INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-10 14:42 UTC

Silver Fox Deploys MODBEACON RAT with gRPC/Xray Transport, Detection Requires Protocol-Level Inspection

THREAT CAMPAIGN | HIGH | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0647
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows systems; technology, education, and state-owned enterprise sectors in Asia; C2 infrastructure hosted on Amazon and Cloudflare CDN
Published	2026-07-10T09:15:23
Discovery Source	Rss

Executive Summary

Silver Fox, a China-linked threat cluster, has deployed MODBEACON, a memory-resident, plugin-based remote access trojan written in Rust, that conceals command-and-control traffic inside gRPC streams using open-source Xray/V2Ray proxy code, making it indistinguishable from legitimate cloud traffic to conventional network monitors. Organizations in technology, education, and state-owned enterprise sectors across Asia are the reported targets, with C2 infrastructure hosted on Amazon and Cloudflare CDN to further blend into normal business traffic. The business risk is significant: the fileless, modular architecture evades most endpoint detection tools, CDN-blended C2 defeats perimeter inspection, and the multi-distributor operational model suggests a sustained, coordinated campaign rather than opportunistic intrusion.

Technical Analysis

MODBEACON is a modular, memory-resident remote access trojan written in Rust, attributed with medium confidence to Silver Fox, a China-linked threat cluster. The malware reuses transport code from the open-source Xray/V2Ray anti-censorship proxy framework to tunnel C2 traffic over gRPC (T1071.001, T1095, T1573.002), blending malicious streaming sessions with legitimate cloud service traffic hosted on Amazon and Cloudflare CDN (T1102, T1608.004). The plugin-based, fileless architecture (T1055, T1129, T1620) minimizes host-based detection surface by loading capability modules into memory without writing to disk. Additional techniques include command execution (T1059), obfuscated/encrypted payloads (T1027, T1140), code signing

abuse (T1553), and possible supply-chain or browser extension delivery vectors (T1195.002, T1176). CWE mappings indicate embedded malicious code (CWE-506), protection mechanism bypass (CWE-693), and hidden functionality (CWE-912). No CVE identifier is associated with this campaign. No vendor patch or PSIRT advisory has been identified in the provided source set. Confidence in the core campaign claim is rated MEDIUM. The Hacker News is the sole primary source; CISA advisory AA24-038a covers PRC state-sponsored activity broadly but does not reference Silver Fox or MODBEACON specifically.

Action Checklist

1. Step 1: Containment, Identify all Windows hosts in technology, education, and state-owned enterprise segments with unexplained outbound connections to Amazon (AWS) or Cloudflare IP ranges over ports associated with gRPC (typically TCP 443 with HTTP/2). Isolate hosts exhibiting anomalous memory-resident process behavior pending investigation. Apply network-level blocks on known-bad infrastructure if IOCs are made available by threat intelligence feeds. (NIST AC-4, Information Flow Enforcement; CIS 4.4, Implement and Manage a Firewall on Servers)
2. Step 2: Detection, Deploy protocol-level behavioral inspection capable of analyzing gRPC streaming patterns over HTTPS/HTTP2 to distinguish malicious multiplexed sessions from legitimate CDN traffic (T1071.001, T1095). Query EDR telemetry for memory-resident Rust-compiled binaries, reflective module loading, and process injection events (T1055, T1129, T1620). Review outbound connection logs for sustained, low-volume gRPC streams to Cloudflare and AWS CDN endpoints that lack corresponding business-application justification. Correlate against AU-6 (Audit Record Review) processes and CIS 8.2 (Collect Audit Logs) requirements to ensure gRPC and HTTP/2 traffic is captured in existing log pipelines. D3FEND countermeasure: D3-SFA (System File Analysis) for memory and process artifact review; D3-LAM (Local Account Monitoring) for lateral movement indicators.
3. Step 3: Eradication, No vendor patch applies to this campaign; eradication centers on removing the implant and its persistence mechanism. For confirmed-infected hosts: terminate and remove memory-resident MODBEACON modules, audit Windows service registrations and scheduled tasks for Silver Fox persistence (T1543.003), remove any unauthorized browser extensions (T1176), and revoke credentials accessible from compromised hosts. (NIST AC-2, Account Management; D3FEND: D3-CRO, Credential Rotation)
4. Step 4: Recovery, Reimage confirmed-compromised hosts where feasible. Validate that gRPC inspection controls are operational and logging before returning hosts to production. Rotate all credentials (service accounts, API keys, privileged user accounts) that may have been accessible on affected systems. Confirm outbound connection baselines have returned to expected patterns via network monitoring. (NIST AU-6, Audit Record Review, Analysis, and Reporting; CIS 7.1, Establish and Maintain a Vulnerability Management Process; D3FEND: D3-CRO, Credential Rotation)
5. Step 5: Post-Incident, This campaign exposes control gaps in protocol-level network visibility and reliance on host-based detection alone. Evaluate whether existing network inspection tooling can parse gRPC over HTTP/2 and flag anomalous streaming session characteristics. Assess CDN traffic whitelisting policies, blanket trust of Amazon and Cloudflare IP ranges creates a blind spot this campaign deliberately exploits. Review and update detection engineering runbooks to include gRPC C2 hunting hypotheses. (NIST AU-2, Event Logging; CIS 4.2, Establish and Maintain a Secure Configuration Process for Network Infrastructure; D3-PBWSAM, Proxy-based Web Server Access Mediation)

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if MODBEACON C2 sessions are confirmed active on hosts with access to intellectual property, source code repositories, or regulated data (PII/PHI/financial records), or if lateral movement indicators (new Kerberos ticket requests, SMB authentication from compromised hosts) suggest the implant has pivoted beyond the initially identified segment.
Recovery Notes	Reimaged hosts should not be returned to production until gRPC protocol inspection is confirmed operational and logging on the network path they use for outbound traffic — returning a host to a network segment with the same CDN whitelisting blind spot that enabled initial C2 communication recreates the condition for re-infection. Monitor all recovered hosts and adjacent systems for 30 days post-recovery using Sysmon Event ID 3 and Zeek HTTP/2 logs, with daily review of outbound connection baselines to AWS and Cloudflare CIDRs. Any recurrence of sustained, low-volume TCP 443 streams from non-browser processes to CDN IP ranges should trigger immediate re-isolation and a renewed compromise assessment.
Forensic Artifacts	MODBEACON in-memory plugin modules: recoverable from a RAM image (WinPmem/DumpIt) of the host process carrying the injection — look for Rust-compiled PE sections (presence of 'tokio', 'std::panicking', or 'core::fmt' strings in .rdata) at anomalous virtual address ranges not corresponding to loaded DLLs on disk | Xray/V2Ray gRPC transport frames: captured via Wireshark or Zeek HTTP/2 analyzer as HTTP/2 HEADERS frames with ':path:' values matching Xray gRPC service routes (e.g., '/GunService/Tun') and ':authority:' resolving to AWS or Cloudflare CDN IPs with no corresponding approved business application domain | Windows Scheduled Task XML artifacts: Silver Fox persistence via T1543.003 leaves task definitions under C:\Windows\System32\Tasks\ or HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks — export full XML before eradication to document the persistence mechanism and execution trigger | Sysmon Event ID 7 (ImageLoad) and Event ID 10 (ProcessAccess) logs: record reflective loading of MODBEACON plugin modules into a host process at runtime — these events capture the source image path (or absence thereof for reflectively loaded modules) and the target process handle access rights used during injection | Windows Security Event Log Event ID 4648 and Event ID 4624 records: document credential access patterns during the MODBEACON dwell period — specifically, logon events from the compromised host process to other internal systems that would indicate lateral movement or credential harvesting activity attributable to the Silver Fox operator

Per-Action IR Details

Step 1: Containment — Identify all Windows hosts in technology, education, and state-owned enterprise segments with unexplained outbound connections to Amazon (AWS) or Cloudflare IP ranges over ports associated with gRPC (typically TCP 443 with HTTP/2). Isolate hosts exhibiting anomalous memory-resident process behavior pending investigation. Apply network-level blocks on known-bad infrastructure if IOCs are made available by threat intelligence feeds. (NIST AC-4 — Information Flow Enforcement; CIS 4.4 — Implement and Manage a Firewall on Servers)

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'Get-NetTCPConnection -State Established | Where-Object { $_.RemotePort -eq 443 } | Select-Object LocalAddress, LocalPort, RemoteAddress, OwningProcess' on each host to surface HTTP/2 connections

on TCP 443. Cross-reference RemoteAddress values against published AWS and Cloudflare CIDR lists (ip-ranges.amazonaws.com/ip-ranges.json and cloudflare.com/ips). Use Windows Firewall with Advanced Security (netsh advfirewall) to block outbound TCP 443 to flagged CIDRs on isolated segments while investigation proceeds. Wireshark with http2 display filter on a network tap can confirm gRPC framing (SETTINGS and HEADERS frames) on flagged connections.

Evidence: Before isolating any host, capture: (1) full RAM image using WinPmem or DumpIt to preserve MODBEACON's memory-resident Rust modules and any decrypted gRPC session keys held in process heap; (2) 'Get-NetTCPConnection' and 'netstat -ano' output with owning PID to record all active outbound connections to AWS/Cloudflare CDN ranges; (3) 'Get-Process' dump listing all running processes with parent-child relationships to identify the host process carrying the injected MODBEACON module; (4) a live packet capture (Wireshark/tcpdump) of at least 60 seconds on the suspect interface to record the gRPC stream framing and TLS SNI values before the session is torn down by isolation.

Step 2: Detection — Deploy protocol-level behavioral inspection capable of analyzing gRPC streaming patterns over HTTPS/HTTP2 to distinguish malicious multiplexed sessions from legitimate CDN traffic (T1071.004, T1095). Query EDR telemetry for memory-resident Rust-compiled binaries, reflective module loading, and process injection events (T1055, T1129, T1620). Review outbound connection logs for sustained, low-volume gRPC streams to Cloudflare and AWS CDN endpoints that lack corresponding business-application justification. Correlate against AU-6 (Audit Record Review) processes and CIS 8.2 (Collect Audit Logs) requirements to ensure gRPC and HTTP/2 traffic is captured in existing log pipelines. D3FEND countermeasure: D3-SFA (System File Analysis) for memory and process artifact review; D3-LAM (Local Account Monitoring) for lateral movement indicators.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), D3-SFA (System File Analysis), D3-LAM (Local Account Monitoring)

Compensating: Deploy Sysmon with a config capturing Event ID 7 (ImageLoad) and Event ID 10 (ProcessAccess) to detect reflective loading of MODBEACON plugins into a host process. Write a YARA rule targeting Rust binary characteristics (magic bytes 'MZ' with '.rdata' section strings containing 'core::panicking' or 'tokio' async runtime markers common in Rust-compiled tooling) and run it against all process memory dumps using YARA-X or the Windows Defender offline scan engine. Use Zeek (formerly Bro) with the http2 analyzer enabled on a network tap to log HTTP/2 HEADERS frames — filter for streams where the ':authority' pseudo-header resolves to AWS or Cloudflare IPs but carries no recognizable SaaS application user-agent string. Sigma rule: detect Sysmon Event ID 3 (Network Connection) where DestinationPort=443, Initiated=true, and the initiating process is not a known browser or business application.

Evidence: This is an analysis step that does not itself alter live state, but analysts must preserve artifacts before any subsequent containment action. Collect: (1) Sysmon Event ID 1 (Process Create) logs for any process spawning from unusual parent chains (e.g., a Windows service or scheduled task spawning a Rust binary); (2) Sysmon Event ID 7 (Image Loaded) entries for unsigned or anomalously-named DLLs loaded into candidate host processes; (3) Windows Security Event Log Event ID 4688 (Process Creation) with full command-line auditing enabled, filtering on processes not in the approved software inventory; (4) HTTP/2 HEADERS frame logs from Zeek showing gRPC ':method: POST' and ':path:' values consistent with Xray/V2Ray gRPC service endpoints (e.g., '/grpc.service.v1.GunService/Tun').

Step 3: Eradication — No vendor patch applies to this campaign; eradication centers on removing the implant and its persistence mechanism. For confirmed-infected hosts: terminate and remove memory-resident MODBEACON modules, audit Windows service registrations and scheduled tasks for Silver Fox persistence (T1543.003), remove any unauthorized browser extensions (T1176), and revoke credentials accessible from compromised hosts. (NIST AC-2 — Account Management; D3FEND: D3-CRO — Credential Rotation)

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), D3-CRO (Credential Rotation)

Compensating: Before terminating processes, use Process Hacker (free) to dump the full memory of the suspect process and export its module list — this preserves MODBEACON plugin evidence. Run 'schtasks /query /fo LIST /v > schtasks_export.txt' and 'sc query type= all state= all > services_export.txt' to enumerate all scheduled tasks and services for anomalous Silver Fox entries (look for tasks with actions pointing to %APPDATA%, %TEMP%, or unusual Rust binary paths). Audit installed browser extensions via 'Get-ChildItem -Recurse "$env:LOCALAPPDATA\Google\Chrome\User Data\Default\Extensions"' and compare against a known-good baseline. Use Autoruns (Sysinternals) to identify all persistence locations and cross-reference with VirusTotal hashes before removal.

Evidence: Before terminating MODBEACON processes or removing persistence artifacts, capture: (1) full memory dump of the host process carrying the injected MODBEACON module (WinPmem/DumpIt) — the in-memory plugin framework will not survive process termination; (2) export of all Windows service binPaths and scheduled task XML definitions ('schtasks /query /xml') to document Silver Fox persistence entries before deletion; (3) a copy of any browser extension directories flagged as unauthorized, including manifest.json and background scripts, to support post-incident attribution; (4) Windows Security Event Log Event ID 4648 (Logon with explicit credentials) and Event ID 4624 (Logon) entries from the compromise window to establish which accounts were accessed by the implant before credential revocation.

Step 4: Recovery — Reimage confirmed-compromised hosts where feasible. Validate that gRPC inspection controls are operational and logging before returning hosts to production. Rotate all credentials (service accounts, API keys, privileged user accounts) that may have been accessible on affected systems. Confirm outbound connection baselines have returned to expected patterns via network monitoring. (NIST AU-6 — Audit Record Review, Analysis, and Reporting; CIS 7.1 — Establish and Maintain a Vulnerability Management Process; D3FEND: D3-CRO — Credential Rotation)

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), D3-CRO (Credential Rotation)

Compensating: Reimage from a known-good golden image stored offline or in an immutable snapshot — do not restore from a backup taken after the earliest estimated MODBEACON implant date. Before returning a host to production, run Sysmon and the YARA rule set (Rust binary signatures, Xray gRPC path patterns) against the freshly imaged host to confirm absence of re-infection. Use 'netstat -ano' on day 1, 3, and 7 post-recovery to verify no new sustained TCP 443 streams to AWS/Cloudflare CIDRs appear from processes not in the approved application list. Credential rotation: use a password manager or AD bulk-reset script ('Set-ADAccountPassword') for all accounts whose NTLM hashes or Kerberos tickets may have been resident in LSASS memory on compromised hosts.

Evidence: Before reimaging, ensure the following have been preserved from the compromised host: (1) a final full disk image (using dcfldd or FTK Imager) to support any later forensic review or legal hold requirements; (2) all Windows Event Logs exported in .evtx format (Security, System, Application, Sysmon operational log) covering the full compromise window; (3) a copy of the MODBEACON implant binary or memory dump if recovered, stored in a password-protected container for malware analysis; (4) network flow logs (NetFlow/IPFIX or Zeek conn.log) covering the period of C2 activity to document the full scope of data potentially exfiltrated over gRPC streams to AWS/Cloudflare infrastructure.

Step 5: Post-Incident — This campaign exposes control gaps in protocol-level network visibility and reliance on host-based detection alone. Evaluate whether existing network inspection tooling can parse gRPC over HTTP/2 and flag anomalous streaming session characteristics. Assess CDN traffic whitelisting policies — blanket trust of Amazon and Cloudflare IP ranges creates a blind spot this campaign deliberately exploits. Review and update detection engineering runbooks to include gRPC C2 hunting hypothesis. (NIST AU-2 — Event Logging; CIS 4.2 — Establish and Maintain a Secure Configuration Process for Network Infrastructure; D3-PBWSAM — Proxy-based Web Server Access Mediation)

NIST Phase: Post Incident

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

Controls: NIST AU-2 (Event Logging), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), D3-PBWSAM (Proxy-based Web Server Access Mediation)

Compensating: Document a gRPC C2 hunting hypothesis in the IR runbook: hunt for outbound HTTP/2 sessions to AWS/Cloudflare IPs where the TLS SNI does not match any approved SaaS application domain, stream duration exceeds 10 minutes with low data volume (characteristic of MODBEACON beacon keep-alive), and the initiating process is not a recognized browser or business application binary. Replace blanket CDN IP allowlisting with domain-based allowlisting enforced through a proxy (Squid or mitmproxy in transparent mode) so that only approved FQDNs within AWS/Cloudflare space are permitted. Add Zeek HTTP/2 analyzer output and Sysmon Event ID 3 (network connection) logs to whatever log aggregation is in use (ELK stack free tier, Graylog CE) to ensure gRPC traffic is captured going forward.

Evidence: Post-incident artifact review should include: (1) retrospective analysis of Zeek conn.log and http.log (or equivalent) for the 90 days preceding detection, hunting for the gRPC session pattern (long-duration, low-byte-count, HTTP/2 POST to Xray/V2Ray service paths) to establish true dwell time; (2) comparison of the MODBEACON sample (if recovered) against open-source Xray/V2Ray gRPC transport code to document the specific protocol obfuscation technique for detection engineering purposes; (3) review of Windows Prefetch files (C:\Windows\Prefetch\) and Shimcache (SYSTEM hive AppCompatCache) on affected hosts to identify any MODBEACON loader or dropper execution that preceded the memory-resident stage and may have been missed in initial triage.

Detection Guidance

Conventional signature-based and host-only detection is insufficient against MODBEACON. Detection requires protocol-level behavioral analysis of gRPC traffic (HTTP/2 over TCP 443). Key indicators to hunt: (1) Outbound HTTP/2 connections to Cloudflare or AWS CDN IP ranges with gRPC content-type headers ('application/grpc') that are not attributable to a known business application, sustained streaming sessions with low data volume and regular beacon intervals are particularly suspicious. (2) Memory-resident processes with no corresponding on-disk binary, especially those loading plugin modules reflectively (T1055, T1129, T1620), query EDR for process injection into legitimate Windows processes without associated file paths. (3) Windows service creation or modification events (Event ID 7045, T1543.003) with unusual binary paths or signed-but-anomalous executables (T1553). (4) Outbound non-repudiation gaps: gRPC streams that persist across expected application session boundaries. (5) Browser extension installations (T1176) not present in software inventory baselines (CIS 2.1). Behavioral hunting hypothesis: 'Host initiates gRPC streaming session to CDN-hosted IP with no user-interactive application context, session persists beyond 10 minutes.' MITRE techniques to prioritize in detection rule coverage: T1071.001 (Application Layer Protocol: Web Protocols), T1095 (Non-Application Layer Protocol), T1573.002 (Encrypted Channel: Asymmetric Cryptography), T1027 (Obfuscated Files or Information), T1102 (Web Service). D3FEND countermeasures: D3-SFA (System File Analysis), D3-LAM (Local Account Monitoring), D3-PBWSAM (Proxy-based Web Server Access Mediation).

Framework Mappings

MITRE-ATTACK

- **T1195.002** — Compromise Software Supply Chain
- **T1543.003** — Windows Service
- **T1071.004** — DNS
- **T1055** — Process Injection
- **T1105** — Ingress Tool Transfer

- **T1059** — Command and Scripting Interpreter
- **T1071.001** — Web Protocols
- **T1608.004** — Drive-by Target
- **T1140** — Deobfuscate/Decode Files or Information
- **T1095** — Non-Application Layer Protocol
- **T1027** — Obfuscated Files or Information
- **T1176** — Software Extensions
- **T1071.002** — File Transfer Protocols
- **T1129** — Shared Modules
- **T1553** — Subvert Trust Controls
- **T1573.002** — Asymmetric Cryptography
- **T1620** — Reflective Code Loading
- **T1102** — Web Service

NIST-800-53R5

- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1195.002	Compromise Software Supply Chain	Initial-Access
T1543.003	Windows Service	Persistence
T1071.004	DNS	Command-And-Control
T1055	Process Injection	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1059	Command and Scripting Interpreter	Execution
T1071.001	Web Protocols	Command-And-Control
T1608.004	Drive-by Target	Resource-Development
T1140	Deobfuscate/Decode Files or Information	Defense-Evasion
T1095	Non-Application Layer Protocol	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1176	Software Extensions	Persistence
T1071.002	File Transfer Protocols	Command-And-Control
T1129	Shared Modules	Execution
T1553	Subvert Trust Controls	Defense-Evasion
T1573.002	Asymmetric Cryptography	Command-And-Control
T1620	Reflective Code Loading	Defense-Evasion
T1102	Web Service	Command-And-Control

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/new-modbeacon-rat-uses-grpc-strea...	T2
Asia's Digital Economy and the Cloudflare Wake-Up Call	https://asiatechdaily.com/asias-digital-economy-and-the-cloudflare-...	T3
Shadow-Earth-053 targets Asian government, defense, critical ...	https://industrialcyber.co/ransomware/shadow-earth-053-targets-asia...	T2

Source	URL	Tier
PRC State-Sponsored Actors Compromise and Maintain Persistent ...	https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a	**T1**

Generated 2026-07-10 14:42 UTC by TJS Security Command Center