TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SECTORIAL THREAT LANDSCAPE

PUBLIC ADMINISTRATION

NOVEMBER 2025

About ENISA

The European Union Agency for Cybersecurity, ENISA, is 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 the 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

Ilias BAKATSIS, ENISA.

CONTRIBUTORS

Jamila BOUTEMEUR, ENISA.

ACKNOWLDGEMENTS

The ENISA Sectorial Threat Landscape authors would like to thank ENISA colleagues Apostolos MALATRAS, Razvan GAVRILA, and Eleni PHILIPPOU as well as the EU ISAC for Cities (I4C+), for their support, review, and feedback on the report.

ISBN 978-92-9204-724-5, DOI 10.2824/4606183

Table of Contents

Executive Summary

This ENISA sectorial threat landscape report provides an overview of the cyber threats faced by the public administration sector in the EU in 2024. Drawing on open-source information, the report highlights the key threats that impacted the sector and provides insights into typical threat types and key adversaries, to support the sector's ongoing efforts to improve its cybersecurity posture, maturity and resilience.

Key points identified for the sector include:

- Ransomware incidents constituted 10% of the total, causing some service disruptions.
- Data-related threats, representing almost one in five incidents, targeted sensitive platforms such as employment services and law enforcement portals.
- Distributed Denial-of-Service (DDoS) attacks, which accounted for nearly two-thirds of incidents, primarily affected ministerial and municipal websites.
- DDoS attacks were the most common threat type, with pro-Russia hacktivist group NoName057(16) responsible for 46% of such attacks. Often linked to geopolitical events, such as EU support for Ukraine, notable spikes in DDoS attacks were observed in July and December.

Data-related threats included breaches and leaks and had significant impacts on public administration entities. Data breaches accounted for 17.4% and data leaks for 1% of collected incidents, with a surge in incidents observed in the last quarter of 2024, accounting for over 40% of all data-related events. Ransomware attacks were prevalent, often involving unauthorised access to sensitive data.

The public administration sector in the EU faces significant cyber threats from various adversaries, with hacktivism being the most prevalent in sheer volume. In 2024, hacktivists accounted for nearly 63% of incidents, while cybercrime operators and state-nexus intrusion sets represented approximately 16% and 2.5%, respectively.

Hacktivist activities in 2024 were primarily driven by ideological motivations linked to geopolitical events, such as Russia's war of aggression against Ukraine. Groups like NoName057(16) and Anonymous Sudan targeted governmental portals and local administrations across EU Member States.

Cybercrime operators continued leveraging ransomware-as-a-service (RaaS) models, leading to operational disruptions in the public administration sector in the EU. Ransomware attacks remained opportunistic, with limited volume but notable disruptions. Ransomware incidents represented about 10% of total events. Ransomware-as-a-Service (RaaS) programs were commonly used, with notable strains deployed against the public administration sector in the EU including RansomHub and LockBit3.0.

State-nexus intrusion sets publicly documented as associated to Russia and China were active in cyberespionage campaigns against the public administration in the EU, notably targeting governmental entities.

Looking forward, given the sector's low maturity and being identified as a potentially high-value target, the public administration sector in the EU is highly likely to remain a target in the mid-to-long term. Hacktivist-led DDoS activity is expected to persist around noteworthy geopolitical events, while state-nexus intrusion sets will probably continue carrying out long-term cyberespionage campaigns. Opportunistic ransomware and data breaches are likely to continue to impact business continuity, and lead to reputational damage.

1. Introduction

This is the first report by the European Union Agency for Cybersecurity (ENISA) on a public administration sectorial threat landscape. It reveals insights into cyber threats targeting the public administration sector in the EU. This sector plays a critical role in delivering essential services to European citizens and is designated as a high-criticality sector under the NIS2 Directive[1].

In 2023, EU general government expenditure represented 49.0% of Gross Domestic Product (GDP), highlighting the economic weight of this sector and underscoring its importance[2]. As public administration entities manage large amounts of sensitive data and provide critical services, the cyber threats they face have a potential to disrupt essential services, ultimately having an impact on national security and possibly undermining public trust. Based on the ENISA NIS360 report[3], despite its role in ensuring effective governance and the delivery of services to civil society, the public administrations sector is among the least mature of the sectors that were assessed and is classified within the 'risk zone'. This highlights the fact that significant work remains to be done and that the sector needs greater support to improve its cyber maturity in line with its criticality. The same report highlights the need to strengthen cyber situational awareness within the sector to improve its understanding of the threats faced by public administration. In this context, our report aims to address this gap by providing an overview of the threats faced by this sector in the cyber domain, and thus to support risk assessment, defensive measures and relevant policy-making.

According to the *ENISA Threat Landscape 2025 report*, public administration is the most targeted sector in the EU, accounting for 38,2% of all identified incidents[4]. Threats faced by the public administration sector notably include Distributed Denial of Service (DDoS) attacks, data-related threats and incidents involving social engineering.

Reporting period. In this report, ENISA analysed cyber incidents targeting the public administration sector in the EU from January to December 2024. This period is referred to as the 'reporting period' throughout this document.

Scope. Data collection and analysis focused on cyber incidents[5] observed in EU Member States (EU MSs). ENISA collected publicly reported cyber incidents affecting the following types of organisations related to public administration, in accordance with the definition[6] in the NIS2 Directive:

- Public administration entities at the central government level, as defined by each Member State;
- Public administration entities at the regional level, as defined by each Member State based on risk assessments, provided the services they offer are critical to societal or economic stability;

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1744178176020#anx_I.
[2] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_expenditure_by_function_%E2%80%93_COFOG#EU_general_government_expenditure_stood_at_49.0.25_of_GDP_in_2023.
[3] https://www.enisa.europa.eu/publications/enisa-nis360-2024.
[4] ENISA, *ENISA Threat Landscape 2025 – July 2024 to June 2025*, 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
[5] Unauthorised access to an information system, usually but not exclusively for malicious purposes.
[6] https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2.

- Local public administration entities, which Member States may choose to include within the Directive's scope.

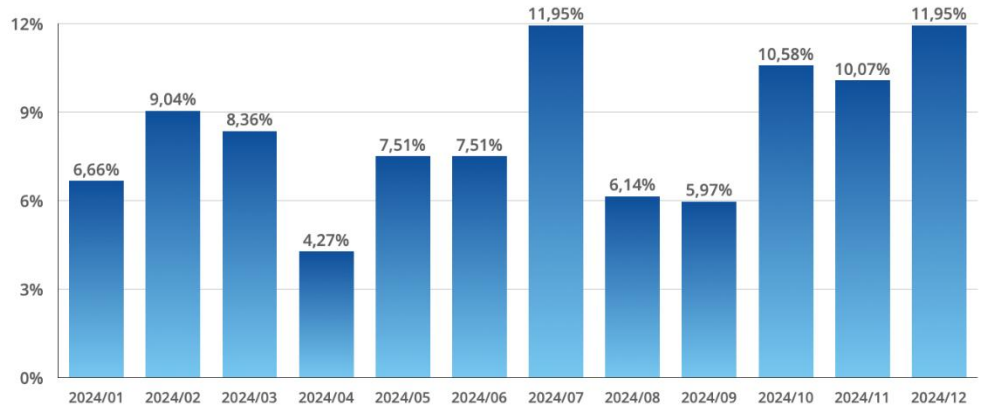
Methodology. To draft this report, ENISA collected a list of cyber incidents based on open sources[7], in alignment with the updated *ENISA Cybersecurity Threat Landscape Methodology* [8]. Identified incidents serve as the foundation for highlighting a list of primary threats and are the source material for statistics in the report. Based on the hereabove delineated scope, and as not all incidents are reported in open sources, numbers reported in this document are almost certainly different from the numbers observed by EU MS National authorities. The objective of this report is to identify trends and provide assessments, conveyed using estimative language[9]. With the inclusion of public administration under the NIS2 Directive, improved visibility is expected through the mandatory reporting procedure.

[7] This is a result of the work done by ENISA in the area of situational awareness in accordance with the EU Cybersecurity Act, Article 7(6): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.
[8] ENISA, ENISA Cybersecurity Threat Landscape Methodology – August 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology.
[9] See appendix.
.

2. Threat Landscape Overview

From January to December 2024, ENISA analysed **a total of 586 publicly reported cyber incidents** targeting public administration in the EU.

Figure 1: Number of incidents identified in 2024



On average, each month accounted for approximately 8.33% of the yearly total, with monthly shares ranging from a low of 4.27% in April to a high of 11.95% in July and December. Observed increases in July and December were notably driven by the geopolitical context at the time, as detailed later in the report (see Section Primary Threats).

Figure 2: Incidents per public administration subsectors in 2024

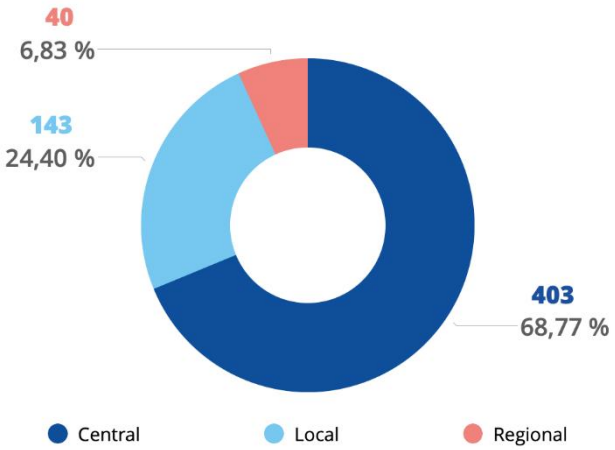


Figure 2 shows the number of incidents observed across EU MSs public administration entities during the reporting period for each subsector. The majority of the targeted public administration entities are

from central government with almost 69%. Local entities follow with 24%, while Regional is the least impacted, accounting for only 6.8% of the total number of incidents.

More than half of the incidents against central government entities targeted the websites of parliaments, ministries and national authorities or agencies, largely skewed by DDoS attacks, as shown in Figure 3.

Figure 3: Incidents per threat type by subsector

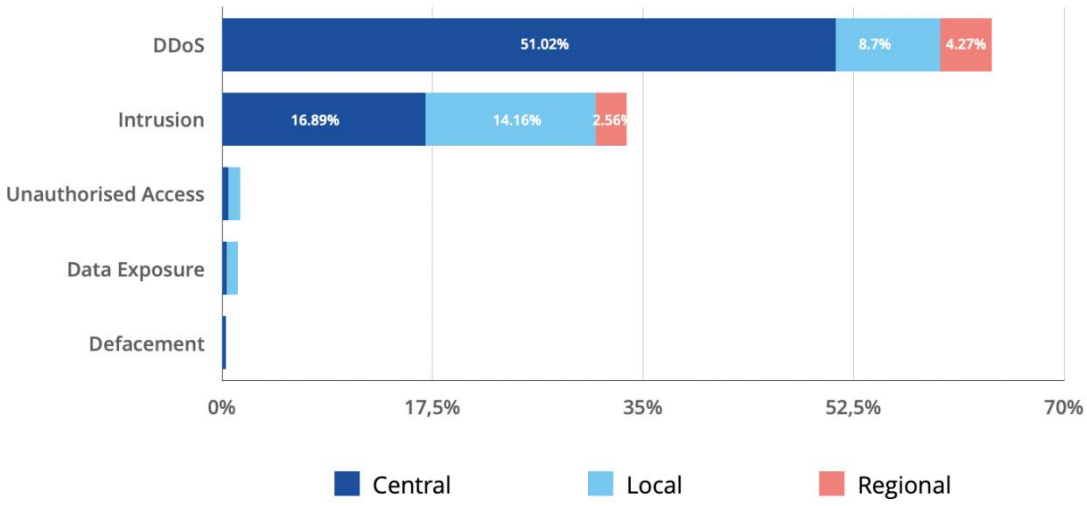
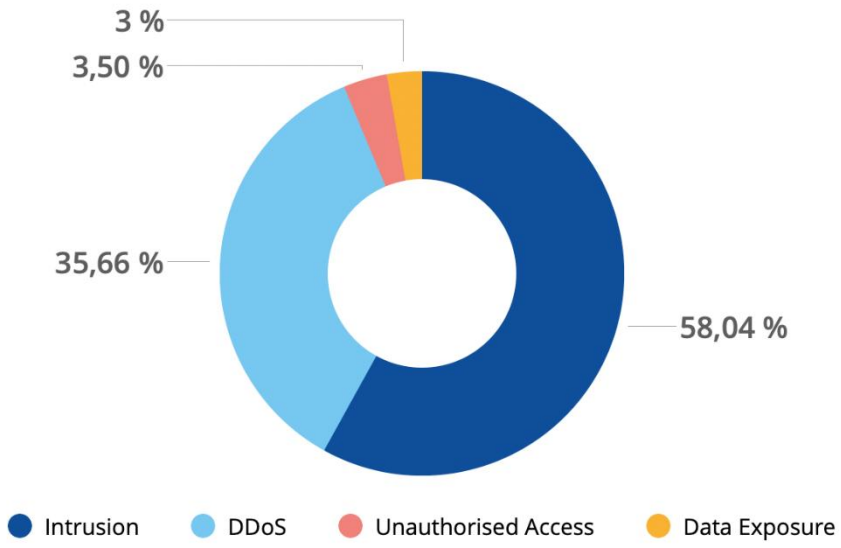
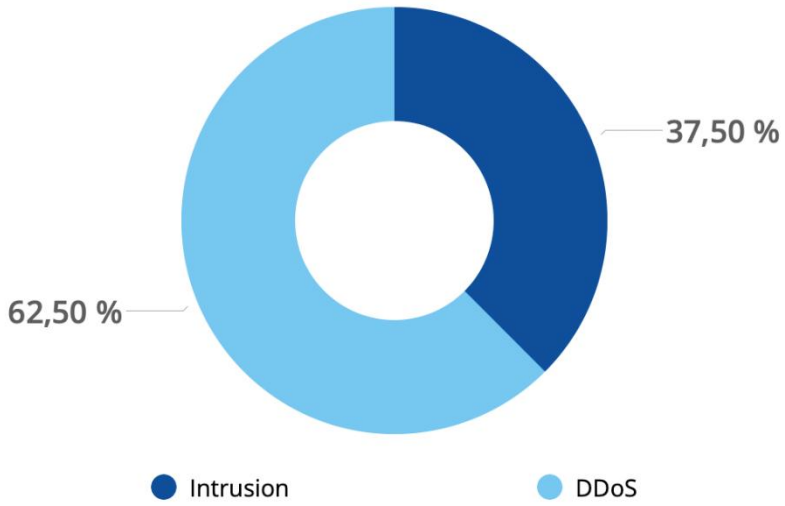


Figure 4: Incidents per threat type targeting local entities



Incidents against local entities are primarily intrusion-related (58%), followed by DDoS attacks (35%). Among local entities, municipalities were the most common target, accounting for almost 44% of incidents[10] [11] [12].

Figure 5: Incidents per threat type targeting regional entities



Regional entities were the least affected during the reporting period. Most of those incidents were DDoS attacks, accounting for more than 60%. Among regional entities, provincial websites were targeted most often, representing almost 33% of cases[13] [14] [15].

[10] https://www.valdereuil.fr/actualites/cyberattaque-sur-les-serveurs-de-la-mairie-la-ville-prend-des-mesures-pour-assurer-la-continuite-du-service-public.
[11] https://www.elbe-heide.de/news/1/987561/nachrichten/eingeschr%C3%A4nkte-erreichbarkeit-der-verwaltung-der-verbandsgemeinde-elbe-heide.html.
[12] https://www.unionesarda.it/news-sardegna/sassari-provincia/attacco-hacker-al-comune-di-sorso-sistema-informatico-in-tilt-chiesto-un-riscatto-per-il-ripristino-n4zd4imy.
[13] https://www.nu.nl/tech/6306531/cyberaanval-legt-websites-van-meerdere-provincies-plat.html.
[14] https://www.vid.gov.lv/lv/jaunums/informacija-wwwvidgovlv-lietotajiem-arvalstis.
[15] https://t.me/noname05716/6369.

Figure 6: Threat types observed in the public administration sector in the EU in 2024

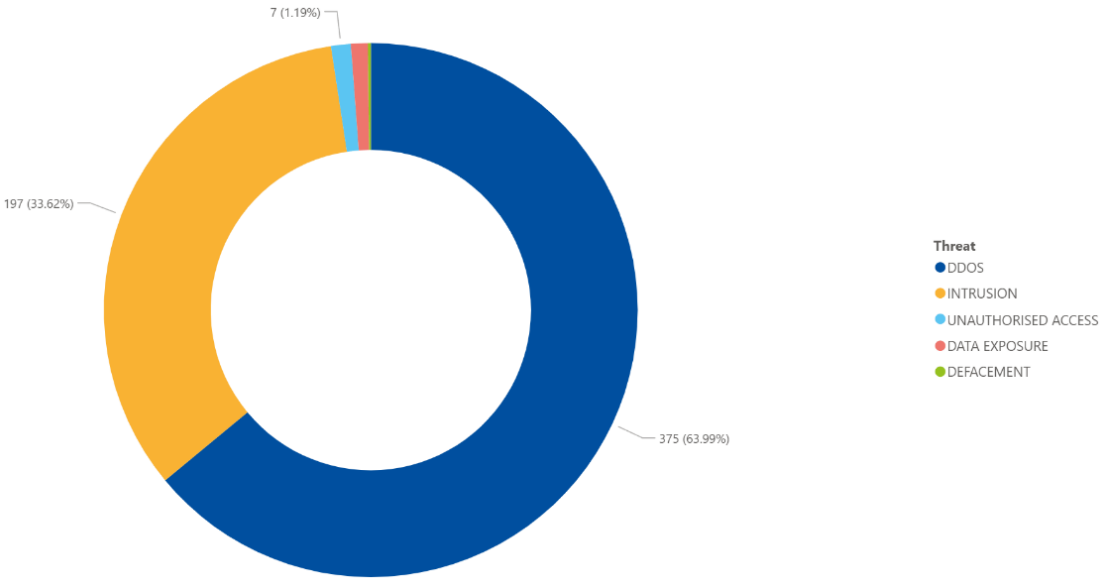
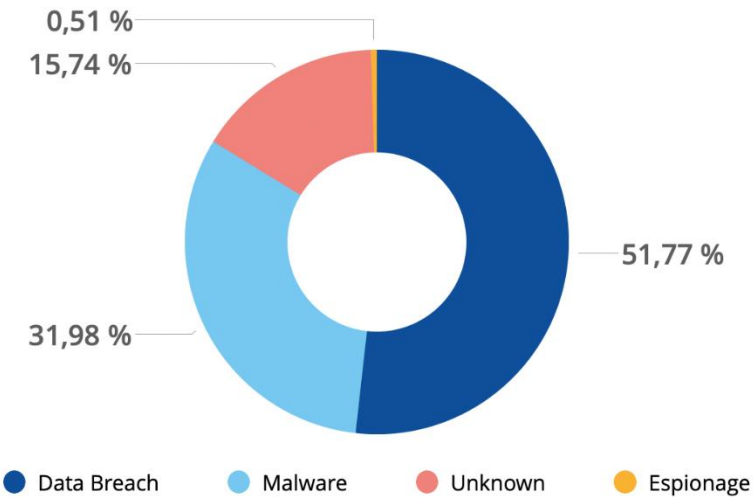


Figure 6: Threat types observed in the public administration sector in the EU in 2024provides a breakdown of the threat types that targeted the public administration sector in the EU during the reporting period. DDoS attacks accounted for over 60% of incidents. These attacks were typically short-lived and rarely resulted in significant impact. Data breaches and ransomware, though fewer in number, had higher impacts. Data breaches in some cases resulted in the unauthorised exposure of personal or operationally sensitive information, such as the incident involving leaked resident data from the Kehra municipality in Estonia[16]. On several occasions, ransomware attacks resulted in the disruption of services, as seen in the case of Calvià town hall in Spain[17]. Intrusion incidents included credential compromise, such as the case in the Lithuanian Central Procurement Information System (CVP IS)[18]. Despite fewer incidents, phishing is still a common initial access vector[19].

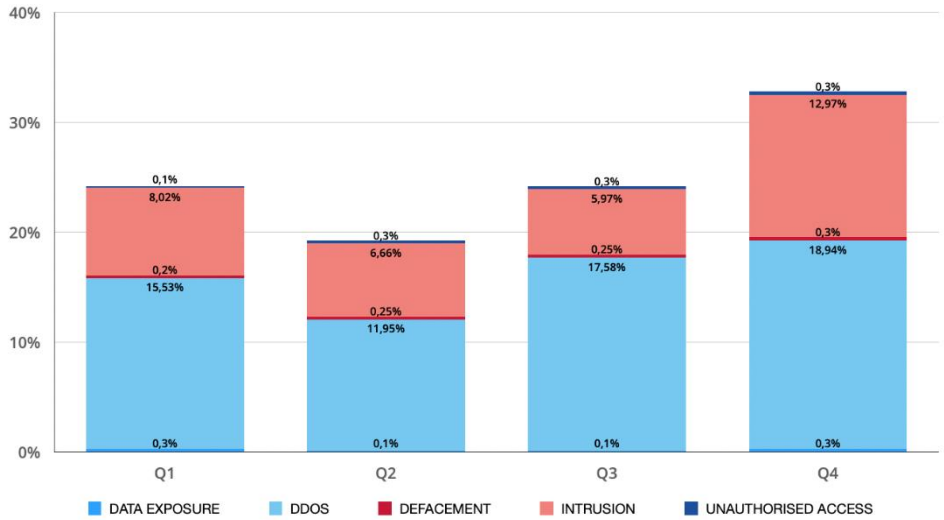
[16] https://www.postimees.ee/7951529/kehra-elanike-andmed-lekkisid-veebi.
[17] https://www.majorcadailybulletin.com/news/local/2024/03/04/122359/calvia-town-hall-cyberattack.html.
[18] https://vpt.lrv.lt/lt/naujienos-3/del-kibernetiniu-ataku-cvp-is-butina-skubiai-pasikeisti-savo-slaptazodzius-due-to-cyber-attacks-it-is-necessary-to-change-the-password-in-the-central-public-procurement-information-system-cvp-is/.
[19] https://www.csoonline.com/de/a/deutschlandweit-phishing-angriff-auf-ihk,4287685.html.

Figure 7: Intrusion-related incidents observed in the public administration sector in the EU in 2024



Within intrusion-related incidents affecting the public administration sector in the EU in 2024, data breaches accounted for the largest share (51.8%), followed by malware (~32%) and unclassified intrusions (15.7%). Espionage and other malware cases were marginal. While these figures describe the outcomes of successful compromises, information on initial access vectors is largely not available in the open sources. However, where details were available, phishing/social engineering and credential abuse were mentioned as initial access vectors, albeit in a limited number of cases.

Figure 8: Threats to the public administration sector in the EU in 2024, by number of incidents per threat type



In Figure 8, the differences between the threats observed are depicted on a quarterly basis. The distribution of threats across quarters remained relatively consistent, with a noticeable surge in Q4. Each quarter was characterised by prevalent DDoS activity.

In the following section, each type of the main threats identified are detailed further. All other threat types were recorded only occasionally, accounting for less than 1% of all incidents, which suggests either lower activity or limited OSINT visibility compared to the main categories.

3. Primary Threats

Of the 586 publicly reported cyber incidents targeting public administration in the EU that were identified over the reporting period, almost 64% were DDoS attacks and 33.6% were intrusion-related threats, including data breaches and ransomware cases.

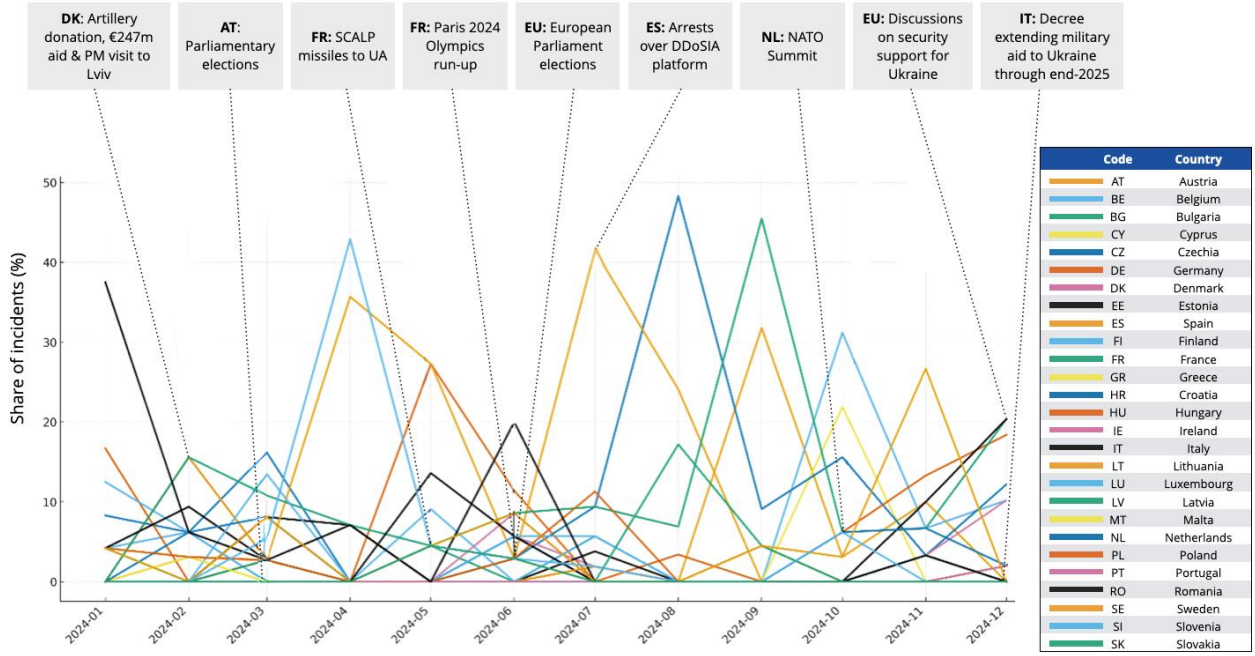
DISTRIBUTED DENIAL-OF-SERVICE ATTACKS (DDOS)

DDoS attacks can be carried out by exhausting a service and its resources or overloading the components of the network infrastructure. Users of a system or service are then not able to access relevant data, services or other resources. From a technical vantage point-of-view, most attacks leveraged Layer-7 HTTP request floods or UDP amplification[20]. This mirrors global telemetry as reported by multiple vendors, which recorded HTTP-layer floods in 51% to 59% of all mitigated attacks in 2024[21] [22]. While these incidents were often limited in scope, their timing and volume did, on some occasions, result in the disruption of services and temporary interruptions.

The systems most commonly affected included ministerial websites, municipal and regional portals, and public information systems. At the functional level, citizen-facing portals (appointment booking, taxation, customs, permit issuance) remained prime targets. A few incidents that were reported against Italian government domains, Swedish local authority portals, Latvian governmental websites and Germany's federal administration systems illustrate this trend[23] [24] [25] [26].

[20] More information about UDP amplification attacks is available here: https://www.cisa.gov/news-events/alerts/2014/01/17/udp-based-amplification-attacks.
[21] https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/.
[22] https://stormwall.network/resources/blog/ddos-attack-statistics-2024.
[23] Claimed attack on Italian government websites. https://t.me/noname05716/5592.
[24] Claimed attack on Swedish municipal portals. https://t.me/noname05716/5606.
[25] Attack on Latvian government and ports. https://t.me/noname05716/5616.
[26] Attack on German transport and public administration. https://t.me/noname05716/5629.

Figure 9: Contextualised DDoS against public administration



The majority (46%) of these attacks were claimed by pro-Russia hacktivist intrusion set NoName057(16) and can be contextualised in the geopolitical or political situation at the time. Of particular relevance was the EU support for Ukraine in the context of Russia's war of aggression against Ukraine, electoral processes at the EU level and high visibility events held within the EU. This is exemplified by the spikes identified in July with a noticeable wave of attacks on the websites of Spanish public institutions claimed by NoName057(16), concomitant to Spain's political and defence alignment and the arrests by Spanish authorities of three individuals suspected of using the DDoSIA platform[27] [28] [29] [30] [31]. Similarly, in December a DDoS campaign targeted French and Czech institutions, launched amid EU-level discussions on security support for Ukraine[32] [33], and Italy's cabinet decree to extend its military assistance to Ukraine through to the end of 2025[34] [35] [36].

Heightened hacktivist activity is frequently observed around election cycles. For example, during the European Parliament elections, HackNet claimed attacks against the website of the Ministry of Home

[27] Claims targeting Spanish municipal and government platforms. See for example: https://t.me/privetOTof222/137, https://t.me/h0lyleague/13, https://t.me/CyberArmyofRussia_Reborn/9017?single.
[28] https://www.reuters.com/world/europe/nato-members-agree-40-billion-euro-financial-pledge-ukraine-diplomats-say-2024-07-03/.
[29] https://t.me/noname05716/8444.
[30] https://t.me/CyberArmyofRussia_Reborn/8897.
[31] https://therecord.media/spain-arrest-noname-russia-hackers.
[32] Claimed DDoS on French Senate. https://x.com/FalconFeedsio/status/1866007322809326208.
[33] Russian Cyber Army and NoName057(16) joint activity against Czech infrastructure. https://t.me/noname05716/7655.
[34] https://www.reuters.com/world/europe/italy-prolong-war-supplies-ukraine-until-end-2025-2024-12-23/.
[35] https://t.me/noname05716engver/769.
[36] https://t.me/cyber_wolff/631.

Affairs in Denmark[37] and NoName057(16) claimed it had attacked governmental entities in Sweden and France[38] [39].

- **ENISA assess that DDoS attacks carried out in this context, while sometimes resulting in disrupting services, also aim at undermining confidence in public institutions. This further confirms that hacktivist-led DDoS attacks are being used not only for disruption, but also as tools for information operations — intended to influence public perception, amplify political messages or generate media attention.**

3.1 Data-related threats

Threats against data can be categorised as a data breach (17.4%) or a data exposure (1%). A data breach is an intentional cyberattack with the goal of gaining unauthorised access to a system or organisation and stealing sensitive, confidential or protected data. A data exposure is an event (such as a misconfiguration) that can cause the unintentional loss or exposure of sensitive, confidential or protected data.

Data-related incidents represented the second most frequent threat type recorded against public administration entities in the EU in 2024. Notable targets included employment services, local government platforms, law enforcement portals and educational systems. For instance, the Spanish employment agency Lanbide experienced unauthorised access in January, resulting in a breach of user data [40]. In Estonia, the local government of Kehra was targeted in February, resulting in a breach of residents' data[41].

Financially motivated attacks were the most prevalent amongst the data-related incidents, following a hack-and-sell pattern. In many events, databases appeared on Telegram or dark-web forums, usually including a sample as a proof of the breach. For example, in May, the user with the alias 'DuckyMummy' listed Greek Police mailbox archives on BreachForums for USD $200[42].

The majority of data-related incidents occurred in the final months of 2024. A notable rise was observed in October, November and December, which collectively accounted for over 40% of all such events. This late-year surge included the publication of administrative files from Romanian institutions[43], credential breaches from Dutch municipal platforms[44] and the compromise of governmental systems in Italy[45].

- **ENISA assess data-related attacks remain opportunistic and are almost certainly leveraged for follow-up attacks, hindering the assessment of their impacts.**

[37] https://t.me/hack_n3t/420.
[38] https://t.me/noname05716/7038.
[39] https://t.me/noname05716eng/3204.
[40] https://www.lanbide.euskadi.eus/noticia/-/noticia/2024/.
[41] https://www.postimees.ee/7951529/kehra-elanike-andmed-lekkisid.
[42] https://www.secnews.gr/566008/webmail-elliniki-astinomia-dark-web/.
[43] https://twitter.com/MonThreat/status/1750465955610665247.
[44] https://www.security.nl/posting/862833/Gemeente+Almere+lekt+door++foutieve+printinstelling+gegevens+inwoners.
[45] https://proton.me/pass/leaked-politicians-dark-web.

3.2 Ransomware

Ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the assets' availability or in exchange for not publicly exposing the target's data[46]. These attacks typically involved the encryption of files and services, as claimed on public Data Leak Sites (DLS).

In 2024, publicly reported ransomware incidents affecting public administration entities in the EU remained relatively limited in volume representing about 10% of the total events. Based on identified incidents, ransomware attacks continue to be opportunistic. Over the reporting period, cybercrime operators leveraged multiple ransomware strains, notably through Ransomware-as-a-Service (RaaS) programs. Based on DLS monitoring, the most frequently deployed ransomware strains against the public administration sector in the EU in 2024 included RansomHub, Lockbit 3.0 and 8Base (further detailed in the 'Key Adversaries' section). Compared with 2023, five newly observed groups targeted the public administration sector in the EU in 2024: Argonauts, Mad Liberator, Mogilevich, PlayBoy and Termite; however all except Argonauts which recorded two incidents were responsible for only one event each. Conversely, Blackbyte, Cuba and Royal, which were active in this sector in 2023, were not reported active in the EU in 2024.

Ransomware attacks are of particular concern in the EU. In addition to putting critical data at risk, they also result in the disruption and/or interruption of services to EU civil society, as well as representing an economic impact on the community. Based on a report by Sophos, the average recovery cost from ransomware attacks for EU state and local entities was USD$ 2.83 million in 2024[47].

Personal identifiable information (PII) or critical data can be exposed during ransomware attacks, as seen in the incident targeting Hungary's defence procurement agency[48] or the Kill Security ransomware attack against Romanian institutions that affected at least 200,000 residents in Bucharest[49] [50].

The disruption and interruption of services is illustrated by the ransomware attacks that targeted the Fouesnant municipality, which resulted in a temporary shutdown of digital systems[51]; the Hellenic Open University, which resulted in significant service disruption[52]; the Teo City Council which reported a multi-week downtime[53]; and also the Romanian Chamber of Deputies, which was targeted by LockBit in January, which resulted in several days of service unavailability, but without a reference to a ransom payment[54].

[46] ENISA, *ENISA Threat Landscape for Ransomware Attacks – July 2022*, 2022, https://data.europa.eu/doi/10.2824/456263.
[47] https://news.sophos.com/en-us/2024/08/14/the-state-of-ransomware-in-state-and-local-government-2024/.
[48] https://forbes.hu/tarsadalom/kibertamadas-honvedelem-freesz-ferenc/.
[49] https://www.romania-insider.com/hackers-data-bucharest-nov-2024.
[50] https://x.com/H4ckManac/status/1856232597728244043.
[51] https://www.ouest-france.fr/societe/cyberattaque.
[52] https://armyvoice.gr/2024/11/kyvernoepithesi-elliniko-anoikto-panepistimio.
[53] https://teo.gal/gl/actualidade/2024/o-concello-de-teo-sufre-un-ataque-informatico.
[54] https://www.digi24.ro/stiri/actualitate/politica/atac-cibernetic-la-camera-deputatilor-buletinul-lui-ciolacu-a-ajuns-pe-mana-hackerilor-2668783.

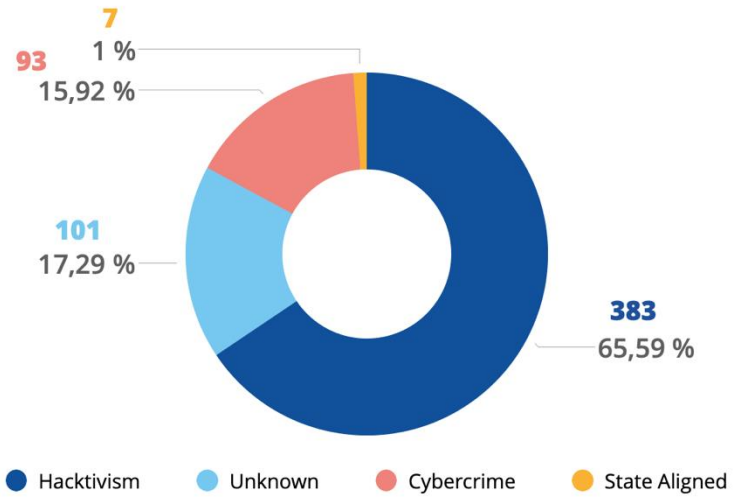
- **NISA assess that, despite some occasional high-impact ransomware incidents, targeting the public administration sector in the EU is likely to remain unprofitable as multiple EU MSs discourage ransom payments[55] [56] [57] [58] [59].**

[55] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares.
[56] https://english.ncsc.nl/binaries/ncsc-en/documenten/factsheets/2020/june/30/factsheet-ransomware/71059_NCSC_FS%2BRansomeware%2BEN_WEB.pdf.
[57] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Ransomware/ransomware_node.html.
[58] https://atwork.safeonweb.be/tools-resources/cyber-attacks-what-do.
[59] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mika-ihmeen-kiristyshaittaohjelma.

4. Key Adversaries

Based on ENISA's observations, key adversaries to the public administration sector in the EU include state-nexus intrusion sets, cybercrime operators and hacktivists. Figure 10 breaks down incidents collected during the reporting period by key categories of adversaries. Hacktivism emerged as the most prevalent category, accounting for nearly 65% of the total. Cybercrime operators and state-nexus intrusion sets accounted for approximately 16% and 1.2%, respectively. An additional 17% of incidents could not be confidently linked to any of these main categories and were marked as unknown.

Figure 10: Key adversaries reported active against the public administration sector in the EU in 2024



4.1 State-nexus intrusion sets

Throughout 2024, state-nexus intrusion sets continued to conduct cyberespionage campaigns against the public administration sector in the EU. Intrusion sets publicly imputed to Russia (APT28 and APT29) and China (APT31, Earth Krahang, Storm-1849 and APT17) were reported as being particularly active.

Between November 2023 and February 2024, **APT28** was seen to be impersonating government organisations from Poland and Ukraine to target Poland[60] [61]. This intrusion set was also reported to be targeting German government entities by leveraging

In May 2024, the High Representative for Foreign Affairs of the EU along with its Member States strongly condemned cyberespionage campaigns against German and Czech entities which they attributed to APT28.

60 https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/.
61 https://harfanglab.io/en/insidethelab/compromised-routers-infrastructure-target-europe-caucasus/.

CVE-2023-23397[62], highly likely as part of the 'Silence' cyberespionage campaign reported in 2023[63]. In May 2024, CERT-PL issued an advisory warning against an ongoing APT28 spearphishing campaign targeting government agencies to deploy their Headlace signature backdoor[64] [65]. The intrusion set was reported to be impersonating the European Union Agency for the Space Program (EUSPA) and the Kiel institute for the World Economy (IfW Kiel) to target government entities and NGOs in Europe[66]. In April 2024, APT28 was reported to be leveraging GooseEgg to exploit the CVE-2022-38028 vulnerability in Windows' Print Spooler service, possibly as early as April 2019[67]. GooseEgg was observed being used as a post-compromise tool against targets including Western Europe government, education and transportation sector organisations, as well as NGOs.

In June 2024, **APT29** (aka Midnight Blizzard, The Dukes, Nobelium, UAC-0215, Earth Koshchei) was reported by ANSSI as targeting French diplomatic interests. Clustering APT29 into three groups, ANSSI documented Nobelium's leveraging of previously compromised email accounts of foreign institutions to target French governmental and diplomatic entities in spearphishing campaigns since at least 2021[68]. In October 2024, APT29 conducted a global rogue RDP campaign using spearphishing emails[69] [70]. Registration of the identified infrastructure would have been started by August 2024 at least. Domains were observed impersonating Amazon and Microsoft services, and masquerading as organisations primarily in the government, NGO, military and IT sectors[71] [72]. EU MSs impacted by this campaign included Austria, Belgium, Czech Republic, Finland, Germany, Greece, Italy, Latvia, Lithuania, the Netherlands, Poland, Portugal, Slovakia and Sweden. NATO and the European Space Agency (ESA) were also, it seems, targeted in this campaign. The same month, APT29 was also reported to have been targeting governments in Western Europe, notably through the exploitation of JetBrains Teamcity and Zimbra vulnerabilities, as well as abusing Microsoft Teams accounts to carry out spearphishing campaigns[73].

Figure 11: Open source documented targeting of public administration in the EU by intrusion sets imputed to Russia

Additional activities imputed to Russia targeting the public administration in the EU over the reporting period in public sources include the exploitation of a zero-day Zimbra vulnerability since October 2023 to target government and military email servers located in Belgium, France and Germany by **Winter Vivern**[74], the targeting of a governmental organisation of an undisclosed EU MS from May 2022 until

62 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html.
63 https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-malicious-activity-against-microsoft-exchange-servers/.
64 https://cert.pl/en/posts/2024/05/apt28-campaign/.
65 https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf.
66 https://xfe-development.xforce.ibm.com/threats/guid:94a630af6a541814f46c892b299ff9b5.
67 https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/.
68 https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-006.pdf.
69 https://cert.gov.ua/article/6281076.
70 https://aws.amazon.com/blogs/security/amazon-identified-internet-domains-abused-by-apt29/.
71 https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/.
72 https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html.
73 https://www.ic3.gov/CSA/2024/241010.pdf.
74 https://go.recordedfuture.com/hubfs/reports/cta-2024-1209.pdf

March 2024 by GoldenJackal[75], and **GreenCube** (overlapping with UAC-0102 and UNC370) targeting Roundcube XSS vulnerabilities in a credential stealing campaign reported to repeatedly target governmental and defence related organisations in Greece and Poland[76].

Since at least early 2022 until at least March 2024, **Earth Krahang** abused compromised government webservers to conduct follow-up spearphishing activities against other government entities, notably against Hungary and Romania[77] [78]. In March 2024, the Finnish police confirmed that **APT31** maintained covert access to the Finnish Parliament e-mail servers breached in 2021[79]. In May 2025, the Czech government publicly attributed the targeting of an unclassified network of the Czech Ministry of Foreign Affairs since 2022 to APT31[80], likely related to the exfiltration of documents from the Czech EU Presidency by i-Soon[81] [82]. In April 2024, Cisco Talos documented a global cyberespionage campaign called ArcaneDoor that had been targeting government-owned perimeter network devices since at least December 2023[83]. Leveraging then zero-day CVE-2024-20353 and CVE-2024-20359, **Storm-1849** (aka UAT4356) was observed deploying two bespoke backdoors called Line Dancer and Line Runner. Italy was also targeted in a campaign conducted by **APT17** (aka DeputyDog) in June and July 2024, leveraging Rat 9002 against companies and governmental entities[84].

Figure 12: Open source documented targeting of public administrations in the EU by intrusion sets imputed to China.

- **ENISA assess that public administration in the EU represents a high-value target for State-nexus intrusion sets for the purposes of strategic data collection to support their foreign policies, economic strategies and possibly their military objectives. While identified cyberespionage campaigns in 2024 against the EU public administration account for only 2.5% of overall incidents, these activities are likely to have a significant impact on the national security of EU MSs, as well as on the stability and growth of the EU single market in the long-term in the case of Intellectual Property (IP) theft.**

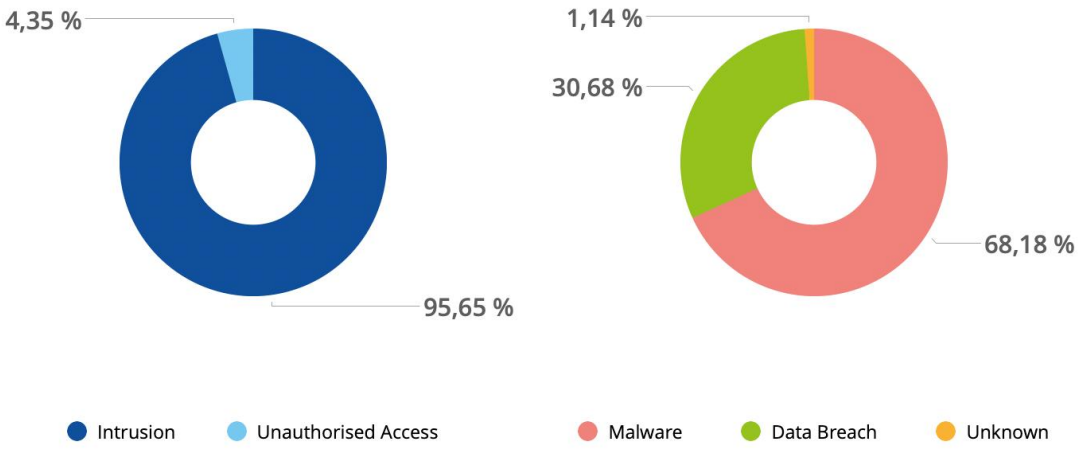
4.2 Cybercrime operators

In 2024, cybercrime operators targeting public administration entities in the EU primarily relied on the ransomware-as-a-service (RaaS) model. While most attacks had minimal impact, at least eight incidents reportedly resulted in operational disruptions. Overall, ransomware remains among the most impactful threats to EU Member States, with a confirmed shift from encryption to data exfiltration. Trends identified in the cybercrime ecosystem pertain to the continuous use of a multi-extorsion

75 https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/.
76 https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2024-q3-2024.pdf.
77 https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html.
78 https://www.trendmicro.com/en_us/research/24/b/earth-lusca-uses-geopolitical-lure-to-target-taiwan.html.
79 https://www.bleepingcomputer.com/news/security/finland-confirms-apt31-hackers-behind-2021-parliament-breach/.
80 https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_by_the_government_of_the_czech.html.
81 https://www.seznamzpravy.cz/clanek/domaci-kauzy-ministerstvo-zahranici-se-stalo-tercem-kyberspionu-cinske-vlady-249478.
82 https://cybule.cz/kyberneticke-utoky/unik-dat-i-soon-nabizi-vhled-do-kyberspionaznich-aktivit-ciny-mezi-obetmi-ceske-mzv/.
83 https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/.
84 https://www.tgsoft.it/news/news_archivio.asp?id=1557&lang=eng.

technique, with a reported increase in the use of AI. Figure 13 displays the breakdown of incidents assessed to have a financially-motivated objective by type of threat.

Figure 13: Financially-motivated cyber operations against the public administration sector in the EU in 2024.



In 2024, LockBit affiliates expanded the double-extortion model, which typically involved data theft and encryption, with DDoS attacks and website defacements, creating a multi-extortion model that increased pressure on victims. The year 2024 also saw the continuous **exploitation of third-party IT and HR service providers, as exemplified by the** compromise of Nordic outsourcer Tietoevry by the Akira ransomware group in January 2024, which had an impact on payroll and case-management platforms used by approximately 120 Swedish government agencies and municipalities[85]. In addition, the LockBit 3.0 group attack against the Torre Pacheco City Council's IT infrastructure resulted in to the activation of a Crisis Committee[86].

The role of Initial-Access Brokers (IAB) in the cybercriminal ecosystem remains prevalent, with underground forums advertising ready-made VPN or RDP access into government networks. Listings offered access to the Polish Government Communications Centre and the French Ministry of Defence intranet for USD $7,000–15,000[87]. Another example was the sale of administrative access to the Italian Civil Protection Portal[88].

[85] https://www.svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda.
[86] https://www.laopiniondemurcia.es/municipios/2024/03/31/ayuntamiento-torre-pacheco-sufre-ciberataque-100474480.html.
[87] https://twitter.com/DailyDarkWeb/status/1750956773358415887.
[88] https://www.redhotcyber.com/post/in-vendita-laccesso-al-potale-della-protezione-civile-italiana/.

Finally, in 2024 an increase in AI-enabled social-engineering campaigns[89] [90] was observed, with national authorities warning about voice-cloned calls and AI-generated phishing[91] [92] [93].

Over the reporting period, cybercrime operators leveraged multiple ransomware variants, notably through Ransomware-as-a-Service (RaaS) programs. Based on DLS, the most deployed ransomware strains against the public administration sector in the EU in 2024 included RansomHub, LockBit 3.0 and 8Base.

First publicly reported in February 2024, **RansomHub** emerged as the top (20.7%) ransomware threat to the public administration sector in the EU during the reporting period. Compared to other RaaS operators, RansomHub operates a more decentralised RaaS operation. RansomHub affiliates reportedly collect ransom payments themselves, then pay a 10% fee to RansomHub operators[94] [95].

LockBit was the most deployed ransomware variant in 2022 being leveraged both by the group and affiliates. On 24 February 2024, they were disrupted by a law enforcement operation, Operation Chronos, and remained mostly inactive after that. Although LockBit quickly relaunched its DLS, the confidence of affiliates in LockBit decreased.

The LockBit 3.0 builder (also known as the LockBit Black builder) was leaked in late 2022 by a LockBit developer. Following the official takedown of LockBit, some LockBit affiliates and other cybercrime groups continued operations using this builder. One example is the group CosmicBeetle, which was observed by ESET researchers in 2024.

8Base is a ransomware operator, active since early 2023, and reported continuing conducting double-extortion attacks throughout 2024, accounting for 5.6% of the total ransomware incidents. Victims typically faced both data encryption and threats of data exposure on public leak sites. In attacks targeting European entities, ransom notes occasionally referenced potential GDPR penalties as a tactic to increase pressure during ransom negotiation[96] [97].

Akira is a ransomware-as-a-service (RaaS) group active since at least March 2023. Over the reporting period Akira was reported active against the public administration exclusively in Sweden, yet accounted for 5.6% of total ransomware incidents. On 18 April 2024, the EC3, NCSC-NL, FBI, and CISA, jointly released a report on Akira ransomware, detailing its tactics, techniques and indicators of compromise based on investigations up to February 2024. The group affected over 250 organisations, earning around USD42 million worth of ransom in cryptocurrency[98].

[89] https://www.fnlondon.com/articles/it-sounds-like-me-even-though-its-not-me-deepfake-scams-put-city-firms-on-high-alert-cb6a2bb6.
[90] https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20For%202030%20Update%202024_0.pdf.
[91] https://safeonweb.be/en/news/beware-investment-fraud-exploiting-deepfakes.
[92] https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/nuevo-metodo-de-fraude-usando-la-voz-de-un-familiar-creada-con-inteligencia-artificial.
[93] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html.
[94] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub.
[95] https://www.scmagazine.com/news/takedowns-spark-affiliate-bidding-war-among-ransomware-gangs.
[96] https://almond.eu/wp-content/uploads/Almond-x-Amossys-8Base.pdf.
[97] A Europol-coordinated operation involving multiple EU MSs in February 2025 seized 27 Command-and-Control (C2) servers and arrested four alleged core operators[97] [97]. 8Base's data leak site was also seized by law enforcement with a takedown notice displaying logos for the Federal Bureau of Investigation (FBI), the United Kingdom's National Crime Agency (NCA), and federal police agencies from Germany, Czechia and Switzerland among others.
[98] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a.

Hunters International is a ransomware-as-a-service (RaaS) group that has been active since at least October 2023. Picus Security traces Hunters' playbook to Hive code-fragments and highlights its aggressive data-exfiltration routine, which begins minutes after initial intrusion[99]. Hunters International claimed via their Dedicated Leak Site (DLS) that they are not affiliated with Hive, claiming that they are an independent group that acquired Hive's source code and infrastructure[100]. Incidents claimed by the group included municipal governments and regional agencies in France, Spain and Sweden. They also accounted for 5.6% of total ransomware incidents[101] [102] [103].

- **ENISA assess that the public administration sector in the EU is an opportunistic target for cybercrime operators, given its low maturity. Although some disruptions occurred and might have a temporary impact on the functioning of the EU single market, these activities did not have an impact on the national security of EU MSs.**

4.3 Hacktivists

Hacktivist activity in 2024 against public administration entities in the EU was primarily claimed in relation to ideological motivation and often related to geopolitical events such as Russia's war of aggression against Ukraine and the conflict in the Middle East. Targets notably included municipal websites and ministry portals. Groups such as NoName057(16), Anonymous Sudan, and UserSec frequently claimed responsibility for operations through Telegram. Their main targets were governmental portals and local administrations. Nearly all Member States were targeted at least once during the reporting period. While the current operational impact remains limited—no dataset entry involved a confirmed compromise of back-office systems—the cumulative reputational damage and incident-response burden are growing.

NoName057(16), a pro-Russia hacktivist group, was responsible for a series of campaigns of politically motivated DDoS attacks across the European Union in 2024, making it one of the most active hacktivist groups targeting the public administration sector. The group targeted central and local government websites, public-facing digital services and municipal infrastructure in countries perceived as hostile to Russian interests. For example, the multi-actor 'OpEU Election' campaign between 3 and 9 June, targeting interior and foreign affairs portals in fourteen Member States while urging followers to 'silence Brussels propaganda'[104] [105].

In 2024, Germany, Poland, France and Italy were repeatedly targeted. NoName057(16) regularly communicates its operations via its Telegram channel, where it claims responsibility and publishes evidence of disruption, including screenshots and attack timestamps. The group's activity appears to be reactive to the political or military support offered to Ukraine by EU Member States, aiming to disrupt essential services and undermine public trust in governments.

[99] https://www.picussecurity.com/resource/blog/hunters-international-ransomware.
[100] https://www.acronis.com/en-us/cyber-protection-center/posts/hunters-international-new-ransomware-based-on-hive-source-code.
[101] https://twitter.com/FalconFeedsio/status/1758468770585059534.
[102] https://twitter.com/FalconFeedsio/status/1758801900546433383.
[103] https://x.com/FalconFeedsio/status/1857032281531035846.
[104] https://cybelangel.com/unmasking-noname05716/.
[105] https://www.radware.com/blog/security/uncovering-the-hacktivist-cyberattacks-targeting-the-eu-election.

People's Cyber Army / Cyber Army of Russia Reborn (CARR) is a pro-Russia group reportedly linked with high confidence to the group Sandworm (also known as APT44)[106] [107]. Active throughout 2024, the group primarily conducted DDoS attacks targeting public administration entities in countries perceived as hostile to Russian interests, particularly those supporting Ukraine, including in the EU (11%). Cooperating with HackNeT, CARR also targeted the Olympic Games that were hosted in Paris. In June 2024, both groups conducted DDoS attacks on multiple French government sites, openly describing the activity as a "final training stage" before the Paris 2024 Games, and sharing reconnaissance scripts that enumerated API and video-stream routes for later exploitation. French authorities confirmed short outages at the Administrative Court of Paris and the health-regulator ANSM during these tests[108] [109] [110] [111].

CyberDragon was among the pro-Russia groups that targeted public administration entities in the EU in 2024. It focused primarily on DDoS attacks against local and regional government infrastructure. In 2024, its targets included administrative platforms and municipal services in the Czech Republic, Denmark, Estonia, Germany and Lithuania. Several campaigns coincided with geopolitical developments — for example, the 28 February attack on Danish entities followed a series of announcements that same month, including Denmark's full donation of its artillery stockpile to Ukraine, the unveiling of a €247 million military aid package, and a visit to Lviv by Prime Minister Frederiksen to formalise long-term security cooperation with Ukraine[112] [113] [114].

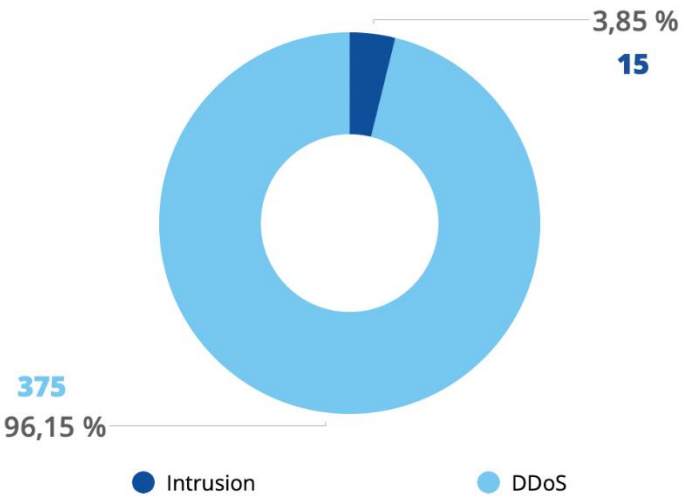
OverFlame is a pro-Russia group that gained attention in 2024 for its involvement in DDoS attacks and website defacements targeting public administration and critical infrastructure such as the Energy and Digital Infrastructure sectors, within the European Union. The group operates through underground forums and encrypted messaging platforms, where they recruit new members and coordinate their attacks[115]. In September 2024, OverFlame collaborated with NoName057(16) in a series of DDoS attacks that targeted over 40 Austrian entities, including government websites, airports, financial services and the Vienna Stock Exchange[116]. Those DDoS attacks took place during Austria's parliamentary elections.

Active since at least June 2023, the pro-Hamas group **RipperSec** intensified its cyber operations in 2024, notably through the use of a custom-developed DDoS tool known as MegaMedusa, primarily focusing on DDoS attacks targeting the public administration sector in France, Austria, Italy and Belgium. They accounted for 2.6% of total DDoS events. Their operations are ideologically driven, targeting nations perceived as supporting Israel or acting against Muslim interests[117].

In Figure 14, ENISA presents the incidents by hacktivists per threat type.

[106] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf.
[107] https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook/.
[108] https://cyble.com/blog/hacktivist-groups-peoples-cyber-army-and-hacknet-launch-trial-ddos-attacks-on-french-websites-prior-to-the-onslaught-during-paris-olympics/.
[109] https://cointelegraph.com/news/cyberattacks-target-french-government-websites-report.
[110] https://t.me/CyberArmyofRussia_Reborn/8273.
[111] https://t.me/CyberArmyofRussia_Reborn/8276.
[112] https://kyivindependent.com/denmark-to-donate-all-its-artillery-to-ukraine-says-pm/.
[113] https://www.reuters.com/world/europe/denmark-unveils-ukraine-aid-package-urges-allies-give-more-2024-02-22/.
[114] https://www.reuters.com/world/europe/danish-pm-frederiksen-meets-ukraines-zelenskiy-lviv-2024-02-23/.
[115] https://www.radware.com/security/threat-advisories-and-attack-reports/pro-russian-hacktivists-target-organizations-in-austria-with-ddos-attack-campaign/.
[116] https://therecord.media/austria-websites-ddos-incidents-pro-russia-hacktivists.
[117] https://www.radware.com/blog/security/megamedusa-rippersec-public-web-ddos-attack-tool/.

Figure 14: Incidents by hacktivists against the public administration sector in the EU in 2024



Persistent DDoS disruption. DDoS attacks accounted for over 95% of the publicly reported incidents by hacktivist groups. Many campaigns were closely aligned with geopolitical flashpoints, particularly concerning EU support for Ukraine and NATO expansion. For instance, attacks on Latvian and German government portals in early January coincided with high-level EU engagement in Ukraine aid[118] [119] [120] [121] [122]. In July, NoName057(16) launched over 50 attacks, many targeting Spanish institutions amid rising defence coordination between Spain and the EU[123] [124] [125] [126] [127]. Several campaigns involved multiple EU Member States being targeted on the same day, such as on 17 January, when NoName057(16) claimed attacks against both the Belgian House of Representatives, the Czech Chamber of Deputies and Prague's public transport authority[128].

Move to application-layer and new vectors. Several logs referenced the Rapid-Reset technique disclosed in late-2023[129]. By using this technique, attackers manage to bypass traditional network-layer defences.

Combo campaigns across sectors. In ~10% of cases the same actor simultaneously targeted transport or energy portals in the affected state. For example, on 28 December 2024, NoName057(16)

[118] https://t.me/noname05716/5616.
[119] https://t.me/noname05716/5629.
[120] https://t.me/noname05716/5661?single.
[121] https://t.me/noname05716/5780.
[122] https://t.me/noname05716/5804?single.
[123] https://t.me/CyberArmyofRussia_Reborn/8897.
[124] https://t.me/h0lyleague/13.
[125] https://t.me/CyberArmyofRussia_Reborn/9017?single.
[126] https://t.me/CyberVolk_K/227.
[127] https://t.me/privetOTof222/137.
[128] https://t.me/noname05716/5693.
[129] https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack.

group targeted the Italian Ministry of Foreign Affairs and the websites of Milan's two international airports, explicitly framing it as retaliation for Italy's support for Ukraine[130].

- **ENISA assess that the public administration sector in the EU constitutes a visible, symbolic target for ideologically motivated hacktivist groups, whose campaigns seek to draw attention through disruption. The operational impact of hacktivist-led DDoS remains limited and these activities are unlikely to undermine the national security of EU MSs or the functioning of the EU single market.**

[130] https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-pro-russian-hacker-2024-12-28.

5. Outlook

The analysis of cybersecurity incidents from January to December 2024 points to several key findings for the public administration sector in the EU. The public administration sector remains a prime target. The assessment of ENISA's sectorial threat landscape editorial team is that, in the short-to-near term, public administration in the EU will remain the most frequently targeted sector. It is highly likely that this sector will face waves of low-impact DDoS attacks and a continuation of cyberespionage campaigns.

For the public administration sector in the EU, ENISA expects to see the following trends in 2025.

- **Continuation of DDoS Attacks.** It is highly likely that DDoS campaigns will continue, especially around key events such as elections or summits, without causing significant operational disruptions.
- **State-nexus activity**. It is highly likely that Russia-nexus and China-nexus intrusion sets will sustain cyber-espionage campaigns against the public administration sector in the EU for strategic data collection.
- **AI-powered social engineering and deep-fake scams.** It is likely that generative LLMs, voice-cloning and face-swap tools will be used for phishing, vishing attacks and misinformation/disinformation. It is likely that campaigns will be observed that go beyond traditional extortion and aim to influence public opinion and undermine trust.
- **Ransomware.** It is expected that opportunistic ransomware attacks against the public administration sector in the EU will continue to happen and will cause a few disruptions.

These emerging trends threaten both operational continuity and public trust in EU governance. AI-driven phishing could breach sensitive citizen-data repositories, triggering identity fraud and regulatory liabilities. Multi-extortion campaigns might amplify service outages—tax portals, e-ID systems and court scheduling—undermining confidence in digital government. Supply-chain exploits risk simultaneous compromise of multiple agencies, triggering complexities in cross-border responses and heightening political fallout.

Given the inclusion of the public administration sector under the NIS2 Directive which underscores the sector's criticality, in the next chapter of this report, ENISA proposes a set of strategic priorities to enhance its maturity and readiness to address ongoing challenges.

6. Recommendations

The recommendations below provide concrete actions for public administration entities in the EU. They are proportionate to the sector's threat landscape findings: high volumes of DDoS, a steady number of data-related incidents, opportunistic ransomware and state-nexus campaigns. They are presented for each threat or type of adversary.

6.1 DDoS-related

As Distributed Denial of Service (DDoS) was the most frequent threat type, ENISA proposes controls that enhance architectural resilience and operational readiness.

- Enrol critical portals (ministries, parliaments, municipal sites) behind Content Delivery Network (CDN) / Web Application Firewall (WAF) with always-on network–application layer protection: DDoS campaigns target availability and CDN/WAF absorb and filter traffic before it reaches the original systems, reducing outages.
  - Filter Network Traffic (M1037)
  - Network Intrusion Prevention (M1031)
- **Publish static-fallback sites with Domain Name System (DNS) failover**: In the case that the original site becomes unavailable, a read-only status site keeps essential information online while full service is restored.
  - Resiliency (M1030)

6.2 Data-related

While typical DDoS attacks usually have little impact, data-related incidents can cause significant disruption to an organisation's operations.

- **Enforce Multi-Factor Authentication (MFA)** everywhere with conditional access and Privileged Access Management (PAM) for administrators as compromised credentials are commonly used in such attacks.
  - Multi-factor Authentication (M1032)
  - Privileged Account Management (M1026)
- Usage of **Data Loss Prevention (DLP)** technologies as they can stop mass exfiltration.
  - Data Loss Prevention (M1057)
- Harden email and web: deploy Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), use current Transport Layer Security (TLS), secure the Content Management System (CMS) and conduct focused application testing.
  - Restrict Web-Based Content (M1021)
  - Software Configuration (M1054)

6.3 Ransomware-related

Despite the public administration sector being mostly an opportunistic target for ransomware operators, the implementation of specific controls related to this kind of threat can minimise potential disruptions and enhance the cybersecurity posture of these entities.

- Deploy **Endpoint Detection and Response (EDR)** with behavioural rules, enforce application allow-listing and restrict administrative tools (PowerShell / **Windows Management Instrumentation Command-line (WMIC)** / PSExec).
  - Execution Prevention (M1038)
  - Restrict Application Execution (M1042)
- Harden document macros (signed-only, blocked by default where possible): this prevents common initial execution paths.
  - Restrict File and Directory Permissions (M1022)
- Segment networks.
  - Network Segmentation (M1030)
- Backups with **immutable/offline** copies, run restore tests frequently.
  - Data Backup (M1053)

6.4 State-Nexus espionage

The public administration sector, as a high-value target for state-nexus intrusions sets, should onboard concrete measures to support the effort against compromise by such adversaries.

- Regular threat-hunting focused on Advanced Persistent Threat (APT) Tactics, Techniques and Procedures (TTPs).
  - Audit (M1047)
- Hardening with a focus on vectors seen in recent cases.
  - Update Software (M1051)
  - Restrict Web-Based Content (M1021)
- Implement proper vulnerability and patch management.
  - Vulnerability Scanning (M1058)
- Limit third-party access (least privilege, time-bound, MFA; monitored service accounts).
  - Limit Access to Resource Over Network (M1048)
  - User Account Management (M1018)

6.5 ENISA NIS360 report recommendations

Additionally, the latest ENISA NIS360 report highlights a maturity – criticality gap for public administration: fragmented governance, limited information-sharing and legacy technology keep the sector in the 'risk-zone'. The actions below directly target those weaknesses and provide a practical pathway to compliance with NIS-2 while boosting overall resilience[131].

- **Build effective remediation capabilities through shared service models.** Partner with peer public entities to operate common security operations, identity and digital wallet platforms, optimising resources and strengthening protections for high-risk services.
- **Leverage the EU Cyber Solidarity Act.** Combine this funding with national budgets to modernise legacy systems, deploy detection–response–remediation tooling and upskill staff—meeting NIS 2 obligations faster and more economically.
- **Enhanced preparedness & response.** Give entities access to simulation environments—cyber ranges and tabletop exercises—where teams can test incident response playbooks in a risk-free setting.
- **Awareness raising.** Run targeted campaigns that explain NIS 2 requirements to leadership and operational staff, clarifying reporting lines, escalation thresholds and compliance deadlines.

[131] ENISA NIS360 – 2024, February 2025, sections 2.3 & Annex D.8. - https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf.

- **Strengthen sector specific threat awareness.** Develop dedicated public administration threat intelligence feeds using ENISA's reports and the capabilities of national CSIRTs.
- **Collaborative engagement.** Organise regular workshops, Public Administration ISAC meetings and cross sector exercises with private stakeholders to exchange good practices and coordinate on shared dependencies.

In closing, by proactively adopting these strategic priorities and fostering closer collaboration across Member States, public administration bodies in the EU will be better positioned to safeguard critical services and to uphold citizen trust in an increasingly volatile cyber threat landscape.

APPENDIX A: Notable Incidents

In this chapter we present a selection of notable incidents that happened during the reporting period. The incidents were chosen based on their operational impact on an EU Member State or Union Entity, the TTPs used and their overall relevance to the European Union as assessed by ENISA.

FRANCE TRAVAIL BREACH

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
France	13-03-2024	Public administration	Unknown	Data	Medium	A1

Description
Malicious activity that began in early February 2024 enabled attackers to exfiltrate identifiers, contact details and social-security numbers from the central job-seeker database. The breach was detected during the week of 11 March and publicly disclosed on 13 March, at which point France Travail (and partner Cap Emploi) notified the Commission Nationale de l'Informatique et des Libertés (CNIL), filed a criminal complaint with the Paris Public Prosecutor's Office, and began directly alerting affected individuals via email and their personal online portals.[132]

Impact: The personal data of approximately 43 million people were exposed, prompting both a preliminary judicial investigation by the Brigade de Lutte Contre la Cybercriminalité and a CNIL enforcement probe.

APT31 ATTRIBUTION FOR FINNISH PARLIAMENT BREACH

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
Finland	26-03-2024	Public administration	APT31	Intrusion	Medium	A1

Description
On 26 March 2024 the National Bureau of Investigation confirmed that malware and C2 infrastructure tied to APT31 were present in Eduskunta's email environment from autumn 2020 until its removal in January 2021. Archived mailbox data was copied during the period of access. Evidence collected during the multi-year investigation was transferred to the Prosecutor-General for indictment[133].

Impact: Exfiltration of parliamentary emails; criminal case opened for aggravated espionage.

[132] https://www.francetravail.org/accueil/communiques/2024/france-travail-et-cap-emploi-victimes-dune-cyberattaque.html?type=article.
[133] https://poliisi.fi/en/-/investigation-into-hacking-of-parliament-s-information-systems-has-been-ongoing.

COMPROMISE OF BELGIAN FOREIGN-AFFAIRS COMMITTEE CHAIR

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
Belgium	25-04-2024	Public administration	Unknown	Intrusion	Medium	B1

Description
On 25 April 2024, the FBI delivered a forensic report to the Belgian authorities revealing that tracking malware had been implanted in an MP's laptop in mid-2021. The implant provided remote persistence, file exfiltration capability and keystroke logging until its removal during a security review in March 2024. Belgian CERT and parliamentary IT staff re-imaged the device, rotated credentials and began a broader sweep of legislative endpoints[134].

Impact: Long term access to strategic data, unknown whether exfiltration occurred.

APT28 MALWARE CAMPAIGN AGAINST POLISH GOVERNMENT NETWORKS

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
Poland	08-05-2024	Public administration	APT28	Intrusion	Medium	A1

Description
Between 29 April and 3 May 2024 spearphishing emails embedding a loader linked to Fancy Bear (APT28) were sent to official Polish government email accounts. On 8 May, the National Research Institute (NASK) published indicators of compromise, enabling SOC teams to block the malicious IP ranges, remove the loader where detected and force password resets for any accounts that had opened the malicious documents[135].

Impact: Attempted credential harvesting; no confirmed operational disruption.

EUROPOL EPE CREDENTIAL SALE OFFER

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
EU	10-05-2025	Public administration	IntelBroker	Data	Medium	B1

[134] https://www.reuters.com/world/europe/head-belgian-foreign-affairs-committee-says-she-was-hacked-by-china-2024-04-25/.
[135] https://www.gov.pl/web/baza-wiedzy/uwaga-csirt-nask-ostrzega---polskie-instytucje-rzadowe-celem-ataku-grupy-hakerow-apt28.

Description
On 10 May 2024, IntelBroker posted screenshots showing credential pairs allegedly extracted from a closed group on Europol Platform for Experts (EPE). Europol's security team verified that a small set of external-partner accounts had been brute-forced, that it had disabled the affected accounts and had forced a global password reset. The team filed a criminal complaint with Dutch police. No restricted operational files were found in the leaked sample[136].

Impact: Limited data-set advertised on dark-web forum; Europol reset all user accounts.

EINDHOVEN MUNICIPALITY BSN EXPOSURE

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
Netherlands	23-05-2024	Public administration	Unknown	Data	Low	B1

Description
On 22 May 2024, during a routine database export at Eindhoven Municipality, a CSV file containing the burgerservicenummers (BSNs) of over 220,000 residents was mistakenly stored in a shared directory without access controls. The file remained accessible to authenticated staff until a routine backup check flagged the anomaly on 23 May at 11:15 CEST, after which it was deleted and the Dutch DPA was notified[137].

Impact: No confirmed cases of unauthorised access to the file were reported.

NOBELIUM ACTIVITY AGAINST FRENCH DIPLOMATIC TENANTS

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
France	19-06-2024	Public administration	Nobelium	Intrusion	Medium	A1

Description
On 19 June 2024, ANSSI published an advisory detailing repeated OAuth-consent phishing operations by the SVR-linked Nobelium group against French ministry staff. Six waves—January, March, May, July and November 2023, plus April 2024—lured users into granting a malicious Azure AD application excessive permissions (e.g. Mail.Read, Sites.Read.All). ANSSI's recommendations included the immediate revocation of all unrecognised app consents, the tightening of Conditional Access policies to block legacy authentication and enforce MFA on consent, and the conducting of a tenant-wide audit of registered enterprise applications[138].

[136] https://www.bleepingcomputer.com/news/security/europol-confirms-web-portal-breach-says-no-operational-data-stolen/.
[137] https://www.ed.nl/eindhoven/eindhoven-liet-bsn-gegevens-van-ruim-220-000-inwoners-rondslingeren~ad2576e5/?referrer=https%3A%2F%2Fwww.ccinfo.nl%2F.
[138] https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-006/.

Impact: No confirmed operational data exfiltration was reported. However, the campaigns triggered a full review of OAuth-consent governance and strengthened identity-protection controls across targeted ministries.

PAYMENT-CARD LEAK AT NATIONAL OBSERVATORY OF ATHENS

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
Greece	09-07-2024	Public administration	Unknown	Data	Medium	A1

Description

On 9 July 2024, the National Observatory of Athens issued an urgent notice after discovering that, between 7 July 19:00 and 8 July 17:00 (UTC +3), its Visitor Centre reservation form had been replaced by a malicious JavaScript skimmer on tickets.astro.noa.gr. The injected script captured the details of visitors' payment-cards and transmitted them to an external domain. The Observatory immediately disabled online ticket sales, notified affected payment processors and the Hellenic Data Protection Authority, and rebuilt the compromised web server[139].

Impact: Credit and debit card data captured for almost 24 hours; ticketing platform taken offline.

LATVIAN STATE REVENUE SERVICE DDOS OUTAGES

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
Latvia	22-08-2024	Public administration	Unknown	DDoS	Medium	A1

Description

Between 19 and 22 August 2024 Latvia's centrally managed Unified Website Platform (TVP), the shared hosting environment for more than a hundred state and municipal websites, including the State Revenue Service's portal and the Cabinet of Ministers site, was targeted by a high-volume DDoS attack. LVRTC and CERT-LV responded to the attack with upstream filtering and blocked all traffic from outside Latvia, making the portal unreachable from abroad even after domestic availability was restored on 20 August[140] [141] [142].

Impact: The four-day geoblock left Latvian residents and businesses abroad unable to reach the tax-filing portal and other government information sites, though no data loss was reported.

[139] https://www.noa.gr/en/news/news/urgent-notice-theft-of-personal-information-in-the-reservation-system-of-the-visitors-centers-of-the-national-observatory-of-athens.
[140] https://www.vid.gov.lv/lv/jaunums/informacija-wwwvidgovlv-lietotajiem-arvalstis.
[141] https://balticnews.com/government-websites-facing-intense-cyber-attacks/.
[142] https://eng.lsm.lv/article/society/defense/20.08.2024-cyber-attacks-on-public-sector-websites-in-latvia-tuesday.a565748/.

RANSOMWARE AT TIMIȘOARA CITY HALL

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
Romania	26-08-2024	Public administration	RansomHub	Ransomware	Low	B1

- **Impact:** Core municipal systems encrypted; partial service outage for five days; sample data leaked on Telegram.

Description
On 24 August 2024 the servers of Timișoara City Hall, the Municipal Fiscal Directorate (DFMT) and the Local Police were targeted by a ransomware attack that aimed to encrypt data and block core systems. Municipal IT staff disconnected the compromised infrastructure and, together with outside contractors and Romania's National Cybersecurity Directorate (DNSC), began repairs to restore the system's functionality[143] [144] [145].

Impact: Citizens temporarily lost the functionality to pay local taxes online or by card at DFMT and could no longer file police reports through the website. Payments were accepted in cash only and complaints had to be lodged by phone until the services were gradually restored.

CNOEC WEBSITE SUSPENSION AFTER SERVER COMPROMISE

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
France	03-09-2025	Public administration	Unknown	Intrusion	Low	B1

Description
On 3 September 2024 CNOEC's hosting provider alerted the organisation about suspicious shell activity on a CNOEC's public-facing web server hosted by the provider. To avoid further spreading on CNOEC systems, the administration decided to isolate their information system, to suspend the Comptexpert portal and related services, and to initiate a third-party forensic investigation. Public access remained disabled until fresh images were deployed on 9 September[146].

Impact: All CNOEC online services taken offline; no confirmed data theft.

DUTCH POLICE OFFICER-DIRECTORY BREACH

Geography	Event noted on	Sector	Intrusion Set	Threat type	Relevancy	Confidence
Netherlands	03-10-2025	Public administration	Laundry Bear	Intrusion	Medium	A1

[143] https://www.primariatm.ro/2024/08/26/atac-cibernetic.
[144] https://www.dnsc.ro/vezi/document/press-release-v20240826-ransomware-cyber-attack-on-public-institutions-in-romania-timisoara-pdf.
[145] https://hotnews.ro/atac-cibernetic-asupra-serverelor-primariei-timisoara-si-a-mai-multor-institutii-subordonate-unele-servicii-online-suspendate-1778550.
[146] https://www.linkedin.com/posts/csoec_cnoec-activity-7236404401379119104-gBlg.

Description
Security monitoring on 1 October 2024 flagged abnormal SQL queries from a compromised user account. An internal investigation confirmed that a full export of the officer-directory table—names, phone numbers and email addresses—were transferred to an external VPS two days earlier. The affected account was disabled, passwords were reset, and the Minister of Justice and Security informed Parliament on 3 October[147]. On 27 May 2025, the Dutch intelligence services AIVD and MIVD reported cyberattacks against multiple Dutch organisations, including the national police on September 2024. Dutch intelligence services associated this attack to a previously undocumented Russia-nexus intrusion set called Laundry Bear. AIVD and MIVD published a technical advisory/report (available in Dutch and English), detailing Laundry Bear's tactics, techniques and procedures (TTPs) as well as indicators of compromise (IOCs)[148]. Microsoft Threat Intelligence confirmed that Laundry Bear (tracked as Void Blizzard) focuses on targeting NGOs, government, defence, transportation, media and healthcare entities, notably in Europe, North America and Ukraine[149].

Impact: Contact details of 65 000 officers stolen; internal security audit launched.

[147] https://www.bleepingcomputer.com/news/security/dutch-police-state-actor-likely-behind-recent-data-breach/.
[148] https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor.
[149] https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/.

APPENDIX B

ASSESMENT METHODOLOGY

This report includes a number of assessments and supporting commentary. When words like ‘possibly’ or ‘likely’ are used, it reflects the assessment of the drafting team on a specific cybersecurity incident or event.

ENISA Threat Landscapes use the following estimative probability language throughout the report:

CONFIDENCE LEVEL	SYNONYMS
●●●●● **HIGHLY LIKELY**	Almost certainly. Virtually certain. High confidence. High likelihood. >90%
●●●●○ **LIKELY**	High to moderate confidence. 60 - 90%
●●●○○ **POSSIBLE**	Moderate confidence. Probable. 40 - 60%
●●○○○ **PLAUSIBLE**	Moderate to low confidence. Possible. 10 - 40%
●○○○○ **UNLIKELY**	Probably not. Not likely. Improbable. Low confidence. Not likely. <10%

For the purpose of this report, the organisation adopted a five-level methodology for describing threat levels, which relies on available information, the capabilities of known intrusion sets, analysis of recently discovered vulnerabilities and exploits (opportunities), potential intent and likelihood of a severe attack in the near-term.

THREAT LEVEL		MEANING
	LOW	A low likelihood of an intrusion set targeting activity that could affect organisations/entities which would impact the European operators of essential services or the functioning of Union entities. Disruption is considered highly unlikely.
	MODERATE	There is potential for some direct targeted intrusion set activity but it is generally considered Unlikely. This activity could lead to some disruption across multiple Member States and Union entities.
	SUBSTANTIAL	It is likely that entities are being directly targeted by intrusion sets or could be exposed to breaches using recent discovered vulnerabilities. Serious disruptions of European operators of essential services and critical entities or Union entities is considered a realistic possibility.
	SEVERE	It is likely that entities will be directly targeted by intrusion sets. Multiple entities and essential operators will be, or are being, impacted. Severe disruptions are likely to be widespread, across multiple Member States and Union entities.
	CRITICAL	It is highly likely organisations are targeted by highly advanced and persistent intrusion sets 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 experienced across multiple Member States and Union entities.

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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union