INVESTIGATION REPORT

Subject:

PASSIVE FORENSIC ANALYSES

OF

PAN & AADHAAR PORTALS

Case ID: BM-PaaS-2026-001

TLP: CLEAR

Prepared by

Mr. Biswadeb Mukherjee

Offensive Security Specialist & Malware Engineer

Report Version: v1

Report Date (IST) : 18-01-2026

Investigation Period (IST):

15-01-2026 to 18-01-2026

Mr. Biswadeb Mukherjee
Offensive Security Specialist & Malware Engineer
+919836763466 || biswadebmukherjee941@gmail.com

THIS PAGE IS INTENTIONALLY LEFT BLANK

Mr. Biswadeb Mukherjee
Offensive Security Specialist & Malware Engineer
+919836763466 || biswadebmukherjee941@gmail.com

Contents

Mr. Biswadeb Mukherjee

Offensive Security Specialist & Malware Engineer

+919836763466 || biswadebmukherjee941@gmail.com

CASE-ID: BM-PaaS-2026-001

TLP: CLEAR

Date: (IST) 18-01-2026

Disclaimer

This report is issued in the interest of public awareness, digital safety, and informed regulatory review.

All observations, findings, and assessments documented herein are derived exclusively from **non-intrusive examination of publicly accessible information**, using methods and tools detailed in the *Methodology* section of this report. No system access controls were bypassed, and no unauthorised access, exploitation, penetration testing, traffic interception, manipulation, or backend interaction was performed at any stage.

This document does not allege guilt, intent, ownership, authorisation, or criminal conduct by any individual, organisation, service provider, registrar, hosting provider, or network operator. References to domain names, website interfaces, service descriptions, or infrastructure characteristics are included solely to document observable patterns and conditions that may warrant independent examination by competent authorities.

This report does not constitute a legal opinion, judicial determination, or regulatory directive. Website content, service representations, infrastructure, ownership, and compliance status may change over time.

The findings presented are factual, pattern-based, and time-bound to the period of observation.

Mr. Biswadeb Mukherjee

Offensive Security Specialist & Malware Engineer

+919836763466 || biswadebmukherjee941@gmail.com

CASE-ID: BM-PaaS-2026-001

TLP: CLEAR

Date: (IST) 18-01-2026

Statement of Authorship and Attribution

This report has been prepared independently by **Mr. Biswadeb Mukherjee** and is issued in good faith and without malice.

All observations and analyses contained herein are based solely on publicly accessible information, open-source intelligence, and non-intrusive examination methods. No confidential sources, privileged materials, or unlawfully obtained information were accessed or relied upon in the preparation of this document.

No compensation, inducement, or external influence was received in connection with the preparation or publication of this document.

The author digitally signs this report. No handwritten or manual signature is required.

Mr. Biswadeb Mukherjee

Offensive Security Specialist & Malware Engineer
+919836763466 || biswadebmukherjee941@gmail.com

CASE-ID: BM-PaaS-2026-001
TLP: CLEAR
Date: (IST) 18-01-2026

1. Executive Summary:

This report documents the investigation of phishing campaigns impersonating Indian government identity services. The investigation was initially scoped to analyse phishing activity targeting PAN-related services, to identify infrastructure, tactics, and operational patterns associated with phishing-as-a-service offerings.

During analysis, additional indicators were identified that revealed the impersonation of Aadhaar-related services operating within the same hosting environments, domain registration patterns, and phishing kit frameworks. These Aadhaar-focused phishing artefacts were found to be technically and operationally correlated with the PAN-related phishing infrastructure already under investigation.

Based on this evidence-driven overlap, the scope of the investigation was expanded in a controlled manner to include Aadhaar-related phishing activity associated with the same threat ecosystem. The findings presented in this report reflect a unified phishing-as-a-service operation that exploits multiple Indian identity services, rather than isolated, independent campaigns.

2. Scope of Review:

2.1 **Objective:** The objective of this investigation is to document observable conditions, pattern-based similarities, and compliance-relevant gaps associated with a class of publicly accessible websites offering PAN- or Aadhaar-linked services, and to assess potential implications for user data safety, informed consent, and public trust.

2.2 **Referenced Domains:** Multiple publicly accessible domains were reviewed as representative samples exhibiting the observed patterns. To maintain focus on systemic behaviour rather than individual entities, the list of reviewed domains is provided separately in **Annexure A (Illustrative Domains Reviewed)**.

3. Scope of Investigation:

The scope of this investigation was limited to the observation of publicly accessible websites and associated artefacts impersonating Indian identity-related services.

➢ **Included within scope:**

- Publicly accessible PAN-related service portals
- Publicly accessible Aadhaar-related service portals identified through evidence-driven correlation
- Visible website content, user flows, and client-side behaviour

- Indicative domain registration and hosting characteristics

➢ **Explicitly excluded from scope:**

- Backend systems, databases, or administrative interfaces
- Authentication bypass, credential testing, or account interaction
- Vulnerability assessment, penetration testing, or exploitation
- Traffic interception or manipulation

4. Methodology:

➢ **Investigative Approach:** This investigation employed a **Passive Digital Forensics** strategy, combined with **OSINT-driven forensic analysis** and a **non-attributional, pattern-based analytical framework**. All investigative activities were performed strictly within the scope boundaries and limitations defined in the *Scope of Investigation* section. The methodology was designed to ensure that findings were derived exclusively from publicly accessible, read-only sources and that no interaction occurred with protected systems or non-public resources. This combined approach reflects industry-accepted investigative practices used in regulatory reviews, platform abuse analysis, threat intelligence, and pre-attribution forensic assessments as of 2026.

➢ **Forensic Strategy Employed:** **Passive Digital Forensics** was adopted as the primary forensic strategy for this investigation. Under this strategy, analysis was limited to information intentionally exposed to the public internet and observable without altering system state, generating intrusive traffic, or interacting with backend components. This approach preserves evidentiary integrity while minimising legal, ethical, and operational risk. The use of Passive Digital Forensics is consistent with contemporary forensic and compliance-oriented investigations where the objective is to document observable conditions rather than perform system-level examination or attribution.

➢ **OSINT-Driven Forensic Analysis:** Open-source intelligence techniques were applied in a forensic context to analyse and correlate observable artefacts across multiple publicly accessible websites.

- These techniques focused on:
  - Visible website content and service representations
  - User-facing service flows and data collection prompts
  - Client-side behaviour observable through standard web interactions
  - Domain naming conventions and structural similarities
  - Publicly resolvable DNS records and registration metadata

- Indicative hosting, CDN, and web application firewall characteristics

OSINT sources were treated as evidentiary inputs rather than intelligence conclusions, and observations were validated through repeatable, non-intrusive examination.

- **Pattern-Based Analytical Framework:** Findings were evaluated using a **pattern-based, non-attributional analytical framework**. This framework focuses on identifying repeated operational characteristics across multiple services, including similarities in:

  - User interface layout and navigation
  - Terminology, prompts, and error handling behaviour
  - Monetisation models and role hierarchies
  - Indicative infrastructure-level convergence

This analytical approach deliberately avoids conclusions regarding ownership, intent, coordination, or actor identity. Attribution was explicitly excluded to maintain analytical neutrality and evidentiary defensibility.

- **Scope Control and Evidence-Driven Expansion:** The investigation was initially scoped to publicly accessible websites impersonating PAN-related services. During analysis, additional Aadhaar-related artefacts were identified through observable technical and operational correlations, including shared infrastructure indicators, service flow similarities, and monetisation structures. Based on these evidence-driven linkages, the scope was expanded in a controlled manner to include Aadhaar-related services that met the same observation criteria. All scope expansion decisions were grounded in repeatable, publicly observable indicators and conducted within the original methodological constraints.

- **Tools and Environment:** All analysis was conducted using non-intrusive, read-only tools and techniques that did not generate exploitative or disruptive activity.

  - **Operating Environment: (Annexure B.1.1)**
    - Kali GNU/Linux Rolling (Version 2025.4)
    - Kernel: Linux 6.17.10+kali-amd64
    - Architecture: x86_64
    - Time synchronisation: Enabled (IST)
  - **Tools and Utilities:**
    - timedatectl – Verification of system time synchronisation
    - curl – Verification of HTTP service availability and response headers
    - dig – Querying authoritative DNS records (NS, MX)
    - findomain – Enumeration of publicly discoverable subdomains

- whois – Retrieval of domain registration and registrar information
- wafw00f – Identification of externally visible web application firewall presence
- sha256 – Used to finalise the evidence with cryptographic chain-based hashing

No automated vulnerability scanners, credential testing tools, or exploitation frameworks were used.

- **Methodological Limitations:** This methodology captures only those conditions and artefacts observable through publicly accessible interfaces at the time of examination. Backend implementations, internal data handling practices, ownership structures, authorisation status, and compliance posture cannot be conclusively determined using non-intrusive methods alone. All findings are time-bound and subject to change as website content, infrastructure, or service representations evolve.

5. Observations:

5.1 Absence of Verifiable Authorisation Indicators:

- **Observed Condition:** The reviewed websites did not display official government domains, verifiable authorisation statements, references to officially appointed PAN service providers, or approval identifiers issued by competent authorities.
- **Resulting Risk:** In the absence of such indicators, users are not provided sufficient information to distinguish these services from authorised or government-operated PAN service portals.

5.2 Absence of Legal Identity and Accountability:

- **Observed Condition:** The reviewed websites did not prominently disclose a registered legal entity name, Corporate Identification Number (CIN), LLPIN, GSTIN, registered business address, or a named grievance or data protection contact.
- **Resulting Risk:** Users lack a verifiable counterparty for accountability, dispute resolution, or the exercise of data subject rights.

Mr. Biswadeb Mukherjee
Offensive Security Specialist & Malware Engineer
+919836763466 || biswadebmukherjee941@gmail.com

5.3 Search Engine Targeting and Lure Keywords:

- **Observed Conditions:**
  - Analysis of phishing page content, metadata, URL structures, and visible text shows deliberate use of search-engine-optimised keywords.
  - Keywords were selected to mirror legitimate search queries related to Indian government identity services.
  - The phishing portals targeted users actively searching for PAN and Aadhaar-related services rather than relying on random victim discovery.
  - Identified lure keywords include commonly searched PAN and Aadhaar service terms, such as login, update, verification, and official portal references.
  - Keywords were embedded across multiple page components, including headings, body text, and visual elements, to enhance search visibility and perceived legitimacy.
  - The coexistence of both PAN and Aadhaar-related keywords within the same infrastructure indicates coordinated targeting of multiple identity services.
- **Resulting Risk:**
  - Users searching for legitimate PAN or Aadhaar services are at increased risk of being redirected to fraudulent phishing portals through organic search results.
  - The use of official-sounding keywords significantly lowers user suspicion, increasing the likelihood of credential submission and identity compromise.
  - SEO-driven discovery enables sustained victim acquisition without direct interaction by threat actors.
  - The combined targeting of PAN and Aadhaar services suggests a scalable phishing-as-a-service model capable of harvesting multiple forms of sensitive identity data.
  - Compromised credentials may lead to identity theft, financial fraud, unauthorised access to government services, and downstream misuse across other linked platforms.

5.4 Collection of Sensitive and Identity-Linked Data:

- **Observed Condition:** The reviewed websites requested combinations of Aadhaar number, date of birth, mobile number (including OTP-based verification), and PAN-related identifiers.
- **Resulting Risk:** Such data constitutes sensitive and identity-linked personal data and, when collected without clear safeguards and disclosures, may increase exposure to misuse, correlation, or downstream fraud.

Mr. Biswadeb Mukherjee
Offensive Security Specialist & Malware Engineer
+919836763466 || biswadebmukherjee941@gmail.com

5.5 Absence of Mandatory Privacy and Data-Handling Disclosures:

- **Observed Condition:** The reviewed websites did not publish privacy policies, terms of service, informed consent statements, data retention or deletion disclosures, breach notification information, or grievance redressal mechanisms.
- **Resulting Risk:** The absence of these disclosures prevents users from understanding how their data is processed, retained, or shared, and limits transparency regarding safeguards and accountability.

5.6 Pattern-Based Similarities Across Domains:

- **Observed Condition:** Strong similarities were observed across multiple domains, including user interface layout, service flow, terminology, registration prompts, error messaging, and notification text.
- **Resulting Risk:** The observed convergence indicates the use of shared templates or common service logic, resulting in the replication of identical risk conditions across multiple publicly accessible services.

5.7 Indicative Infrastructure-Level Convergence:

- **Observed Condition:** At an indicative level, multiple reviewed domains exhibited overlapping hosting or infrastructure characteristics.
- **Resulting Risk:** These observations demonstrate infrastructural convergence but do not imply ownership, coordination, or complicity by hosting or network service providers.

5.8 Common Monetisation and Payment Flow Structure:

- **Observed Condition:** Across multiple reviewed domains, a consistent tiered monetisation structure labelled “Retailer”, “Distributor”, “Super Distributor”, and “White Label” was observed. Plan taxonomy, pricing presentation, and feature descriptions were near-identical across domains.
- During non-intrusive testing, payment initiation using a placeholder or invalid inputs resulted in consistent transaction failure behaviour. The identity of the payment gateway, merchant entity, and grievance redressal mechanism was not disclosed before transaction failure. No payment instrument details or real identity data were submitted, and no transaction was completed.
- **Resulting Risk:** The convergence of monetisation models reinforces the assessment of a shared operational pattern and limits user visibility into financial accountability and dispute resolution pathways.

Mr. Biswadeb Mukherjee
Offensive Security Specialist & Malware Engineer
+919836763466 || biswadebmukherjee941@gmail.com

6. Risk Assessment:

6.1 User Impact:

- Insufficient informed consent for sensitive data processing
- Limited transparency regarding data handling and retention
- Increased exposure to identity misuse or downstream fraud
- Absence of accessible grievance redressal mechanisms

6.2 Systemic Impact:

- Aggregation of identity-linked data without visible safeguards
- Expansion of attack surface for high-impact data breaches
- Erosion of public trust in legitimate digital governance services
- Difficulty in attribution and remediation in the event of misuse

7. Indicative Regulatory Relevance:

The statutory references below are provided to contextualise how the observable conditions documented in this report align with established Indian legal and regulatory frameworks governing digital services, identity-related data, and user protection. This section does not assert violations, intent, ownership, or liability and is included to assist competent authorities and compliance bodies in assessing whether independent examination or regulatory review is warranted.

➢ Information Technology Act, 2000

- **Section 43A** is contextually relevant in relation to the collection of sensitive personal data in environments where no visible reasonable security practices, data-handling disclosures, or accountability mechanisms were observed.
- **Sections 66C and 66D** are contextually relevant in circumstances involving publicly accessible services that replicate or impersonate identity-related service flows, creating ambiguity regarding authenticity and increasing exposure to identity-related misuse or deception.

➢ Information Technology (SPDI) Rules, 2011

- **Rules 4, 5, and 8** are contextually relevant where websites collect identity-linked personal data without publishing privacy policies, consent notices, purpose limitation disclosures, grievance mechanisms, or stated data protection safeguards.

➢ Digital Personal Data Protection Act, 2023

- **Sections 5 and 6** are contextually relevant in relation to observed data collection flows lacking visible notice, consent articulation, or purpose specification.
- **Sections 8 and 10** are contextually relevant where no user-facing mechanisms were observed for grievance redressal, data principal rights, or accountable entity identification.

➢ Bharatiya Nyaya Sanhita, 2023 (Indicative)

- Provisions relating to deception, impersonation, or misuse of identity-linked information are contextually relevant for independent examination in cases involving the public-facing representation of identity services without verifiable authorisation indicators.
- These references are indicative and non-exhaustive. Determination of applicability, interpretation, and enforcement remains the exclusive function of appropriate legal and regulatory authorities.

8. Indicators Warranting Independent Review

- Ambiguity in service representation and branding
- Omission of mandatory disclosures during sensitive data collection
- Replication of service models across multiple domains
- Search engine targeting of PAN-related queries

9. Recommendations

1. Independent verification of authorisation and service legitimacy
2. Compliance assessment under applicable data protection frameworks
3. Correlation analysis of domain registration, hosting, and payment flows
4. Review of search engine representation and user-facing disclosures
5. Establishment of coordinated disclosure channels for reporting unauthorised PAN-related service portals

10. Conclusion:

This document records a consistent pattern of publicly observable conditions associated with multiple PAN-related service websites, including the absence of authorisation indicators, legal accountability disclosures, and mandatory data protection safeguards.

Mr. Biswadeb Mukherjee

Offensive Security Specialist & Malware Engineer

+919836763466 || biswadebmukherjee941@gmail.com

CASE-ID: BM-PaaS-2026-001

TLP: CLEAR

Date: (IST) 18-01-2026

The observations documented herein provide a factual basis for independent examination by competent authorities and stakeholders concerned with digital governance, consumer protection, and data safety.

11. Annexures

➢ Annexure A – Illustrative Domains Reviewed:

Sl No	Domain	Observed Service Description	Hosting Provider	CDN	WAF	Screenshot Reference
1	panfind.org	PAN retrieval via Aadhaar/DOB	Godaddy	Not Found	Not Found	**Annexure B.A**
2	panfind.net	Know your PAN card no, using Aadhaar no and dob	Hostinger	hcdn	Not Found	**Annexure B.B**
3	mystoreservice.site	My Aadhaar service portal	Atak Domain Bilgi Teknolojileri A.S.	Not Found	Unstable Result	**Annexure B.C**
4	aadhaar.digital-shop.ak-47.site	Aadhaar Client Portal	HostBet Cloud Technologies Private Limited	Not Found	Not Found	**Annexure B.D**
5	vehiclex.top	Know your PAN card no using Aadhaar no and dob	Godaddy	Cloudflare	Cloudflare	**Annexure B.E**
6	atpanfind.top	Know your PAN card no using Aadhaar no and dob	Godaddy	Cloudflare	Not Found	**Annexure B.F**
7	vstech. support	Tech Support	QTIME BUSINESSES PRIVATE LIMITED	Not Found	Not Found	**Annexure B.G**
8	anushkaservices.help	Aadhaar Support	Key-System	Not Found	Litespeed	**Annexure B.H**

Table A.1

➢ Annexure B – Supporting Materials

- All supporting materials referenced in this report, including but not limited to screenshots, HTML artefacts, header responses, DNS records, and other non-intrusive evidentiary captures, are maintained in a case-scoped evidence repository titled **CASE-ID-BM-PaaS-2026-001**. Each **Annexure** folder also includes a short operational description in note.txt of each observed service
  Each evidentiary artefact is preserved in its original captured form and is individually hashed using the SHA-256 algorithm. A consolidated hash manifest is included within the repository to enable independent integrity verification.
  The repository contains a cryptographically signed commit by the author, providing authorship attribution, temporal anchoring, and tamper-evidence for the complete evidence set.
  The repository link and verification instructions are provided in the **References** section of this report.
  No supporting materials are embedded directly within this document to preserve evidentiary integrity and maintain a clear separation between analytical narrative and raw artefacts.

12. References:

➢ **[R-1]** Case Evidence Repository – **CASE-ID-BM-PaaS-2026-001**
Public repository containing supporting evidentiary artefacts, hash manifest, and signed commit.
Repository URL: https://github.com/official-biswadeb941/CASE-ID-BM-PaaS-2026-001

END OF REPORT

NO CONTENT FOLLOWS THIS SECTION

Digitally Signed by:
Biswadeb Mukherjee
Date: 19-01-2026
12:02 am