blackpoint

THREAT SNAPSHOT

TaskWeaver

THREAT TYPE	PLATFORM	FIRST OBSERVED	CONFIDENCE
Loader	Windows	June 21, 2026	High

Summary

TaskWeaver is a modular, heavily obfuscated Node.js malware loader, identified by the Blackpoint Adversary Pursuit Group (APG), designed to fingerprint compromised systems, establish encrypted command and control (C2) communications, and retrieve and execute additional payloads. Rather than embedding a fixed set of post-exploitation capabilities, it functions as a reusable deliver framework capable of deploying follow-on malware such as information stealers while leveraging the trusted Node.js runtime to blend in with legitimate developer activity.

Aliases and Related Activity:

- Associated with Djinn Stealer
- Observed following exploitation of SimpleHelp vulnerability CVE-2026-48558

Key TTPs

Tactic	Technique	ATT&CK ID
Execution	Command and Scripting Interpreter: JavaScript	T1059.007
Stealth	Obfuscated Files or Information	T1027
	Masquerading	T1036
Discovery	System Information Discovery	T1082
Command and Control	Application Layer Protocol: Web Protocols	T1071.001

Tooling & Family Links

Tool / Family	Role
Djinn Stealer	Observed second-stage information stealer delivered by TaskWeaver.
Node.js (node.exe)	Legitimate JavaScript runtime abused to execute TaskWeaver.

Indicators of Compromise

Type	Value
TaskWeaver Execution	node.exe <path>\jquery.js
TaskWeaver	00cc86d1144020c24c8fbb3a8dc6b908926497ebd23be3bf854360f93d1c8f4c
TaskWeaver	jquery.js
TaskWeaver C2	a[.]dev-tunnels[.]com
TaslWeaver URI Pattern	POST /api/<base64url>.<base64url>.<base64url>

Recommendations

- Apply application control and restrict or monitor the execution of Node.js (node.exe) on systems where it is not operationally required.
- Monitor for abnormal outbound HTTPS communications initiated by node.exe, particularly to newly observed or low-reputation domains.
- Limit remote management software access using least-privilege principles and multi-factor authentication (MFA), and regularly audit technician accounts for unauthorized activity.
- Place administrative interfaces behind a VPN or identity-aware proxy and enforce phishing-resistant MFA, source restrictions, and dedicated administrative workstations.
- Restrict temporary tunneling services, such as trycloudflare[.]com when not required.

References

Beal, Nevan; Decker, Sam (2026, June 29) Blackpoint Cyber: “A Djinn in the Machine: TaskWeaver’s Node.js Intrusion Chain.” https://blackpointcyber.com/blog/a-djinn-in-the-machine-taskweavers-node-js-intrusion-chain/