

Forum:[Hack Forums](#)

Thread: [\[WTS+WTP\] DEEPFAKE - AI-Powered Android C2 Infrastructure RAT](#)

CYBERWAR WEAPONS - January 4, 2026, 3:41 pm

? DEEPFAKE - AI-Powered Android C2 Infrastructure

Introducing DEEPFAKE, the next generation of Command & Control (C2) infrastructure. We've integrated cutting-edge Generative AI directly into your botnet management, allowing for psychological and behavioral manipulation through advanced contextual hijacking.

? Core Features

? Contextual Service Impersonation

1. Automatic Infrastructure Detection:

ISP Fingerprinting: AI analyzes Wi-Fi SSIDs to identify the provider (e.g., "Xfinity_XXX"), enabling deepfake technician calls to "fix line issues" and extract router security questions.

Financial & Career Mapping: Scans billing SMS and app data to identify primary banks (e.g., Chase) and workplace platforms (Slack, Outlook).

Property Management Discovery: Parses rental agreements and communication logs to identify house management services.

? Advanced Deepfake Voice Calls & Automation

Ghost Caller (Contextual Voice Mimicry): Dynamic source selection from history/contacts to initiate calls using cloned voices. Phantom Chat (In-App Message Injection): Injecting artificial messages into real messaging apps (WhatsApp, Signal) to simulate group consensus or urgent peer pressure.

Audio Environment Injection: Playing subtle sounds (crowds, nature, office chaos) during deepfake calls to enhance realism and urgency. OSINT & IRS Integration: Automated web search for provider IVR scripts and office locations. Uses Transformer-based agents to connect to legacy Internet Relay System (IRS) support call systems to retrieve provider-specific greetings and scripts when public data is unavailable.

? Universal App Hijacking & C2 Dashboard

Universal App Logic (UAL): AI-driven UI injection that perfectly replicates the design tokens and architecture of target applications.

Mandatory ID Confirm: Blocks OS-level interaction until PII is extracted.

Card Verification Trap: Simulated errors on e-commerce checkouts to force card re-entry.

Fee-Gated Logic: Intercepts cash transfers to request a "Security Validation Fee" via a secondary payment method.

Shadow Execution & Transaction Spoofing: Background app manipulation and real-time payment recipient modification hidden from the target's view.

? Documentation

- [DESIGN.md](./DESIGN.md): Detailed UI/UX architecture, UAL, and deepfake attack space concepts.

- [DEVELOPMENT.md](./DEVELOPMENT.md): Implementation roadmap, technical architecture, and OSINT integration plans.

? Getting Started

1. Deploy C2: Set up the Express/React dashboard.
 2. Fingerprint: Connect a node and allow AI to map the infrastructure.
 3. Ponder: Define an objective and let the AI generate a contextual hijacking strategy.
 4. Execute: Trigger stealth impersonations or deepfake calls.
- [contract=tid]Start Contract[/contract]