INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 14:10 UTC

OFAC Sanctions Nobitex and Three Iranian Crypto Exchanges for IRGC Ransomware Financing

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0408
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Nobitex, Wallex, Bitpin, Ramzinex (Iranian cryptocurrency exchanges and named executives)
Published	2026-06-03T16:31:22
Discovery Source	Rss

Executive Summary

The U.S. Treasury's OFAC sanctioned Iran's largest cryptocurrency exchange, Nobitex, along with Wallex, Bitpin, and Ramzinex, for processing ransom payments on behalf of IRGC-affiliated ransomware operators and facilitating large-scale sanctions evasion. Any organization that has paid a ransom routed through these exchanges, or that holds any financial relationship with these entities, now faces direct OFAC compliance exposure. Security teams should treat wallet addresses and transaction paths associated with these exchanges as high-confidence IRGC-linked indicators and escalate any potential exposure to legal counsel immediately.

Technical Analysis

This is a sanctions and threat intelligence action, not a software vulnerability. No CVE or CWE applies. OFAC's designation establishes a documented financial infrastructure link between IRGC-affiliated ransomware operators and four Iranian cryptocurrency exchanges: Nobitex, Wallex, Bitpin, and Ramzinex, along with named executives at each entity. Relevant MITRE ATT&CK techniques: T1486 (Data Encrypted for Impact, ransomware deployment by IRGC-affiliated operators), T1583.006 (Acquire Infrastructure: Web Services, use of exchange infrastructure for financial operations), T1020.001 (Automated Exfiltration: Traffic Duplication, ransom payment flow obfuscation), T1657 (Financial Theft, monetization via sanctioned exchange infrastructure). Chainalysis data cited in secondary reporting attributes over 50% of Iran's estimated $7.8 billion in 2025 crypto inflows to Nobitex; IRGC-associated wallets reportedly accounted for more than half of Q4 2025 Iranian crypto ecosystem volume. Confidence on sanctions facts: HIGH (primary source:

home.treasury.gov/news/press-releases/sb0519). Confidence on volume figures: MEDIUM (cited in secondary reporting; original Chainalysis report not directly accessed). No patch or software remediation applies. Exposure is financial, legal, and intelligence-focused.

Action Checklist

1. Step 1: Containment. Immediately query your organization's payment records, crypto transaction logs, and vendor payment systems for any transactions involving Nobitex, Wallex, Bitpin, or Ramzinex wallet addresses or exchange identifiers. Freeze any pending transactions that cannot be confirmed as unrelated to these entities. Escalate findings to legal counsel before taking further action; OFAC violations carry strict liability.
2. Step 2: Detection. Search SIEM and financial transaction logs for wallet addresses or routing identifiers associated with the four sanctioned exchanges. Cross-reference any prior ransomware incident payment records against OFAC's SDN list (sdnsearch.ofac.treas.gov). If your organization uses a crypto compliance or blockchain analytics tool (e.g., Chainalysis, Elliptic), run a retroactive screening of all crypto transactions against the newly designated addresses. Log sources: payment processor records, incident response case files, crypto wallet transaction histories. No specific event IDs apply; this is a financial records review, not a log-based detection task.
3. Step 3: Eradication. Block all wallet addresses and exchange endpoints associated with Nobitex, Wallex, Bitpin, and Ramzinex in any crypto payment or compliance tooling your organization operates. Update your sanctions screening lists to include the newly designated entities and associated executives per the OFAC SDN list. If your organization uses a ransomware payment intermediary or cyber insurance carrier, confirm they have applied the same blocks and are aware of the designation.
4. Step 4: Recovery. Validate that sanctions screening lists have been updated across all payment, procurement, and incident response workflows. If any historical exposure is identified, prepare a voluntary self-disclosure to OFAC; this is a mitigating factor under OFAC's enforcement framework. Confirm with legal counsel that no pending or future ransomware payment paths route through Iranian exchange infrastructure. Document all remediation steps taken with timestamps for regulatory record-keeping.
5. Step 5: Post-Incident. Review your ransomware response playbook to include mandatory sanctions screening of any proposed ransom payment address prior to authorization. Add OFAC SDN list screening as a required step in your incident response runbook for any ransomware event. Map this gap to NIST AC-1 (Policy and Procedures) to ensure the policy reflects current OFAC obligations. Consider adding IRGC-affiliated wallet address feeds to your threat intelligence platform as standing IOC watchlists.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if any transaction record — including prior ransomware payments made through a cyber insurance carrier or intermediary — can be traced to a wallet address or exchange identifier associated with Nobitex, Wallex, Bitpin, or Ramzinex, as OFAC violations carry strict liability and voluntary self-disclosure timelines are time-sensitive mitigating factors under the OFAC enforcement framework.

Recovery Notes	Post-containment, verify that sanctions screening lists are updated and enforced across all payment, procurement, and IR workflows — not only in the security team's tooling but also in finance, procurement, and any third-party ransomware payment intermediaries or cyber insurance carriers. Monitor OFAC's SDN list for additional designations of IRGC-affiliated crypto infrastructure on a weekly basis, as follow-on designations targeting related exchanges or executives are common after initial OFAC actions. Maintain the complete evidentiary record of remediation actions with UTC timestamps and file hashes for a minimum of five years, consistent with OFAC record-keeping expectations for sanctions compliance programs.
Forensic Artifacts	Crypto wallet transaction histories (exported from payment processor or wallet software) with full transaction paths including intermediary hops — required to trace whether any prior ransomware payment touched Nobitex, Wallex, Bitpin, or Ramzinex infrastructure even indirectly | Prior ransomware IR case files including ransom negotiation communications, payment authorization records, and TXIDs of any payments made — the primary source for retroactive OFAC exposure analysis | Payment processor and procurement system export records (CSV or native format) filtered for any vendor, counterparty, or wallet address matching OFAC SDN entries for the four designated Iranian exchanges and their named executives | Written communications (email, ticketing system records) with cyber insurance carriers and ransomware payment intermediaries referencing payment routing decisions — relevant because OFAC liability is not eliminated by routing payments through an intermediary | Sanctions screening configuration exports (pre- and post-remediation) from any crypto compliance tooling, payment processor blocklist, or manual screening process — timestamped and hashed to establish the remediation baseline for OFAC voluntary self-disclosure documentation

Per-Action IR Details

Step 1: Containment — Immediately query your organization's payment records, crypto transaction logs, and vendor payment systems for any transactions involving Nobitex, Wallex, Bitpin, or Ramzinex wallet addresses or exchange identifiers. Freeze any pending transactions that cannot be confirmed as unrelated to these entities. Escalate findings to legal counsel before taking further action — OFAC violations carry strict liability.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (CSF RS.MA-01: Execute IR plan in coordination with relevant third parties, including legal counsel, before proceeding with financial transaction actions involving OFAC strict-liability exposure)

Controls: NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement)

Compensating: For teams without a dedicated crypto compliance platform: export all payment processor records (ACH, wire, crypto) to CSV and run a grep/PowerShell search against OFAC's published SDN list wallet addresses. Example PowerShell: `Import-Csv payments.csv | Where-Object { $_.WalletAddress -match 'NOBITEX_ADDRESS_PATTERN' }`. Freeze pending crypto transactions by revoking API keys or disabling outbound payment authorization in your payment processor portal immediately — no tooling required.

Evidence: Before freezing, capture full transaction records including timestamps, wallet addresses (sender/receiver), transaction IDs (TXIDs), exchange identifiers, and any intermediary hop addresses from your payment processor and crypto wallet systems. Preserve these records in write-protected storage — they constitute potential regulatory evidence for OFAC voluntary self-disclosure or enforcement proceedings. If any prior ransomware payment was made through a cyber insurance carrier or intermediary, capture all correspondence and payment authorization records referencing those incidents.

Step 2: Detection — Search SIEM and financial transaction logs for wallet addresses or routing identifiers associated with the four sanctioned exchanges. Cross-reference any prior ransomware incident payment records against OFAC's SDN list (sdnsearch.ofac.treas.gov). If your organization uses a crypto compliance or

blockchain analytics tool (e.g., Chainalysis, Elliptic), run a retroactive screening of all crypto transactions against the newly designated addresses. Log sources: payment processor records, incident response case files, crypto wallet transaction histories. No specific event IDs apply — this is a financial records review, not a log-based detection task.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (CSF DE.AE-07: Integrate up-to-date CTI — in this case the OFAC SDN designation — into adverse event analysis; CSF DE.AE-03: Correlate information from multiple sources including payment processor records, IR case files, and blockchain transaction histories)

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention)

Compensating: Without Chainalysis or Elliptic: download OFAC's SDN list in CSV format from sdnsearch.ofac.treas.gov, filter for Digital Currency Address entries tagged to Nobitex, Wallex, Bitpin, and Ramzinex, and run a manual cross-reference against your exported crypto wallet transaction histories using Excel VLOOKUP or Python pandas `df.merge()`. For blockchain public tracing, use free tools Blockchair.com or blockchain.com explorer to trace TXIDs from prior ransomware payments and identify if any hop in the transaction chain touches a newly designated address. Document all search queries and timestamps for regulatory record-keeping.

Evidence: Retrieve all prior ransomware incident response case files, including any payment authorization records, ransom negotiation communications, and TXIDs of payments made. Pull blockchain transaction histories for any organizational crypto wallets used in ransomware payments and trace full transaction paths (including intermediary hops) to identify exposure to Nobitex, Wallex, Bitpin, or Ramzinex infrastructure. Preserve payment processor export files and IR case documentation in original format with hash verification (sha256sum) before analysis begins.

Step 3: Eradication — Block all wallet addresses and exchange endpoints associated with Nobitex, Wallex, Bitpin, and Ramzinex in any crypto payment or compliance tooling your organization operates. Update your sanctions screening lists to include the newly designated entities and associated executives per the OFAC SDN list. If your organization uses a ransomware payment intermediary or cyber insurance carrier, confirm they have applied the same blocks and are aware of the designation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (CSF RS.MA-01: Coordinate IR plan execution with third parties — specifically cyber insurance carriers and ransomware payment intermediaries — to ensure OFAC-designated addresses are blocked across the full payment chain, not only within your own tooling)

Controls: NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without enterprise crypto compliance tooling: manually import OFAC SDN wallet addresses for all four exchanges into your payment processor's blocklist or deny-list configuration. For organizations using raw crypto wallet software, configure outbound transaction signing rules or pre-authorization scripts that reject transactions to blocked addresses. Maintain a versioned, dated blocklist file (CSV with sha256 hash) as a configuration artifact. Contact your cyber insurance carrier in writing (email with read receipt) to confirm they have applied equivalent blocks — retain that confirmation for regulatory records.

Evidence: Before updating blocklists, capture and archive the current state of your sanctions screening configuration (screenshot or export with timestamp) to demonstrate the pre-remediation baseline for OFAC purposes. Document the specific OFAC SDN list version and publication date used as the source for the new blocks. Retain written confirmation from any ransomware payment intermediary or cyber insurance carrier that they have applied equivalent screening updates, as third-party exposure through an intermediary does not eliminate your organization's OFAC liability.

Step 4: Recovery — Validate that sanctions screening lists have been updated across all payment, procurement, and incident response workflows. If any historical exposure is identified, prepare a voluntary self-disclosure to OFAC — this is a mitigating factor under OFAC's enforcement framework. Confirm with legal counsel that no pending or future ransomware payment paths route through Iranian exchange infrastructure. Document all remediation steps taken with timestamps for regulatory record-keeping.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (CSF RC: Execute recovery plan, verify integrity of remediated controls, and communicate status; voluntary self-disclosure to OFAC functions as the regulatory notification analog to breach notification in this context)

Controls: NIST AU-3 (Content Of Audit Records), NIST AU-8 (Time Stamps), NIST AU-11 (Audit Record Retention), NIST AC-1 (Policy And Procedures)

Compensating: For teams without GRC tooling: create a timestamped remediation log in a plain text or spreadsheet file, recording each action taken, the person responsible, date/time (UTC), and the evidence artifact preserved. Hash each artifact file with sha256sum and record hashes in the log. For OFAC voluntary self-disclosure preparation, OFAC's online submission portal (ofac.treas.gov) accepts structured narrative submissions — no specialized legal software required, though legal counsel review before submission is mandatory given strict liability exposure.

Evidence: Compile a complete, timestamped audit trail of all sanctions screening updates, transaction freezes, and communications with third parties (insurance carriers, payment intermediaries, legal counsel) from Steps 1–3. Retain original transaction records, blockchain TXIDs, and IR case files in unmodified form with sha256 hashes logged — these constitute the evidentiary package required for OFAC voluntary self-disclosure and will be the primary record reviewed in any enforcement action. Ensure audit records satisfy NIST AU-3 requirements: what occurred, when, where, who performed the action, and what outcome resulted.

Step 5: Post-Incident — Review your ransomware response playbook to include mandatory sanctions screening of any proposed ransom payment address prior to authorization. Add OFAC SDN list screening as a required step in your incident response runbook for any ransomware event. Map this gap to NIST AC-1 (Policy and Procedures) to ensure the policy reflects current OFAC obligations. Consider adding IRGC-affiliated wallet address feeds to your threat intelligence platform as standing IOC watchlists.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (CSF GV, ID: Update IR policies and runbooks based on lessons learned; integrate CTI — specifically IRGC-affiliated ransomware actor wallet address feeds — into standing detection and prevention workflows to reduce recurrence risk)

Controls: NIST AC-1 (Policy And Procedures), NIST AU-2 (Event Logging), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a commercial TIP: create a structured IOC watchlist file (STIX 2.1 JSON or plain CSV) of IRGC-affiliated wallet addresses sourced from the OFAC SDN list and CISA advisories on IRGC ransomware operations (e.g., AA22-257A). Import this watchlist into an open-source TIP such as MISP (free) or maintain it as a recurring grep/PowerShell check against payment exports on a defined schedule (weekly minimum). For playbook updates, embed the OFAC SDN search URL (sdnsearch.ofac.treas.gov) and a mandatory legal-counsel-approval gate as a decision node in your ransomware runbook — implementable in any document-based runbook with no tooling cost.

Evidence: Document the specific policy or playbook gap identified — the absence of OFAC sanctions screening as a mandatory pre-authorization step in ransomware response — with reference to this OFAC designation event as the triggering incident. Retain the lessons-learned record per NIST 800-61r3 §4 post-incident reporting requirements. Archive the OFAC SDN list version used to update IOC watchlists, including publication date and the specific Nobitex, Wallex, Bitpin, and Ramzinex entries, to demonstrate that TIP feeds reflect the current designation at the time of playbook update.

Detection Guidance

No software vulnerability or network-based indicator drives this detection; exposure is determined by financial transaction history and ransomware incident records. Detection actions: (1) Screen all historical crypto transaction records against wallet addresses listed in the OFAC SDN designation (primary source: home.treasury.gov/news/press-releases/sb0519). (2) If your organization experienced a ransomware incident in

2024 or 2025 and made a ransom payment, submit the payment wallet address to a blockchain analytics service to trace whether the funds transited Nobitex, Wallex, Bitpin, or Ramzinex infrastructure. (3) In your SIEM or threat intelligence platform, create watchlist entries for any wallet addresses published in the OFAC designation or associated Elliptic analysis (elliptic.co/blog/ofac-sanctions-nobitex-and-three-other-iranian-cryptoasset-exchanges, search-retrieved URL, recommend human validation). (4) Monitor for IRGC-associated TTPs using MITRE ATT&CK T1486, T1657 as hunt hypotheses in EDR and network telemetry. Behavioral indicators of IRGC-affiliated ransomware operators include double-extortion patterns, large enterprise targets, and ransom demands routed through intermediary wallets before reaching exchange on-ramps. Confidence on specific wallet address values: defer to the live OFAC SDN list; do not rely on addresses from secondary reporting alone.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`nobitex.ir`	Nobitex exchange domain — OFAC-sanctioned Iranian cryptocurrency exchange linked to IRGC ransomware payment processing	HIGH
DOMAIN	`wallex.ir`	Wallex exchange domain — OFAC-sanctioned Iranian cryptocurrency exchange, named in Treasury designation	HIGH
DOMAIN	`bitpin.ir`	Bitpin exchange domain — OFAC-sanctioned Iranian cryptocurrency exchange, named in Treasury designation	HIGH
DOMAIN	`ramzinex.com`	Ramzinex exchange domain — OFAC-sanctioned Iranian cryptocurrency exchange, named in Treasury designation	HIGH

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1583.006** — Web Services
- **T1020.001** — Traffic Duplication
- **T1657** — Financial Theft

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1583.006	Web Services	Resource-Development
T1020.001	Traffic Duplication	Exfiltration
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/the-us-sanctions-nob...	T3
The US Treasury has blacklisted Iran's largest digital ... - Facebook	https://www.facebook.com/anadoluagencyenglish/posts/-the-us-treasur...	T3
Economic Fury Targets Iran's Largest Digital Asset Exchange for ...	https://home.treasury.gov/news/press-releases/sb0519	T1
Today's sanctions against Nobitex, Wallex, Bitpin, and Ramzinex ...	https://x.com/maxmeizlish/status/2061901303194833241	T3
OFAC sanctions Nobitex and three other Iranian cryptoasset ... - Elliptic	https://www.elliptic.co/blog/ofac-sanctions-nobitex-and-three-other...	T3

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-04 14:10 UTC by TJS Security Command Center