INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-05 06:17 UTC

Encryption-Free Extortion: How Kairos Extracted $1 Million from a U.S. County Government Using Data Alone

THREAT CAMPAIGN | HIGH | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0620
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Union County, Ohio (U.S. government entity); no specific software products identified; initial access via password guessing against accounts lacking MFA; temp.sh used as exfiltration staging service
Published	2026-07-04T08:47:53
Discovery Source	Rss

Executive Summary

A threat actor identified as Kairos breached Union County, Ohio's systems by guessing passwords on accounts without multi-factor authentication, exfiltrating over 2 terabytes of sensitive government records without deploying ransomware. The county paid approximately $1 million USD in bitcoin under threat of public data release, receiving only a non-enforceable deletion promise in return. This incident demonstrates that encryption is no longer a prerequisite for extortion, and that weak authentication controls alone can produce eight-figure financial and reputational consequences for public-sector organizations.

Technical Analysis

Kairos conducted a data-theft extortion operation against Union County, Ohio using credential guessing (T1110) against accounts lacking MFA as the initial access vector, exploiting weak password requirements (CWE-521) and absent or insufficient authentication controls (CWE-308). No ransomware or encryption component was deployed. Following access, the actor staged over 2 TB of exfiltrated records (T1074) and transferred data to temp.sh, a public file-hosting service, via T1567.002 (Exfiltration to Cloud Storage). The payment of approximately $1 million USD in bitcoin was traced through exchanges Bybit and OKX before routing to BELQI, a Russia-linked cryptocurrency service, within hours of receipt, per blockchain analysis reported by The Hacker News. The county received a non-enforceable 'proof of deletion' document with no verifiable assurance of

destruction. No CVE is associated with this campaign; the attack relied entirely on authentication control failures (CWE-308, CWE-521, CWE-284). This incident aligns with a 2025 Sophos finding, cited in source reporting, that fewer than half of ransomware-affiliated attacks now involve encryption, the lowest rate recorded in six years.

Action Checklist

1. Step 1: Containment. Audit all externally accessible accounts immediately; enforce MFA on every account with remote access (CIS 6.3, CIS 6.4, CIS 6.5, NIST AC-17). Identify and disable any accounts showing anomalous authentication patterns. Block outbound connections to temp.sh at the perimeter firewall (NIST AC-4).
2. Step 2: Detection. Review authentication logs for credential-guessing patterns: high-volume failed logon events followed by a single success from unfamiliar IPs or geolocations (NIST AU-2, AU-6). Query DNS and proxy logs for connections to temp.sh or other ephemeral file-staging services. Look for large-volume outbound data transfers, particularly to unapproved cloud storage endpoints. Apply local account monitoring to flag accounts with sudden access to broad file shares.
3. Step 3: Eradication. Reset credentials on all accounts that were accessible without MFA (NIST IA-4, CIS 5.2). Enforce a password policy that rejects weak or previously breached passwords (CWE-521 remediation). Implement MFA across all remote-access pathways (CIS 6.3, 6.4, 6.5, NIST IA-2). Apply network segmentation to limit lateral access to sensitive record stores (CWE-284 remediation, NIST AC-4, CIS 3.3).
4. Step 4: Recovery. Validate that MFA enforcement is confirmed active on all external-facing accounts before restoring normal operations. Monitor authentication events continuously for at least 30 days post-remediation (NIST AU-6, CIS 8.2). Confirm no residual staging data remains accessible on temp.sh or similar services. Engage legal counsel and relevant government notification authorities; the deletion assurance received is non-enforceable and does not confirm data destruction.
5. Step 5: Post-Incident. Conduct a full access control review: identify all accounts, classify by privilege level, and enforce least privilege (NIST AC-6, CIS 5.4). Establish a documented vulnerability and remediation management process covering authentication hygiene (CIS 7.1, 7.2). Review data inventory to determine the full scope of what was accessible from compromised accounts (CIS 3.2). Brief leadership on the encryption-free extortion model; existing ransomware playbooks may not account for data-theft-only scenarios, and incident response plans should be updated accordingly.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if any account compromise is confirmed on systems holding PII, PHI, or CJIS-regulated data, or if evidence of active exfiltration to temp.sh or similar staging services is found in live network traffic — U.S. state breach notification laws and potentially federal CJIS obligations are triggered by confirmed unauthorized access to such records, and the non-enforceable deletion assurance from Kairos does not satisfy any regulatory safe harbor.

Recovery Notes	Before restoring any externally accessible service, generate a complete MFA-enrollment attestation report confirming zero accounts with remote-access capability remain unenrolled — this was the single exploitable condition Kairos leveraged. Monitor Windows Security Event Log for Event ID 4625 anomalies and firewall egress logs for connections to ephemeral file-staging domains (not only temp.sh, but also file.io, gofile.io, and similar services) for a minimum of 30 days, as Kairos or affiliated actors may reattempt access under the assumption that remediation was incomplete. Because the exfiltrated 2 TB of county records is confirmed outside organizational control regardless of the deletion promise, ongoing monitoring for public data releases on leak sites associated with Kairos should be assigned to a threat intelligence function or a designated analyst using Google Alerts and dark-web monitoring appropriate to the organization's budget.
Forensic Artifacts	Windows Security Event Log — Event ID 4625 (Failed Logon) and 4624 (Successful Logon) sequences on all internet-facing systems, specifically filtered on Logon Type 3 (Network) and Type 10 (RemoteInteractive), showing high-volume failure bursts converging to a single success from an external IP not previously seen in authentication history — this is the direct forensic signature of Kairos's password-guessing initial access method. | Firewall and proxy egress logs — HTTP/HTTPS sessions to temp.sh (and its underlying IP range), particularly large-body POST or PUT requests indicating staged upload; total egress volume to this domain should approximate the claimed 2 TB exfiltration and provides the most direct evidence of data-theft scope. | Windows DNS debug log or recursive resolver syslog — DNS queries for temp.sh resolved from internal hosts, timestamped to correlate with post-authentication activity; establishes which internal host(s) performed the staging upload and narrows the set of systems requiring forensic imaging. | Windows Security Event ID 4663 (An attempt was made to access an object) and 4656 (A handle to an object was requested) from file servers hosting sensitive county records — filtered on the compromised account's SID, these events reconstruct exactly which files and directories were accessed during the exfiltration window and determine the regulatory scope of the breach. | Active Directory replication metadata and admin account creation audit (Event ID 4720 — A user account was created; Event ID 4728 — A member was added to a security-enabled global group) — confirms whether Kairos established persistence or additional accounts beyond the initially guessed credential, which would indicate a dwell period longer than the county detected.

Per-Action IR Details

Step 1: Containment — Audit all externally accessible accounts immediately; enforce MFA on every account with remote access (CIS 6.3, CIS 6.4, CIS 6.5 — NIST AC-17). Identify and disable any accounts showing anomalous authentication patterns. Block outbound connections to temp.sh at the perimeter firewall (NIST AC-4).

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Export Active Directory authentication events using `Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet | Export-Csv` to identify stale accounts. Block temp.sh (and its ASN if a budget firewall lacks domain-blocking) via a deny rule on pfSense or Windows Defender Firewall using `netsh advfirewall firewall add rule name='Block temp.sh' dir=out action=block remoteip=`. Enable Windows account lockout policy via Group Policy (Account Lockout Threshold: 5 attempts) as an emergency credential-guessing brake.

Evidence: BEFORE disabling any account or blocking outbound traffic: capture Windows Security Event Log Event ID 4624 (Successful Logon) and 4625 (Failed Logon) filtered on Logon Type 10 (RemoteInteractive) and Type 3

(Network) for the 90 days preceding discovery, preserving the full sequence of high-volume 4625 failures converging to a 4624 success from an unfamiliar IP — this sequence is the forensic fingerprint of Kairos's password-guessing entry. Also capture live `netstat -ano` output and DNS resolver cache (`ipconfig /displaydns`) on any suspected entry-point hosts before blocking to confirm active or recent temp.sh connections.

Step 2: Detection — Review authentication logs for credential-guessing patterns: high-volume failed logon events followed by a single success from unfamiliar IPs or geolocations (NIST AU-2, AU-6). Query DNS and proxy logs for connections to temp.sh or other ephemeral file-staging services. Look for large-volume outbound data transfers, particularly to unapproved cloud storage endpoints. Apply D3-LAM (Local Account Monitoring) to flag accounts with sudden access to broad file shares.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Run this PowerShell one-liner against exported Security logs to surface the guessing pattern: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625} | Group-Object {$_.Properties[19].Value} | Where-Object {$_.Count -gt 20} | Sort-Object Count -Descending`. For DNS, parse Windows DNS debug log or pfSense DNS resolver log with `grep -i 'temp.sh' /var/log/resolver.log`. Detect bulk file access without a SIEM by enabling object access auditing on sensitive file shares (Group Policy → Audit Object Access) and parsing Event ID 4663 for a single account accessing >500 distinct objects within a short window using `Get-WinEvent` filtering.

Evidence: Collect before any account action: DNS query logs showing resolution of temp.sh (Windows DNS debug log at `%SystemRoot%\System32\dns\dns.log` if enabled, or firewall syslog); proxy/firewall egress logs showing HTTP POST or PUT to temp.sh with large Content-Length headers indicating staged upload of the 2 TB exfiltration; Windows Security Event ID 4663 (Object Access) and 4656 (Handle Request) from file servers hosting sensitive county records, filtered on the compromised account — these will show the breadth of files touched prior to exfiltration. Capture all logs to write-protected offline storage before any remediation alters the host state.

Step 3: Eradication — Reset credentials on all accounts that were accessible without MFA (NIST IA controls, CIS 5.2, D3-CRO). Enforce a password policy that rejects weak or previously breached passwords (CWE-521 remediation). Implement MFA across all remote-access pathways (CIS 6.3, 6.4, 6.5, D3-MFA). Apply network segmentation to limit lateral access to sensitive record stores (CWE-284 remediation, NIST AC-4, CIS 3.3).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-4 (Information Flow Enforcement), CIS 5.2 (Use Unique Passwords), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Perform bulk credential resets via `Set-ADAccountPassword` in a PowerShell loop against an exported list of all accounts with Logon Type 10 capability. Integrate Have I Been Pwned's Pwned Passwords API (free, k-anonymity model) into a custom password filter DLL or validate new passwords against the downloadable hash list offline using `$hash = (Get-FileHash -InputStream ([System.IO.MemoryStream]::new([System.Text.Encoding]::UTF8.GetBytes($pwd))) -Algorithm SHA1).Hash` before committing resets. Implement Windows Firewall rules on file-server hosts using `New-NetFirewallRule` to restrict SMB (TCP 445) inbound access to only designated workstation subnets, reducing lateral reach to sensitive record stores without enterprise NAC.

Evidence: BEFORE resetting any credentials: acquire a memory image of any host confirmed to have been accessed by the compromised account using WinPmem (free) or `procdump -ma` on relevant processes, preserving any attacker tooling or staging utilities that may have been run interactively. Capture `quser` and `query session` output on all Remote Desktop-capable servers to document any active or disconnected sessions under the compromised account. Export the full Kerberos ticket cache (`klist`) and NTLM authentication table before invalidating credentials, as these may show lateral movement paths the attacker used after initial password-guess success.

Step 4: Recovery — Validate that MFA enforcement is confirmed active on all external-facing accounts before restoring normal operations. Monitor authentication events continuously for at least 30 days post-remediation (NIST AU-6, CIS 8.2). Confirm no residual staging data remains accessible on temp.sh or similar services. Engage legal counsel and relevant government notification authorities — the deletion assurance received is non-enforceable and does not confirm data destruction.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Verify MFA enrollment completeness by running `Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0}` (Microsoft 365) or querying your IdP's API for unenrolled users before declaring recovery complete. Set a scheduled task or cron job to run the Event ID 4625/4624 pattern query daily for 30 days and email results to the IR team. Use CanaryTokens (free, canarytokens.org) placed in previously accessed sensitive directories — if the attacker retained a copy of files and attempts to open them, you receive an alert, providing partial evidence against the non-enforceable deletion claim.

Evidence: No live-state alteration occurs in this phase beyond re-enabling services, but before restoring any system to production: validate integrity of authentication infrastructure by reviewing AD replication metadata (`repadmin /showrepl`) and confirming no unauthorized admin accounts were created during the breach window using `Get-ADUser -Filter {adminCount -eq 1} -Properties whenCreated | Where-Object {$_.whenCreated -gt [datetime]"}`. Retain all firewall egress logs showing temp.sh connections as legal evidence in anticipation of regulatory notification obligations under applicable state breach notification law.

Step 5: Post-Incident — Conduct a full access control review: identify all accounts, classify by privilege level, and enforce least privilege (NIST AC-6, CIS 5.4). Establish a documented vulnerability and remediation management process covering authentication hygiene (CIS 7.1, 7.2). Review data inventory to determine the full scope of what was accessible from compromised accounts (CIS 3.2). Brief leadership on the encryption-free extortion model — existing ransomware playbooks may not account for data-theft-only scenarios, and incident response plans should be updated accordingly.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Generate a privilege-tier map using `Get-ADGroupMember 'Domain Admins' -Recursive` and `Get-ADUser -Filter * -Properties MemberOf` exported to CSV, then audit which accounts had file-share access to sensitive county record repositories by parsing Event ID 4663 history. Draft a data-theft-only extortion playbook addendum using the NIST 800-61r3 §4 lessons-learned template, explicitly adding decision gates for: (1) no encryption present but data confirmed exfiltrated, (2) ransom demand received, (3) legal hold triggered — this gap in existing ransomware playbooks was a direct contributor to Union County's $1M payment outcome.

Evidence: No volatile evidence capture required in post-incident phase; focus on preserved log sets. Assemble the complete forensic timeline from: Windows Security Event Log 4625/4624 sequences establishing the credential-guessing entry window; Event ID 4663 records showing which file shares and records were accessed under the compromised account; firewall egress logs confirming the temp.sh upload sessions and approximate data volume; and any email or communication records related to the extortion demand and bitcoin payment, which are material to legal proceedings and regulatory notifications.

Detection Guidance

Query authentication infrastructure (Active Directory, Azure AD, Okta, or equivalent) for accounts that experienced more than a threshold number of failed logon attempts followed by a successful login within a short window, particularly from IPs not previously associated with the account (NIST AU-2, AU-3, AU-6). Flag any successful logins from accounts lacking MFA enrollment. Monitor DNS resolution and proxy logs for requests to temp.sh; any outbound connection to this domain warrants immediate investigation. Alert on outbound data transfer volumes exceeding baseline thresholds, especially to ephemeral or consumer file-hosting services. Apply local account monitoring to detect sudden, broad file-share access by accounts not normally accessing those stores. Review firewall egress logs for sustained large-volume uploads to cloud storage endpoints not on an approved list (T1567.002 indicator). IOC: temp.sh as a staging domain; Bybit and OKX as cryptocurrency exchange endpoints in financial transaction logs if applicable.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`temp.sh`	Public file-staging service used by Kairos to host exfiltrated data prior to threatened public release	HIGH

Framework Mappings

MITRE-ATTACK

- **T1657** — Financial Theft
- **T1531** — Account Access Removal
- **T1537** — Transfer Data to Cloud Account
- **T1567.002** — Exfiltration to Cloud Storage
- **T1074** — Data Staged
- **T1489** — Service Stop
- **T1110** — Brute Force
- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **AC-7** — Unsuccessful Logon Attempts
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CA-7** — Continuous Monitoring

- **SC-7** — Boundary Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

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
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1531	Account Access Removal	Impact
T1537	Transfer Data to Cloud Account	Exfiltration
T1567.002	Exfiltration to Cloud Storage	Exfiltration

Technique ID	Technique Name	Tactic
T1074	Data Staged	Collection
T1489	Service Stop	Impact
T1110	Brute Force	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/us-government-entity-paid-kairos-...	T2
Data Staged, Technique T1074 - Enterprise - MITRE ATT&CK®	https://attack.mitre.org/techniques/T1074/	T1
What Is Data Exfiltration? MITRE ATT&CK® Exfiltration Tactic | TA0010	https://socprime.com/blog/what-is-data-exfiltration-mitre-attack/	T3
Defending against data exfiltration threats - ITSM.40.110 - Cyber.gc.ca	https://www.cyber.gc.ca/en/guidance/defending-against-data-exfiltra...	T1
Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and ...	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-250a	T1

Generated 2026-07-05 06:17 UTC by TJS Security Command Center