INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:39 UTC

UK Sanctions Xinbi: A $19.9B Illicit Marketplace at the Center of Pig Butchering, North Korean Laundering, and Southeast Asian Scam Infrastructure

THREAT CAMPAIGN | CRITICAL | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0108
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	Cryptocurrency ecosystem broadly; Telegram platform (used as marketplace infrastructure); financial institutions exposed to sanctioned entities; no specific enterprise software products affected
Published	2026-03-26
Discovery Source	Rss

Executive Summary

The UK government sanctioned Xinbi, a Telegram-based illicit marketplace that processed over $19.9 billion in cryptocurrency between 2021 and 2025, serving as core financial infrastructure for pig butchering fraud networks, North Korean state-linked money laundering, and Southeast Asian human trafficking operations. The sanctions also target #8 Park, assessed as Cambodia's largest scam compound, and its operator Legend Innovation Co, both tied to the Prince Group transnational organized crime ring. Organizations exposed to sanctioned entities through cryptocurrency transactions, vendor relationships, or Telegram-based business channels face regulatory and reputational risk under UK financial sanctions law.

Technical Analysis

Xinbi operated as a Chinese-language marketplace on Telegram, leveraging the platform's pseudonymous channels and bot infrastructure to facilitate cryptocurrency-denominated transactions across multiple criminal verticals. No software vulnerability or CVE is associated with this item. The threat is financial crime infrastructure and platform abuse. MITRE ATT&CK techniques observed across associated operations include: T1566/T1566.002 (phishing and spearphishing for victim recruitment into pig butchering schemes), T1583.006 (web services acquisition for scam infrastructure), T1657 (financial theft), T1020 (automated exfiltration of victim

assets), T1531 (account access removal to prevent victim recovery), T1567 (exfiltration over web services), and T1650 (acquiring access to tools/infrastructure). Lazarus Group is assessed at medium confidence as a laundering nexus through Xinbi (per threat intelligence corroboration). TRM Labs independently corroborated Xinbi's scale and confirmed continued marketplace activity despite prior OFAC designations and DOJ enforcement actions. No patch, CVE, or software remediation applies. The threat vector is transactional exposure and platform-facilitated financial crime.

Action Checklist

1. Containment: Immediately screen all cryptocurrency wallet addresses, Telegram channels, and business relationships against the UK FCDO consolidated sanctions list (updated to include Xinbi, Legend Innovation Co, and #8 Park). Block any flagged addresses at the exchange, custody, or payment processor level. Source: UK FCDO consolidated sanctions list at https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.
2. Detection: Query transaction records for transfers involving wallets associated with Xinbi or entities in the Prince Group network. Flag any Telegram-sourced vendor or contractor relationships for review. If your organization operates fraud monitoring, add detection rules for pig butchering contact patterns: unsolicited investment platform referrals, requests to move funds to unfamiliar exchanges, and rapid small-to-large transaction escalation sequences.
3. Eradication: Terminate any business relationships, payment flows, or platform integrations that touch sanctioned entities. If your organization uses Telegram for business operations, audit active channels and bot integrations for exposure to Xinbi-adjacent infrastructure. Report any confirmed exposure to your compliance officer and, where legally required, to the relevant financial intelligence unit (UKFIU for UK-regulated entities, FinCEN for US-regulated entities).
4. Recovery: Verify that all wallet screening and transaction monitoring tools have ingested the updated UK sanctions designations. Confirm your sanctions screening vendor has published a list update reflecting the Xinbi, Legend Innovation Co, and #8 Park additions. Document any transactions reviewed and cleared to support regulatory audit trails. Monitor for secondary designations as Western enforcement actions against overlapping infrastructure continue.
5. Post-Incident: This action exposes a broader control gap: cryptocurrency transaction monitoring programs may not adequately cover Telegram-based marketplace infrastructure or peer-to-peer laundering channels used by state-linked actors. Review your AML/CFT controls for coverage of Telegram-native financial flows. Assess whether your threat intelligence feeds include TRM Labs, Chainalysis, or equivalent blockchain analytics sources with coverage of illicit marketplace activity. Consider tabletop exercises covering pig butchering exposure scenarios for employees with personal investment accounts, as social engineering entry points frequently bypass corporate controls.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and the designated compliance officer if any confirmed transaction exposure to Xinbi, Legend Innovation Co, or Prince Group entities is identified — UK-regulated entities must file a Suspicious Activity Report with UKFIU (NCA) and US-regulated entities must file with FinCEN within 30 days of detection, and any delay creates direct regulatory liability; additionally escalate if transaction volumes exceed jurisdictional reporting thresholds or if North Korean state-linked laundering nexus is confirmed, which triggers OFAC secondary sanctions risk.
Recovery Notes	Post-containment, verify sanctions list ingestion is confirmed active in all screening tools with a dated audit record before resuming any cryptocurrency transaction processing involving counterparties touched during the review period. Monitor FCDO, OFAC, and allied enforcement feeds (EU, Australia, Canada) for secondary designations against Prince Group affiliates and overlapping Southeast Asian scam compound infrastructure — the Xinbi action is assessed as part of a coordinated Western enforcement campaign likely to produce additional designations within 30–90 days. Maintain enhanced transaction monitoring on any accounts or counterparties that were reviewed and cleared during this incident for a minimum of 180 days to detect activity from entities designated in subsequent enforcement rounds.
Forensic Artifacts	USDT-TRC20 on-chain transaction records: Xinbi processed the dominant share of its $19.9B volume in USDT on the Tron blockchain — export full TRC-20 transaction history from your custody/exchange platform and query TronScan for counterparty wallet interaction history with known Xinbi-designated addresses, preserving raw transaction data including block height, transaction hash, sender/receiver addresses, and timestamp | Telegram channel and bot audit logs: export Telegram account data (Settings → Export Telegram Data, JSON format) for all business accounts, preserving channel membership lists, bot authorizations, admin roles, and message metadata — Xinbi operated as a Telegram-native marketplace, so channel join history and bot API token usage records are primary forensic artifacts for establishing exposure scope | Internal KYC and onboarding records for cryptocurrency counterparties: retrieve onboarding files for any exchange customers or business counterparties where the relationship was initiated via Telegram or where cryptocurrency wallet addresses in payment terms match the Xinbi/Prince Group designation list — these records establish the timeline of relationship formation relative to Xinbi's known operational period (2021–2025) | Sanctions screening tool ingestion logs: extract the ingestion confirmation records from your sanctions screening vendor or in-house screening tool showing the exact timestamp and list version when Xinbi, Legend Innovation Co, and #8 Park entries were loaded — this artifact defines the window of unscreened exposure and is a primary document for regulatory examination | Internal fraud alert disposition records (2022–2025): retrieve any fraud monitoring alerts generated for accounts showing pig butchering transaction escalation patterns (small initial deposits escalating to large transfers within 30–180 days) that were reviewed and cleared during Xinbi's operational window — these records may require reclassification and SAR amendment if the counterparty is now confirmed as Xinbi-linked

Per-Action IR Details

Containment — Immediately screen all cryptocurrency wallet addresses, Telegram channels, and business relationships against the UK FCDO consolidated sanctions list (updated to include Xinbi, Legend Innovation Co, and #8 Park). Block any flagged addresses at the exchange, custody, or payment processor level. Source: UK FCDO sanctions list at gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate and prevent further exposure to sanctioned financial infrastructure before eradication steps begin

Controls: NIST IR-4 (Incident Handling) — implement containment as part of the incident handling capability, NIST SI-4 (System Monitoring) — extend monitoring scope to cover blockchain transaction flows touching designated wallet addresses, CIS 3.3 (Configure Data Access Control Lists) — enforce blocking rules at the exchange/custody/payment processor layer for flagged Xinbi and Prince Group wallet addresses, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — treat newly sanctioned entity designations as high-priority remediation items requiring immediate action within defined SLAs

Compensating: For teams without enterprise blockchain analytics tooling: download the FCDO consolidated sanctions list (CSV/XML from gov.uk) and cross-reference against internal transaction records using a Python script with pandas — filter on wallet address fields against the Xinbi/Legend Innovation Co/Prince Group entries. Use OFAC SDN list search API (free, no account required) for US-nexus addresses. Manually query Etherscan, Tron's TronScan, or USDT address lookups (Xinbi operated heavily in USDT on Tron) for flagged addresses to confirm on-chain activity before blocking. A 2-person team can complete initial screening of known wallet lists within one business day.

Evidence: Before blocking wallet addresses, capture and preserve: (1) complete transaction history exports from your exchange/custody platform showing all interactions with Xinbi-associated addresses, including counterparty wallet addresses, timestamps, and USDT/crypto amounts — Xinbi processed predominantly USDT on Tron, so prioritize TRC-20 transaction logs; (2) Telegram channel membership logs, message metadata, and any bot interaction records if Telegram is used in your business operations; (3) internal payment processor logs showing origination and destination fields for any flagged transactions; (4) KYC/onboarding records for any business relationships that may have listed Telegram contact channels associated with Xinbi vendors.

Detection — Query transaction records for transfers involving wallets associated with Xinbi or entities in the Prince Group network. Flag any Telegram-sourced vendor or contractor relationships for review. If your organization operates fraud monitoring, add detection rules for pig butchering contact patterns: unsolicited investment platform referrals, requests to move funds to unfamiliar exchanges, and rapid small-to-large transaction escalation sequences.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate transaction data and communication records against known Xinbi/Prince Group indicators to determine exposure scope and classify the incident

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — conduct structured review of transaction audit logs against Xinbi-associated wallet indicators on a defined frequency, NIST AU-2 (Event Logging) — verify that transaction-level events (origination wallet, destination wallet, amount, asset type, timestamp) are captured in sufficient detail to support retrospective analysis, NIST SI-4 (System Monitoring) — add detection signatures for pig butchering transaction escalation patterns: sequential deposits starting under $1,000 escalating to five-figure transfers within 30–90 days, NIST IR-5 (Incident Monitoring) — track and document all flagged transactions and Telegram relationship reviews as incident records, CIS 8.2 (Collect Audit Logs) — ensure transaction monitoring logs are centrally collected and retained with sufficient history to cover Xinbi's active window (2021–2025)

Compensating: Without a SIEM or commercial blockchain analytics platform: export transaction records to CSV and run a Python/pandas query joining your transaction history against the wallet address indicators published by TRM Labs or Chainalysis (both publish free community IOC lists post-sanctions). For Telegram exposure detection, use Telegram's export feature (Settings → Export Telegram Data) on business accounts to extract channel memberships and contact lists, then grep for known Xinbi-associated channel names or usernames. For pig butchering pattern detection without automated fraud tooling, write a SQL query against your transaction database: SELECT account_id, COUNT(*), MIN(amount), MAX(amount), DATEDIFF(MAX(date), MIN(date)) FROM transactions GROUP BY account_id HAVING MIN(amount) 10000 AND DATEDIFF(MAX(date), MIN(date)) BETWEEN 30 AND 180 — flag accounts matching the escalation profile for manual review.

Evidence: Before running detection queries, preserve: (1) unmodified transaction database snapshots or exports covering 2021–2025 (Xinbi's full operational window) including counterparty wallet addresses, asset type (prioritize USDT-TRC20), and transaction timestamps; (2) Telegram account audit logs showing channel joins, bot authorizations, and contact additions for any business accounts — export before any account modifications; (3) vendor onboarding records where the vendor relationship was initiated via Telegram, including usernames, channel links, and any cryptocurrency payment details; (4) internal fraud alert records from 2022–2025 for accounts showing small-to-large escalation in crypto transfers that were reviewed and cleared — these may now require reclassification.

Eradication — Terminate any business relationships, payment flows, or platform integrations that touch sanctioned entities. If your organization uses Telegram for business operations, audit active channels and bot integrations for exposure to Xinbi-adjacent infrastructure. Report any confirmed exposure to your compliance officer and, where legally required, to the relevant financial intelligence unit (UKFIU for UK-regulated entities, FinCEN for US-regulated entities).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all confirmed touchpoints to sanctioned infrastructure and fulfill mandatory reporting obligations before moving to recovery

Controls: NIST IR-4 (Incident Handling) — execute eradication procedures as part of the incident handling plan, including termination of sanctioned relationships and regulatory reporting, NIST IR-6 (Incident Reporting) — report confirmed exposure to the compliance officer and to UKFIU (Suspicious Activity Report via the National Crime Agency portal) or FinCEN (SAR via BSA E-Filing) within jurisdictionally mandated timeframes, NIST SI-2 (Flaw Remediation) — treat confirmed sanctions exposure as a control deficiency requiring documented remediation with completion tracking, CIS 6.2 (Establish an Access Revoking Process) — apply the access revocation process to terminate API keys, payment processor integrations, and platform access for any sanctioned entity relationships, CIS 2.3 (Address Unauthorized Software) — audit and remove any Telegram bot integrations that served as operational conduits for Xinbi-adjacent services

Compensating: For teams without enterprise GRC tooling to manage regulatory reporting workflows: use the NCA's online SAR portal (National Crime Agency, UK) or FinCEN's BSA E-Filing system (US) directly — both are free and accessible without specialized software. Document the eradication steps in a structured incident log (a shared spreadsheet with date/action/owner/status columns is compliant for small teams). For Telegram bot audit without MDM tooling: review the Telegram Bot API token list in your organization's password manager or code repositories (search codebase for 'api.telegram.org' and 'bot_token') to identify active integrations, then revoke tokens for any bots connected to channels that appear in the Xinbi infrastructure profile.

Evidence: Before terminating relationships or integrations, capture and preserve: (1) complete API key and webhook configuration records for all Telegram bot integrations, including the channel IDs they are connected to and the services they interface with — this establishes the scope of potential exposure; (2) signed contracts, payment terms, and correspondence records for any vendor or counterparty relationships being terminated, including any cryptocurrency wallet addresses listed in payment terms; (3) screenshots and metadata exports of Telegram channels being exited or removed, preserving channel membership counts, admin lists, and pinned message content as evidence of the relationship's nature; (4) internal compliance review records showing which transactions were cleared versus flagged, to support the SAR narrative filed with UKFIU or FinCEN.

Recovery — Verify that all wallet screening and transaction monitoring tools have ingested the updated UK sanctions designations. Confirm your sanctions screening vendor has published a list update reflecting the Xinbi, Legend Innovation Co, and #8 Park additions. Document any transactions reviewed and cleared to support regulatory audit trails. Monitor for secondary designations as Western enforcement actions against overlapping infrastructure continue.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore and verify the integrity of screening controls, confirm updated designations are operationally active, and establish ongoing monitoring for follow-on enforcement actions

Controls: NIST SI-7 (Software, Firmware, and Information Integrity) — verify that sanctions list ingestion by screening tools produces verifiable confirmation (checksum, ingestion timestamp, record count) that the Xinbi/Legend Innovation Co/Prince Group entries are present and active, NIST AU-11 (Audit Record Retention) — ensure all transactions reviewed and cleared during this incident are retained with sufficient documentation to support regulatory audit and examination, NIST AU-9 (Protection of Audit Information) — protect cleared-transaction documentation from modification to preserve its evidentiary value for regulatory review, NIST IR-5 (Incident Monitoring) — maintain active tracking of OFAC, FCDO, and allied enforcement actions against Prince Group and Southeast Asian scam compound infrastructure for secondary designation monitoring, CIS 7.2 (Establish and Maintain a Remediation Process) — document the sanctions list update verification as a recurring remediation action with defined SLA for ingestion

confirmation after each FCDO list publication

Compensating: For teams using free or limited sanctions screening tools: manually download the FCDO consolidated list (XML format from gov.uk) after each update and run a diff against the prior version using a command-line tool (diff prev_list.xml new_list.xml | grep -A5 'Xinbi\|Legend Innovation\|Park') to confirm new entries are present. For transaction documentation without a GRC system: maintain a signed-off spreadsheet log with columns for transaction ID, counterparty wallet, review date, reviewer name, cleared/flagged status, and disposition — this constitutes an adequate audit trail for most regulatory examinations. Set a Google Alert or RSS monitor on 'FCDO financial sanctions' and 'OFAC SDN update' to receive notification of secondary designations against Prince Group affiliates without requiring commercial threat intelligence subscriptions.

Evidence: Before closing the recovery phase, collect and retain: (1) sanctions screening vendor ingestion confirmation records — specifically the timestamp and record count from the list update that included Xinbi, Legend Innovation Co, and #8 Park, to prove when controls became effective; (2) the complete cleared-transaction log from the detection and review phase, with reviewer identity and rationale documented for each cleared item; (3) a point-in-time export of your wallet screening configuration (blocked address lists, watchlist rules) showing the new designations are active, dated and signed by the responsible control owner; (4) any vendor communications confirming their list update publication date for the relevant FCDO designations, preserving evidence of the gap between FCDO announcement and vendor ingestion.

Post-Incident — This action exposes a broader control gap: cryptocurrency transaction monitoring programs may not adequately cover Telegram-based marketplace infrastructure or peer-to-peer laundering channels used by state-linked actors. Review your AML/CFT controls for coverage of Telegram-native financial flows. Assess whether your threat intelligence feeds include TRM Labs, Chainalysis, or equivalent blockchain analytics sources with coverage of illicit marketplace activity. Consider tabletop exercises covering pig butchering exposure scenarios for employees with personal investment accounts, as social engineering entry points frequently bypass corporate controls.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons learned to identify control gaps exposed by Xinbi/Prince Group activity and update detection, monitoring, and training programs before the next enforcement cycle

Controls: NIST IR-4 (Incident Handling) — update the incident handling capability to include Telegram-native marketplace infrastructure as an explicit threat vector in detection and containment procedures, NIST IR-2 (Incident Response Training) — develop and deliver pig butchering social engineering awareness training targeting employees with personal investment accounts, framing it as a corporate risk entry point, NIST IR-8 (Incident Response Plan) — revise the IR plan to include AML/CFT escalation paths, sanctions exposure playbooks, and regulatory reporting timelines (UKFIU SAR: within 'as soon as practicable'; FinCEN SAR: within 30 days of detection), NIST RA-3 (Risk Assessment) — formally assess the residual risk from peer-to-peer and Telegram-native laundering channels not covered by current transaction monitoring rules, and document accepted or mitigated risk, NIST SI-5 (Security Alerts, Advisories, and Directives) — establish a formal intake process for blockchain analytics threat intelligence from TRM Labs, Chainalysis, or Elliptic to ensure illicit marketplace designations reach the transaction monitoring team promptly, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate sanctions designation monitoring into the vulnerability management cycle, treating new FCDO/OFAC designations as time-sensitive remediation items, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — extend account inventory scope to include cryptocurrency exchange accounts and Telegram business accounts to support future sanctions screening

Compensating: For teams without budget for TRM Labs or Chainalysis subscriptions: subscribe to free IOC publications from both vendors (TRM Labs publishes free research reports on illicit marketplaces; Chainalysis publishes the Crypto Crime Report annually and issues free sanctions-related advisories). For tabletop exercises without a facilitator budget: use the CISA Tabletop Exercise Packages (CTEPs) framework (free from cisa.gov) adapted with a pig butchering scenario — script the exercise around an employee reporting an unsolicited investment opportunity received via Telegram and walk through the detection, escalation, and response steps. For AML/CFT control gap assessment without a consultant: map your current transaction monitoring rules against the FATF Virtual Assets guidance (free from fatf-gafi.org) to identify coverage gaps for P2P and Telegram-native flows.

Evidence: For the lessons learned record, collect and preserve: (1) the timeline from Xinbi's initial 2021 operational launch to the UK FCDO sanctions designation, documenting at which point (if any) internal controls would have flagged

exposure — this gap analysis is the primary post-incident artifact; (2) the results of the AML/CFT control coverage review, specifically documenting which transaction monitoring rules had coverage for Telegram-sourced payment flows and which did not; (3) any internal reports or escalations from 2021–2025 that touched Xinbi-adjacent activity and were closed without sanctions consideration — these represent detection failures requiring root cause documentation; (4) employee awareness training records showing whether pig butchering or crypto fraud social engineering was covered in prior training cycles, to establish the baseline before updated training is delivered.

Detection Guidance

No host-based or network IOCs are applicable; this is a financial crime infrastructure designation, not a malware campaign. Detection focus areas: (1) Cryptocurrency compliance screening, run all wallet addresses in transaction history against updated OFAC SDN and UK FCDO consolidated sanctions lists; Xinbi-linked addresses have been documented by TRM Labs (see https://www.trmlabs.com/resources/blog/xinbi-marketplace-remains-active-with-usd-17-9-billion-in-total-volume-despite-enforcement-actions). (2) Fraud pattern detection, pig butchering campaigns use a consistent behavioral sequence: establish trust via social or messaging platforms, introduce investment opportunity, direct victims to fraudulent trading platforms, allow small withdrawals to build confidence, then lock accounts and demand fees. Behavioral indicators include unsolicited contact via Telegram or WhatsApp, investment platform URLs not matching regulated entity registries, and pressure to use specific cryptocurrency exchanges. (3) Threat intelligence enrichment, if your SIEM or SOAR ingests threat intel feeds, add Xinbi and Prince Group as tracked actor tags. Monitor for Lazarus Group TTPs in your environment given the medium-confidence laundering nexus: T1566.002 (spearphishing links), T1583.006 (web service infrastructure), and T1020 (automated asset exfiltration). (4) Employee exposure, consider issuing a fraud awareness advisory to staff, particularly those in finance or executive roles who may be targeted individually through personal channels.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`t.me (Telegram platform)`	Xinbi marketplace operated via Telegram channels and bots; no specific channel identifiers are confirmed in available sources	LOW
URL	`https://www.trmlabs.com/resources/blog/xinbi-marketplace-remains-active-with-usd-17-9-billion-in-total-volume-despite-enforcement-actions`	TRM Labs reporting on Xinbi transaction volume and continued activity; consult for blockchain analytics IOCs including wallet clusters	HIGH

Framework Mappings

MITRE-ATTACK

- **T1531** — Account Access Removal
- **T1650** — Acquire Access
- **T1020** — Automated Exfiltration

- **T1583.006** — Web Services
- **T1567** — Exfiltration Over Web Service
- **T1566** — Phishing
- **T1566.002** — Spearphishing Link
- **T1657** — Financial Theft

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SR-2** — Supply Chain Risk Management Plan

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1531	Account Access Removal	Impact
T1650	Acquire Access	Resource-Development
T1020	Automated Exfiltration	Exfiltration
T1583.006	Web Services	Resource-Development
T1567	Exfiltration Over Web Service	Exfiltration
T1566	Phishing	Initial-Access
T1566.002	Spearphishing Link	Initial-Access

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/uk-sanctions-xinbi-m...	T3
	https://www.bleepingcomputer.com/news/security/uk-sanctions-xinbi-m...	T3
	https://www.bleepingcomputer.com/news/security/us-sanctions-russian...	T3
	https://www.bleepingcomputer.com/news/security/uk-privacy-watchdog-...	T3
Xinbi Marketplace Remains Active with USD 17.9 Billion in Total ...	https://www.trmlabs.com/resources/blog/xinbi-marketplace-remains-ac...	T3

Generated 2026-03-29 18:39 UTC by TJS Security Command Center