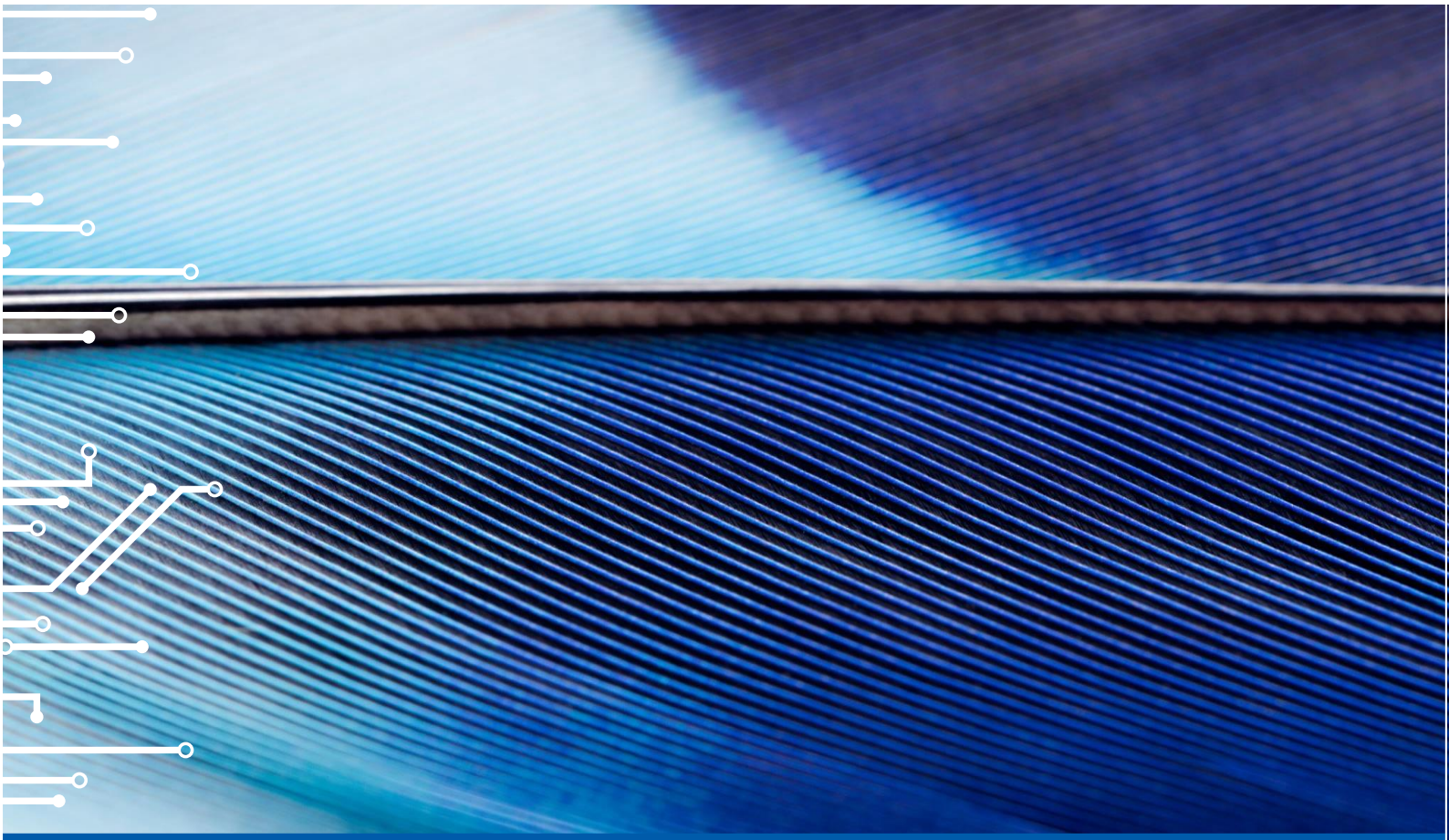
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



SITUATIONAL AWARENESS REPORT

Energy Sector

January 2024

Reporting period: 01 November – 31 December

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

AUTHORS

Konstantinos Moulinos, Ricardo Figueiredo, Eleni Philippou
Policy Development and Implementation Unit

INTRODUCTION

The ENISA Situational Awareness Report – Energy Sector is a bimonthly report aiming to provide updated situational awareness[1] based on information gathered from open sources (OSINT), together with information from threat intelligence providers that ENISA has access to.

DISCLAIMER

Information provided in the report is intended to be used for situational awareness purposes only and within the scope of report. Sources and the accuracy of information is referenced and verified to the possible extent on a best effort basis at the moment of reporting.

DOCUMENT HANDLING

This document is marked as **TLP GREEN**

Recipients may share the report with members of the NIS CG WS on energy as well as with energy national competent authorities, regulatory bodies and EU agencies, and should not use publicly available channels. This information is not for public disclosure.

RELEVANT INFORMATION TO THE READER

The overall threat level for the Energy sector (both globally and at EU) is presented in this report by making use of the following scale, together with a rationale behind such level.

Low	Guarded	**Elevated**	High	Severe

The domain/geographic reach of the incidents presented in this report is set according to the following criteria[2]:

	If affected networks, systems, services, controlled and assured…	**If affected population is…**
NEAR	are within the EU borders	within the EU borders
MID	rely on non-EU institutional or MS public or private authorities	in geographical areas in proximity to EU borders
FAR	lie beyond EU institutional or MS public or private authorities	in geographical areas far from the EU borders
GLOBAL	Incidents with a global impact to networks, systems, services and/or population	

[1] In accordance with the EU cybersecurity act Art.7 Par.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)
[2] Definitions for the Near, Mid, Far attributes can be found at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf, p.40

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This report seeks to provide NIS Cooperation Group WS on Energy national authorities with a brief overview of the incidents with a relevant impact on the Energy sector in Europe and globally over the period ranging from 01 November to 31 December 2023.

Noteworthy Trends

Cybercriminal and nation-state adversaries observed targeting energy sector organisations in Europe

The reporting period saw a continuation of cybercriminal activity targeting European energy sector entities, as ransomware actor listings increased again following a temporary dip in activity between September and October 2023. Initial access brokers (IABs) were also seen advertising alleged access to energy sector entities, as seen via the below advertisement published to the Russian Anonymous Market Place (RAMP).

Most notable were a series of high-profile disruptive attacks targeting power generation facilities, both in the EU (e.g., Slovenia's HSE and various critical service providers in Denmark) and globally (Serbia's EPS and an unnamed Ukrainian power facility). Such activity comes amidst warnings from the United States' Federal Bureau of Investigation (FBI) anticipating increased nation-state targeting of Western critical energy infrastructure amidst changes in global energy supplies.

Sandworm's attacks against Ukrainian power facilities showcase the types of tooling and capabilities that may feature in potential such state-backed operations targeting EU energy infrastructure, specifically in their use of OT-specific living-off-the-land (LotL) techniques, wherein group operators leverage native binaries to execute unauthorised commands and manipulate physical process controls within OT environments.

Particularly as European leaders consider the feasibility of seizing frozen Russian assets to fund rebuilding efforts in Ukraine, there is a reasonable possibility that Russian APT groups may seek to establish long-term footholds in European energy sector operators as a form of strategic prepositioning to prepare for future scenarios where EU-Russia relations deteriorate further.

Based on notable trends, threat actors' activity, behaviour and tactics, the overall threat level to the Energy sector for the reporting period is rated:

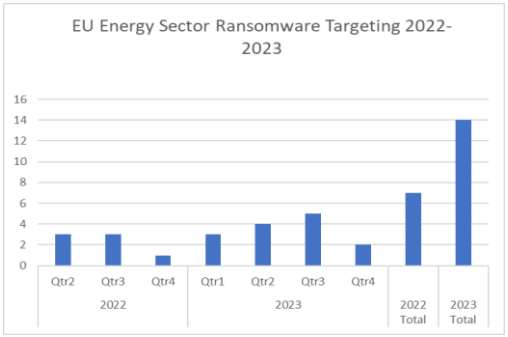
- **ELEVATED, at a European level;**
- **GUARDED, at a Global level;**

In the following sections, and based on information from various sources, this report provides details concerning the most impactful incidents affecting the Energy sector.

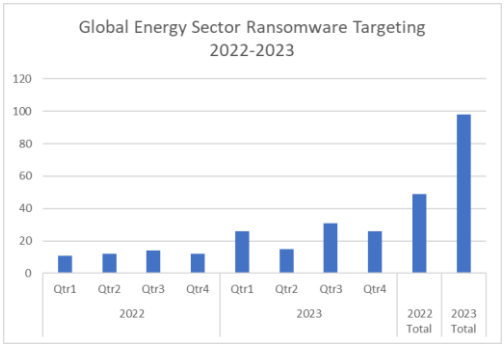
2. RAMSOMWARE – TREND ANALYSIS OF 2022/23

2023 saw a 75% increase in the number of European energy undertakings listed on ransomware leak sites compared to 2022.

In 2022, no quarter stood out as a peak quarter, with an equal number of European companies listed in the first, second and third quarters. However, the number of entities steadily rose in Q1-Q3 2023, comprising 85% of total listings for the year.



A similar trend can be seen in global energy sector ransomware targeting, with a total of 98 incidents recorded so between January and December 2023, compared to 49 recorded over the course of 2022.



Worldwide, the most active ransomware operators during the November - December 2023 reporting period were LockBit3.0 and Play, with 4 incidents and 3 incidents respectively. This was followed by 8base, ALPHV/Blackcat, Akira, NoEscape and Ragnar Locker, each with one recorded incident.

3. ENERGY SECTOR THREAT ASSESSMENT

The report highlights incidents that did or are believed to have had an effect on the Energy Sector.

3.1 ENERGY SECTOR: EUROPE

Assessment: The European threat level has been maintained at ELEVATED.

This assessment is based on continued targeting of European energy sector entities by ransomware groups and nation-state actors, including incidents impacting power generation facilities in Denmark, Slovenia, Serbia and Whilst there have been no cyber-attacks with a significant enough impact to warrant a change to threat levels, ransomware actors and other organised criminal groups (OCGs) are assessed to pose an acute threat to energy operators, both in the EU and globally.

Meanwhile, reports concerning Sandworm-attributed attacks against a Ukrainian power generation facility highlights the types of sophisticated tooling and techniques that OT-oriented nation-state groups are capable of leveraging in attacks against energy sector operators.

3.2 ENERGY SECTOR: GLOBAL

Assessment: The GLOBAL threat level has been maintained at Guarded.

Threat actors continue to target energy sector entities for espionage-oriented and financially motivated operations, with several disruptive attacks targeting the sector recorded in the reporting period.

3.3 NOTABLE VULNERABILITIES

Firsy Disclosed	**25/04/2023**
Product Affected	Zyxel Firewalls (Unspecified versions/models)
Summary	On 25 April 2023, Zyxel published information concerning an OS command injection vulnerability impacting the Internet Key Exchange (IKE) packet decoder in several of its firewall appliances. Proof-of-concept (PoC) analysis from Rapid7 published 19 May 2023 showed that the flaw, tracked as CVE-2023-28771, enables an unauthenticated attacker to execute certain OS commands remotely by sending crafted packages to an impacted device.
Observed Usage	On 11 November 2023, Denmark's SektorCERT published a report disclosing a series of attacks targeting Danish critical infrastructure providers which the report partially attributes to the Russia-nexus APT Sandworm. According to the report, likely numerous actors – potentially to include Sandworm - were observed leveraging CVE-2023-28771 to target at least 11 Danish CNI operators in several waves of attacks, the first of which began on 11 May 2023, over a week before Rapid7's PoC was first published.
CVSS	**CRITICAL: 9.8**

Date Disclosed	**31/03/2023**
Product Affected	Microsoft Outlook
Summary	CVE 2023-23397 is a vulnerability affecting Microsoft Outlook which can be exploited by sending a specially crafted email which triggers automatically when processed by the Outlook client.
Observed Usage	No attacks have been thus far reported related to the vulnerabilities mentioned in Cisco Talos's report; however, as of the time of reporting, Yifan has yet to release an official patch.
CVSS	**CRITICAL: 9.8**

4. ENERGY SECTOR INCIDENTS – REPORTING PERIOD (MOST RELEVANT)

NEAR	*Affected networks, systems, services, controlled and assured within the EU borders. Affected population within the EU borders.*

4.1 HSE IMPACTED BY DISRUPTIVE CYBER INCIDENT

	THREAT ACTOR	TYPE	GEOGRAPHY
SUMMARY	Rhysida	Ransomware	[SI]

Overview

HSE Group operates Slovenia's Šoštanj thermal plant as well as hydroelectric plants around the country, accounting for approximately 60% of domestic electrical production.

On 24 November, the Slovenian state-owned power generation company Holding Slovenske Elektrarne (HSE) reported that it had fallen victim to a disruptive cyber-attack. Whilst the company acknowledged the incident, the company's statement asserts that the breach resulted in no identifiable impact on HSE's power generation operations.

Assessment

According to a statement published by HSE on their website, the incident was described as a "crypto-virus" that encrypted company files and led to staff being temporarily locked out of systems. According to initial statements from HSE, data available to investigators remains insufficient to attribute the incident to a known intrusion set; however, later reporting from media, citing sources with knowledge of the investigation, attributed the incident to the Rhysida ransomware group and stated that initial access was likely obtained via exploitation of an unprotected cloud storage instance. Several weeks later, on 10 December 2023, Rhysida ransomware listed HSE on their dark web leak site, demanding a ransom payment.

4.2 DK-CERT REPORTS TARGETING OF DANISH CRITICAL INFRASTRUCTURE

	THREAT ACTOR	TYPE	GEOGRAPHY
SUMMARY	Sandworm	Malware	[DK]

Overview

On 11 November 2023, Denmark's SektorCERT published a report disclosing a series of attacks targeting Danish critical infrastructure providers, which the report partially attributes to the Russia-nexus APT Sandworm. According to the source, likely numerous actors - to include Sandworm - were observed targeting at least 11 Danish CNI operators by leveraging a combination of known (CVE-2023-28771) and zero-day (CVE-2023-33009, CVE-2023-33010) vulnerabilities in Zyxel firewalls.

Assessment

Following an initial wave of attempted intrusions that began on 10 May 2023 involving exploitation of CVE-2023-28771, a second wave took place between 22 and 25 May 2023, with some attacks involving efforts to recruit devices into variants of the Mirai botnet. Some impacted devices were then reportedly used to conduct brute force and distributed denial-of-service (DDoS) attacks against companies in the U.S., Canada and Hong Kong. Later reporting from Forescout in January 2024 suggests the two waves were likely unrelated and that, more broadly, assessed links to Sandworm are likely tenuous given that the indicators cited in SektorCERT's initial attribution assessment (C2 IP addresses) have been elsewhere linked to other IoT botnet activity.

4.3 CYBER INCIDENT IMPACTS ACER

	THREAT ACTOR	TYPE	GEOGRAPHY
SUMMARY	Ragnar Locker	Ransomware	[EU]

Overview

On 27 November, the EU's Agency for the Cooperation of Energy Regulators (ACER) reported that they had been targeted in a cyber-attack. The Agency remained fully functional and at the time of writing, a full investigation was underway with the appropriate stakeholders such as CERT-EU taking part.

Assessment

ACER is the EU Agency for the Cooperation of Energy Regulators (ACER). ACER ensures that the integration of national energy markets and the implementation of legislation in the Member States are met according to the EU's energy policy objectives and regulatory frameworks[3]. While attribution details for the incident remain unknown, the current threat landscape and geopolitical tensions may render ACER as a high-profile target of potential interest to both financially motivated threat actors or state-sponsored actors with an interest in the European energy sector.

4.4 CYBER INCIDENT IMPACTS DENA

	THREAT ACTOR	TYPE	GEOGRAPHY
SUMMARY	Unknown	Unknown	[DE]

Overview

Between 11-12 November 2023, the German Energy Agency (Dena) was targeted in a cyber-attack. According to a spokesperson for the organisation, internal server systems have failed, and an external team of forensic experts moved on site to investigate the incident. Further details of the nature, scope, and impact of the attack were not disclosed.

[3] https://www.acer.europa.eu/the-agency/about-acer

Assessment

It is currently unclear who targeted Dena. There are currently no ransomware listings that would indicate a financially motivated attack, although this is plausible. Due to the sector and geographical location of the German Energy Agency, Russian state aligned activity is also plausible. However, with no additional details surrounding the incident currently available, attribution is speculative.

MID	*Affected networks, systems, services, controlled and assured in geographical areas in proximity to EU borders. Affected population is in geographical areas in proximity to EU borders.*

4.5 UK'S SELLAFIELD NETWORK BREACHED

SUMMARY	THREAT ACTOR	TYPE	GEOGRAPHY
	Unknown	Breach	[UK]

Overview

On 04 December, a report released by the UK-based newspaper The Guardian claimed that cyber actors linked to Russia and China successfully breached the network of the UK's Sellafield nuclear site in Cumbria. Citing unnamed sources, the report's authors state that initial compromise may have occurred as early as 2015, and that the full extent of potential data loss or exposure of sensitive systems to disruption remains unconfirmed due to the alleged failure of plant administrators to notify nuclear regulators upon discovery of the breach. Two days later, on 06 December, Sellafield Ltd released a statement via the UK government's website refuting the central claims of The Guardian's article, stating that "there hasn't been a successful attack on [Sellafield's] networks by state or non-state actors". On the same day, UK Energy Secretary announced that a letter to the UK Nuclear Decommissioning Authority had been submitted requesting an explanation for the "serious and concerning" allegations regarding activities impacting the site.

Assessment

Given a lack of publicly available evidence, it is not possible to independently confirm the central claims made by The Guardian's initial report. However, it is worth noting that the Sellafield nuclear site has been subject to criticism in the past for its handling of security issues. According to reporting published 09 December 2023 by The Times, a former Sellafield employee stated that site administrators maintained a "complacent" and "lax" attitude toward cybersecurity, with staff occasionally being asked to work on sensitive projects using their personal computers. Additionally, sources from Cumberland Council, the region in which the Sellafield site is located, released a statement to the press in October 2023 acknowledging that council authorities remain unable to confirm the scope of data potentially lost following a series of WannaCry ransomware attacks impacting the council in 2017. This is potentially of significance given that Cumberland Council maintains documents containing potentially sensitive information about the Sellafield site, such as details regarding the plant's nuclear inventory and water management activities, as well as other operational data that could be used to target Sellafield directly.

FAR	*Affected networks, systems, services, controlled and assured lie beyond EU institutional or MS public or private authorities. Affected population in geographical areas far from the EU borders.*

4.6 ESPIONAGE ISRAEL ELECTRIC CORPORATION BREACHED

	THREAT ACTOR	TYPE	GEOGRAPHY
SUMMARY	CyberAv3ngers	Data Breach	[IL]

Overview

On 23 December, the threat actor known as CyberAv3ngers claimed to be in possession of 1TB of data belonging to the IEC (Israel Electric Corporation), the largest supplier of electrical power in Israel and the Palestinian territories. The IEC is responsible for the building, maintenance and operation of power generation stations and sub-stations, as well as the transmission and distribution of networks within Israel. On their X channel "@CyberAv3ngers", the group has posted various screenshots of documents which may pertain to IEC facilities, along with a link to a Telegram channel where a sample packet of alleged IEC data may be downloaded.

Assessment

The CyberAv3ngers group have been observed targeting and compromising various systems and entities associated with Israel. In December 2023 the group targeted Israeli-made Unitronics Vision Series programmable logic controllers (PLCs) in water treatment facilities worldwide, stating that all products 'Made in Israel' are legitimate targets. The group is also deemed by the FBI and CISA to be an APT affiliated with the IRGC (Islamic Revolutionary Guard Corps), a multi-service branch of the Iranian Armed Forces. The IEC are yet to comment on the veracity of CyberAv3ngers claims.

5. THREAT SPOTLIGHT

OPERATION: SANDWORM CONDUCTS DISRUPTIVE ATTACK AGAINST UKRAINIAN POWER FACILITY	
Threat Actor	Sandworm (aka Telebots, BlackEnergy, Sandworm, Quedagh, VoodooBear, Iron Viking, Electrum, Industroyer, G0034, GRU Unit 74455, UAC-0082)
Capability	The Sandworm group is a highly capable group which has conducted disruptive cyber-attacks largely targeting Ukrainian critical infrastructure including the energy and banking sectors since 2015. The group is known for the deployment of KillDisk, CaddyWiper and NotPetya.
Motivation	Disruption, Data Theft, Espionage
Threat Level	**HIGH**

OPERATION: SANDWORM CONDUCTS DISRUPTIVE ATTACK AGAINST UKRAINIAN POWER FACILITY	
Operation Summary	• On 09 November 2023, Mandiant released a blog post detailing a series of disruptive cyber physical incidents that occurred in late 2022 wherein an unnamed Ukrainian power utility was targeted by the Russia-linked threat actor Sandworm. According to Mandiant researchers, Sandworm operators leveraged novel operational technology (OT)-level living-off-the-land (LotL) techniques to overload the victim's substation circuit breakers, causing an unplanned power outage that coincided with large-scale Russian missile attacks against critical infrastructure targets across Ukraine. • Mandiant reports that the intrusion likely began as early as June 2022, but states that the initial access vector the attackers used to gain access to the victim's IT environment currently remains unknown. Sandworm then reportedly accessed the victim's OT environment through a hypervisor hosting a supervisory control and data acquisition (SCADA) management instance for the victim's substation environment and likely maintained this access for up to three months before acting on its objectives.
Tactics, Techniques and Procedures (TTPs)	**Lateral movement** • **T847 - Replication Through Removable Media:** Upon gaining access to the victim's OT environment through a hypervisor hosting a supervisory control and data acquisition (SCADA) management instance, Sandworm deployed an optical disc (ISO) image named "a.iso" as a logical CD-ROM inserted into the CD-ROM drive of the SCADA virtual machine. **Execution** • **T871 - Execution Through API:** Sandworm utilised the native MicroSCADA "Scilc.exe" binary (likely using "n.bat") to execute an external Supervisory Control Implementation Language (SCIL)-based program via the SCIL-API. **Defense Evasion** • **T872 - Indicator Removal on Host:** Sandworm deployed CADDYWIPER malware within the victim's IT environment to remove forensic artifacts left behind during the operation.

6. RECOMMENDATIONS BASED ON OBSERVED ACTIVITY

Based on observed activity, to reduce the risk and impact of potential future intrusions, the following practices are advised:

Mitigating attacks targeting vulnerable public facing services (T1190)

Several high-profile incidents impacting energy sector entities observed during the reporting period featured attempts to exploit public facing applications or appliances (T1190) as a means of initial access. Whilst adversaries may target a range of services, general mitigation steps such as those mentioned below can improve the security posture of an organisation to such attacks:

- **Update Software (M1051):** It is highly recommended that organisations implement regular software updates to mitigate the risk of exploitation from known vulnerabilities. Software should be updated regularly as part of a robust and thorough a thorough patch management process, including verification of unmaintained and/or previously vulnerable dependencies, unnecessary features, components, files and documentation.
- **Exploit Protection (M1050):** Administrators can use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. This can be useful in the event an attacker is successful in compromising an account or device outside the protection of an organisation's security controls, such as that of a third-party contractor.

Mitigating Living-off-the-Land (LotL) techniques:

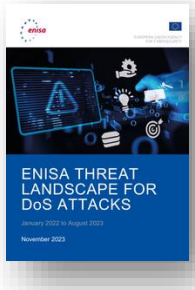
Sandworm's attacks against Ukrainian power facilities highlight the risks posed to energy sector entities by adversaries leveraging living-off-the-land (LotL) techniques, namely the use of native binaries to execute unauthorised commands (T0855) and manipulate physical process controls (T0831) within OT environments. While specific LotL techniques may vary based on characteristics specific to a given target environment, the below strategies may help mitigate against:

- **Network Segmentation (M1030)**: Access to critical IT or OT devices should be properly limited via network segmentation to prevent lateral movement from potentially exposed assets to sensitive devices or infrastructure elements.
- **SSL/TLS Inspection (M1020):** Even where proper segmentation is implemented, defenders should deploy OT-sensitive deep packet inspection solutions to monitor for potentially malicious device communications. Logging capabilities should also be enabled to enable investigators to review suspicious connections or abnormal communication activity.

7. SUGGESTED READINGS

NIS Investments Report 2023 – This report aims at providing policy makers with evidence to assess the effectiveness of the existing EU cybersecurity framework specifically through data on how Operators of Essential Services (OES) and Digital Service Providers (DSP) identified in the European Union's directive on security of network and information systems (NIS Directive) invest their cybersecurity budgets and how the NIS Directive has influenced this investment. This fourth iteration of the report presents data from 1,080 OES/DSPs from all 27 EU Member States.

ENISA Threat Landscape for DDoS attacks – Denial-of-Service (DoS) attacks have been a constant security concern for organisations. However, in the last few years, DoS attacks have become easier, cheaper and more aggressive than ever before. This report aims to bring new insights to the DoS threat landscape through a careful analysis of the motivations and impact of DoS attacks.



ANNEX A – LIST OF ACRONYMS/DEFINITIONS

AD: Active Directory
APT: Advanced Persistent Threat. Term to describe well-defined and capable threat actors.
AV: Anti-Virus
BEC: Business Email Compromise, an attack technique focusing on inserting oneself into email communications and issuing fake payment instructions
CNA: Computer Network Attack
CERT: Computer Emergency Response Team
CNE: Computer Network Exploitation
CNI: Critical National Infrastructure
DMZ: Demilitarized Zone
DPI: Deep Packet Inspection
FIN: Common naming convention for APTs which focus solely on financial crime
HfH: Hackers for Hire
IACS: Industrial Automation and Control System
ICS: Industrial Control System
IDS: Intrusion Detection System
ISMS: Information Security Management System
MaaS: Malware as a Service
MFA: Multi-factor authentication
OCG: Organised Criminal Group
OWASP: Open Web Application Security Project
OSINT: Open Source Intelligence
PII: Personally Identifiable Information (US terminology for EU “personal data”)
PoC: Proof-of-concept code, usually to exploit a specific vulnerability.
RaaS: Ransomware as a Service
RDP: Remote Desktop Protocol
SIEM: Security Information and Event Management
SOC: Security Operation Center
UNC: Term to describe a low-confidence grouping of attack activity (will develop into a APT once sufficient evidence obtained)
VPN: Virtual Private Network

For further information please refer to ENISA glossary https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/glossary and ENISA list of acronyms https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary

ANNEX B – TERMINOLOGY

Threat Levels

This report adopts a 5-level method for describing Threat Levels, which is commonly used by ISACs and working groups. These are calculated through an assessment of key actor activity and an analysis of recently exposed vulnerabilities and exploits (Opportunity). Analysis is conducted monthly and combines multiple Intelligence sources.

- **SEVERE –** It is almost certain that organisations are being targeted by threat actors. High severity vulnerabilities with no known remediation are being exploited and significant damage and outages are being observed across sectors.
- **HIGH** – It is highly likely that entities will be directly targeted by threat actors. Multiple entities will be, or are being, affected. Sector disruption is expected to be widespread, across multiple organisations.
- **ELEVATED –** It is likely that entities are being directly targeted by threat actors or could be exposed to breaches using recent vulnerabilities. Sector disruption is considered a realistic possibility.
- **GUARDED –** There is potential for some direct targeted threat actor activity but it is generally considered Unlikely. This activity could lead to some minor disruption.
- **LOW –** A low likelihood of threat actor targeting activity that could affect organisations/entities. Disruption is considered highly unlikely.

Severity Scores

5	Very High: Highly likely to be an imminent threat, with high relevance to the sector or entity with possibly severe consequences
4	High Threat: Likely a threat in the short term that is highly relevant to the sector or entity with the possibility to cause disruption
3	Medium Threat: Possibly a threat in the short to medium term that may be relevant to the sector or entity. Realistic possibility of having an effect
2	Low Threat: Unlikely to be a threat in any time scale yet remain relevant for awareness purposes. Unlikely to affect an entity
1	Very Low Threat: Highly unlikely to be a threat. A score of 1 is used for awareness and information purposes.

Assessment Language

STATEMENT	PROBABILITY RANGE
Remote	<5%
Highly Unlikely	10 - 20%
Improbable or Unlikely	25 - 35%
Realistic Possibility / Possible	40 - 50%
Probable or Likely	55-75%
Highly Probable/Likely	80-90%
Almost Certain	>95%

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu