INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-10 06:15 UTC

UAT-10362 Targets Taiwan Civil Society with LucidRook Lua-Based Modular Malware

THREAT CAMPAIGN | HIGH | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0164
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Taiwanese NGOs and universities; Trend Micro Worry-Free Business Security Services (impersonated in lure), Microsoft Edge (abused for DLL sideloading), Gmail GMTP protocol (abused for C2 exfiltration)
Published	2026-04-09T18:04:31
Discovery Source	Rss

Executive Summary

A threat group tracked as UAT-10362 has been running targeted spear-phishing attacks against Taiwanese NGOs and universities since at least October 2025, deploying a novel modular malware called LucidRook. The malware uses an embedded Lua interpreter to let attackers retool their attack logic per target without rewriting core code, making detection and forensic analysis significantly harder. Organizations with ties to Taiwanese civil society, academic institutions, or regional policy work face elevated risk of data exfiltration through channels that bypass standard network controls.

Technical Analysis

UAT-10362 delivers LucidRook via spear-phishing (T1566.001) using lures that impersonate Trend Micro Worry-Free Business Security Services (T1036.005). The initial payload abuses Microsoft Edge for DLL sideloading (T1574.002), loading the malware into a trusted process context to evade endpoint controls. LucidRook's core binary embeds a Lua interpreter, enabling operators to push modular execution logic post-deployment without modifying the binary, complicating static analysis and hash-based detection (T1027, T1059). A companion tool, LucidKnight, exfiltrates collected data via Gmail's GMTP protocol (T1048.003, T1071.003), exploiting network environments that allowlist Google infrastructure. Additional behaviors include process discovery (T1057), file and directory enumeration (T1083), archive collection (T1560.001), and malicious file execution via user interaction (T1204.002). No CVE is associated with this campaign; exploitation relies on abuse of legitimate software rather than unpatched vulnerabilities. Relevant CWEs: CWE-693 (Protection Mechanism Failure), CWE-326 (Inadequate Encryption Strength), CWE-506 (Embedded Malicious

Code). Primary technical reporting is from BleepingComputer (T3 source); no vendor advisory or CISA alert confirmed at time of writing.

Action Checklist

1. Containment, Block or alert on outbound SMTP/GMTP connections to Gmail infrastructure from endpoints and servers that have no legitimate business need to send email via Gmail's API or GMTP protocol. Alert on and investigate any hosts showing unexpected msedge.exe child processes or DLL loads from non-standard paths.
2. Detection, Hunt for msedge.exe loading DLLs from user-writable directories (e.g., %APPDATA%, %TEMP%, %LOCALAPPDATA%). Query EDR telemetry for Lua interpreter activity or embedded Lua engine artifacts in process memory. Review email gateway logs for inbound messages impersonating Trend Micro Worry-Free Business Security Services, particularly with attachment-based lure chains.
3. Eradication, Remove any unauthorized DLLs found in Edge browser directories or adjacent user-writable paths. Terminate and remediate processes associated with LucidRook or LucidKnight artifacts. Re-image compromised hosts where modular payload execution is confirmed (or implement equivalent host remediation if re-imaging is not feasible - ensure kernel and memory are cleared of Lua-injected logic before returning to service).
4. Recovery, Validate that msedge.exe and associated browser binaries match known-good hashes from the Microsoft update catalog. Confirm no unauthorized Gmail GMTP exfiltration sessions occurred by reviewing DLP and proxy logs for the campaign window (October 2025 onward). Monitor reinstated hosts for recurrence of sideloading indicators for a minimum of 30 days.
5. Post-Incident, Review DLL sideloading exposure across all Electron-based and Chromium-based applications in your environment; this campaign exploits a class of abuse applicable beyond Edge. Assess whether network egress controls adequately restrict Google-infrastructure-bound traffic from non-mail endpoints. Update spear-phishing awareness training to include security vendor impersonation lures.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal/privacy counsel if proxy or DLP logs confirm successful GMTP exfiltration to Gmail infrastructure from any host — particularly if the affected endpoint belonged to staff handling sensitive civil society communications, donor data, research subjects, or policy work that could trigger Taiwan PDPA notification obligations or institutional data breach reporting requirements.

Recovery Notes	Post-containment, validate all reinstated hosts against a clean Microsoft Edge installation from the Update Catalog (https://www.microsoft.com/en-us/edge/business/download) before returning to production, as LucidRook's modular Lua-based architecture may stage secondary payloads in non-obvious directories that survive a simple process kill. Monitor reinstated hosts for a minimum of 30 days using Sysmon Event ID 7 watchlists scoped to msedge.exe and other Chromium/Electron-based application processes loading DLLs from user-writable paths, and retain all proxy logs covering outbound traffic to Google infrastructure for the same period to detect late-stage GMTP C2 re-establishment. Given that UAT-10362 has been active since at least October 2025 and targets civil society organizations with persistent access goals, treat any recurrence of sideloading indicators within the monitoring window as a reinfection event requiring full re-imaging rather than targeted remediation.
Forensic Artifacts	Sysmon Event ID 7 (ImageLoaded) logs: entries where Image matches '*\msedge.exe' and ImageLoaded path falls under %APPDATA%, %TEMP%, or %LOCALAPPDATA% — these directly evidence the LucidRook DLL sideloading execution chain and will include the malicious DLL's SHA-256 hash and signing status | Lua bytecode files on disk: files matching the Lua bytecode magic header (0x1B4C7561 / ESC 'Lua') dropped to user-writable directories, representing compiled LucidRook modular payloads — recoverable via YARA scan even if file extensions have been altered or files have been partially deleted | Proxy and firewall logs for outbound GMTP/SMTP sessions: TCP connections from non-mail-client processes to smtp.gmail.com (74.125.0.0/16) on ports 587 or 993, or HTTPS POSTs to Gmail API endpoints — constituting the LucidRook C2 exfiltration channel specific to this campaign's GMTP abuse technique | Spear-phish email artifacts in gateway quarantine or user mailboxes: raw .eml files from October 2025 onward with sender display names or attachment filenames referencing 'Trend Micro', 'Worry-Free', or 'WFBS' — preserving the full header chain (SPF/DKIM/DMARC results, originating IP, Message-ID) enables UAT-10362 infrastructure attribution | In-memory forensic snapshot of msedge.exe process: a full process memory dump captured via ProcDump ('procdump -ma ') before termination, required to recover in-memory Lua interpreter state and any LucidRook modules that execute purely in memory without writing complete artifacts to disk — critical given the campaign's stated design goal of reducing forensic traceability

Per-Action IR Details

Containment — Block or alert on outbound SMTP/GMTP connections to Gmail infrastructure from endpoints and servers that have no legitimate business need to send email via Gmail's API or GMTP protocol. Isolate any hosts showing unexpected msedge.exe child processes or DLL loads from non-standard paths.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-4 (System Monitoring), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On hosts without EDR, deploy Sysmon with a configuration that captures Event ID 7 (ImageLoaded) and Event ID 1 (Process Create) to flag msedge.exe loading DLLs outside of 'C:\Program Files (x86)\Microsoft\Edge\Application\'. For network containment without a NGFW, push Windows Firewall rules via GPO or PowerShell: 'New-NetFirewallRule -DisplayName "Block Gmail GMTP" -Direction Outbound -RemoteAddress 74.125.0.0/16,108.177.0.0/17,142.250.0.0/15 -Protocol TCP -RemotePort 587,465,993 -Action Block'. Use Wireshark or TCPDump on a network tap to capture pre-block baseline of any active GMTP sessions to Gmail API endpoints (smtp.gmail.com, imap.gmail.com) for evidence preservation.

Evidence: Before isolating the host, capture: (1) Sysmon Event ID 7 logs showing DLL load events from %APPDATA%, %TEMP%, or %LOCALAPPDATA% attributed to msedge.exe process tree — note the full DLL path, hash, and parent process; (2) Active network connections via 'netstat -anob' output, specifically any established TCP

sessions from msedge.exe or child processes to Google infrastructure (74.125.0.0/16, 142.250.0.0/15) on ports 587 or 993; (3) Windows Security Event Log Event ID 4688 (Process Creation) showing msedge.exe spawning unexpected child processes such as cmd.exe, powershell.exe, or wscript.exe; (4) Memory dump of the msedge.exe process (PID-specific) using ProcDump prior to termination to preserve in-memory Lua interpreter artifacts and loaded LucidRook modules.

Detection — Hunt for msedge.exe loading DLLs from user-writable directories (e.g., %APPDATA%, %TEMP%, %LOCALAPPDATA%). Query EDR telemetry for Lua interpreter activity or embedded Lua engine artifacts in process memory. Review email gateway logs for inbound messages impersonating Trend Micro Worry-Free Business Security Services, particularly with attachment-based lure chains.

NIST Phase: Detection Analysis

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

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

Compensating: Without EDR, use Sysmon Event ID 7 (ImageLoaded) with a Sigma rule filtering on 'Image: *\msedge.exe' AND 'ImageLoaded: (*\AppData* OR *\Temp* OR *\LocalAppData*)'. For Lua interpreter detection without memory scanning tools, search process image paths for 'lua*.dll' or 'luajit.dll' in non-standard locations using: 'Get-Process | ForEach-Object { $_.Modules | Where-Object {$_.FileName -match "lua"} | Select-Object @{N="PID";E={$_.Id}}, FileName }'. For email gateway hunting without enterprise SIEM, export inbound email headers from October 2025 onward and grep for sender domains spoofing 'trendmicro.com' or display names containing 'Worry-Free' or 'WFBS' using: 'Select-String -Path *.eml -Pattern "Worry-Free|WFBS|trendmicro" -CaseSensitive:$false'. Use YARA rules targeting Lua bytecode magic bytes (0x1B4C7561) in files dropped to user-writable paths.

Evidence: Preserve before analysis: (1) Full Sysmon Event ID 7 log export filtered to msedge.exe DLL loads from user-writable paths, including ModuleLoadReason and signing status of each loaded DLL — unsigned or self-signed DLLs in %APPDATA%\Microsoft\Edge\ or adjacent paths are primary LucidRook indicators; (2) Email gateway quarantine queue and delivery logs for messages from October 2025 onward with sender display names referencing 'Trend Micro', 'Worry-Free Business Security', or 'WFBS' — export raw .eml files including headers for sender authentication analysis (SPF/DKIM/DMARC results); (3) Windows Application Event Log and Edge browser crash logs at '%LOCALAPPDATA%\Microsoft\Edge\User Data\Crashpad\reports\' for anomalous DLL load failures indicative of sideloading probing; (4) File system timeline artifacts in user-writable directories created or modified within 48 hours of the earliest suspicious msedge.exe DLL load event, using 'dir /T:C /O:D %APPDATA%\Microsoft\Edge\ /S' to identify newly introduced files.

Eradication — Remove any unauthorized DLLs found in Edge browser directories or adjacent user-writable paths. Terminate and remediate processes associated with LucidRook or LucidKnight artifacts. Re-image compromised hosts where modular payload execution is confirmed — Lua-based logic injection may leave incomplete forensic traces.

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-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 2.3 (Address Unauthorized Software), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Before removal, hash all suspect DLLs with 'Get-FileHash -Algorithm SHA256 ' and submit to VirusTotal via API or manual upload for UAT-10362/LucidRook correlation. Use Sysinternals Autoruns to enumerate persistence mechanisms associated with the sideloaded DLL chain — check 'AppInit_DLLs', known DLL hijack paths, and scheduled tasks created by the msedge.exe process tree. For hosts where re-imaging is not immediately possible, use ClamAV with a custom signature targeting Lua bytecode magic (LucidRook module pattern) to scan %APPDATA%, %TEMP%, and %LOCALAPPDATA% recursively: 'clamscan -r --detect-pua=yes C:\Users\\AppData\'. Document all removed artifact paths and hashes in the incident ticket before deletion — Lua-based modular payloads

may stage additional modules in non-obvious subdirectories.

Evidence: Capture before eradication: (1) Full forensic image or at minimum logical acquisition of %APPDATA%\Microsoft\Edge\, %LOCALAPPDATA%\Microsoft\Edge\, %TEMP%, and any path identified in Sysmon Event ID 7 as a non-standard DLL load location for msedge.exe — preserve file metadata (MAC timestamps) to establish the LucidRook deployment timeline; (2) Registry export of 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run', 'HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs', and 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs' to identify UAT-10362 persistence mechanisms prior to removal; (3) List of all DLLs loaded by the msedge.exe process at time of compromise with signing certificate details — LucidRook DLLs will lack valid Microsoft or Edge signing chains; (4) Lua script or bytecode files (extension .lua, .luac, or files matching Lua bytecode magic 0x1B4C7561) dropped to disk, which represent the modular attack logic and are critical threat intelligence artifacts.

Recovery — Validate that msedge.exe and associated browser binaries match known-good hashes from the Microsoft update catalog. Confirm no unauthorized Gmail GMTP exfiltration sessions occurred by reviewing DLP and proxy logs for the campaign window (October 2025 onward). Monitor reinstated hosts for recurrence of sideloading indicators for a minimum of 30 days.

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 7.4 (Perform Automated Application Patch Management)

Compensating: For hash validation without enterprise tooling, download the canonical msedge.exe SHA-256 hash for the installed Edge version from the Microsoft Security Update Guide (https://msrc.microsoft.com/update-guide/) and compare locally: 'Get-FileHash "C:\Program Files (x86)\Microsoft\Edge\Application\\msedge.exe" -Algorithm SHA256'. For GMTP exfiltration review without DLP, parse Windows Firewall logs ('%SYSTEMROOT%\System32\LogFiles\Firewall\pfirewall.log') for outbound TCP connections to Gmail IP ranges (74.125.0.0/16, 142.250.0.0/15) on ports 587/993/443 from non-mail processes. Deploy a persistent Sysmon Event ID 7 watchlist rule on reinstated hosts specifically monitoring msedge.exe DLL loads for the 30-day observation window, forwarding events to a central syslog receiver (e.g., a Graylog or ELK stack on a spare VM).

Evidence: Preserve before declaring recovery complete: (1) Proxy or firewall log export covering October 2025 through the containment date, filtered to outbound connections from the affected host(s) to Gmail infrastructure — look for GMTP sessions (TCP 587/993) or HTTPS POST traffic to 'smtp.gmail.com' or Gmail API endpoints ('oauth2.googleapis.com', 'mail.google.com') from processes other than legitimate mail clients; (2) DLP alert history or email gateway send logs for the affected accounts to detect any data staged and transmitted via the LucidRook GMTP C2 channel before containment; (3) Baseline hash of all DLLs in the Edge application directory post-reinstallation from Microsoft Update Catalog, documented for comparison during the 30-day monitoring window; (4) Windows Security Event Log Event ID 4698/4702 (Scheduled Task Created/Modified) exports to verify no UAT-10362 persistence survived remediation.

Post-Incident — Review DLL sideloading exposure across all Electron-based and Chromium-based applications in your environment; this campaign exploits a class of abuse applicable beyond Edge. Assess whether network egress controls adequately restrict Google-infrastructure-bound traffic from non-mail endpoints. Update spear-phishing awareness training to include security vendor impersonation lures.

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-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For DLL sideloading exposure review without enterprise asset management tooling, use osquery to enumerate all Electron/Chromium-based application install paths: 'SELECT name, path FROM programs WHERE

name LIKE "%electron%" OR name LIKE "%chrome%" OR name LIKE "%edge%" OR name LIKE "%teams%" OR name LIKE "%slack%" OR name LIKE "%discord%"', then manually check each application directory for writable subdirectories using 'icacls /T | findstr "(W) (F) (M)"'. For egress policy review, audit Windows Firewall outbound rules and proxy allowlists for any rule permitting non-mail process access to Google SMTP/IMAP infrastructure. For awareness training, create a phishing simulation using a Trend Micro 'Worry-Free Business Security Services' branded lure — this specific UAT-10362 social engineering theme is actionable training material.

Evidence: Preserve for post-incident review and threat intelligence sharing: (1) Full timeline of the LucidRook infection chain reconstructed from Sysmon, email gateway, and proxy logs — document the spear-phish delivery date, first DLL sideload event, first GMTP C2 beacon, and containment timestamp to establish dwell time; (2) Inventory of all Electron/Chromium-based applications identified during the exposure review, with their DLL search order paths documented, to anchor the remediation scope; (3) Anonymized copies of the Trend Micro Worry-Free Business Security Services impersonation lure emails (headers, attachment metadata, sender infrastructure) for submission to CISA, Taiwan CERT (TWCERT/CC), and internal threat intelligence feed; (4) Any recovered Lua scripts or LucidRook module bytecode — these represent novel malware artifacts and should be shared with Trend Micro and relevant ISACs (e.g., MS-ISAC for academic/NGO sector) under TLP:AMBER.

Detection Guidance

Primary behavioral indicators: (1) msedge.exe or msedge helper processes loading DLLs from user-writable paths outside standard Edge installation directories, query EDR for ImageLoad events where ImagePath contains %APPDATA% or %TEMP% and ParentImage contains msedge.exe; (2) outbound network connections to Gmail SMTP/GMTP endpoints (smtp.gmail.com:587, smtp-relay.gmail.com) originating from non-mail-client processes, proxy and firewall logs should show process name alongside destination; (3) processes spawning Lua-related file artifacts or exhibiting dynamic code execution patterns inconsistent with their declared function; (4) inbound emails impersonating Trend Micro Worry-Free Business Security Services, filter on sender domain mismatches, display name spoofing, and attachment types (.exe, .dll, .zip) from non-trendmicro.com domains. MITRE coverage: T1574.002 (DLL Sideloading), T1048.003 (Exfiltration over alternative protocol), T1071.003 (Application layer protocol: mail). No public IOC list confirmed at time of writing; monitor BleepingComputer's original reporting and Trend Micro's threat research blog for released indicators.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`smtp.gmail.com`	LucidKnight abuses Gmail GMTP protocol for C2 exfiltration; outbound connections to Gmail SMTP infrastructure from non-mail processes are a behavioral indicator — note this is a legitimate Google domain being abused, not a malicious domain	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1574.002** — DLL Side-Loading
- **T1041** — Exfiltration Over C2 Channel

- **T1059** — Command and Scripting Interpreter
- **T1083** — File and Directory Discovery
- **T1048.003** — Exfiltration Over Unencrypted Non-C2 Protocol
- **T1566.001** — Spearphishing Attachment
- **T1560.001** — Archive via Utility
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1027** — Obfuscated Files or Information
- **T1071.003** — Mail Protocols
- **T1057** — Process Discovery
- **T1204.002** — Malicious File

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **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

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1574.002	DLL Side-Loading	Persistence
T1041	Exfiltration Over C2 Channel	Exfiltration
T1059	Command and Scripting Interpreter	Execution

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery
T1048.003	Exfiltration Over Unencrypted Non-C2 Protocol	Exfiltration
T1566.001	Spearphishing Attachment	Initial-Access
T1560.001	Archive via Utility	Collection
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1071.003	Mail Protocols	Command-And-Control
T1057	Process Discovery	Discovery
T1204.002	Malicious File	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-lucidrook-malwar...	T3
Analyzing Email Services Abused for Business Email Compromise	https://www.trendmicro.com/en/research/21/j/analyzing-email-service...	T3
Trend Micro False Positive Detection Reported with Microsoft Edge ...	https://success.trendmicro.com/en-US/solution/KA-0012989	T3
Trend Micro Discovers Actively Exploited Microsoft Vulnerability ...	https://www.youtube.com/watch?v=yY08S4-aICA	T3
Microsoft warns of new signed malware which deploys remote ...	https://www.cybersecurity-review.com/microsoft-warns-of-new-signed-...	T3

Generated 2026-04-10 06:15 UTC by TJS Security Command Center