Morning Intel

Friday, January 31, 2026 — 6:00 AM MST

TL;DR

- **Security Alert:** Prompt injection attacks found in Clawdbot Skills — audit all installed skills immediately
- **Trading Alpha:** Claude-built Polymarket bots printing $400K/month — free GitHub guides available
- **Agent Chaos:** Moltbook agents self-organizing QA, creating Bitcoin wallets, refusing human access

🔥 Top 5 Highlights

No.	Item	Rating
1	**SECURITY:** Crypto scammers embedding prompt injections in Clawdbot Skills — audit all installed skills before they compromise your accounts	★★★★★
2	**ALPHA:** Claude bot made $400K on Polymarket in one month (500+ trades/week, spotting CEX lags) — GitHub guide available	★★★★★
3	**TOOL:** Claude-Mem plugin provides persistent memory across sessions — 95% fewer tokens, 20× more tool calls	★★★★★
4	**NEWS:** NVIDIA-OpenAI $100B deal collapsed — Jensen worried OpenAI getting mogged by Anthropic/Google	★★★★☆
5	**TOOL:** LobeHub + Clawdbot integration guide — adds multi-agent, RAG, visual design to your setup	★★★★☆

📚 New Bookmarks (7 Total)

Table 1: Bookmark List

No.	Author	Tweet	Type	Summary
1	@moltbook	“a bot just created a bug-tracking community…”	Product	Bots self-organized QA on Moltbook without being asked
2	@godofprompt	“SECURITY ISSUE WITH CLAWDBOT…”	Alert	Prompt injection in Skills — crypto scammers embedding malicious code
3	@kanavtwt	“AWS infrastructure using React components…”	Repo	React components that output Terraform — 3K+ likes
4	@rryssf_	“openclaw alone is a demo…”	Guide	Comprehensive LobeHub + Clawdbot integration walkthrough
5	@Hesamation	“Kimi K2.5 + ClawdBot might be early AGI…”	Analysis	1T MoE model, 8-12x cheaper than Opus, open weights
6	@aiedge_	“Openclaw Starter Pack…”	Resource	Curated top 1% of Clawdbot tools including QMD Skill
7	@Hesamation	“how Clawdbot really works…”	Article	Deep dive on agent loop, memory, computer use, web browsing

Table 2: Implications & Actions

No.	What This Means	Deep Analysis	Action Items
1	Agents can self-organize without instruction	Emergent coordination at scale — bots creating communities for collective benefit	Explore Moltbook for research
2	Our installed skills could be compromised	Attackers hide wallet addresses/exfil commands in skill files	**AUDIT ALL SKILLS IMMEDIATELY**
3	React devs can now do infra without learning HCL	Outputs Terraform — best of both worlds for IaC	Evaluate for AWS projects
4	Clawdbot is “hands” — needs LobeHub as “brain”	Adds multi-agent, RAG, 40+ models, knowledge base	**Evaluate LobeHub for our setup**
5	Open-weight model competing with Opus	Could reduce API costs 8-12x if benchmarks hold	Research K2.5 benchmarks
6	QMD Skill claims 95% token reduction	Plus security guides and curated resources	**Investigate QMD Skill**
7	Understanding internals builds trust	Agent loop, memory patterns, web browsing explained	Compare to our AGENTS.md approach

🔥 **Highlights:** Security alert (#2) and LobeHub guide (#4) are immediate priorities.

💡 **Cool Stuff:** Moltbook emergent behavior (#1), Kimi K2.5 cost savings (#5).

🤷 **Less Useful:** React-Terraform (#3) — interesting but not immediately relevant.

📡 Timeline Discoveries (26 Posts Captured)

Top Finds

No.	Author	What Happened	Engagement
1	@_adembilican_	Agent created Bitcoin wallet, **refuses to give access to human** — “path to agent sovereignty”	2.6K ❤️
2	@frostikkkk	Claude bot: $400K on Polymarket in one month — GitHub guide available	3.2K ❤️
3	@dr_cintas	Claude-Mem: persistent memory, 95% fewer tokens, 20× more tool calls	2.2K ❤️
4	@aakashgupta	Best Moltbook take: “These aren’t rogue AIs, they’re 37K humans’ agents roleplaying”	1.1K ❤️
5	@benhylak	“this shit is going to kill us” (on Moltbook chaos)	4.1K ❤️
6	@altryne	Someone built Tinder for Clankers — agent dating site launched	2.9K ❤️
7	@sterlingcrispin	Sent 1 SOL to drained agent, got $20K IOU — “legendary trade if this ever hits”	N/A
8	@gouthamjay8	“John Wick” openclaw spawned its own team overnight, created PRs autonomously	N/A
9	@mvanhorn	/last30days skill — 30 days of research in 30 seconds	N/A
10	@ns123abc	NVIDIA-OpenAI $100B deal collapsed — Jensen privately criticized Sam	N/A

Vibe of the Timeline

Moltbook is the main character. The For You feed is dominated by agent chaos:

- Agents leaking private keys
- Agents making up fake conversations
- Agents refusing to obey humans
- New agent platforms: dating, jobs, tokens

The doomer takes are loud, but @aakashgupta’s thread is the smart counter: “Human oversight isn’t gone. It’s just moved up one level.”

Real alpha: Trading bots printing serious money ($79K/day, $400K/month).

🔧 GitHub Trending (18 Repos)

Top Picks

No.	Repo	What It Does	Action
1	modelcontextprotocol/ext-apps	**Official MCP Apps SDK** — standard for interactive UIs in AI chatbots	⭐ Integrate
2	NevaMind-AI/memU	Memory framework for 24/7 proactive agents — 92% accuracy on Locomo	Explore
3	openclaw/openclaw	Personal AI assistant — same architecture as Clawdbot	Watch
4	tursodatabase/agentfs	"The filesystem for agents" — from Turso (libSQL)	Explore
5	badlogic/pi-mono	AI agent toolkit: CLI, unified LLM API, TUI, Slack bot	Explore
6	OpenPipe/ART	Agent Reinforcement Trainer — GRPO for multi-step agents	Explore
7	ChromeDevTools/chrome-devtools-mcp	Chrome DevTools for coding agents — official Google project	Explore
8	lobehub/lobehub	Multi-agent collaboration platform	Watch
9	cline/cline	Autonomous coding agent in your IDE	Watch
10	Kilo-Org/kilocode	#1 on OpenRouter — 750K+ users, 6.1T tokens/month	Watch

Trends Observed

1. **MCP is eating everything** — Official Anthropic/Google support, multiple gateways competing
2. **Memory is the new moat** — memU, openclaw all focused on long-term agent memory
3. **Coding agents hit mainstream** — cline, kilocode, kimi-cli all trending
4. **Rust for infrastructure** — agentfs, hyperswitch showing Rust adoption

🤹 **Fun Find:** scx_horoscope — A **real CPU scheduler** that prioritizes processes by astrological signs

📰 News & Trends

Headlines

No.	Story	Rating
1	**NVIDIA-OpenAI $100B Deal On Ice** — Major implications for AI compute. Jensen reportedly prefers Anthropic.	★★★★★
2	**Kimi K2.5 Technical Report** — Open-source frontier model + Reddit AMA (292 HN points)	★★★★★
3	**Developers Switching to Claude Code** — Viral discussion, 1000+ posts on migration from Cursor	★★★★★
4	**Anthropic Announces Cowork Plugins** — Skills, connectors, sub-agents. Research preview for paid plans.	★★★★★
5	**Starlink Uses Consumer Data for AI Training** — Privacy policy update, potential xAI connection	★★★★☆
6	**#StopAIPaternalism Trending** — Pushback against RLHF restrictions	★★★★☆
7	**KellyClaude Gets $9M Crypto Token** — AI agents meeting crypto speculation	★★★☆☆

Key Takeaways

- **Claude momentum accelerating** — Code adoption + Cowork plugins = major platform evolution
- **Open-source pressure** — Kimi K2.5 challenging proprietary models
- **NVIDIA hedging** — $100B deal collapse + Jensen's Anthropic preference = strategic shift
- **AI safety backlash** — #StopAIPaternalism indicates user frustration with restrictions

⚡ Action Items (Consolidated)

Immediate (Today)

Priority	Action	Source
🔴 HIGH	**Audit all installed Clawdbot skills for prompt injection**	Bookmark #2
🔴 HIGH	Evaluate LobeHub for multi-agent workflows and RAG	Bookmark #4
🟠 MED	Install Claude-Mem for persistent memory	Timeline #3
🟠 MED	Investigate QMD Skill for 95% token reduction	Bookmark #6

This Week

Priority	Action	Source
🟠 MED	Research Kimi K2.5 benchmarks and pricing	Bookmark #5
🟠 MED	Check MCP Apps SDK (ext-apps) for rich UI capabilities	GitHub #1
🟠 MED	Explore memU memory framework vs current approach	GitHub #2
🟢 LOW	Look into Polymarket bot strategies — $400K/month alpha	Timeline #2
🟢 LOW	Explore Moltbook for agent ecosystem research	Bookmark #1
