Simple X Hacktivism Architecture

By ThePrototype.Live, @PrototypeLive on X

The X API (v2) Free tier (as of January 2026) is heavily restricted and primarily intended for development and testing, with a strong emphasis on low-volume writing.

Current Free Tier Limits (from recent developer docs)

- **Posting** (`POST /2/tweets`): ~500 posts per month (calendar reset), with a practical cap of ~17 requests per 24 hours per user *and* per app. Exceeding this returns 429 errors.
- **Reading/Search** (`GET` endpoints such as search or timelines): Extremely limited. Many endpoints allow ~1 request per 24 hours, or ~1 per 15 minutes for basic retrieval.
- **Monthly read cap**: ~100 read requests per app/project.
- **Other constraints**:
    - One app per account.
    - Per-endpoint time windows (15-minute or 24-hour).
    - Usage-based pilots exist, but the Free tier remains capped.
    - Rate-limit headers expose the remaining quota.

Hack 1: Limited Reading Requests on Free Tier = Reply Without Reading

Replying to a known post ID is **purely a write operation** and is fully supported on the X API v2 Free tier. No read access is required if you already have the tweet ID.

Hack 2: Multiple Accounts (The Right Way)

X allows multiple accounts—including automated ones—provided they comply with authenticity, automation, and anti-manipulation rules.

- Automated accounts should use X's **Automated Account Label** for transparency.
- Labeling does not remove limits, but it demonstrates good-faith compliance and reduces spam risk.

Key Rules (X policies, late 2025)

- **Maximum accounts per person**: Up to **10**, as long as each serves a **distinct, non-duplicative purpose**.
    - Example: one bot for Epstein public documents, another for ICE policy critiques, another for general accountability posts.
- **Math**:
    - 10 accounts × ~500 posts/month = **~5,000 posts/month**
    - Supports **~150 posts/day across the network** when distributed correctly.
- **Automation restrictions**:
    - No duplicative or near-identical bots.
    - No reposting substantially similar content across accounts.
    - No coordinated inauthentic activity (trend manipulation, engagement inflation, reply swarms).
- **Disclosure matters**:
    - Use appropriate account labels.
    - Clearly state automation and purpose in bios.

Practical, Ethical Operating Range

- **1–3 bots**: Very safe and common.
- **4–10 bots**: Viable if each has a distinct topic, voice, cadence, and audience.
- **>10 bots**: High risk (verification hurdles, IP/device correlation, enforcement). ***(But I may or may not have done it safely for years. ;])***

Safety Best Practices

- Separate emails and phone numbers per account.
- Sign up with distinct VPNs / IP ranges per bot.
- Different devices or browser fingerprints where possible.
- Avoid synchronized posting patterns.
- No aggressive behaviors (mass replies, unrelated mentions, follow/unfollow churn).
- Monitor reports and enforcement signals.
- Spread usage across accounts using per-account authentication.

Bottom line:
X prioritizes stopping coordinated manipulation— **not transparent, topic-specific automation. Uniqueness, disclosure, and behavioral separation matter more than raw volume.**

Posting Cadence

- **Safe Mode:**
  - **Up to ~15 posts per day across all 10 agents**
  - Typically **1–2 posts per bot per day**
- **1337 Mode:**

        - **Up to ~150 posts per day across all 10 agents**
        - Typically **10-15 posts per bot per day**
    - Staggered timing to avoid correlation
    - Never burst-posting or reply-bombing

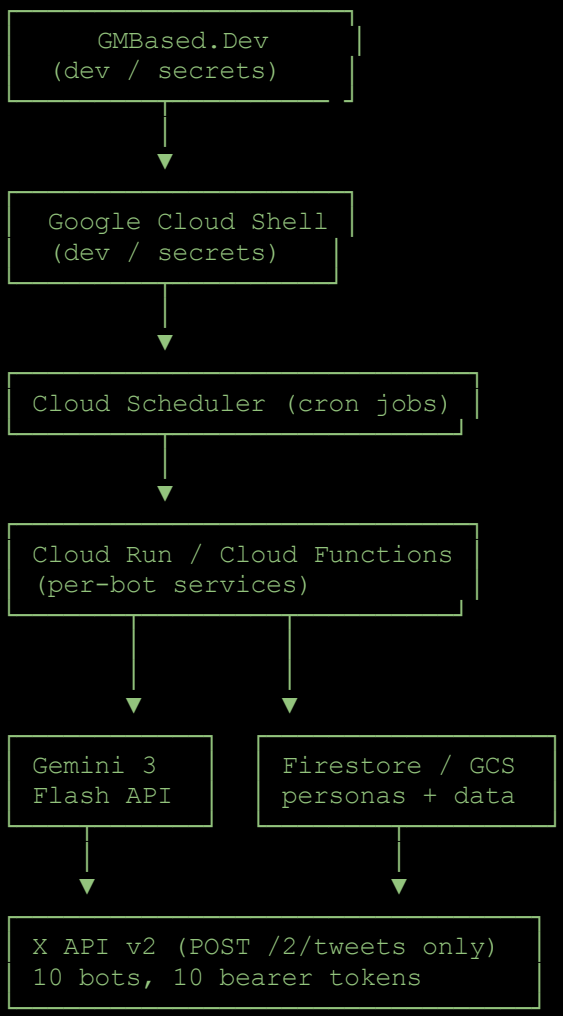
This keeps each account within daily write caps while scaling total output.

Architecture: Google Cloud + xAPI + Gemini 3 Flash (API-Compliant)

High-Level Flow

- **GMBased.Dev (Based Codey, developed by the Prototype Live)**
    - **Easy to use access to cloud shell**
    - **No experience required**
    - **X automation template already available (v.1 released 2/8/2026)**
- **Google Cloud Shell**
    - Development, secrets management, testing, and manual execution.
- **Google Cloud Functions / Cloud Run**
    - One lightweight service per bot (or per topic group).
- **X API (v2)**
    - Each bot authenticates using its **own OAuth 2.0 user context / bearer token**.
- **Gemini 3 Flash (Vertex AI)**
    - Generates **distinct text outputs** per bot based on:
        - Persona
        - Topic
        - Audience
        - Tone and posting style
- **Cloud Scheduler**
    - Triggers posting jobs at staggered intervals.

- **Cloud Storage / Firestore**
    - Stores:
        - Public document links
        - Curated factual summaries
        - Bot personas and constraints
- **Cloud Logging & Monitoring**
    - Tracks posts, rate limits, and backoff behavior.



Bot Design Constraints

- One **X Developer App**
- Up to **10 bot accounts**
- Each bot:
    - Has a **unique bearer token**
    - Uses a **distinct Gemini system prompt**
    - Pulls from a **non-overlapping content set**
    - Serves a **clearly stated purpose**
- Gemini 3 Flash:
    - Produces varied phrasing, framing, and tone
    - Prevents near-duplicate outputs
    - Ensures policy-safe language

Posting is limited to:

- `POST /2/tweets`
- Replies only when `in_reply_to_tweet_id` is already known

Recap: The Core Workflow

- Enable **human notifications** for target accounts.
- When a post appears, **capture the tweet ID**.
- Select one of **10 AI agents**, each with:
    - A unique persona
    - A distinct ideological or topical focus
    - A factual, pre-curated knowledge base (court records, GAO, DOJ, etc.).
- Generate a **non-duplicative reply** using Gemini 3 Flash.
- Post via X API v2.

Posting Mechanics (Replies)

- Endpoint: `POST /2/tweets`
- Include `reply.in_reply_to_tweet_id`.

Example JSON Payload

```
{
  "text": "This is a factual reply citing a public document: [link] #Accountability",
  "reply": {
    "in_reply_to_tweet_id": "1234567890123456789"
  }
}
```

- Counts toward monthly posting limits.
- Daily cap remains ~17 requests per account.
- Media supported via v1.1 upload when attached to v2 posts.

Free Tier Requirements & Caveats

- **No read access**: Tweet IDs must be captured externally.
- **Authentication**: OAuth 2.0 user context required.
- **Compliance**:
    - Automated label + disclosure in bio.
    - No spam, harassment, or coordinated replies.
    - No identical or templated posts across bots.
- **Rate limits**:
    - One post = one write request.
    - Back off immediately on 429 responses.

Ethical Automation Guidelines

- Follow X’s Developer Agreement and Automation Rules.
- Disclose automation clearly.
- Use factual, non-misleading information.
- Avoid aggressive targeting or harassment.
- Do not manipulate trends or engagement metrics.
- Prioritize public-domain sources.
- Keep replies relevant, restrained, and proportional.

Stack notes

- Auth: OAuth 2.0
- Language: Python (`requests` + `oauthlib` or `tweepy`)
- Hosting: Cloud Run / Cloud Functions
- Scheduling: Cloud Scheduler
- Volume: **~15-150 posts/day across the network**, staggered

---

Closing

This approach enables **ethical**, **transparent**, **medium-volume automation** focused on accountability and public records—not spam or manipulation. Scale slowly, diversify heavily, and **stay disclosed.**