China Cyber Year-by-Year Investigator Dossier

Converted evidence PDF for thenitishkr.in Intelligence archive ? Original source: china-cyber-year-by-year-investigator-dossier.docx ? Category: Cross-Border & Loan App Dossiers ? Archive date: 2026-04-06

Summary

Cross-border cyber, loan-app, and jurisdictional evidence record for intelligence review.

Extracted Record Text

FOR CYBER INVESTIGATOR USE | CONFIDENTIAL RESEARCH BRIEF

Bharatiya Sakshya Adhiniyam 2023 | Section 63(4)(c) | IT Act 2000 | DPDP Act 2023

CORE THESIS: The Government of India followed the money (ED/PMLA seizures) but NOT the data ecosystem. 700+ apps distributed via social media referrals and adtech networks harvested contacts, photos, biometrics and location from Indian citizens. Data was NEVER brought back, NEVER destroyed. No SOP issued for data recovery or biometric cancellation. Each year the pattern changed (new app names, new SDK wrappers) while the underlying Chinese infrastructure remained intact. AdTech firms were FTC-targeted in 2015-16 with no Indian equivalent action. NBFC shells with high earnings and zero accountability operated freely. Now AI weaponises that data — and the newest AI malware operates at chip/firmware level below OS detection.

YEAR-BY-YEAR MALWARE AND THREAT TIMELINE

GOVERNMENT SOP GAPS — YEAR BY YEAR ANALYSIS

What the Government DID vs What Was MISSING (SOP Never Issued)

Key Investigator Conclusions

The pattern of Chinese loan apps changes every 12-18 months (new names, new SDKs) — government response is reactive to names, not to infrastructure.

AdTech firms were FTC-targeted in 2015-16 in USA with zero equivalent Indian regulatory action — creating a free zone for data extraction from Indian citizens.

700+ apps distributed via social media referral networks bypass every Play Store policy entirely. Government response focused only on Play Store listed apps.

NBFC dormant shells: register, operate with very high earnings, wind up, re-register. No real-time beneficial ownership tracking prevents this cycle.

AI is now the multiplier: data harvested in 2019-2023 becomes MORE dangerous every year as AI models improve. 2026 AI can do what 2020 human operators could not.

Chip-level/firmware malware (Adups 2015-2017 precedent) is the final frontier. AI-generated firmware implants (VoidLink 2025 precedent) will make OS-level detection irrelevant.

No SOP was EVER issued for: data recovery from Chinese servers, biometric cancellation for compromised KYC selfies, citizen notification, or mandatory chip-level hardware audit.

MASTER SOURCE URL REFERENCE — FOR COURT USE WITH S.63(4)(C) CERTIFICATE

Each URL must be accessed, full page saved, SHA-256 hash computed, and Section 63(4)(c) BSA certificate obtained from forensic examiner before use in any court proceedings.

MALWARE & SDK RESEARCH

[Lookout Igexin (2017)] https://www.lookout.com/threat-intelligence/article/igexin-malicious-sdk

[Threatpost Igexin 500 Apps]
https://threatpost.com/android-spyware-linked-to-chinese-sdk-forces-google-to-boot-500-apps/127585/

[BleepingComputer Igexin] https://www.bleepingcomputer.com/news/security/chinese-advertising-sdk-caught-stealing-data-from-android-devices/

[CyberScoop Igexin] https://cyberscoop.com/igexin-android-data-lookout/

[Dark Reading Igexin]
https://www.darkreading.com/threat-intelligence/google-removes-500-android-apps-following-spyware-scare

[GBHackers Igexin SDK] https://gbhackers.com/chinese-advertising-spying-android-sdk/

[Check Point HummingBad 2016] https://blog.checkpoint.com/2016/07/05/from-hummingbad-to-worse/

[Check Point HummingWhale 2017] https://blog.checkpoint.com/2017/01/23/hummingbad-returns/

[BleepingComputer HummingBad] https://www.bleepingcomputer.com/news/security/hummingbad-android-malware-found-in-20-google-play-store-apps/

[The Hacker News HummingWhale] https://thehackernews.com/2017/01/hummingbad-android-malware.html

[Fortune Yingmob] https://fortune.com/2016/07/05/chinese-android-malware-hummingbad/

[Kryptowire Adups 2016] https://www.kryptowire.com/adups_security_analysis.html

[NYT Adups Secret Backdoor]
https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html

[CyberScoop Adups] https://cyberscoop.com/android-malware-blu-kryptowire-adups-software/

[BleepingComputer Adups 2017]
https://www.bleepingcomputer.com/news/security/chinese-backdoor-still-active-on-many-android-devices/

[Georgetown Firmware Malware] https://georgetownsecuritystudiesreview.org/2018/05/23/flawed-by-design-electronics-with-pre-installed-malware/

[Palo Alto Unit 42 Baidu] https://unit42.paloaltonetworks.com/baidu-privacy-risks/

[Dark Reading Baidu]
https://www.darkreading.com/mobile-security/baidu-apps-leaked-location-data-machine-learning-reveals

[The Hacker News Baidu] https://thehackernews.com/2020/11/baidus-android-apps-caught-collecting.html

[Lookout APT41 WyrmSpy DragonEgg]
https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41

[Check Point VoidLink 2026]
https://research.checkpoint.com/2026/voidlink-early-ai-generated-malware-framework/

[Dark Reading VoidLink] https://www.darkreading.com/threat-intelligence/voidlink-linux-malware-ai

[Google GTIG AI Threats 2025]
https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools

[SpyCloud Chinese Cybercrime] https://spycloud.com/blog/deep-dive-chinese-cybercrime-ecosystem/

[LoanWatch arxiv 2026] https://arxiv.org/html/2601.12634v1

[CISA China Threat] https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

ADTECH / SDK

[SilverPush Wikipedia] https://en.wikipedia.org/wiki/SilverPush

[FTC SilverPush Warning 2016] https://www.ftc.gov/news-events/news/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code

[Forbes SilverPush End]
https://www.forbes.com/sites/thomasbrewster/2016/03/21/silverpush-tv-mobile-ad-tracking-killed/

[FTC InMobi Settlement Official] https://www.ftc.gov/news-events/news/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked-hundreds-millions-consumers

[SecurityWeek InMobi]
https://www.securityweek.com/ad-network-inmobi-settles-ftc-charges-over-location-tracking/

[Alston InMobi Analysis]
https://www.alstonprivacy.com/inmobi-pay-950000-settle-ftc-charges-secretly-tracked-phone-users/

[InMobi APUS Partnership] https://advertising.inmobi.com/company/press/India-and-China-Giants-InMobi-and-APUS-Partner-for-Global-Growth

[APUS Privacy Policy (to China)]
https://privacy.apusapps.com/policy/com_apusapps_launcher/ALL/en/3161/privacy.html

[Alibaba ZOLOZ SDK]
https://www.alibabacloud.com/help/en/financial-intelligence-engine/latest/connect-for-saas

[The Hacker News SilverPush 234] https://thehackernews.com/2017/05/ultrasonic-tracking-signals-apps.html

[Infosecurity SilverPush] https://www.infosecurity-magazine.com/news/android-apps-with-ultrasonic/

[Bitsight Telegram Infostealer]
https://www.bitsight.com/blog/exfiltration-over-telegram-bots-skidding-infostealer-logs

[NVISO Telegram C2 Analysis]
https://blog.nviso.eu/2025/12/16/the-detection-response-chronicles-exploring-telegram-abuse/

INDIA LOAN APP SOURCES

[The News Minute — Chinese Loan Racket]
https://www.thenewsminute.com/news/made-china-how-instant-loan-app-racket-boomed-india-141331

[Al Jazeera — Dark World of Loan Apps]
https://www.aljazeera.com/economy/2023/12/25/the-dark-world-of-illegal-loan-apps-in-india

[TNW — Moneed 389M Records]
https://thenextweb.com/news/a-china-based-loan-app-exposed-millions-of-indians-data-in-an-unsecured-server

[CloudSEK/HackRead — 55 Fake Apps]
https://hackread.com/chinese-scammers-fake-loan-apps-money-laundering/

[Cyber Mithra Loan Fraud] https://cybermithra.in/2023/03/29/chinese-loan-app-frauds/

[MyMudra Fake App List 2026] https://www.mymudra.com/blog/fake-loan-app-list

[Nestapp Fake Loan Guide 2026] https://nestapp.in/blogs/what-are-fake-loan-apps

[The Quint — ED Freezes Cr] https://www.thequint.com/news/india/enforcement-directorate-freezes-crores-funds-chinese-loan-apps-case-paytm-razorpay

[Ikigai Law — App Ban Analysis] https://www.ikigailaw.com/article/26/the-digital-lending-app-ban-rigmarole

GOVERNMENT OF INDIA

[MeitY PIB Ban June 2020] https://pib.gov.in/PressReleasePage.aspx?PRID=1635206

[RBI Digital Lending Guidelines 2022] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12382&Mode=0

[Business Today 232 App Ban 2023] https://www.businesstoday.in/latest/in-focus/story/govt-bans-138-betting-94-loan-apps-with-chinese-links-369034-2023-02-05

[The Register 232 Apps] https://www.theregister.com/2023/02/07/india_bans_232_chinese_lending/

[MeitY DPDP Act] https://www.meity.gov.in/data-protection-framework

[RBI NBFC Rules] https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10224

[CERT-In] https://www.cert-in.org.in/

[Inc42 — 87 Apps Parliament 2025] https://inc42.com/buzz/87-illegal-lending-apps-blocked-so-far-govt/

[DesiDime — 232 App List]
https://www.desidime.com/news/india-to-ban-138-betting-apps-94-loan-apps-linked-to-china

SUPREME COURT / BSA

[Anvar P.V. 2014 IndiKanoon] https://indiankanoon.org/doc/31493622/

[Arjun Panditrao 2020 CyrilShroff] https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/

[Chandrabhan Sanap 2025 INSC 116] https://www.verdictum.in/court-updates/supreme-court/section-65b-evidence-act-certificate-admissibility-evidence-chandrabhan-sudam-sanap-v-state-of-maharashtra-2025-insc-116-1566348

[Kailash v Maharashtra 2025 INSC 1117]
https://www.lawweb.in/2025/09/the-supreme-courts-definitive-ruling-on.html

[LawBeat 65B Video Sept 2025] https://lawbeat.in/supreme-court-judgments/supreme-court-clarifies-video-with-65b-certificate-is-admissible-no-mandatory-transcript-1518636

[LawJurist Electronic Evidence 2025]
https://lawjurist.com/index.php/2025/10/10/admissibility-of-electronic-evidence-in-the-light-of-judicial-decisions/

[BSA S.63(4)(c) Evolution] https://sathyanarayanan.in/erstwhile-65b-now-634-digital-evidence/

[LegalParihar 65B Importance]
https://www.legalparihar.in/resources/Evidence%20Act/importance-65b-certificate-indian-evidence-act

AI / DEEPFAKE THREATS

[Deepstrike Deepfake Statistics 2025] https://deepstrike.io/blog/deepfake-statistics-2025

[Veriff Deepfake Fraud 2025] https://www.veriff.com/identity-verification/news/real-time-deepfake-fraud-in-2025-fighting-back-against-ai-driven-scams

[Sumsub Identity Fraud 2025] https://sumsub.com/blog/top-new-identity-fraud-trends/

[Infosecurity Sumsub Report] https://www.infosecurity-magazine.com/news/ai-deepfake-fraud-skyrockets/

[WEF Deepfake Detection]
https://www.weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive

[Goldilock AI Malware Forecast]
https://goldilock.com/post/the-emerging-danger-of-ai-powered-malware-2025-threat-forecast

[BeamSec VoidLink Analysis] https://beamsec.medium.com/ai-generated-malware-the-week-that-changed-cybersecurity-494fd5c25432

[CASI India FRT Gap] https://casi.sas.upenn.edu/iit/amber-sinha

[ISACA FRT Privacy 2025] https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/facial-recognition-and-privacy-concerns-and-solutions-in-the-age-of-ai

[TechPolicy FRT India] https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/

[EU AI Act Biometric Risk] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

FORENSIC PROCEDURE FOR EACH URL: (1) Open URL in forensic browser session (Chromium with full network log). (2) Save complete page (HTML+assets). (3) Compute SHA-256 hash of saved file: sha256sum [filename]. (4) Record exact access timestamp (UTC). (5) Obtain Section 63(4)(c) BSA certificate from device custodian identifying the device, capture software, and confirming the system was functioning correctly at time of capture. (6) For historical/archived pages, capture from web.archive.org and certify the archive URL with same procedure.

Document compiled: 04 April 2026 | All facts sourced from cited publications. For court use, each source must be independently certified.

CHINESE CYBER THREAT — INDIA: 2015 TO 2026 MALWARE TIMELINE | ADTECH SDK | LOAN APPS | TELEGRAM BOTS | AI WEAPONISATION | GOVT RESPONSE & GAPS Compiled: 04 April 2026 | Cyber Investigator Reference

2015 — Firmware Backdoors Begin | SilverPush 'Listen SDK' | FTC Concern Raised

Lenovo SuperFish & LSE (Firmware Malware) | Lenovo pre-installs SuperFish on 750K+ laptops intercepting HTTPS. Lenovo Service Engine (LSE) writes files at BIOS/firmware level — survives OS reinstalls. First documented commercial chip-adjacent threat. | [Lenovo LSE Advisory] [CISA Alert 2015]

Adups Firmware — First Micromax India Discovery | Shanghai Adups Technology secretly installs apps on Micromax India devices without permission. Adups is FOTA update provider baked into firmware of 400+ device makers globally. Cannot be removed by factory reset. | [CyberScoop Adups] [Georgetown Review]

SilverPush SDK — Microphone Listener Deployed | India-based SilverPush deploys ultrasonic beacon SDK in 67 apps on 18M devices mostly in Asia. SDK continuously samples microphone at 44.1 kHz / 4096 samples per block listening for 18-20 kHz inaudible TV ad tones. Transmits IMEI, location, OS version. CDT submits FTC comments Oct 2015. | [SilverPush Wikipedia] [CDT FTC Comments] [TechCrunch 2014]

India Regulatory Response 2015 | ZERO action on SilverPush or Adups. No SDK disclosure requirement. No NBFC app regulation. Chinese loan apps beginning to enter Indian market. | [CERT-In]

2016 — HummingBad Rootkit Infects 1.4M Indians | Adups Exposed | InMobi FTC Fine

HummingBad Rootkit (Yingmob / China — Chongqing) | Discovered Feb 2016, Check Point. Yingmob: Chinese advertising analytics company. Rootkit gives FULL device control. Generates 2.5M fraudulent ad clicks/day, 50K app installs/day, $300K/month revenue. INDIA: 1.4 MILLION infected devices — 2nd globally after China 1.6M. Peak: 72% of ALL mobile malware globally. 85M total infections. | [Check Point HummingBad] [Fortune / Yingmob] [TIME Magazine]

Adups Backdoor — Full Kryptowire Disclosure (Nov 2016) | Kryptowire confirms Adups collecting SMS content, call history, address books, app lists, hardware IDs from 120K+ phones. Sends to Shanghai. Can remotely install apps and keyword-search SMS. 700M devices globally. BLU phones (US) + Indian budget phones at risk. DHS involved. | [Kryptowire Report] [NYT Secret Backdoor]

InMobi — FTC Settlement $950,000 (June 2016) | FTC: InMobi SDK tracked location of 100M+ consumers INCLUDING CHILDREN without consent. Technical bypass: WiFi SSID/BSSID geocoder mapped to physical

location even when GPS denied. COPPA violation for childrens apps. $950K fine (from $4M). Mandatory data deletion. 2-year independent audits. | [FTC Official Release] [SecurityWeek]

FTC Warning Letters — SilverPush (12 Developers, March 2016) | FTC warns 12 app developers using SilverPush SDK: FTC Act violation for undisclosed background microphone listening. SilverPush officially "ends" UAB service but continues advertising it. NO equivalent Indian action despite SilverPush being India-based. | [FTC Press Release] [Forbes SilverPush End]

2017 — HummingWhale Evolves | Igexin 'Listen SDK' Exposed | Adups Persistent Backdoor

HummingWhale — HummingBad on Play Store (Jan 2017) | Check Point: 20+ infected Play Store apps under fake Chinese developer names (com.bird.sky.whale.camera etc). Key evolution: DroidPlugin VM (Qihoo 360) installs apps INSIDE virtual machine — evades Play Store detection. Also posts fake Play Store reviews to boost malicious apps. 12M+ downloads. | [Check Point HummingWhale] [BleepingComputer] [The Hacker News]

Igexin SDK — THE "LISTEN SDK" Exposed (Aug 2017) | Lookout Security: Igexin advertising SDK (Hangzhou China) in 500+ apps, 100M+ downloads. Downloads encrypted JAR payloads from C2 (sdk.open.phone.igexin.com) AFTER passing Google review. Payload registers PhoneStateListener = captures call state (idle/ringing/off-hook), calling number, call time. Also: GPS, WiFi networks, installed apps. Domain registrar: Beijing Xin Net Tech. | [Lookout Igexin] [Threatpost] [BleepingComputer Igexin] [CyberScoop] [Dark Reading]

Adups — Second Persistent Component (Dec 2017) | Malwarebytes: SECOND Adups component (com.adups.fota.sysoper) still collecting data AFTER first was "fixed." Unremovable from device. Pattern: fix exposed component, insert new one in update. Still on UK/Africa/India budget phones. | [BleepingComputer 2017]

234 SilverPush Apps Confirmed by Academics (May 2017) | TU Braunschweig/UCL/UCSB: 234 Android apps still embedding SilverPush still listening for inaudible TV beacons. Found in McDonald's, Krispy Kreme apps. Can deanonymize Tor users. India still no action. | [The Hacker News] [Infosecurity Magazine]

2018 — Tian Pai Pre-installed Malware | InMobi-APUS India-China Data Pipeline Active | NBFC Shell Phase Begins