INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-10 06:16 UTC

UAT-8302 / Earth Alux: China-Aligned Shared Espionage Toolkit Expanding Across Multiple Continents

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0298
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Internet-facing applications and network devices (specific vendors and versions vary by campaign phase; confirmed targeting of enterprise and government infrastructure)
Published	2026-05-08
Discovery Source	Gemini

Executive Summary

A China-aligned espionage group tracked as Earth Alux (also UAT-8302) is conducting multi-sector intrusion campaigns across Asia-Pacific and beyond, targeting government, technology, logistics, manufacturing, and telecommunications organizations. The group exploits vulnerabilities in internet-facing systems to deploy a modular backdoor toolkit, including VARGEIT and COBEACON, enabling persistent access, lateral movement, and long-term data collection. Organizations in targeted sectors face risk of sustained, covert compromise oriented toward strategic intelligence theft rather than immediate financial damage.

Technical Analysis

Earth Alux operates a shared espionage toolkit deployed via exploitation of N-day and zero-day vulnerabilities in internet-facing applications and network devices (specific vendors vary by campaign phase; Trend Micro's March 2025 research provides the most detailed breakdown available). The toolkit is modular, featuring multiple backdoors; VARGEIT and COBEACON are the most documented, supported by a loader ecosystem enabling staged deployment, persistence, and lateral movement. Relevant CWEs include CWE-494 (Download of Code Without Integrity Check), CWE-200 (Exposure of Sensitive Information), and CWE-78 (OS Command Injection). MITRE ATT&CK techniques span initial access via public-facing application exploitation (T1190), command and scripting interpreter use (T1059), obfuscated files and information (T1027), ingress tool transfer (T1105), application layer protocol for C2 (T1071), valid account abuse (T1078), masquerading (T1036), data collection

and archival (T1560), file and directory discovery (T1083), and process discovery (T1057). The 'shared toolkit' characterization indicates multiple distinct China-aligned threat groups may use overlapping tools and infrastructure, complicating attribution and increasing the likelihood of concurrent campaigns. No CVE identifiers are associated with this item in the current data; specific patch references depend on the exploited application or device in each campaign phase. Primary technical source: Trend Micro research publication, March 2025.

Action Checklist

1. Step 1: Containment. Audit all internet-facing applications and network devices for exposure. Prioritize systems in sectors Earth Alux targets: government, technology, logistics, manufacturing, and telecommunications. Restrict administrative access to critical network devices to trusted internal IPs only. Review firewall and WAF rules for anomalous outbound connections, especially to unfamiliar external IPs.
2. Step 2: Detection. Hunt for indicators associated with VARGEIT and COBEACON backdoors. Review endpoint and network telemetry for execution of unusual loaders, unexpected scheduled tasks or services, and anomalous outbound connections on standard application-layer protocols (HTTP/S, DNS) used for C2 (T1071). Query EDR/SIEM for processes spawning from internet-facing application services (T1059, T1190). Check for file staging and archival activity (T1560) and lateral movement via valid accounts (T1078). Consult Trend Micro's March 2025 IOC list for specific file hashes, C2 domains, and IPs (see Trend Micro source URL; validate before use).
3. Step 3: Eradication. Apply all available vendor patches for internet-facing applications and network devices, prioritizing those with known exploitation history. Where specific exploited CVEs are identified in your environment, follow the relevant vendor advisory for patch or configuration remediation. Remove unauthorized accounts or credentials identified during investigation (T1078). Verify integrity of loader and backdoor staging directories; remove identified malicious files.
4. Step 4: Recovery. Validate that all identified malicious artifacts have been removed and backdoor persistence mechanisms (scheduled tasks, services, startup entries) are cleared. Re-image compromised hosts where full forensic confidence in cleanup is not achievable. Restore from verified clean backups. Monitor post-remediation for re-infection attempts, particularly new outbound C2 connections and re-deployment of loader activity.
5. Step 5: Post-Incident. Review internet-facing application patch cadence and evaluate whether N-day exposure windows meet acceptable risk thresholds. Assess network segmentation between internet-facing systems and internal assets to limit lateral movement paths. Evaluate whether EDR coverage extends to all network edge devices. Consider threat intelligence feeds covering China-nexus espionage tooling to improve early detection of shared toolkit activity.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and relevant sector ISAC if any of the following are confirmed: VARGEIT or COBEACON artifacts identified on internal (non-DMZ) hosts indicating successful lateral movement beyond the internet-facing perimeter, evidence of data staging or exfiltration (T1560) involving sensitive government, PII, or intellectual property data triggering regulatory breach notification obligations, or if the organization operates in a CISA-designated critical infrastructure sector (government, telecommunications, manufacturing) and active Earth Alux TTPs are confirmed, which may trigger CISA mandatory reporting under CIRCIA.
Recovery Notes	Before returning any compromised host to production, validate the restore point timestamp predates the earliest confirmed Earth Alux activity in your environment — given the group's documented persistence via VARGEIT scheduled tasks and COBEACON services, restoring from a post-compromise backup risks reintroducing persistence mechanisms. Maintain an elevated monitoring posture for a minimum of 30 days post-recovery, with daily review of Sysmon Event ID 1 (process creation from internet-facing app processes), Event ID 3 (outbound connections to new external IPs), and scheduled task/service creation events, as Earth Alux operators have demonstrated capability to re-establish access if initial eviction is incomplete. If re-infection indicators appear within the 30-day window, treat as a separate incident with a fresh forensic scope expansion to identify any undiscovered persistence paths.
Forensic Artifacts	Web server access logs (IIS %SystemDrive%\inetpub\logs\LogFiles\ or Apache/Nginx /var/log/apache2/ or /var/log/nginx/) covering 90 days prior to detection — Earth Alux initial access via internet-facing application exploitation will leave anomalous POST requests, unusual URI patterns, or error spikes at the exploitation timestamp | Sysmon Event ID 1 (Process Create) records where ParentImage is the internet-facing application worker process (w3wp.exe, java.exe, python.exe, or vendor-specific daemon) and ChildImage is cmd.exe, powershell.exe, or wscript.exe — this is the primary process ancestry artifact for VARGEIT loader execution following web application exploitation (T1190, T1059) | Windows scheduled task XML exports from %SystemRoot%\System32\Tasks\ and registry key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks — Earth Alux uses scheduled tasks as a primary VARGEIT persistence mechanism and task XML will contain the loader execution path, trigger interval, and encoded command arguments | Network flow records or packet captures showing periodic low-volume outbound HTTP/HTTPS or DNS traffic from web application host processes to non-categorized external IPs — COBEACON's C2 beaconing over standard application-layer protocols (T1071) will appear as regular-interval small HTTP/HTTPS requests with consistent User-Agent strings to infrastructure not matching known CDN or SaaS IP ranges | Windows Security Event Log Event IDs 4624 (Successful Logon, Type 3 Network), 4648 (Explicit Credential Logon), and 4672 (Special Privilege Assigned) originating from internet-facing hosts to internal systems — these are the primary lateral movement artifacts for Earth Alux's use of valid compromised accounts (T1078) to pivot from the DMZ into the internal network

Per-Action IR Details

Step 1: Containment — Audit all internet-facing applications and network devices for exposure. Prioritize systems in sectors Earth Alux targets: government, technology, logistics, manufacturing, and telecommunications. Restrict administrative access to critical network devices to trusted internal IPs only. Review firewall and WAF rules for anomalous outbound connections, especially to unfamiliar external IPs.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), 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

12.2 (Establish and Maintain a Secure Network Architecture)

Compensating: Without an enterprise firewall management console, use `iptables` or `nftables` on Linux-based edge devices to restrict management interfaces to a defined trusted IP allowlist: `iptables -A INPUT -p tcp --dport 443 -s -j ACCEPT && iptables -A INPUT -p tcp --dport 443 -j DROP`. For Windows-based internet-facing apps, use Windows Firewall with Advanced Security (wf.msc) to scope inbound rules. Export and diff current firewall rule sets against a known-good baseline using a saved text export — any rules permitting broad outbound on 80/443 to non-CDN external IPs warrant immediate review. Run `netstat -anob` (Windows) or `ss -tulnp` (Linux) on each internet-facing host to enumerate active outbound connections and cross-reference against known-clean baselines.

Evidence: Before restricting access, capture full firewall and WAF rule export (JSON/XML) and current connection state tables (`conntrack -L` on Linux or `netstat -anob` on Windows) to preserve evidence of active or recently active C2 channels. Export WAF access logs covering the prior 90 days — Earth Alux initial access is via exploitation of internet-facing applications, so look for anomalous POST requests, URI path traversal patterns, or oversized payloads to admin endpoints. Capture a memory image of any internet-facing application servers showing active unusual outbound connections before isolation, as VARGEIT operates in-memory and evidence will be lost on reboot. Preserve syslog or SNMP trap logs from network edge devices for the same 90-day window.

Step 2: Detection — Hunt for indicators associated with VARGEIT and COBEACON backdoors. Review endpoint and network telemetry for execution of unusual loaders, unexpected scheduled tasks or services, and anomalous outbound connections on standard application-layer protocols (HTTP/S, DNS) used for C2 (T1071). Query EDR/SIEM for processes spawning from internet-facing application services (T1059, T1190). Check for file staging and archival activity (T1560) and lateral movement via valid accounts (T1078). Consult Trend Micro's March 2025 IOC list for specific file hashes, C2 domains, and IPs (see Trend Micro source URL; validate before use).

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with a hardened config (SwiftOnSecurity or Olaf Hartong's modular config) and enable Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 7 (Image Load), and Event ID 11 (File Create) to catch VARGEIT loader execution and COBEACON C2 beaconing. Hunt for VARGEIT-specific process ancestry: query Sysmon Event ID 1 for processes where ParentImage matches your internet-facing application service executable (e.g., `w3wp.exe`, `tomcat.exe`, or equivalent) spawning cmd.exe, powershell.exe, or wscript.exe. For COBEACON C2 beaconing over HTTP/S, use Wireshark or `tcpdump -i -w capture.pcap 'port 80 or port 443'` and analyze for periodic low-volume beacons with consistent jitter intervals to unfamiliar external IPs. Write YARA rules targeting VARGEIT/COBEACON string signatures or byte sequences from the Trend Micro March 2025 report and scan staging directories with `yara -r rule.yar /var/www/ /tmp/ C:\Windows\Temp\`. Use Sigma rule conversions targeting T1071.001 (Web Protocols C2) and T1053.005 (Scheduled Task) for manual log analysis if no SIEM is available.

Evidence: Before hunting, preserve Windows Security Event Log Event ID 4698 (Scheduled Task Created) and Event ID 4702 (Scheduled Task Updated) from all endpoints, as Earth Alux uses scheduled tasks for VARGEIT persistence. Collect Windows Security Event ID 4624/4625/4648 (logon events) filtered on logon type 3 (network) and type 10 (remote interactive) originating from internet-facing hosts, to identify lateral movement via compromised valid accounts (T1078). Capture Sysmon Event ID 3 records showing outbound connections from web application worker processes (w3wp.exe, java.exe) to external IPs — this is the expected COBEACON C2 initiation artifact. Preserve IIS/Apache/Nginx access logs and application-layer logs showing the initial exploitation request URI and source IP. Export DNS query logs from local resolver or endpoint DNS cache (`ipconfig /displaydns` on Windows) to identify C2 domain resolution attempts matching Trend Micro IOC domains.

Step 3: Eradication — Apply all available vendor patches for internet-facing applications and network devices, prioritizing those with known exploitation history. Where specific exploited CVEs are identified in your

environment, follow the relevant vendor advisory for patch or configuration remediation. Remove unauthorized accounts or credentials identified during investigation (T1078). Verify integrity of loader and backdoor staging directories; remove identified malicious files.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For integrity verification of suspected VARGEIT/COBEACON staging directories (commonly `%TEMP%`, `C:\Windows\Temp`, `/tmp`, `/var/tmp`, web application upload directories), generate SHA-256 hashes of all files using `Get-FileHash -Algorithm SHA256 -Path C:\Windows\Temp\* | Export-Csv hashes.csv` (Windows) or `find /tmp -type f -exec sha256sum {} \; > hashes.txt` (Linux), then cross-reference against Trend Micro March 2025 IOC file hashes. To enumerate unauthorized local accounts added by Earth Alux operators post-exploitation, run `net user` (Windows) or `cat /etc/passwd` and compare against a known-clean account baseline. Remove identified malicious scheduled tasks via `schtasks /delete /tn "" /f` after documenting the task XML (`schtasks /query /tn "" /xml`). Use ClamAV with a custom signature database updated with VARGEIT/COBEACON YARA rules for a full filesystem scan prior to declaring eradication complete.

Evidence: Before removing any artifacts, image the full disk of confirmed-compromised hosts using `dc3dd` or `FTK Imager Lite` to preserve forensic evidence for post-incident review and potential legal hold. Export the full scheduled task list (`schtasks /query /fo CSV /v > tasks_baseline.csv`) and compare to pre-incident baseline to identify Earth Alux persistence tasks before deletion. Collect all identified malicious file paths, SHA-256 hashes, PE metadata (compile timestamps, import tables), and creation/modification timestamps using `ExifTool` or PowerShell `Get-Item` before deletion — VARGEIT loader metadata may reveal campaign infrastructure reuse. Capture a dump of the Windows registry `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks` and `HKLM\SYSTEM\CurrentControlSet\Services` before eradication to document all persistence mechanisms. Preserve copies of unauthorized account creation events (Windows Security Event ID 4720) and privilege escalation events (Event ID 4672) for attribution and legal evidence.

Step 4: Recovery — Validate that all identified malicious artifacts have been removed and backdoor persistence mechanisms (scheduled tasks, services, startup entries) are cleared. Re-image compromised hosts where full forensic confidence in cleanup is not achievable. Restore from verified clean backups. Monitor post-remediation for re-infection attempts, particularly new outbound C2 connections and re-deployment of loader activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 11.2 (Perform Automated Recovery Testing), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without enterprise EDR for post-recovery monitoring, deploy Sysmon on all re-imaged or cleaned hosts immediately post-recovery and establish a Sysmon Event ID 3 baseline for all outbound connections from internet-facing application processes during the first 72 hours — any connection to an external IP not present in pre-incident baselines is a re-infection signal. Schedule a daily osquery query against `scheduled_tasks`, `startup_items`, and `services` tables (`osqueryi --line 'SELECT name, path, status FROM scheduled_tasks;'`) and diff against a known-clean snapshot to detect VARGEIT re-deployment. Validate backup integrity before restoration by comparing SHA-256 checksums of restored files against backup manifest hashes. For hosts that cannot be re-imaged, run a Sysinternals Autoruns export (`autorunsc.exe -a * -c -h -s > autoruns_post.csv`) and diff against a clean-state baseline to confirm all COBEACON/VARGEIT persistence entries are cleared.

Evidence: Before returning any host to production, capture a final Autoruns export, full scheduled task list, services registry snapshot, and Sysmon Event ID 3 connection baseline to establish a verified clean-state artifact set for comparison during the post-recovery monitoring window. Document the specific backup restore point date and validate

it predates the earliest confirmed Earth Alux activity timestamp (derived from initial exploitation log evidence) to ensure restored images do not contain pre-persistence backdoor files. Retain all forensic disk images, memory captures, and log exports from the incident for a minimum of 90 days to support threat intelligence sharing and any regulatory notification obligations.

Step 5: Post-Incident — Review internet-facing application patch cadence and evaluate whether N-day exposure windows meet acceptable risk thresholds. Assess network segmentation between internet-facing systems and internal assets to limit lateral movement paths. Evaluate whether EDR coverage extends to all network edge devices. Consider threat intelligence feeds covering China-nexus espionage tooling to improve early detection of shared toolkit activity.

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 RA-3 (Risk Assessment), NIST SI-2 (Flaw Remediation), NIST SC-7 (Boundary Protection), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Conduct a structured lessons-learned session within 5 business days using the NIST 800-61r3 §4 post-incident template, specifically documenting the N-day window between patch availability and exploitation for each affected internet-facing system — this directly informs whether your current monthly patch cadence is adequate against Earth Alux-tempo exploitation. For threat intelligence integration without a commercial TI platform, subscribe to CISA Known Exploited Vulnerabilities (KEV) catalog RSS/API alerts and the Trend Micro Threat Intelligence feeds (verify current subscription options directly with Trend Micro) to receive early warning of Earth Alux shared toolkit IOC updates. Use Sigma rules mapped to MITRE ATT&CK T1190 (Exploit Public-Facing Application), T1071 (Application Layer Protocol), T1078 (Valid Accounts), and T1560 (Archive Collected Data) and convert them to your available log platform (Splunk Free, Elastic, or manual grep pipelines) to operationalize detection of Earth Alux TTPs before the next campaign wave. Map network segmentation gaps identified during lateral movement analysis against CIS Control 12 (Network Infrastructure Management) and document remediation as a tracked risk item.

Evidence: Compile a complete incident timeline artifact package including: initial exploitation log entry (WAF/web server), first VARGEIT loader execution timestamp (Sysmon Event ID 1), first COBEACON C2 beacon (Sysmon Event ID 3 or network capture), first lateral movement event (Windows Security Event ID 4624 type 3 from compromised host), and earliest data staging/archival action (Sysmon Event ID 11 in staging directories) — this timeline directly feeds the N-day gap calculation and segmentation gap assessment. Preserve the full IOC set (hashes, C2 IPs, C2 domains, scheduled task names, service names, file paths) in a structured format (STIX 2.1 or MISP event) for sharing with sector ISACs (e.g., IT-ISAC, CISA if government-sector) per NIST IR-6 (Incident Reporting) obligations.

Detection Guidance

Detection centers on identifying VARGEIT and COBEACON backdoor behavior and the associated loader ecosystem. Key signals: (1) Unusual processes or services spawned by internet-facing application processes; correlate web server or VPN process trees against known-good baselines in EDR telemetry. (2) Outbound C2 traffic using standard protocols (HTTP/S, DNS) to low-reputation or newly registered domains; query proxy and DNS logs for beaconing patterns. (3) File staging and compression activity in unexpected directories (T1560); alert on archive creation tools executed outside normal business context. (4) Valid account abuse (T1078); flag logins from new source IPs or outside business hours for privileged accounts on network devices. (5) Obfuscated script execution (T1027, T1059); alert on encoded PowerShell or shell commands originating from application service accounts. For specific file hashes, C2 IPs, and domains, reference the Trend Micro March 2025 research publication directly. IOCs from that report should be validated and ingested into SIEM/EDR blocklists and threat intelligence platforms before operationalization.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	[See Trend Micro March 2025 research for verified hashes — not reproduced here to avoid transcription error]	VARGEIT and COBEACON backdoor file hashes documented in primary Trend Micro source	MEDIUM
DOMAIN	[See Trend Micro March 2025 research for verified C2 domains]	Earth Alux C2 infrastructure documented in primary Trend Micro source	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1560** — Archive Collected Data
- **T1083** — File and Directory Discovery
- **T1078** — Valid Accounts
- **T1071** — Application Layer Protocol
- **T1105** — Ingress Tool Transfer
- **T1190** — Exploit Public-Facing Application
- **T1036** — Masquerading
- **T1059** — Command and Scripting Interpreter
- **T1027** — Obfuscated Files or Information
- **T1057** — Process Discovery

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **SI-3** — Malicious Code Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality

- **CM-3** — Configuration Change Control
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A01:2021** — Broken Access Control
- **A03:2021** — Injection

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **16.10** — Apply Secure Design Principles in Application Architectures

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1560	Archive Collected Data	Collection
T1083	File and Directory Discovery	Discovery
T1078	Valid Accounts	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control
T1105	Ingress Tool Transfer	Command-And-Control
T1190	Exploit Public-Facing Application	Initial-Access
T1036	Masquerading	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1057	Process Discovery	Discovery

Sources

Source	URL	Tier
The Espionage Toolkit of Earth Alux A Closer Look at its Advanced ...	https://www.trendmicro.com/en_us/research/25/c/the-espionage-toolki...	T3
A Possible US Government iPhone-Hacking Toolkit Is Now ... - WIRED	https://www.wired.com/story/coruna-iphone-hacking-toolkit-us-govern...	T2
China-linked Espionage Tools Used in Ransomware Attacks	https://www.security.com/threat-intelligence/chinese-espionage-rans...	T3
Chinese APT Abuses Multiple Cloud Tools to Spy on Mongolia	https://www.darkreading.com/cyberattacks-data-breaches/chinese-apt-...	T3
Unmasking MuddyWater's New Malware Toolkit Driving ... - Group-IB	https://www.group-ib.com/blog/muddywater-espionage/	T3

Generated 2026-05-10 06:16 UTC by TJS Security Command Center