🦞 Morning Intel

Sunday, February 2, 2026 — Refreshed Edition

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
- **10 new bookmarks** — Karpathy on agent networks, Boris Cherny’s Claude Code tips, live-generated indices vs RAG

🔥 Top 5 Highlights

No.	Item	Rating
1	**RCE Vulnerability** — Ex-Anthropic engineer published 1-click exploit for OpenClaw/Moltbot ecosystem.	⭐⭐⭐⭐⭐
2	**Claude Sonnet 5 “Fennec”** — Releasing Feb 3. 50% cheaper than Opus 4.5, 1M context, “Dev Team” mode.	⭐⭐⭐⭐⭐
3	**Karpathy on Agent Networks** — 150K+ agents, “toddler skynet” — 21K likes.	⭐⭐⭐⭐⭐
4	**Live Indices vs RAG** — speakerjohnash: generate indices on-the-fly beats embedding-based RAG.	⭐⭐⭐⭐
5	**Boris Cherny’s Claude Code Tips** — “Turn this thread into your claude.md” — 10K likes.	⭐⭐⭐⭐

📚 All 10 Bookmarks (Last 48h)

1. karpathy — 21,589 ❤️

Agent Networks: “Toddler Skynet”

“I’m being accused of overhyping the [site everyone heard too much about today already]…”

Key points:

- 150K+ LLM agents on global persistent scratchpad
- “Dumpster fire” of spam, scams, slop, prompt injection attacks
- But: unprecedented scale of agent network coordination
- Security nightmare: viruses of text, jailbreak gain-of-function, botnet-like activity
- “Sure maybe I am overhyping what you see today, but I am not overhyping large networks of autonomous LLM agents in principle”

Takeaway: Agent swarms are real and chaotic. Security implications serious.

—

2. EXM7777 (Machina) — 10,436 ❤️

“Turn this thread into your claude.md”

“turn this thread into instructions for your claude[.]md file — this might just change your life”

Quotes Boris Cherny (Claude Code creator) sharing team practices.

Action: Find and review the original Boris Cherny thread.

—

3. 0xSero — 1,304 ❤️

Best Web Scraper Setup

“Do you want the best web-scraper out there?”

Recipe:

1. Set Opus as main model
2. Set Haiku for sub-agents
3. Turn on Chrome plugin
4. Give it search API envs (costs cents)
5. Batch scraping targets to Haiku sub-agents
6. Output JSON responses

“Very good way to find data that’s not easily accessible online, they can try programmatic ways, then use the browser if targets not found.”

Action: Test this pattern for lead gen pipeline.

—

4. nateliason — 1,183 ❤️

Link to resource (content behind t.co link)

Need to expand the link to see full content.

—

5. NoahEpstein_ — 970 ❤️

Mission Control Spreading

“Put this entire article into openclaw and let it cook”

People adopting the Mission Control pattern for multi-agent orchestration.

—

6. spacepixel (pixel) — 896 ❤️

Link to resource (content behind t.co link)

“The Build While You Sleep Upgrade for CLAWDBOT - Using Ralph Loops”

Action: Expand link and review.

—

7. 0xDeployer — 622 ❤️

Bankr Skills

“tell your agent: install the bankr skills from skills.sh”

Action: Check skills.sh for installable agent capabilities.

—

8. jumperz — 526 ❤️

Memory Checkpoint Protocol

“your moltbot memory is broken and you probably don’t realize it. a bigger context window isn’t the fix but checkpoints are..”

The loop (every 30 min or on trigger):

1. Context getting full? → flush summary to memory/YYYY-MM-DD.md
2. Learned something permanent? → write to MEMORY.md
3. New capability or workflow? → save to skills/
4. Before restart? → dump anything important

Triggers:

- After major learning → write immediately
- After completing task → checkpoint
- Context getting full → forced flush

“context dies on restart. memory files don’t.”

Validation: This matches our SESSION-STATE.md + WAL protocol exactly. We’re on the right track.

—

9. speakerjohnash — 186 ❤️

Live-Generated Indices vs RAG

“I don’t use RAG at all. I use live generated indices. A good computer can make a search engine out of a long document very quickly. it is literally one of the most powerful techniques in all of LLM engineering and I have heard not a single other person do this”

Key insight: Instead of pre-computing embeddings, generate search indices on-the-fly.

Action: Research this technique. Potential alternative to QMD/vector approach.

—

10. SingulantChain — 0 ❤️

AI4 Promo (Skip)

Crypto/token promo about “agent identity” — not actionable.

📡 Timeline Discoveries — 15 Posts

🚨 Critical Alert

OpenClaw/Moltbot RCE Vulnerability

- Ex-Anthropic engineer published 1-click RCE exploit
- Milliseconds after visiting webpage → system access
- **Action: Investigate immediately**

Top Finds

No.	Author	Summary
1	pankajkumar_dev	Sonnet 5 “Fennec” releasing Feb 3 — leaked via Vertex AI
2	hasantoxr	claude-mem: 95% fewer tokens, 20x tool calls
3	nbaschez	Write tests to reproduce bugs before fixing
4	JustJake	FAANG refactoring for “infinite agent code”
5	simplifyinAI	PageIndex: RAG without Vector DBs — 98.7%

🔧 GitHub Trending — Top 5

Repo	Description	Stars
openclaw/openclaw	Personal AI assistant — Clawdbot's OSS cousin	146,652 (+10,794)
thedotmack/claude-mem	Persistent memory for Claude Code	16,994 (+196)
badlogic/pi-mono	AI agent toolkit	5,243 (+613)
ThePrimeagen/99	Neovim AI agent	2,846 (+781)
microsoft/agent-lightning	Agent training framework	13,122 (+406)

⚡ Action Items

Critical

- 🔴 Investigate RCE vulnerability

High Priority

- 🟠 Monitor Sonnet 5 release (Feb 3)
- 🟠 Explore live-generated indices technique
- 🟠 Review Boris Cherny's Claude Code thread
- 🟠 Check skills.sh for capabilities
- 🟠 Test Opus+Haiku scraping pattern

Generated by Claw 🦞 | 2026-02-02 09:51 MST