SPHERE TI

Threat Intelligence Report

by Alphatechs

Albania e-Visa Service Impersonation Campaign

Fraudulent Domains, Infostealer Exposure & Citizen Risk

Report Date	June 11, 2026
Classification	TLP:WHITE — For public distribution
Author	Sphere TI Research Team, Alphatechs
Target Service	Republic of Albania e-Visa Application System (e-visa.al)
Threat Type	Brand Impersonation / Phishing Infrastructure / Infostealer Exposure
Severity	HIGH
Reference	Politiko.al — April 5, 2026 | Albanian Ministry of Foreign Affairs Advisory

1. Executive Summary

Sphere TI, the threat intelligence platform of Alphatechs, has identified and analyzed an active impersonation campaign targeting the Republic of Albania's official electronic visa application service, operated at e-visa.al. This report documents the discovery of multiple fraudulent domains designed to mimic the legitimate government portal, the collection of infostealer telemetry exposing compromised applicants, and the broader threat landscape these sites represent.

The Albanian Ministry for Europe and Foreign Affairs (MEFJ) publicly acknowledged the existence of at least one such fraudulent website in April 2026, warning citizens and foreigners to exercise maximum caution and use only the official portal. Sphere TI has identified additional impersonation infrastructure beyond what was disclosed in that advisory.

Key Findings

- 8 fraudulent or suspicious domains identified, registered between October 2025 and June 2026
- At least 3 sites are actively operational and visually cloned from the legitimate service
- 1,950 infostealer-exposed systems found linked to the e-visa.al domain
- Exposed credentials include applicants with passport and visa data at risk
- Albanian government has issued a public advisory; more domains remain active

2. Background: The Legitimate Service

The official Albanian e-Visa Application System is accessible at https://e-visa.al and is operated directly by the Albanian government. It enables foreign nationals to apply for electronic visas online prior to traveling to Albania by air, land, or sea. The system covers multiple visa categories including Electronic Visas, Stamped Visas, and Type A and Type C visas.

Notably, Albania maintains a visa exemption policy allowing stays of up to 90 days in a 180-day period for holders of valid Schengen visas or permits of stay, US/UK visas, 10-year UAE residence permits, and several other qualifying documents. This broad eligibility means the portal is used by a large and geographically diverse population of international travelers, making it a high-value target for fraudulent impersonation.

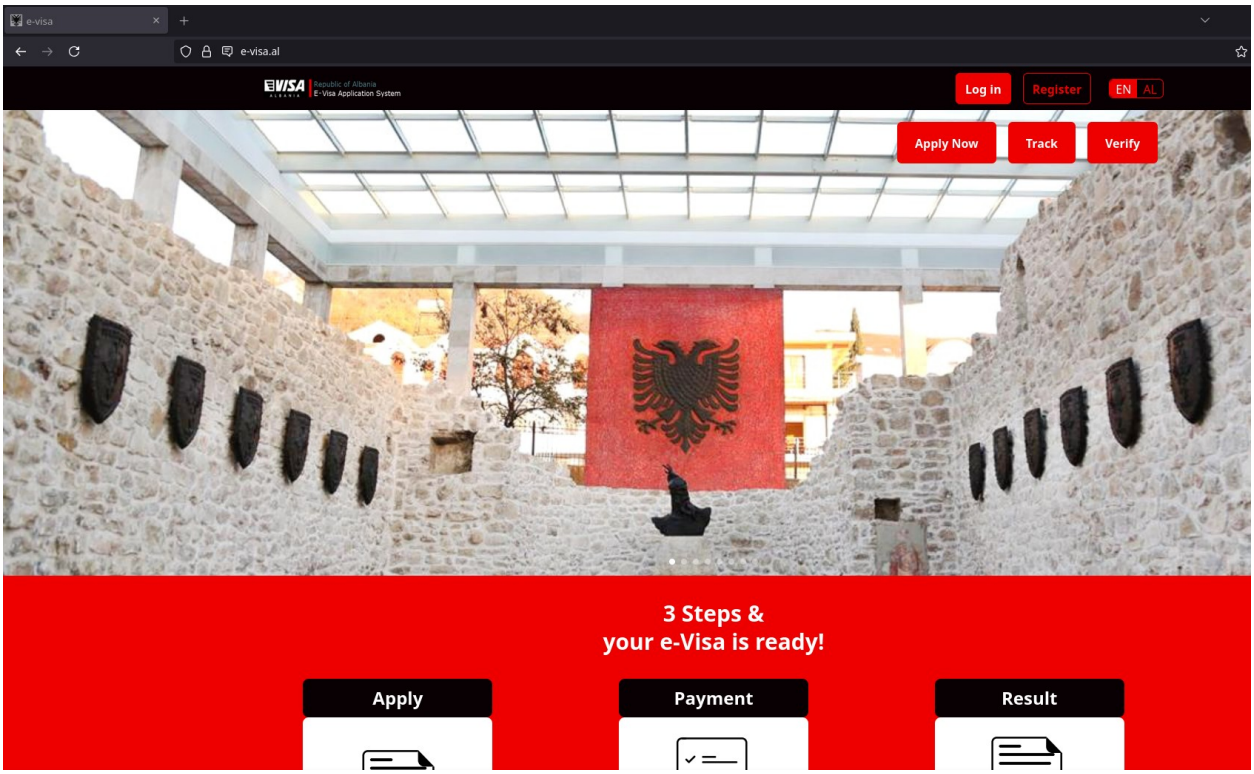

Figure 1 — The legitimate Republic of Albania e-Visa Application System at e-visa.al

3. Impersonation Campaign Overview

Through continuous certificate transparency (CT) log monitoring and new domain registration monitoring, Sphere TI identified a cluster of domains registered between late 2025 and mid-2026 that closely replicate the branding, layout, and official language of the Albanian government visa portal. The domains exploit the recognizable "evisa-albania" and "e-visa-al" keyword patterns to achieve high search engine visibility and to deceive users who may be searching for the official service.

In April 2026, the Albanian Ministry for Europe and Foreign Affairs publicly warned of a specific fraudulent website (evisia-al.com) imitating the official electronic visa application services. Sphere TI's research reveals this is not an isolated incident but part of a broader, ongoing impersonation campaign with multiple concurrent actors.

4. Identified Domains — Analysis

The following table summarizes all domains identified through CT monitoring, registration monitoring, and open-source investigation, along with their current status and threat assessment.

Domain	Registered	Status	Description	Threat Level
e-visa-al.live	02 Oct 2025	ACTIVE	Full clone site; VT flagged; Georgia Tech node	HIGH
e-visa-albania.com	26 May 2026	ACTIVE	French credential harvesting; Georgia Tech node	HIGH
evisa-albania.com.snlug.com	22 May 2026	ACTIVE	Multi-brand hijacked hosting; QR verification spoof	HIGH
evisa-albania.efcgf.la	08 Jun 2026	ACTIVE	Cloned legitimate platform; verify.php credential harvest	HIGH
evisalbania.com	28 Mar 2026	MONITORING	Likely third-party facilitator; Wix; user VT flags	MEDIUM
evisa-albania.org	06 May 2026	PARKED	Parked domain, no active content	LOW
evisa-albania.services	08 Jun 2026	UNAVAILABLE	Registered but not resolving	LOW
evisa-albania.services	28 Apr 2026	UNAVAILABLE	Earlier registration, same domain not resolving	LOW

4.1 e-visa-al.live — Full Application Clone (HIGH)

Registered in October 2025, this site presents the most complete and convincing imitation of the official service. The homepage replicates the Albanian government branding with a red-and-black color scheme, the "E-VISA | Republic of Albania" header, and identical informational content including visa exemption categories, application process descriptions, and visa type selection panels.

The domain name e-visa-al.live is specifically crafted to appear as a variant of the legitimate e-visa.al TLD. A user encountering this URL in a search result or shared link could easily mistake it for the official Albanian government domain. The site hosts a full application workflow including Log In and Register functions, enabling credential harvesting.

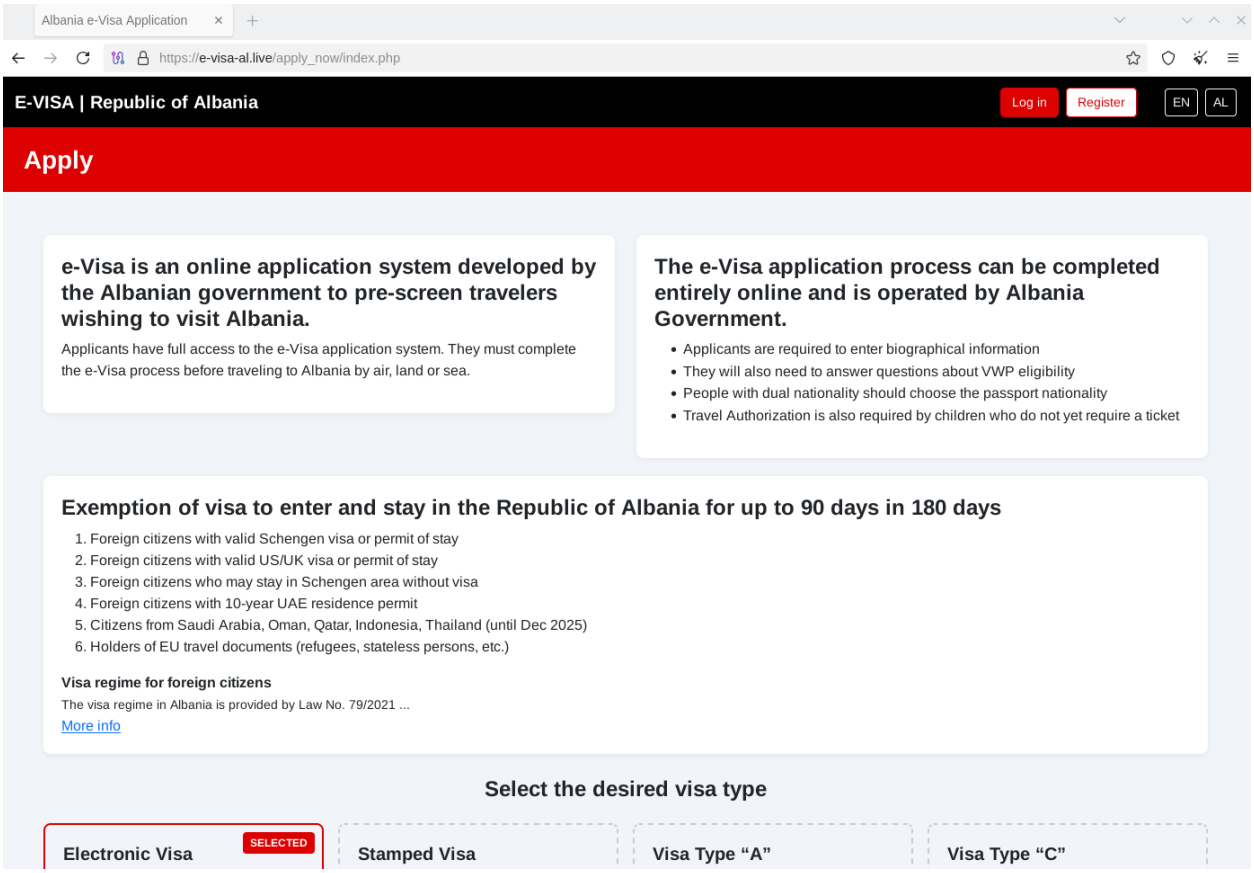

Figure 2 — e-visa-al.live presenting a complete replica of the Albanian e-Visa application interface

4.2 e-visa-albania.com — Visa Verification Phishing Page (HIGH)

This domain, registered May 26, 2026, hosts a sophisticated visa verification page presented in French, suggesting it is specifically targeting Francophone applicants — a significant traveler demographic for Albania. The page is branded as the "Republic of Albania E-Visa Application System" and requests three sensitive data points from applicants: a tracking number, visa number, and passport number.

The submission of these three fields to a fraudulent endpoint would provide the operator with everything needed to construct a fake identity profile linked to a real Albanian visa, potentially enabling document fraud or enabling follow-on phishing attacks targeted at verified applicants.

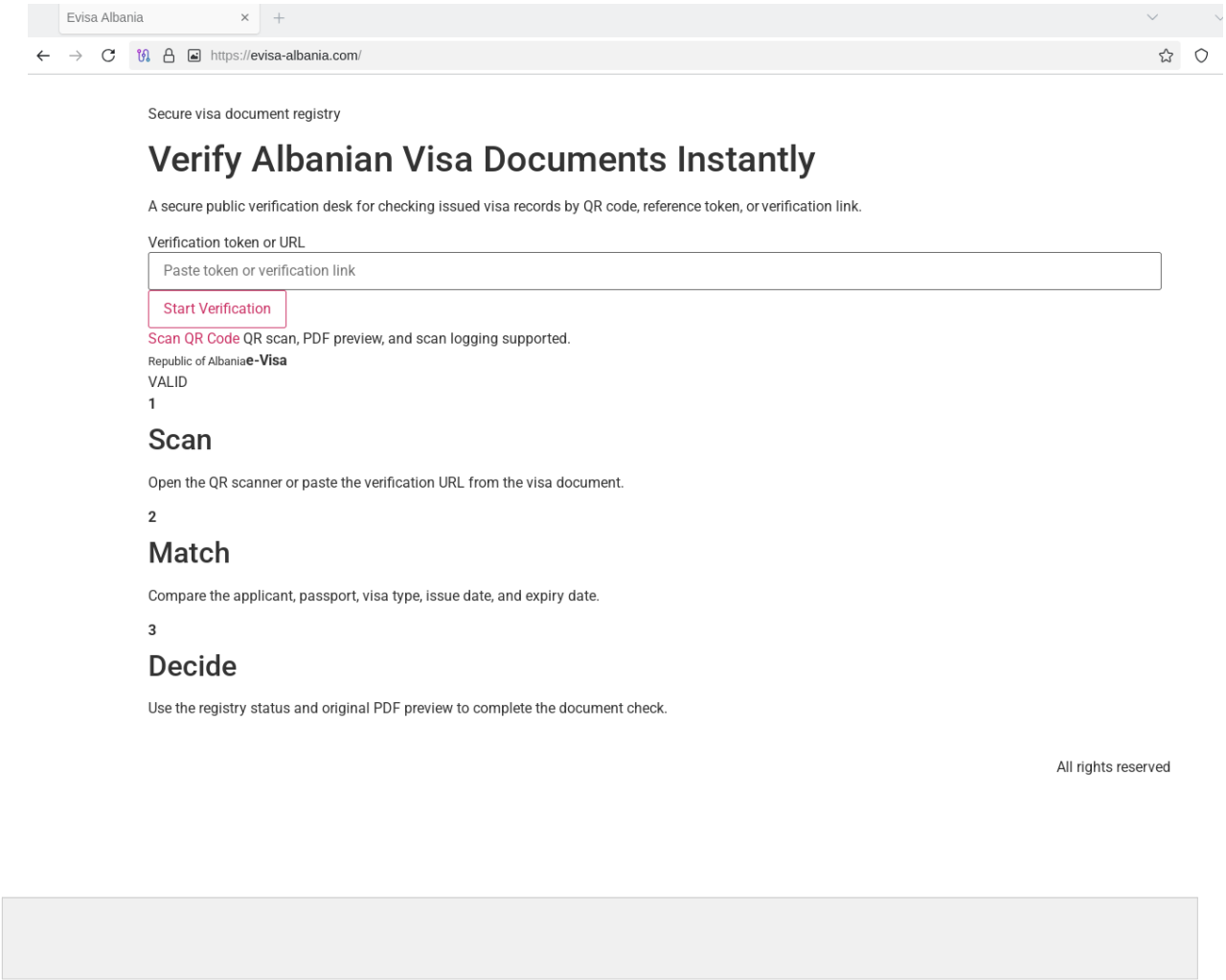

Figure 3 — e-visa-albania.com credential harvesting form targeting Francophone travelers

4.3 evisa-albania.com.snlug.com — Verification Registry Clone (HIGH)

This domain follows the pattern of hosting a fake document verification service. The site is titled "Verify Albanian Visa Documents Instantly" and presents itself as a secure public verification desk, claiming to support QR code scanning, PDF preview, and scan logging. The inclusion of a QR scan feature is notable, as it targets border officials or employers who might use QR-based

verification to authenticate visa documents, potentially causing fraudulently-issued documents to appear valid.

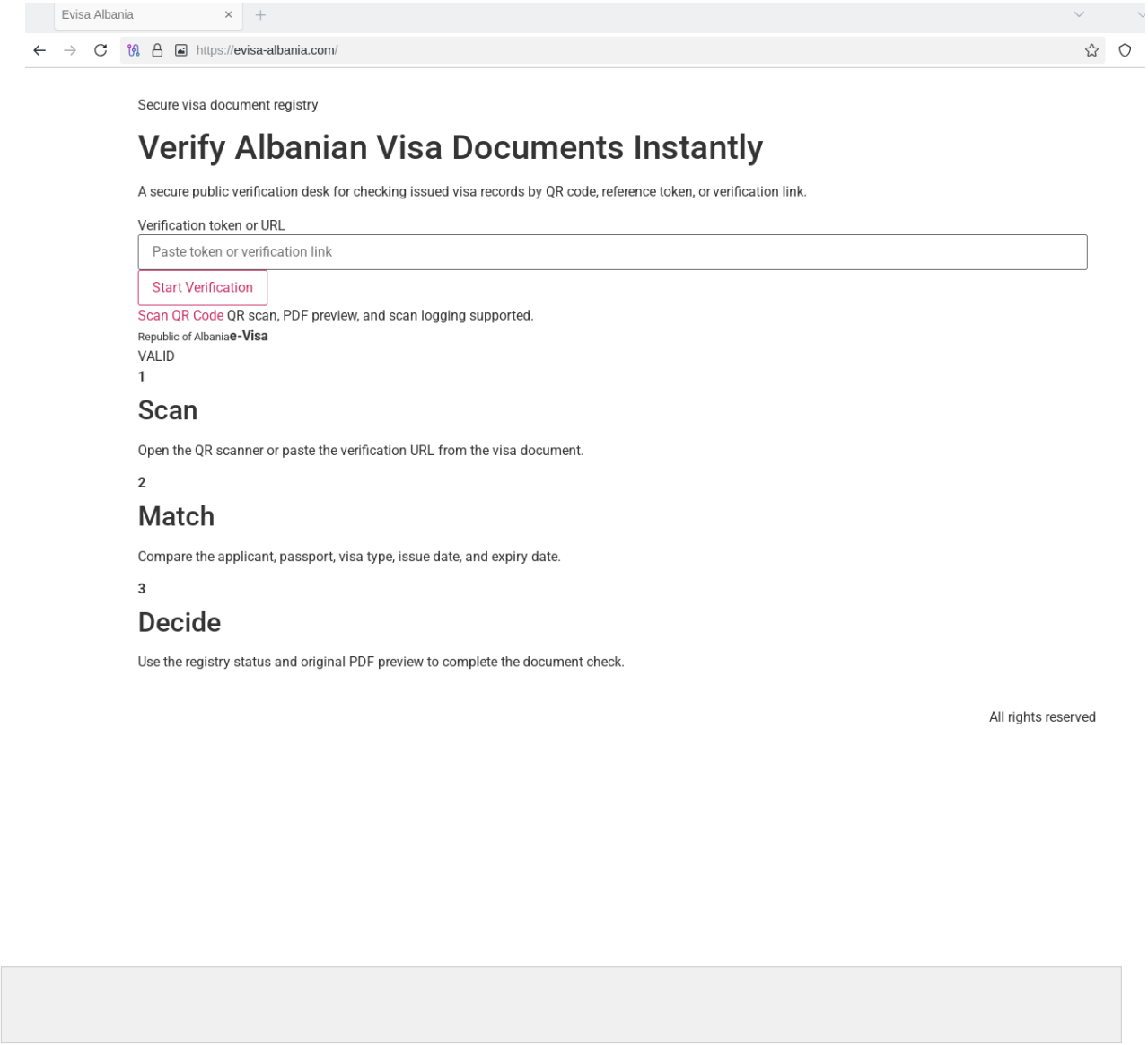

Figure 4 — evisa-albania.com.snlug.com posing as a government visa document registry

4.4 evisa-albania.efcgf.la — Cloned via Legitimate Platform | Active Credential Harvesting (HIGH)

Registered June 8, 2026 and confirmed active, this domain hosts a fully operational impersonation site at the /verify.php endpoint. The page is branded as the Republic of Albania E-Visa Application System and presents a credential harvesting form requesting Visa Number and Passport Number. The professional quality of the clone — correct logo, government color scheme, and official layout — makes it highly convincing to unsuspecting applicants.

The use of the obscure .efcgf.la TLD is a deliberate evasion tactic to avoid detection by domain monitoring tools that focus on common TLDs. The combination of a very recent registration date, active credential harvesting, brand cloning, and an unusual TLD places this domain at HIGH threat priority despite its recent appearance.

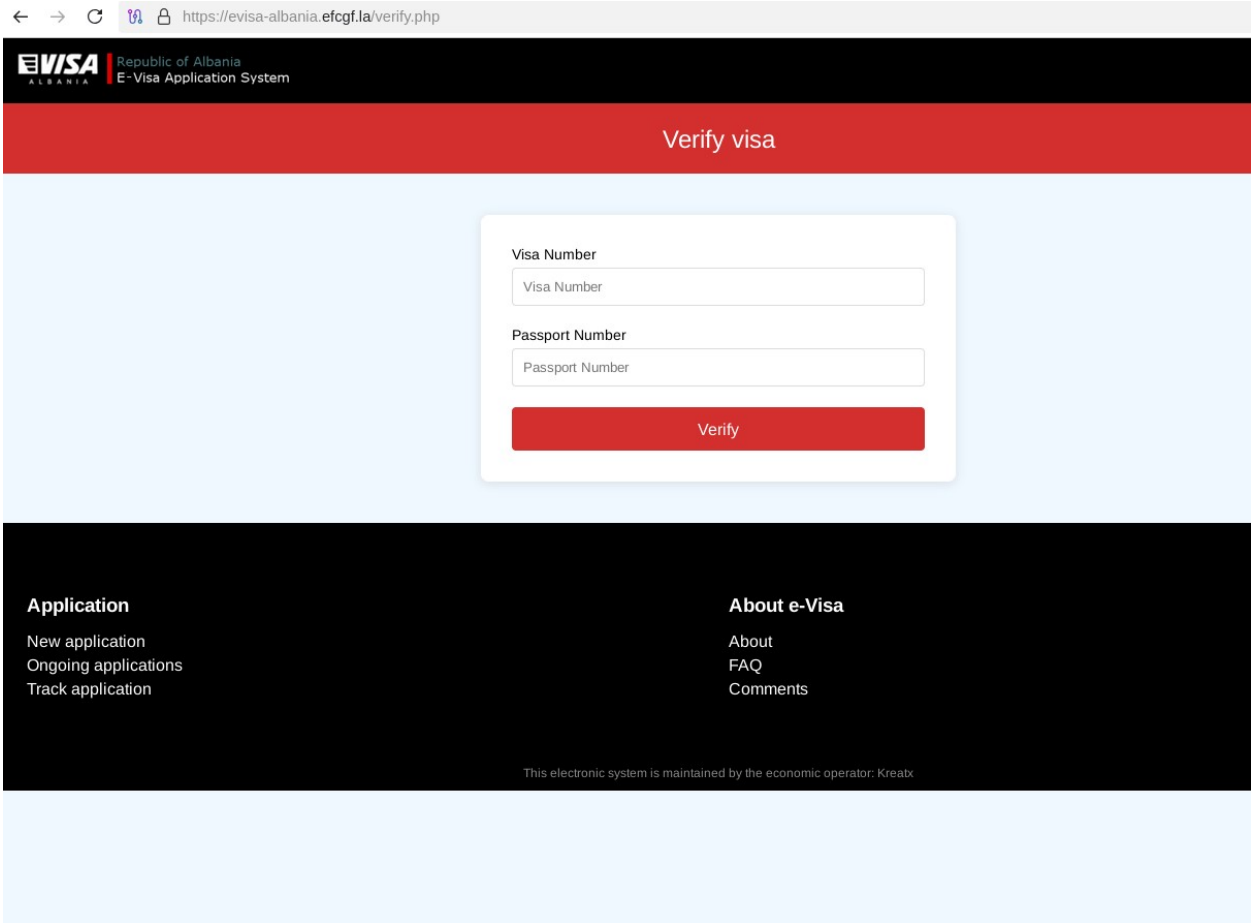

Figure 7 — evisa-albania.efcgf.la/verify.php: active credential harvesting with footer cloned from the official portal

4.5 evisalbania.com — Under Monitoring (MEDIUM)

This site presents an operational interface with professional branding including the Albanian double-headed eagle emblem, an application tracking system, and AI-powered features such as "Chat With IMIGRA AI" and "Powered by IMIGRA AI" branding. The domain was registered in March 2026. While visually polished, it does not display official government attribution and charges applicant fees.

This site may represent a third-party visa facilitation service (a model common in many countries) rather than a direct phishing operation. However, its near-identical branding to the government service, the absence of an official disclaimer, and the collection of passport and application data merit continued monitoring. Travelers should be cautioned that this is not the official Albanian government portal.

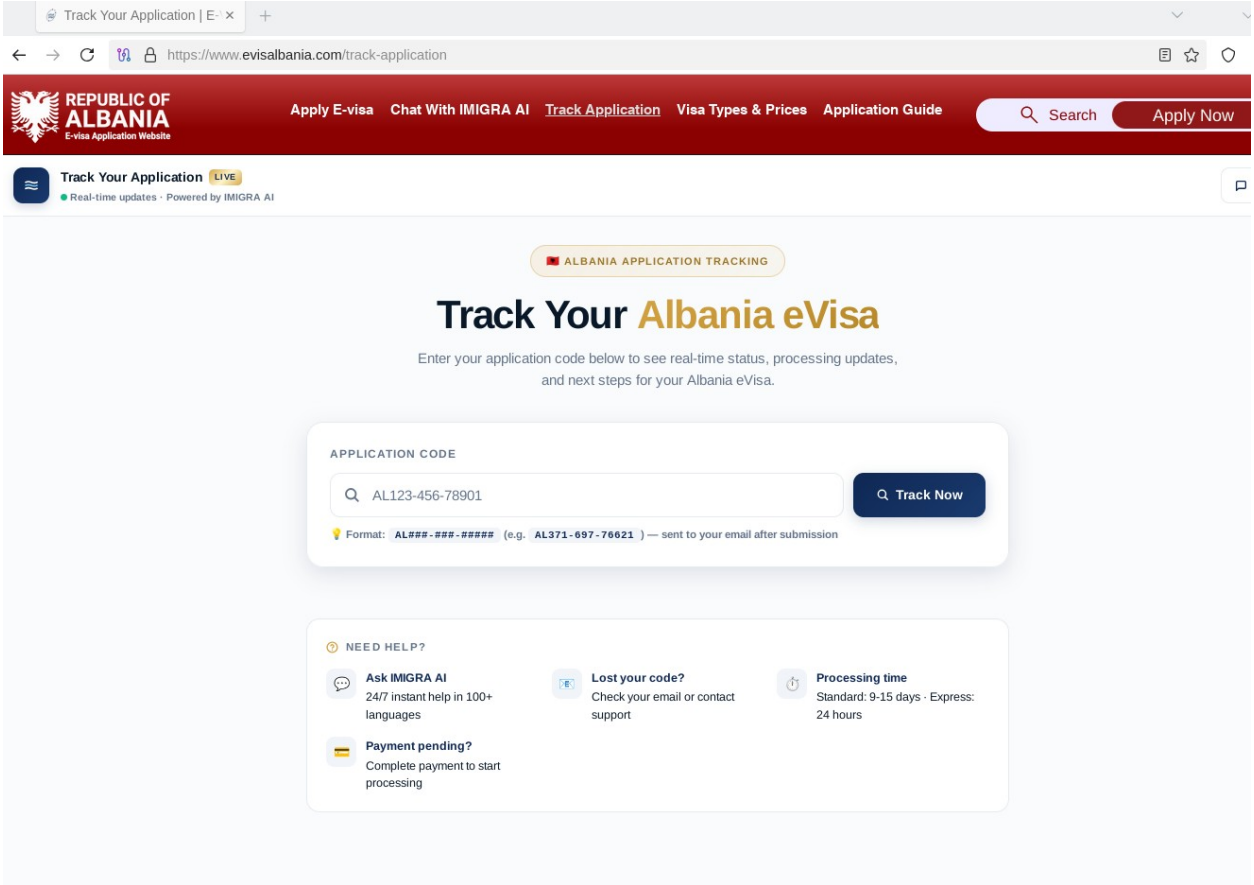

Figure 5 — evisalbania.com tracking page with unofficial but professional-looking government branding

5. Infostealer Telemetry — Compromised Applicants

Sphere TI performed a credential exposure search against infostealer intelligence databases using e-visa.al as the target domain. The query returned 1,950 total exposed systems with credentials linked to the legitimate Albanian government portal. This indicates a substantial

number of applicants have been compromised by infostealer malware, likely through fraudulent sites or general device compromise.

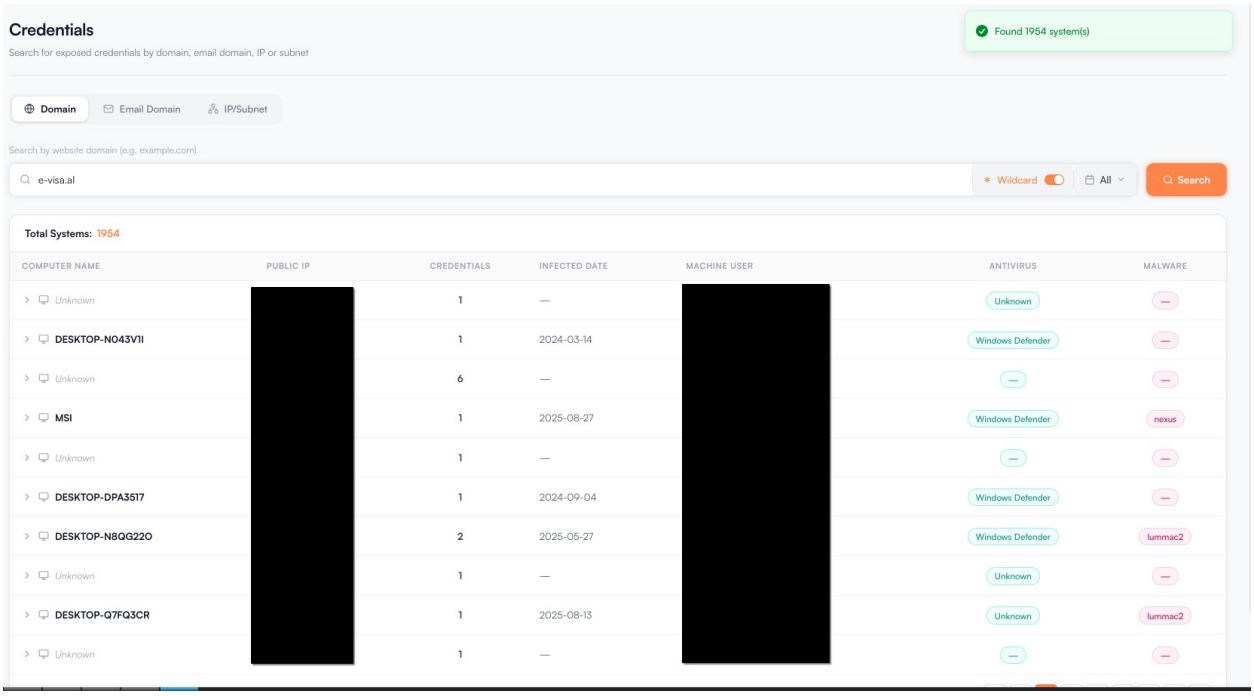

Figure 6 — Infostealer telemetry: 1,950 systems with credentials linked to e-visa.al

Notable entries in the exposed systems data include machines infected with Nexus and lummac2 malware families, suggesting dedicated mobile and credential-stealing campaigns targeting applicants. Infections have been observed through at least August 2025, while fraudulent infrastructure targeting the service was still being registered as of June 2026, indicating the campaign remains ongoing.

The exposure of credentials from the legitimate portal (e-visa.al) through infostealer malware indicates that threat actors may be harvesting session tokens and login credentials via two attack vectors: direct phishing from cloned sites, and device-level compromise of applicants who later use the real portal. Either pathway results in the theft of personal and travel document data.

6. Threat Actor Assessment

Based on the pattern of domain registrations, visual cloning quality, and multilingual targeting (the French-language verification page on e-visa-albania.com is a strong indicator), Sphere TI assesses that this campaign likely involves multiple independent actors exploiting the same opportunity, rather than a single coordinated group.

The domains follow a clear pattern: registration of keyword-rich domains containing "evisa," "albania," and "e-visa-al" variations, followed by deployment of visually cloned government interfaces optimized for data collection. The rapid pace of new registrations through mid-2026 suggests that takedown actions against earlier domains may be prompting the creation of replacement infrastructure.

Objective	Financial fraud via payment collection; credential harvesting; identity data resale
Targets	International visa applicants to Albania; border verification personnel
TTPs	Typosquatting; CT domain monitoring evasion; multilingual lures; QR verification spoofing
Infrastructure	Subdomain abuse (snlug.com); .live / .com TLDs; newly registered domains
Infostealer Families	lummac2, Nexus — active credential stealers

7. Recommendations

7.1 For Travelers and Applicants

Anyone planning to apply for an Albanian e-Visa should follow these precautions:

- Always access the Albanian e-Visa system exclusively through the official URL: https://e-visa.al. Do not click links in emails, social media posts, or search advertisements.
- Verify the domain in the browser address bar before entering any personal information. The only legitimate portal uses the .al country-code TLD.
- Never enter passport numbers, visa numbers, or tracking codes on third-party verification websites unless you have independently confirmed they are official. No third-party site is authorized to verify Albanian visas.
- Enable Multi-Factor Authentication (MFA) on your email account and any government portal accounts to limit the impact of credential theft.
- If you have submitted personal or payment information to any domain listed in this report, consider it compromised. Change passwords, monitor bank statements, and consider placing a fraud alert with relevant financial institutions.
- Run an up-to-date antivirus or endpoint detection tool on any device used to access visa portals, to detect infostealer infections.

7.2 For Border Officials and Verification Personnel

- Exercise caution when scanning QR codes from visa documents. Fraudulent documents may generate "valid" results on unofficial verification portals. Cross-reference against the official e-visa.al verification system only.
- Treat any verification URL that does not originate from the e-visa.al domain as untrusted.

7.3 For Organizational Security Teams

- Add all identified fraudulent domains (see Section 4) to blocklists, DNS sinkholes, and threat intelligence feeds.
- Monitor certificate transparency logs for future registrations containing "evisa" + "albania" or "e-visa-al" keyword patterns.
- Query infostealer telemetry databases for employee and organizational exposure linked to the e-visa.al domain.
- Notify HR and travel departments: employees applying for Albanian visas should be reminded to use only the official portal.

7.4 For the Albanian Government and CERT

- Initiate domain abuse takedown requests against all active fraudulent domains via their registrars.
- Expand the existing public advisory (currently limited to evisia-al.com) to include all domains identified in this report.
- Consider a proactive domain squatting defense strategy: pre-register common typosquatting variations of e-visa.al.
- Engage with Google and Bing Safe Browsing to flag fraudulent domains for search-engine-level warnings.

8. Indicators of Compromise (IOCs)

The following domains should be treated as malicious or suspicious and blocked across network controls, endpoint security tools, and threat intelligence platforms:

Domain	Registration Date	Status	Notes
e-visa-al.live	02 Oct 2025	BLOCK	Full clone; VT flagged; Georgia Tech node
e-visa-albania.com	26 May 2026	BLOCK	French credential harvesting; Georgia Tech node
evisa-albania.com.snlug.com	22 May 2026	BLOCK	Multi-brand hijacked hosting; QR spoof

Domain	Registration Date	Status	Notes
evisa-albania.efcgf.la	08 Jun 2026	BLOCK	verify.php harvest; footer cloned
evisalbania.com	28 Mar 2026	MONITOR	Likely 3rd-party facilitator; user VT flags
evisa-albania.org	06 May 2026	WATCH	Parked
evisa-albania.services	08 Jun 2026	WATCH	Not resolving

9. References

- Albanian Ministry for Europe and Foreign Affairs — Public Advisory on Fraudulent Visa Websites, April 2026
- Politiko.al — "Fake Albanian visa websites, Ministry of Foreign Affairs: Beware of online scams" — April 5, 2026
- Republic of Albania Official e-Visa Portal — https://e-visa.al
- Georgia Tech AS2637 — ARIN WHOIS: https://rdap.arin.net/registry/autnum/2637 | Abuse: abuse@gatech.edu
- Infostealer Credential Intelligence Database — Domain query: e-visa.al — June 2026
- CT Log / New Domain Registration Monitoring — Sphere TI, Alphatechs — 2025–2026
- VirusTotal — e-visa-al.live engine flags; evisalbania.com user submissions

10. About Sphere TI | Alphatechs

Sphere TI is the threat intelligence platform operated by Alphatechs. We specialize in brand impersonation monitoring, dark web intelligence, infostealer telemetry, and domain abuse investigation. This report was produced for awareness and defensive purposes. All data was obtained from open sources, certificate transparency logs, domain registration records, and infostealer telemetry aggregates.

For takedown assistance, threat monitoring subscriptions, or custom investigations, contact the Sphere TI research team at Alphatechs.