Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

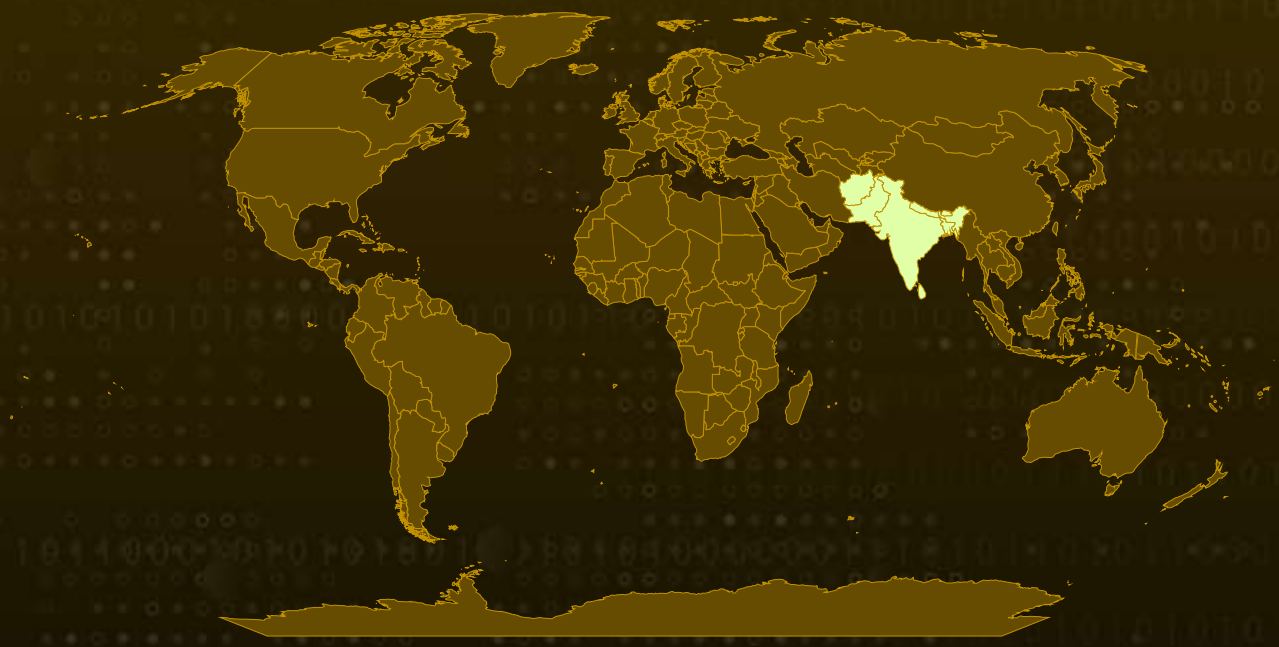
XCSSET v40 Locks macOS Out of Its Own Security Updates

Date of Publication	Admiralty Code	TA Number
August 06, 2026	A1	TA2026223

Summary

First Seen: April 2026 (XCSSET v40)
Targeted Regions: South Asia
Targeted Platform: macOS
Targeted Products: Xcode, Xcode project files (.xcodeproj, .pbxproj), CocoaPods, Git and GitHub repositories, Google Chrome, Safari, Mozilla Firefox, Opera, Brave, Microsoft Edge, Yandex Browser, 360 Browser, Telegram Desktop, Apple Notes, Apple Reminders, Finder, Terminal, Launchpad, MetaMask, TokenPocket, TronLink, BNB Chain Wallet, Phantom Wallet, Evernote, Skype, WeChat, XProtect, MRT, TCC
Malware: XCSSET
Attack: XCSSET is a modular macOS malware family that hides a downloader script in Xcode projects and Git repositories. The host is only infected when a developer builds the poisoned project. Version 40, tracked across two waves from mid-April 2026, was found in the Xcode projects of dozens of legitimate applications with thousands of users and infects every other Xcode project on a host it reaches.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

XCSSET is a modular macOS malware family that spreads by injecting a downloader script into benign files inside Xcode projects and Git repositories, with endpoint infection triggered only when a developer builds the poisoned project locally. The v40 iteration, tracked from mid-April 2026 across two attack waves, hides itself in the Xcode projects of dozens of legitimate applications with thousands of active users and infects every remaining Xcode project on a compromised host, turning developer workstations into self-propagating supply chain vectors.

#2

XCSSET spreads through the developer supply chain. The operators hide a downloader script in benign files inside Xcode projects and vulnerable Git repositories, and since early April 2026 have concealed it in dozens of legitimate applications with thousands of users, including open-source projects on GitHub. A poisoned codebase stays dormant until the developer builds it, when a malicious run-script build phase runs silently and contacts the attacker's server for the next stage. The pattern is old: the 2020 version hid its components in a .xcodeproj file and used two zero-days to read Safari's protected cookies and run JavaScript outside the browser sandbox.

#3

Execution runs in four stages. The staging payload reports basic host metadata; if the server accepts the profile, it returns an obfuscated script that fingerprints the hardware, drops a loader, and compiles an AppleScript wrapper that osascript runs in memory before both staging files are deleted. The resulting orchestrator pulls further modules and decrypts them in memory, loading keyloggers, clipboard hijackers, and browser hijackers without writing to disk.

#4

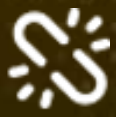
Version 40 rotates its fingerprints at every level, recompiling the loader every few hours and encrypting each module under a per-build key, so hashes and string signatures have no lasting value. Persistence spans Git hooks, Launch Daemons, trojanized applications, .zshrc, the Dock, and a new fileless loop that stores its payload in the macOS defaults system. The malware also blocks XProtect, MRT, and TCC updates, suppresses Apple's telemetry service, locks the XProtect rule database, and resets AppleEvents consent to re-prompt the user while posing as System Settings. Hosts identified as virtual machines receive no further modules.

#5

Exfiltration runs over the same command-and-control channel, with separate endpoints for logs, file upload, heartbeat, configuration, and browser-hijack events. Data is archived before transmission, and the 2020 inventory also encrypted and renamed files under Documents, Downloads, and Desktop. The infrastructure was prepared in advance: roughly 40 domains registered in short bursts in early 2026 across a small pool of IP addresses, then aged for months to defeat new-registration detection. The 2025 campaigns used .ru domains posing as content delivery networks; the 2026 wave added .in siblings, matching the targeting of South Asian developers. The operators then undercut themselves by reusing those IPs across separate campaigns and linking all four through one shared SSL thumbprint, reused SSH keys, and a shared self-signed remote desktop certificate.

Recommendations

Scan Every Xcode Project on Compromised Developer Hosts: Because the malware infects all existing Xcode projects on a host for maximum impact, including projects stored inside .zip archives, a single confirmed infection requires a full sweep of the developer's home directory and any archives within it, not just the project that triggered the alert.



Inspect Git Hooks and Shell Startup Files: Check the hooks/pre-commit file in every .git directory on affected systems, and review ~/.zshrc and ~/.zshrc_aliases for appended payload lines. These persistence points survive removal of the primary payload and re-infect the host on the next commit or shell session.

Monitor AppleScript and osascript Execution: Deploy behavioral detection for abnormal osascript instances, especially processes spawned from Xcode build phases, multi-pass Base64 or xxd decoder chains piped to a shell, and osascript activity that establishes outbound network connections. Because v40 executes its modules in volatile memory and deletes staging files immediately, process telemetry is often the only durable evidence.

Block Ad Hoc Signed and Untrusted Local Binaries: Track ad hoc code-signed applications and untrusted local code signers, and isolate binaries that bypass Gatekeeper requirements. The malware ad hoc signs its fake Launchpad, Reminders, Finder, Terminal, and Xcode bundles as well as its trojanized Telegram replacement.

Rotate Credentials, Cookies, and SSH Keys: Treat browser cookies, session tokens, password-manager contents, cloud and repository credentials, Apple ID credentials, and cryptocurrency wallet material on affected hosts as compromised. Audit ~/.ssh for keys the user did not create, revoke any authorized keys added during the incident, and verify that remote login was not enabled without authorization.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
Initial Access	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
Execution	T1059: Command and Scripting Interpreter	T1059.002: AppleScript
		T1059.004: Unix Shell
		T1059.007: JavaScript
	T1569: System Services	T1569.001: Launchctl
Persistence	T1546: Event Triggered Execution	T1546.004: Unix Shell Configuration Modification
	T1543: Create or Modify System Process	T1543.004: Launch Daemon
	T1647: Plist File Modification	
	T1554: Compromise Host Software Binary	
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1548: Abuse Elevation Control Mechanism	T1548.006: TCC Manipulation
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
		T1027.004: Compile After Delivery
	T1140: Deobfuscate/Decode Files or Information	
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
	T1070: Indicator Removal	T1070.004: File Deletion
	T1574: Hijack Execution Flow	T1574.006: Dynamic Linker Hijacking

Tactic	Technique	Sub-technique
Defense Evasion	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
	T1222: File and Directory Permissions Modification	T1222.002: Linux and Mac File and Directory Permissions Modification
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Checks
Credential Access	T1539: Steal Web Session Cookie	
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1056: Input Capture	T1056.001: Keylogging
		T1056.002: GUI Input Capture
	T1185: Browser Session Hijacking	
Discovery	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	
	T1083: File and Directory Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1217: Browser Information Discovery	
	T1087: Account Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery
Collection	T1005: Data from Local System	
	T1115: Clipboard Data	
	T1113: Screen Capture	
	T1560: Archive Collected Data	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation
	T1486: Data Encrypted for Impact	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6fa938770e83ef2e177e8adf4a2ea3d2d5b26107c30f9d85c3d1a557db2aed41, 7e5343362fceeae3f44c7ca640571a1b148364c4ba296ab6f8d264fc2c62cb61, 857dc86528d0ec8f5938680e6f89d846541a41d62f71d003b74b0c55d645cda7, 6614978ab256f922d7b6dbd7cc15c6136819f4bcfb5a0fead480561f0df54ca6, ac3467a04eeb552d92651af1187bdc795100ea77a7a1ac755b4681c654b54692, d11a549e6bc913c78673f4e142e577f372311404766be8a3153792de9f00f6c1, 532837d19b6446a64cb8b199c9406fd46aa94c3fe41111a373426b9ce59f56f9, 4f78afd616bfefaa780771e69a71915e67ee6dbcdc1bc98587e219e120f3ea0d, 819ba3c3ef77d00eae1afa8d2db055813190c3d133de2c2c837699a0988d6493, 73f203b5e37cf34e51f7bf457b0db8e4d2524f81e41102da7a26f5590ab32cd9, ccc2e6de03c0f3315b9e8e05967fcc791d063a392277f063980d3a1b39db2079, 6622887a849b503b120cfef8cd76cd2631a5d0978116444a9cb92b1493e42c29, 32fa0cdb46f204fc370c86c3e93fa01e5f5cb5a460407333c24dc79953206443, 924a89866ea55ee932dabb304f851187d97806ab60865a04ccd91a0d1b992246, af3a2c0d14cc51cc8615da4d99f33110f95b7091111d20bdba40c91ef759b4d7, 534f453238cfc4bb13fda70ed2cda701f3fb52b5d81de9d8d00da74bc97ec7f6, 172eb05a2f72cb89e38be3ac91fd13929ee536073d1fe576bc8b8d8d6ec6c262, a238ed8a801e48300169afae7d27b5e49a946661ed91fab4f792e99243fbc28d,

TYPE	VALUE
SHA256	d338dc9a75a14753f57399815b5d996a1c5e65aa4eb203222d8c85fb3d74b02f, 56670f51f94080f1ae45f2a433767f210f290835bf582e1a2e1876f1028832de, f67e2a27f0d1a4667b065ab05f884ff881eb7627e9d458f97f2204647b339c6e, 25d226d5cb0c74ed5b1b85f12d53a4c2de2147ff464b2a35db03987015b11e24, c2a7970216576a6b8f74528ffcfa51aa2b72b7f3e4237d97715b1b5ba80b25ca, 8cec3c106659709017bb253becf68296c7bf13e76fa92b4450c281003d225645, ea90c72e67f1c9a9231732119576a7dcb29471f7da428866187d4326e78097f2, ff83f53a383ba3f1d6b002006adf16a7f0b3263185d56cb70104889874d67c5d, cc37a01d3351b3c166f04aec6f52849e909b0b9c8d55095d730c660691b1ba66
Domains	accapple[.]ru, adschecks[.]ru, adsmobi[.]ru, adsmorein[.]in, adsmoreme[.]in, amdcdn[.]ru, amzndev[.]in, amzndev[.]ru, amznprod[.]in, applecdn[.]ru, appledisk[.]ru, appledns[.]ru, applehosts[.]ru, appletime[.]in, bulksec[.]ru, cdnamz[.]in, cdnamz[.]ru, cdnapple[.]in, cdnatapple[.]ru, cdnroute[.]ru, checkcdn[.]ru,

TYPE	VALUE
Domains	chromeads[.]ru, cnmag[.]ru, devnetaps[.]ru, dnsapple[.]ru, dnsrelays[.]ru, explorecdn[.]ru, fiddlejoy[.]ru, figmacat[.]ru, figmanets[.]in, funchats[.]ru, gironetcdn[.]ru, goalmate[.]ru, googlenets[.]ru, greencn[.]ru, icloudsnet[.]ru, imails[.]ru, legalads[.]in, littleads[.]in, littledns[.]ru, maganet[.]ru, mindelgate[.]ru, netapsdev[.]ru, netcdnads[.]in, netcdnamz[.]ru, netcdndev[.]in, netcorps[.]ru, netsprot[.]in, netsproto[.]in, networkads[.]in, rigacdn[.]in, rigmajoys[.]in, rigmanet[.]ru, rigmanets[.]in, sahusuzuki[.]in, stuffdns[.]in, testjoys[.]ru, timewebnet[.]in, vigmanet[.]ru, whitead[.]in, whiteads[.]ru,

TYPE	VALUE
Domains	wincdn[.]ru, windsecure[.]ru, bulknames[.]ru, castlenet[.]ru, chaoping[.]ru, devapple[.]ru, gigacells[.]ru, gizmodoc[.]ru, trixmate[.]ru, itoyads[.]ru, rigglejoy[.]ru, rutornet[.]ru, sigmate[.]ru, vivatads[.]ru, figmasol[.]ru, adobestats[.]com, flixprice[.]com
URLs	hxxps[:]//amzndev[.]in/d/zw_sfp64, hxxps[:]//amzndev[.]ru/d/zw_sfp64, hxxps[:]//googlenets[.]ru/d/zw_sfp64, hxxps[:]//netcdndev[.]in/d/zw_sfp64, hxxps[:]//whitead[.]in/d/zw_sfp64, hxxps[:]//whiteads[.]ru/d/zw_sfp64, hxxps[:]//bulknames[.]ru/a
IPv4	91[.]108[.]106[.]229, 95[.]142[.]35[.]34, 95[.]142[.]35[.]206, 95[.]142[.]37[.]159, 151[.]243[.]109[.]188, 178[.]208[.]92[.]129, 178[.]208[.]92[.]168, 46[.]101[.]126[.]33
Filename	main.scpt, xcassets, Assets.xcassets, Pods, Pods_shad, project.xworkspace,

TYPE	VALUE
Filename	build.sh, speedd, firefoxd, operad, yandexd, edged, braved, agentd, agentdkill, agentdlog, dskwalp, chkdsk, zw_sfp64, chrome_remote, looz, safari.zip, run-safari-dev.py, Safari131Mojave.pkg, Safari1304Mojave.pkg, 7za, dockutil, base_tr_file.txt, base_tr_map.txt, InfoPlist.locatable
File Path	/tmp/r, /tmp/p.app, /tmp/b, /tmp/l.app, /tmp/.n, /tmp/.f, /tmp/.i, /tmp/.e, /tmp/out.txt, ~/.tr, ~/.tr_map, ~/.a, ~/.zshrc, ~/.zshrc_aliases, ~/Library/Caches/GameKit/,

TYPE	VALUE
File Path	~/Library/Caches/com.apple.finder, ~/Library/Frameworks.app, ~/Library/CoreFramework, ~/Library/LaunchAgents/com.apple.core.launchd.plist, ~/Library/LaunchAgents/com.apple.core.accountsd.plist, ~/Library/Cookies/Cookies.binarycookies, /Library/Application Support/com.apple.frameworks, /Applications/SimulatorTrampoline.app, /Applications/Reminders.app, /Applications/Reminders.app/Notes/, /Applications/Terminal.app, /Applications/Finder.app, /Applications/Safari.app/Contents/MacOS/SafariForWebKitDevelopment
SSL Certificate Thumbprint	6e480d648fa1b70612f5d198a66875e28847547d

References

https://unit42.paloaltonetworks.com/xcsset-v40-malware-analysis/

https://www.jamf.com/blog/osx-xcsset-subverts-developer-environments/

https://documents.trendmicro.com/assets/pdf/XCSSET_Technical_Brief.pdf

https://attack.mitre.org/software/S0658/

https://www.microsoft.com/en-us/security/blog/2025/03/11/new-xcsset-malware-adds-new-obfuscation-persistence-techniques-to-infect-xcode-projects/

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

August 06, 2026 • 07:30 AM

More at www.hivepro.com