INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:42 UTC

SnappyClient C2 Implant Combines Credential Theft and Crypto Wallet Targeting in Multi-Stage Attack Chain

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0077
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Cryptocurrency wallets (specific vendors not identified in source material); organizations with employee crypto asset exposure; financial infrastructure
Published	2026-03-21

Executive Summary

SnappyClient is a newly identified C2 implant that combines persistent remote access, credential theft, and cryptocurrency wallet targeting into a single attack chain, posing elevated financial risk to organizations where employees hold or manage crypto assets on company systems. Unlike commodity stealers, this toolset integrates multiple capability classes. Attribution remains unconfirmed; the full scope of targeting, initial access vector, and affected wallet vendors have not been publicly disclosed as of the reporting date. [Note: Sourced from T3 reporting only; no primary or secondary authority confirmation is available. Treat campaign details as preliminary.]

Technical Analysis

SnappyClient is a multi-stage C2 implant with three integrated capability classes: persistent remote access, credential harvesting, and cryptocurrency wallet data theft. Relevant weaknesses include CWE-522 (insufficiently protected credentials), CWE-312 (cleartext storage of sensitive information), and CWE-200 (exposure of sensitive information). MITRE ATT&CK technique coverage spans input capture and credential access (T1056, T1555, T1552, T1539), persistence mechanisms (T1053, T1547, T1543), C2 communication (T1071), local data collection (T1005), and exfiltration (T1041). Valid account abuse (T1078) is also mapped, suggesting possible credential reuse after harvest. [Note: No CVE identifier applies; SnappyClient is malware, not a discoverable software vulnerability. Defensive posture centers on detection and containment, not patching.] Initial access vector, specific wallet vendor targeting, and full technical indicators have not been publicly disclosed in available source material. Source reporting originates from Dark Reading (T3); no primary

or secondary authority sources (NIST, CISA, MITRE, official vendor threat intelligence) have confirmed additional technical detail. Treat all specifics as preliminary pending corroboration.

Action Checklist

1. Step 1 (Immediate): Audit endpoints with access to cryptocurrency wallets or financial platforms, prioritize systems where employees manage crypto assets. Restrict wallet application access to approved, inventoried devices only.
2. Step 2 (Detection): Hunt for MITRE T1071 indicators, anomalous outbound C2 traffic patterns, especially encrypted or protocol-misuse traffic on non-standard ports. Cross-reference with T1547/T1543 persistence artifacts: new scheduled tasks, services, or autorun registry entries created in the past 30 days.
3. Step 3 (Detection): Review credential store access logs for T1555/T1552 activity, unexpected reads of browser credential stores, OS credential managers, or application config files containing stored secrets. Flag any processes accessing wallet-related file paths or browser extension storage.
4. Step 4 (Assessment): Inventory all systems and user accounts with access to cryptocurrency wallets, exchange accounts, or financial platforms. Assess exposure if credentials harvested from those systems were exfiltrated. Rotate credentials for any account with crypto asset access as a precautionary measure.
5. Step 5 (Communication): Notify relevant stakeholders, finance, treasury, and any teams managing organizational crypto assets, of elevated risk. Brief on behavioral indicators to watch for. No patch action is available; defense posture centers on detection and access restriction.
6. Step 6 (Long-term): Review policy on employee crypto wallet use on corporate endpoints. Consider endpoint controls blocking or sandboxing wallet applications. Update detection rules to cover T1056, T1071, T1543, T1547, T1555, and T1552 based on EDR and SIEM capabilities. Baseline all behavioral rules against normal credential access and persistence activity in your environment before deploying. Monitor for IOC disclosure from Dark Reading or corroborating sources.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or law enforcement if: (1) forensic evidence confirms data exfiltration to external C2 server, (2) cryptocurrency exchange account credentials were confirmed accessed/modified, (3) unauthorized fund transfers are detected, or (4) organization has regulatory obligations (SOX, PCI-DSS) requiring formal incident disclosure.
Recovery Notes	Post-eradication: verify all SnappyClient-related processes are terminated and persistence mechanisms (scheduled tasks, services, registry autorun entries) are removed via Process Explorer, Services MMC, and Task Scheduler verification. Rebuild or fully patch affected endpoints if forensic analysis confirms execution of implant. Re-baseline all credential stores (password managers, browser secrets, API keys) and confirm exchange account activity logs show no unauthorized logins post-recovery. Resume normal monitoring and update detection rules with confirmed IOCs; continue elevated monitoring for 90 days post-incident.

Forensic Artifacts	Windows Event Log 4688 (Process Creation) — 90-day window, command-line arguments, parent process hierarchy | Windows Event Log 4663 (Object Access) — file system access to credential stores and wallet application directories | Windows Registry (SYSTEM, SOFTWARE, NTUSER.dat, USRCLASS.dat hives) — persistence mechanisms, scheduled task definitions, browser extension storage | Browser credential databases (SQLite: Login Data in Chrome, logins.json in Firefox) — access timestamps and stored secrets metadata | Scheduled Tasks and Services registry (HKLM\System\CurrentControlSet\Services, HKCU\Software\Microsoft\Windows NT\CurrentVersion\Schedule) — creation dates and binary paths | Firewall logs (C:\Windows\System32\LogFiles\Firewall\pfirewall.log) — outbound HTTPS/encrypted traffic to non-standard ports and unusual destinations | MFT ($Mft) and USN Journal ($UsnJrnl) — file modification timelines for persistence and data exfiltration activity | Network traffic captures (pcap via netsh trace or Wireshark) — C2 communication patterns, encryption methods, and destination IPs/domains | Memory dump (if available) — injected code, C2 beacon configuration, decrypted credentials in process memory

Per-Action IR Details

Step 1 (Immediate): Audit endpoints with access to cryptocurrency wallets or financial platforms — prioritize systems where employees manage crypto assets. Restrict wallet application access to approved, inventoried devices only.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools, processes, and capabilities)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 CM-2 (Baseline Configuration), CIS 6.1 (Establish and Maintain a Data Inventory)

Compensating: Use Windows built-in (Get-WmiObject Win32_UserProfile + registry query HKCU\Software), PowerShell query (Get-Process | Where-Object {$_.ProcessName -match 'wallet|crypto|exchange'}) to enumerate endpoints with crypto-related applications. Cross-reference against Active Directory user group membership via dsquery or csvde export. Document results in Excel pivot table keyed by device, user, and application hash. For wallet binary inventory, use MD5 hashing via certutil -hashfile on all suspected binaries and maintain in a baseline CSV.

Evidence: Before restricting access: capture baseline of all processes with 'wallet,' 'crypto,' 'exchange,' or 'ledger' in name (process name, PID, command-line arguments, parent process, user context, file hash). Extract this from Get-Process output, Windows Event Log 4688 (Process Creation) for past 90 days filtered by command-line keywords, and browser extension inventory (HKCU\Software\Google\Chrome\Extensions or equivalent for all browsers). Export MFT ($Mft) snapshot to preserve file access timestamps for wallet application directories.

Step 2 (Detection): Hunt for MITRE T1071 indicators — anomalous outbound C2 traffic patterns, especially encrypted or protocol-misuse traffic on non-standard ports. Cross-reference with T1547/T1543 persistence artifacts: new scheduled tasks, services, or autorun registry entries created in the past 30 days.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis phase: identify indicators and confirm incident)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-12 (Audit Generation), CIS 8.1 (Establish and Maintain Detailed Asset Inventory), CIS 13.1 (Establish and Maintain Network Segmentation)

Compensating: Without EDR/SIEM: query Windows Event Log 4688 (Process Creation) for past 30 days, filter on outbound DNS queries (Windows Event Log 4104 for PowerShell if available, or use netsh int ipv4 show tcpstats). Hunt scheduled tasks via schtasks /query /tn * /v /fo list > tasks.txt; cross-reference creation dates with Get-ScheduledTask -TaskPath '\' | Get-ScheduledTaskInfo | Where-Object {$_.LastTaskResult -ne 267}. Query registry for persistence: query HKLM\Software\Microsoft\Windows\CurrentVersion\Run*, HKCU\Software\Microsoft\Windows\CurrentVersion\Run*, and HKLM\System\CurrentControlSet\Services for items created in past 30 days (reg query key /s > baseline.txt, then timestamp via dir /tw). Monitor netstat output (netstat -anob -f) and DNS cache (ipconfig /displaydns) for unusual external IPs/domains. Use DNSViz or DNS audit logs if

available.

Evidence: Before hunting: preserve Windows Event Logs 4688, 4689, 4697 (New Service Installation), 4699 (Scheduled Task Deleted), 4700 (Scheduled Task Disabled), 4701 (Scheduled Task Updated), 4702 (Scheduled Task Imported). Export registry hives (SYSTEM, SOFTWARE, NTUSER.dat, USRCLASS.dat) from all affected user profiles. Capture full netstat -anob output with timestamps. If Firewall Logs are available (C:\Windows\System32\LogFiles\Firewall), export last 30 days. Preserve MFT ($Mft) and USN Journal ($UsnJrnl) to identify file creation ordering. Screenshot/export full Scheduled Tasks MMC tree for comparison.

Step 3 (Detection): Review credential store access logs for T1555/T1552 activity — unexpected reads of browser credential stores, OS credential managers, or application config files containing stored secrets. Flag any processes accessing wallet-related file paths or browser extension storage.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.5 (Indicators of Compromise and scope determination)

Controls: NIST 800-53 IA-5 (Authentication), NIST 800-53 SC-7 (Boundary Protection), CIS 5.3 (Restrict Access to Credential Stores)

Compensating: Without EDR: enable Windows Event Log Auditing for file system access (Group Policy: Audit Object Access, then apply to wallet directory paths). Query Event Log 4663 (File Object Accessed) filtered to wallet directories (chrome\User Data\Default\Login Data, Firefox profile folders, Roaming\Ledger, etc.). Examine NTFS file access logs using autoruns, process monitor (live capture on suspected endpoints), or icacls /audit /c. Query browser extension storage: examine HKCU\Software\Google\Chrome\Extensions and HKCU\AppData\Roaming\Mozilla\Firefox for suspicious extension GUIDs. Use strings/grep on browser credential database files (SQLite databases in Chrome/Firefox profiles) to identify recent access timestamps via sqlite3 tool: sqlite3 'Login Data' 'select * from logins;'. Monitor Windows Credential Manager via cmdkey /list and extract stored credentials metadata.

Evidence: Before querying credentials: preserve exact file paths and timestamps of browser credential stores (SQLite databases in Chrome, Firefox, Edge profile directories). Capture Windows Event Log 4663 (Object Access) for 30 days filtered to wallet/crypto-related directory paths. Export registry hives containing stored credentials: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU, HKCU\Software\RealVNC\vncviewer4 (if VNC detected), and Credential Manager keys. Use NTFS journal ($UsnJrnl) to identify which processes accessed credential database files and when. Preserve memory dump from affected process if available (use Volatility or WinDbg). Screenshot browser extension list and installed extensions directory contents. Preserve $MFT entries for wallet application config directories.

Step 4 (Assessment): Inventory all systems and user accounts with access to cryptocurrency wallets, exchange accounts, or financial platforms. Assess exposure if credentials harvested from those systems were exfiltrated. Rotate credentials for any account with crypto asset access as a precautionary measure.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment, Eradication, and Recovery: credential rotation and access control updates)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-4 (Identifier Management), NIST 800-53 IA-5 (Authentication), CIS 5.2 (Use Multi-Factor Authentication for All Administrative Access)

Compensating: Inventory via Active Directory export (Get-ADUser -Filter * -Properties * | Export-Csv users.csv) cross-referenced with file access logs to wallet directories. Use group membership queries (dsquery group -name '*crypto*' -o dn | dsquery group -exec dsget group -members) to identify finance/treasury groups. Query DHCP logs and ARP tables to map user accounts to endpoints (arp -a, nbtstat -a). Document credentials: extract password policy settings via net accounts /domain, check password age (net user username /domain), and force rotation via net user username /logonpasswordexpirynotification. Enable MFA via AD/Azure AD Set-MsolUser -UserPrincipalName user@org.com -StrongAuthenticationRequirements. Document rotation in change log with timestamp and authorizer.

Evidence: Before credential rotation: preserve hashed passwords from Security Accounts Manager (SAM registry hive) and NTDS.dit (Active Directory database) for forensic comparison post-rotation. Capture screenshots of stored credentials in password managers (if accessible). Export list of systems accessing credential stores in past 30 days via Windows Event Log 4688 filtered by processes accessing HKCU\Software\Microsoft\Windows Credential Manager.

Preserve MFA enrollment status pre-rotation (screenshot Azure AD MFA settings). Document baseline privileged account access logs (Event Log 4648 — Logon with Explicit Credentials) for comparison.

Step 5 (Communication): Notify relevant stakeholders — finance, treasury, and any teams managing organizational crypto assets — of elevated risk. Brief on behavioral indicators to watch for. No patch action is available; defense posture centers on detection and access restriction.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Notification: determining what to communicate and to whom)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 SI-5 (Security Alerts, Advisories, and Directives)

Compensating: Create a one-page incident brief template: Threat Name (SnappyClient), Date Discovered, Affected Systems (specific count + user names), IOCs (file hashes, domains, IPs if known), Detection Indicators (unusual task creation, outbound HTTPS on non-standard ports, browser credential access), Recommended Actions (restrict wallet app access, enable MFA on exchange accounts, monitor process execution logs). Distribute via email with read receipt enabled. Schedule follow-up briefing for finance/treasury teams covering: watch for unexpected system logins (monitor logon type 3 via Event Log 4624), processes with 'wallet' or 'ledger' in name run by non-IT users, and unusual outbound traffic during non-business hours. Provide weekly summary of detection rule hits.

Evidence: Before communication: preserve incident timeline document with discovery date, initial indicators observed, and scope of affected systems. Capture screenshots of detection data (anomalous processes, network connections, registry changes) for briefing materials. Document which stakeholders were notified, on what date, and receipt confirmation. Preserve communication logs (email, meeting notes) as part of post-incident review.

Step 6 (Long-term): Review policy on employee crypto wallet use on corporate endpoints. Consider endpoint controls blocking or sandboxing wallet applications. Update detection rules to cover T1056, T1071, T1541, T1543, and T1555 based on EDR and SIEM capabilities. Monitor for updated IOC disclosure from the original source.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities: lessons learned and process improvement)

Controls: NIST 800-53 CA-2 (Security Assessments), NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CM-3 (Configuration Change Control), CIS 6.2 (Ensure Authorized Software is Currently Installed)

Compensating: Without EDR/SIEM: create AppLocker rules (New-AppLockerPolicy -Xml (New-AppLockerPolicy -RuleType Publisher,Path,Hash) -Outfile policy.xml) or Windows Defender Application Guard policies blocking wallet executables by hash or publisher. Build detection rules using Windows Event Log 4688 process creation auditing: search for processes matching regex wallet|ledger|coinbase|kraken|binance|metamask with parent process NOT explorer.exe or chrome.exe. Create scheduled task to query monthly: Get-WmiObject Win32_Process | Where-Object {$_.CommandLine -match 'wallet'} and export results. Set up DNS sinkhole/proxy rule blocking known wallet application update domains (if available from threat intel sources). Maintain IOC tracking spreadsheet keyed by hash/domain/IP with source, date discovered, and detection rule ID. Subscribe to threat intel feeds (CISA, NVD, vendor advisories) and create monthly review task.

Evidence: Before implementing controls: preserve baseline of currently-allowed wallet applications (approved list with file hash, path, publisher signature). Export current Group Policy Objects (gpresult /h report.html, copy C:\Windows\System32\GroupPolicy\Adm\ files). Capture before/after screenshots of AppLocker policy editor. Log initial process creation events for 7 days pre-implementation to establish baseline of legitimate crypto-related activity. Preserve list of all users who legitimately use wallet applications (needed to refine detection rules to avoid false positives).

Detection Guidance

No confirmed IOCs have been publicly released for SnappyClient as of the reporting date. Detection must rely on behavioral indicators aligned to the mapped ATT&CK techniques. Focus on the following: (1) Persistence,

new scheduled tasks (T1053), new or modified services (T1543), or autorun registry keys (T1547) created by non-standard parent processes; (2) Credential access, process access to browser credential databases (Login Data, key4.db), Windows Credential Manager, or application config files containing tokens or keys (T1555, T1552); (3) Input capture, unexpected keyboard hook registrations or screenshot capture activity (T1056); (4) C2 communication, outbound connections from non-browser processes to uncommon external destinations, particularly over HTTP/HTTPS or other standard-protocol tunneling (T1071); (5) Data exfiltration, large or frequent outbound transfers from endpoints with wallet software installed (T1041); (6) Session hijacking, access to browser session cookie storage (T1539). SIEM query focus: process creation events with unusual parent-child chains, file access events targeting credential store paths, and network connections from processes that do not typically initiate outbound traffic. EDR behavioral rules covering credential store reads and persistence mechanism creation are the highest-yield starting point given current information gaps. Baseline all behavioral rules against normal credential access and persistence activity in your environment before deploying. False-positive tuning is critical given the lack of malware-specific IOCs. Monitor Dark Reading and threat intelligence feeds for IOC disclosure updates as this campaign matures.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`not disclosed`	No IOCs have been publicly released for SnappyClient as of the reporting date. This field will be updated if indicators are published by the original source or corroborating authorities.	LOW

Framework Mappings

MITRE-ATTACK

- **T1056** — Input Capture
- **T1555** — Credentials from Password Stores
- **T1053** — Scheduled Task/Job
- **T1071** — Application Layer Protocol
- **T1547** — Boot or Logon Autostart Execution
- **T1005** — Data from Local System
- **T1041** — Exfiltration Over C2 Channel
- **T1543** — Create or Modify System Process
- **T1078** — Valid Accounts
- **T1539** — Steal Web Session Cookie
- **T1552** — Unsecured Credentials

NIST-800-53R5

- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **SI-3** — Malicious Code Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **5.2**
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1056	Input Capture	Collection
T1555	Credentials from Password Stores	Credential-Access
T1053	Scheduled Task/Job	Execution
T1071	Application Layer Protocol	Command-And-Control
T1547	Boot or Logon Autostart Execution	Persistence

Technique ID	Technique Name	Tactic
T1005	Data from Local System	Collection
T1041	Exfiltration Over C2 Channel	Exfiltration
T1543	Create or Modify System Process	Persistence
T1078	Valid Accounts	Defense-Evasion
T1539	Steal Web Session Cookie	Credential-Access
T1552	Unsecured Credentials	Credential-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/new-c2-impla...	T3
A UI Flaw in Top Crypto Wallets We Need to Address - Coinspect	https://www.coinspect.com/blog/wallet-eip-712-injection-vulnerability/	T3
The Crypto Wallet Vulnerability That Went Undetected for Over Six ...	https://medium.com/@john-s4d/the-crypto-wallet-vulnerability-that-w...	T3
How to fix cryptocurrency wallet vulnerabilities? - Tencent Cloud	https://www.tencentcloud.com/techpedia/124112	T3
Wallet Drainers: How Scams Steal Funds - Darktrace	https://www.darktrace.com/blog/crypto-wallets-continue-to-be-draine...	T3

Generated 2026-03-29 18:42 UTC by TJS Security Command Center