INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-01 18:41 UTC

UAC-0255 Impersonates CERT-UA to Distribute AGEWHEEZE RAT in Multi-Sector Phishing Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0135
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Windows systems (scheduled task, registry, startup persistence); ukr.net email platform users; Files.fm hosting service; Ukrainian government, healthcare, finance, education, and security sector endpoints
Published	2026-04-01T12:10:00
Discovery Source	Rss

Executive Summary

On March 26-27, 2026, threat actor UAC-0255 (self-identified as 'Cyber Serp') impersonated Ukraine's official CERT-UA to distribute AGEWHEEZE, a newly documented Go-based remote access trojan, via phishing emails sent through the ukr.net platform. The campaign targeted Ukrainian government, healthcare, finance, education, and security sector organizations; CERT-UA confirmed actual infections were limited to a small number of educational institution endpoints, despite the actor's unverified claim of 200,000 compromised devices. The primary business risk is credential theft, remote system control, and persistent access to sensitive networks through a trusted-brand impersonation vector that lowers recipient suspicion.

Technical Analysis

UAC-0255 delivered AGEWHEEZE via spearphishing emails (T1566.001) and link-based delivery (T1566.002) through ukr.net, using password-protected archives disguised as official CERT-UA security tooling. The malware is written in Go and establishes persistence through three mechanisms: Windows Scheduled Tasks (T1053.005), registry Run key modifications (T1547.001), and startup folder entries (T1547.001, formerly T1060). Post-compromise capabilities observed include remote access/C2 (T1219), screen capture (T1113), clipboard monitoring (T1115), command execution (T1059), obfuscated payload delivery (T1027), and ingress tool transfer (T1105). C2 communication uses HTTP/S (T1071.001). Delivery infrastructure was AI-generated

(T1583.006) and hosted via Files.fm cloud storage. The actor masqueraded as a legitimate organization binary (T1036.005). Relevant weaknesses are CWE-451 (UI Misrepresentation of Critical Information, the CERT-UA brand spoofing) and CWE-494 (Download of Code Without Integrity Check, the archive delivery mechanism). No CVE is associated with this campaign. No vendor patch applies; the attack chain is entirely social engineering and Windows native persistence mechanisms. Source quality score for this item is 0.632, reflecting T3-tier sourcing; CERT-UA's direct public statements (referenced within those sources) are the authoritative confirmation of actual infection scope.

Action Checklist

1. Containment, Block Files.fm at the web proxy and DNS layer organization-wide. Block inbound emails with ukr.net sender domains impersonating CERT-UA display names; apply header-based rules that flag mismatches between display name and sender domain. Isolate any Windows endpoints where AGEWHEEZE artifacts are found before further investigation.
2. Detection, Query email gateway logs for messages with display names containing 'CERT-UA' or 'CERT UA' where the sending domain is not cert.gov.ua. Search endpoint logs for scheduled task creation events (Windows Event ID 4698) and registry modifications under HKCU\Software\Microsoft\Windows\CurrentVersion\Run occurring within the March 26-27, 2026 timeframe or after. Hunt for Go-compiled executables in user-writable directories (AppData, Temp, startup folders). Monitor for outbound HTTP/S connections to unknown hosts initiated by newly created scheduled tasks. MITRE techniques to prioritize for detection rule coverage: T1053.005, T1547.001, T1566.001, T1566.002, T1036.005.
3. Eradication, Remove identified scheduled tasks via Task Scheduler or 'schtasks /delete'. Delete AGEWHEEZE binaries and any dropped payloads from affected endpoints. Purge malicious registry Run keys and startup folder entries. Revoke and rotate credentials on any confirmed compromised accounts. Re-image endpoints where full artifact enumeration cannot be confirmed.
4. Recovery, After eradication, monitor affected endpoints for 72 hours for recurrence of scheduled task creation, registry modifications, and anomalous outbound connections. Validate that no lateral movement occurred from confirmed infected educational sector endpoints before returning systems to production. Confirm email gateway rules are active and logging correctly.
5. Post-Incident, This campaign exploited brand trust and the absence of sender authentication enforcement. Review and enforce DMARC, DKIM, and SPF policies for inbound mail. Conduct targeted user awareness for sectors identified as campaign targets (government, healthcare, finance, education, security). Evaluate whether Go-compiled binary execution in user-writable directories is preventable via application control policy (e.g., Windows Defender Application Control or equivalent). Document CERT-UA as a spoofed brand in your threat intelligence platform for future phishing rule tuning.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if forensic analysis confirms AGEWHEEZE exfiltrated data from healthcare or government endpoints (triggering potential breach notification obligations under Ukrainian law and sector-specific regulations), if lateral movement is detected beyond the confirmed educational sector endpoints, or if the team lacks the capability to perform complete artifact enumeration on any infected host — re-imaging without forensic preservation at that scale requires documented authorization.
Recovery Notes	After eradication, enforce a 72-hour continuous monitoring period on all recovered endpoints using Sysmon Event IDs 1, 3, 11, 12, and 13 to detect AGEWHEEZE re-establishment via any secondary dropper or persistence mechanism not enumerated during initial response — UAC-0255's use of both scheduled tasks (T1053.005) and registry Run keys (T1547.001) simultaneously suggests a layered persistence strategy where incomplete removal of one mechanism can re-trigger the other. Before returning any educational sector endpoint to production, confirm via Security Event ID 4624 and 5140 analysis that no credential-based lateral movement or file server access occurred from the infected host during the dwell window. Retain all forensic images, memory captures, and email header evidence for a minimum of 90 days in write-protected storage to support any regulatory inquiry or intelligence-sharing request from CERT-UA.
Forensic Artifacts	Windows Task Scheduler event log ('%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational.evtx') and Security Event ID 4698 entries dated March 26-27, 2026 — contain the full XML definition of the AGEWHEEZE-created scheduled task including binary path in a user-writable directory, trigger type, and any command-line arguments passed to the RAT at launch | Registry hive export of 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' from affected user profiles — the AGEWHEEZE Run key value name and binary path reflect UAC-0255's persistence naming convention and the exact file system location chosen for the Go-compiled executable | Prefetch files ('%SystemRoot%\Prefetch\[AGEWHEEZE_BINARY_NAME]-[hash].pf') — provide first execution timestamp of the AGEWHEEZE binary independent of file system timestamps (which may be manipulated), and enumerate DLLs and file paths accessed during AGEWHEEZE's first run including any secondary payload staging paths | Browser download history and 'C:\Users\[username]\Downloads' directory metadata timestamped to March 26-27, 2026 — preserve the exact files.fm URL path used to host the AGEWHEEZE payload, the downloaded filename, and file size for correlation with other campaign-linked infrastructure and CERT-UA intelligence sharing | Memory image from any endpoint where AGEWHEEZE was confirmed active prior to containment — Go-based RATs frequently store C2 configuration, decrypted command channels, and operator-issued tasking only in process memory; a Volatility 3 analysis using 'windows.netscan' and 'windows.cmdline' plugins against the memory image is the only reliable method to recover AGEWHEEZE's C2 IP/domain and any commands executed during the dwell period before process termination destroys this evidence

Per-Action IR Details

Containment — Block Files.fm (files.fm) at the web proxy and DNS layer organization-wide. Block inbound emails with ukr.net sender domains impersonating CERT-UA display names; apply header-based rules that flag mismatches between display name and sender domain. Isolate any Windows endpoints where AGEWHEEZE artifacts are found before further investigation.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User

Devices)

Compensating: On pfSense or OPNsense, add files.fm and its CDN IP ranges to an Alias block list under Firewall > Aliases, then enforce at the LAN boundary rule. For DNS-layer blocking without enterprise tooling, add 'files.fm' to Pi-hole blocklists and verify resolution fails with 'nslookup files.fm'. For email header inspection without a commercial gateway, use a free Postfix milter or SpamAssassin rule: flag any message where the 'From:' display name contains 'CERT-UA' or 'CERT UA' and the envelope sender domain is not cert.gov.ua. Isolate AGEWHEEZE-positive endpoints by disabling their NIC via 'netsh interface set interface [name] admin=disabled' — do not power off before imaging.

Evidence: Before isolating endpoints, capture: full memory image using WinPmem or Magnet RAM Capture (AGEWHEEZE as a Go-based RAT may maintain C2 configuration or decrypted strings only in memory); preserve the files.fm download URL from browser history at '%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\History' or Chrome equivalent, which will contain the exact payload filename and hosting path used by UAC-0255; export email headers from any received ukr.net messages impersonating CERT-UA (From, Reply-To, X-Originating-IP, Message-ID, DKIM-Signature fields) before quarantine actions delete them; document the network state with 'netstat -bno' to capture any live AGEWHEEZE C2 connection before NIC isolation.

Detection — Query email gateway logs for messages with display names containing 'CERT-UA' or 'CERT UA' where the sending domain is not cert.gov.ua. Search endpoint logs for scheduled task creation events (Windows Event ID 4698) and registry modifications under HKCU\Software\Microsoft\Windows\CurrentVersion\Run occurring within the March 26-27, 2026 timeframe or after. Hunt for Go-compiled executables in user-writable directories (AppData, Temp, startup folders). Monitor for outbound HTTP/S connections to unknown hosts initiated by newly created scheduled tasks. MITRE techniques to prioritize for detection rule coverage: T1053.005, T1547.001, T1566.001, T1566.002, T1036.005.

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)

Compensating: Deploy Sysmon with SwiftOnSecurity's config (minimum) to capture Event ID 1 (Process Create), Event ID 11 (File Create), Event ID 12/13 (Registry Create/Modify) — Sysmon Event ID 12 will log HKCU\Software\Microsoft\Windows\CurrentVersion\Run writes by AGEWHEEZE. For scheduled task hunting, run: 'Get-ScheduledTask | Where-Object {$_.Date -ge "2026-03-26"} | Select TaskName, TaskPath, Date, @{n="Actions";e={$_.Actions}} | Export-Csv tasks_audit.csv'. To hunt Go-compiled binaries in user-writable paths without EDR, use: 'Get-ChildItem -Path $env:APPDATA, $env:TEMP, "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup" -Recurse -Include *.exe | Select FullName, Length, LastWriteTime | Export-Csv go_hunt.csv' and then verify PE headers — Go binaries have a distinctive import table and often embed 'Go build ID' strings detectable with 'strings.exe' from Sysinternals or 'grep -a "Go build id" suspect.exe' on Linux. Use the Sigma rule for T1053.005 (scheduled task creation via schtasks.exe or Task Scheduler COM interface) converted to native Windows Event Log queries via 'sigma convert'. For C2 detection without a SIEM, run Wireshark or 'netsh trace start capture=yes' on suspect endpoints and filter for established outbound connections from svchost.exe or the AGEWHEEZE process name to non-Microsoft IP ranges.

Evidence: Windows Security Event Log Event ID 4698 (A scheduled task was created) with the task XML body — export the full event including the task definition which will name the AGEWHEEZE binary path and execution trigger; Windows Security Event ID 4657 (A registry value was modified) or Sysmon Event ID 13 for HKCU\Software\Microsoft\Windows\CurrentVersion\Run showing the AGEWHEEZE persistence key name and binary path; email gateway logs filtered on sender display name 'CERT-UA' with envelope-from @ukr.net showing recipient addresses across all targeted sectors (government, healthcare, finance, education, security) — this scopes lateral exposure before full detection sweep; browser download history and 'C:\Users\[user]\Downloads' directory listing timestamped to March 26-27, 2026 capturing the files.fm payload filename; Prefetch files ('%SystemRoot%\Prefetch\') for the AGEWHEEZE binary name — Go executables appear in Prefetch on first execution and provide first-run timestamp even if the binary is later deleted.

Eradication — Remove identified scheduled tasks via Task Scheduler or 'schtasks /delete'. Delete AGEWHEEZE binaries and any dropped payloads from affected endpoints. Purge malicious registry Run keys

and startup folder entries. Revoke and rotate credentials on any confirmed compromised accounts. Re-image endpoints where full artifact enumeration cannot be confirmed.

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 AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Execute scheduled task removal via: 'schtasks /delete /tn "[AGEWHEEZE task name]" /f' and confirm deletion with 'schtasks /query /tn "[task name]"' returning an error — do not rely only on Task Scheduler GUI which can be spoofed by persistence hiding techniques. Remove the HKCU Run key with: 'reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "[value name]" /f' and verify absence with 'reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"'. Delete startup folder entries from '%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\'. For credential revocation on endpoints without centralized IAM, use 'net user [username] /passwordreq:yes' to force password reset and audit accounts that authenticated during March 26-27, 2026 via Event ID 4624. For endpoints where AGEWHEEZE dwell time is uncertain or artifact enumeration is incomplete, re-image is the correct call — Go-based RATs can drop secondary stages or modify legitimate binaries; absence of known artifacts does not confirm clean state.

Evidence: Before deletion, forensically image or at minimum hash (SHA-256) all AGEWHEEZE binaries and dropped payloads using 'certutil -hashfile [path] SHA256' — preserve these as evidence and for YARA rule development against future UAC-0255 campaigns; export the full scheduled task XML before deletion via 'schtasks /query /tn "[task name]" /xml > task_evidence.xml' to preserve UAC-0255's task naming convention, trigger configuration, and any embedded command-line arguments passed to AGEWHEEZE; export the malicious Run key value before deletion via 'reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" run_key_evidence.reg'; document all accounts that were active on confirmed infected endpoints during the March 26-27, 2026 campaign window using Windows Security Event ID 4624 (Logon) and 4648 (Explicit Credential Logon) — these accounts require credential rotation regardless of confirmed compromise status.

Recovery — After eradication, monitor affected endpoints for 72 hours for recurrence of scheduled task creation, registry modifications, and anomalous outbound connections. Validate that no lateral movement occurred from confirmed infected educational sector endpoints before returning systems to production. Confirm email gateway rules are active and logging correctly.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Establish a 72-hour monitoring baseline on recovered endpoints by enabling enhanced Sysmon logging (Events 1, 3, 11, 12, 13, 22) and running a scheduled PowerShell task every 4 hours that hashes all executables in '%APPDATA%', '%TEMP%', and startup paths, comparing against the post-eradication clean baseline — alert on any new or modified hash. For lateral movement validation from the confirmed educational sector endpoints, query Windows Security Event ID 4648 (Logon with explicit credentials) and 4624 Type 3 (Network Logon) originating from the infected machine's IP or hostname during the March 26-27, 2026 window through present; use 'net session' and review '%SystemRoot%\System32\winevt\Logs\Security.evtx' on adjacent systems if a SIEM is unavailable. Validate email gateway rule efficacy by sending a controlled test message with display name 'CERT-UA' from a non-cert.gov.ua domain and confirming it is flagged and logged before returning mail flow to normal.

Evidence: During the 72-hour monitoring window, continuously capture: Sysmon Event ID 3 (Network Connection) logs filtered on the recovered endpoint's process list to detect any AGEWHEEZE re-establishment of C2; Windows Security Event ID 4698 to detect re-creation of the previously deleted scheduled task (UAC-0255 may use a dropper or second-stage to re-establish persistence if initial eradication was incomplete); SMB access logs (Security Event ID 5140 — A network share object was accessed) on file servers queried from the educational sector endpoints during the infection window to scope any data access or credential-based lateral movement that AGEWHEEZE may have facilitated prior to containment.

Post-Incident — This campaign exploited brand trust and the absence of sender authentication enforcement. Review and enforce DMARC, DKIM, and SPF policies for inbound mail. Conduct targeted user awareness for sectors identified as campaign targets (government, healthcare, finance, education, security). Evaluate whether Go-compiled binary execution in user-writable directories is preventable via application control policy (e.g., Windows Defender Application Control or equivalent). Document CERT-UA as a spoofed brand in your threat intelligence platform for future phishing rule tuning.

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-5 (Security Alerts, Advisories, and Directives), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For DMARC enforcement without a commercial email security platform, publish a DMARC record at '_dmarc.[yourdomain]' set to 'p=quarantine' minimum, and use the free MXToolbox DMARC analyzer or Google Postmaster Tools to review aggregate reports (rua tag) for spoofing attempts impersonating your domain. For WDAC application control policy to block Go-compiled executables in user-writable paths without enterprise licensing, create a policy in audit mode first using 'New-CIPolicy -Level FilePath -UserPEs -ScanPath C:\Windows -FilePath WDACPolicy.xml', then deny execution from '%APPDATA%' and '%TEMP%' path rules — test against a benign Go binary before enforcement. For the threat intelligence platform entry, if no commercial TIP is available, document the UAC-0255 / 'Cyber Serp' actor profile, AGEWHEEZE binary hashes, files.fm hosting pattern, and ukr.net-as-phishing-vector in MISP (free, open source) with tags mapping to MITRE T1036.005 (Masquerading: Match Legitimate Name or Location) and T1566.001 (Spearphishing Attachment) for automated future detection rule generation.

Evidence: For the post-incident review, assemble: all preserved AGEWHEEZE binary hashes (SHA-256) for TIP ingestion and YARA rule authoring targeting Go build ID strings and UAC-0255's binary naming convention; the complete set of email headers from the CERT-UA-impersonating ukr.net messages to document the specific display name format ('CERT-UA', 'CERT UA') and any X-Originating-IP or routing headers that fingerprint UAC-0255's sending infrastructure for future phishing rule tuning; the Task Scheduler XML exports and Run key exports preserved during eradication, which define UAC-0255's persistence naming conventions and AGEWHEEZE launch parameters for detection rule documentation; a timeline log correlating Event ID 4698 (task creation), 4624 (first logon post-delivery), and Sysmon Event ID 3 (first outbound network connection) to calculate AGEWHEEZE's time-to-persistence and time-to-C2 metrics — these dwell time figures feed directly into detection threshold tuning for future campaigns.

Detection Guidance

Primary detection pivot: scheduled task creation (Windows Event ID 4698) combined with a parent process that is not a known administrative tool. Secondary pivot: new registry Run key entries (monitor HKCU\Software\Microsoft\Windows\CurrentVersion\Run via Sysmon Event ID 13 or equivalent) created by user-context processes. Behavioral indicator: Go-compiled executables (identifiable by Go runtime strings in binary analysis) executing from AppData, Temp, or startup directories. Network indicator: HTTP/S beaconing to low-reputation or newly registered domains from processes matching the above profile. Email indicator: display name 'CERT-UA' or variations with sender domain not matching cert.gov.ua; subject lines referencing security alerts or tool downloads; password-protected archive attachments. Files.fm URLs in email body or attachment metadata are a specific delivery IOC for this campaign. If your SIEM has MITRE ATT&CK tagging, prioritize alerting on T1053.005 and T1547.001 in combination with T1566.001 phishing precursor events.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`files.fm`	Cloud hosting platform used for AGEWHEEZE payload delivery infrastructure	MEDIUM
DOMAIN	`ukr.net`	Email platform used to distribute phishing emails impersonating CERT-UA; not inherently malicious — flag emails from this platform impersonating CERT-UA display names	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1219** — Remote Access Tools
- **T1027** — Obfuscated Files or Information
- **T1583.006** — Web Services
- **T1060**
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1113** — Screen Capture
- **T1053.005** — Scheduled Task
- **T1115** — Clipboard Data
- **T1105** — Ingress Tool Transfer
- **T1071.001** — Web Protocols
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1566.001** — Spearphishing Attachment
- **T1059** — Command and Scripting Interpreter
- **T1566.002** — Spearphishing Link

NIST-800-53R5

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

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

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

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1219	Remote Access Tools	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1583.006	Web Services	Resource-Development
T1060		
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1113	Screen Capture	Collection
T1053.005	Scheduled Task	Execution
T1115	Clipboard Data	Collection
T1105	Ingress Tool Transfer	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1566.001	Spearphishing Attachment	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1566.002	Spearphishing Link	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/cert-ua-impersonation-campaign-sp...	T3

Source	URL	Tier
Evil on Schedule: Investigating Malicious Windows Scheduled Tasks	https://www.thedfirspot.com/post/evil-on-schedule-investigating-mal...	T3
[PDF] Ticket: # 705801 - unsolicited email advertising Description	https://www.fcc.gov/sites/default/files/foia-consumer-complaints-09...	T1
UAC-0255 Attack Detection: Threat Actors Impersonate CERT-UA to ...	https://socprime.com/blog/uac-0255-distributing-agewheeze-rat/	T3
UAC-0255 Uses AGEWHEEZE in Fake CERT-UA Alerts - SOC Prime	https://socprime.com/active-threats/cyberattack-uac-0255-from-cert-ua/	T3

Generated 2026-04-01 18:41 UTC by TJS Security Command Center