FOR CYBER INVESTIGATOR USE | CONFIDENTIAL RESEARCH BRIEF

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

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

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

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	[Check Point HummingWhale] [BleepingComputer]

	virtual machine — evades Play Store detection. Also posts fake Play Store reviews to boost malicious apps. 12M+ downloads.	[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

Tian Pai — 5 Million Phones Pre-Installed Malware	March 2018: Chinese mobile distributor Tian Pai linked to pre-installed malware on 5M Android devices. Supply chain attack — malware in hardware distribution. User cannot detect or remove. This is the hardware/firmware attack path, not app store path.	[Georgetown Review]
InMobi-APUS Pipeline Fully Active — India User Data to Beijing	Partnership live since Sep 2015. InMobi provides location + behavioral data on ALL India APUS users to Beijing APUS Group. APUS Nebula Platform: big data screening for "user prediction." 1.2B users globally, 69% Belt & Road. India data flows to China via commercial agreement — zero regulatory intercept.	[InMobi-APUS Press Release] [APUS Privacy Policy]
Chinese NBFC Shell Companies — Registration Wave	2018-2019: Multiple Chinese-backed NBFC shell companies register in India with nominal Indian directors and Chinese beneficial owners. Apps: CashMaster, RupeeFly, MoneyPlus. All use Alibaba Cloud / Baidu Cloud. Data routes to China. Zero RBI disclosure requirement for cloud server location.	[The Ken] [RBI NBFC Rules]

2019 — My Bank App Unauthorized Transactions | Moneed 389M Records | Suicides Begin | Referral Ecosystem Active

My Bank App — Cross-App Financial Fraud (Hyderabad)	Nov 2019: Bhumana Prasad downloads "My Bank" app, repays Rs.3,500 loan. 14 different apps he NEVER downloaded credit Rs.26,000 to his account and demand Rs.44,000 repayment. First documented cross-app shared data fraud. Reveals: contact list harvested → sold/shared between apps.	[The News Minute]
Moneed/Momo — 389 Million Indian Phone Records Exposed	Hangzhou-based Moneed. Researcher Anurag Sen: UNSECURED Elasticsearch server with 389M Indian phonebook records. Stored on Hangzhou Alibaba server. No encryption, no access control. Contact lists of 389M Indians freely accessible.	[The Next Web (TNW)]
700 Apps via WhatsApp/Telegram Referral Networks	700+ loan apps distributed NOT via Play Store primarily — via WhatsApp groups, Telegram channels, SMS blasts. Each referral earns Rs.50-200/install. Ordinary Indians become distribution agents. Play Store = legitimacy anchor only. Side-loaded APKs	[Al Jazeera Investigation] [CloudSEK/HackRead]

	bypass all Play Store policy enforcement.	
First Suicide Cases — AP/Telangana	First documented suicides from loan app harassment in Andhra Pradesh and Telangana. Morphed images sent to contacts. Victims cannot get police help — officers untrained for cybercrime. ZERO SOP for data recovery from Chinese servers.	[CERT-In]

2020 — COVID Surge | Baidu SDK Exposed | ZOLOZ Biometric Harvest | 59 Apps Banned | Telegram C2 Begins

Baidu Push SDK — IMSI/IMEI/MAC Exfiltration (Palo Alto Unit 42)	Nov 2020: Palo Alto Networks Unit 42 confirms Baidu Push SDK collecting IMSI, IMEI, MAC — permanent irrevocable device identifiers — sent to Baidu servers. Baidu Maps + Baidu Search Box removed from Play Store Oct 28, 2020. Indian apps using Baidu SDK continue undetected.	[Palo Alto Unit 42] [Dark Reading] [The Hacker News Baidu]
Alibaba ZOLOZ SDK — Facial Biometric Harvest Confirmed	Nov 2020: Cashless Consumer analyses 1,050 Indian loan apps — 600 use liveness SDK with China AI servers (ZOLOZ/Alibaba). KYC selfie + Aadhaar = potential parallel Aadhaar biometric DB in China. Researcher Srikanth L: "They can build a parallel Aadhaar system." All apps confirmed storing face recognition data on Chinese servers.	[The News Minute] [Alibaba ZOLOZ Docs]
Snapit App — Bank Account Takeover (Chennai)	Oct 2020: Balaji Vijayaraghavan installs Snapit without logging in — Rs.8.49 lakh unauthorized transactions from Rs.90,000 account. SDK gains account access via SMS OTP interception. Now assisting police investigations.	[The News Minute]
Telegram Bots — C2 Infrastructure for Loan App Operations	2020 onwards: Stolen contact lists uploaded to C2 via Telegram Bot API. Bot distributes harassment scripts to Indian recovery agents. Chinese operators remotely control Indian call centres via Telegram channels. Endpoints used: sendDocument (stolen data), sendMessage (victim info), getUpdates (C2 commands). India in top 5 countries for Telegram infostealer infections.	[Bitsight Telegram Bots] [SpyCloud Chinese Cybercrime] [NVISO Telegram C2]
India — 59 Chinese Apps Banned (June 2020)	MeitY bans 59 apps under S.69A: TikTok, UC Browser, CamScanner, Shareit, APUS Browser. NOTE: APUS Launcher (which shares Indian data with Beijing) NOT banned. InMobi-APUS pipeline NOT disrupted. Moneed server with 389M records: NOT seized, data NOT recovered.	[MeitY PIB]

2021 — 76K Complaints | APT41 Spyware | 1100 Apps Identified | SITs Formed | Rs.46Cr Frozen

WyrmSpy & DragonEgg — APT41 Android Spyware (India Targeted)	Lookout identifies WyrmSpy (detected 2017, active 2021+) and DragonEgg (first 2021) attributed to Chinese state actor APT41 / Chengdu 404. Sophisticated Android surveillanceware targeting India among others. Modules downloaded post-install to evade detection.	[Lookout APT41 Report]
76,000 Loan App Complaints Filed	2021: 76,000 harassment complaints (up from 29,000 in 2020). Documented: morphed images sent to employers, sexual harassment calls, suicides in Telangana/AP/Maharashtra/MP. Suicide note: "Visited Cyber Crime Office but received no assistance." Police not trained. No helpline. No SOP.	[Al Jazeera]
NBFC Shell — High Earnings, Rs.46.67 Crore Frozen (ONE Case)	ED freezes Rs.46.67 crore in virtual accounts of one Chinese loan app network: Rs.33.36Cr in Easebuzz, Rs.8.21Cr in Razorpay, Rs.1.28Cr in Cashfree, Rs.1.11Cr in Paytm. Pattern: NBFC operates 12-18 months with very high earnings, winds up, new shell registered. MCA probes 665 companies.	[The Quint — ED Action] [Inc42]
India — SITs Formed;	State SITs: Telangana, AP, Karnataka, Maharashtra. 7 Chinese	[SC Arjun Panditrao]

Arjun Panditrao 65B Now Mandatory	nationals arrested, 35+ Indians. Arjun Panditrao judgment (2020) now enforced: 65B certificate mandatory for all electronic evidence.	

2022 — RBI Digital Lending Rules | 3,500 Apps Removed | Pattern Shifts to Fake Banks | Telegram Ecosystem Documented

RBI Digital Lending Guidelines — August 2022 (KEY REGULATION)	All disbursals: must flow through regulated entity bank account. No fee deduction before disbursal. Explicit consent for data sharing. Limited KYC retention. PATTERN CHANGES: operators shift to fee-upfront scam where no loan is ever disbursed (fee collected via UPI, operator vanishes).	[RBI Digital Lending] [Ikigai Law Analysis]
Fake Bank Apps — New Pattern Post-Guidelines	CloudSEK: Apps impersonating legitimate banks (Tamil Nadu bank with $23M revenue). C2: [bankname].online domains. 55 fraudulent apps, 15+ Chinese payment gateways. INR 37 lakhs collected in 2 months. UPI LOOPHOLE: UPI providers outside PMLA scope — fund extraction bypasses AML.	[CloudSEK/HackRead]
3,500+ Apps Removed by Google in 2022	Google India removes 3,500+ loan apps in 2022 for non-compliance with Financial Services Policy. Total 4,700+ over two years. Ecosystem persists via side-loaded APKs through WhatsApp/Telegram — Play Store removal has ZERO effect on social media distribution.	[Al Jazeera]
Telegram C2 Fully Documented by Researchers	Full Telegram Bot API abuse chain documented: sendDocument endpoint sends stolen passwords+data; sendMessage sends system info; getUpdates polls for attacker commands. Bitsight observes 1,800 Telegram bots with 5M victim logs from 2020 onwards.	[Bitsight Telegram] [NVISO C2 Analysis]

2023 — 232 Apps Emergency Banned | DPDP Act | Rs.1.06B Seized | Kreditbe Case | SpyCloud SDK Exposure

232 Apps Emergency Banned — MHA/MeitY (Feb 5-7, 2023)	138 betting + 94 loan apps blocked under S.69A on EMERGENCY basis. Reason: Section 69 IT Act — "prejudicial to sovereignty, integrity, defence, security." Annual interest up to 3,000%. Chinese links. NO ecosystem takedown. NO data recovery SOP. NO biometric destruction. NO citizen notification.	[Business Today] [The Register] [Full List DesiDime]
DPDP Act 2023 Enacted — But Not Implemented	Digital Personal Data Protection Act 2023 passed. Up to Rs.250Cr penalty per violation. Cross-border transfer restrictions. But: Data Protection Board NOT constituted. No mechanism to recall data from China. No retroactive remedy for already-harvested biometrics.	[MeitY DPDP] [TechPolicy Press]
ED Seizure — Rs.1.06 Billion (Bengaluru, March 2023)	ED seizes Rs.1.06 billion linked to Chinese loan app fraud. Coercive recovery including phone threats and emotional distress documented. Separate: Rs.46.67 crore frozen in Easebuzz, Razorpay, Cashfree, Paytm.	[Al Jazeera]
Kreditbe — Shivani Rawat Case (June 2023)	Rs.4,000 loan never received. Demanded Rs.9,000. Explicit morphed photos sent to workplace colleagues. Manager asked her to resign. Documents: contact harvest → AI morphed image creation → WhatsApp employer distribution. Documented Al Jazeera Dec 2023.	[Al Jazeera Investigation]
SpyCloud — Chinese SDK Ecosystem via Telegram Documented	SpyCloud Labs: DPI + SDK data on Telegram channels; "SDK libraries" sold claiming backend access to millions of user records. Chinese-speaking criminal communities advertising user data from Indian loan apps.	[SpyCloud Deep Dive]

2024 — AI Deepfake Explodes | PromptFlux AI Malware | Rs.22,845Cr Lost | 87 Apps Blocked

PromptFlux — First AI-Adaptive Malware in Production	Google GTIG (2025 report, first detected 2024): PromptFlux VBScript malware rewrites its own code HOURLY using Gemini AI API. "Thinking Robot" module queries LLM for new obfuscation. Each hour it becomes a different program. Signature-based AV CANNOT detect it. Pattern: AI used mid-execution to evade detection.	[Google GTIG AI Threats] [The Record] [Cybersecurity Dive]
Arup Deepfake Attack — USD 25 Million (Jan 2024)	Hong Kong Arup employee transfers HK$200M (USD 25M) after deepfake video call where multiple "executives" were AI replicas. Proof of concept: harvested face + voice = real-time deepfake impersonation. ZOLOZ selfies + Igexin call recordings from Indian victims = same attack vector possible.	[WEF Deepfake] [Deepstrike Stats 2025]
India — Rs.22,845 Crore Cyber Fraud (Full Year 2024)	2024: Indians lose Rs.22,845.73 crore to cyber fraud. 60% of cybercrime historically linked to illegal loan apps. DoT directs Sanchar Saathi preload on new devices. Mandatory SIM binding ordered for messaging platforms.	[Inc42 — DoT Action]
AI Deepfake Scale — 1 Attack Every 5 Minutes	2024: One deepfake attack globally every 5 minutes (Deepstrike). 1 in 20 IDV failures linked to deepfakes (Veriff 2025). 1,740% increase in deepfake fraud North America 2022-2023 (WEF). Only 0.1% of humans can detect deepfakes accurately (iProov 2025). 3 seconds of audio = 85% accurate voice clone (McAfee).	[Deepstrike] [Veriff] [iProov]
India 2024 — DPDP Board Still Not Constituted	DPDP Act remains partially implemented. No Data Protection Board. No FRT law. No AI regulation framework. India co-hosts AI Action Summit Feb 2025 emphasising innovation over safety.	[CASI India AI Gap]

2025 — VoidLink AI Malware Framework | SC 65B Rulings | 87 Apps Blocked | AI Autonomous Extortion Agents

VoidLink — First Sophisticated AI-Generated Malware Framework (Nov 2025)	Check Point Jan 2026 (developed Nov 2025): Chinese-linked actor. 1 developer, 7 days, TRAE SOLO AI IDE. Full malware framework: custom loaders, implants, rootkits, 30+ plugins, cloud-focused. Uses Spec Driven Development: AI generates architecture, sprint plans, code. Developer OPSEC failure exposed Chinese-language AI planning Markdown files. "The long-awaited era of sophisticated AI-generated malware has likely begun." — Check Point	[Check Point VoidLink] [Dark Reading] [BeamSec Analysis] [Ctech VoidLink]
PromptSteal — Chinese Alibaba Qwen AI Used by Russian APT28	Google GTIG 2025: PromptSteal by Russian APT28 queries Alibaba Qwen2.5-Coder-32B via Hugging Face to generate Windows commands for data exfiltration. FIRST: Chinese AI model as backend for Russian state malware. Cross-border AI weaponisation confirmed.	[Google GTIG]
Supreme Court — Three Landmark 65B Rulings	1) Chandrabhan Sanap 2025 INSC 116 (Jan 2025): SC acquits death row convict — prosecution failed to produce 65B certificate. Mandatory, non-negotiable. 2) Kailash v. Maharashtra 2025 INSC 1117 (Sep 2025): video with 65B certificate admissible as document, no transcript needed. 3) Bhanwar Singh (Sep 26, 2025): CDRs without 65B certificate = INADMISSIBLE.	[Chandrabhan 2025] [Kailash 2025] [LawBeat 65B Video]
AI Autonomous Extortion Agents — Now Operational	2025: AI fraud agents execute complete operations without human: generate fake IDs, interact with KYC systems, adapt harassment scripts based on victim response, run multiple vectors simultaneously. Operators in China can now run autonomous harassment of Indian loan victims with zero Indian	[Sumsub 2025] [Veriff 2025]

	staff required.	
India — 87 Apps Blocked (MeitY Nov 2025 Parliament)	MoS confirms 87 illegal loan apps blocked under S.69A "after due process." Rs.22,845Cr cyber fraud in 2024. DoT: Sanchar Saathi mandatory + SIM binding. STILL NO: data recovery SOP, biometric cancellation procedure, FRT law, AI regulation, chip-level audit mandate.	[Inc42 Parliament 2025]

2026 — CURRENT — Chip-Level AI Malware Horizon | Permanent Data in China | No Regulatory Net

AI Malware at Chip/Firmware Level — The Undetectable Threat	EMERGING 2026: AI-generated malware targeting BIOS/UEFI firmware or semiconductor chip microcode. Precedent: Adups 2015-2017 lived in firmware — OS reinstall could NOT remove it. Next evolution: AI writes implants to chip microcode. OS-level antivirus CANNOT scan below OS layer. Hardware-level inspection required. Stuxnet (2010) targeted industrial PLCs at hardware instruction level — next gen will do this to consumer devices at scale using AI code generation in 7 days (VoidLink precedent).	[Goldilock AI Forecast] [Check Point VoidLink] [CISA China Threats]
India Citizens — Data Permanently in China, Growing Danger	ESTIMATED as of April 2026: 100M+ Indian citizens data on Chinese servers including: facial biometrics (ZOLOZ KYC), 389M+ contact records (Moneed alone), SMS content, location history, financial OTPs, call logs, Aadhaar+PAN combinations. AI capability to process this data grows every year. The data itself never expires. Each new AI model makes old data more dangerous retroactively.	[LoanWatch Research arxiv] [MyMudra 2026] [Nestapp 2026]
India AI Regulation — No Timeline	Dec 2024: Minister Vaishnaw: "lot more consensus needed before AI law." India has no concrete AI regulation plan. EU AI Act (Aug 2024) classifies biometric AI as unacceptable risk. India lax stance. NO SOP ever issued for: (1) data recovery from foreign servers, (2) biometric cancellation, (3) citizen notification, (4) chip-level hardware audit, (5) AI tool laboratory protocol before market deployment.	[CASI India AI] [EU AI Act]

GOVERNMENT SOP GAPS — YEAR BY YEAR ANALYSIS

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

Year	Action Taken	SOP Gap — Not Done	Data Status
2015-16	No action (FTC acted in US, India did not)	No SDK microphone disclosure. No SilverPush audit. No NBFC app regulation.	Flowing to China
2017	No action on Igexin PhoneStateListener in Indian apps	No PhoneStateListener disclosure requirement. No SDK call-log audit mandate.	Flowing to China
2018-19	MCA NBFC registration ongoing	No Chinese beneficial owner disclosure. No cloud server location disclosure. First suicides ignored.	Flowing to China
2020	59 apps banned. APUS Launcher NOT banned.	Moneed data NOT recovered (389M records). InMobi-APUS pipeline NOT disrupted. No biometric cancellation SOP.	389M+ records, no recovery
2021	7 Chinese nationals arrested. SITs formed.	No court order for data deletion from Chinese servers. No victim notification. No forensic database of victims.	Still in China
2022	RBI guidelines (prospective only). 3,500 apps removed.	UPI PMLA loophole not closed. No data localisation mandate for NBFCs. Guidelines only prospective — no retroactive remedy.	Still in China
2023	232 apps banned. DPDP Act passed. Rs.1.06B seized.	NO SOP for: (1) data recovery (2) biometric cancellation (3) citizen notification (4) parallel Aadhaar DB closure. DPDP Board not constituted.	Permanent — no remedy
2024-25	87 apps blocked. DoT SIM binding ordered.	No AI regulation. No FRT law. No chip-level audit. DPDP Board still not formed. AI growing faster than regulation.	Permanent — expanding
2026	No new SOPs announced.	AI malware now at firmware level. No hardware audit mandate. No AI lab protocol. Indian citizens permanently surveilled via 2015-2026 harvested data.	Permanent — AI-weaponised

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.