress past this initial access point. In another, the threat actor Termite exploited CVE-2024-50623 on a vulnerable Cleo server to exfiltrate sensitive data.
- **Internet-facing devices:** One incident observed unauthorized access to a web-facing Domain Controller from a suspicious external IP range. In another, Hunters International ransomware utilized internet facing systems open on port 445 to spread, leading to exfiltration of 290GB of PII and ransom demanded.
- **Lack of MFA:** In another instance, lack of MFA was used to exploit a local account via VPN, to eventually gain domain level access to most DCs on the network.

OSINT Analysis

From January 2022 to October 2024, 93 OSINT articles were retrieved via the LLM. 50 of these were directly relevant to known compromises and were analyzed. Most articles related to US energy sector compromises, followed by EMEA (excluding UK). Few articles discussed UK energy sector compromises explicitly. Of the compromises analyzed, none explicitly mentioned utilization of AI-driven techniques to affect their speed, scale, or TTPs themselves.

LLM Literature Review Findings

The LLM analyzed the relevant articles and produced the following insights on trends in the energy sector threat and attack landscape.

General

Overall, the analysis provided from the LLM indicated a rise in attacks on OT environments, increased exploitation of supply chain vulnerabilities, ransomware and disruptive attacks for financial gain. Nation-state actors, especially those linked to Russia, Iran, China, and North Korea, are also actively targeting critical infrastructure for espionage and potential disruption.

UK

Recent incidents and regulatory actions highlight significant cybersecurity gaps, particularly in OT systems. Despite this, ransomware remains the top threat to UK critical infrastructure, with supply chain attacks also increasing. As the UK transitions to net-zero emissions and expands nuclear energy, addressing these vulnerabilities is crucial for national security and energy resilience.

US

An increasing number of sophisticated cyberattacks targeting OT have been observed. In response, government agencies and private sector organizations are expanding efforts to improve cybersecurity practices, information sharing, and incident response capabilities for critical infrastructure.

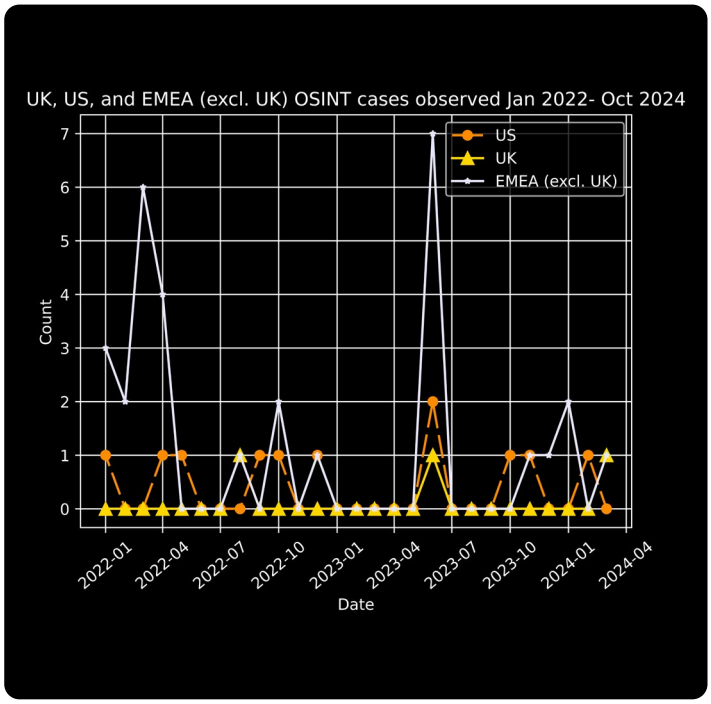


Figure 07: Selected OSINT articles per region between January 2022 and October 2024.

Attack Vectors

Rise in OT-attacks:

Various OT-specific malware was discovered during this research's time frame. In April 2024, Frosty Goop, the ninth OT specific malware, was discovered. This is the first OT malware to target the Modbus protocol, and may have been used in a cyber-attack against Ukrainian energy infrastructure [49].

COSMICENERGY was discovered, proposing to work similarly to Industroyer malware [50], and CHERNOVITE targets PLCs within SCADA and Field Device Management systems [51]. Despite being few in number, the observed rise in OT-malware during this period indicates the growing OT proficiency of threat actors.

Similarly, the OSINT data showed a rise in observed OT-targeted attacks. A disclosed Siemens Remote Terminal Unit vulnerability posed destabilizing the power grid and causing blackouts [52]. The 2017 attack of Russian Triton malware on Saudi Arabian petrochemical plant, for example, notably accessed Triconex safety controller models to be able to control safety instrumented systems [53]. If exploited, this could have caused multiple physical human impacts.

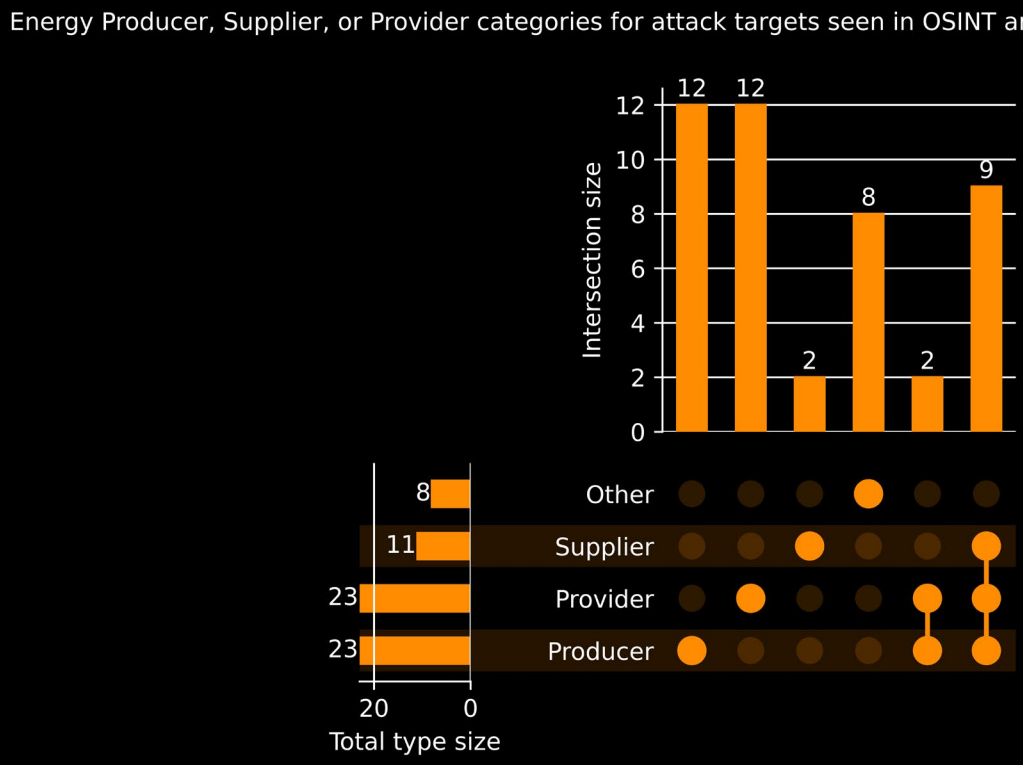


Figure 08: Function/s of energy sector attack targets observed in selected OSINT articles January 2022-December 2024.

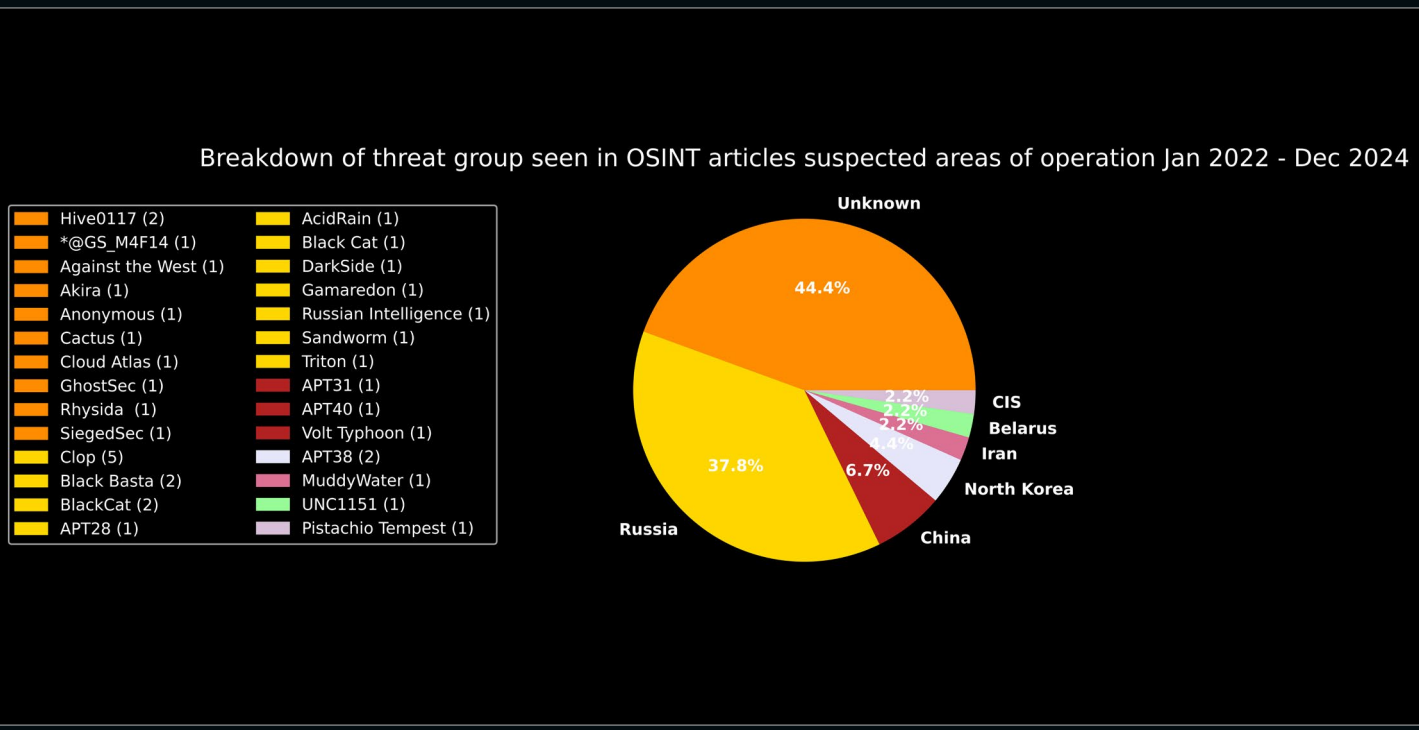


Figure 09: Threat groups involved in energy sector attacks in selected OSINT articles January 2022-December 2024, via suspected geographical area of operation.

Renewable energy producers:

Since 2022, there has been a definitive increase in attacks in EMEA on renewable energy producers and providers.

- Renewable energy companies and OT technology providers such as Honeywell and Schneider Electric were targeted in an espionage campaign thought to be linked to APT28 between 2019 and 2022 [55].
- In 2022, the European energy sector faced large-scale attacks. Notably, wind turbine manufacturer Enercon, was compromised when a misconfiguration on a VPN appliance was exploited to gain remote access to the Viasat KA-SAT satellite network, leading to over 5,800 wind turbines in Germany malfunctioning, impacting the output of 11 GW of energy [56]. This was later linked to a state-sponsored cyber-attack [57]. The renewable energy sector is becoming an increasing target for cyber-attacks, due to its likelihood and impact.
- **Likelihood:** As discussed in earlier sections, the move to net-zero has encouraged increased renewable energy infrastructure and adoption; a rise in physical assets, as observed with wind farms [58]. A drive to meet net-zero targets has also caused the increased adoption of technological advancements in the sector - namely IT/OT convergence and the increased ability to manage the electricity sources remotely along the supply chain. This increase in assets and technological convergence increases their attack surface and risk [59].
- **Impact:** As observed with the Wind turbine attack, the impacts of a cyber attack on electricity production and distribution are high. This becomes a strategic and attractive asset to attackers, incentivised by disruption [60].

Such an increase in attacks has led the Federal Bureau of Investigation (FBI) in July 2024, to warn private industry that expanding US renewable energy capacity increased the risk of cyber attacks [61].

Geopolitically driven attacks:

The high volume of EMEA compromises is likely due to geopolitical tensions during the timeframe. It is well documented that geopolitical tensions can lead to a rise in cyber-attacks and cyberwarfare from state-sponsored actors, APTs, and hacktivist groups. There is a rise in attacks on OT environments as means of targeting CNI and therefore threatening national security [62], often aiming to disrupt national services.

In this research's time period, 25% of EMEA articles analyzed discussed attacks in light of Russian-Ukraine war. Of these, multiple discussed hacktivist group attacks and Nation-state attacks targeting OT environments:

Hacktivist groups:

In September 2022, Israeli power providers' SCADA/OT systems were targeted, by hacktivist group GhostSec. 55 Berghof PLCs were compromised. Attackers exfiltrated data from the controllers and had access to control panels to alter chemical chlorine and pH levels, although this was not carried out [63].

In February 2022, hacktivist group 'Against the West' attacked Gazprom, and GhostSec targeted Booster control systems of the Russian Nuclotron-based Ion Collider facility [64].

Such groups increase attacks during times of geopolitical tension. In April 2024, UK's NCSC and US' CISA issued a warning about cyber threat from pro-Russias hacktivist threat actors targeting CNI [65]. These groups are thought to be acting on their own accord, on ideological grounds; pro-Russian hacktivists have publicly stated their intensions to deploy attacks on CNI since the Russian invasion of Ukraine in 2022 [66].

Nation-states specifically targeting disruption of OT environments:

In April 2022, electrical substations in Ukraine were targeted by Sandworm (Russian General Staff of the Armed Forces of the Russian Federation (GRU). The IT IEC-104 protocol was targeted which interacts with electrical utility equipment to send power flow commands to substation devices. Industroyer2 and CaddyWiper malware were used to propagate to the OT environment [67]. Although this attack was unsuccessful, a blackout could have impacted 2 million people. This follows the original Industroyer variant that was used in 2016 to compromise Ukrainian power grids, causing a portion of Kyiv to lose power for over an hour [67].

In 2023, Ukraine's CERT intercepted APT28 on a Ukrainian critical energy infrastructure facility. The initial attack vector was a phishing email and used living-off-the-land (LOTL) techniques to persist in the network [68].

UK Findings

In the UK, fewer compromises were noted, with only three within the analysis period.

Interconnected operations:

In August 2023, an attack on Australian company EnergyOne Australian affected UK corporate systems operations, highlighting the global impact an attack can have on interconnected departments around the world [69].

Increase in supply chain attacks:

Third parties were increasingly observed being targeted to impact the ultimate victim, echoing warnings that the US energy sector would be increasingly targeted by such attacks [70]. Supply chain attacks on the energy sector have been observed historically, via third-party software provider, such as the 2011 attack by the Dragonfly group on energy companies in Europe and North America [106].

However, Darktrace's OSINT analysis research showed a spike in supply chain attacks via third-party data stores; namely APT ransomware group Clop utilizing MOVEit file transfer tool zero-day vulnerability to deploy ransomware and exfiltrate data from energy sector targets. OSINT examples include:

- CNI water provider South Staffordshire Plc was affected in this way by Clop, leading to internal credentials being leaked, claims of access to OT workstations, and 5 TB of data being exfiltrated [71].
- UK Oil and Gas firm Shell was affected twice by Clop in 2021 and 2023 via MOVEit and Accellion File Transfer Appliance vulnerabilities [72]. Clop also deployed supply chain attacks on Schneider Electric and Siemens Energy in EMEA and US Energy departments in May-June 2023 [73].

US Findings

Physical attacks:

Attacks causing physical implications on the US energy sector have been well documented, spiking following the Colonial pipeline attack in May 2021 where DarkSide targeted the Billing and Accounting department, impacting a five-day pipeline outage and eventual East Coast fuel shortage [46].

However, there has also been an increase in physical attacks themselves on the power grid where the aim is destruction, as of 2022, such as shooting of North Carolina electric substations belonging to Duke Energy Corporation [74].

Nation-state attacks:

APT groups continue to exploit cyber posture and vulnerabilities to attack the sector, supporting Darktrace's observations.

- Lazarus group (North Korea-sponsored APT) affected energy companies across US, Canada and Japan by exploiting the Log4j vulnerability (CVE-2021-44228) on internet exposed VMware Horizon and Unified Access Gateway servers. Custom malware such as 'VSingle', 'YamaBot', and 'MagicRAT' was implanted, C2 established, and proprietary data exfiltrated to North Korea [75].
- The People's Republic of China has been targeting the US energy sector since at least 2011 with the US government providing multiple public advisories and numerous legal indictments. The US government assessed that these threat actors were "targeting U.S. pipeline infrastructure for the purpose of holding U.S. pipeline infrastructure at risk". The "U.S. Government identified and tracked 23 U.S. natural gas pipeline operators targeted from 2011 to 2013 in this spearphishing and intrusion campaign. Of the known targeted entities, 13 were confirmed compromises, 3 were near misses, and 7 had an unknown depth of intrusion." [103].
- More recently, in November 2023, it became apparent that Chinese APT group VoltTyhpoon had conducted a prolonged attack since February 2023 against a US power utility in Massachusetts. Here, the group conducted lateral movement over SMB and RDP to exfiltrate sensitive data regarding its operational technology (OT) infrastructure and energy grid operations, with intent to propagate from the IT network to OT environment to control its physical functions [107] [108].
- Akira ransomware group attacked BHI Energy in June 2023, using stolen VPN credentials for a third-party contractor to access the VPN without MFA, scan the network, encrypt files and exfiltrate PII data [76].
- Potentially new state-sponsored groups formed during the time frame of this research.
  - In May 2024, High Society, was formed, in alliance with Cyber Army of Russia. They publicised their intentions to target US energy entities; including the Nuclear Energy Institute (NEI) and the Electric Power Research Institute (EPRI) [77].
  - Cyber Army has historically targeted US and European utilities via targeting of HMIs. Such collaboration signals increased efforts to disrupt the energy sector. This could be state sponsored to pursue strategic objectives by jeopardising nations' energy security [77].

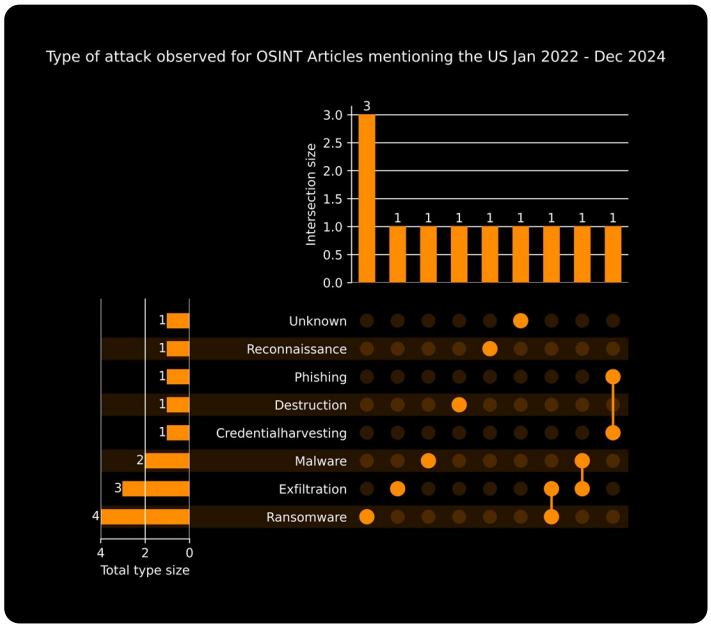


Figure 10: Attack types observed in US incidents in selected OSINT articles January 2022-December 2024.

Threat Profile Spotlight

APT28

APT28 is a Russian state-sponsored APT group, widely believed to have been active since the mid-2000s. Associated with GRU Unit 26165 85th Main Special Service Centre (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [78]. This attribution is mainly based on an indictment unsealed by the US Department of Justice (DoJ) in 2018 [79].

According to public estimates, the GRU consists of around 12,000 people [79], so those indicted likely only represent a fraction of APT28's force structure. As one of the service's main cyber groups, APT28 may also draw on personnel resources of the 6th Directorate, the GRU signal and electronic intelligence division. APT28 has used a wide range of tools, including tailored malware. for Mac OS X, Linux, iOS, and Android. The group also has frequently used zero-day exploits alongside other techniques such as spear-phishing.

Regional Focus

UK: From Darktrace's own investigations, APT28 indicators were seen more frequently across the Europe region than any other and the UK was the third within Europe. Tor exit nodes and APT28 hostnames were the most common indicators amongst the UK organizations. APT28 targets organizations that align with Russian interests, primarily government and defense-related targets. These targets can be espionage and information gathering related, as seen in attacks against Polish and Ukrainian governments, but the group has also been targeting energy infrastructure in Ukraine [80].

The group was also responsible for a false-flag attack against French TV station TV5 Monde in 2015, which included disrupting and defacing the broadcast [81].

US: Malicious endpoints used by APT28 and other possible IoCs were still observed by the Darktrace Threat Research team in their US investigations. While another attacker could abuse residual tools, it could also be indicative APT28 is still active, and organizations should be prepared for them. APT28 has a history of attempting to disrupt elections both in the US and the UK. Seen in the UK in 2018 and 2019, and very prominently in the 2016 US presidential election when the group was involved in the breach and release of sensitive material from the US Democratic National Committee and the World Anti-Doping Agency in 2015-2016 [82]. Since these events gained a lot of publicity, the APT repressed its activity, moving towards more covert operations.

Energy Focus

Darktrace assesses that APT28 will likely continue to support Russian strategic interests and as such organizations or governments that are opposed to those interests are at risk. APT28 has attacked multiple Ukrainian energy-related entities, ranging from companies experiencing unplanned outages to deploying malware that targets power grids.

Volt Typhoon

Volt Typhoon is a Chinese state-sponsored APT group. Volt Typhoon's botnet, the KV Botnet, is mainly comprised of infected SOHO devices [83].

As Volt Typhoon has only been known to be active since 2021 [84], knowledge of their internal operations is limited. Volt Typhoon prepares for attacks by researching the target organization, gathering information that will allow them to understand how to surreptitiously remain within the network. They combine this with LOTL techniques to remain undetected [83].

They often use zero-days, believed to have been discovered from a research community centred around educational establishments in Chengdu and the Sichuan province, and then shared with entities associated with the Chinese government, including Volt Typhoon [85].

Based on the lateral movement, and the CNI organizations targeted, it is believed that Volt Typhoon's aim is to remain in the network unnoticed for years, prepositioning themselves to move laterally into the OT networks. Then, when they may wish to cause real-world disruption or damage, they are in a position to do so [83].

Regional Focus

UK: Volt Typhoon's main target is believed to be the US and allies such as the UK may also be targeted. However, based on Darktrace's research and threat hunt there was no evidence of Volt Typhoon compromising the UK customer base or that it heavily targets UK-based devices for the KV Botnet.

US: US Federal organizations including CISA, National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) confirmed that Volt Typhoon has compromised the IT environments of multiple CNI organizations predominantly in communications, energy, transportation systems, and water and wastewater systems sectors [83].

The US was also a target for the KV Botnet. The US was successfully able to disrupt the botnet in January and February 2024, however, the effects appear to only have been temporary [86]. Based on Darktrace's research, there were a number of US-based devices likely compromised by the KV-Botnet malware. However, evidence was limited to be able to attribute any activity to Volt Typhoon within the US customer base.

Energy Focus

As a CNI, the energy sector is a prime target for Volt Typhoon, and in February 2024 the US Department of Energy (DoE) co-signed the advisory released by CISA demonstrating the threat Volt Typhoon poses to the Energy sector [83].

Threat Hunts

Hypotheses

The Darktrace observed incidents, OSINT findings, and APT spotlights informed hypotheses-driven threat hunts across energy sector customer base.

The hypotheses crafted and tested were:

01 Hypothesis 1: Volt Typhoon will target energy sector providers, using their KV-Botnet to compromise SOHO router devices, and move laterally to achieve their end goal of accessing OT environments.

Volt Typhoon will be more prevalent in suppliers and providers rather than producers. Initial access may be seen from various internet-facing systems, specifically Fortinet FortiGate devices. Connections will be received from compromised SOHO devices, mostly manufactured by ASUS, Cisco, D-Link, NETGEAR, and Zyxel, as these allow the owner to expose HTTP or SSH management interfaces to the internet.

Lateral movement will be seen via PsExec, PowerShell/WMI, and RDP. Target devices would include file servers, domain controllers, and OMSs. However, the end goal will likely be a VMware vCenter or equivalent virtual centers, as this allows for access into the OT environment. The access would likely be via SSH, Telnet, or other protocols supported by PuTTY.

02 Hypothesis 2: APT28 will target the energy sector, via spear-phishing campaigns and abuse Ivanti Connect Secure VPN to perform remote arbitrary code and malware execution.

APT28 will continue to target government, energy, and defense-related entities with aims to cause disruption, gather intelligence, and spread disinformation. These attacks will likely be politically motivated and distributed via spear-phishing campaigns that are sent with malicious Outlook notes and tasks.

The attacks typically abuse a vulnerability in Ivanti Connect Secure VPN to perform remote arbitrary code execution. Once established, APT28, a highly resourceful group, will use tailored malware and zero-day exploits to carry out their attacks.

03 Hypothesis 3: Exploitation of internet facing HMIs and PLCs to C2 externally and establish persistence.

Attackers will target internet-facing PLCs and remote HMIs at energy companies in western democracies around the world. They will gain initial access via default or brute-forced credentials. Next, they will use insecure protocols such as MODBUS and DNP3 to establish persistence on the network.

Destination devices could include circuit breakers, electricity generation devices, and electricity transfer devices. Finally, the attackers will cause an outage or disruption on the power grid, substation, or critical energy infrastructure at a politically opportune moment.

04 Hypothesis 4: Utilization of PerfectData software and MFA bypass to compromise user accounts and destruct data.

Attackers will launch phishing campaigns to harvest credentials of M365 accounts to gain initial access via compromised user accounts. Using the compromised account, attackers will edit authentication methods and/or use software, such as PerfectData, to exfiltrate whole mailboxes as PST files.

They will establish new email rules with the intention to obfuscate their activity, compromise further user accounts, exfiltrate sensitive data, and destruct data.

Based on the research, the Darktrace research team made predictions on the likelihood of the threat hunt findings aligning with them.

The team queried the hypotheses using an LLM to observe if they matched open-source data of the energy threat landscape. As explained in the methodology section, experimental models looking for IoCs associated with the hypotheses were created and executed in test mode, to assess whether findings from the energy customer base supported the hypotheses.

This process, in addition to the findings, are explored in the table and below.

	Darktrace predictions	Does LLM prediction agree with hypothesis?	Experimental model	Outcome
Hypothesis 1	ASUS devices will be targeted, like routers. KV Botnet will be used. Providers are more likely to be targeted.	**Yes**	**KV Botnet Indicator** Detects potential KV-Botnet devices. Looks for a device (typically SOHO devices) making connections to the IoC IPs.	There was little evidence of Volt Typhoon in the customer set.
Hypothesis 2	Tor exit nodes will be abused, in line with historical attacks.	**Yes**	**Suspicious HTTP Indicators** Detects IoCs observed in previous APT28 attacks. IPs and URI commands that could be signs that a vulnerability in Ivanti Connect Secure VPN was being used. Model hits analyzed in conjunction with email environments for evidence of APT28 using spear-phishing tactics.	Energy sector devices had connected to APT28 IoCs, but no further signs of compromise via email or Ivanti Secure Connect VPN vulnerability.
Hypothesis 3	OT devices will be internet-facing in small-to-midsize organizations with bad segmentation, followed by engaging with anomalous external connectivity.	**Yes**	**Internet-Facing HMI/PLC Device** Detects internet facing OT devices, or devices using OT protocols (namely HMI or PLC devices). Model hits were analyzed to see if internet facing OT devices then made or received connections to or from external endpoints.	Although internet facing OT devices were observed in energy sector, investigation revealed little evidence to support Darktrace's hypothesis that following this detection, the devices engaged in external C2 connections.
Hypothesis 4	Phishing emails will be used as initial attack vector to compromise account credentials. Software (PerfectData), or MFA bypass, will be used for persistence in further attack.	**Yes**	**PerfectData Software Activity** Detects a SaaS user performing activity relating to 'PerfectData Software'. Model hits were analyzed in conjunction with existing SaaS and Email models that would indicate multi-stage attack in line with the hypothesis.	The evidence supports this hypothesis. PerfectData Software is being used in SaaS-Email attacks on energy sector companies to enable access to and exfiltration of mailbox data, as well as registering authentication apps to bypass MFA.

Threat Hunt Findings

Hypothesis 1

Outcome

Low fidelity Volt Typhoon IoCs were observed across energy sector base, including KV-Botnet IoCs on networking gear (routers) and ASUS devices, file hashes and user agents, but no further evidence was found to confirm definite presence.

Interesting Findings

Darktrace found a number of devices likely infected with KV-Botnet malware. Observed device vendors included ASUS, with device types such as desktops, laptops, and routers, supporting the hypothesis that SOHO devices may be compromised to gain initial access.

- The KV botnet appears to be distributed across various countries, with an emphasis on the US, which could align with the distribution of the Darktrace customer base.
- There was a trend towards IoT vendors, with an example being Advantech.
- Further deep dives did not show any significant signs of Volt Typhoon across the energy customer base. This does not provide any further evidence to prove or disprove the hypothesis.
- Two devices investigated were observed potentially moving laterally via admin RDP, CertUtil, or WinRM, and were also targeting servers and DNS servers, but this is a low fidelity association with Volt Typhoon.

Hypothesis 2

Outcome

Energy sector devices had connected to low fidelity APT28 IoCs, specifically Tor exit nodes, as historically observed by this APT. No further signs of compromise via email or Ivanti Secure Connect VPN vulnerability.

Interesting Findings

- The results found that IP addresses and hostnames used by APT28 are still being observed. Just under 1% of model hit rates were seen from the energy sector.
- The history of APT28 suggests they adapt to evade detection and are likely using new zero-day vulnerabilities.
- Tor exit nodes still appear to be abused and were the most frequently seen indicators from Darktrace's findings. IP 185.220.100[.]253 was seen in nearly 40% of the results.

Device Types Observed

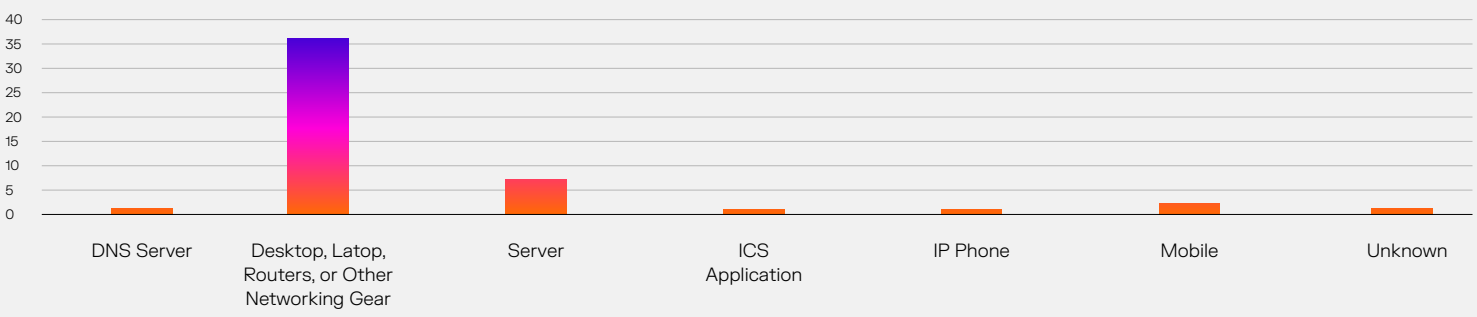


Figure 11: Device Types that triggered experimental model: 'KV Botnet Indicator'.

Hypothesis 3

Outcome

Internet-facing PLCs are prevalent in the energy sector. Little evidence was found that this risk is being exploited to C2 externally.

Interesting Findings

Energy was the top customer sector where internet facing OT devices were observed.

- The highest number of internet-facing OT devices (HMIs and PLCs) were found to be in the energy sector, ahead of manufacturing, construction and other sectors.
- Within energy sector customers, Darktrace only observed one instance of an external connectivity attempt from an internet-facing OT device after the model alert, which was found to be legitimate Rocky Linux activity.

Hypothesis 4

Outcome

PerfectData experimental model hits were found in the energy sector, including a Saudi Arabian oil and gas investor. Upon investigation across the customer base, PerfectData software and MFA bypass are being used to compromise user accounts and destruct data, and in one case facilitated exfiltration of sensitive industrial machine data, demonstrating intent to conduct an OT attack.

Interesting Findings

In four energy sector cases, findings aligned with the hypothesis' multistage attack:

- Unusual logins (often from PIA VPN or anonymization network infrastructure).
- The user consented/granted OAuth permissions to the PerfectData application.
- The user then accessed mail items, created a new email rule to obfuscate activity, sent outbound emails, and deleted or downloaded mass emails.

Other findings included:

- Compromised users also registered the Authenticator App with Notification and Code before setting up a new email rule, indicating a method to bypass MFA.
- Prior to granting permissions to PerfectData Software, the user granted permissions and consented to another application, eM Client. This was also observed in other email compromises in the sector.

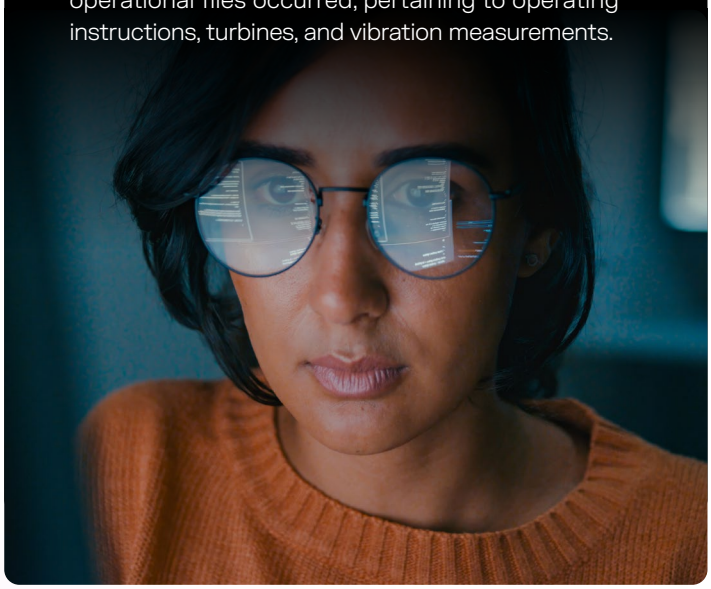
Finding Focus

As part of the threat hunt, Darktrace researchers found that in June 2024, a renewable energy infrastructure provider was affected by a PerfectData Software attack, and demonstrated intent to conduct an OT attack.

A user logged into Azure AD from a rare US IP address. Consent was granted to eM Client from the same IP. Shortly after, AddServicePrincipal via Azure was granted to PERFECTDATA SOFTWARE. Two days later, a new email rule was created from a London IP to move emails to an RSS Feed Folder, stop processing rules, and mark emails as read.

Mail items in the \Sent folder were then accessed from a malicious IP belonging to PIA VPN. Mass email deletions then took place, deleting multiple instances of emails with the same name from the \Sent folder, indicating an email containing a file storage link: [Name] shared "[Company Name] Proposal" With You. This represents an attempt to obfuscate a potential outbound phishing email campaign. A month later, the same user was observed downloading mass mLog csv files (used by Mahlo devices).

This could be proprietary and operational technology-related information. In September, three months after the initial attack, another mass download of operational files occurred, pertaining to operating instructions, turbines, and vibration measurements.



Discussion and Implications

Interviews

Findings from the threat hunts and from the research overall were posited to key UK and US energy sector stakeholders in eight interviews.

AI adoption in energy sector

When asked whether the energy sector utilizes AI, stakeholders agreed that AI was "everywhere" within the sector and CNI in general. They have been using AI, particularly on the operations side, for around 20 years, but it has only recently started to be called as such. More basic adoption included using CoPilot to speed up processes, assist employees with business correspondence, and improve customer service.

More energy operation examples provided included Le Caleya wind farm using AI to optimize the running of turbines in response to external factors. Stakeholders also discussed their AI usage within cybersecurity, such as building models to decode malware, but this was proving difficult. They also posited logical applications of AI, helping to reveal visibility gaps in their estate, and a consumer power plant model, where consumers use AI to optimize their supply and sell it back to the grid or switch their heat pump on during optimal times.

However, the sector is not yet AI-driven, and stakeholders considered numerous factors as to why:

- **Readiness.** EDF UK stakeholders commented that despite a desire from stakeholders towards becoming AI-driven, but they are "not an AI ready company" yet, due to having incomplete datasets, where data is not labelled or cleaned to feed the AI to produce actionable outputs. "We need to improve our data before we can move to AI".
- **Regulation.** According to the RUSI stakeholders, larger-scale AI adoption in the sector, such as using AI to manage and predict frequency on the grid, is currently unlikely and would not be allowed on an operator basis, unless worked on in collaboration with Ofgem.
- **Cyber security risks.** EDF UK stakeholders expressed usage of public AI models such as ChatGPT is restricted in more critical energy units, due to sensitive data being shared with the third party and used to retrain models. In response, the software engineering team is working with the cyber team to build an in-house AI tool using LLM and Retrieval-Augmented Generation (RAG) models to assist with work, without risking third parties accessing the data or leaving their own tenant.

Risks of tech transformation and AI in the energy sector

Stakeholders agreed that technological transformation in the sector is creating more cyber risks:

- **IT/OT convergence.** A Darktrace OT SME pointed to IT/OT convergence taking place in the sector. Closer proximity to OT network is always a risk, as any attacks on the OT network could cause high-impact physical disruption. Multiple vendors suggested the increased interconnectedness makes air gapping or 'islanding' operations more difficult when responding to cyber incidents.
- **IoT.** The increased adoption of IoT devices has increased initial attack vectors and entry points. Smart meters could be used to propagate botnets or could be used to target cellular nodes to switch all meters off and cause a potential blackout.
- **Net-zero.** According to the think tank, the shift towards net-zero in the energy sector has led to more control automation in non-dispatchable solar and wind sectors, which cannot be turned on or off to meet energy demands, compared to dispatchable sources such as coal or natural gas. Increased control automation increases the attack surface of these energy sources. However, these renewable power sources have more in-built resiliency and can cope more easily with fluctuating patterns. Redundancy is already built into the UK oil and gas sectors where excess generation is accounted for in case of an attack or shutdown, but the non-dispatchable nature of renewable energy means it is more resilient to such changes in case of an attack.

> "We're not an AI ready company... We need to improve our data before we can move to AI".
>
> - **Stakeholder, EDF UK**

Stakeholders also agreed that AI could create more risks and change the threat landscape:

- **Training.** It is thought that AI adoption within the sector can create more risks if usage is not accompanied by sufficient training. EDF UK stakeholders indicated that prompt engineering training is needed to ensure that sensitive data is not disclosed when training models.
- **Conceived AI-driven attacks.** AI adoption by attackers could change the modus operandi, scale and speed of attacks targeting the sector, potentially causing more damage. Mark Bristow, MITRE, explained that as AI allows for easier scaling, it could theoretically be used by adversaries to train language models to conduct reconnaissance and targeting methodologies on a larger scale. EDF UK has undertaken training about how AI could be used to power malware, and considered how Nation-states could use AI to train on attack data and generate successful attack paths.

"Nation states could use AI to train on attack data and generate successful attack paths".

- James Sutton, EDF UK

Future Threat Landscape

AI-driven attacks

As discussed in earlier sections, AI-driven attacks are feasible, from AI phishing campaigns to executing ransomware.

Although both Darktrace and interviewed stakeholders have not yet identified any AI-driven attacks in the sector, this could quickly change. EDF UK stakeholders mentioned that they had not found any evidence that threat actors were using AI against them.

Mark Bristow, from MITRE, which has mapped TTPs across AI systems, stated that whilst "there are stories of AI going to take down the power grid, under a cursory review it looks plausible on the surface but a lot of the time they're not technically astute... I don't think we're there yet in any stretch of the imagination; we're a long way off".

Additionally, the consensus is that AI-driven attacks could change the scale of the attacks and, therefore, the countermeasures needed to respond, more than their nature.

"I don't think we're there yet in any stretch of the imagination; we're a long way off"

- Mark Bristow, MITRE

A stakeholder mentioned "AI can be a human augmenter, but I've not seen AI replace a human targeter".

Even on scale and efficiency terms, this stakeholder stressed that right now, AI is not portable enough, as the same model cannot be taken and plugged into different environments. This echoes a recent Bridewell report stating that AI-driven attacks have not yet surfaced in the wild. Criminals are currently in a proof-of-concept phase, but no AI techniques are as effective as conventional TTPs [87].

Non-AI-Driven Attacks

When stakeholders were asked what the top cyber threats and risks were, AI was not explicitly named. Top attack threats to the sector included:

Less Complex TTPs

Interestingly, for many stakeholders, less complex, known attack vectors are still their main concern. RUSI commented "There is a risk to overfocus on sophisticated attacks... these shouldn't be downplayed and we should keep up with new attack vectors, but relatively simple attacks can also cause significant damage." Mark Bristow, MITRE, captured this sentiment, stating, "There are no bonus points for a cool hack. Adversaries and Nation-states have bosses and spreadsheets like every other business. If the easy stuff works, they're going to use it, and these will continue to be prevalent."

Example TTPs or attack vectors mentioned by stakeholders included:

- **LOTL + Edge devices.** Stakeholders mentioned living off the land techniques are being used to capture credentials and targeting of edge devices such as Citrix and Fortinet.
- **Phishing.** A Darktrace OT SME mentioned that spear-phishing is still a well-used attack vector in the sector.
  - **Whaling.** EDF UK noted that phishing is the number one threat they're seeing, with attackers targeting the senior leadership team via whaling.
  - **Identity and Access Management (IAM).** A stakeholder mentioned that attackers are using phishing to target IAM and to steal identity tokens, which can have a huge impact.
  - **Training.** For EDF UK, this threat has led to a large security awareness effort within the company to "change the culture of user behavior which can circumvent security controls". They are teaching users about the creativity of phishing emails, simulating attacks in users' inboxes, and monitoring repeat clickers and weaknesses in alerting suspicious emails.

"There are no bonus points for a cool hack...If the easy stuff works, they [nation states] are going to use it".

- Mark Bristow, MITRE

"On our Cyber Ops calls, phishing is the number one thing we're seeing".

- **Siobhan Waldron, EDF UK**

"Users are not the first line of defense, and if they are, we have failed the community, not the other way around."

- **Mark Bristow, MITRE**

Mark Bristow, MITRE, views phishing still being such a large problem as a failure of the cybersecurity community, rather than individual users. "Users are not the first line of defense, and if they are, we have failed the community, not the other way around."

He stressed that the cybersecurity community needs to come up with solutions to make phishing training no longer relevant and to push attackers off this technique.

Nation-State Attacks

Stakeholders discussed the likelihood of Nation-states attacking the energy sector. The UK think tank mentioned that Office of Gas and Electricity Markets (Ofgem) and Department for Energy Security and Net Zero (DESNZ) recently stated Nation-state threats as a direct concern to the sector.

The NCSC has also noted the increase in sophisticated attacks targeting UK CNI. Such attacks include:

APT Groups.

- Darktrace OT SMEs informed that the Canadian government has recently warned the power sector about Russia and China APT groups prepositioning and conducting reconnaissance on the grid.
- A threat intelligence cybersecurity provider shared that Russia's APT BlueAlpha recently conducted reconnaissance on a UK CNI provider by using Cloudflare tunnels to obfuscate and deploy GammaDrop malware to establish persistence.

Geopolitically- driven Nation-state attacks.

- A stakeholder reflected on cyberattacks in Ukraine, such as 2016 Industroyer attack on electric systems, and more recently, where cyber is being targeted to drive military objectives.
- However, they also mentioned that there have been fewer attacks with observable impacts recently, compared to those observed in 2012-2021. Adversaries arguably develop such attacks as a strategic capability more than a tactical one, so do not reveal these unless launching such attacks for intent only.

Upstream attacks

- Stakeholders discussed upstream attacks on generation assets as the bigger opportunity targets, compared to elsewhere in the energy supply chain.
- These attacks are harder to achieve as operations are usually site specific. Few public cases of attacks on generation assets have been observed.
- Actual attacks are therefore hitting providers and suppliers more, with real attacks occurring on transmission and distribution parts of the grid.

Lack of Resources

Stakeholders discussed current resource gaps and limitations, putting the energy sector at risk as companies are reactive to incidents, rather than proactive in preventing them.

Cyber skills gap. Both US and UK stakeholders acknowledged a skills gap in cyber within the sector.

- A US stakeholder mentioned this is exacerbated by "greyout" in US public and private energy sector, where people who understand legacy systems and power grid operations are now retiring, leading to a loss of knowledge within the US sector. This includes how to revert to manual operations without using control systems, if needed. The stakeholder was concerned that operational plans to survive on limited capacity are diminishing.
- In addition, knowledge transfer to new staff is inhibited as there are few requirements to document such plans or how operations are configured. Pia Hüsch, RUSI stressed that this skills shortage is also felt at the regulatory level; there are not enough people on the ground to implement regulations, despite there being vacancies.

Lack of collaboration. Multiple stakeholders mentioned collaboration lacks within energy companies and across the sector.

- EDF UK mentioned that communication lacks within the company, and configuration of business-wide controls is difficult due to different risks and policies across business units.
- They also noted a lack of collaboration across the sector; they are not currently part of an energy Information Sharing and Analysis Center (ISAC), making it difficult to share threat intelligence, incident response plans, and lessons learned across the sector. This echoes calls for a UK energy ISAC discussed earlier [17].

According to a US stakeholder, different parts of the US energy supply chain do not collaborate as there are economic incentives not to.

"Ofgem and DESNZ recently stated nation state threats as a direct concern to the sector".

- **UK Think Tank**

Over-dependency

Over-dependency is a historic problem faced by the energy sector, which continues to emerge in new ways.

- **Historic dependencies.** There is over-dependency on few vendors and systems, at the expense of a diverse ecosystem.
  - This increases the risk within the sector if one of these major vendors is targeted. As raised by RUSI, "Key software systems are controlled by a handful of companies, which introduces risk as supplier diversity is key".
  - Another stakeholder mentioned that co-dependency means attackers are positioning to hold all of CNI at risk. They criticized CNI for not thinking systematically about how things would run operationally if large players were targeted.
  - This was observed in 2012 when Telvent's SCADA remote administration tool was targeted by the Chinese hacking group Comment Group. Telvent managed more than 60% of hydrocarbon movements in American pipelines. Compromising one vendor could have given access to energy infrastructure and crippled global operations [88].
  - This risk has persisted. In the 2017 Colonial Pipeline attack, dependency on one pipeline and perceived dependency leading to panic buying caused a fuel shortage on the East Coast [46].
- **Emerging dependencies.** This dependency continues to evolve in new ways. A US stakeholder warned of dependencies forming as energy operations move to the cloud.
  - Energy industry executives are starting to consider hosting OT devices such as HMIs and very small aperture terminals (VSATs) in the cloud, as well as their discrete logic control systems and 5G communications. "The risk is ending up with assets screwed to the ethernet convertors and plugged to the cloud... we're not there yet, but industry is moving this way".
  - This introduces a new type of dependency on cloud environments which may not be effectively secure, thereby increasing risk within the sector, as "before a plant could work without anyone else, but now cannot operate without the cloud or communications providers, so from an adversary perspective, if cloud providers are attacked and go down, then plants are impacted and their business".

Supply chains, lack of visibility

Although such dependency exists, further downstream risks are also arising from tangled supply chains.

- **Risks of outsourcing.** The UK energy supplier explained that operations are outsourced to other suppliers, who select and use their own software.
  - If this is not analyzed when entering into business with the company, it could have disastrous impacts, as seen with the SolarWinds attack. The energy supplier is responsible for checking and securing their third-party tools.
- **Lack of visibility.** This complicated supply chain contributes to a lack of visibility regarding what assets a company has, which party is responsible, and their overall cyber posture, making it difficult to manage.
  - The UK energy supplier admitted they do not have complete visibility over their weak spots or darker corners of their environment, and "attackers could uncover things we don't know."
  - Another stakeholder echoed the difficulty, stating that this outsourcing leads to a "complicated web of supply chain which is unmanageable from a security perspective."
  - This difficulty in mapping assets and supply chains is impacting the sector. "The tangled trust weave of supply chain is unpackable and difficult to resolve, so market economies like insurance are exiting the market as they cannot price the premiums... this should be a warning sign to the industry."

"Key software systems are controlled by a handful of companies, which introduces risk as supplier diversity is key".

- Dan Marks, RUSI

"Co-dependency means attackers are positioning to hold all of CNI at risk".

- Mark Bristow, MITRE

"Attackers could uncover things we don't know".

- James Sutton, EDF UK

AI and Cyber Defense

Currently, it is perceived that cyber defences in the sector and CNI are not keeping pace with threats. As quoted by Pia Hüsch, RUSI, the former CEO of NCSC, Ciaran Martin, has said the energy sector has "bad security but good safety measures".

Given the opportunities and risks presented by AI within the energy sector, it is crucial that AI is also used within the sector's cyber defenses and capabilities [89]. AI can be used in cyber defences to detect unknown attacks at machine speed, ensuring organisations are resilient and able to detect and respond to attacks; AI-enabled or otherwise.

At its core, Darktrace's approach applies AI to detect and to respond to anomalies within an organisation's environment, including IT, OT and email. Newer products allow critical attack paths to be mapped and evaluated, and provides an overview of infrastructure and assets to be managed; integral to supply chain monitoring and management.

Policy implications

The ever-changing threat landscape for CNI and energy sector is being reflected in policy and regulation. Findings from the OSINT research and stakeholders interviews shed insight on these changes and their implications.

These include existing general regulations that apply to certain energy sector organizations, energy sector specific cybersecurity initiatives, and relevant upcoming policy.

UK Policy Landscape

The UK is continuing to strengthen cyber security regulation for its essential CNI services, including in the energy sector.

Type	Policy	Requirement/Details
General	**NIS Regulations**	▪ In 2018, the UK transposed the NIS Directive, designed to boost the security (cyber and physical resilience) of network and information systems ▪ As many Energy Delivery Systems (EDS) operators are designated as Operators of Essential Services (OES), they had to comply with NIS' requirements ▪ The NIS Regulators, such as The Office of Communications (Ofcom), set cyber security compliance requirements against NIS, drawing from the NCSC's guidance

	NCSC's Cyber Assessment Framework (CAF)	▪ Provides a framework to help organizations assess their cybersecurity posture and identify areas for improvement
		▪ This is broken up into 4 Objectives and Principles within them, from managing cyber risk (including crucial sections on Risk Management, Asset Management and Supply Chain) through to incident response and recovery planning
		▪ The CAF is used as a basis for regulatory compliance requirements
		▪ **Such emphasis on risk management in the energy sector reflects in EMEA more widely:**
		  ▪ The EU launched the EU Network Code on Cybersecurity for the Electricity Sector (C/2024/1383) in March 2024
		  ▪ This demands electricity providers and their suppliers to conduct a risk assessment every three years to identify and manage cyber risks, increasing cyber and supply chain security [90]

Energy specific	**ENA Energy Delivery Systems – Cyber Security Procurement Guidance (EDS – CSPG)**	▪ A set of guidelines to help energy sector organizations manage cybersecurity risks associated with their procurement processes ▪ It was created through collaboration between the Department for Business, Energy and Industrial Strategy (BEIS), the Energy Networks Association (ENA), vendors, and operators to ensure a baseline level of cybersecurity for products and services used within EDS ▪ This also focuses on asset management, critical assets and system dependencies as a requirement for third-party supply chain management
	The 2022 Civil Nuclear Cyber Security Strategy	▪ Sets out goals to secure the UK's civil nuclear CNI ▪ Targeted completion date is 2026, which has been criticized for leaving gaps in cybersecurity in this sector until then [91]

	Civil nuclear regulation	▪ **Regulation relevant to the cyber security of the civil nuclear sector includes:**
		  ▪ Radiation (Emergency Preparedness and Public Information) Regulations (2019)
		  ▪ Nuclear Safeguards Act (2018)
		  ▪ Nuclear Industries Security Regulations (2003)
		  ▪ The Civil Contingencies Act (2004)
		  ▪ Nuclear Installations Act (1966)
		▪ The nuclear safety, security and safeguards laws and regulations are enforced by the sector's independent regulator, the Office for Nuclear Regulation (ONR), working with the Environment Agency, Department for Transport, and the Information Commissioner's Office, amongst others

Upcoming	**Cyber Security and Resilience Bill**	▪ The King's Speech in 2024 introduced a Cyber Security and Resilience Bill aimed at strengthening the country's defenses against cyber threats and enhancing the resilience of critical infrastructure
		▪ **The Bill will:**
		  ▪ Expand the remit of the regulation to protect more digital services and supply chains
		  ▪ Put regulators on a stronger footing by enhancing their investigation powers
		  ▪ Mandate increased incident reporting to give government better data on cyber-attacks

US Policy Landscape

The Biden Administration saw an increased focus and commitment to national cybersecurity and CNI preparedness. Stakeholders are eager to see if this approach will change in Trump's administration, and whether it will be met with the same political will.

Type	Policy	Requirement/Details
General	**2021 Executive Order 14028 on Improving the Nation's Cybersecurity**	▪ This was a federal government policy focused on prevention, detection, assessment, and remediation of cyber incidents as key to national security [92] ▪ More specifically, this focused on incident response plans, sharing threat intelligence, and ensuring secure software supply chains
	2023 National Cyber Security Strategy	▪ Biden released the National Cyber Security Strategy, which has been endorsed by the National AI and Cybersecurity ISAO (NAIC-ISAO) ▪ It focuses on securing software supply chains and critical infrastructure, partially via international collaboration and investments into emerging technologies [93]
	NIST Cybersecurity Framework	▪ NIST SP-1800-23 - "Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry" [94]

Energy specific	**DoE Cybersecurity Strategy**	▪ The US takes a sectoral approach to governing CNI specifically. Energy is overseen by the DoE
		▪ The DoE published their Cybersecurity Strategy in January 2024 [95]
		  ▪ Internally, for DOE's own government-owned or operated OT/IOT, their Strategy's Goal 1.3 is to comply with CISA's BOD 23-01 Implementation Guidance for Improving Asset Visibility and Vulnerability Detection on Federal Networks [96]
		  ▪ This Binding Operational Directive (BOD) is the strongest language in Federal issuances toward asset management and visibility, applying only to Federal Civilian Executive Branch (FCEB) over which CISA has jurisdiction
		  ▪ Externally, for DOE's external role for private sector owned or operated OT/Critical Infrastructure, DOE plans to take across Goal 5, of the cybersecurity strategy

	Federal Energy Regulatory Commission (FERC)	▪ Regulates US's non-nuclear energy
	North American Electric Reliability Corporation (NERC)	▪ Regulates US bulk power/electricity
Upcoming	**White House OCND Energy Modernization Cybersecurity Implementation Plan**	▪ Outlines 32 initiatives to secure the energy ecosystem to be implemented by 2027 [97]

"It is hard to know what to classify [as AI] when making policies/regulations".

- **Pia Hüsch, RUSI**

Gaps and considerations for regulation and policy

Given the recent political priority given to boosting the UK's cyber resilience, and the opportunity presented by the Bill for the UK to become as cyber-secure as global peers, like the US, the following recommendations are made:

Implementing regulations in practice

Stakeholders warned that energy companies may struggle to implement new regulations. One noted that implementation capabilities depend on company size and resources. "Larger utilities can absorb the costs of expanding cybersecurity regulations and increased controls more easily than medium or smaller utilities, which have less financial margin and operational flexibility. Additionally, larger entities have more staff to implement these controls, while medium and smaller utilities have fewer personnel to manage the required tasks."

Updating regulation to account for AI

Regulation will need to be adapted to address the impact of AI usage and AI on cybersecurity.

- **AI adoption in energy sector.** As mentioned in an earlier section, AI has been utilized in the sector for over 20 years.
  - Stakeholders mentioned that regulation of AI usage in the sector could be difficult, due to ambiguity in defining it. RUSI mentioned that it is hard to know exactly what AI is widely thought to refer to, pre and post ChatGPT.
- **Impact of AI on cybersecurity.** To deliver the UK government's goals for the Cyber Security and Resilience Bill, and to meet NIS2's requirement of entities adopting 'state-of-the-art' cyber security measures, legislative frameworks in the UK will need to be updated to ensure that the UK's cyber security is not "comparatively more vulnerable" than the EU [98].
  - Given the proposed impact of AI on cybersecurity, it will be important for technical authorities globally to encourage the adoption of AI-enabled cyber defenses.
    - The CAF will need to be updated to require organisations to adopt state-of-the-art cyber defences to best prepare for and be resilient to advanced and AI-enabled attacks, should these come to fruition [99] [100]. This can be done through NCSC providing regular regulatory guidance on how to meet the requirement, raising the bar over time to ensure that defenders can manage increasingly sophisticated threats.
    - This also echoes in the US, where the DHS has called for CNI to be stress tested for resiliency against AI scenarios [101].
    - This will ensure that defenders are adequately equipped and able to respond to the evolving threat landscape.

Funding for industry innovation

Funding of innovation is required to realize the emerging opportunities and understand the risks associated with new technologies, as suggested by the upcoming UK Bill. This is being realized in the US. In 2024, the DoE recently granted USD 45 million funding of 16 projects developing tools and technologies to reduce cyber risks to energy infrastructure [102]. This includes Georgia Tech Research Corporation's development of "DerGuard", a framework utilizing AI techniques for automated vulnerability assessment, discovery, and mitigation in distributed energy resources (DER) devices.

In the UK, initiatives such as the National Cyber Security Programme and the Industrial Strategy Challenge Fund include significant investments in AI and cybersecurity technologies. The newly established ARIA, inspired by US Defense Advanced Research Projects Agency (DARPA), is funding high-risk, high-reward scientific research and innovation, which has a work stream looking at "future proofing our climate and weather". However, the scale and focus of these initiatives differ from the US' explicit focus on the energy sector.

No similar funding opportunities for UK energy sector were identified during this research. The UK energy supplier mentioned that although funding from the Department for Business, Energy & Industrial Strategy (BEIS) was discussed five years ago, nothing transpired, and they have not received funding from DESNZ more recently.

Focusing on Nation-state attacks

As seen in the OSINT and Darktrace incident analyses, CNI in general and in the energy sector is being increasingly targeted by Nation-state attacks. In the UK, the CAF does not target Nation-state attacks. It would be beneficial for regulatory guidance to be updated to prepare and respond to the threat to essential services posed by Nation-state and large-scale attacks.

This also requires more collaboration and less siloes across the energy sector as a whole. One interviewed stakeholder noted that wind sector Original Equipment Manufacturers (OEMs) do take cybersecurity seriously, but these efforts are siloed where borders cross and there seems to be little coordination or communication. Open threat intelligence sharing, tabletop exercises, and incident response scenarios would enhance cooperation, preparation, and response to such attacks.

Supply chain cyber security risk management and accounting for transition in supply chain and large players leaving the market

The EU's NIS2 Regulations have been updated to make clear that essential and important service providers in the energy sector must also assess and manage cyber security risks in their supply chain. In the UK, the Cyber Security and Resilience Bill should include this same clarification to ensure that the obligations currently included in NIS2 are consistently adopted across the sector. The energy sector could also take greater reassurance in the cyber security of its supply chain if the UK government followed through with its proposals to introduce security and resilience regulations for data centres.

"As the US is so widespread and made up of various large, medium, and small utilities, I would assume we see these [implementation] issues more in the US. Other countries, have fewer electric utilities, making the implementation of these controls across the board more straightforward".

- Jeffrey Macre, Darktrace OT SME

A stakeholder further raised a potential gap in the UK's management of risks during transitions and ownership of assets. They questioned how well another operator would be positioned to take over if Vestas or Siemens left the market within the next two years, and whether the regulations and frameworks in place would facilitate this. Examples included obtaining software updates and generator configurations, as there is currently no requirement to document such handover processes.

According to the stakeholder, "There is not much in place to allow a third party to come in and take control of the software… and this may cause problems with regulations".

Future Considerations

	Boardroom Considerations	Government Considerations
01	Continuous monitoring of assets across the supply chain	Increasing preparedness and response to Nation-state attacks
02	Reducing likelihood of vulnerabilities being exploited, by patching, enforcing MFA policies, and securing internet facing IT and OT devices	Ensuring technical authorities globally, including the UK, update their frameworks such as the CAF, or secondary legislation, to reflect the risks posed by AI powered threats, by encouraging organizations to adopt proactive and 'state of the art' cyber defences.
03	Conducting regular risk assessments, mitigation strategies and scenario test plans. Regularly update incident response plans, including how to segment a potentially IT/OT converged environment and introducing role-based controls on admin workstations in times of limited capacity.	Updated regulation should include recognition that supply chains are often the weakest link in organization's cyber defence, and account for critical dependencies in the sector.
04	Increasing collaboration with other companies	Increasing information sharing and collaboration throughout the sector, including threat intelligence and incident response plans in case of national emergency
05	Ensuring email security to reduce common initial attack vector	Funding innovation of cyber detection and defense in energy sectors specifically

Conclusion

Technological transformation in the energy sector, including IT/OT convergence, IoT, net-zero technologies, and AI adoption, is changing its cyber threat landscape. As such, the energy sector has become a prime target for attackers, be it through non-sophisticated or sophisticated means.

Stakeholders note that their main concerns are phishing attack vectors and Nation-state attacks, exacerbated by other factors such as over-dependency in the sector, lack of collaboration, and lack of visibility and control across the supply chain. Our research and data supports their concerns. Between 2022-2024, the most common attack vector for Darktrace energy sectors customers was Email to SaaS propagation. As one US stakeholder noted, "There are no bonus points for a cool hack."

However, AI is positioned to be used by adversaries to launch sophisticated phishing campaigns, poison data and power malware at a large-scale. Such means are feasible, but were not observed in our research alone.

Looking forward, it is anticipated that Email to SaaS attacks will continue to be pertinent in the sector. Given the developments in OT specific malware discoveries and vulnerabilities, it is expected that such OT specific compromises will affect the sector. As Nation-states become more sophisticated and collaborations emerge, Nation-state attacks will continue to target critical energy infrastructure. It is expected for AI to be utilized in future attacks on the sector.

Such findings impress the need of energy organizations to adopt continuous monitoring of assets across the supply chain, reduce the likelihood of vulnerabilities being exploited, and have practiced incident response plans in place. Governments need to assist with critical dependencies in the sector that is the supply chain, increase intelligence sharing across their sectors, and ensure frameworks and innovation reflect the need to detect and respond to the increasing AI powered threat.

References

[1] https://www.rockwellautomation.com/en-us/company/news/press-releases/New-Research-Finds-Cyberattacks-Against-Critical-Infrastructure-on-the-Rise-State-affiliated-Groups-Responsible-for-Nearly-60.html

[2] https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Critical%20National%20Infrastructure%20(CNI)&sort=date%2Bdesc

[3] https://www.gov.uk/government/news/data-centres-to-be-given-massive-boost-and-protections-from-cyber-criminals-and-it-blackouts

[4] https://www.sciencedirect.com/topics/social-sciences/energy-sector

[5] https://www.energy-uk.org.uk/insights/different-parts-of-the-energy-market/

[6] https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-critical-infrastructure-security-resilience.pdf

[7] https://assets.publishing.service.gov.uk/media/66a76bf2ce1fd0da7b592e5d/UK_Energy_in_Brief_2024.pdf

[8] https://assets.publishing.service.gov.uk/media/66a7e14da3c2a28abb50d922/DUKES_2024_Chapters_1-7.pdf

[9] https://www.gov.uk/government/publications/net-zero-strategy

[10] https://www.energy-uk.org.uk/insights/future-of-energy/

[11] https://rusi.org/explore-our-research/publications/commentary/uk-general-election-crucial-inflection-point-energy-and-industry

[12] https://www.vind.ai/customers/success-stories

[13] https://www.ignitec.com/insights/iot-in-uk-smart-grids-powering-a-reliable-and-energy-efficient-future/

[14] https://www.smart-energy.com/industry-sectors/energy-grid-management/bp-to-deploy-ai-for-battery-to-grid-flexibility/

[15] https://assets.publishing.service.gov.uk/media/65fc3d0a65ca2f001b7da7c5/Q4_2023_Smart_Meters_Statistics_Report.pdf

[16] https://www.ofgem.gov.uk/sites/default/files/2022-04/ofgem_ca_guidance_for_dge_gb_v1.0_final.pdf

[17] https://www.napier.ac.uk/-/media/worktribe/output-2880543/practical-cyber-threat-intelligence-in-the-uk-energy-sector-submitted-version.ashx

[18] https://www.energynetworks.org/assets/images/Resource%20library/BEIS%20ENA%20Cyber%20Security%20Procurement%20Language%20Guidance%20(final).pdf?1740562417

[19] https://securitybrief.co.uk/story/uk-wind-energy-firms-lack-sufficient-cybersecurity-warns-cyber-energia

[20]https://www.cepa.co.uk/images/uploads/documents/CyberSecurityInTheEnergySector_WhatDoesItMeanForNetworkRegulation.pdf

[21] https://www.ofgem.gov.uk/sites/default/files/2024-07/RIIO-3_Business_Plan_Guidance.pdf

[22] https://www.eia.gov/energyexplained/electricity/delivery-to-consumers.php

[23] https://www.eia.gov/energyexplained/us-energy-facts/

[24] https://www.rff.org/publications/explainers/us-electricity-markets-101/

[25] https://isorto.org/

[26] https://climateactiontracker.org/countries/usa/net-zero-targets/

[27] https://oyelabs.com/ai-in-oil-and-gas-industry-use-cases-and-examples/

[28] https://www.fdmgroup.com/news-insights/ai-in-energy-sector/

[29] https://www.wirecable.in/opgw-the-smart-energy-transmission-solution/

[30] https://www.energy.gov/oe/grid-modernization-and-smart-grid

[31] https://www.energy.gov/ceser/cybersecurity

[32] https://www.energy.gov/sites/default/files/2024-04/i2X%20Transmission%20Interconnection%20Roadmap.pdf

[33] https://www.pcienergysolutions.com/2024/09/11/u-s-energy-market-comparison-differences-similarities-among-major-isos/

[34] https://www.usa.gov/agencies/federal-energy-regulatory-commission#:~:text=The%20Federal%20Energy%20Regulatory%20Commission,projects%20and%20natural%20gas%20terminals

[35] https://www.energy.gov/sites/default/files/2024-04/i2X%20Transmission%20Interconnection%20Roadmap.pdf

[36] https://www.eisac.com/s/

[37] https://www.energy.gov/policy/articles/cyber-threat-and-vulnerability-analysis-us-electric-sector

[38] https://www.energy.gov/policy/articles/cyber-threat-and-vulnerability-analysis-us-electric-sector

[39] https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

[40] https://www.utilitydive.com/news/minimize-artificial-intelligence-cyber-risks-to-energy-infrastructure-start-with-design/731446/

[41] https://researchbriefings.files.parliament.uk/documents/POST-PN-0735/POST-PN-0735.pdf

[42] https://www.researchgate.net/publication/379381999_The_Diamond_Model_of_Intrusion_Analysis

[43] https://www.mandiant.com/sites/default/files/2022-10/catalog-mandiant-training-courses-000033-23.pdf

[44] https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

[45] https://news.sophos.com/en-us/2021/06/11/relentless-revil-revealed/

[46] https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

[47] https://www.darkreading.com/cyber-risk/ransomware-has-outsized-impact-on-gas-energy-and-utility-firms

[48] https://assets.sophos.com/X24WTUEQ/at/75tnw38cqsnrrv56wpwc78k/sophos-state-of-ransomware-critical-infrastructure-2024.pdf

[49] https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_.pdf

[50] https://www.csoonline.com/article/575439/researchers-find-new-ics-malware-toolkit-designed-to-cause-electric-power-outages.html/amp

[51] https://www.schneier.com/blog/archives/2023/05/pipedream-malware-against-industrial-control-systems.html

[52] https://www.securityweek.com/critical-siemens-rtu-vulnerability-could-allow-hackers-to-destabilize-power-grid/amp/

[53] https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

[54] https://www.darkreading.com/vulnerabilities-threats/volt-typhoon-hits-multiple-electric-cos-expands-cyber-activity

[55] https://industrialcyber.co/threats-attacks/honeywell-schneider-electric-targeted-in-cyber-espionage-campaign-aimed-at-renewable-energy-companies/

[56] https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack

[57] https://cetas.turing.ac.uk/publications/enhancing-cyber-resilience-offshore-wind

[58] https://www.aon.com/en/insights/articles/enhancing-cyber-resilience-in-the-renewables-sector

[59] https://www.baxenergy.com/why-is-cybersecurity-a-top-priority-for-renewable-energy-operators/

[60] https://cyberenergia.com/renewable-energy-hybrid-warfare/#:~:text=Why%20is%20Renewable%20Energy%20a,modern%20society%20cannot%20be%20overstated

[61] https://www.utilitydive.com/news/fbi-cyber-threat-renewable-generation-microgrids-dragos/720509/

[62] https://industrialcyber.co/features/growing-convergence-of-geopolitics-and-cyber-warfare-continue-to-threaten-ot-and-ics-environments-in-2024/

[63] https://thehackernews.com/2022/09/palestinian-hacktivist-group-ghostsec.html

[64] https://securityaffairs.com/129009/cyber-warfare-2/russia-ukraine-critical-infrastructure-attacks.html

[65] https://www.computerweekly.com/news/366583203/NCSC-updates-warning-over-hacktivist-threat-to-CNI

[66] https://www.techtarget.com/searchsecurity/news/366583201/US-warns-of-pro-Russian-hacktivist-attacks-against-OT-systems

[67] https://www.ironnet.com/blog/industroyer2-malware-targeting-ukrainian-energy-company

[68] https://thehackernews.com/2023/09/ukraines-cert-thwarts-apt28s.html

[69] https://securityintelligence.com/articles/uk-energy-expanding-ot-threat-landscape/#:~:text=The%20US%20energy%20sector%20is,breaches%20across%20all%20other%20industries

[70] https://www.infosecurity-magazine.com/news/us-energy-vulnerable-supply-chain/#:~:text=The%20US%20energy%20sector%20is,breaches%20across%20all%20other%20industries

[71] https://industrialcyber.co/features/cl0p-ransomware-attack-yet-again-puts-pressure-on-water-sector-to-fix-cybersecurity-gaps/

[72] https://securityaffairs.com/147545/cyber-crime/shell-clop-ransomware-attacks.html

[73] https://cyberscoop.com/schnieder-electric-siemens-energy-moveit-cl0p/

[74] https://www.politico.com/newsletters/power-switch/2022/12/05/who-shot-the-north-carolina-power-grid-00072235

[75] https://www.itpro.com/security/cyber-attacks/369032/north-korea-linked-hackers-target-us-energy-sector-by-exploiting

[76] https://www.bleepingcomputer.com/news/security/us-energy-firm-shares-how-akira-ransomware-hacked-its-systems/amp/

[77] https://thecyberexpress.com/cyber-army-of-russia-affiliate-high-society/

[78] https://attack.mitre.org/groups/G0007/

[79] https://www.globalsecurity.org/intell/world/russia/gru-staff.htm

[80] https://www.darkreading.com/cyberattacks-data-breaches/russia-fancy-bear-apt-ukrainian-energy-facility

[81] https://securityaffairs.com/52133/hacking/tv5monde-cyber-attack.html

[82] https://securingdemocracy.gmfus.org/incident/russian-government-backed-hackers-target-american-political-parties-

[83] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[84] https://cloudsecurityalliance.org/blog/2024/12/17/decoding-the-volt-typhoon-attacks-in-depth-analysis-and-defense-strategies

[85] https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/

[86] https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[87] https://144806018.fs1.hubspotusercontent-eu1.net/hubfs/144806018/Reports/CNI_Research_Report_2024.pdf?utm_campaign=Whitepapers%20%26%20Reports&utm_medium=email&_hsmi=97860955&utm_content=97860955&utm_source=hs_automation

[88] https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/

[89] https://www.utilitydive.com/news/minimize-artificial-intelligence-cyber-risks-to-energy-infrastructure-start-with-design/731446/

[90] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401366

[91] https://www.chathamhouse.org/2024/07/uk-needs-move-faster-nuclear-energy-cybersecurity

[92] https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028

[93] https://aithority.com/machine-learning/national-artificial-intelligence-and-cybersecurity-isao-welcomes-the-new-cybersecurity-strategy/

[94] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-23.pdf

[95] https://www.energy.gov/cio/articles/doe-cybersecurity-strategy-2024

[96] https://www.cisa.gov/news-events/directives/bod-23-01-implementation-guidance-improving-asset-visibility-and-vulnerability-detection-federal

[97] https://www.whitehouse.gov/wp-content/uploads/2024/12/Energy-Modernization-Cybersecurity-Implementation-Plan.pdf

[98] https://www.gov.uk/government/collections/cyber-security-and-resilience-bill#:~:text=They%20have%20now%20been%20superseded,digital%20services%20and%20supply%20chains

[99] https://www.techuk.org/resource/techuk-report-enabling-growth-and-resilience-the-uk-tech-sector-in-an-uncertain-world.html

[100] https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/f024001d-62c1-48b5-873a-64d240d73f1f

[101] https://www.rand.org/pubs/commentary/2025/01/the-united-states-needs-to-stress-test-critical-infrastructure.html

[102] https://www.energy.gov/ceser/articles/selected-projects-cyber-research-development-and-demonstration-funding-opportunity

[103] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a

[104] https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/12/09/fact-sheet-biden-%E2%81%A0harris-administration-leads-by-example-leveraging-the-federal-government-to-catalyze-clean-energy-jobs-and-cut-costs-and-pollution/

[105] https://cybercorner.tech/malicious-azure-application-perfectdata-software-and-office365-business-email-compromise/

[106] https://www.ncsc.gov.uk/collection/supply-chain-security/third-party-software-providers

[107] https://www.darkreading.com/cyberattacks-data-breaches/volt-typhoon-strikes-massachusetts-power-utility

[108] https://www.securitymagazine.com/articles/101469-chinese-threat-actor-resided-in-us-electric-grid-for-almost-one-year

Appendices

Appendix A: APT28 TTPs

Category	Tactics, Techniques, and Procedures (TTPs)
Initial Access	T1189: Drive-by Compromise, T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1091: Replication Through Removable Media, T1199: Trusted Relationship, T1078.004: Cloud Accounts
Reconnaissance	T1598.003: Spearphishing Link, T1595.002: Vulnerability Scanning, T1589.001: Credentials
Resource Development	T1583.001: Domains, T1583.003: Virtual Private Server, T1583.006: Web Services, T1586.002: Email Accounts, T1584.008: Network Devices, T1588.002: Tool
Command and Control	T1092: Communication Through Removable Media, T1105: Ingress Tool Transfer, T1071.003: Mail Protocols, T1071.001: Web Protocols, T1001.001: Junk Data, T1573.001: Symmetric Cryptography, T1090.002: External Proxy, T1090.003: Multi-hop Proxy, T1102.002: Bidirectional Communication
Credential Access	T1110.001: Password Guessing, T1110.003: Password Spraying, T1040: Network Sniffing, T1003.001: LSASS Memory, T1003.003: NTDS, T1528: Steal Application Access Token, T1557.004: Evil Twin, T1056.001: Keylogging
Persistence	T1098.002: Additional Email Delegate Permissions, T1547.001: Registry Run Keys / Startup Folder, T1037.001: Logon Script (Windows), T1546.015: Component Object Model Hijacking, T1137.002: Office Test, T1542.003: Bootkit, T1505.003: Web Shell
Privilege Escalation	T1068: Exploitation for Privilege Escalation, T1134.001: Token Impersonation/Theft
Lateral Movement	T1210: Exploitation of Remote Services, T1021.002: SMB/Windows Admin Shares
Execution	T1203: Exploitation for Client Execution, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1559.002: Dynamic Data Exchange, T1204.002: Malicious File, T1204.001: Malicious Link
Collection	T1560.001: Archive via Utility, T1119: Automated Collection, T1213.002: Sharepoint, T1005: Data from Local System, T1039: Data from Network Shared Drive, T1025: Data from Removable Media, T1113: Screen Capture, T1074.001: Local Data Staging, T1074.002: Remote Data Staging, T1114.002: Remote Email Collection, T1056.001: Keylogging
Exfiltration	T1030: Data Transfer Size Limits, T1567: Exfiltration Over Web Service, T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

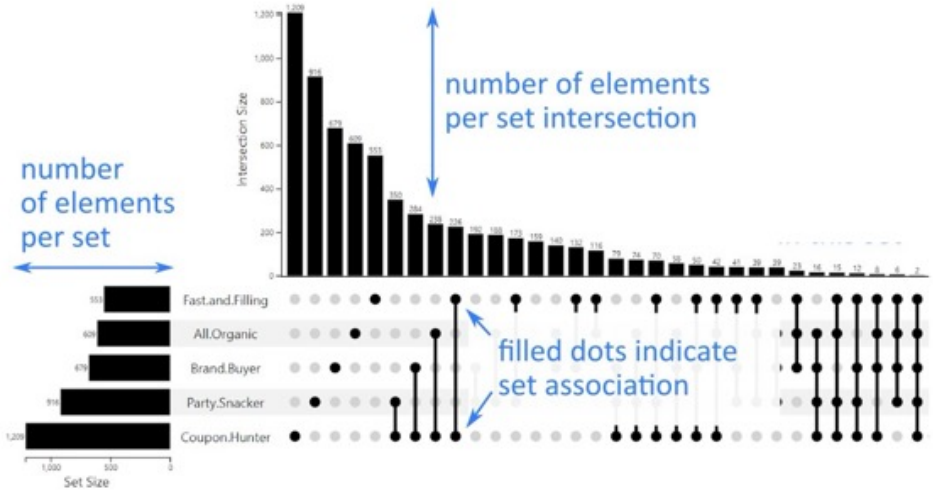
Appendix B: Volt Typhoon TTPs

Category	Tactics, Techniques, and Procedures (TTPs)
Initial Access	Exploit Public Facing Application (T1190), Obtain Capabilities: Exploits (T1588.005), Develop Capabilities: Exploits (T1587.004), Valid Accounts: Cloud Accounts (T1078.004)
Reconnaissance	Proxy (T1090), Proxy: Internal Proxy (T1090.001), Encrypted Channel (T1573)
Resource Development	System Information Discovery (T1082), Query Registry (T1012), Network Service Discovery (T1046), Permission Groups Discovery (T1069), System Owner/User Discovery (T1033), Log Enumeration (T1654), Process Discovery (T1057), Account Discovery: Local Account (T1087.001), Application Window Discovery (T1010), System Network Configuration Discovery (T1016), System Network Configuration Discovery: Internet Connection Discovery (T1016.001), System Service Discovery (T1007), File and Directory Discovery (T1083)
Command and Control	Compromise Infrastructure: Server (T1584.004)
Credential Access	Exploitation for Privilege Escalation (T1068), Unsecured Credentials (T1552), OS Credential Dumping: NTDS (T1003.003), Brute Force: Password Cracking (T1110.002), Credentials from Password Stores: Credentials from Web Browsers (T1555.003), Unsecured Credentials: Private Keys (T1552.004)
Persistence	Obfuscated files or information: Software Packing (T1027.002), Indicator Removal: Clear Windows Event Logs (T1070.001), Indicator Removal: Clear Persistence (T1070.009), Indicator Removal: File Deletion (T1070.004), Masquerading: Match Legitimate Name or Location (T1036.005), Direct Volume Access (T1006), Modify Registry (T1112)
Privilege Escalation	External Remote Services (T1133), Valid Accounts (T1078), Server Software Component: Web Shell (T1505.003)
Lateral Movement	Remote Services: Remote Desktop Protocol (T1021.001), Use Alternate Authentication Material (T1550), Remote Services Session Hijacking (T1563), Remote Services: Cloud Services (T1021.007)
Execution	Command and Scripting Interpreter (T1059), System Binary Proxy Execution (T1218), Ingress Tool Transfer (T1105), OS Credential Dumping: LSASS Memory (T1003.001), Windows Management Instrumentation (T1047), Command and Scripting Interpreter: PowerShell (T1059.001), Command and Scripting Interpreter: Unix Shell (T1059.004)
Collection	Data Staged (T1074), Archive Collected Data: Archive via Utility (T1560.001)
Exfiltration	Exfiltration Over Alternative Protocol (T1048)

Appendix C: Experimental Model IoCs

Hypothesis 1: KV Botnet Indicator model	Hypothesis 2: Suspicious HTTP Indicators model
IPs:	
144.202.49[.]189	174.53.242[.]108
45.63.60[.]39	85.240.182[.]23
216.128.179[.]235	202.175.177[.]238
95.162.229[.]105	24.11.70[.]85
45.11.92[.]176	68.76.150[.]97
59.203.113[.]25	146.70.105[.]61
152.32.138[.]247	77.75.78[.]125
193.36.119[.]48	185.220.100[.]253
45.32.174[.]131	173.239.196[.]198
216.128.180[.]232	
45.159.209[.]228	
Commands:	
	· ^/+dana/+meeting
	· ^/+dana/+fb/+smb
	· ^/+dana-cached/+fb/+smb
	· ^/+dana-ws/+namedusers
	· ^/+dana-ws/+metric

Appendix D: Reading UpSet Plots



Source: https://appsource.microsoft.com/en-us/product/power-bi-visuals/wa200002018?tab=overview

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

North America: +1 (415) 229 9100 Europe: +44 (0) 1223 394 100 Asia-Pacific: +65 6804 5010 Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com