INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-08 18:47 UTC

Chaos Botnet Pivots to Cloud Infrastructure, Adds SOCKS Proxy to Expand Monetization Beyond DDoS

THREAT CAMPAIGN | HIGH | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0159
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Misconfigured Hadoop deployments (exposed RCE), Linux/cloud server environments; prior variants targeted routers and edge devices
Published	2026-04-08T13:51:00
Discovery Source	Rss

Executive Summary

A new Chaos botnet variant is actively compromising misconfigured cloud servers, with a primary focus on Hadoop instances exposing unauthenticated remote code execution endpoints. The variant has been retooled to deploy SOCKS proxy capabilities, expanding attacker monetization beyond cryptomining and DDoS-for-hire to include traffic laundering and infrastructure rental. Organizations running exposed Hadoop or Linux cloud workloads without authentication controls are at direct risk of silent compromise and potential use as attacker relay infrastructure.

Technical Analysis

This Chaos variant targets Linux-based cloud environments, specifically Hadoop deployments with exposed RCE endpoints (CWE-284: Improper Access Control; CWE-306: Missing Authentication for Critical Function). Initial access is achieved via exploitation of publicly exposed services (MITRE T1190). The variant drops SSH propagation and router exploitation modules present in prior versions, replacing them with a SOCKS proxy module (T1090, T1572) used to tunnel attacker traffic through compromised hosts. Ingress tooling is retrieved post-compromise (T1105), and a Linux shell script is used for execution (T1059.004). The malware employs obfuscation (T1027) and file deletion to reduce forensic footprint (T1070.004). Prior variants deployed cryptomining payload (T1496); this variant prioritizes SOCKS proxy monetization but may retain resource hijacking capability. Infrastructure overlaps consistent with Silver Fox, a Chinese cybercrime group associated with ValleyRAT (T1583, T1583.001), have been observed; attribution remains unconfirmed. No CVE is currently

assigned. Relevant CWEs: CWE-284, CWE-306, CWE-16 (Configuration). No vendor patch exists for this malware; remediation is configuration-based. Source: Darktrace direct detection reporting, April 2026.

Action Checklist

1. Step 1: Containment, Immediately audit all cloud-hosted Hadoop deployments for publicly exposed RCE-capable endpoints (YARN ResourceManager, JobTracker, WebHDFS). Block inbound access to Hadoop management ports (default: 8088, 8032, 50070, 14000) at the network perimeter or cloud security group level. Isolate any hosts showing unexpected outbound SOCKS proxy traffic or connections to unknown external IPs.
2. Step 2: Detection, Query cloud and host-level logs for unexpected processes spawning from Hadoop service accounts. Look for outbound connections on non-standard high ports consistent with SOCKS proxy behavior. Search for ingress tool transfer patterns: wget or curl commands downloading binaries to /tmp or world-writable directories. Review authentication logs for any unauthenticated access to Hadoop REST APIs. Correlate with Darktrace-published IOCs from their April 2026 detection blog.
3. Step 3: Eradication, Enable authentication and authorization on all Hadoop services (Kerberos for YARN, HDFS; configure hadoop.security.authentication). Remove world-accessible Hadoop management interfaces from public network exposure. Terminate and reimage any confirmed compromised hosts rather than attempting in-place cleanup, as the variant actively deletes forensic artifacts (T1070.004). Audit and revoke any cloud IAM credentials accessible from compromised instances.
4. Step 4: Recovery, After reimaging, validate Hadoop authentication configuration against CIS Benchmarks for Hadoop or vendor hardening guides before returning to production. Monitor reinstated hosts for 72 hours for recurrence of outbound proxy traffic or unexpected child processes from Hadoop service accounts. Confirm cloud security group rules are enforced and no Hadoop management ports are publicly reachable via an external port scan.
5. Step 5: Post-Incident, This campaign exposes a persistent control gap: cloud workload misconfiguration review is not integrated into deployment pipelines. Implement infrastructure-as-code scanning (e.g., checkov, tfsec) to flag exposed service ports and missing authentication configs pre-deployment. Map control gap to NIST SP 800-53 CM-6 (Configuration Settings) and CM-7 (Least Functionality). If Silver Fox infrastructure overlap is confirmed in your environment, escalate to threat intelligence team for broader ValleyRAT exposure assessment.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if: any cloud IAM role credential harvested from a compromised Hadoop instance shows subsequent API activity (indicating lateral movement or data exfiltration from cloud storage); if HDFS data accessible from the compromised cluster contains PII, PHI, or PCI-scoped data triggering breach notification requirements; or if Silver Fox infrastructure IOC overlap is confirmed, indicating potential nation-state attribution requiring regulatory and executive notification.

Recovery Notes	After reimaging, do not return Hadoop hosts to production until Kerberos authentication is validated end-to-end with a test kinit/klist cycle and an attempted unauthenticated REST API call to YARN ResourceManager (:8088/ws/v1/cluster/apps) returns HTTP 403 from an external IP. Monitor reinstated hosts for a minimum of 72 hours using continuous YARN ResourceManager log tailing and outbound connection monitoring focused on high-port SOCKS proxy patterns, as the Chaos botnet has demonstrated re-exploitation of insufficiently hardened hosts within hours of reimage if network exposure is not fully remediated. Validate cloud security group changes persist across any infrastructure automation runs by testing with an external nmap scan post-deployment, as IaC pipeline re-runs have been known to revert manual security group modifications.
Forensic Artifacts	YARN ResourceManager REST API access logs at '/var/log/hadoop-yarn/hadoop-yarn-resourcemanager-.log' — contains the initial exploit HTTP POST to '/ws/v1/cluster/apps/new-application' and '/ws/v1/cluster/apps' with the malicious shell command payload in the 'commands' field of the AM container spec; the source IP in these logs is the initial Chaos botnet exploitation node. | YARN NodeManager container working directories at '/var/log/hadoop-yarn/containers/application_/container_/' — contains stdout and stderr of the malicious YARN application container execution, capturing the exact shell command used to download and execute the Chaos ELF binary dropper (typically a wget/curl one-liner to a remote IP targeting /tmp). | Deleted-but-running ELF binary reference in '/proc//exe' showing path as '/tmp/ (deleted)' — the Chaos variant unlinks its dropper from /tmp immediately after execution to evade file-based detection (MITRE T1070.004); the process map at '/proc//maps' and binary content recoverable via 'cp /proc//exe /tmp/chaos_recovered.elf' before process termination. | Cloud provider VPC Flow Logs showing outbound connections from the compromised Hadoop host on high ephemeral ports (typically 1080 or randomly selected high ports above 10000) to external IPs at high frequency — these represent the SOCKS5 proxy relay traffic pattern and will show a distinct many-to-one or one-to-many external IP communication pattern inconsistent with normal Hadoop cluster traffic. | Cloud instance metadata service access logs (AWS IMDSv1: 169.254.169.254 in VPC Flow Logs; AWS IMDSv2: token request headers in proxy logs if captured) — the Chaos variant harvests cloud instance role credentials via the metadata endpoint to enable lateral movement to other cloud resources; presence of HTTP GET to 169.254.169.254/latest/meta-data/iam/security-credentials/ from the Hadoop host process UID during the compromise window confirms credential harvesting.

Per-Action IR Details

Step 1: Containment — Immediately audit all cloud-hosted Hadoop deployments for publicly exposed RCE-capable endpoints (YARN ResourceManager, JobTracker, WebHDFS). Block inbound access to Hadoop management ports (default: 8088, 8032, 50070, 14000) at the network perimeter or cloud security group level. Isolate any hosts showing unexpected outbound SOCKS proxy traffic or connections to unknown external IPs.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), 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: For teams without a cloud SIEM: run 'nmap -sV -p 8088,8032,50070,14000 --open ' from an external vantage point to enumerate exposed Hadoop ports across your cloud footprint before modifying security groups. On the host, use 'ss -tulnp | grep -E "8088|8032|50070|14000"' to confirm which process is binding each port. For outbound SOCKS proxy detection without EDR, run 'ss -tnp state established | awk "{print $5}" | cut -d: -f1 | sort | uniq

-c | sort -rn' on each Hadoop host to surface high-frequency outbound connection destinations; manually resolve top IPs against threat intel feeds (e.g., AbuseIPDB CLI or GreyNoise community API). Isolate suspect hosts by modifying cloud security group egress rules to deny-all except approved management CIDRs.

Evidence: Before modifying any security group or firewall rule, capture a full snapshot of current cloud security group/ACL configurations (AWS: 'aws ec2 describe-security-groups --output json'; GCP: 'gcloud compute firewall-rules list --format=json') to preserve the pre-incident exposure state. Capture live network connections from each Hadoop host: 'ss -tnp > /tmp/connections_$(hostname)_$(date +%Y%m%dT%H%M%S).txt' and 'netstat -antp >> /tmp/connections_$(hostname)_$(date +%Y%m%dT%H%M%S).txt'. Dump active listening services: 'ps aux > /tmp/proctree_$(hostname)_$(date +%Y%m%dT%H%M%S).txt'. These capture the SOCKS proxy listener process and outbound C2 connections before network isolation destroys live state. On AWS, preserve VPC Flow Logs for the 48 hours preceding discovery — these will contain the inbound exploit HTTP POST to YARN ResourceManager (:8088/ws/v1/cluster/apps/new-application and /ws/v1/cluster/apps) and subsequent outbound binary download connections.

Step 2: Detection — Query cloud and host-level logs for unexpected processes spawning from Hadoop service accounts. Look for outbound connections on non-standard high ports consistent with SOCKS proxy behavior. Search for ingress tool transfer patterns: wget or curl commands downloading binaries to /tmp or world-writable directories. Review authentication logs for any unauthenticated access to Hadoop REST APIs. Correlate with Darktrace-published IOCs from their April 2026 detection blog.

NIST Phase: Detection Analysis

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

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

Compensating: Without a SIEM, deploy auditd on each Hadoop host with rules targeting the hadoop service account UID: 'auditctl -a always,exit -F arch=b64 -F uid= -S execve -k chaos_exec'. Parse results with 'ausearch -k chaos_exec --start today | aureport -x --summary'. For YARN REST API abuse detection without WAF logging, parse the YARN ResourceManager log directly: 'grep -E "POST.*(new-application|submit-application)" /var/log/hadoop-yarn/hadoop-yarn-resourcemanager-*.log | grep -v "'". To hunt for Chaos dropper activity, run: 'find /tmp /var/tmp /dev/shm -type f -newer /proc/1 -perm /111 2>/dev/null' to identify recently written executables. Use YARA with a rule matching the Chaos botnet ELF signature (look for the string "socks5" or SOCKS5 handshake byte sequences 0x05, 0x01, 0x00 in ELF binaries) against /tmp artifacts. Deploy the Sigma rule targeting 'hadoop' parent process spawning 'bash','sh','wget','curl','chmod' (map to auditd execve events).

Evidence: Collect YARN ResourceManager application submission logs at '/var/log/hadoop-yarn/hadoop-yarn-resourcemanager-.log' — the Chaos botnet exploits YARN's unauthenticated REST API by submitting a malicious application that executes a shell command; look for POST requests to '/ws/v1/cluster/apps/new-application' and '/ws/v1/cluster/apps' from external IP addresses with a shell command payload in the 'am-container-spec' field. Collect '/var/log/auth.log' or '/var/log/secure' for su/sudo events under the yarn or hdfs service accounts at the time of initial exploitation. Capture bash_history for the hadoop, yarn, and hdfs OS users: '/home/yarn/.bash_history', '/var/lib/hadoop-yarn/.bash_history'. Retrieve cloud provider access logs: AWS CloudTrail for any IAM role assumption or credential API calls (GetCallerIdentity, AssumeRole) originating from the compromised instance's IP after the initial exploit window. Capture '/proc//exe', '/proc//cmdline', and '/proc//net/tcp6' before process termination to document the SOCKS proxy listener port binding. Note: the Darktrace April 2026 IOC blog reference cannot be verified from current knowledge base — treat IOCs from that source as unverified until human-validated against the published post.

Step 3: Eradication — Enable authentication and authorization on all Hadoop services (Kerberos for YARN, HDFS; configure hadoop.security.authentication). Remove world-accessible Hadoop management interfaces from public network exposure. Terminate and reimage any confirmed compromised hosts rather than attempting in-place cleanup, as the variant actively deletes forensic artifacts (T1070.004). Audit and revoke any cloud IAM credentials accessible from compromised instances.

NIST Phase: Eradication

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

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST IA-2 (Identification and Authentication — Organizational Users), NIST CM-6 (Configuration Settings), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Before reimaging, take a forensic memory snapshot using LiME (Linux Memory Extractor) loaded as a kernel module to capture the Chaos botnet implant in-memory before it completes artifact deletion: 'insmod lime-.ko path=/mnt/evidence/mem_$(hostname).lime format=lime'. Hash the dump immediately: 'sha256sum /mnt/evidence/mem_$(hostname).lime > /mnt/evidence/mem_$(hostname).lime.sha256'. For IAM credential revocation without a CSPM tool, on AWS run: 'aws iam list-instance-profiles' to identify roles attached to compromised instances, then 'aws iam create-policy-version' to attach a deny-all policy immediately, followed by full role audit. For Kerberos configuration validation on a budget, use the Hadoop built-in 'hadoop checknative' and review 'core-site.xml' for 'hadoop.security.authentication=kerberos' and 'hadoop.security.authorization=true' prior to service restart post-eradication.

Evidence: Before terminating the instance, preserve the following artifacts specific to Chaos botnet T1070.004 (Indicator Removal: File Deletion) behavior: run 'find /tmp /var/tmp /dev/shm -maxdepth 3 -type f 2>/dev/null' and hash all findings — the Chaos variant downloads its ELF binary to /tmp, executes it, then unlinks the file while keeping the process running (detectable via '/proc//exe' pointing to a deleted path, shown as '/tmp/ (deleted)'). Capture 'ls -la /proc/*/exe 2>/dev/null | grep deleted' output. Collect the YARN NodeManager container launch logs at '/var/log/hadoop-yarn/containers/' — these directories contain stdout/stderr of each YARN application container execution, including the malicious shell payload that bootstrapped the Chaos implant. Enumerate and document all cloud instance metadata API calls from the host during the compromise window using cloud provider logs (AWS: CloudTrail 'GetMetadata' equivalent via VPC flow logs to 169.254.169.254) to determine if the implant harvested the instance role credentials — this is critical before determining the blast radius of IAM revocation.

Step 4: Recovery — After reimaging, validate Hadoop authentication configuration against CIS Benchmarks for Hadoop or vendor hardening guides before returning to production. Monitor reinstated hosts for 72 hours for recurrence of outbound proxy traffic or unexpected child processes from Hadoop service accounts. Confirm cloud security group rules are enforced and no Hadoop management ports are publicly reachable via an external port scan.

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 CM-6 (Configuration Settings), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: For configuration validation without a commercial hardening scanner, use the open-source Lynis tool ('lynis audit system') on the reimaged Hadoop host and review the Authentication and Networking sections. Manually validate Hadoop config files post-reimage: 'grep -E "authentication|authorization|security" /etc/hadoop/conf/core-site.xml /etc/hadoop/conf/hdfs-site.xml /etc/hadoop/conf/yarn-site.xml' — confirm 'hadoop.security.authentication' is set to 'kerberos' (not 'simple') and 'hadoop.security.authorization' is 'true'. For the 72-hour monitoring window without EDR, deploy a cron job running every 5 minutes that checks for new executables under the hadoop UID and unexpected outbound SOCKS connections: 'crontab -e' adding '*/5 * * * * ss -tnp state established | grep >> /var/log/hadoop_conn_monitor.log'. Validate external exposure by running an nmap scan from a non-internal IP: 'nmap -Pn -p 8088,8032,50070,14000 ' — all four ports must return filtered or closed.

Evidence: During the 72-hour monitoring window, collect continuous snapshots of YARN ResourceManager application submission activity: 'tail -f /var/log/hadoop-yarn/hadoop-yarn-resourcemanager-.log | grep -E "(POST|application_submit|ACCEPTED|RUNNING)"' — any new unauthenticated application submission indicates re-exploitation or a missed exposure. Preserve cloud security group audit trail logs showing the point-in-time rule changes applied during containment (AWS: CloudTrail 'AuthorizeSecurityGroupIngress'/'RevokeSecurityGroupIngress' events) as documentation of remediation actions taken, satisfying NIST AU-11 (Audit Record Retention) requirements. Capture a post-reimage baseline of all listening processes: 'ss -tulnp > /tmp/baseline_postrecovery_$(date +%Y%m%dT%H%M%S).txt' for comparison during the monitoring window.

Step 5: Post-Incident — This campaign exposes a persistent control gap: cloud workload misconfiguration review is not integrated into deployment pipelines. Implement infrastructure-as-code scanning (e.g., checkov, tfsec) to flag exposed service ports and missing authentication configs pre-deployment. Map gap to NIST SP 800-53 CM-6 (Configuration Settings) and CM-7 (Least Functionality). If Silver Fox infrastructure overlap is confirmed in your environment, escalate to threat intelligence team for broader ValleyRAT exposure assessment.

NIST Phase: Post Incident

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

Controls: NIST CM-6 (Configuration Settings), NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), 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: Integrate checkov (free, open-source) into the CI/CD pipeline with a check policy targeting Hadoop-related Terraform or CloudFormation templates: 'checkov -d ./terraform --check CKV_AWS_25' (Security Group unrestricted ingress) and write a custom checkov check that flags any security group resource permitting inbound 0.0.0.0/0 on ports 8088, 8032, 50070, or 14000. For teams without a formal threat intel platform, create a structured lessons-learned document mapping this Chaos botnet incident to MITRE ATT&CK T1190 (Exploit Public-Facing Application) for initial access, T1071 (Application Layer Protocol) for C2, T1496 (Resource Hijacking) for cryptomining, and T1070.004 (Indicator Removal: File Deletion) for defense evasion — use this as the detection engineering backlog to write Sigma rules for each technique. For Silver Fox/ValleyRAT overlap assessment without a commercial TI platform, query open sources including VirusTotal community, OTX AlienVault, and MISP public feeds for Silver Fox infrastructure IOCs and cross-reference against your VPC Flow Logs and DNS query logs from the incident window.

Evidence: Compile a complete incident timeline from YARN ResourceManager logs (first malicious POST timestamp), VPC Flow Logs (first outbound SOCKS proxy connection), and CloudTrail (first IAM API call from the compromised instance) to establish the true dwell time — this is the primary metric for the lessons-learned report and regulatory disclosure determination. Preserve all collected IOCs (process hashes, C2 IPs, SOCKS proxy destination IPs, malicious YARN application payloads) in a structured format (STIX 2.1 or CSV) for sharing with sector ISACs and for seeding future detection rules. If Silver Fox infrastructure overlap is identified through IOC correlation, preserve the full evidence package (memory dumps, network captures, YARN container logs) under legal hold, as ValleyRAT attribution may implicate nation-state actors and could trigger mandatory reporting obligations depending on sector — escalation to legal counsel is warranted before public disclosure.

Detection Guidance

Primary behavioral indicators: (1) Hadoop service account (e.g., 'yarn', 'hdfs') spawning shell processes or executing wget/curl to external IPs, check Linux auditd logs or cloud host-level process telemetry. (2) Outbound TCP connections on high ports (typically 1080, 1081, or randomized high ports) from cloud instances that do not normally proxy traffic, review VPC flow logs or cloud firewall logs. (3) New binaries written to /tmp, /dev/shm, or other world-writable paths followed by immediate execution, correlate file creation and process execution events. (4) Evidence of T1070.004: file deletion events immediately after binary execution, particularly in temp directories. (5) Inbound HTTP requests to Hadoop YARN ResourceManager REST API (port 8088, path /ws/v1/cluster/apps/new-application) without authentication headers from external IPs, this is a known RCE trigger pattern for YARN exploitation. SIEM query focus: process parent-child chains where parent is a Hadoop JVM process and child is /bin/bash or /bin/sh executing a download command. Cross-reference outbound destination IPs against Darktrace-published IOCs (April 2026 blog). No public YARA or Sigma rules confirmed available at time of this writing; monitor Darktrace blog and threat intel feeds for rule releases.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Darktrace April 2026 blog — specific IOCs not confirmed extractable from training data`	Darktrace published direct detection IOCs including IPs and hashes in their April 2026 campaign report. Retrieve from source.	LOW
DOMAIN	`[not available — no confirmed IOC values in source data provided]`	No specific domain IOCs were included in the item data. Consult Darktrace and Help Net Security April 2026 reporting for confirmed indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1496** — Resource Hijacking
- **T1071** — Application Layer Protocol
- **T1583** — Acquire Infrastructure
- **T1070.004** — File Deletion
- **T1583.001** — Domains
- **T1090** — Proxy
- **T1190** — Exploit Public-Facing Application
- **T1572** — Protocol Tunneling
- **T1027** — Obfuscated Files or Information
- **T1105** — Ingress Tool Transfer
- **T1059.004** — Unix Shell

NIST-800-53R5

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

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

NIST-CSF-2

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

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1496	Resource Hijacking	Impact
T1071	Application Layer Protocol	Command-And-Control
T1583	Acquire Infrastructure	Resource-Development
T1070.004	File Deletion	Defense-Evasion
T1583.001	Domains	Resource-Development
T1090	Proxy	Command-And-Control
T1190	Exploit Public-Facing Application	Initial-Access
T1572	Protocol Tunneling	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1059.004	Unix Shell	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/new-chaos-variant-targets-misconf...	T3
New Chaos Malware Variant found Exploiting Misconfigurations in ...	https://www.darktrace.com/blog/darktrace-identifies-new-chaos-malwa...	T3
Chaos malware expands from routers to Linux cloud servers	https://www.helpnetsecurity.com/2026/04/08/chaos-malware-cloud-misc...	T3
RST Cloud	https://x.com/rst_cloud/status/2041879748230418676	T3
Linux Malware targets misconfigured misconfigured Apache ...	https://securityaffairs.com/160093/hacking/linux-malware-cryptocurr...	T3

Generated 2026-04-08 18:47 UTC by TJS Security Command Center