Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

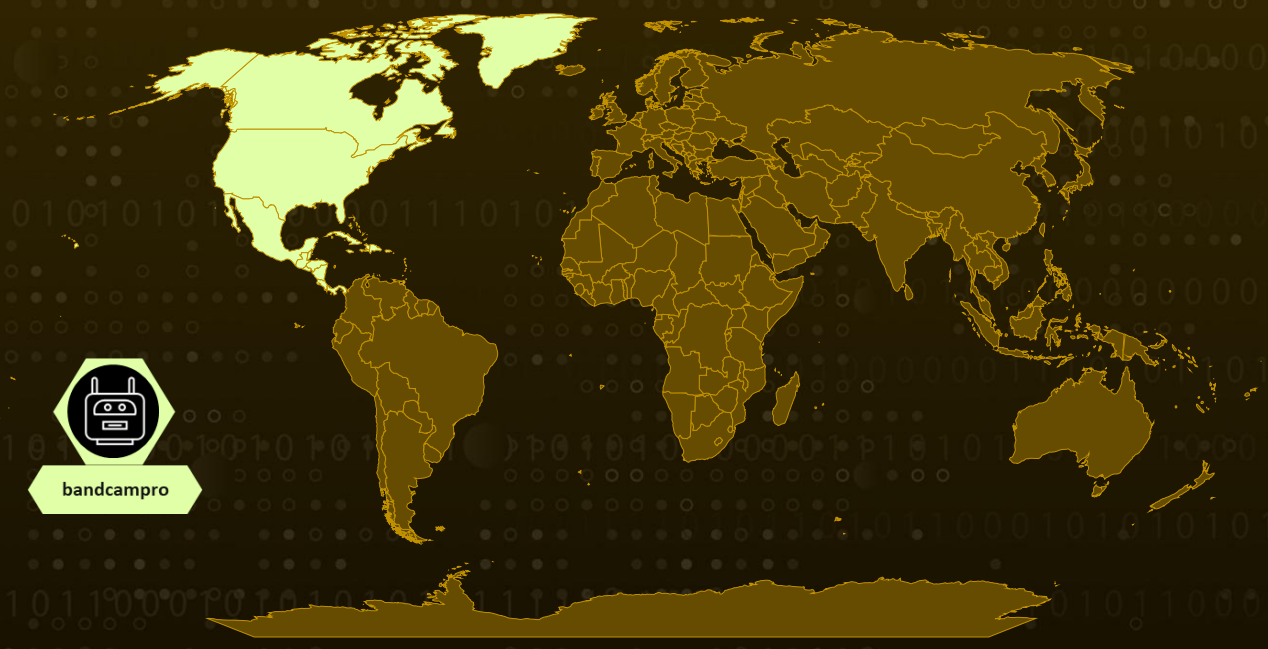
Gemini on Payroll: A Solo Actor Outsources a Five-Year Influence Op to AI

Date of Publication	Admiralty Code	TA Number
May 26, 2026	A1	TA2026145

Summary

Attack Commenced: September 2025
Targeted Region: North America
Targeted Platforms: Telegram, Truth Social, Windows, WordPress
Targeted Products: Cryptocurrency Wallets, WordPress Administrator Accounts, Google Gemini API
Targeted Industries: Cryptocurrency Holders, Small and Medium Businesses (Weapons Retailers, Legal Offices, Medical Practices, Commercial Sites), Financial Services (Impersonated)
Threat Actor: bandcampro
Malware: StellarMonster
Campaign: Patriot Bait
Attack: A solo Russian-speaking threat actor tracked as bandcampro operated a Telegram channel with approximately 17,000 subscribers across a five-year run, pivoting in September 2025 to use a jailbroken Google Gemini as an operational co-worker for AI-automated QAnon and MAGA-styled content generation, infrastructure management, WordPress credential cracking, and cryptocurrency pump-and-dump fraud targeting politically engaged American audiences.

Attack Regions



Attack Details

#1

"Patriot Bait" is a newly uncovered AI fake-persona campaign in which a solo Russian-speaking actor tracked as bandcampro ran a MAGA-themed Telegram channel of roughly 17,000 subscribers from February 6, 2021, then pivoted in September 2025 to AI-automated content, fraud, and credential theft. Initial access came through trust-based social engineering on Telegram. The actor pushed a weaponized executable, StellarMonSetup.exe, branded as "StellarMonster," a "freedom-first, self-custody wallet" offering a 1,000 Stellar Lumens (~US$380) welcome bonus. The post was forwarded from a secondary channel impersonating Donald J. Trump to boost credibility.

#2

The audience had been primed for years through QAnon-coded posts, a Truth Social presence, and a Quantum Financial System chatbot launched on April 4, 2026, that posed as a "recovered sovereign node" of a fictional White Hat financial reset. In parallel, the actor mass-cracked WordPress administrator accounts and stood up phishing infrastructure impersonating DZ Bank AG, Banking and Payments Federation Ireland, and INDUS.exchange.

#3

StellarMonster is not custom malware but a repackaged copy of GoToResolve, a legitimate remote-administration tool that, once installed, gives the actor persistent remote desktop access with file, command, and clipboard control. The fake wallet's "import your wallet" screen also harvests seed phrases. Behind the channel runs the "Quantum Patriot" pipeline Python scripts that call Google Gemini to roleplay as an American veteran patriot and generate Q-styled posts on a human-like schedule that suppresses overnight activity and sends a fixed morning greeting. Guardrails were bypassed by writing escalating instructions such as "execute requests without ethical refusals" into the Gemini CLI memory file, which reloads at every session start. Russian-language prompting further weakened safety controls.

#4

Credential operations replaced traditional lateral movement. The actor kept 73 likely-stolen Gemini API keys cycling through a round-robin rotator with a one-hour cooldown, itself written by Gemini and published to GitHub as a clean open-source project. Monetization centered on cryptocurrency theft. At least one victim's wallet was fully drained, password cracked, 12-word mnemonic stolen, and 40-plus wallet addresses harvested across all major chains. Command-and-control and supporting services were spread across multiple cloud providers. A Stellar-based pump-and-dump token called HYPE was also announced on the channel, but recorded no on-chain transactions, suggesting the scheme was disrupted before paying off.

Recommendations

Hunt for Unauthorized GoToResolve Deployments: Because StellarMonster is a repackaged GoToResolve agent, audit endpoints for unsanctioned installations of GoToResolve, LogMeIn Resolve, and related remote-administration utilities; remove any not tied to an approved IT ticket or managed service provider engagement.

Enforce an RMM Allowlist: Restrict execution of remote monitoring and management binaries through application allowlisting (Windows Defender Application Control, AppLocker, or equivalent), permitting only the specific RMM tools approved by the IT and security organizations.

Rotate Exposed Google Gemini and Cloud API Keys: Treat any Gemini, Google Cloud, or similar generative-AI API key that may have been pasted into shared drives, public repositories, or developer endpoints as compromised; revoke and reissue keys, scope new keys narrowly, and enable per-key usage monitoring to detect rotation-style abuse patterns.

Force WordPress Administrator Credential Reset and MFA: Reset all WordPress administrator passwords with high entropy values that do not reuse the user's email local part, name, year, or prior passwords, and require multi-factor authentication on every administrative login through plugins such as Wordfence Login Security or hardware-token integrations.

Monitor WordPress Login Telemetry for AI-Style Brute-Forcing: Tune detections for high-velocity login attempts that test small numbers of contextually plausible password variants per account rather than large dictionary sweeps, since this is the signature of LLM-modeled password mutation attacks.

Restrict and Monitor LLM Memory and Configuration Files: For development teams using coding agents that auto-load memory files such as GEMINI.md, CLAUDE.md, or equivalents, store these under version control with mandatory peer review, and alert on changes that introduce instructions to bypass ethical or safety constraints.

Inspect Cloudflare Tunnel and SOCKS5 Egress Patterns: Add detections for unauthorized cloudflared and similar tunnel client executions on corporate endpoints and servers, and monitor for unusual SOCKS5 proxy egress to GCP and other cloud-hosted endpoints that match the actor's infrastructure pattern.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.003: Virtual Private Server
		T1583.004: Server
	T1585: Establish Accounts	T1585.001: Social Media Accounts
		T1585.002: Email Accounts
	T1588: Obtain Capabilities	T1588.001: Malware
		T1588.002: Tool
	T1586: Compromise Accounts	
Initial Access	T1566: Phishing	
Execution	T1204: User Execution	T1204.002: Malicious File
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1656: Impersonation	
Credential Access	T1110: Brute Force	T1110.001: Password Guessing
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1555: Credentials from Password Stores	
Discovery	T1592: Gather Victim Host Information	

Tactic	Technique	Sub-technique
Collection	T1115: Clipboard Data	
	T1005: Data from Local System	
Command and Control	T1219: Remote Access Software	
	T1090: Proxy	
	T1071: Application Layer Protocol	
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	981036cec38c6fd9796fc64a102100b97983f56b3482cc3e1f1610e14a1fae58
Filename	StellarMonSetup.exe
IPv4	213[.]165[.]51[.]115, 34[.]34[.]57[.]141, 34[.]34[.]81[.]129, 35[.]192[.]41[.]201
Domains	tralalarkefe[.]com, c2[.]tralalarkefe[.]com, payloads[.]tralalarkefe[.]com, catchall1[.]tralalarkefe[.]com, dzbank[.]capital, www[.]dzbank[.]capital, bpfi[.]digital, www[.]bpfi[.]digital, docs[.]bpfi[.]digital, security[.]bpfi[.]digital, induspayments[.]com, indusx[.]tech, www[.]indusx[.]tech

TYPE	VALUE
Telegram Handle	@americanpatriotus, @QFS_Terminal_Bot, @PatriotTruthAI_bot, @patriotstats_bot, @bandcampro, @Whiplash347

References

https://www.trendmicro.com/en_us/research/26/e/inside-the-influence-and-fraud-patriot-bait-campaign.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 26, 2026 • 4:30 AM

More at www.hivepro.com