Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

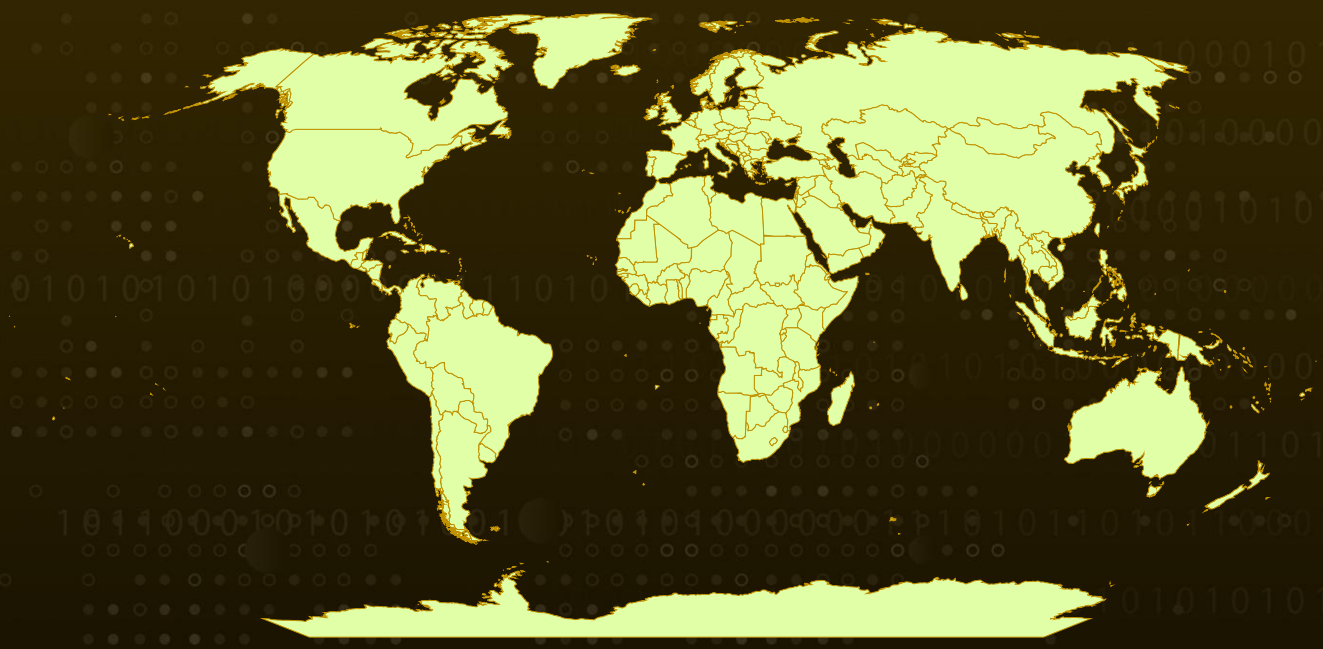
JSCeal: Crypto Stealer Hidden in V8 Bytecode

Date of Publication	Admiralty Code	TA Number
September 08, 2026	A1	TA2026261

Summary

First Seen: Early 2025
Targeted Regions: Worldwide
Targeted Platforms: Windows, macOS
Targeted Industries: Cryptocurrency, Financial Services
Malware: JSCeal
Attack: JSCeal is a cryptocurrency-focused information stealer spread through malicious Facebook and Google ads that steer would-be traders toward counterfeit trading sites and fake TradingView installers. Delivered as compiled V8 bytecode run by a bundled Node.js runtime, it lifts saved passwords and cookies from browsers, harvests Telegram sessions, logs keystrokes, captures screenshots, and installs a local proxy with a rogue certificate to intercept and rewrite traffic to crypto services such as Binance, Bybit, and Ledger. Using stolen cookies, it can replay live sessions to take over a victim's Google account.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

JSCeal is a cryptocurrency-focused stealer that reaches well beyond simple theft, layering in credential harvesting, on-host surveillance, and live traffic interception, all shipped as compiled V8 bytecode (JSC files). It reaches its targets through paid-advertising abuse rather than email: its operators buy malicious ads on Facebook and Google that funnel would-be cryptocurrency traders toward counterfeit trading portals impersonating trusted brands, most notably TradingView. Once there, visitors are prompted to download what looks like a legitimate trading-app installer. Because the victim runs the fake installer themselves, that first execution step quietly sidesteps many perimeter defenses.

#2

After the bait is taken, PowerShell stages the infection by unpacking two ZIP archives, one carrying a Node.js runtime, the other the main payload and its components. The payload is the unusual part: rather than plain JavaScript, it ships as compiled V8 bytecode (a .jsc file) run directly by the bundled Node.js, so the source never lands on disk. Before compilation, the code is put through a commercial JavaScript obfuscator that renames symbols, RC4-encrypts strings for runtime reconstruction, flattens control flow, and routes calls through proxy helpers. Newer builds add an AES-256-CBC layer around the Brotli-compressed payload, with the key supplied by an earlier stage rather than stored in the bundle. Together, these layers push the malware outside the analysis workflows defenders normally rely on.

#3

Once running, JSCeal acts as a broad theft toolkit aimed straight at the victim's accounts. It enumerates installed Chromium-based browsers, walks their profile directories, and pulls saved passwords and cookies from Chrome, Edge, Brave, Opera, Opera GX, Avast Secure Browser, Vivaldi, and Cốc Cốc, while also collecting Telegram session data, stored secrets, and OAuth tokens, and running a keylogger and screenshot module. Rather than just banking a password list, it weaponizes what it steals: harvested cookies let it replay a live browser session, and it drives the victim's own browser through Google's real authentication flow with anti-bot automation to obtain a fresh, valid OAuth token and full account access.

#4

For its endgame, JSCeal installs a locally generated, attacker-controlled certificate and stands up a local proxy, giving it an adversary-in-the-middle position over the victim's HTTPS traffic. This is not passive interception: dedicated handlers rewrite requests and responses for Binance, Bybit, and Ledger, swapping login QR codes, injecting fake security prompts, and replacing legitimate scripts, while generic handlers swap HTML, block hosts, clear cookies, and record account details and crypto balances. The exact command-and-control and exfiltration channel is not detailed in the available reporting, though payload staging relies on Brotli compression and AES encryption.

Recommendations

Block Malvertising Delivery Paths: Treat search and social-media ads as an active malware vector. Use DNS and web filtering to block newly registered and known-malicious trading-lookalike domains, and consider ad-blocking or ad-verification controls on managed endpoints to cut off the Facebook and Google ad redirects JSCeal relies on.

Enforce Trusted-Source Software Installation: Restrict installation of trading and financial applications to official vendor sources and an approved software catalog. Application allowlisting (for example, WDAC or AppLocker) stops the fake TradingView installer from executing even if a user downloads it.

Constrain PowerShell and Script Execution: Enable PowerShell Constrained Language Mode, script-block and module logging, and alert on PowerShell spawning archive extraction or launching a bundled Node.js runtime, the staging behavior used to unpack JSCeal's two ZIP archives.

Hunt for Rogue Node.js and .jsc Execution: Baseline legitimate Node.js usage and flag node.exe (or a bundled node binary) executing .jsc bytecode files from user-writable or temporary directories, especially shortly after a browser-based download.

Detect Unauthorized Root Certificate Installation: Monitor and alert on additions to the local trusted root certificate store and on unexpected local proxy configuration. A newly installed self-generated certificate paired with a local proxy is a strong indicator of JSCeal's traffic-interception stage.

Protect Browser Credential and Cookie Stores: Discourage saving passwords in browsers for privileged and finance-related accounts, deploy endpoint protection that guards browser credential and cookie databases, and monitor for processes reading multiple browsers' user-data directories in quick succession.

Reset Credentials and Revoke Tokens on Suspicion: If infection is suspected, rotate passwords from a clean device, revoke active browser and OAuth sessions (including Google), sign out all sessions, and reset Telegram sessions to cut off replay of anything already stolen.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583.008: Acquire Infrastructure	
Initial Access	T1189: Drive-by Compromise	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.007: JavaScript
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1140: Deobfuscate/Decode Files or Information	
	T1553: Subvert Trust Controls	T1553.004: Install Root Certificate
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1539: Steal Web Session Cookie	
	T1056: Input Capture	T1056.001: Keylogging

Tactic	Technique	Sub-technique
Discovery	T1217: Browser Information Discovery	
Collection	T1113: Screen Capture	
	T1005: Data from Local System	
	T1557: Adversary-in-the-Middle	
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	03f4e47b9c2283c32bb8f8f042ce6e41, 0b8015cbb1ffdc6efe6a306ff5b1115f, 1026743185dfa10e9ddc21b5a4c578d5, 201f28b5e62e52e269757930f941c774, 2fe27eb8c99626e8c02e4bfd02aca962, 376ec4dbc3363fa7131367e4c6327a46, 462195f7f8033df7371e899fe9bc51de, 499184635d56a9827d2059256a35e530, 533d0b93ea03cd5bab4eec0f0ebadd03, 68ac84a8470d1f365f0bb2f37b6256d5, 6e023b9b3097a2dba311cb06a91fe259, 7b659fa5c93af29c4e11d8c8be437058, 8fb3e6acb2024601eba0ba484091ff3d, af105a6d4dc10b2bfefd75e917245523, b2dad3f88b7f6870f83eb1ad852b7f7e, d064dfaaef30c057b832c79996c35e89, d5b4137135cf121e3ea07b1c81fe1108, e26687982d924ffebef6fbf2d9d43350, e27ae65977287bdfb7b0e15fd3603f85, e711a90b5ece5380e1acaed56827e8d5, 0d1fce0cb2b9dec26a10f0822aeffb19, e8b5448b4f7b013e8c6191b20d3f8291, fd4494c555adda2eb54b88f5c9c08801, 91038aebe528a065c3e995a418db6826, 13823095b8d31013ba41a5c98ce69b59, 454fb012cdd0736e4ed41fabf0916f46, 975319142460fc43e3dc5e495d2313c9, 09dbfac09f9cafdbc7d225eb144f0e69, c8db5e53572e68349c76107f03544491, a2aa25f0d5b23a2897576e4cf9596a7c, 2841170a19c028c16990cdcc6fd499bc, 30f23bb28ce56584f8f098ff0035b029, cd7afa032d5f5be0db037edb617f438b, a6f5bb2b8a3e1abe332dd40e50d78aa3, 6626b8caf2734c83a93f78d31b703584, 469c60508d4470bc1cc5e4a70d0e7112, e57f6ca6543616f75f7811273616fe47, a308fa1524c9d5b8dc55d2b296a2629b, 576e94d705bd50811dc9525a45732bc3, 710cc97e64618c68ffca72ac405a48a1, c605371a8caf11497f1879597292e338, 2477fd3e348c51bf575ede398253d0b3, 7650ec266b414d097101da12c4384659,

TYPE	VALUE
MD5	1b7f4288b12373c8d6488fde69c8ce0d, e81b35b76b4d97751c0724bc0c7f3b83, fa0180946b9a6ad373b7a8f983e2e597, 10c576a57fc040eddd84d631786b8dda
SHA256	de213ebc44c614d0b2324787e267183dbbbbb19e1ad866435a322ee00e24e7b6, 4757f3d26bc7110e9c7f4da8050afc2ed661cd92aec9cf7d301d9b9b24e0b668, 212d21ed1c4b5bd9b9104e04f2876842b99cd17def3591df72781891d584dca0, f720d6f6baebd4ef76df978f2678387385ee2d20a37423e7957c2341fe46f9ca, 8d389f56c5b71d194bddd5b6ce5906e7e22730034ad882606cc8ae701011bf8c, 2ef1ea37a941330a79a3056461e61992864e6e38c0f68cbb626ebf1f96e362c5, 62ba626bce09db5f8750938edced3768b401084a7d6584cd6ff9d53d2517781d, c12ac711b4ceaa17a4e48b16fca7dabd615e4eaf35bb65fe9131ceac1687095a, 484da78b0fef35711f86876f7c1c77264b8e4295d7393369379c384c05337ec5, 0c31453e74a3b763c7aea550b4f5f194e7656226012b243221eb93fa22da118e, 5f071a36c0a79ddce92824a49fd8e9bd048b87cabb635671073402365afc342a, 82f8215c7e68f4a6b656b7dc6638982a6625c662ce6d6a05330eefbfde2637ac, 31b38e76ccaca6f38168b4fdd9cbdedd8efa7e65fe6090240e281bd3152a6feb, caf8bfc90e4300b8a18c3fe3a4badbe44c106830e7432d8eea227857a790ec91, 1f5acba97db6d514e4b35ba0601c5269697e8ab3bb99d097db25ec7e74464594, 9b5359dc99501ef2a4667d265e9b032f76dc28c97437a463965e2168d20e5c38, 8abffe0d13d3b93ca3469045e4cebbee25b3631e6bba13880f04b7c8acac2536, 95b39a0bad021f33e08df042b02d3267faee7bbc3e3080dda295c35b464dd607, b73c3d732bb6bff8b9088cc0dcbadb35eea0802056324f1b6295cb9277c62755, 1b0efeb1d988b7bc11014ccc9fdff141fc16425d659f553f6cc6946872499667,

TYPE	VALUE
SHA256	5b4edd9bffdd7909b8b432eacd463d59eb23eba151c9e218161ab15dd72d55ed, 05db78bff1a48a674e70368b96a550a5f9f93271eb261ab63b36ee37e0e8b9f8, 058ae4136e241f116d8c5b1a1cad15b53090797154539faa35706568fbd85d9b, c77b3b7a507162bfc03cfeb8ef18d5ee7017e8fcbd6d7e005f986a3c967b8d45, b90e3aaae14e7787e5ea4a6d4beee672049bd5eb05427f2c80b64f605860d2b8, 55ee2359b12fbce928532d1d4efcfbbbd63340502d0107466c803d6517b44437, b3f76851a8e55a967029be7ffe4c15afd63656d6946a3df77206455e5ac28ea1, 67e3d7bcdf4cfd25750425ac0682e0ed98b3cb473448696fb79bf311fcdb18cd, 99b8124c2a64d26567f19a44618144b1d6a7501a5892918f0120a496f983a0f2, dc561df51d27ed3a99cb916bf08452c901956778c26709e69705cbdf77f74816, dd2bb7316be55446aebfa31d05e57e936eb9a18d5d9c20d60d87493100d05fe6, 684aabefe516539cda48c65cb08014e6eb645b4f1e668d159fe0c18cf74eb407, f6c670e65765d10a5ca0205a6ece3a3e6c7c730b0a8534c5adef4a3cbf06eb9c, 3d800b7dbdcb6874e29ddd2e9a1313f3d82b323e89a720c632c708098a7ca0e9, 6b498ec73d32860202b6a6ff8d21f8b5216c3903e066136f9d69ef2969955a78, 5fe810cb5b34c8fd07c7eca301b32ef2d3b86290828d67edaad8444db811f20b, 7f3e73b2e0ebea3eaffa3685e0a162d10fde388282060d9e35b173b743676916, 8c674f58b157a7319b564bb774e7aeb35135d615511838e4a553fe7ea9e94759, 5a024ae97242be3b1b954f845f7a87a1411c47830f81a2b54f47ec2cf741e2a0, 09f803f69bde280adbd4e584ed26a01affac9721db8c5730275d385f084b422a, 18347a39f174c97947649b3f1de55e8409ff805e808f2101e5953a956e9ee99f, 9615f60ea3cc1c65eb8fe6d77bb85fe6b455503193eab02310a873fccadd332e,

TYPE	VALUE
SHA256	acdaba94e9975e8e03fa13bae7f0f93f165f42226aeecea3af5a4e0111bdfb7e, 2d42aa747f7ebc3280b14d30c6b71043545888946d9d6acd6abbaf4545841462, 84db0663b6aa8df2ac04470288fd5528f5537fb89d78a2e01cabdce371a686e8, 7e1c82cdcff73ac69fee3ba71d67353a062103f1bfae4f263d03b3b84e48d782, c288e79ed9d1fb654a341b92d878a3165a09fb21dfa826f3559b46738fdbbdeb, 8b3ed808822479eb62d78d819db35362e4e79138ac82310d30e0c351a17992b6, 2cf2d22d1317df6c49171be61ef35c4f6c3da17785fa73e68aa95109075f79bd, 94191824bb5062622663e2434d2b749a8c936eb573aaac23594dee8dda304731, 742ad2dd3d2444bd3758b6e46dd76f9c43dfaae03bdffc3598ce7d8ab3cd3ac5, 504345099ba4c77cbb4224101794e525f2bc9adb40904159195c17d7e345085e, 11e85a8306057945accc65395b780377c07d4ec9ae52d78185554bf1957e3caa, 43c57c60a8008e617b16dc6dab29372347ebe144f043200c106149c3106438ba, cfdb3bb9edea8de7c7a70275a2b8689619276f1e5f2b8805e67ceab1ee252f6d, 6075cd41edb59c43c13aa3591e054cdb127b17bf34e036dae591244ea2f8868f, c13fcb214a576401cd624dacf248480c38b8bcbb85e5d3da52cc204a61395d14, 395f4c1562a1a8caeba254ccbc7d278b8194795ff5ad3824cfc0c5662738335f0, 192342a5e4fcfc5e8ec430427e1dfa773fd324e3d7215047f36f1114ef930f4e, 0c72513efdae9785894b6e925590d0b59b652dda53b8cd882037a87e672a4a5a, 9f673e3b361f438e9986f2a7b2423d3d02dbecea0c220163566850ef6ab56626, 59c9038227c634f4e512afaa98f2ca998b0aaac83437c218686c51acbda7873e, 88b1d75d330cf6be9a7f48cdfd51c48125a86f9bcb6bcb736fb8399e0617d680, 2c29b4089845b010428f8be48e62f165e0f7f8a48e58200629c6020c7ac2cab7,

TYPE	VALUE
SHA256	aec3e252c429e150c42976d6badeea31e48a0356ecbd27796df83fc6d3de16ea, 57f32b3942d5543177f07e49fc84f1409a49b5df7d25549e543607c223b87695, fa02e707af9a353f0e2d7a77489c11c2249a1d9dbccf74070130b31834e8d7c3, 36d34b6405a33fcb95e1323e2ca8c688af02b315fc1bded19fa27bd1c7ca6f1c, 22833568125bcc55000503cfe6b470925b7d095ff7592bef79fe52e0573123cc, 06dce0f294c62f2a2393c812ff711bde831bf420a4df484bcf5b6241fc0f00d0

References

https://research.checkpoint.com/2026/breaking-the-seal-static-deobfuscation-of-jsceals-compiled-v8-bytecode/

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

September 08, 2026 • 07:40 AM

More at www.hivepro.com