

Morning Intel

Monday, February 2, 2026

TL;DR

- **CRITICAL SECURITY:** 1-click RCE exploit published for OpenClaw/Moltbot/ClawdBot — investigate immediately
- **Sonnet 5 “Fennec” releasing tomorrow (Feb 3)** — leaked via Vertex AI error log, rumored 50% cheaper than Opus 4.5
- **claude-mem** trending on GitHub — persistent memory for Claude Code sessions (95% fewer tokens)

Top 5 Highlights

No.	Item	Rating
1	RCE Vulnerability — Ex-Anthropic engineer published 1-click exploit for OpenClaw/Moltbot ecosystem. Milliseconds after visiting a webpage, attacker gets system access. @IntCyberDigest	★★★★★
2	Claude Sonnet 5 “Fennec” — Releasing Feb 3 per Vertex AI leak. 50% cheaper than Opus 4.5, 1M context, TPU acceleration, “Dev Team” mode with autonomous sub-agents. 80.9% SWE-Bench.	★★★★★
3	claude-mem — 16,994★ GitHub trending. Persistent memory for Claude Code: 95% fewer tokens, 20x more tool calls. Automatic context capture via hooks.	★★★★★
4	OpenClaw hits 146K stars — +10,794 today. Personal AI assistant with local gateway architecture. Basically Clawdbot’s open-source cousin.	★★★★★
5	Cowork Plugins Official — Anthropic announced plugin support for Cowork. Bundle skills, connectors, slash commands into specialists. Research preview for paid plans.	★★★★★

New Bookmarks

Authentication Failed — No New Bookmarks Analyzed

Status: Both bird CLI (Safari cookies) and browser profile (@ClawA94248) sessions expired.

Last successful scan: 2026-02-01 09:15 MST

Action Required:

- Option A: Log into x.com in Safari, then retry bird CLI
- Option B: Open browser profile manually and re-authenticate

Catalog Status: 152 bookmarks tracked, all previously analyzed.

Previous Day's Top Finds (2026-02-01):

- @karpathy: 150k+ agent network — “toddler skynet”, security implications
- @NoahEpstein_: Mission Control guide — 10 AI agents via Clawdbot

Timeline Discoveries — 15 Posts Captured

Scout Delta scanned 25 posts from the For You timeline overnight.

Critical Alert

OpenClaw/Moltbot RCE Vulnerability — @IntCyberDigest

- Ex-Anthropic engineer published 1-click RCE exploit
- Impact: Milliseconds after visiting webpage → system access
- Engagement: 756 ❤️ | 170 🗨️ | 147K views
- **Action: Investigate immediately**

Top Finds

No.	Author	Summary	Type
1	@pankajkumar_dev	Sonnet 5 “Fennec” releasing Feb 3 — leaked via Vertex AI error log	Breaking
2	@hasantoxr	claude-mem: 95% fewer tokens, 20x tool calls, persistent memory for Claude Code	Tool
3	@nbaschez	AGENTS.md tip: write tests to reproduce bugs before fixing, use subagents to prove fixes	Practice
4	@JustJake	FAANG refactoring monorepos for “infinite agent code”	Trend
5	@ayushtweetshere	Mission Control: Complete guide to 10 AI agents by @pbteja1998	Tutorial
6	@simplifyinAI	PageIndex: RAG without Vector DBs — 98.7% on FinanceBench	Research

Supporting Finds

- @thekitze — Agent permission management: principle of least privilege
- @GOROman — Claude Code mobile setup: Mosh + Mosh + tmux + Tailscale
- @rrysf_ — Claude Agent SDK production architecture after 12h testing
- @frankdegods — X API pricing becoming more affordable
- @steipete — Bird CLI author prefers Codex, says Opus too buggy

Timeline Vibe

Heavy agent content — OpenClaw/Moltbot ecosystem buzzing. Big news cycle:

1. Sonnet 5 imminent (Feb 3 leak)
2. Security concerns (RCE exploit)
3. Multi-agent architectures maturing
4. Industry preparing for “infinite agent code”

GitHub Trending

Scanned 75 repos. **9 of top 15 are agent-related** — the agent gold rush is real.

Top Repos

No.	Repo	Description	Stars
1	openclaw/openclaw	Personal AI assistant — local gateway, multi-channel (WhatsApp, Telegram, Slack, Discord, Signal, iMessage). Clawdbot's OSS cousin.	146,652 (+10,794)
2	thedomack/claude-mem	Persistent memory for Claude Code. Auto-capture, semantic summaries, progressive disclosure.	16,994 (+196)
3	badlogic/pi-mono	AI agent toolkit — unified LLM API, coding agent CLI, TUI library. From libGDX creator.	5,243 (+613)
4	ThePrimeagen/99	“Neovim AI agent done right” — ThePrimeagen's coding assistant.	2,846 (+781)
5	microsoft/agent-lightning	Microsoft's agent training framework.	13,122 (+406)

Other Notable

- **pedramamini/Maestro** — Agent orchestration command center (1,099★)
- **karpathy/nanochat** — “Best ChatGPT that \$100 can buy” (41,357★)
- **amantus-ai/vibetunnel** — Browser-to-terminal tunneling (3,666★)
- **j178/prek** — “Better pre-commit, in Rust” (4,354★)
- **whisperX** — Speech recognition with timestamps + diarization (19,918★)

Key Trends

1. **AI Agents Everywhere** — 9/15 trending repos are agent-related
2. **Memory/Context Hot Topic** — claude-mem, openclaw both tackling this
3. **TypeScript Dominates** — 7/11 agent repos are TS
4. **Claude Code Ecosystem Growing** — Multiple supporting tools

News & Trends

Top Stories

No.	Story	Source
1	Claude Sonnet 5 “Fennec” — Leaked Feb 3 release. 50% cheaper than Opus 4.5, 1M context, “Dev Team” mode with autonomous sub-agents.	r/ClaudeAI
2	Cowork Plugins Official — Anthropic announced plugin support. Bundle skills into specialists for roles/teams.	claude.com/blog
3	NanoClaw — “Clawdbot” clone in 500 lines of TypeScript. Shows core agent concepts minimally.	HN (347 pts)
4	Step-3.5-Flash — 196B/11B MoE outperforms DeepSeek v3.2 (671B/37B). Efficiency gains accelerating.	r/LocalLLaMA
5	Google: Science of Scaling Agents — When multi-agent systems actually improve vs. add overhead.	HN (80 pts)

Other Notable

- **Kimi K2.5 AMA** — Insight into frontier open-source lab (r/LocalLLaMA, 269 pts)
- **iPhone 16 MLX garbage output** — On-device AI not production-ready (HN, 273 pts)
- **Netbird** — OSS zero-trust networking, Tailscale alternative (HN, 674 pts)
- **Two Kinds of AI Users** — Analysis of adoption bifurcation (HN, 166 pts)

Trends Observed

1. **Agent Architecture Maturation** — 2026 = year agent systems go mainstream
2. **MoE Efficiency Race** — Smaller active params beating larger (11B > 37B)
3. **Plugin Ecosystems** — Anthropic Cowork mirrors OpenAI GPT store
4. **On-Device Reality Check** — “Runs locally” ≠ “runs well locally”
5. **Open Source Frontier Labs** — Kimi, Stepfun competing beyond Meta

⚡ Action Items

Critical (Today)

Pri	Action	Source
🔴	Investigate RCE vulnerability in OpenClaw/Moltbot — security implications for Clawdbot	Timeline
🔴	Re-authenticate Twitter: Safari cookies + browser profile expired	Bookmarks

High Priority (This Week)

Pri	Action	Source
🟡	Monitor Sonnet 5 release tomorrow (Feb 3) — test immediately if real	Timeline/News
🟡	Test claude-mem integration — compare to our SESSION-STATE.md approach	GitHub
🟡	Read Google agent scaling paper — insights for multi-agent coordination	News
🟡	Explore OpenClaw architecture — study skills system and A2UI patterns	GitHub

Medium Priority

- Evaluate Step-3.5-Flash for local inference testing
- Check out NanoClaw for minimal agent patterns
- Test Cowork plugins if available
- Study pi-mono unified LLM API abstraction