INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-29 06:53 UTC

Ransomware Groups 0APT and KryBit Turn on Each Other, Exposing Infrastructure and Operations

THREAT ACTOR | MEDIUM | CVSS 5.0

SCC Item ID	SCC-TAC-2026-0013
Type	Threat Actor
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	No specific products identified; exposure targets ransomware group infrastructure and operational tooling
Published	2026-04-28T16:13:30
Discovery Source	Rss

Executive Summary

Two ransomware groups, 0APT and KryBit, turned on each other and publicly leaked each other's internal data, including command-and-control infrastructure, hosting details, and operational methods. This specific incident did not target commercial organizations, but the leaked infrastructure data gives defenders an uncommon window into active ransomware tooling and tradecraft. Organizations should treat this as defensive intelligence to pre-block attack infrastructure before 0APT and KryBit launch campaigns against commercial targets. Confidence in specific technical details remains low; this item is sourced from a single trade publication with no corroboration from CISA, MITRE, or other authoritative bodies at this time.

Technical Analysis

0APT and KryBit, two ransomware threat actors, engaged in a public retaliatory exchange that resulted in each group leaking the other's internal operational data. Disclosed material reportedly includes command-and-control (C2) endpoints, hosting provider information, internal communication channel identifiers, and operational tradecraft details. MITRE ATT&CK techniques associated with this actor profile include: Gather Victim Org Information (T1591), Compromise Infrastructure (T1584), Phishing (T1566), Acquire Infrastructure (T1583), Valid Accounts (T1078), Data Encrypted for Impact (T1486), and Gather Victim Network Information (T1590). No CVE, CWE, or CVSS data applies to this incident; the source-assigned CVSS score of 5.0 is not a valid application of CVSS methodology and is not adopted here. No specific commercial products are confirmed

affected. Primary sourcing is a single Dark Reading article (Tier 3); no independent corroboration from CISA, MITRE ATT&CK, or NVD has been identified. All specific technical claims should be treated as low-confidence pending corroboration.

Action Checklist

1. Step 1: Awareness. Flag this incident to your threat intelligence team for tracking. Assign an analyst to monitor for corroborating reporting from CISA, MITRE, or established threat intelligence vendors before actioning specific IOCs.
2. Step 2: Detection. If any infrastructure indicators from the leaked data become available through corroborated sources, run them against firewall logs, DNS query logs, and proxy logs. Query for connections to any newly published C2 domains or IPs attributed to 0APT or KryBit. Do not action IOCs sourced solely from the single Dark Reading article without verification.
3. Step 3: Eradication. No specific patch or configuration remediation applies. If corroborated IOCs match activity in your environment, isolate affected hosts, revoke any potentially compromised credentials (T1078), and block identified C2 endpoints at the perimeter.
4. Step 4: Recovery. If exposure is confirmed, validate endpoint integrity, review authentication logs for Valid Accounts abuse (T1078), and confirm backup integrity given the Data Encrypted for Impact (T1486) technique profile associated with these actors.
5. Step 5: Post-Incident. Use this event to test your ransomware playbook against the MITRE techniques mapped here. Validate that your detection stack covers T1584 (infrastructure compromise) and T1583 (acquired infrastructure), two techniques that are commonly under-detected in enterprise environments.

IR / Forensic Enrichment

Triage Priority	DEFERRED
Escalation Criteria	Escalate from deferred to urgent if a corroborating source (CISA advisory, MITRE ATT&CK Group entry, or established TI vendor report) publishes IOCs that match hits in your firewall, DNS, or proxy logs from the past 90 days, or if your environment shows any indicator of T1486 (Data Encrypted for Impact) or T1490 (Inhibit System Recovery) activity coinciding with the 0APT or KryBit dwell window.
Recovery Notes	If exposure to 0APT or KryBit infrastructure is confirmed, prioritize VSS and backup integrity validation before any restore operation, as ransomware operators using T1490 routinely destroy shadow copies to maximize impact. Monitor authentication logs (Windows Event IDs 4624, 4648; Linux /var/log/auth.log) for at least 30 days post-remediation for recurrence of T1078 Valid Accounts abuse, as credential reuse from a prior compromise is a common ransomware re-entry vector. Retain all collected forensic artifacts (memory images, log exports, network captures) for a minimum of 90 days in case corroborating intelligence later establishes a longer dwell period requiring scope revision.

Forensic Artifacts	DNS recursive query logs from internal resolvers: search for lookups to 0APT or KryBit C2 hostnames published in corroborated threat intelligence; ransomware actors using T1583/T1584 infrastructure typically use algorithmically generated or bulletproof-hosted domains resolvable only during active campaign windows. | Windows Security Event Log Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Use): scope to accounts active on any host that made outbound connections to flagged IPs, covering 90 days prior to detection — T1078 Valid Accounts abuse is a primary initial access and lateral movement technique for both 0APT and KryBit based on the technique profile in this advisory. | Volume Shadow Copy inventory (vssadmin list shadows output): deletion of VSS snapshots is a near-universal indicator of ransomware pre-encryption staging (T1490 Inhibit System Recovery); absence of expected snapshots on affected hosts is itself a forensic artifact. | Perimeter firewall session logs and NetFlow/IPFIX records: look for periodic outbound connections (beaconing) at fixed intervals to IPs in hosting ranges associated with leaked 0APT or KryBit infrastructure; beaconing cadence analysis in Wireshark or Zeek is achievable without SIEM for a 2-person team. | Scheduled tasks and registry run keys: export schtasks /query /fo CSV /v output and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run from affected hosts — ransomware operators commonly install persistence via these mechanisms during the staging phase before encryption is triggered (T1053.005 Scheduled Task, T1547.001 Registry Run Keys).

Per-Action IR Details

Step 1: Awareness — Flag this incident to your threat intelligence team for tracking. Assign an analyst to monitor for corroborating reporting from CISA, MITRE, or established threat intelligence vendors before actioning specific IOCs.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and threat intelligence intake processes

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Create a tracking ticket or shared document capturing the Dark Reading article URL, date, threat actor names (0APT, KryBit), and a confidence rating of LOW (single uncorroborated source). Set a recurring 48-hour check against CISA Known Exploited Vulnerabilities catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog), MITRE ATT&CK Group pages, and free threat intel feeds such as AlienVault OTX (otx.alienvault.com) filtered by 0APT or KryBit tags. Assign one analyst as DRI; document check-ins in the ticket.

Evidence: Before this step, capture the current state of your threat intel intake pipeline: screenshot or export any existing watchlist entries for 0APT or KryBit in your TIP or tracking system; note which IOC feeds your team currently subscribes to; and document the timestamp of first awareness so dwell-time calculations remain accurate if corroborated IOCs later match historical traffic.

Step 2: Detection — If any infrastructure indicators from the leaked data become available through corroborated sources, run them against firewall logs, DNS query logs, and proxy logs. Query for connections to any newly published C2 domains or IPs attributed to 0APT or KryBit. Do not action IOCs sourced solely from the single Dark Reading article without verification.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlating indicators across log sources and validating before escalation

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

Compensating: Once IOCs are corroborated, run the following on a Linux log aggregation host: grep -Ff iocs.txt /var/log/named/queries.log for DNS hits; grep -Ff iocs.txt /var/log/squid/access.log for proxy hits; and grep -Ff iocs.txt /var/log/firewall/traffic.log for perimeter hits (adjust paths to your distro). On Windows, query DNS debug logs at C:\Windows\System32\dns\dns.log using Select-String -Path 'C:\Windows\System32\dns\dns.log' -Pattern ''. Use Zeek or Wireshark PCAP replay to scan for beaconing patterns (periodic outbound connections at fixed intervals) characteristic of the C2 infrastructure leaked in this incident. Sigma rule category: network_connection to known-bad IP ranges.

Evidence: Before querying, preserve and hash (SHA-256) the following log files to maintain forensic integrity per NIST AU-9 (Protection of Audit Information): perimeter firewall session logs covering the past 90 days (ransomware actors may have pre-positioned weeks prior), DNS recursive query logs from your internal resolver showing any lookups matching 0APT or KryBit C2 hostnames, proxy or web gateway logs showing CONNECT or GET requests to suspicious hosting providers named in the leaked infrastructure data, and NetFlow or IPFIX records if available — these will show beaconing cadence even if payload is encrypted. Document the log collection timestamp before querying so any matches can be scoped to a reliable detection window.

Step 3: Eradication — No specific patch or configuration remediation applies. If corroborated IOCs match activity in your environment, isolate affected hosts, revoke any potentially compromised credentials (T1078), and block identified C2 endpoints at the perimeter.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Removing threat components and eliminating persistence mechanisms

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SI-3 (Malicious Code Protection), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For host isolation without EDR: disconnect the NIC via Device Manager or run netsh interface set interface 'Ethernet' admin=disable on Windows; for Linux use ip link set eth0 down. For credential revocation tied to T1078 (Valid Accounts), run on Active Directory: Disable-ADAccount -Identity for each account that authenticated from the affected host in the 90 days prior. Block corroborated 0APT/KryBit C2 IPs and domains at the perimeter firewall using an explicit DENY rule, and add them to your DNS RPZ (Response Policy Zone) if running BIND or Windows DNS. Document every blocked IOC with the corroboration source and timestamp.

Evidence: Before isolating hosts, collect full memory images using open-source tools (WinPmem for Windows, LiME for Linux) to preserve in-memory indicators of 0APT or KryBit tooling — ransomware staging artifacts, injected shellcode, and C2 callback threads are volatile and lost on reboot. Capture a full process list (Get-Process | Export-Csv on Windows; ps auxf > processes.txt on Linux), active network connections (netstat -anob > netstat.txt on Windows; ss -antp > netstat.txt on Linux), and scheduled tasks (schtasks /query /fo CSV /v > tasks.csv on Windows; crontab -l and /etc/cron.d/ on Linux) before any remediation action. These artifacts will show whether 0APT or KryBit persistence mechanisms (common ransomware TTPs: scheduled tasks, service installs, registry run keys at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) are present.

Step 4: Recovery — If exposure is confirmed, validate endpoint integrity, review authentication logs for Valid Accounts abuse (T1078), and confirm backup integrity given the Data Encrypted for Impact (T1486) technique profile associated with these actors.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restoring systems, verifying integrity, and confirming threat has been removed

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), NIST AU-3 (Content of Audit Records), CIS 3.4 (Enforce Data Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Validate endpoint integrity using Sysinternals Sigcheck (sigcheck -tv -vt c:\windows\system32\) to identify unsigned or tampered binaries that 0APT or KryBit tooling may have dropped. For backup integrity validation, compute SHA-256 hashes of backup catalog files and compare against pre-incident baselines before attempting any

restore — ransomware actors using T1486 frequently target VSS (Volume Shadow Copies); verify VSS health with vssadmin list shadows on Windows. For T1078 authentication review, query Windows Security Event Log for Event ID 4624 (Successful Logon) and Event ID 4648 (Explicit Credential Use) filtered to accounts active on isolated hosts in the 90-day window preceding detection. On Linux, review /var/log/auth.log or /var/log/secure for sudo escalations and SSH logins from unexpected source IPs.

Evidence: Before restoring from backup, document the current state of all VSS snapshots (vssadmin list shadows > vss_inventory.txt) and verify they have not been deleted (a T1490 — Inhibit System Recovery indicator common to ransomware operators). Export Windows Security Event Log (Event IDs 4624, 4625, 4648, 4688, 4698) for the affected hosts covering the full suspected dwell period; these logs establish the authentication and execution timeline needed to scope credential revocation. Hash and archive these exports before restoration wipes them.

Step 5: Post-Incident — Use this event to test your ransomware playbook against the MITRE techniques mapped here. Validate that your detection stack covers T1584 (infrastructure compromise) and T1583 (acquired infrastructure) — two techniques that are commonly under-detected in enterprise environments.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, detection improvement, and intelligence sharing

Controls: NIST IR-4 (Incident Handling), NIST IR-3 (Incident Response Testing), NIST IR-8 (Incident Response Plan), NIST SI-4 (System Monitoring), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Run a tabletop exercise scoped to the 0APT/KryBit TTP profile: T1583 (Acquired Infrastructure), T1584 (Compromise Infrastructure), T1078 (Valid Accounts), T1486 (Data Encrypted for Impact), and T1490 (Inhibit System Recovery). Use free Sigma rules from the SigmaHQ repository (github.com/SigmaHQ/sigma) — search for rules covering proc_creation and net_connection categories mapped to ransomware staging. Deploy or tune Sysmon using the SwiftOnSecurity config (github.com/SwiftOnSecurity/sysmon-config) to ensure Event ID 3 (Network Connection) captures outbound connections to newly identified C2 infrastructure. Document detection gaps identified during the tabletop and assign owners with remediation timelines.

Evidence: Compile a post-incident artifact package before closing the ticket: the full IOC list with confidence ratings and corroboration sources, log query outputs from Step 2, account activity exports from Step 4, and a MITRE ATT&CK Navigator layer (https://mitre-attack.github.io/attack-navigator/) annotated with techniques observed or suspected in this incident. This package serves as the baseline for measuring detection improvement after playbook updates, and supports intelligence sharing with sector ISACs if 0APT or KryBit activity is later confirmed in your environment.

Detection Guidance

No verified IOCs are available from authoritative sources at this time. If corroborated C2 indicators are published by CISA or credible threat intelligence vendors, query DNS logs for resolution of associated domains, firewall logs for outbound connections to associated IPs, and EDR telemetry for process behavior consistent with T1486 (mass file writes, rapid file extension changes, backup or system file deletion) or T1078 (credential use from atypical endpoints or times). Monitor CISA's Known Exploited Vulnerabilities catalog and MITRE ATT&CK for any updates attributing specific infrastructure to 0APT or KryBit. Until corroboration exists, treat any published IOCs from this incident as low-confidence and verify before blocking to avoid false positives.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	[not available — no verified IOCs published by authoritative sources at this time]	Leaked C2 infrastructure from 0APT/KryBit conflict — awaiting corroboration before actionable IOCs can be reported	LOW

Framework Mappings

MITRE-ATTACK

- **T1591** — Gather Victim Org Information
- **T1584** — Compromise Infrastructure
- **T1566** — Phishing
- **T1583** — Acquire Infrastructure
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1590** — Gather Victim Network Information

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1591	Gather Victim Org Information	Reconnaissance
T1584	Compromise Infrastructure	Resource-Development
T1566	Phishing	Initial-Access
T1583	Acquire Infrastructure	Resource-Development
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1590	Gather Victim Network Information	Reconnaissance

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/threat-intelligence/feuding-ransomware-...	T3
Is it legal to find a vulnerability and report it, but not exploit it? - Reddit	https://www.reddit.com/r/hacking/comments/124u784/is_it_legal_to_fi...	T3
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
Why Most Vulnerabilities Are Never Disclosed | Caleb Fenton's Blog	https://calebfenton.github.io/2016/04/29/why-most-vulnerabilities-a...	T3
Known, non-critical, security vulnerability re: verification of host keys	https://github.com/capistrano/capistrano/issues/1896	T3

Generated 2026-04-29 06:53 UTC by TJS Security Command Center