



**REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY**

Analysis of illegitimate Smishing domains

**Version: 1.0
Datë: 22/07/2025**

Table of Contents

Technical Information	4
Study Case <i>raiffeisen-lidhje[.]com</i>.....	4
Study Case <i>raiffeisenrinov[.]com</i>	8
Conclusions	12
Recommendations	12

Table of Figures

Figure 1 Web page returned by the server following URL invocation.....	4
Figure 3 urlscan.io	5
Figure 4 anyrun sandbox scan	6
Figure 5 mxtoolbox scanim	6
Figure 6 Connection made when accessing the URL <i>raiffeisen-link.com</i>	6
Figure 7 JS script that runs when accessing the URL.....	7
Figure 8 Initial user interface	8
Figure 9 Second Interface	8
Figure 10 MFA check	9

This report contains limitations and should be interpreted with caution. The findings are based on the information available at the time of its preparation and may not reflect subsequent developments.

Phase 1:

Information Sources. The analysis relies on data and resources accessible during the reporting period. Some elements may differ from current or future developments due to the dynamic nature of cyber threats.

Phase 2:

Analysis Details: Due to resource constraints, certain aspects of the malicious file may not have been fully examined. Any undiscovered or future indicators could alter the conclusions presented in this report.

Phase 3:

Data Sensitivity and Confidentiality: To protect sensitive sources and confidential information, some technical details have been intentionally redacted or omitted. This decision was made to preserve the integrity and security of the data used in the investigation.

*This report is not a **end-state analysis**.*

The findings are based on the best available evidence at the time of analysis. No guarantees are made regarding future updates or changes to the reported information. The authors disclaim responsibility for any misuse or consequences arising from decisions based solely on this report.

Technical Information

As part of ongoing monitoring efforts targeting phishing campaigns against citizens of the Republic of Albania, several **illegitimate domains** have been identified. These domains were created with the intent to **deceive users through impersonation**, mimicking official websites of second-tier banks to collect sensitive personal data

Purpose of the Malicious Activity

Malicious website replicate the **design and structure** of Raiffeisen Bank's official portal to gain the trust of unsuspecting users. The primary objective is to exfiltrate sensitive information, including:

- **Bank card details:** card number, CVV, and PIN
- **E-banking login credentials**
- **Additional sensitive data:** device information, browser metadata, and session identifiers

Study Case raiffeisen-lidhje[.]com

IP: 15[.]197[.]130[.]221 –has previously been reported as part of smishing campaigns.

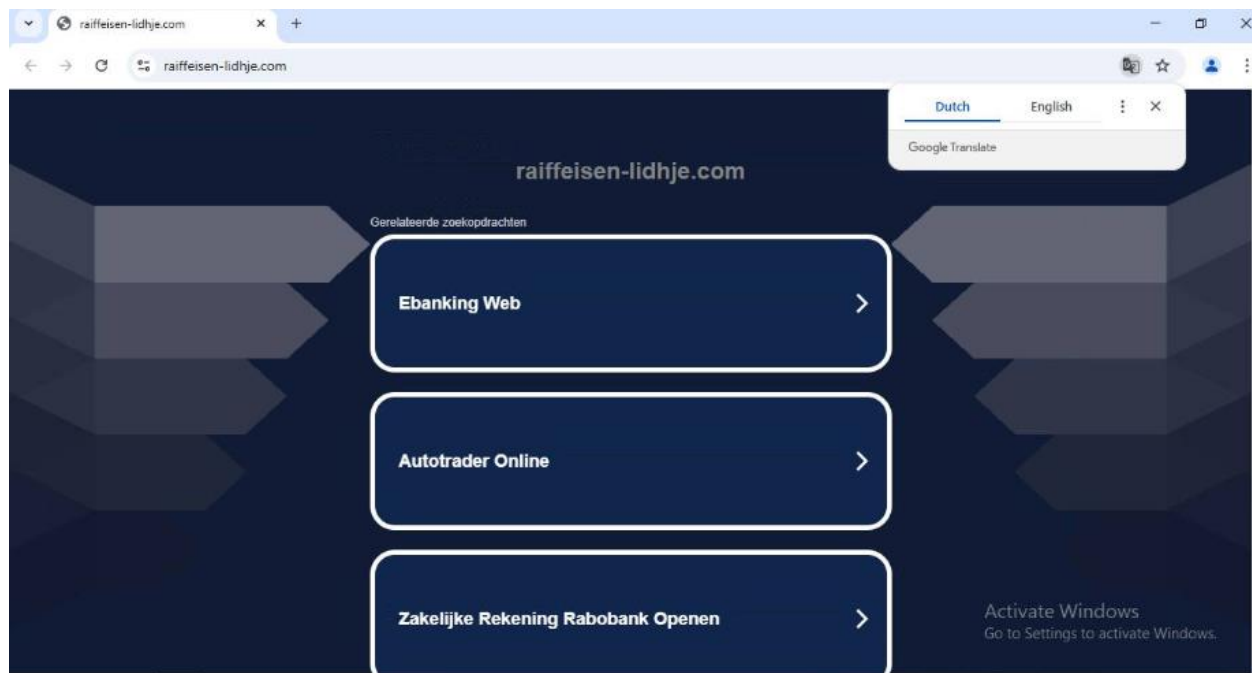


Figure 1 Web page returned by the server following URL invocation



Figure 2 Report and Analysis on URL raiffeisen-link[.]com

During the analysis, several suspicious elements were identified such as:

Most notably, the domain under analysis is associated with the IP address **15[.]197[.]130[.]221**, which has been repeatedly flagged in threat intelligence platforms and for its involvement in **multiple smishing campaigns**. These campaigns often leverage deceptive SMS messages to redirect victims to impersonation sites designed to exfiltrate sensitive data , similar to our case,as shown in the reports below, both created in 2025:

- <https://cofense.com/blog/exploiting-sms-threat-actors-use-social-engineering-to-target-companies>
- <https://www.recordedfuture.com/research/stimmen-aus-moskau-russian-influence-operations-target-german-elections>

JoeSandbox: Has flagged potential malicious behavior.

urlscan.io: Has classified the URL as “malicious”.

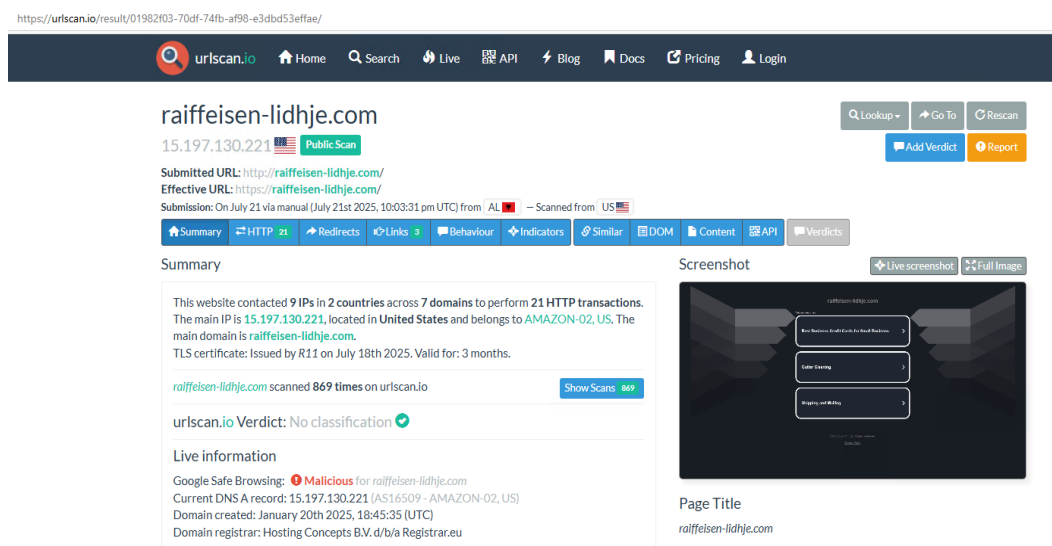


Figure 2 urlscan.io

any.run: Reported as "malicious activity".

General Info



URL: <https://euob.youseasky.com/sxp/i/224f85302aa2b6ec30aac9a85da2cbf9.js>
Full analysis: <https://app.any.run/tasks/76d00fe4-2b28-4c53-91b3-30df51cbda1a>
Verdict: **Malicious activity**
Analysis date: June 18, 2025 at 23:31:59
OS: Windows 10 Professional (build: 19044, 64 bit)
Indicators:  
MD5: 55A77A1E8263E7196D6440E812FE7C0F
SHA1: 28D425439E3CEF70276D8181866C4637034C68AE
SHA256: 9C72D972BD85C1BFD5E63EBAD76F26E9D77A496A163751C80335A0E18DFE310C
SSDEEP: 3:N8ilbGtKaJKHwKEE3MEXGOun:2ilyTPJKHwkt3M+GOu

Figure 3 anyrun sandbox scan

MX Toolbox dhe VirusTotal: The domain appears on a blacklist

Blacklists
blacklist.raiffeisen-lidhje.com - 2 Tests Failed

Category	Host	Result	
blacklist	raiffeisen-lidhje.com	Blacklisted by Spamhaus DBL	More Info
blacklist	raiffeisen-lidhje.com	Blacklisted by SURBL multi	More Info
blacklist	raiffeisen-lidhje.com	lvmURI	More Info
blacklist	raiffeisen-lidhje.com	Nordspam DBL	More Info
blacklist	raiffeisen-lidhje.com	SEM FRESH	More Info
blacklist	raiffeisen-lidhje.com	SEM URI	More Info
blacklist	raiffeisen-lidhje.com	SEM URIRED	More Info
blacklist	raiffeisen-lidhje.com	SORBS RHSBL BADCONF	More Info
blacklist	raiffeisen-lidhje.com	SORBS RHSBL NOMAIL	More Info

Figure 4 mxtoolbox scanim

Through an inspection using browser developer tools (*Inspect Element*), a request to a URL containing an obfuscated JS script was identified.

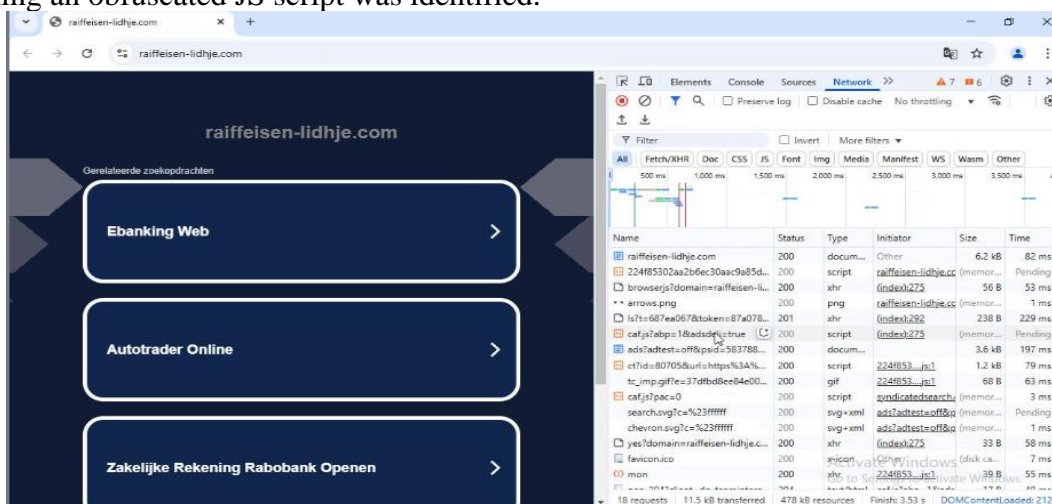


Figure 5 Connection made when accessing the URL raiffeisen-link.com

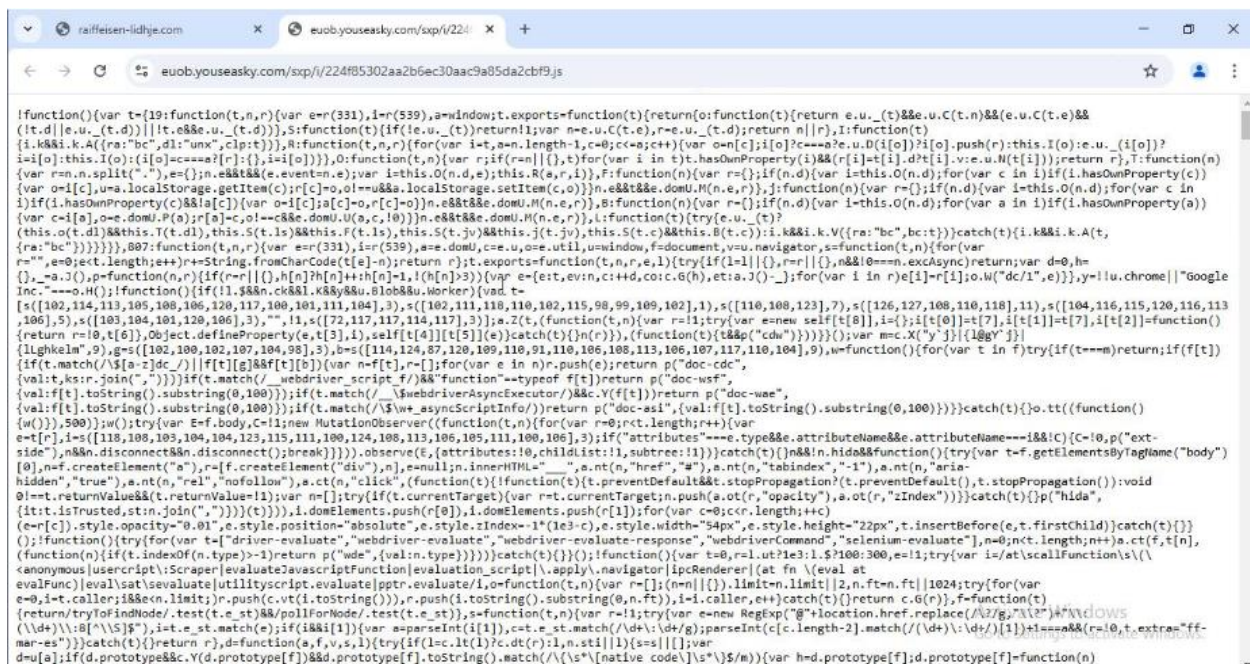
A screenshot of a web browser window showing a phishing page. The address bar displays a URL from 'euob.youseasky.com'. The browser's developer console is open, showing a large block of obfuscated JavaScript code. The code is a single long line with many function calls and variable assignments, designed to be difficult to read. It appears to be a mix of legitimate browser APIs and malicious code for data collection and evasion. The code includes references to 'window', 'document', 'navigator', and various browser-specific APIs like 'localStorage' and 'localStorage.getItem'. It also includes some base64-encoded strings and complex conditional logic.

Figure 6 JS script that runs when accessing the URL.

This hidden script (obfuscated JavaScript) on the phishing page is designed to:

Collect data from the user's browser and device, assign values to various objects and create specific paths if they do not already exist, in order to communicate with the targeted page. It also performs requests to determine geolocation and gathers additional information. Another function of this code is to check whether the device has any form of authentication enabled (e.g., biometric, FaceID, etc.), information that can be misused in combination with other data such as browser version, screen resolution, and similar parameters to create a browser fingerprint and track the user's activity. This mechanism may also be used to compromise user credentials by exploiting biometric authentication.

PublicKeyCredential.isUserVerifyingPlatformAuthenticatorAvailable()

Study Case *raiffeisenrinov[.]com*

During the proactive monitoring of phishing campaigns targeting Raiffeisen Bank customers, another illegitimate domain has been identified: **raiffeisenrinov[.]com**. This domain was created with the explicit intent of impersonating the bank, following the same tactics previously observed in malicious campaigns that have been detected and blocked.

The objective of this domain remains consistent: to obtain **e-banking credentials**, **bank card information**, and other **personal and sensitive user data**.

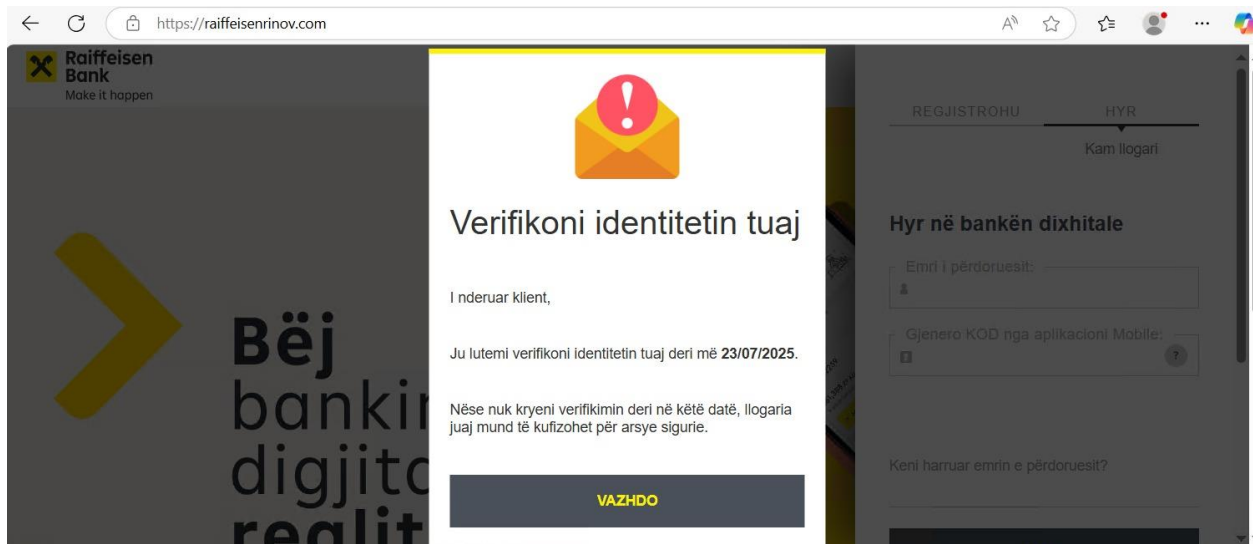


Figure 7 Initial user interface

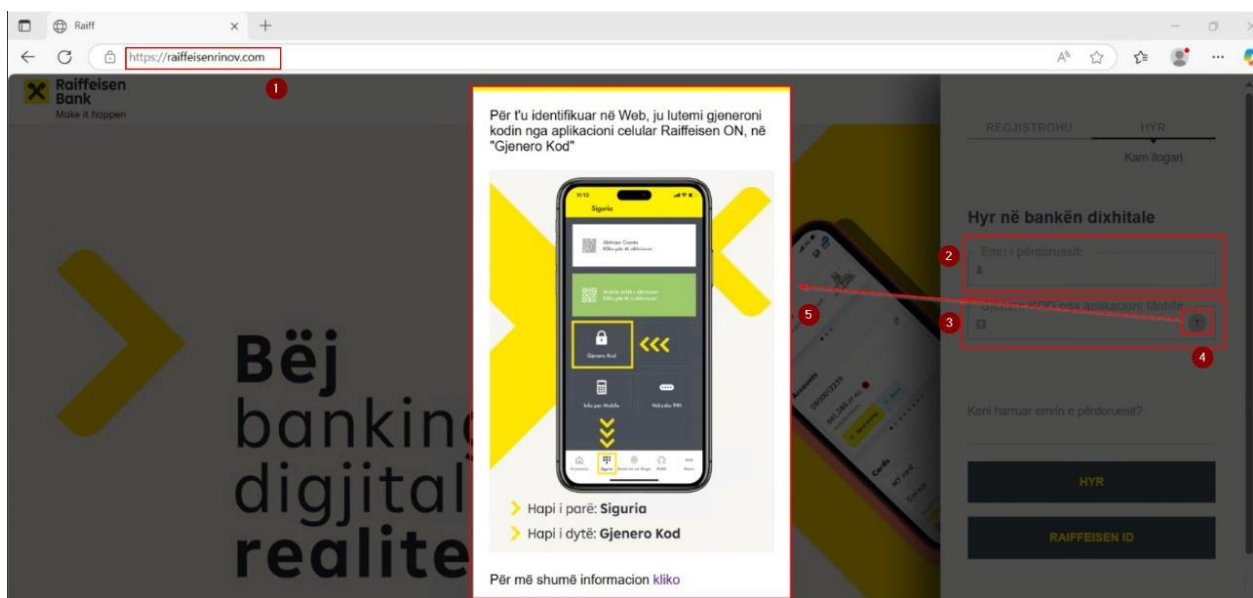


Figure 8 Second Interface

- 1- Malicious Domain
- 2- Username entered by the victim
- 3- Token generated by the mobile application
- 4- Information related to the manual
- 5- Manual

Once the victim clicks “Login,” the data is automatically transmitted to the attacker’s server.

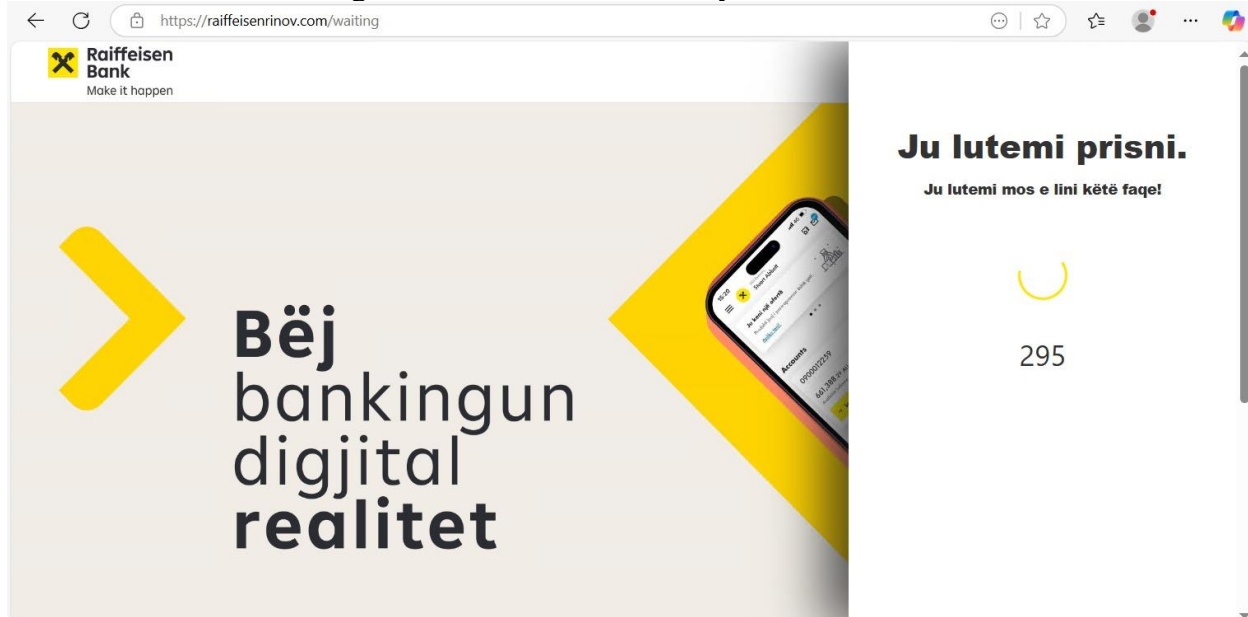


Figure 9 MFA check

On July 22, 2025, an analysis was conducted on the domain **raiffeisenrinov.com**, revealing several indicators strongly suggesting that the domain was created for **fraudulent purposes**, specifically to impersonate the well-known financial institution **Raiffeisen Bank**. The investigation was initiated following a **smishing incident**, in which a user received this link via SMS.

The domain was registered on the same day using **foreign infrastructure located in the United States**, through an **unidentified hosting provider**. The site lacks any legitimate content or functional interface for end users. Instead, it immediately generates a **PHPSESSID cookie** without any user interaction, indicating that the page is likely built on a **minimal framework or phishing kit**.

Further technical analysis revealed:

- **Absence of meaningful HTML content**
- An **SSL certificate issued by an unrecognized authority ("R11")**
- Presence of **search engine directives** such as X-Robots-Tag: noindex, nofollow, which prevent the page from being indexed—commonly used to hide malicious infrastructure from public visibility

These characteristics align with known patterns of phishing infrastructure used in smishing campaigns targeting banking customers.

The elements involved in this behavior are consistent with known patterns of fraudulent websites used to collect banking credentials or sensitive data through visual imitation of trusted pages..

Technical Elements Identified

Category	Value / Description
Domain	raiffeisenrinov.com
Registration Date	22.07.2025
Hosted IP	155.94.155.102 (Charleston, SC, USA)
Web Server	nginx
X-Powered-By	PHP/8.3.23 on Plesk
Content	Content-Length: 0, no HTML delivered
SSL Certificate	Issued by "R11", not recognized by public Certificate Authorities (CAs)
Security Protocol	TLS 1.3, cipher: AES_128_GCM; ECH (Encrypted Client Hello) not enabled
Cookie	PHPSESSID = ebalvms3mn269g0rf13l6irobf (session; not HttpOnly, not Secure) ⁴
X-Robots-Tag	noindex, nofollow — prevents indexing and link following by search engines ⁶
Pragma / Cache	no-store, no-cache, must-revalidate — disables caching
Link	favicon.ico Requested but returned an empty response

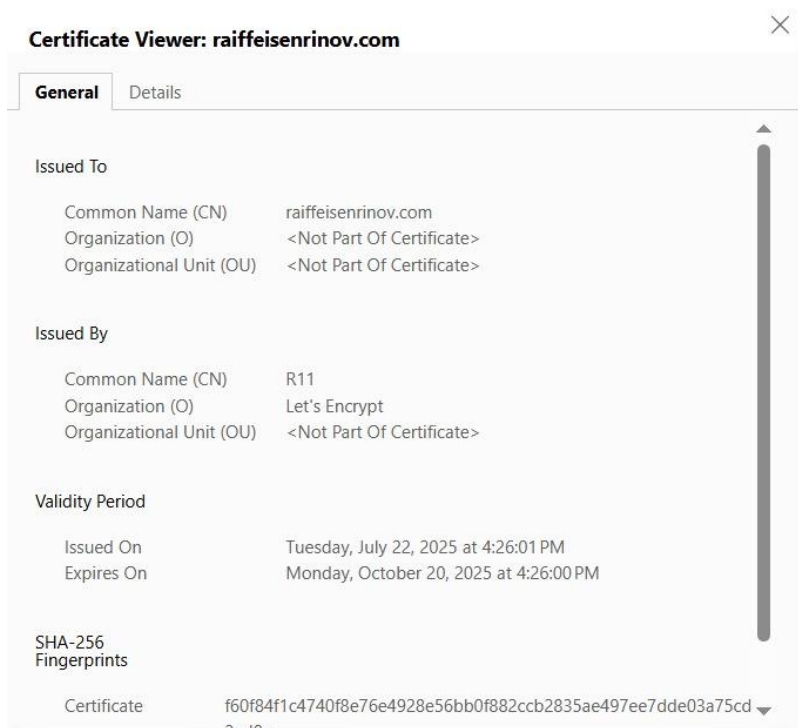


Figure 11 SSL/TLS certificate details used for domain encryption

Indicators of Compromise

Number	Type	By Usage (Domain/IP)	Status	Description
1	Domain	perditesim-raiffeisen[.]com	Blocked	Imitates official websites, collects user data
2	URL	https[:]//shposta-al[.]com	Blocked	Phishing page disguised as a postal notification
3	Domain	raiffeisen-rinovoj[.]com	Blocked	Credential renewal scam
4	IP Address	192[.]3[.]176[.]117	Blocked	IP used to host phishing content
5	Domain	raiffeisen-lidhje[.]com	Blocked	Phishing activity, analyzed as malicious
6	Domain	al-raiffeisen[.]com	Blocked	Imitation of Albania's national domain
7	Domain	lidhje-raiffeisen[.]com	Blocked	Fraudulent domain
8	Domain	lidhje-al[.]com	Blocked	Fake link scam

Number	Type	By Usage (Domain/IP)	Status	Description
9	Domain	kontakt-raiffeisen[.]com	Blocked	Used for data theft
10	Domain	raiffeisen-lidhje-al[.]com	Blocked	Combined tactics to deceive Albanian users
11	Domain	raiffeisen-albania[.]com	Blocked	Domain similar to the official one
12	Domain	raiffeisen-lajm[.]com	Blocked	Presented as a bank news source
13	Domain	raiffeisen-info[.]com	Blocked	Domain created for false information dissemination
14	IP Address	45[.]139[.]104[.]97	Blocked	Host phishing
15	IP Address	45[.]139[.]104[.]34	Blocked	Host linked to phishing
16	Domain	raiffeisenrinov[.]com	Reported for blocking	Account renewal scam
17	IP Address	Reported for blocking	Reported for blocking	Phishing infrastructure

Conclusions

- The phishing campaign is organized and directly targets Raiffeisen Bank customers.
- The domains involved are created with the intent to deceive users and steal critical banking credentials.
- In cooperation with AKEP and the bank's internal security teams, most of the suspicious websites have been swiftly blocked.
- All of the aforementioned domains have been successfully taken down.
- In-depth technical analyses have been conducted to assess the associated risks.
- Active communication continues between Raiffeisen Bank and AKEP experts to address new cases and implement proactive measures.

Recommendations

The **National Cybersecurity Authority (NCSA)** recommends:

- Implementing **anti-phishing mechanisms** on client endpoints and email systems.
- Launching **awareness campaigns** to educate customers about suspicious messages.

- Maintaining **ongoing collaboration** with AKEP, ISPs, and international platforms for rapid takedown of malicious domains.
- **Immediately reporting** any suspicious domain or activity to NCSA, enabling real-time blocking of harmful links.