enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY 20 years!

SITUATIONAL AWARENESS REPORT

Energy Sector

July 2024

Reporting period: 01 May – 30 June

TLP:GREEN

For comments and suggestions reach out to: enisa-nis-directive@enisa.europa.eu

TABLE OF CONTENTS

INTRODUCTION

The objective of this bimonthly Sectorial Report is to provide stakeholders with situational awareness regarding the threats facing the energy sector prioritising incidents with a direct impact in the EU.

DISCLAIMER

The information provided in this report is solely meant to be used for situational awareness within the scope of this document. The sources and accuracy of the referenced information have been verified to the extent possible, on a best effort basis, at the time of reporting.

DOCUMENT HANDLING

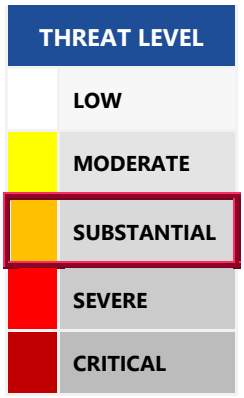
This document is marked as **TLP GREEN.** It may be shared with members of the broader community or sector (e.g., the NIS CG WS on Energy, Energy national competent authorities etc.), but not via publicly available channels.

1. ENERGY SECTOR THREAT ASSESSMENT

1.1 ENERGY SECTOR: EUROPE

The threat level for the **Energy** sector in **Europe,** remains **SUBSTANTIAL**.

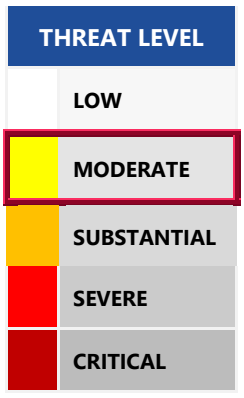
- During the reporting period, Energy sector entities within the European Union were targeted by both financially and politically motivated threat actors. While no major incidents resulting in significant operational disruption to European energy infrastructure were recorded, the level of capability and intent of state-nexus actors to target said entities is likely to remain elevated in the current geopolitical context.
- The United States also published advisories about pro-Russian hacktivists targeting vulnerable industrial control systems (ICS) in Europe and North America. These advisories reported limited physical disruptions, including manipulation of human-machine interfaces (HMIs), altered alert settings and alarms, and resets of administrative passwords.



1.2 ENERGY SECTOR: GLOBAL

The **Global** threat level for the **Energy** sector has been maintained at **MODERATE**.

- Although financially and ideologically motivated threat actors continue to target energy sector entities globally, this activity is diffused and varied across different geographies. Within the reporting period observed, the most significant incidents affecting organisations outside of the EU, impacted gas and oil companies in the United States and United Kingdom.



2. NOTABLE TRENDS

Operational technology (OT) assets remain priority target for pro-Russian hacktivists

Throughout May and June this year, pro-Russian hacktivist personas were observed targeting numerous energy sector entities throughout the European Union, focusing primarily on Germany, Finland, Slovakia and Romania. As in previous reporting periods, nearly all activities observed were DDoS attacks, most of which were conducted in response to EU Member State anouncements of additional defence assistance to Ukraine. Recent examples include Romania's pledge to provide Kyiv with a Patriot missile system and Germany's decision to provide electric grid support to Ukraine in the wake of blackouts caused by Russian missile and drone attacks on Ukrainian energy infrastructure.

During the same period, pro-Russian hacktivist actors also claimed to have conducted numerous operations against European critical infrastructure targets, including those in the energy sector. Of these, the most active persona during the past two months was Hunt3rKill3rs, who claimed to have compromised multiple industrial control systems (ICS) and small-scale operational technology (OT) systems in Europe and North America, including those using power grid control terminals produced by Schneider Electric. According to a recent alert from the United States Cybersecurity and Infrastructure Security Agency (CISA), while current activities mainly involve unsophisticated methods with limited impact on ICS equipment, investigations suggest that these actors possess capabilities that could pose physical threats to insecure and misconfigured OT environments. Given that the current state of confrontation between Russia and states within the European Union is likely to persist in the immediate to medium term, OT operators are advised to implement security best practices such as implementing multifactor authentication across OT networks and disconnecting all human machine interfaces (HMIs) from the public facing internet.

Sources

Source[1]: https://www.ft.com/content/4d583259-7565-4cbc-972e-ea77f4a76175
Source[2]: Romania to send Patriot missile system to Ukraine (lemonde.fr),
Source[3]: Germany supports Ukraine's efforts to rebuild power grid | BMZ
Source[4]: https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf

3. NOTEWORTHY UPDATE

ENISA 7TH biannual Cyber Europe exercise focused on EU Energy Sector

In June 2024, the European Union Agency for Cybersecurity (ENISA) held its 7th biannual Cyber Europe exercise. Due to the increasing attacks on the energy sector both globally and within Europe since 2017, this year's exercise focused on the energy sector and was intended to help identify weaknesses in the European Union's energy infrastructure to prepare defenders for future threat scenarios. The event simulated a cyber threat to the EU energy sector based on ongoing political tensions between the EU and a hypothetical foreign nation, highlighting the need for increased cybersecurity awareness among key stakeholders in the energy sector. Following the exercise, an analytical report will be produced and disseminated providing updated guidance on how to best strengthen the resilience of the EU energy sector.

Sources

Source[1]: https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme
Source[2]: https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme/cyber-europe-2024
Source[3]: https://energy.ec.europa.eu/news/pan-european-exercise-foster-preparedness-case-large-scale-cyber-attacks-energy-sector-2024-06-20

4. SPOTLIGHT ON VULNERABILITIES

Multiple vulnerabilities identified in Siemens grid sensors

Product Name	Date Disclosed	CVSS	POC Available	0-day Exploited
Siemens Sicam A8000, EGS grid sensors and Sicam 8	01/07/2024	HIGH: 8.6	Yes	No

In May 2024, Siemens identified two high-severity and one medium-severity vulnerabilities in its Sicam products that could be exploited in attacks aimed at the energy sector. The vulnerabilities affect Sicam A8000 remote terminal unit, Sicam EGS grid sensors and Sicam 8 power automation software. CVE-2024-31484 is a buffer overread issue that can lead to arbitrary code execution and allow an attacker to read sensitive data from memory. CVE-2024-31485 is a command injection issue in the products interface and CVE-2024-31486 is related to MQTT client passwords. All the impacted products are power grid solutions designed for substation automation.

Observed Usage

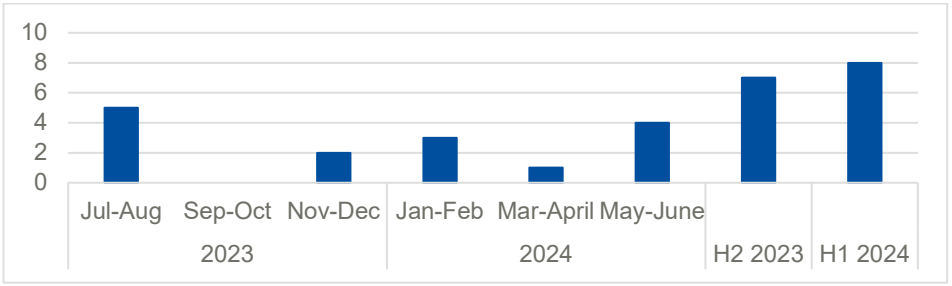
One of the vulnerabilities, CVE-2024-31484, was identified and disclosed to Siemens over a year ago; however, no known indication of prior exploitation has thusfar been reported. In order to exploit these vulnerabilities, an attacker needs to first gain network-level access on port 443/80 in order to interact with the target. By abusing CVE-2024-31484, information from the global memory segment can be compromised and used to aid further operations. So far, no proof-of-concept exploit code has been made public for any of the vulnerabilities detailed.

Sources

Source[1]: https://cert-portal.siemens.com/productcert/html/ssa-871704.html
Source[2] : https://www.securityweek.com/siemens-sicam-vulnerabilities-could-facilitate-attacks-on-energy-sector/
Source[3] : https://seclists.org/fulldisclosure/2024/Jul/4

5. SPOTLIGHT ON RANSOMWARE[1]

EU Energy Sector Ransomware Listings H2 2023-H1 2024

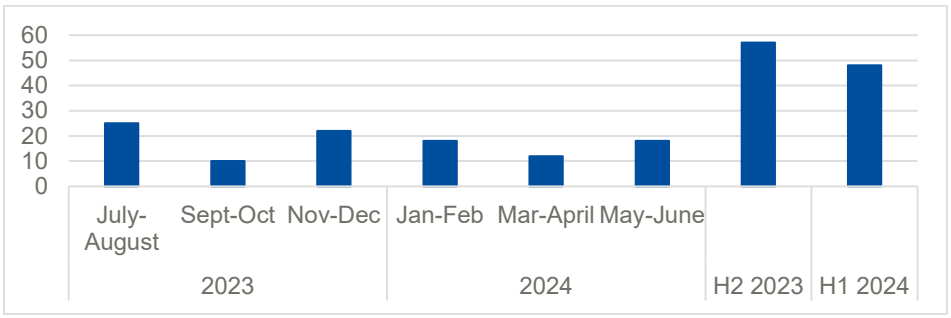


Short-term Trend

Following a relative decline in data leak site activity impacting the EU energy sector in Mar-Apr 2024, the number of observed listings in May-Jun 2024 increased to its highest level since Jul-Aug 2023. Overall, however, the volume of ransomware leak site activity during H1 2024 only saw a small increase in the number of EU-based ransomware victims relative to H2 2023.

However, EU organisations made up 22% of all ransomware listings affecting entities in the sector during the May-June reporting period. This represents a higher percentage compared to the first half of 2024, when EU-based energy victims accounted for only 17% of all known sector-related incidents.This also represents an increase from the 12% recorded during H2 2023, suggesting that Europe is likely a priority geography for threat actors targeting the energy sector.

Global Energy Sector Ransomware Listings H2 2023-H1 2024



Short-term Trend

Similarly, the number of global incidents increased relative to the prior reporting period, from 12 to 18. The number of global incidents notably decreased between H2 2023 and H1 2024, likely as a result of the takedown operations targeting LockBit ransomware in February 2024 and the self-imposed takedown of Blackcat (ALPHV)'s Tor-based website the following March. Both factors likely contributed to the short-term decrease in overall ransomware leak site activity, as affiliates had to establish relationships with alternative RaaS operators.

[1] This data is based on observed listings published to ransomware operator dark web leak sites.

6. RELEVANT INCIDENTS

Hunt3r Kill3rs allegedly compromise Schneider Electric PowerLogic terminals

Geography	Event noted on	Sector	Threat actor	Threat type
Germany	20/05/2024	Energy	Hunt3rs Kill3rs	Data Theft/Disruption

In late May 2024, the Russian-speaking Hunt3r Kill3rs hacktivist persona claimed to have compromised the multinational energy management conglomerate Schneider Electric. In a series of posts published to the actor's Telegram channel (@Hunt3rkill3rs1) since May 20, 2024, the actor claimed to have taken control of "many" of the company's PowerLogic systems and published screenshots appearing to show the web portals of several Schneider Electric PowerLogic systems including the PowerLogic ION7650 Enterprise Energy Mangement (EEM) software, an energy management solution used in power grid operations as well as the PowerLogic EGX100, an ethernet gateway used to transmit power-monitoring information. The screenshots also show what appear to be modified control settings on the impacted terminals.

Analyst comment

Active since at least April 2024, Hunt3r Kill3rs is a primarily Russian-speaking hacktivist persona known for alleged data breaches, historically targeting Israeli entities in the government, manufacturing, and energy sectors. Despite their focus on Israel and amplification of known Iran-linked personas like @CyberAveng3rs, Hunt3rKill3rs predominantly operates in Russian and closely collaborates with other Russian-affiliated Telegram personas, including those believed to have ties to Russian intelligence services, such as @CyberArmyofRussia_Reborn.

One of Hunt3Kill3rs' recent posts specified the reason for their alleged activity targeting Schneider Electric to be Germany's ongoing support for NATO; however, based on analysis of the screenshots provided, the device times indicated on the allegedly targeted PowerLogic ION7650 terminals appear in GMT+3:00 and GMT-8:00, indicating that the terminals presented by the threat actor are likely not located in Germany, which was on GMT+2:00 during the time of the alleged attacks. At the time of reporting, the validity and potential impact of the claimed activity remain unconfirmed and Schneider Electric has made no official statement concerning the actor's claims. However, there is a realistic possibility that these are legitimate, given that PowerLogic ION and EGX systems may be trivially accessible via the use of default credentials if said systems are exposed to the public internet and improperly configured [see Section 2.1 High Level Trends].

Sources

Source[1]: https://www.rewterz.com/threat-advisory/hunt3r-kill3rs-group-claims-to-breach-german-schneider-electric-systems
Source[2]: https://socradar.io/dark-web-profile-hunt3r-kill3rs/
Source[3]: https://t.me/Hunt3rkill3rs1/469
Source[4]: https://t.me/Hunt3rkill3rs1/484
Source[5]: https://t.me/Hunt3rkill3rs1/491
Source[6]: https://t.me/Hunt3rkill3rs1/502
Source[7]: https://www.se.com/us/en/faqs/FA272266/

LAPSUS$ group allegedly leaked the database of French multinational Engie SA

Geography	Event noted on	Sector	Threat actor	Threat type
France	05/05/2024	Energy	Unknown/Unconfirmed	Data Breach

On May 5, 2024, a Telegram channel named 'LAPSUS$' posted a screenshot suggesting it had compromised the French energy company ENGIE. The dataset compromised includes data such as names, addresses, appointment dates, types of equipment installed etc. The dataset compromised appears to contain over 1,300 names and includes details such as full names, addresses, order request dates, and types of equipment installed.

Analyst comment

Headquartered in France, ENGIE is one of the largest energy suppliers in France. At the time of writing, ENGIE has not confirmed the validity of the actor's data breach claims or of any compromise of its systems or networks. It is also unclear whether the Telegram channel has any links to the LAPSUS$ cybercrime group or any of its members. For reference, LAPSUS$ gained notoriety in 2022 for its members' involvement in several high-profile attacks on organisations such as Okta, Microsoft and Uber. The original LAPSUS$ channel was shut down and its core members were convicted in a UK court in 2023. In the absence of evidence linking the two personas, however, there is a realistic possibility that the individuals operating the Telegram channel are not affiliated with the original group and are using the name to gain attention by capitalising on LAPSUS$'s notoriety.

Sources

Source [1]: https://t.me/GroupLapsus/234
Source [2]: https://www.clubic.com/actualite-526124-engie-un-groupe-de-hackers-revendique-le-piratage-de-donnees-sensibles-de-clients-du-fournisseur-d-energie.html

German energy solutions company HOPPECKE hit by DragonForce ransomware

Geography	Event noted on	Sector	Threat actor	Threat type
Germany	08/06/2024	Energy	DragonForce	Ransomware

On 08 June 2024, targeted the German energy solutions company HOPPECKE with a ransomware operation by DragonForce. DragonForce is a relatively new and highly aggressive ransomware strain, and during operations the group employ double extortion tactics. The group claimed to have accessed 25.33GB of sensitive dtaa belonging to the company and at the time of their post, planned to publish the data within 14 days; in previous operations the group has followed this extortion tactic.

Analyst comment

HOPPECKE specialises in energy storage solutions and manufactures industrial battery systems. The company is headquarted in Germany but employees over 2,000 people worldwide and operates in 150 countries via 23 international subsidiaries. The company's products are used by a variety of industries including railway systems, renewable energy and for backup power for critical infrastructure. The loss of data and disruption to the company's production likely poses a significnat risk to their company reputation and client trust, the length of downtime also highly likely impacted the company's financial gain over the period. DragonForce has also been linked to the use of a leaked ransomware builder, previously used by ransomware group LockBit, indicating a trend of ransomware operators repurposing existing malware tools.

Sources

Source[1]: https://ransomwareattacks.halcyon.ai/attacks/dragonforce-ransomware-halts-hoppecke-battery-production

Data of 850,000 Spanish Electricity Supplier Iberdrola Customers Up for Sale

Geography	Event noted on	Sector	Threat actor	Threat type
France	05/05/2024 – 07/05/2024	Energy	Unknown/Unconfirmed	Data Breach

Between May 5 and 7, 2024, the data of 850,000 Iberdrola customers was stolen in a cyber attack, representing about 8% of its users. According to Iberdrola, the attackers accessed customer data by breaching one of the files where it was stored. The stolen data does not include passwords, personal codes, or account numbers, but it does contain full names, email addresses, and ID numbers. Of the 850,000 stolen records, 600,000 were taken directly from the company, and 250,000 were accessed via the marketing company Curenergía.

Analyst comment

The company has informed its customers about the breach and advised them to be vigilant of emails and messages from unknown senders. Due to the breach, gaining access to some customer information increases the likelihood of secondary breaches. This attack aligns with the current trend of compromises against EU organizations in countries that have supported Ukraine during the Russia-Ukraine conflict. As the conflict continues, such operations are likely to persist.

Sources

Source[1]: https://www.surinenglish.com/spain/the-data-850000-iberdrola-customers-stolen-cyberattack-20240530083933-nt.html
Source[2]: https://air-institute.com/blog/2024/07/13/iberdrola-and-santander-victims-cybercrime

British Multinational oil and gas giant Shell targeted by 888 In Data Breach

Geography	Event noted on	Sector	Threat actor	Threat type
Britain	29/05/2024	Energy	888	Data Breach

The cybercriminal group 888 has claimed to have targeted oil and gas giant Shell in a data breach operation, that saw around 80,000 of Shell's customer's private data breached. The customers are allegedly from around the world with the affected countries listed on 888's leak site as the UK, Australia, France, India, Singapore, Phillippines, Netherlands, Malaysia and Canada. The dataset allegedly contains sensitive information including, first names, last names, email addresses, phone numbers, home addresses, login credentials and phone numbers.

Analyst comment

Shell have received much criticism from climate activists and by social media users in recent years due to the company's impact on the environment, making them a more attractive target to both hacktivist groups and financially-motivated cybercriminal groups looking to ransom either system access or sensitive data. According to Shell, the data breach was allegedly caused by a third-party that experienced a cybersecurity incident; this incident exposed the data that the third-party stored on a platform. The incident also highlights that securing third-party supplier access and shared data is of utmost importance in security procedures when protecting sensitive data.

Sources

Source[1]: https://cybernews.com/news/shells-customer-data-leak/
Source[2]: https://dailysecurityreview.com/security-spotlight/shell-data-breach

Black Basta Target US Oil Company Atlas Oil in Ransomware Attack

Geography	Event noted on	Sector	Threat actor	Threat type
Global	20/05/2024	Energy	Black Basta	Ransomware

On 20 May 2024, it was reported that the US oil company Atlas Oil was the victim of a ransomware attack conducted by Black Basta. Active since early 2022, the Black Basta ransomware-as-a-service (RaaS) operation is known for its double extortion tactics. The group has been linked to other cybercriminal groups including FIN7 and has targeted a wide-range of organisations globally, particularly North America, Europe and Australia. Black Basta claimed to have exfiltrated 730 GB of sensitive data from Atlas Oil's systems, and was focused on corporate data. Allegedly the dataset contained user and employee data including; data sheets, payroll, ID cards and information from accounts, human resources, finance and executive departments.

Analyst comment

Atlas Oil is one of the largest national fuel distributors in the United States (US), with its services feeding into 49 of the 50 US states. The company distributes over one billion gallons of oil per year and its victimisation demonstrates the continued vulnerability of critical infrastructure to ransomware threats. Considering the company's size and advanced technologies, this breach demonstrates that even industry leaders are at risk of sophisticated cyber threats.

Sources

Source[1]: https://ransomwareattacks.halcyon.ai/attacks/black-basta-ransomware-attack-on-atlas-oil-implications-and-response
Source[2]: https://securityaffairs.com/163489/cyber-crime/blackbasta-claims-atlas-hack.html

7. OTHER NOTEWORTHY EVENTS

Major grid incident affects Continental Europe power system

On June 21, 2024, a significant grid incident occurred in the South-Eastern part of the Continental Europe power system. This incident led to a blackout in the electricity grids of Albania, Montenegro, and Bosnia-Herzegovina, as well as a partial blackout in Croatia. The affected Transmission System Operators (TSOs), with support from neighboring TSOs, restored power to their grids within about two hours, aiming to minimize the impact of the disruption on consumers.

Sources
Source[1]: https://www.entsoe.eu/news/2024/06/21/grid-incident-report-south-eastern-part-of-the-continental-europe-power-system/

Baltic TSOs have sent a notice on decoupling from Russia-controlled electricity system in February 2025

Elering, AST, and Litgrid, the electricity transmission system operators of Estonia, Latvia, and Lithuania, have informed Russian and Belarusian operators that they will not extend the BRELL agreement, which is set to expire in February 2025. At that time, the Baltic states will disconnect from the Russian-controlled IPS/UPS system and join the Continental Europe Synchronous Area. The Baltic states are prepared for emergency synchronisation and have undertaken infrastructure projects to support this transition. The EU is providing €1.2 billion in funding to support this effort.

Sources
Source[1] : https://www.litgrid.eu/index.php/news-events-/news/baltic-tsos-have-sent-a-notice-on-decoupling-from-russia-controlled-electricity-system-in-february-2025/32852

Ukrainian energy sector experiences blackouts after Russian military attacks

On 04 June 2024, it was reported that imports of electricity will continue in Ukraine due to the increased physical attacks from Russia. Attacks have included missile and drone operations and their frequency has increased significantly since March this year. Repairs to one of the lines that connects Ukraine to the European energy system are ongoing, however, blackouts in many regions have continued. Large-scale blackouts have led to increased electricity imports from European Union nations. Previous electricity imports have come from nations including Romania, Poland, Hungary, Moldova and Slovakia.

Sources
Source[1]: https://www.reuters.com/business/energy/ukraines-electricity-imports-remain-high-even-power-line-undergoes-repairs-2024-06-04/
Source[2]: https://www.nytimes.com/2024/06/05/world/europe/ukraine-energy-blackouts-summer-i.html

LilacSquid data theft campaign targets European energy entities

On May 30, 2024, a report was published by Cisco Talos regarding observed data theft activity attributed to a newly identified threat group dubbed LilacSquid. According to Cisco Talos researchers, LilacSquid's victimology is diverse and includes EU-based energy sector entities, pharmaceutical companies in Asia and information technology firms known to work with the US reserach and industrial sectors. The campaign also featured the post-exploitation use of an open-source remote management tool named MeshAgent and a customised version of the QuasarRAT dubbed PurpleInk. Although Cisco Talos researchers do not currently attribute LilacSquid to any known threat group or state sponsor, it is worth noting that many of the tactics, techniques, and procedures (TTPs) used in the observed campaign—such as the use of MeshAgent for maintaining post-compromise access—overlap with those employed by groups linked to the Democratic People's Republic of Korea (DPRK), including Andariel and its parent group Lazarus.

Sources

Source[1] : https://blog.talosintelligence.com/lilacsquid/

8. BIMONTHLY THREAT SPOTLIGHT

China-Nexus UNC3886 observed leveraging zero-day exploits and custom tooling

Operation Summary

- On June 18, 2024, Google's Mandiant published a blog post detailing recently observed malicious activity linked to the China-nexus threat actor Mandiant tracks as UNC3886. Active since at least 2021, UNC3886 is known for targeting organisations in the energy and utility sectors, aerospace, defense, government etc.
- Notable tactics seen leveraged in UNC3886 operations include the frequent exploitation of zero-day vulnerabilities in edge infrastructure for initial access, the use of publicly available rootkits (i.e., REPTILE and MEDUSA) for long-term persistence and the deployment of malware leveraging trusted third parties such as GitHub and Google Drive for C2 and data exfiltration.
- UNC3886 was also observed leveraging multiple zero-day flaws including CVE-2022-41328 (Fortinet FortiOS), CVE-2022-22948 (VMWare vCenter) and CVE-2023-20867 (VMWare Tools). During certain intrusions, UNC3886 operators were seen chaining multiple vulnerabilities together to support lateral movement and code execution tasks when obtaining and abusing credentials of existing accounts proved infeasible. While many China-nexus threat actors have been observed leveraging zero-day vulnerabilities in public facing edge infrastructure for initial access, UNC3886's ability to chain several zero-day vulnerabilities in a single operation may indicate a higher degree of resourcing and capability available to the actor relative to other China-nexus threat actors.

TTP Overview

Initial Access:

- **Exploit Public-Facing Application (T1190).** UNC3886 exploits n-day and zero-day vulnerabilities in public-facing applications (e.g., VMWare and Fortinet) for initial access, lateral movement and code execution.
- **Valid Accounts (T1078).** UNC3886 utilises valid accounts for initial access and lateral movement.

Credential Access and Lateral Movement:

- **Keylogging (T1056.001).** UNC3886 conducts keylogging activity to intercept credentials as users type them; using these credentials the group can gain access to target systems.
- **Remote Services (T1021).** The group leverages valid account access to access services that allow for remote connections including SSH (Secure Shell) to conduct lateral movement activities.

Malware & Tooling

- Reptile – publicly available rootkit
- Medusa – publicly available rootkit
- SEAELF - installer
- MOPSLED - backdoor
- RIFLESPINE - backdoor

Capability

UNC3886 is a state-sponsored Chinese-nexus threat group known for exploiting zero-days in vulnerable software for initial access. The group is assessed to maintain a high level of capability and access to resources, often using custom malware and tooling in its operations.

Motivation

Espionage and data theft.

Threat

HIGH

Sources

Source [1] : https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

9. RECOMMENDATIONS BASED ON OBSERVED ACTIVITY

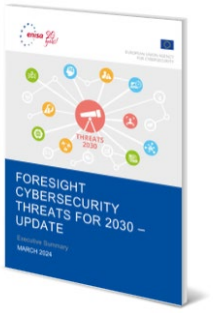
To reduce the risk and impact of potential future cyberattacks, the following practices are advised:

- **Mitigating vulnerability exploitation (T1190):** N-day and zero-day vulnerabilities continue to be a leading cause of compromise for organisations across a range of sectors and industry verticals. The following practices are recommended to mitigate the impact of such intrusions:
  - **Prioritise Remediation of Vulnerabilities on Internet-facing Systems (M1016):** This can be done by conducting automated and/or routine vulnerability scans.
  - **Update Software (M1051):** Follow a routine patching cycle for all operating systems, applications and software (including all third-party software) to limit the potential for exploitation.
- **Mitigating remote services exploitation (T1021):** Threat actors have been observed targeting remote services including Secure Shell (SSH) services using valid accounts. This allows an unauthorised or malicious actors to perform actions as the logged-on user. To reduce the impact of such intrusions, the following practices are recommended:
  - **Multi-factor Authentication (M1032):** Wherever possible, organisations should require multi-factor authentication for SSH connections such as password protected SSH keys.
  - **User Account Management (M1018):** Organisations should also, where possible, limit which user accounts are allowed to login via SSH.
- **Mitigating attacks targeting vulnerable public facing services (T1190):** Although a majority of the potentially vulnerable platforms utilised in ICS contexts are traditionally isolated from the open internet, energy sector entities are nonetheless susceptible to attempts by threat actors to exploit public facing applications or appliances as a means of gaining initial access to their environments. Particular attention should be paid to third-party suppliers and systems used by organisations to support remote working activities such as, cloud services. The below mitigation steps are presented as a means of improving the security posture of an organisation to such attacks:
  - **Update Software (M1051):** Organisations should implement routine software updates and vulnerability scans 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 through the verification of unmaintained and/or previously vulnerable dependencies and the disablement of unnecessary features, components and files.
  - **Multi-factor Authentication (M1032):** Wherever possible, organisations should extend multi-factor authentication protection to all terminals and accounts with access to OT systems. Said systems should also be disconnected from the public-facing internet wherever feasible.
  - **Network Segmentation (M1030):** Given the extant risk of n-day and zero-day vulnerability exploitation of network edge devices used in ICS settings, it is critical that infrastructure operators practice comprehensive network segmentation to prevent lateral movement from potentially exposed assets to sensitive devices or infrastructure elements. To do so, all externally facing servers and infrastructure should ideally be physically or logically separated from the rest of the operational network, either via the use of a DMZ or on separate hosting infrastructure.

10. SUGGESTED READINGS FROM ENISA

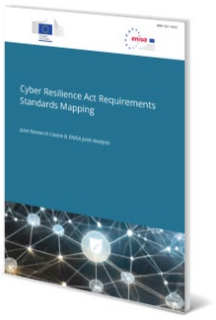
Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report

This is the second iteration of the “ENISA Foresight Cybersecurity Threats for 2030” study that represents a comprehensive analysis and assessment of emerging cybersecurity threats projected for the year 2030. The report reassesses the previously identified top ten threats and respective trends whilst exploring the developments over the course of a year.



Cyber Resilience Act Requirements Standards Mapping
- Joint Research Centre & ENISA Joint Analysis

To facilitate adoption of the CRA provisions, these requirements need to be translated into the form of harmonised standards, with which manufacturers can comply. In support of the standardisation effort, this study attempts to identify the most relevant existing cybersecurity standards for each CRA requirement, analyses the coverage already offered on the intended scope of the requirement and highlights possible gaps to be addressed.



ANNEX A – TERMINOLOGY

THREAT LEVEL ASSESSMENT

As of July 2024, this report employs the following five levels to communicate threat assessments. The threat levels are determined through an evaluation of key actor activity and an analysis of recently exposed vulnerabilities and exploits (Opportunity). This analysis is conducted monthly and integrates multiple intelligence sources.

THREAT LEVEL		MEANING
	LOW	A low likelihood of threat actor targeting activity that could affect organisations/entities in highly critical or other critical sectors. Disruption is considered highly unlikely.
	MODERATE	There is potential for some direct targeted threat actor activity but it is generally considered unlikely. This activity could lead to some disruption across multiple countries.
	SUBSTANTIAL	It is likely entities are being directly targeted by threat actors or could be exposed to breaches using recent discovered vulnerabilities. Serious disruptions of operators of essential services are considered a realistic possibility.
	SEVERE	It is likely that entities will be directly targeted by threat actors. Multiple entities will be, or are being, impacted. Essential operators or severe disruption are expected to be widespread, across multiple countries.
	CRITICAL	It is highly likely organisations are targeted by highly sophisticated and persistent threat actors with a clear intent to cause societal harm. High severity vulnerabilities with no known remediation are being exploited and significant damage and outages are being across multiple countries.

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

LEGAL NOTICE

COPYRIGHT NOTICE

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