



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



# **International workshop on conducting criminal investigations of ransomware attacks**

The Hague, Netherlands  
3-4 November 2022



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



# Threats, trends and impact of ransomware attacks in Albania



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## “Albania in the Digital Age”

From 2008 one of the main objectives of the Albanian government was "Albania in the Digital Age".

New legislation was adopted in line with EU standards which made possible the creation of a digitalized National Civil Registry, Electronic Procurement System, Tax Service Electronic System and Customs Declarations Electronic System.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## The National Agency for Information Society (AKSHI)

**AKSHI** was founded as an institution of the Albanian Government under the direct supervision of the Prime Minister's Office.

AKSHI's mission is to coordinate the development and administration of state and public information systems and to promote the development of “Information Society” in Albania.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## The National Agency for Information Society (AKSHI)

“GOVnet” is the network that enables safe communication and Internet communication to Albanian government institutions.

Government Data Center provides contemporary services and virtual resources to all state institutions.

There are 251 related institutions on the “GOVnet” network.

There are 473 Government web pages hosted at AKSHI's Data Center.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## e-Albania

In 2012, AKSHI developed and presented the “e-Albania” portal, which serves as a gateway through which any interested citizen can access, via electronic means, services provided by public institutions in Albania. At that time this portal offers 12 services.

In 2015, “e-Albania” was completely redesigned and brings innovations with online payments and increased the capacity of services.

“e-Albania” is connected to the Government Interaction Platform, which is the basic architecture on which interaction with the electronic systems of public institutions is enabled.

In 2022, there are 1.225 electronic services provided by the government portal “e-Albania”.




Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe










## e-Albania



**KRYESORE E-SHËRBIME SHËRBIME INFORMATIVE NDIHMË DHE SUPORT**

[Hyr](#) | [Regjistrohu / Register](#)  
Register your business as a foreign citizen

*kërko shërbimin* 

 <p><b>DOKUMENTE ME VULË ELEKTRONIKE</b></p>	 <p><b>PAGESA ELEKTRONIKE</b></p>		
 <p><b>FAMILJA</b></p> <ul style="list-style-type: none"><li>&gt; Certifikatë personale</li><li>&gt; Certifikatë familjare</li><li>&gt; Deklarimi i adresës së shte...</li></ul> <p><a href="#">Të tjera...</a></p>	 <p><b>ARSIMI</b></p> <ul style="list-style-type: none"><li>&gt; Regjistrimi në klasë të dhjetë</li><li>&gt; Regjistrimi në gjimnaz me k...</li><li>&gt; Regjistrimi në shkollë të m...</li></ul> <p><a href="#">Të tjera...</a></p>	 <p><b>PUNA</b></p> <ul style="list-style-type: none"><li>&gt; Leje Pune</li><li>&gt; Vërtetim si punëkërkues</li><li>&gt; Aplikim për regjistrim në p...</li></ul> <p><a href="#">Të tjera...</a></p>	 <p><b>SHËNDETËSIA DHE MBROJTJA SOCIALE</b></p> <ul style="list-style-type: none"><li>&gt; Kërkesë për vaksinim Covid-19</li><li>&gt; Certifikatë Vaksinimi, Test...</li><li>&gt; Aplikim për recetë të rimbu...</li></ul> <p><a href="#">Të tjera...</a></p>



Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented  
by the Council of Europe



## e-Albania



### KONTRIBUTET DHE PENSIONI

- > Aplikim për pension pleqërie
- > Vërtetim për pagesën e kont...
- > Kërkesë për shpërblim lindj...

Të tjera...



### GJENDJA GJYQËSORE

- > Formulari dekriminalizimit
- > Dëshmia e Penalitetit
- > Vërtetim i periudhës

Të tjera...



### BIZNESI IM

- > Vërtetim për aktivitet ekon...
- > Aplikim për regjistrimin e ...
- > Gjendja e llogarisë parapag...
- > Kërkesë për ushtrimin e ve...

Të tjera...



### LEJE DHE LICENCA

- > Leje Ndërtimi
- > Licencë individuale
- > Lëshim i titullit të licenc...

Të tjera...



### TRANSPORT DHE AUTOMJETE

- > Rezervim për Kontrollin Tek...
- > Vërtetim leje drejtimi
- > Taksat e automjeteve

Të tjera...



### PASURI E PALUAJTSHME

- > Certifikatë pronësie
- > Aplikim për lëshim vërtetim...
- > Vërtetim për legalizim

Të tjera...



### SHËRBIMET KONSULLORE ONLINE

- > Pasaportë dhe kartë identiteti
- > Vërtetim konsullor
- > Regjistrim fëmije
- > Vërtetim për vetëdeklarim p...

Të tjera...



### SHËRBIMET DOGANORE

- > Statusi i deklarimit të tra...
- > Statusi i deklarimit dogano...
- > Statusi i pagesave në doganë

Të tjera...

**E RËNDËSISHME!**





Funded  
by the European Union  
and the Council of Europe

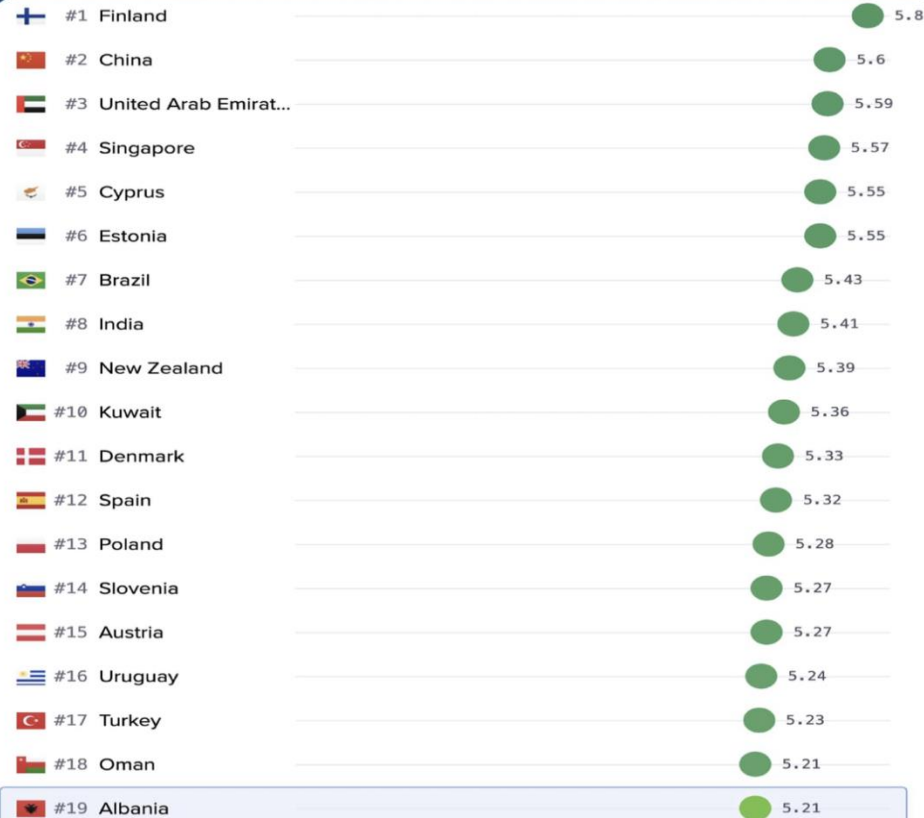


Implemented  
by the Council of Europe



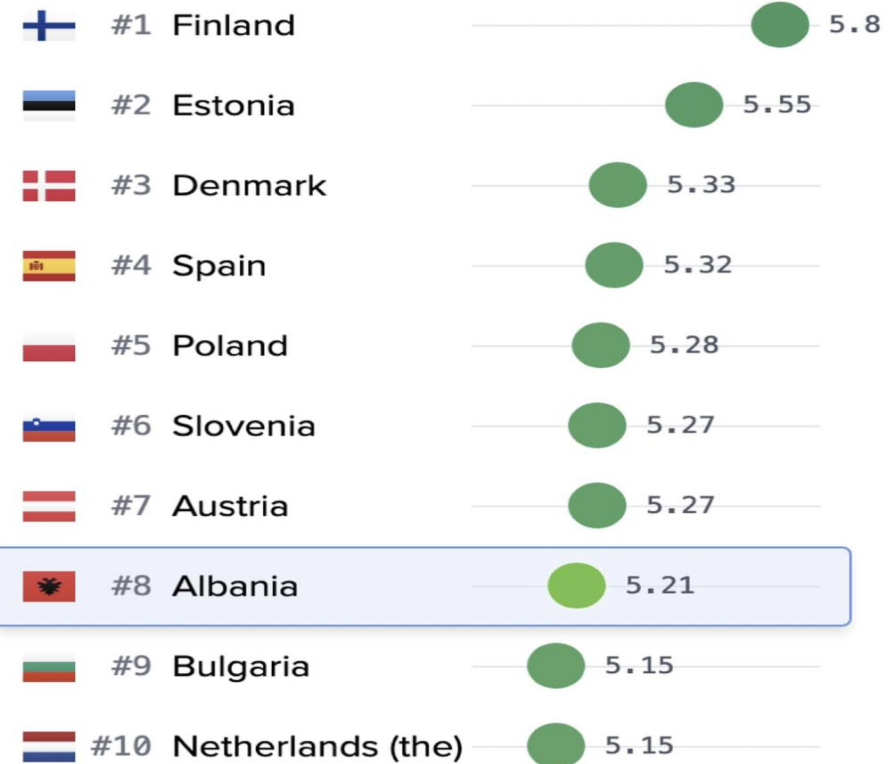
## DIGITAL PUBLIC SERVICES

 **#19**  
**WORLD**



## DIGITAL PUBLIC SERVICES

 **#8**  
**EUROPE**





Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

- On 15 July 2022.

At 13:00, security platforms identified the start of the distribution of a Ransomware attack on the network, which affected some end users in public institutions.

The Albanian government announced that all government websites, including the online services platform “e-Albania”, are temporarily out of service, following a cyber attack from an undisclosed source.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

- On July 16 (Wiper Attack).

When network defenders identified the attack and began to respond to the ransomware activity, the cyber actors changed the attack methodology in an attempt to accomplish the final objective: wiping out all digital systems.

Immediately after the wiping process was detected, AKSHI took the drastic measure of isolating all government infrastructures and systems, to prevent the expansion of the activity.

Only 10% of digital systems managed to be affected by the wiper process.



Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

- On July 18, the “Cybercrime Unit” of the State Police and the Prosecutor's Office of Tirana started investigations regarding the cyberattack on all government websites, including the online services platform “e-Albania”.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber Crime Legislation

Albania is a Party to the Council of Europe Convention on Cybercrime CETS No. 185 (Budapest Convention) and the Additional Protocol on Xenophobia and Racism Committed through Computer Systems CETS No. 189.

In 2008, Albania incorporated substantive and procedural law provisions of the Budapest Convention and relevant EU/CoE standards into the Criminal Code through Law No. 10023 date 27.11.2008 and into The Criminal Procedural Code through Law No. 10054 date 29.12.2008.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber Crime Institutions

Specialized institutions:

- Albanian State Police, Cybercrime Unit
- Prosecutor's Office, Cybercrime Unit
- Cyber Forensic Laboratory
- Electronic and Postal Communication Authority (AKEP)
- National Authority for Electronic Certification and Cyber Security (AKCESK)
- Information Society National Agency (AKSHI)
- National Cyber Security Agency (ALCIRT)
- The Information and Data Protection Commissioner
- Etc.





Funded  
by the European Union  
and the Council of Europe

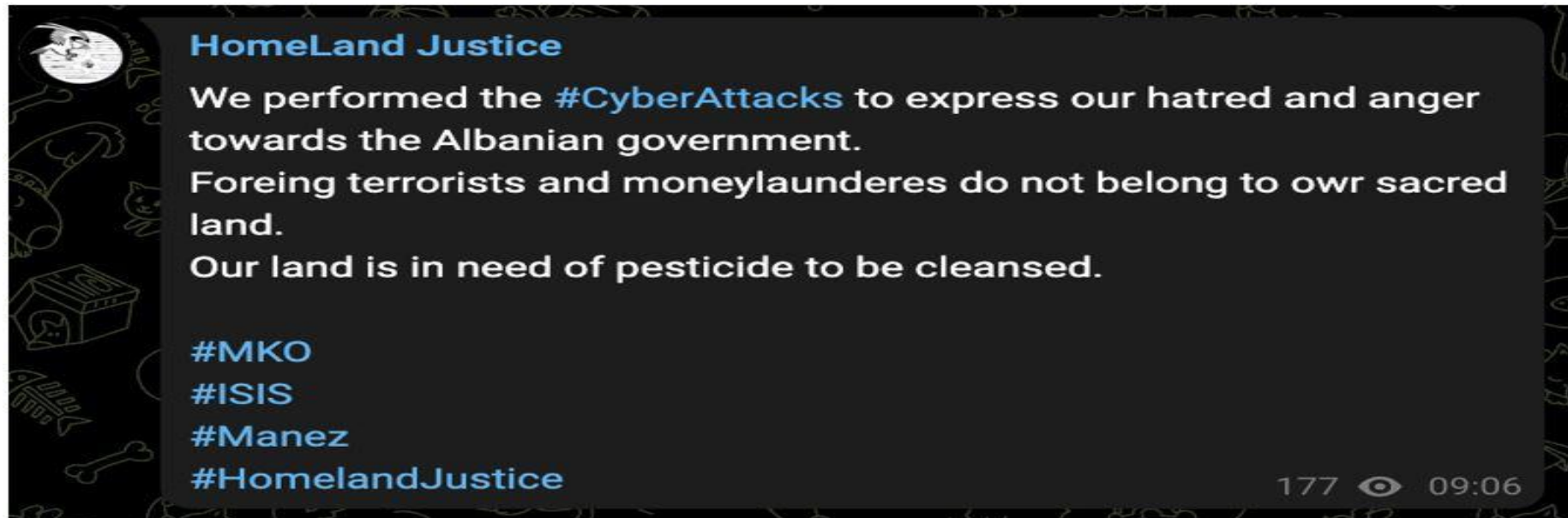


Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

- On July 23, Homeland Justice posted videos of the cyber attack on the website “homelandjustice.ru” and to a link of a Telegram channel named “HomeLand Justice.”
- On July 26, HomeLand Justice directly claimed credit for the operation on its “Telegram” channel in a message alleging corruption in the Albanian government and repeating the message from the ransom note.







Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

From late July to mid-August 2022, social media accounts associated with HomeLand Justice demonstrated a repeated pattern of advertising Albanian Government information for release, posting a poll asking respondents to select the government information to be released by HomeLand Justice, and then releasing that information—either in a .zip file or a video of a screen recording with the documents showed.





Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

- Manëz is a town in Durrës County, where are sheltered some 3,000 members of the Iranian opposition group Mujahedeen-e-Khalq, or MEK, who had left Iraq, in 2014.
- Ties between Iran and Albania have been tense since that time. In two separate instances in 2018 and 2020, the Albanian Government expelled four Iranian diplomats for “threatening national security.”
- In July 23-24, MEK had planned to hold the “Free Iran World Summit”, with U.S. lawmakers among the invitees.
- The meeting was canceled “for security reasons and due to terrorist threats and conspiracies”.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

In the framework of the investigations carried out for this criminal proceeding, the Prosecutor's Office used the investigative tools as follows:

- Article 299/a of the Criminal Procedural Code, the prosecutor orders expeditious preservation of computer data, including traffic data, etc.
- Article 299/b CPC: the prosecutor orders expedited preservation and partial disclosure of traffic data.
- Article 191/a CPC (Production Order) The court, orders to hand over the computer data stored in a computer system or in another means of storage, from one keeping or supervising them. The court shall also order the service provider to disclose any information on the subscribers and on the services provided by it. When it is an emergency the prosecutor shall order the obligation to disclose the computer data.
- Article 208/a (Search and seizure of stored computer data) The court orders the seizure of stored computer data from computer systems. For the executions of such actions, the prosecutor can authorize an expert from Cyber Forensic Labs.
- Article 221: Interception of content data.
- *MLA requests: 22 MLA requests to England, Nederland, China, Russia, etc.*



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

Albanian IT experts and Microsoft Detection and Response Team (DART), lead an investigation into the attacks.

The experts assessed with high confidence that on July 15, 2022, actors conducted a destructive cyberattack against the Albanian government, disrupting government websites and public services.

At the same time, a separate actor leaked sensitive information that had been exfiltrated months earlier. Various websites and social media outlets were used to leak this information.



Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

Different actors responsible for distinct phases in this attack :

DEV-0842 deployed the ransomware and wiper malware

DEV-0861 gained initial access and exfiltrated data

DEV-0166 exfiltrated data

DEV-0133 probed victim infrastructure

*DEV-#### designations was a temporary name given to an unknown, emerging, or a developing cluster of threat activity*



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

### Forensic analysis

**DEV-0861** gained access to the network of an Albanian government victim in May 2021 by exploiting the CVE-2019-0604 vulnerability on an unpatched SharePoint Server, “*administrata.al*”, and fortified access by July 2021 using a misconfigured service account that was a member of the local administrative group.

Analysis of Exchange logs suggests that DEV-0861 later exfiltrated mail from the victim’s network between October 2021 and January 2022.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

DEV-0861 was observed operating from some specific IP-s, that has been used actively since 2020 in some other activities for exfiltrating mails from different organizations in the countries like Israel, Jordan, Kuwait, Saudi Arabia, Turkey, and the UAE—aligns with Iranian interests and have historically been targeted by Iranian state actors, particularly MOIS-linked actors (Iran's Ministry of Intelligence and Security ).

DEV-0166 was observed exfiltrating mail from the victim between November 2021 and May 2022.

DEV-0166 likely used the tool *Jason.exe* to access compromised mailboxes. This tool was reportedly used by actors affiliated with MOIS.



Funded  
by the European Union  
and the Council of Europe



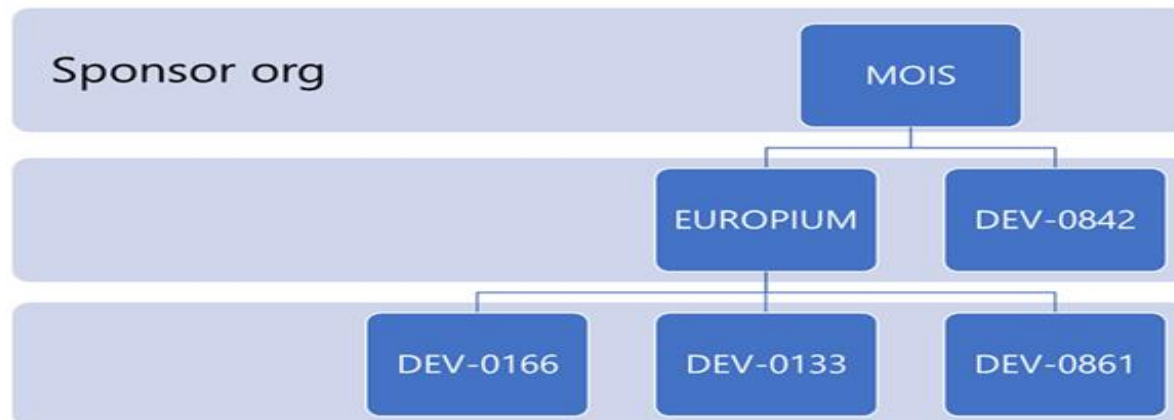
Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

The wiper that **DEV-0842** deployed in this attack used the same license key and EldoS RawDisk driver as ZeroCleare, a wiper that Iranian state actors used in an attack on a Middle East energy company in mid-2019.

In that case, IBM X-Force assessed that actors affiliated with EUROPIUM gained initial access nearly a year ahead of the wiper attack. The wiper attack was subsequently performed by a separate and unknown Iranian actor.



MSFT group name	Alias
Europium	OilRig/APT34
DEV-0861	N/A
DEV-0166	IntrudingDivisor
DEV-0133	Lyceum
DEV-0842	N/A





Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

Evidence gathered during the forensic response indicated that Iran-affiliated actors conducted the attack. This evidence includes, but is not limited to:

- The attackers were observed operating out of Iran.
- The attackers responsible for the intrusion and exfiltration of data used tools previously used by other known Iranian attackers.
- The attackers responsible for the intrusion and exfiltration of data targeted other sectors and countries that are consistent with Iranian interests.
- The wiper code was previously used by a known Iranian actor.
- The ransomware was signed by the same digital certificate used to sign other tools used by Iranian actors.



Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

On 7 September, the Albanian Government set Expulsion Order to Iranian Diplomats.

Iranian embassy staff were given 24 hours to leave the country over a the major cyberattack that the Albanian government blames on Iran.

It is the first known case of a country cutting diplomatic relations over a cyberattack.



Funded  
by the European Union  
and the Council of Europe



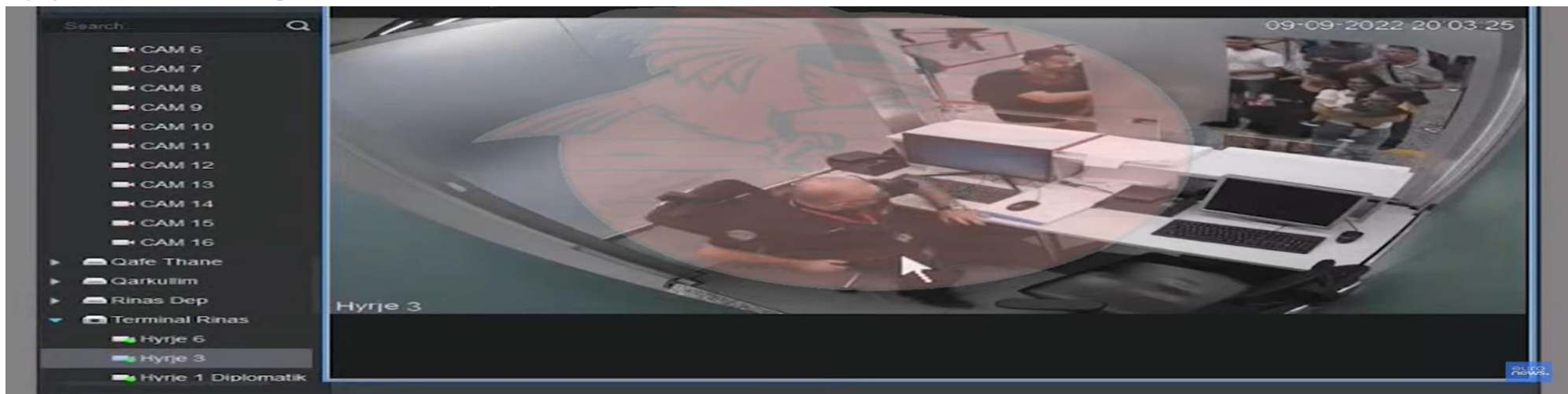
Implemented  
by the Council of Europe



## Cyber attacks against the Government of Albania

At 20:00 on September 9, the TIMS system at the border crossing points was hit by a cyber attack. All border computer systems went offline, causing chaos at border crossings and airports.

A message was sent to the policemen's computers at the border crossing points, was written "Albania is suffering and will continue to suffer for the support it has given to the MEK Iranians".





Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



## Total Information Management System (TIMS)

TIMS is a sustainable, modern and integrated, information management system, implemented within the Albanian State Police to enhance capabilities in criminal investigation, case management, criminal intelligence analysis, border control and overall police administration.

TIMS enables police officials, deployed throughout the country to access the integrated border, criminal records and criminal analysis databases.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



The data storage and transmission systems of the State Police were found under a cyber attack.

Systems and infrastructures of the General Directorate of the State Police, are totally independent network, independent Active Directory, Exchange - system of email, unrelated to other infrastructures.

For safety reasons, State Police systems, including TIMS, have been temporarily closed.

It has been proven that actors accessed a part of TIMS system, specifically, the data related to Border Crossing Points.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



A number of emails, documents and memos between authorities, institutions, politicians and ambassadors have been published via the Homeland Security Telegram channel.

One published document reveals that the Counter-Terrorism Unit in Kosovo was made aware of a plan to kill Prime Minister.

Another document relates to an alleged plot to kill the leader of the the Albanian opposition party, in 2017.



Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe



Cyber actors use similar TTPs and malware as the cyber attacks in July.

These actions were likely done in retaliation for public attribution of the cyber attacks in July and severed diplomatic ties between Albania and





Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented  
by the Council of Europe



Telegram: @HomelandJustice

Selling:

E-Albania - 0.025 BTC  
TIMS system - 0.025 BTC  
Both of them - 0.04 BTC

Contact @HomelandJustice on Telegram

1

13 11:20 AM

Homeland Justice

Homeland Justice Today at 11:35

To get the full e-Albania database (every file included)  
800GB+  
0.025 BTC  
Payment in DMs

The TIMS system and database (includes all persons who leave and enter Albania)  
0.025 BTC  
Payment in DMs

If you want e-Albania + TIMS  
0.04 BTC for both

Links will be sent immediately  
Telegram: @HomelandJustice

Contact @HomelandJustice on Telegram

6 4

394 11:42 AM





Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented  
by the Council of Europe



← **Homeland Justice** 9.3K subscribers

**Pinned Message**  
The Pandora's box has been opened. Arroga...

2 1 9.9K 6:30 PM

**October 10**

**Homeland Justice** Today at 21:46  
Deep Sea system (multi-database of police)  
Full system includes more than 100,000 individuals.  
0.5 BTC

Payment in DMs, links will be sent immediately.  
Info of what this system includes, will be explained below.  
Telegram: @HomelandJustice

The Pandora's box has been opened.  
Arrogant government continues to  
desperately deny the truth.

Deep Sea system (multi-database of police)  
Full system includes more than 100,000 individuals.  
0.5 BTC

Payment in DMs, links will be sent immediately.  
Info of what this system includes, will be explained below.  
Telegram: @HomelandJustice

The Pandora's box has been opened.  
Arrogant government continues to  
desperately deny the truth.

Deep Sea includes all possible information  
for any person with any criminal history. It  
includes detailed background information,  
current known location and contacts,  
detailed reports made by police agents,  
also information of these police agents.  
Around 100,000 names are on this system,  
passport info and travel info are also  
attached.  
Contains more than 20 small databases  
inside  
Contact @HomelandJustice to purchase



Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented  
by the Council of Europe



A few days after the cyber attack, the **TIMS** system and other digital systems of the State Police are back to work.

After 3 weeks of the attack, 1214 out of 1.225 electronic services provided on the government portal “**e-Albania**”, can be used by citizens and businesses with the same speed and quality as before.

Investigations for this cyber attack are running.



---

Funded  
by the European Union  
and the Council of Europe



---

Implemented  
by the Council of Europe



Thank YOU