INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:38 UTC

CL-STA-1087: China-Linked Espionage Operation Targets Southeast Asian Military C4I Systems with Custom Malware Since 2020

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0011
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Windows systems (lsass.exe, dllhost.exe); Southeast Asian military organizations; Pastebin and Dropbox abused for dead drop resolver and C2 retrieval
Published	2026-03-13

Executive Summary

A suspected Chinese state-sponsored threat cluster, CL-STA-1087, has conducted targeted espionage operations against Southeast Asian military organizations since at least 2020, focusing on C4I systems and intelligence related to joint Western military collaboration. The actor deploys custom backdoors and a modified credential-harvesting tool while abusing legitimate cloud services (Pastebin, Dropbox) to evade network-level detection. Organizations supporting or allied with affected military partners face secondary exposure risk; the primary business impact is unauthorized access to sensitive strategic and operational military intelligence.

Technical Analysis

CL-STA-1087 deploys two custom backdoors, AppleChris and MemFun, alongside a modified Mimikatz variant targeting LSASS memory (T1003.001) for credential extraction. Initial access likely leverages valid accounts (T1078). Persistence is established via boot/logon autostart mechanisms (T1547). The actor uses process hollowing into legitimate Windows processes lsass.exe and dllhost.exe (T1055.012, Process Hollowing) to evade endpoint detection. DLL search order hijacking (T1574.001) supports payload delivery. Payloads are delivered modularly via ingress tool transfer (T1105). C2 communication uses web services (T1102) with Dropbox abused for command retrieval (T1102.001, Dead Drop Resolver) and Pastebin used for staging resolver data (T1583.006). The actor employs PowerShell (T1059.001), masquerading of process names (T1036.005), timestomping (T1070.006), indicator removal targeting security tools (T1562.001), file and directory discovery (T1083), and proxy-based C2 routing (T1090). Relevant weaknesses include CWE-494

(Download of Code Without Integrity Check) and CWE-426 (Untrusted Search Path), consistent with the DLL hijacking and modular payload delivery chain. No CVE identifiers are associated with this campaign; exploitation relies on tradecraft and abuse of legitimate tools rather than unpatched software vulnerabilities. Primary technical detail derives from Unit 42 research (Palo Alto Networks).

Action Checklist

1. Step 1, Immediate: Block outbound connections to Pastebin and Dropbox at the perimeter firewall and proxy for all systems in sensitive network segments, or restrict to explicitly authorized business use cases only.
2. Step 2, Detection: Hunt for process hollowing indicators, audit processes where lsass.exe or dllhost.exe have unusual parent processes, unexpected network connections, or anomalous memory regions using EDR telemetry; also search for LSASS memory access events from non-system processes.
3. Step 3, Detection: Review PowerShell execution logs (Script Block Logging, Module Logging) for encoded commands, unusual download cradles, or references to cloud storage APIs (Dropbox, Pastebin endpoints).
4. Step 4, Assessment: Inventory Windows endpoints in environments with any connection to Southeast Asian government, defense, or military partners; prioritize those with access to C4I, joint exercise planning, or Western military collaboration data.
5. Step 5, Assessment: Audit DLL load paths for critical executables to identify DLL search order hijacking opportunities (T1574.001); validate integrity of DLLs loaded by high-value processes against known-good baselines.
6. Step 6, Communication: If your organization supports or is partnered with affected regional military entities, notify your security leadership and relevant intelligence-sharing partners (ISAC, CISA liaison if applicable) of potential secondary targeting risk.
7. Step 7, Long-term: Implement application allowlisting on sensitive systems to block unauthorized payload execution; enforce Credential Guard on Windows endpoints to protect LSASS memory from direct access; review and harden cloud service egress policies using a zero-trust outbound traffic model aligned to NIST SP 800-207.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and military liaison if any evidence of breach, data exfiltration, or successful lsass.exe compromise detected; engage external DFIR firm if forensic scope exceeds internal team capacity or if systems are classified/sensitive.
Recovery Notes	Post-eradication: (1) Re-image all confirmed-compromised systems from clean, verified media; validate restoration against golden baselines. (2) Reset all credentials with administrative access to affected systems and data repositories; force password change for all users in sensitive network segments. (3) Conduct 30-day enhanced monitoring (daily log review, weekly endpoint EDR summary) to detect post-remediation reinfection; maintain incident-related YARA rules and IOCs in detection tooling for 90 days minimum.

Forensic Artifacts	Windows Event Log Security (4688 Process Creation, 4656/4663 Handle Audit, 10 Sysmon ProcessAccess, 3 Sysmon Network Connection) | PowerShell Operational/Analytic logs (Event ID 4104 Script Block Logging, 4103 Module Logging, 600 Engine State) | LSASS.exe memory dump and full-disk forensic image of affected systems; registry hives (HKEY_LOCAL_MACHINE\Software, HKEY_CURRENT_USER\Software, Amcache.hve, ShimCache) | Firewall/proxy egress logs with timestamps, source IP, destination, port, and user context; DNS query logs (Event ID 3008 Windows DNS, full DNS packet capture if available) | Dropbox/Pastebin account access logs (if accessible via law enforcement; ISP-level traffic captures showing C2 communication patterns and timing); file system artifacts (MFT, $J journal, thumbnail cache, prefetch files, recent files)

Per-Action IR Details

Step 1, Immediate: Block outbound connections to Pastebin and Dropbox at the perimeter firewall and proxy for all systems in sensitive network segments, or restrict to explicitly authorized business use cases only.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3

Controls: NIST 800-53 AC-4 (Information Flow Enforcement), NIST 800-53 SC-7 (Boundary Protection), CIS 6.6 (Deny or Restrict Unnecessary Inbound/Outbound Network Traffic)

Compensating: If proxy unavailable, use Windows Firewall Group Policy to block outbound HTTPS on port 443 to Pastebin (104.21.26.0/24) and Dropbox (162.125.0.0/16) IPs via firewall rules; validate with: netsh advfirewall firewall add rule name='Block-Pastebin' dir=out action=block remoteip=104.21.26.0/24 protocol=tcp remoteport=443. Monitor with: netstat -anob every 60 seconds on critical systems.

Evidence: Capture firewall/proxy logs 7 days pre-block to establish baseline of legitimate Pastebin/Dropbox usage; export Windows Firewall blocked connection logs (Event ID 5157) to identify which processes attempted blocked destinations after rule deployment; preserve DNS query logs (Event ID 3008 on Windows DNS servers) showing resolver timestamps.

Step 2, Detection: Hunt for process hollowing indicators, audit processes where lsass.exe or dllhost.exe have unusual parent processes, unexpected network connections, or anomalous memory regions using EDR telemetry; also search for LSASS memory access events from non-system processes.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-12 (Audit Generation), CIS 8.4 (Protect Memory from Unauthorized Access)

Compensating: Without EDR: (1) Enable Windows Event Log Auditing: auditpol /set /subcategory:'Process Termination' /success:enable and auditpol /set /subcategory:'SAM' /success:enable. (2) Query Event ID 4688 (Process Creation) and Event ID 10 (ProcessAccess via Sysmon) for lsass.exe parent != wininit.exe, services.exe, winlogon.exe. (3) Use Volatility 3 (free): vol -f memory.dmp windows.handles | grep -E 'lsass|dllhost' to detect unexpected handle references. (4) Monitor for 4656 events (Handle Audit) with ObjectName=*lsass* and AccessReason != SYNCHRONIZE.

Evidence: Capture memory dump of lsass.exe before any remediation (procdump -accepteula -ma lsass.exe lsass.dmp); preserve Windows Event Log security.evtx, Sysmon operational log (Event ID 10, 3, 8); record running processes with their parents (Get-Process | Select-Object -Property Name, Id, @{Name='ParentProcessId'; Expression={(Get-Process -Id $_.Id).Parent.Id}} > baseline.txt); snapshot LSASS DLL import table (dumpbin /imports C:\Windows\System32\lsass.exe).

Step 3, Detection: Review PowerShell execution logs (Script Block Logging, Module Logging) for encoded commands, unusual download cradles, or references to cloud storage APIs (Dropbox, Pastebin endpoints).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-2 (Audit Events), CIS 8.4 (Command and Scripting Interpreter Logging)

Compensating: Enable GPO: Set-GPO 'PowerShell Logging' with: Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell > Turn on PowerShell Script Block Logging = Enabled. Query Event ID 4104 (Script Block Logging) from Microsoft-Windows-PowerShell/Operational log: Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-PowerShell/Operational'; ID=4104} | Where-Object {$_.Message -match 'pastebin|dropbox|WebClient|DownloadString|Invoke-WebRequest'} | Select-Object TimeCreated, Message. Check for Base64 encoding: decode base64 strings found and inspect for APIs like DropboxAPI, WebClient, HttpClient.

Evidence: Export Microsoft-Windows-PowerShell/Operational event log (Event ID 4104, 4103, 600); capture command history from %APPDATA%\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt on all user profiles; preserve HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging registry hive; snapshot Get-History output if session is still active; log all ShellHistoryCount entries in user registry hives.

Step 4, Assessment: Inventory Windows endpoints in environments with any connection to Southeast Asian government, defense, or military partners; prioritize those with access to C4I, joint exercise planning, or Western military collaboration data.

NIST Phase: Preparation

Reference: NIST 800-61r3 §3.1 (Preparation Phase)

Controls: NIST 800-53 CM-2 (Baseline Configuration), NIST 800-53 IA-4 (Identifier Management), CIS 1.1 (Establish and Maintain Detailed Asset Inventory)

Compensating: Without CMDB: (1) Query Active Directory for relevant OUs: Get-ADComputer -SearchBase 'OU=Military,OU=Defense' -Filter * | Select-Object Name, IPv4Address, OperatingSystem > inventory.csv. (2) Cross-reference IP geolocation and subnet ownership logs (check DHCP scope assignments). (3) Interview network/data owners to identify systems storing: *C4I*, *exercise*, *joint operation*, *coalition*, *ITAR*, *EAR* data via file share audits (e.g., DIR /S \\server*C4I* for Windows file servers). (4) Check DNS resolution history for military-related internal domains; query DNS logs for 30-day historical record: Get-DnsServerQueryStatistics.

Evidence: Preserve current Active Directory snapshot (ntdsutil snapshot create; then backup database files); capture network device configs (router ACLs, VLAN assignments) showing data segment isolation; log current SMB shares and NTFS permissions (Get-SmbShare | Get-SmbShareAccess); record user group memberships for military/sensitive data access; snapshot firewall rule sets and access control lists protecting sensitive subnets.

Step 5, Assessment: Audit DLL load paths for critical executables to identify DLL search order hijacking opportunities (T1574.001); validate integrity of DLLs loaded by high-value processes against known-good baselines.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2; NIST 800-53 SI-7 (Software, Firmware, and Information Integrity)

Controls: NIST 800-53 SI-7 (Software, Firmware, and Information Integrity), NIST 800-53 CM-5 (Access Restrictions for Change), CIS 2.6 (Ensure Minimal Legitimate DLL Prefetching Occurs)

Compensating: Use free Sigcheck (Sysinternals): sigcheck -v C:\Windows\System32\lsass.exe > baseline_lsass.txt to capture DLL load order and hashes. Compare against pristine ISO: mount Windows media and run same command against reference system. Check for unsigned DLLs: Get-Item C:\Windows\System32*.dll | Where-Object {(Get-AuthenticodeSignature $_.FullName).Status -ne 'Valid'} > unsigned_dlls.txt. Monitor DLL load events via Sysmon Event ID 7 (Image Loaded): wevtutil qe Microsoft-Windows-Sysmon/Operational /f:text /rd:true | findstr 'lsass.exe dllhost.exe' | findstr /I 'image loaded'. Validate DLL hash against NIST NSRL or VirusTotal.

Evidence: Capture baseline DLL load order pre-and post-patch (Sigcheck snapshots); preserve Windows Event Log Sysmon operational log with Image Load events (Event ID 7); document current DLL search order via registry (HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs); snapshot NTFS file permissions on System32 and SysWOW64 directories; preserve file timestamps (Get-Item -Force C:\Windows\System32*.dll |

Select-Object Name, LastWriteTime, Length > dll_inventory.txt).

Step 6, Communication: If your organization supports or is partnered with affected regional military entities, notify your security leadership and relevant intelligence-sharing partners (ISAC, CISA liaison if applicable) of potential secondary targeting risk.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.2.6 (Post-Incident Activity — Sharing Information)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 IR-4 (Incident Handling), CIS 19.1 (Establish and Maintain a Formal Incident Response Process)

Compensating: Document findings in incident report following template: [Affected Org Name] | Exposure Window | Indicators Observed | Mitigation Taken | Date Notified | Contact (name/email/phone). Send via secure channels (CISA portal, encrypted email, secure phone line if classified). If no formal ISAC membership, contact CISA directly: cisa.gov/report or call CISA 24/7 operations (1-888-282-0870). Maintain notification audit trail with signed receipts.

Evidence: Preserve incident report with IOCs (file hashes, C2 IPs, domains, file paths); capture timeline of detection (initial alert timestamp, confirmation steps, assessment completion); document communication log with timestamps and recipients; preserve any indicators or TTPs shared back by intelligence partners; maintain signed acknowledgment of receipt from leadership and external parties.

Step 7, Long-term: Implement application allowlisting on sensitive systems to block unauthorized payload execution; enforce Credential Guard on Windows endpoints to protect LSASS memory from direct access; review and harden cloud service egress policies using a zero-trust outbound traffic model aligned to NIST SP 800-207.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.2.5 (Recovery); NIST 800-207 (Zero Trust Architecture)

Controls: NIST 800-53 CM-7 (Least Functionality), NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 SC-7 (Boundary Protection), CIS 2.1 (Maintain and Enforce Application Allowlists), CIS 6.6 (Deny or Restrict Unnecessary Inbound/Outbound Network Traffic)

Compensating: (1) Application Allowlisting (free): Windows Defender Application Guard (WDAG) for isolated execution; AppLocker (built-in): Set-AppLockerPolicy -XmlPolicy C:\applock_policy.xml (requires Server 2012 R2+). For legacy systems, use SRP (Software Restriction Policy) via GPO: Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies. (2) Credential Guard (free on Pro/Enterprise): Enable via Registry: reg add HKLM\System\CurrentControlSet\Control\Lsa /v LsaCfgFlags /t REG_DWORD /d 1 or Group Policy: Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security. (3) Zero-Trust Egress: Restrict all outbound to explicit allowlist via Windows Firewall with Advanced Security (WFAS); create GPO rules blocking by destination: netsh advfirewall firewall add rule name='Block-All-Outbound' dir=out action=block, then add exceptions: netsh advfirewall firewall add rule name='Allow-DNS' dir=out action=allow remoteport=53 protocol=tcp.

Evidence: Pre-implementation: baseline current allowed/blocked executables (Get-AppLockerPolicy -Effective > baseline_applocker.xml); capture Credential Guard status (Get-ComputerInfo | Select-Object DeviceGuardUserModeCodeIntegrityPolicyEnforcementStatus); log current egress firewall rules (netsh advfirewall firewall show rule dir=out). Post-implementation: capture AppLocker Event Log (Event ID 8004 — policy applied); monitor Credential Guard events (Event ID 5379 — successful initialization); log firewall rule application timestamp and number of blocked connections (netsh advfirewall firewall show rule dir=out | findstr 'Block').

Detection Guidance

Focus detection efforts on four behavioral clusters. (1) LSASS abuse: Alert on any process other than lsass.exe itself, the Windows Security subsystem, or your approved EDR agent reading LSASS memory (Windows Security Event ID 4656/4663 with object name containing lsass.exe; Sysmon Event ID 10). (2) Process

hollowing in dllhost.exe or lsass.exe: Look for instances where the executable image path does not match the expected on-disk binary, or where network connections originate from these processes to external IPs or cloud service domains. (3) Cloud C2 abuse: Monitor DNS queries and HTTP/S connections to pastebin.com, dropbox.com, and dl.dropboxusercontent.com from endpoints that do not have a documented business need; flag high-frequency or scripted access patterns. Specific pattern: PowerShell or cmd.exe initiating connections to these domains should be treated as high-confidence suspicious activity. (4) DLL hijacking: Use Sysmon Event ID 7 (ImageLoad) with unsigned or unexpected DLL loads in the directories of high-value executables; cross-reference against process creation chains. Behavioral IOC summary: process hollowing into lsass.exe or dllhost.exe; PowerShell downloading from Pastebin or Dropbox URLs; LSASS memory reads from non-system processes; DLL loads from writable user directories; persistence entries in Run keys or scheduled tasks pointing to unusual paths. Note: As of publication of the primary Unit 42 research, no file hashes, IPs, or domains for AppleChris or MemFun were publicly disclosed. Operators should consult the Unit 42 research publication directly for any indicators released subsequently.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`pastebin.com`	Abused as dead drop resolver for C2 configuration retrieval by CL-STA-1087; legitimate service weaponized, not a malicious domain per se, flag anomalous access patterns from endpoints, not the domain itself	MEDIUM
DOMAIN	`dropbox.com`	Abused for C2 command retrieval (T1102.001); monitor for scripted or high-frequency access from non-user-interactive processes	MEDIUM
DOMAIN	`dl.dropboxusercontent.com`	Dropbox content delivery subdomain used in C2 retrieval chain; monitor alongside dropbox.com	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1070.006** — Timestomp
- **T1071.001** — Web Protocols
- **T1078** — Valid Accounts
- **T1055.012** — Process Hollowing
- **T1090** — Proxy
- **T1574.001** — DLL
- **T1547** — Boot or Logon Autostart Execution
- **T1583.006** — Web Services
- **T1102** — Web Service

- **T1059.001** — PowerShell
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1083** — File and Directory Discovery
- **T1003.001** — LSASS Memory
- **T1105** — Ingress Tool Transfer
- **T1102.001** — Dead Drop Resolver
- **T1562.001** — Disable or Modify Tools

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5**
- **2.6**
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1070.006	Timestomp	Defense-Evasion
T1071.001	Web Protocols	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1055.012	Process Hollowing	Defense-Evasion
T1090	Proxy	Command-And-Control
T1574.001	DLL	Persistence
T1547	Boot or Logon Autostart Execution	Persistence
T1583.006	Web Services	Resource-Development
T1102	Web Service	Command-And-Control
T1059.001	PowerShell	Execution
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1003.001	LSASS Memory	Credential-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1102.001	Dead Drop Resolver	Command-And-Control
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/chinese-hackers-target-southeast-...	T3
Behind the Clouds: Attackers Targeting Governments in Southeast ...	https://unit42.paloaltonetworks.com/windows-backdoor-for-novel-c2-c...	T3
Suspected China-Based Espionage Operation Against Military ...	https://www.hendryadrian.com/suspected-china-based-espionage-operat...	T3
LSASS Memory - Red Canary Threat Detection Report	https://redcanary.com/threat-detection-report/techniques/lsass-memory/	T3

Source	URL	Tier
I get a lot of these lately is this a malware or something? all ... - Reddit	https://www.reddit.com/r/antivirus/comments/x6p7yc/i_get_a_lot_of_t...	T3

Generated 2026-03-29 18:38 UTC by TJS Security Command Center