EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA INFORMATION SHARING ACTIVITIES FOR THE ENERGY SECTOR

Energy Community, Cybersecurity Coordination Group - 6th Meeting

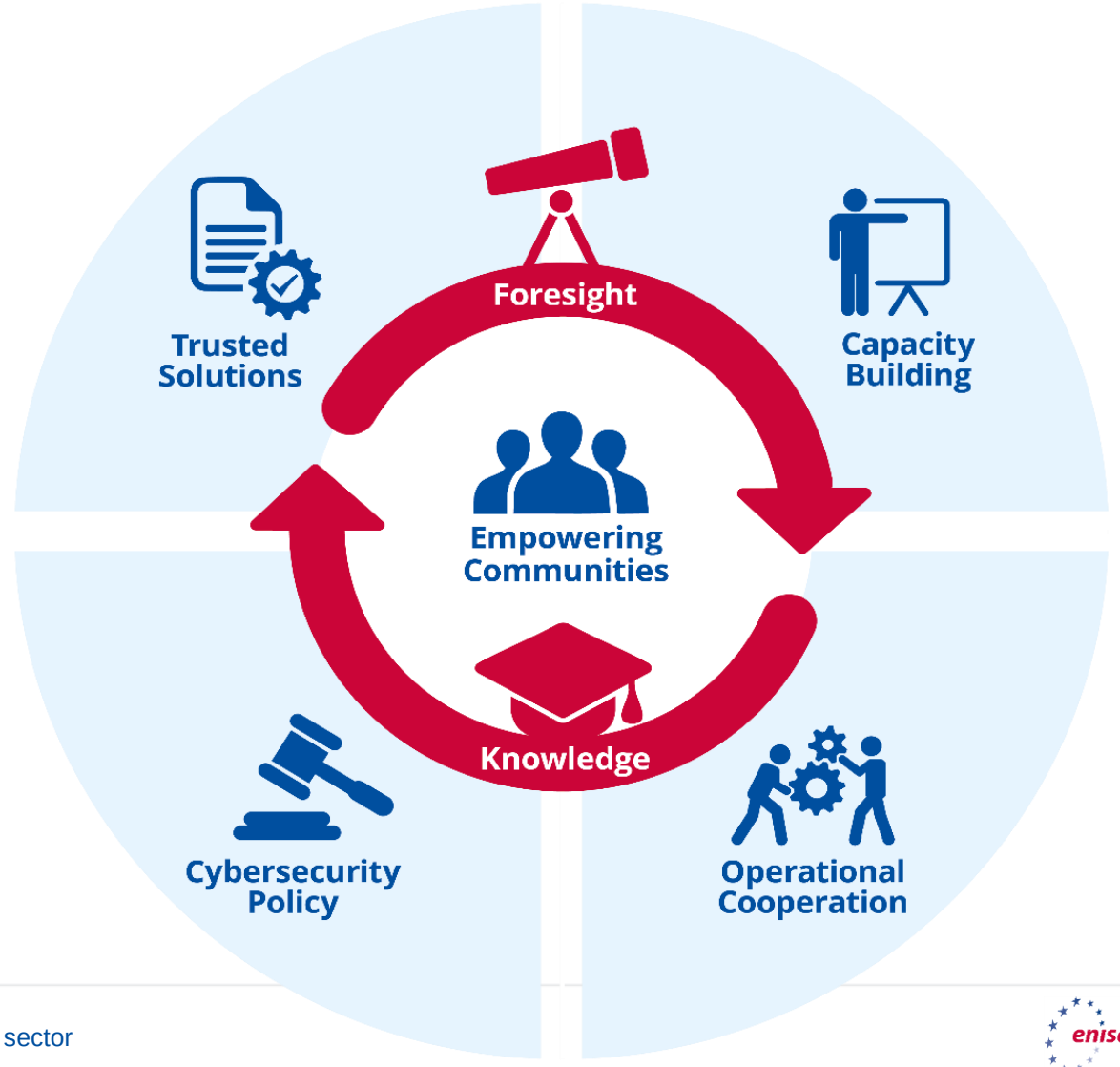
Konstantinos Moulinos
Policy Development and Implementation Unit

5 | 7 | 2022

ABOUT ENISA

A TRUSTED AND CYBER SECURE EUROPE

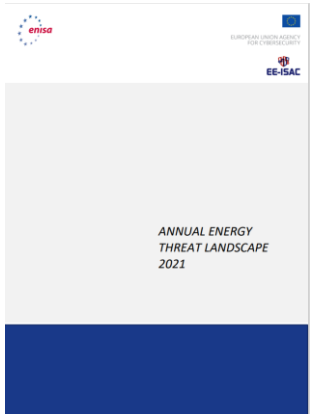
Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community



1. EE-ISAC Threat Landscape
2. Situational Reports
3. Situational Awareness Picture and threat outlook calls

EU ENERGY ISAC THREAT LANDSCAPE

ANNUAL REPORT
TLP: AMBER



Data collection & analysis

DATA SOURCES

- Detections from the EE-ISAC's MISP
- Public sources (e.g. ICS Strive)
- ENISA weekly SAT reports
- ThreatMatch
- Valuable inputs from various security professionals

DATA ANALYSIS – A MULTIPLE ENTRIES' REPOSITORY

- Threat_ID
- ENISA Threat
- ENISA Threat Details
- ENISA High Level Threat
- Threat Vector
- Date/Period
- Affected Subsectors
- Other Affected Sectors
- Affected Assets
- Geographical Spread
- Severity
- Trends
- Key Findings/Comments
- References

					ENISA High Level Threat	Threat Vector	Date/Period	Affected Subsector	Affected Assets	Geographical Spread	Impact (Severity)	Trends details	Key Findings / Comments	References
				ession facility according to nent of Homeland tructure Security Agency	Nefarious Activity/ Abuse	Spearphishing Link to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network.	Jan-20	Gas	Control and communication assets on the facility's operational technology (OT) network.	USA	Shutdown of a natural gas pipeline for two days. Some assets were prevented from processing real-time operational data and a partial loss of situational awareness was created.	ceased	Although the victim's emergency response plan did not specifically consider cyberattacks, the decision was made to implement a deliberate and controlled shutdown to operations. This lasted approximately two days, resulting in a Loss of Productivity and Revenue, after which normal operations resumed.	https://www.jdsupra.com/legalnews/cyberattack-forces-gas-pipeline-shutdown-76217/
				hat Russian military ian threat actor with GRU gas company Burisma, impeachment case. able to confirm the	Nefarious Activity/ Abuse	The attackers have set up fake websites, designed to imitate the sites of Burisma and its subsidiaries, in an effort to trick employees into handing over their email credentials.	late 2019 - early 2020	Oil and Gas	Email credentials of employees at Burisma Holdings and its subsidiaries and partners	Ukraine, USA	It is not clear which information the hackers have accessed, experts believe Russian spies were searching for potentially embarrassing material on the rival Biden and his son.	increasing	The attack was linked to a threat actor tracked as APT28, Pawn Storm, Fancy Bear, Sofacy, Strontium, and Tsar Team. This group has been connected to Russia's Armed Forces, specifically its Main Directorate of the General Staff, also known as the GRU.	CERT-EU, CERT for the EU Institutions, Bodies and Agencies https://www.securityweek.com/phishing-campaign-targeting-ukrainian-firm-burisma-linked-russian-cyberspies
Tick hacking group	Compromising confidential information (data breaches)	Information Leakage	had suffered a security breach in mid-2019 that led to data exfiltration. Mitsubishi Electric has attributed the actions to the likely Chinese Tick group. Researchers later identified that the Trend Micro antivirus product was the point of infiltration.		Nefarious Activity/ Abuse	Unauthorized access by third parties Antivirus product was the point of infiltration.	mid 2019 - early 2020		Servers and computers at Mitsubishi headquarters and other offices belonging to the company	Japan	Investigation of the incident uncovered no evidence that any sensitive data connected to its business partners or government defense contracts had been stolen or misused.	ceased	When announcing the incident, Mitsubishi didn't explain why it had waited so long after discovering the breach to go public with the news. However, the inclusion of the comment "to date, no damage or impact related to this matter has been confirmed" could imply that the company chose to hold back information until it had a clear idea of what the effects of the breach might be.	CERT-EU, CERT for the EU Institutions, Bodies and Agencies https://www.infosecurity-magazine.com/news/mitsubishi-electric-discloses/
	Social Engineering	Phishing Attack	Endeavor Energy Resources, L.P. ("Endeavor"), an oil and gas exploration and production company, discovered on Jan. 14 that earlier that day an unauthorized party, through a phishing scam, possibly gained access to unsecured protected health information stored in the corporate, Office		Nefarious Activity/ Abuse	Employee Fell Prey to Phishing Attack	Jan-20	Oil and Gas	Employee information files	USA	The unauthorised party possibly gained access to unsecured protected health information stored in the corporate, Office 365 account of an Endeavor employee.	ceased	Endeavor has sent notice letters to all potentially impacted individuals in compliance with HIPAA's Breach Notification Rule but has received no indication that any protected health information has been misused.	https://www.databreaches.net/endeavor-energy-resources-notifies-employees-and-dependents-after-employee-fell-prey-to-phishing-attack/

SITUATIONAL REPORTS

SCOPE

- The “Energy Threat Report” is an initiative/proposal from ENISA, for the national authorities with a cyber security interest on energy e.g. the NIS Cooperation Group Work Stream on Energy and the Electricity Coordination Group
- Bi-monthly dissemination

OBJECTIVES

- Up-to-date reporting about **cybersecurity incidents on the energy sector**
- Present an **overall threat level assessment for the sector and notable trends**
- Share **useful recommendations** towards the vulnerabilities and modus operandi underlying the reported incidents
- Contribute to a more secure European Energy sector

METHODOLOGY

3 Conclusions & Recommendations

4 Final Report

- **2021 – 3 REPORTS**
- **2022 – 6 REPORTS**

Jan-Dec

2 Statistics

Data collection & analysis 1

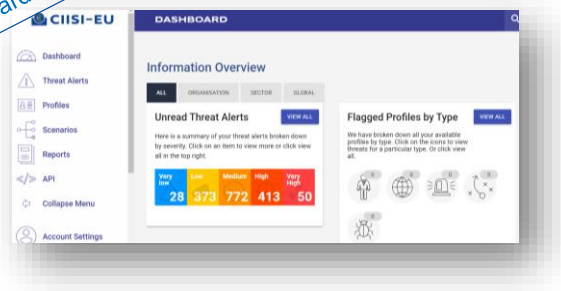
Supporting NIS CG WS8 & ECG

"Less is more" approach
Delivering a non technical, comprehensive reading..
…while still able to address key information

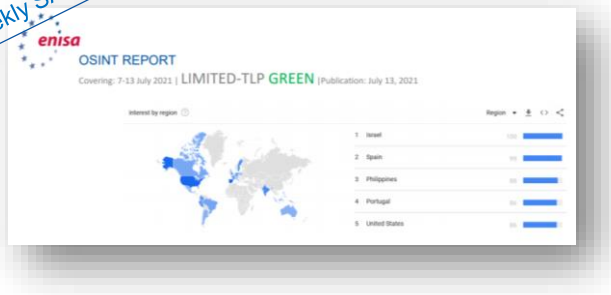
MAIN INFORMATION SOURCES

- The report builds on multiple sources, from OSINT to limited disclosure information and intelligence accessed by ENISA

Intelligence Dashboard



ENISA Weekly SAT Report



STATE OF PLAY AND CURRENT ACTIVITIES

- Bi-monthly report, in 2022 two reports have been shared with NIS CG WS on energy and ECG getting overall praise and support
- 2022: 3rd report due in July

SAMPLE REPORT

Focus on key relevant incidents for the energy sector

4.3 Colonial Pipeline

Colonial Pipeline Company provides pipeline services. The Colonial Pipeline is the largest pipeline system for refined oil products in the U.S.[10]

	THREAT ACTOR	TYPE	GEOGRAPHY
FOR INFORMATION	Darkside Group	Ransomware/Extortion	

Associated Root Cause

Unsecured VPN (Virtual Private Network) account, lacking MFA (Multifactor Authentication).

Incident Description and *Modus Operandi*

On 07 May 2021, Colonial Pipeline administration reported a successful compromise of its network by Darkside group. Darkside group is a threat actor known to target several sectors including the energy sector for the purpose of extortion. The incident resulted in the encryption of critical systems which caused the shutdown of operations. This affected fuel prices due to shortages as the pipeline supplied 45% of the United States East Coast's gasoline, diesel and jet fuel. The incident also cause some panic in the population with some individuals stockpiling fuel. This episode had wide media coverage, more information can be found in news pieces such as https://www.cnbc.com/2021/05/08/colonial-pipeline-shuts-pipeline-operations-after-cyberattack.html

Recommendations

Colonial shed light into overall lack of systems security and information management practices, in particular as unlike electricity industry, pipelines utilities in US (oil, natural gas, hazardous liquids) are not subject to mandatory cybersecurity requirements[11]. Both technical and organizational measures are

Structured information for a quick overall picture

Threat assessment for the energy sector

Easy reading, relevant recommendations and useful links

Up-to-date info on key Figures and major trends

3 ENERGY SECTOR THREAT ASSESSMENT – KEY TRENDS

3.1 Energy Sector: GLOBAL

Based on the high operational tempo of ransomware operators and nation state actors, the threat globally is assessed to be ELEVATED.

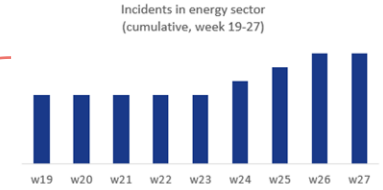
Rationale:

- Over the last 60 days, there has been six reported ransomware incidents affecting some energy companies in Europe and globally. Most of these have had only minor impact on the operations of the victims, with some disclosure of information.
- Globally, there has been an increasing level of targeting by Chinese, Russian, and Pakistani threat actors.

2 KEY STATISTICS

According to the NIS Cooperation Group[3], in 2020, EU Member States reported 756 cybersecurity incidents overall, compared to 432 for the previous year, 2019. Regarding the energy sector, incidents more than doubled (109%) in the same period, from 43 in 2019 to 90 in 2020.

According to various sources, ENISA identified seven relevant incidents in the energy sector over the past 2 months, from which this report provides details concerning those deemed the most impactful (see chapter 4).



The cumulative number of incidents in the energy sector for the past 2 months (July 7-September 7) has risen[4], as depicted in the chart above, and the compound growth rate is 5.2% per week.

CALLS WITH ENERGY STAKEHOLDERS

Weekly Situational Awareness Picture and threat outlook calls

- DG-ENER, ENTSO-E, ENTSO-G, Energy Community (upon invitation)
- Exchange views on the current situation (state of the sector, threats)
- Bi-directional information sharing and joint situational awareness
- Discuss how can ENISA provide assistance to public and private stakeholders

Overall:

- the levels of activity are on the rise on a global scale

- to have a good understanding of the (subsector) situational picture DSOs should be also involved

Ad hoc Preparedness calls with energy stakeholders

- EE ISAC, ENTSO-E, ENTSO-G, EU.DSO entity, E.DSO, EURELECTRIC, CEDEC, GEODE, NIS CG WS on energy, ACER, DG-ENER
- Update the energy stakeholders on preparedness, maturity, risks, and needs with respect to the UA crisis
- 8,11 March 2022

Overall: Sector is considered mature and contingency plans are in place

KEY FINDINGS

- Ransomware and supply chain attacks are one the rise
- No major escalation or spill-over into the EU
- Authorities are in alert mode, holding frequent meetings with other authorities at national level, reinforcing existing channels with national CSIRTs
- Industry notes that the situation is under control
- Authorities need more TLP GREEN to be able to share with operators
- NCAs would need information on affected supply chain
- Lessons learned drawn from VIASAT incident (it should be in scope of network code)
- EE-ISAC sees value in information sharing with ISACs from other sectors

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Agamemnonos 14 Str
15231 Chalandri
Athens, Greece

+30 2814409629

info@enisa.europa.eu

www.enisa.europa.eu