INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-09 18:37 UTC

UAT-10362 Deploys Lua-Based LucidRook Against Taiwanese NGOs Using Tiered, Geofenced Malware Architecture

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0161
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Windows systems; organizations operating in Traditional Chinese (zh-TW) language environments; Taiwanese NGOs and universities; Trend Micro branding abused as lure
Published	2026-04-09T12:23:00
Discovery Source	Rss

Executive Summary

A previously undocumented threat cluster, UAT-10362, has been conducting targeted spear-phishing attacks against Taiwanese NGOs and universities since at least October 2025, deploying a novel Lua-based malware family called LucidRook. The campaign abuses Trend Micro branding as a lure and uses geofencing to restrict payload delivery to Traditional Chinese language environments, limiting collateral exposure and complicating broad detection. Organizations with ties to Taiwan, cross-strait policy sectors, or diaspora communities face elevated risk of targeted intrusion and data exfiltration.

Technical Analysis

UAT-10362 delivers LucidRook via spear-phishing emails (T1566.001) carrying malicious attachments requiring user execution (T1204.002). The malware embeds a Lua 5.4.8 interpreter to execute staged payloads, with initial access established through DLL side-loading (T1574.002), likely abusing a legitimate Trend Micro binary as the host process (T1036.005). Geofencing logic (T1480.001, T1614.001) restricts full payload delivery to systems operating in Traditional Chinese (zh-TW) locale, reducing sandbox detonation fidelity and broad telemetry visibility. Post-execution, LucidRook performs file system reconnaissance (T1083), exfiltrates data over C2 channels (T1041, T1071.003), and retrieves additional payloads (T1105). Obfuscation techniques include command obfuscation (T1027, T1027.010) and scripting via PowerShell (T1059.001) and general interpreter abuse (T1059). No CVE is assigned. Relevant CWEs: CWE-116 (improper encoding/escaping), CWE-506 (embedded malicious code), CWE-829 (inclusion of functionality from untrusted control sphere,

LucidRook stages untrusted Lua payloads from C2 infrastructure). Attribution is unconfirmed; tradecraft and targeting align with China-nexus APT patterns. No patch is applicable, this is a malware campaign, not a software vulnerability.

Action Checklist

1. Step 1: Containment. Identify Windows endpoints in your environment running Traditional Chinese (zh-TW) locale settings or used by staff with Taiwan-facing roles. Isolate any systems showing unexpected DLL loads from Trend Micro-named binaries or Lua interpreter activity. Block outbound C2 traffic using IOCs published by Cisco Talos (blog.talosintelligence.com/new-lua-based-malware-lucidrook/) pending full IOC list retrieval.
2. Step 2: Detection. Query EDR telemetry for DLL side-loading events involving Trend Micro-named executables loading unexpected DLLs. Search process creation logs for Lua interpreter invocations (lua.exe, lua54.dll) outside of known-legitimate software. Review email gateway logs for spear-phishing lures referencing Trend Micro tools or security software delivered to Traditional Chinese-locale users. Check PowerShell logs (Event ID 4104) for obfuscated script execution.
3. Step 3: Eradication. Remove confirmed LucidRook implants identified during forensic review. Re-image affected endpoints where full scope of implant activity cannot be confirmed. Revoke and reissue credentials for any accounts accessed from compromised hosts. Remove malicious DLLs identified through side-loading analysis and restore legitimate application binaries from verified sources.
4. Step 4: Recovery. Validate remediated endpoints against a known-good baseline before returning to production. Monitor for re-infection attempts via email gateway alerts targeting the same user population. Confirm no persistence mechanisms (scheduled tasks, registry run keys, modified startup items) remain on remediated systems. Maintain elevated logging on zh-TW locale endpoints for 30 days post-remediation.
5. Step 5: Post-Incident. Conduct a gap assessment on DLL side-loading prevention controls, evaluate application whitelisting or WDAC policies to restrict unsigned DLL loads. Review spear-phishing resilience: test user awareness for lures mimicking trusted security vendors. Assess whether existing sandbox tooling enforces locale normalization to detect geofenced malware samples. Map detection coverage against T1574.002, T1480.001, and T1614.001 in your SIEM or XDR platform.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if forensic evidence confirms data exfiltration from NGO policy, research, or donor databases; if LucidRook C2 beaconing is confirmed on more than two endpoints indicating lateral movement beyond initial compromise; or if the affected organization is subject to Taiwan PDPA or cross-jurisdictional data protection obligations triggered by confirmed PII exposure.

Recovery Notes	Before returning any zh-TW locale endpoint to production, validate DLL integrity across the full Trend Micro installation directory using Sigcheck against vendor-published hashes and confirm no unsigned DLLs remain. Maintain enhanced Sysmon logging (Event IDs 1, 3, 7, 11, 13) on all previously targeted endpoints and the broader zh-TW user population for a minimum of 30 days, as UAT-10362's geofenced architecture suggests the campaign is deliberate and ongoing, making re-targeting of the same organizations likely. Coordinate with Cisco Talos and share any novel IOCs or Lua bytecode variants discovered during forensics to support industry-wide detection improvements for this previously undocumented malware family.
Forensic Artifacts	Malicious DLL in Trend Micro application directory: Collect the side-loaded DLL from the Trend Micro executable's working directory or a user-writable path it searches before the legitimate system path — hash (SHA-256), PE compile timestamp, and import table will differentiate the LucidRook loader from legitimate vendor DLLs. | Lua bytecode or script files on disk: LucidRook's Lua-based payload may persist as .lua or .luac files in %APPDATA%, %TEMP%, or a subdirectory of the Trend Micro install path — the Lua 5.4 bytecode magic header (0x1B 0x4C 0x75 0x61 0x54) in binary files outside known Lua application paths is a definitive indicator. | Sysmon Event ID 7 (ImageLoaded) logs: Records showing a Trend Micro-signed parent process loading a DLL from a non-standard, user-writable path with no valid Authenticode signature — the combination of signed parent and unsigned child DLL is the forensic fingerprint of this side-loading technique (T1574.002). | Windows locale API call artifacts in memory: A full memory dump of the compromised Trend Micro host process processed through Volatility may reveal in-memory evidence of GetUserDefaultUILanguage or GetSystemDefaultLCID API calls consistent with UAT-10362's geofence check (T1614.001) preceding Lua interpreter initialization. | Email gateway logs with Traditional Chinese-language Trend Micro lures: Raw SMTP headers, sender domains, attachment filenames (likely mimicking Trend Micro security tools with zh-TW naming conventions), and delivery timestamps for messages to NGO/university staff — these establish the initial access vector (T1566.001 Spear-Phishing Attachment) and scope of potentially exposed accounts requiring credential review.

Per-Action IR Details

Step 1: Containment — Identify Windows endpoints in your environment running Traditional Chinese (zh-TW) locale settings or used by staff with Taiwan-facing roles. Isolate any systems showing unexpected DLL loads from Trend Micro-named binaries or Lua interpreter activity. Block outbound C2 traffic using IOCs published by Cisco Talos (blog.talosintelligence.com/new-lua-based-malware-lucidrook/) pending full IOC list retrieval.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-4 (Information Flow Enforcement), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run PowerShell on domain controllers to enumerate zh-TW locale endpoints: `Get-WmiObject Win32_OperatingSystem | Where-Object {$_.MUILanguages -like '*zh-TW*'} | Select-Object CSName`. For DLL side-loading detection without EDR, deploy Sysmon with EventID 7 (ImageLoaded) filtering on ImagePath matching 'Trend Micro' signed executables loading unsigned DLLs from user-writable directories (e.g., %APPDATA%, %TEMP%). Use Windows Firewall with Advanced Security (netsh advfirewall) to block known C2 IPs/domains at the host level on isolated endpoints immediately. Manually review Trend Micro-named process directories using Sysinternals Process Monitor filtered on DLL load operations.

Evidence: Before isolating any endpoint, capture: (1) Full memory dump using WinPmem or Magnet RAM Capture to preserve in-memory Lua interpreter state and LucidRook implant artifacts that may not persist on disk. (2) Sysmon

Event ID 7 (ImageLoaded) records showing which DLL was loaded, the signing status, and the parent Trend Micro-named executable from C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx. (3) Active network connections at time of isolation via `netstat -anob > connections.txt` and `Get-NetTCPConnection | Where-Object State -eq 'Established'` to capture live C2 beacon sessions before the endpoint is network-isolated. (4) Running process list with parent-child relationships via Sysinternals PsList or `Get-WmiObject Win32_Process | Select-Object Name,ProcessId,ParentProcessId,CommandLine`.

Step 2: Detection — Query EDR telemetry for DLL side-loading events involving Trend Micro-named executables loading unexpected DLLs. Search process creation logs for Lua interpreter invocations (lua.exe, lua54.dll) outside of known-legitimate software. Review email gateway logs for spear-phishing lures referencing Trend Micro tools or security software delivered to Traditional Chinese-locale users. Check PowerShell logs (Event ID 4104) for obfuscated script execution.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without EDR, deploy Sysmon with a configuration enabling Event ID 1 (Process Create), Event ID 7 (ImageLoaded), and Event ID 3 (Network Connection). Write a Sigma rule targeting: parent image matching `*\TrendMicro\*` with child image or loaded module matching `lua*.dll` not in the vendor's known file list. Query Windows Security Event Log for Event ID 4688 (Process Creation) filtered on `lua.exe` or `lua54.dll` as CommandLine token: `Get-WinEvent -LogName Security | Where-Object {$_.Message -match 'lua'}`. For email, parse MTA logs (Postfix, Exchange message tracking logs) for subjects or attachment names referencing 'Trend Micro', '[redacted]', or security tool names sent to recipients with zh-TW locale attributes. Use osquery `SELECT * FROM process_events WHERE cmdline LIKE '%lua%'` if osquery is deployed.

Evidence: Before pivoting on detections, preserve: (1) Windows Security Event Log Event ID 4688 entries (Process Creation) capturing the full command line of any lua.exe or lua54.dll invocations, specifically the parent process being a Trend Micro-named binary (e.g., PccNTMon.exe, TMBMSRV.exe, or a lookalike). (2) Sysmon Event ID 7 logs showing DLL load path discrepancies — legitimate Trend Micro DLLs load from `C:\Program Files (x86)\Trend Micro\` whereas side-loaded DLLs in this campaign are expected to load from user-writable paths or the executable's working directory. (3) Email gateway raw message headers and attachment metadata (MIME type, filename, sender domain) for Trend Micro-branded lures targeting zh-TW recipients — export from Exchange Transport logs or MTA logs filtering on subject keywords in Traditional Chinese. (4) PowerShell Script Block Logging Event ID 4104 from `Microsoft-Windows-PowerShell/Operational` log capturing any stage-two payload retrieval or geofence-check scripts that verify locale before executing.

Step 3: Eradication — Remove confirmed LucidRook implants identified during forensic review. Re-image affected endpoints where full scope of implant activity cannot be confirmed. Revoke and reissue credentials for any accounts accessed from compromised hosts. Remove malicious DLLs identified through side-loading analysis and restore legitimate application binaries from verified sources.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 5.3 (Disable Dormant Accounts)

Compensating: Use Sysinternals Sigcheck to verify the digital signatures of all DLLs in Trend Micro installation directories: `sigcheck -s -u 'C:\Program Files (x86)\Trend Micro\'` — any unsigned or differently-signed DLL in that path is a candidate artifact. Validate against known Trend Micro file hashes using the vendor's published file manifest if available, or VirusTotal batch hash lookup via the public API using PowerShell. For credential revocation without a PAM tool, use `net user [username] /domain` to force password reset and `Disable-ADAccount` for any service accounts that authenticated from compromised hosts. For re-imaging verification, run DISM `/online /cleanup-image`

/checkhealth` on rebuilt endpoints and compare installed software inventory against a pre-incident baseline captured via `Get-Package | Export-Csv`.

Evidence: Before eradication actions, preserve forensic copies of: (1) The malicious side-loaded DLL(s) from the Trend Micro application directory — collect file path, SHA-256 hash, PE compile timestamp, and import table (use PEView or pestudio) to characterize the LucidRook loader stage. (2) Any Lua bytecode or Lua script files (.lua, .luac) dropped to disk, typically in user-writable directories like %APPDATA%, %TEMP%, or subdirectories of the Trend Micro install path — hash and preserve before removal. (3) Prefetch files (`C:\Windows\Prefetch\LUA*.pf` or prefetch for the Trend Micro host process) to establish execution timeline and loaded module history using Eric Zimmerman's PECmd. (4) Registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` to document any LucidRook persistence entries before removal. (5) Credential access artifacts from Windows Security Event ID 4624 (Logon) and 4648 (Explicit Credential Use) on compromised hosts to identify all accounts that must be revoked.

Step 4: Recovery — Validate remediated endpoints against a known-good baseline before returning to production. Monitor for re-infection attempts via email gateway alerts targeting the same user population. Confirm no persistence mechanisms (scheduled tasks, registry run keys, modified startup items) remain on remediated systems. Maintain elevated logging on zh-TW locale endpoints for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 8.2 (Collect Audit Logs)

Compensating: Verify persistence clearance using Sysinternals Autoruns targeting all known LucidRook persistence vectors: scheduled tasks (`schtasks /query /fo LIST /v > tasks.txt`), registry run keys (`reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run backup.reg`), and startup folder contents (`dir '%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup'`). For ongoing re-infection monitoring without a SIEM, configure Windows Event Forwarding (WEF) to centralize Sysmon logs from all zh-TW locale endpoints to a single collector and run daily PowerShell queries against the collected logs for Lua interpreter invocations or Trend Micro directory DLL loads. Set email gateway rules to quarantine any message referencing Trend Micro product names or '[redacted]' sent to the previously targeted NGO staff distribution lists for the 30-day monitoring window.

Evidence: During recovery validation, collect: (1) Autoruns baseline export (XML format) from each remediated endpoint using `autorunsc -a * -c > autoruns_baseline.csv` and diff against pre-incident or reference baseline to confirm no residual LucidRook scheduled task or run-key persistence. (2) Sysmon Event ID 11 (FileCreate) and Event ID 13 (RegistryValueSet) logs from the 30-day monitoring window, filtered on file paths and registry keys associated with the original LucidRook implant locations, to detect re-deployment attempts. (3) Email gateway quarantine and delivery logs for the targeted zh-TW staff population covering the 30-day window to identify follow-on UAT-10362 spear-phishing waves using new lure themes or updated Trend Micro branding variants.

Step 5: Post-Incident — Conduct a gap assessment on DLL side-loading prevention controls — evaluate application whitelisting or WDAC policies to restrict unsigned DLL loads. Review spear-phishing resilience: test user awareness for lures mimicking trusted security vendors. Assess whether existing sandbox tooling enforces locale normalization to detect geofenced malware samples. Map detection coverage against T1574.002, T1480.001, and T1614.001 in your SIEM or XDR platform.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For WDAC policy creation without enterprise tooling, use the WDAC Wizard (free Microsoft tool) to generate a policy that enforces publisher rules for Trend Micro signed binaries and blocks DLL loads not signed by

Microsoft or whitelisted vendors from user-writable paths. Write a YARA rule targeting the Lua 5.4 bytecode header (`\x1bLua\x54`) in files loaded from non-standard paths to catch future LucidRook staging. For sandbox locale normalization, configure any Cuckoo Sandbox instance to run samples with `locale=zh-TW` and `keyboard=0x0404` system settings to bypass UAT-10362's geofence check. Create Sigma rules for T1574.002 (DLL Side-Loading) scoped to Trend Micro process names, T1480.001 (Environmental Keying on locale) triggering on locale-check API calls (GetUserDefaultUILanguage, GetSystemDefaultLCID), and T1614.001 (System Language Discovery) triggering on locale enumeration immediately preceding Lua interpreter launch.

Evidence: Post-incident documentation must include: (1) Lessons-learned record of exactly which Trend Micro-named executable was abused as the side-loading host, the DLL search order vulnerability exploited, and the file system path where the malicious DLL was planted — this drives the WDAC policy scope. (2) ATT&CK navigator layer export showing current detection coverage gaps against T1574.002, T1480.001, and T1614.001 with specific data sources mapped (Sysmon Event ID 7 for T1574.002; API monitoring for T1480.001; Windows locale API calls for T1614.001). (3) Sandbox detonation reports with zh-TW locale enforced, capturing network IOCs, file drops, and registry modifications from the full LucidRook kill chain for future threat intel sharing.

Detection Guidance

Before implementing detection rules, retrieve the full IOC list (file hashes, C2 domains, C2 IPs) from the Talos blog at blog.talosintelligence.com/new-lua-based-malware-lucidrook/. The detection strategies below are architecture-focused; operationalization requires IOC integration.

Primary detection focus areas: (1) DLL side-loading, alert on Trend Micro-named parent processes (e.g., TmListen.exe, PccNTMon.exe, or similar) loading DLLs from non-standard paths or with unsigned/mismatched signatures; (2) Lua interpreter activity, flag process creation or DLL load events for lua54.dll or lua.exe outside known-legitimate software contexts; (3) Geofencing bypass detection, configure sandboxes to emulate zh-TW locale when detonating suspicious attachments from campaigns targeting Taiwan-related organizations; (4) Spear-phishing lures, filter inbound email for Trend Micro-branded attachments or links from non-Trend Micro sending domains; (5) Exfiltration indicators, monitor for unexpected outbound HTTP/S or application-layer protocol traffic (T1071.003) from endpoints used by NGO or academic staff.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`[retrieve from Talos report — not fabricated here]`	LucidRook malware sample hashes published by Cisco Talos — retrieve directly from blog.talosintelligence.com/new-lua-based-malware-lucidrook/	LOW
DOMAIN	`[retrieve from Talos report — not fabricated here]`	LucidRook C2 infrastructure — retrieve directly from Talos intelligence report	LOW

Framework Mappings

MITRE-ATTACK

- **T1614.001** — System Language Discovery
- **T1105** — Ingress Tool Transfer

- **T1083** — File and Directory Discovery
- **T1041** — Exfiltration Over C2 Channel
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1071.003** — Mail Protocols
- **T1027.010** — Command Obfuscation
- **T1059** — Command and Scripting Interpreter
- **T1480.001** — Environmental Keying
- **T1574.002** — DLL Side-Loading
- **T1059.001** — PowerShell
- **T1566.001** — Spearphishing Attachment
- **T1027** — Obfuscated Files or Information
- **T1204.002** — Malicious File

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1614.001	System Language Discovery	Discovery
T1105	Ingress Tool Transfer	Command-And-Control

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery
T1041	Exfiltration Over C2 Channel	Exfiltration
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1071.003	Mail Protocols	Command-And-Control
T1027.010	Command Obfuscation	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1480.001	Environmental Keying	Defense-Evasion
T1574.002	DLL Side-Loading	Persistence
T1059.001	PowerShell	Execution
T1566.001	Spearphishing Attachment	Initial-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1204.002	Malicious File	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/uat-10362-targets-taiwanese-ngos-...	T3
New Lua-based malware “LucidRook” observed in targeted attacks ...	https://blog.talosintelligence.com/new-lua-based-malware-lucidrook/	T3
ZDI-CAN-25373 Windows Shortcut Exploit Abused as Zero-Day in ...	https://www.trendmicro.com/en_us/research/25/c/windows-shortcut-zer...	T3
Fake Security Tool Spreads LucidRook in Taiwan Cyberattacks	https://gbhackers.com/lucidrook-in-taiwan-cyberattacks/	T3
Trend Micro Discovers Actively Exploited Microsoft Vulnerability ...	https://www.youtube.com/watch?v=yY08S4-aICA	T3

Generated 2026-04-09 18:37 UTC by TJS Security Command Center